Proceedings of the 1st Blockchain and Cryptocurrency Conference (B2C' 2022)

9-11 November 2022
Barcelona, Spain

Edited by Sergey Y. Yurish

Sergey Y. Yurish, *Editor*
B2C' 2022 Conference Proceedings

E-mail (for orders and customer service enquires): ifsa.books@sensorsportal.com

Visit our Home Page on http://www.sensorsportal.com

e-ISBN: 978-84-09-45763-2
BN-20221105-XX
BIC: UNKD

Contents

Foreword

On behalf of the B2C' 2022 Organizing Committee, I introduce with pleasure these proceedings devoted to contributions from the inaugural Blockchain and Cryptocurrency Conference (B2C' 2022), 9-11 November 2022.

Blockchain and cryptocurrencies are now topics of substantial impact that society needs to contemplate, exploit and adopt. According to the recent market study, the Blockchain Technologies Market value was $ US 4.9 billion in 2021 and projected to reach $ US 67.4 billion by 2026, at a Compound Annual Growth Rate (CAGR) of 68.4 % during the forecast period. The major driving factors contributing to the high growth rate of Blockchain Market include increasing venture capital funding and investment in blockchain technology; extensive use of blockchain solutions in banking and cybersecurity; high adoption of blockchain solutions for payment, smart contracts, and digital identities; and rising government initiatives. The main restrictions of the market growing is uncertain regulatory, compliance environment luck of skilled professionals. The main goal of the B2C' 2022 conference is to decrease significantly, and to help eliminate completely in the future, the mentioned above restraints.

The first Blockchain and Cryptocurrency Conference (B2C' 2022) aims to provide a forum for researchers, scientists, engineers, and students from both the industry and the academia to present their latest research findings, advances and innovations on blockchain technologies as well as to helps decision-makers, technologists, and developers understand the value of blockchain to their businesses regardless of industry.

It will feature keynotes, peer-reviewed technical paper presentations, companies, startups, solution vendors, research institutes, open-source projects, and academia. The event will be also the forum for exchange of the latest innovation results, regulations, policies, standards, and applications in this exciting and challenging area.

Unlike existing, narrowly focused technical conferences and commercial trade events, the B2C' 2022 will cover all technical and social aspects of blockchain and cryptocurrency. In addition, startups, working in this area will be able to present their pitch decks during the event.

The inauguration B2C' 2022 is organized and sponsored by IFSA - the non-profit professional association serving for industry and academy more than 20 years, together with their media partners *IFSA Publishing, Eco IFSA, Inveready, Coinpedia Fintech News, Coin Gape and CryptoCoin News*.

Prof., Dr. Sergey Y. Yurish
B2C' 2022 Chairman

(Keynote Presentation)

Private Datapods and the Future Web 3.0 Do Not Automatically Mean Blockchain

Stephen Castell
CITP CPhys FIMA MEWI MIoD, CASTELL Consulting
PO Box 334, Witham, Essex CM8 3LP, UK
Tel: +44 1621 891 776, Mob: +44 7831 349 162
PO Box 270529, San Diego, CA 92198, USA
Tel: +1 310-890-9859
E-mail: stephen@castellconsulting.com
http://www.e-expertwitness.co.uk
https://archivesit.org.uk/interviews/stephen-castell/

1. Introduction

In my recent paper [1]:

- I articulated a clarification of the characteristics of Sir Tim Berners-Lee's ***Web 3.0***, noting that ICT and blockchain professionals must be careful not to equate Web 3.0 automatically with blockchain, or *vice versa* – that would be an incorrect equivalence. Blockchain is certainly one possible architecture on which to base a Web 3.0 implementation. However, the essence of Sir Tim Berners-Lee's Web 3.0 concept is nothing automatically or implicitly to do with blockchain, but in my view, is, rather, focused on the important idea of ***Private Datapods***. [2]
- I described the architecture and future development of my own invention, Zykme / ZykPass, an available working hybrid App (beta test version) compliant with this Web 3.0 Private Datapod fundamental principle, ushering-in a new era of user-controlled and user-owned 'social media' based on secure P2P personal data communications, implemented using edge computing.
- I further noted that this includes potential addition of a future blockchain-based 'social media' ***ZykToken***, awarded to, and owned and tradeable by, each Zykme / ZykPass user, implementing my novel ***CapChere*** (Customer Corporation) IP and business ownership structure.

With the addition of this blockchain-based 'social media' ZykToken, implementation of CapChere contends to be an example of a new breed of *Decentralized Social Networks* **[3]**, and, uniquely, one that offers a transformative, socially useful re-purposing of traditional industrial capitalism, in which 'all are winners'.

In this presentation:

- I demonstrate my patentable Zykme / ZykPass invention, available and offering secure one-time-code instant P2P communication, using edge computing.
- I elaborate on the future development through the ZykToken and CapChere models of a socially useful, transformative re-purposing of traditional capitalism.

Finally, for those who could perhaps be interested in partnering with this Web 3.0 innovation, I give an outline of the Zykme Business Plan.

2. Web 3.0 and Private Datapods

To recap and remind: the Web 3.0 principles as put forward by its proposer, Sir Tim Berners-Lee, in my view mean, above all, P2P **Private Datapods**, the systems architecture for delivery and operation of which fundamentally *does not automatically mean blockchain*.

It should be also be noted that the same caveat goes for the much talked-about 'Metaverse', discussion of which often seems to assume automatic equivalence of the terminology 'Metaverse' with both Web 3.0 and use of blockchain. This, too, is a false equivalence – for example, see the links given at [4].

With this understanding accepted, it is equally true that much active effort and investment is going into Web 3.0 (or 'Web3') projects that *do* utilise the decentralization architecture of blockchain. A summary of both these distinct 'truths' is given in the 2022 article by Selig, underscoring and re-confirming overall the significant features of Web 3.0 [5]:

"In Web 3.0, data is stored securely and distributed across many devices, removing the need for centralized servers. Such a design also reduces the risks of massive data leaks because data is no longer centrally stored … If you look for a Web 3.0 definition you probably won't find a clear and unique explanation. … Web 3.0 is highly decentralized … The result is real-world human communication. Users retain control over their data and content, and they can sell or trade their data without losing ownership, risking privacy or relying on intermediaries. … Key to the innovation in Web 3.0 is the digitization of assets via tokenization. …".

With conception, development and prototyping commencing back in 2015-2016, my own invention, Zykme / ZykPass is, I contend, compliant with these features:

- Data is stored securely and distributed across many user devices and platforms, removing the need for centralized servers;
- The design reduces the risks of data leaks because data is no longer centrally stored, making it more resilient – indeed impervious – to compromise;
- Its patentable proprietary one-time code data transfer protocol results in real-world, real-time P2P secure human communication;
- Users retain control over their data and content; and
- Users can sell or trade their data without losing ownership, risking privacy or relying on intermediaries.

3. Presentation of Zykme / ZykPass: Live Demonstration of its Operation

In my recent paper [1], there is given a full explanatory description of the operation of Zykme by way of a screen-by-screen, step-by-step detailed User Guide to Zykpass, the special version of Zykme developed for the use case of a Vaccination or Test Certificate 'Passport'.

At this conference, with, I trust, the active participation and interaction of any/all of those here attending my keynote presentation, I actively demonstrate, live, the operational functionality and Web 3.0 Private Datapod-compliant features of my Zykme / Zykpass invention.

<< Live demonstration of Zykme >>.

5. Adding the Zyktoken, and CapChere: re-fashioning industrial capitalism

"Nothing is more powerful than an idea whose time has come" and I suggest that one such potentially powerful idea contender is my Zykme / ZykPass hybrid App Web invention. To recapitulate: Zykme does not require or encompass any blockchain architecture or component in its fundamental functioning. Zykme is a unique P2P secure 'social communications media', whose algorithms are implemented using wholly-on-platform, device-resident (e.g. smartphone) *edge computing*, with no private or personal user data being recorded, held, processed or analysed remotely. Its essential patentable proprietary P2P secure one-time code data transfer protocol uses neither a blockchain nor any other third-party centralized or decentralized system, database, repository or ledger.

In the wider social and business media context, the Zykme Private Datapod architecture was nevertheless always conceived as capable of being developed with addition of a blockchain-based 'customer loyalty program' *ZykToken* awarded to, and owned and tradeable by, each Zykme / ZykPass user [6]. This will furthermore allow an implementation of my novel *CapChere* (Customer Corporation) IP and business ownership structure. The objectives of and aspirations for these developments include that they are intended to be a socially useful, transformative re-purposing and re-fashioning of traditional industrial capitalism, in which all are winners [7].

These additional ZykToken and CapChere blockchain developments and objectives have the following important features:

- Each user earns a ZykToken each time they use the Zykme App.
- The ZykToken uniquely creates a new corporate structure whereby ownership of Zykme and its IP becomes more and more spread into and by its users, in accord with my novel *CapChere* (Customer Corporation) construct.

This ZykToken social utility paradigm is consistent also with two other recent innovations:

(1) The *QE2-Coin*, already minted as an Ethereum Token, a Specialized National Utility Token ('SNUT'), targeted at stimulating and expanding the UK affordable homebuilding sector economy [8].

(2) Tokenization of ownership by the People of my conception of the *Genesis Algorithm*, under Direct Government By Algorithm ('GBA'), in tune with my proposed *Algorithmic Compact with the People* [9].

I am working with the innovative team at *Minima* to create *ZykMinima*, an operational *maquette* that adds these features, the Zyktoken, and CapChere, to my basic Zykme App:

https://www.minima.global/

"Welcome to complete decentralization
A cooperative network that enables everyone to freely connect and prosper …
The world's first completely decentralized blockchain
The only blockchain controlled entirely by users
The only blockchain to run in full on a mobile phone …".

6. Zykme Business Plan

The Zykme/ZykMinima Business Plan is potentially a uniquely pioneering business model in the Decentralized Social Networks space. An outline of this Business Plan is as follows (Table 1).

I would be happy to discuss this in more detail, privately and confidentially, with anyone who could be interested in partnering with this Web 3.0 innovation, based on development of this outline Business Plan.

Table 1. Highlights of Zykme/ZykMinima Business Plan: Cash Flow Projections.

Item (Estimates;NB Risk Factors)	**To end Year 0**	**To end Year 1**	**To end Year 5**
App Users			
Number of Users	0	500,000	20,000,000
Number of Zytokens Issued	0	250,000	10,000,000
Valuation of Zytoken per User **(i)** £	0	1.0	8.00
Cash In			
Venture Capital £	10 m First Round		10 m Second Round
Brand Marketing			
Number of Brand Partners	0	2	10
Brand Partner Fees **(ii)** £	0	12 m	90 m
Brand Adtech Commissions £	0	1 m	5 m
Patent Licensing			
Number of Licensees	0	1	5
Fees **(iii)** £	0	0	0.5 m
(a) Total Cash In £	**10 m**	**13 m**	**105.5 m**
Cash Out			
Software & Systems £	0.1 m	0.5 m	2.5 m
Business Development £	0.1 m	1.5 m	5 m
IP Rights Acquisition £	1.5 m	0	0
Patent Development £	0.2 m	1 m	5 m
Admin £	0.1 m	4 m	10 m
Marketing £	0	5 m	50 m
(b) Total Cash Out £	**2.0 m**	**12 m**	**72.5 m**
Net Cash Flow In (a) – (b) £	**8 m**	**1 m**	**33 m**
Cumulative Cash Flow £	**8 m**	**9 m**	**42 m**
Rough Balance Sheet/ Net Asset Profile £			
Cash at Bank **(iv)**	8 m	7.2 m	36.4 m
Patent Valuation	0.5 m	5 m	10 m
Zyktoken 'Share Value' **(v)**	8 m	9.5 m	202 m
Total	**8.5 m**	**21.7 m**	**248.4 m**

Year 6 onwards: Trade Sale at £0.5bn minimum or Stock Exchange Flotation at £2bn market valuation minimum.

Year 8 onwards: Assuming a SE Flotation, Acquisitions to realise a Group Market valuation by **Year 10** of £10bn market valuation minimum.

Notes

(i) Zyktoken valued at £1 at initial issue; value assumed to grow at a rate of 30% pa.
(ii) Each Brand Partner pays £0.5m per month in Year 1, growing to £0.75pm in Year 5.
(iii) Each Patent Licensee pays zero in first year; then £0.1m pa thereafter.
(iv) Assumed net of 20% Corporation Tax charge on Cumulative Cash Flow**.**
(v) Cumulative Cash Flow plus (Number of Users x Valuation of Zytoken per User).

7. References and Background Reading

[1]. Castell, S., Private Datapods: Web 3.0 does not Automatically Mean Blockchain Decentralization, *Studies in Social Science Research*, Vol 3, No 2, 2022, pp. 90-118; Online Published May 27, 2022. http://www.scholink.org/ojs/index.php/sssr/article/view/4849/5689

[2]. https://www.reworked.co/information-management/why-web3-and-web-30-are-not-the-same/#
Why Web3 and Web 3.0 Are Not the Same MARCH 24, 2022 By Siobhan Fagan
Web3 and the Semantic Web
Anyone who has followed the development of the World Wide Web and Tim Berners-Lee's concept for a semantic web will have good reason to be confused. In 2006, the computer scientist — who's also the founder and CTO of tech startup Inrupt — described the semantic web as a component of Web 3.0, which is not the same as Web3 in the crypto context. The Semantic Web is an extension of the World Wide Web through standards set by the World Wide Web Consortium. The goal of the Semantic Web is to make internet data machine-readable. This vision describes a web of linked data-encompassing technologies to enable people to create data stores online, build vocabularies and write rules for handling data. The problem is that in recent discussions about Web 3.0, the terminology has become interchangeable with the term Web3 in the crypto context. That term, Web3, coined in 2014 by Polkadot founder and Ethereum co-founder Gavin Wood, refers to a decentralized online ecosystem based on blockchain. ...

[3]. https://inlea.com/decentralized-social-networks/
What are Decentralized Social Networks? 30/03/2022
In response to the evolution towards Web 3.0, decentralized social networks have arrived as the alternative to traditional social media. It was around 2004 when Web 1.0 (the static web) was completely absorbed by Web 2.0 (the web as a platform). Web 2.0 is the web we know today, which focuses on user-created content (social media and blogs). This content and the corresponding data generated are stored on a centralized server owned by a company, such as Google or Facebook. This way, the power and influence that companies have behind social networks is incalculable. The main criticism towards these is the use of the large amount of data they have as a currency for brand advertising. In response, we are in the midst of the process of evolution towards Web 3.0, an even more intelligent web that will be able to interpret and interconnect a greater number of data, in a decentralized way and without intermediaries. In this article, we explain what decentralized social networks are, how they work, and we list some of the most popular decentralized social networks at the moment: ... Decentralized social networks are those social media that operate on servers that run independently. In other words, they are social networks that are not in the hands of a company, but rather their users make the decisions. ...

[4]. https://www.bloomberg.com/features/2022-the-crypto-story/?sref=PhB3liAe&leadSource=uverify%20wall
The Crypto Story Where it came from, what it all means, and why it still matters. By Matt Levine Featured in Bloomberg Businessweek, Oct. 31, 2022.
... If you're a disciple, this new dimension is the future. If you're a skeptic, this upside-down world is just a modern Ponzi scheme that's going to end badly ... But crypto has dug itself into finance, into technology, and into our heads. And if crypto isn't going away, we'd better attempt to understand it. Which is why we asked the finest finance writer around, Matt Levine of Bloomberg Opinion, to write a cover-to-cover issue of Bloomberg Businessweek ... Joel Weber, Editor, Bloomberg Businessweek ...

https://mixed-news.com/en/meta-halves-targeted-user-base-for-horizon-worlds/
Meta halves targeted user base for Horizon Worlds Oct 16 2022 Matthias Bastian
Meta's proto-metaverse Horizon Worlds is still not going well. In addition, strategic decisions and critical issues keep leaking out, further damaging confidence in Meta's metaverse plans.
Following the leaked, highly critical internal memos from metaverse CEO Vishal Shah, the Wall Street Journal has now also gained access to internal papers with usage data on Horizon Worlds. These are significantly below Meta's self-imposed targets and also around 30 percent below the figures officially communicated in February. ... According to internal documents obtained by the WSJ, Meta wanted to bring half a million active users to Horizon Worlds by the end of the year. That number has now been cut nearly in half, to 280,000. Currently, Horizon Worlds has fewer than 200,000 active users, twice as many of whom are men as women. In February 2022, there was still talk of 300,000 users, but the VR event platform Venues was included here with users who possibly only dialed in once for a heavily advertised Foo Fighters concert. ...

https://www.techtarget.com/whatis/feature/Web3-vs-metaverse-Whats-the-difference
Web3 vs. metaverse: What's the difference? 04 Aug 2022 Buzzwords come and go, but some stick around. Two new terms you may have heard recently -- Web 3.0 and the metaverse -- are frequently used interchangeably, but they are two different technologies. ...

https://www.thecoinrepublic.com/2022/07/05/is-metaverse-well-off-without-blockchain/
... here's the thing, metaverse can be developed without the blockchain technology, in fact, the top two contenders in this race, Apple and Meta, do not use blockchain. So, undoubtedly, the digital realm can be built without this groundbreaker ...

https://www.analyticsvidhya.com/blog/2022/08/how-is-web30-related-to-the-metaverse/
... How do Web 3.0 and Metaverse relate to each other? Web3, the third phase of the World Wide Web's evolution, should not be confused with the Metaverse. ...

https://brave.com/web3/intro-to-blockchain/
... blockchain is a novel system for generating consensus among network participants without a governing authority. Web3, meanwhile, is the decentralized web—where apps, online services, even finance—no longer need a centralized authority. ...

https://www.freethink.com/technology/web-3-vs-metaverse
... Web 3.0 and the metaverse both describe the internet of the future, but they aren't the same thing...

[5]. Selig, J.,. The 8 Defining Features of Web 3.0. Jay Selig, 8 April 2022.
https://www.expert.ai/blog/web-3-0/

[6]. Chris Shalchi, C., Customer Loyalty Blockchain: Ecommerce Shops Take Advantage of Blockchain Rewards Programs, 2018.
https://www.bigcommerce.co.uk/blog/customer-loyalty-blockchain/

https://tokend.io/loyalty/ 'Tokenization solution for Loyalty'

Nebula Ziya, N., How Crypto Tokens Can Be Used In Customer Rewards Programs? October 2020.
https://www.cryptocurrencyguide.org/how-crypto-tokens-can-be-used-in-customer-rewards-programs/

Davies, A., How to Make Blockchain Rewards Program App
https://www.devteam.space/blog/make-your-blockchain-rewards-program-app/

[7]. See the 'Thoughts, quotes testimonials and links' page at: http://www.e-expertwitness.co.uk/newtqtl.html

[8]. Castell, S., At Last a Really Socially Useful Stablecoin: Snut (The Specialized National Utility Token), *Journal of Financial Transformation*, *55*, 202294-99.
https://ideas.repec.org/a/ris/jofitr/1683.html
https://kovan.etherscan.io/token/0xD8d619C5719152482884Af794025d664732F6efd

[9]. Castell, S., Direct Government by Algorithm Towards Establishing and Maintaining Trust when Artificial Intelligence Makes the Law: a New Algorithmic Trust Compact with the People, *Acta Scientific Computer Sciences,* 3, 12, 2021, pp. 04-21.
https://www.actascientific.com/ASCS/ASCS-03-0194.php

Invited Keynote Speaker at the Third Democracy4All: Blockchain And Democracy Conference (D4A 2022), *10-11 November 2022*, Barcelona, Spain: **"Reinventing the Good Governance of Capitalism".** https://www.d4a.io/

Recently published:

Stephen Castell. "New Financial Risks Arising from Digital Finance: Disputes Over Automated Decision Systems and Algorithmic Assessments by ICT Forensic Expert Witnesses". *Acta Scientific Computer Sciences*, Volume 4 Issue 7 - 2022 (Published July 01, 2022): 24-36. https://www.actascientific.com/ASCS-4-7.php https://www.actascientific.com/ASCS/pdf/ASCS-04-0291.pdf
https://scholar.google.com/citations?view_op=list_works&hl=en&hl=en&user=TJHeIBsAAAAJ

https://www.expertpages.com/united-states/san-diego/expert/dr-stephen-castell
https://www.expertwitness.co.uk/articles/journal/in-a-new-survey-a-majority-of-attorneys-and-expert-witnesses-call-for-increased-cryptocurrency-regulation
https://www.jurispro.com/expert/stephen-castell-5169

(001)

Tax Treatment of Cryptocurrencies

Alexander Szívós
University of Pécs, Faculty of Law, Doctoral School, 1. 48-as tér, 7622 Pécs, Hungary
Tel.: + 36306104077
E-mail: szivos.alexander@ajk.pte.hu

Summary: As new technologies transforming the existing financial system, shaping the future of finance into the digital space, the legislator needs to keep pace with the undergoing changes. One of the biggest challenges for policymakers is to face the blockchain revolution, which poses serious risks to the existing financial framework next to the many benefits. Investment in digital assets, such as cryptocurrencies has grown at an incredible rate, with the crypto economy achieving a market capitalization of more than USD 3 trillion at its peak in less than 13 years. A significant size of income from crypto investments remained invisible to tax authorities, which are currently struggling to come to grips with the exponential growth in digital assets. By presenting some of the major efforts and achievements from both global and local perspectives, the study aims to reveal a couple of policy challenges linked to the taxation of cryptocurrency to call attention to the growing need for a uniform regulative environment, especially in the field of taxation.

Keywords: Cryptocurrency, Taxation, Tax evasion, Tax compliance, Transparency

1. Introduction

After the 2007-2008 global financial crisis there was a decline in consumer confidence in the reigning financial regime. The idea came up by the mysterious Satoshi Nakamoto [1] offered a promising alternative for us with a purely peer-to-peer version of electronic cash which allows online payments to be sent directly from one party to another without going through a financial institution. Nakamoto promoted an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. [2] The mentioned construction offers many benefits e.g., by removing layers of administration, the decentralization reduces the cost of payments, especially for cross-border and international transactions. Furthermore, it is also significantly accelerating the speed of transactions. Thanks to the undisputed advantages the scheme has spread all over the world and the cryptocurrency market have become a major factor in today's economy. Although the original concept was to create a digital currency, which is an alternative form of payment, blockchain technology can be used for more than just money. In recent years the investment character dominated the crypto industry. Thus, many investors reached fortunes by trading the most volatile and risky investment in history. [3] However, a large amount of this income has been hidden from tax authorities. [4, 5] Several characteristics of cryptocurrencies are likely to pose novel challenges in tax administrations' efforts to ensure taxpayer compliance.

2. Hypothesis and Methodology

Currently, tax administrations are struggling to come to grips with the exponential growth in digital assets. This has led to a lack of consensus among tax authorities about how to treat them. The tax implications of purchase, ownership, and sale vary widely between jurisdictions. The intermediaries involved in the Crypto-asset market also pose a serious risk and the recent gains in global tax transparency could be gradually eroded. [6] The uncertainty and lack of uniform guidance on the appropriate taxation of cryptocurrency are reducing taxpayer compliance and opening the door for tax evasion activities. To properly support the research hypothesis, the study reveals some of the most common initiatives aiming the centralization. Next to this, the paper also presents some of the local treatments driving to inconsistencies, paving the ground to a comparative analysis.

3. Discussion

The tax treatment of cryptocurrencies varies across the globe. The different legal and tax conditions range from a totally prohibitive legislative environment to liberal, technology supportive solutions. The current ecosystem easily drives contrary interpretations, misconceptions, and unclear definitions from both the authorities' and both taxpayers' sides. Thus, supranational and international organizations like the European Union and the Organisation for Economic Co-operation and Development (hereinafter OECD) have initiated steps toward creating a more uniform environment.

In 2020, the OECD compiled the key taxable stages and events which may occur in a cryptocurrency's "lifecycle". [7] According to this, the first possible taxable event related to a unit of virtual currency arises when it is created. The creation could mean the process of mining via rewards under a proof of work protocol, initial airdrops, or the initial coin offerings of new

tokens. Among the mentioned versions of creation, the tax situation of mining has received the most attention from the tax authorities. [8]

The majority of the taxable events may rise when disposal happens in the cryptocurrency's life. Disposals may occur in exchange for consideration e.g., through exchanges for fiat currency, another virtual currency, or digital asset, or for a good or service – or in a situation without a reciprocal exchange of value e.g., via gift, or inheritance. [9]

Beyond the mentioned events, the mining, exchange, or disposal of cryptocurrencies may also have value added tax (hereinafter VAT) consequences. In contrast with income taxation, countries tend to treat virtual currencies as akin to fiat currencies in the VAT treatment of transactions involving their exchange or disposal. This treatment is in part due to pragmatism, given the consequences of treating these assets as barter transactions, and in the European Union, has been heavily influenced by the Skatteverket versus David Hedqvist case C-264/14 decision of the European Court of Justice. [10] The judgment stated that transactions, which consist of the exchange of traditional currency for units of the 'bitcoin' virtual currency and vice versa, in return for payment of a sum equal to the difference between, on the one hand, the price paid by the operator to purchase the currency and, on the other hand, the price at which he sells that currency to his clients, constitute the supply of services for consideration. The transactions exempt from VAT. [11].

In order to ensure international tax transparency, the OECD published the Common Reporting Standard (hereinafter CRS) [12] in 2014. However, crypto-assets will in most instances not fall within the scope of the CRS, which applies to traditional financial assets and fiat currencies. Even where crypto-assets do fall within the definition of financial assets, they can be owned either directly by individuals in cold wallets or via crypto-asset exchanges that do not have reporting obligations under the CRS, and are therefore unlikely to be reported to tax authorities in a reliable manner.

Recognising the importance of addressing the mentioned tax compliance risks with respect to cryptocurrencies, the OECD developing the Crypto-Asset Reporting Framework (hereinafter CARF), which is designed to ensure the collection and exchange of information on crypto-transactions. The proposal build upon of three main blocks: the rules and commentary that can be transposed into domestic law to collect information from resident crypto-asset intermediaries; a framework of bilateral or multilateral competent authority agreements or arrangements for the automatic exchange of information collected under the CARF with jurisdiction(s) of residence of the crypto-Asset users, based on relevant tax treaties, tax information exchange agreements, or the Convention on Mutual Administrative Assistance in Tax Matters [13]; and technical solutions to support the exchange of data. [14]

For the first time, the European Union brings crypto-assets, crypto-assets issuers and crypto-asset service providers under a regulatory framework. As a part of the larger digital finance package, which aims to develop a European approach that fosters technological development and ensures financial stability and consumer protection, the markets in crypto-assets (hereinafter MiCA) proposal reached a provisional agreement on the way of the adoption procedure. [15] From a taxation perspective, MiCA hopefully provide the legal certainty necessary to determine the taxation rules applicable to crypto-assets across member states by defining the legal status of cryptocurrencies. Furthermore, MiCA is complemented by the proposal of the Commission for the eighth update of the Directive on Administrative Cooperation (hereinafter DAC8) [16], which aims to expand the exchange of information between EU tax authorities, regarding revenues stemming from investments in, or payments with crypto-assets and e-money. [17]

Although the European Union has made significant steps towards ensuring greater tax transparency and removing barriers to the free flow of information, the country-level tax treatments differ widely. On the one hand, there are high-tax countries like Iceland, Austria, Switzerland, Hungary, and Belgium, on the other hand, we find some crypto-friendly jurisdictions like Portugal, Germany, Italy, and Slovenia, with low or non-tax burdens on cryptocurrency gains. [18]

The situation is the same in the USA, where cryptocurrencies have been the focus of much attention by both federal and state level, albeit at federal level little formal rulemaking has occurred. [19] The Internal Revenue Service (hereinafter IRS) published a notice in 2014, which describes how existing general tax principles apply to transactions using virtual currency. According to the IRS, virtual currency is a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value. The authority declared that for federal tax purposes, cryptocurrencies fall under the property taxation rules, because virtual currencies are treated as property. General tax principles applicable to property transactions apply to transactions using virtual currency. [20]

In contrary at the federal level, several state governments have passed laws affecting the blockchain technology. There are two general approaches to regulation at the state level. On the one side a very liberal and crypto-friendly regulation takes place, with the leading of Wyoming. [21] Currently, the city is recognized as one of the top blockchain destinations in the world. On the other side the conservative narrative is preferred. According to the multi-level regulation and the lack of uniformity and clear ruling in a federal level, the amount of tax evasion connected to cryptocurrencies has grown in the recent years. The inadequate guidelines drive to a lot of non-reporting activities and opens the space for financial litigation [22]. As a consequence, the IRS continuously struggling to chase unpaid cryptocurrency taxes. [23]

4. Conclusions

To sum up, the study presented some of the most promising efforts that will make the crypto sector more orderly. Both the European Union both the OECD realized that legal certainty is fundamental for the industry. Innovation and legal certainty may be the twin foundations upon which crypto flourishes. However, in order to promote taxpayer compliance, key jurisdictions should unify their crypto tax regime and agree at least on the regular tax consequences of crypto investments and transactions. We need to resolve the contradictory interpretations and find a common viewpoint on the technology. The OECD's efforts to ensure global minimum taxation can be an example to follow. Until the centralized resolution tax evasion activities and cross-border disputes will continue to rise.

References

[1]. Satoshi Nakamoto is the name used by the presumed pseudonymous person who developed bitcoin, authored the bitcoin white paper, and created and deployed bitcoin's original reference implementation.

[2]. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, (https://bitcoin.org/bitcoin.pdf)

[3]. Advisor.morganstanley (https://advisor.morganstanley.com/perrone-wealth-management-group/documents/field/p/pe/perrone-wealth-management-group/Investing_in_Cryptocurrency.pdf)

[4]. M. Omri, Are cryptocurrencies super tax havens? *Michigan Law Review First Impressions*, Vol. 112, Issue 38, pp. 38-48.

[5]. Robby Houben, Alexander Snyers, Cryptocurrencies and blockchain, *Policy Department for Economic, Scientific and Quality of Life Policies*, Europa.eu (https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf)

[6]. OECD, Public consultation document (https://www.oecd.org/tax/exchange-of-tax-information/public-consultation-document-crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf)

[7]. OECD.org (https://www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax treatments-and-emerging-tax-policy-issues.pdf)

[8]. OECD, Public consultation document (https://www.oecd.org/tax/exchange-of-tax-information/public-consultation-document-crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf)

[9]. OECD, Public consultation document (https://www.oecd.org/tax/exchange-of-tax-information/public-consultation-document-crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf)

[10]. OECD, Public consultation document (https://www.oecd.org/tax/exchange-of-tax information/public-consultation-document-crypto asset-reporting-framework-and-amendments-to-the common-reporting-standard.pdf)

[11]. C-264/14 decision of the European Court of Justice

[12]. The CRS is a key tool in ensuring transparency on cross-border financial investments and in fighting offshore tax evasion. The CRS has improved international tax transparency by requiring jurisdictions to obtain information on offshore assets held with financial institutions and automatically exchange that information with the jurisdictions of residence of taxpayers on an annual basis.

[13]. The Convention on Mutual Administrative Assistance in Tax Matters was developed jointly by the OECD and the Council of Europe in 1988 and amended by Protocol in 2010. The Convention is the most comprehensive multilateral instrument available for all forms of tax co-operation to tackle tax evasion and avoidance. (https://www.oecd.org/tax/exchange-of-tax-information/convention-on-mutual administrative-assistance-in-tax-matters.htm)

[14]. OECD: Public consultation document Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard P. 5.

[15]. Europa.eu, (https://www.consilium.europa.eu/em/press/pressreleases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/)

[16]. The DAC directs all European Union member states to share certain information for taxable periods starting on or after 1 January 2014. The information exchanged is in relation to residents of other member states and includes employment income, directors fees, life insurance products (not covered by other directives), pensions ownership and income from immovable property.

[17]. International tax review (https://www.internationaltaxreview.com/article/2a6a9z41xb9ag7b1rdyps/impact-of-the-mica-proposal-on-the-taxation-of-crypto-assets-within-the-eu)

[18]. OECD: Public consultation document Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard (https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf)

[19]. J. Marcus, S. Cannuli, Crypto Bills Show Consensus On Need For Federal Oversight (https://www.skadden.com/-/media/files/publications/2021/04/cryptobillsshowconsensusonneedforfederaloversight.pdf)

[20]. IRS.gov (https://www.irs.gov/pub/irs-drop/n-14-21.pdf)

[21]. Reuters.com (https://www.reuters.com/breakingviews/cryptocurrencys-wild-west-is-wyoming-2021-07-07/)

[22]. CNBC.com (https://www.cnbc.com/2022/09/26/what-the-latest-irs-crypto-tax-records-summons-means-for-investors.html)

[23]. A. Parsons, Cryptocurrency, Legibility and Taxation Duke Law Journal Online, Vol. 72, Issue 1 Oct. 2022, pp.1-20.

(002)

A Last Mile Blockchain Based Proof of Delivery System

Jake Carabott and Frankie Inguanez
Institute of Information & Communication Technology
Malta College of Arts, Science & Technology, Paola, Malta
Tel.: + 356 23987350
E-mail: jake.carabott.a100984@mcast.edu.mt, frankie.inguanez@mcast.edu.mt

Abstract: This study investigates the applicability of blockchain in the logistics industry, to improve the proof-of-delivery (PoD). In this study, a complete blockchain solution was developed as an alternative PoD system where an Internet-of-Things device acts as a locking/unlocking mechanism for a storage compartment. A courier or owner of the IoT device can interact with the device via a mobile application and each transaction is validated and verified on the Ethereum network. This study researched the duration and cost of each transaction, arguing on the financial risk of such a solution. A business insider from the logistics industry identified opportunities and challenges in adopting our proposal. A qualitative survey was undertaken to explore the public perception, which was well received with an 82% approval. The applicability of blockchain in the logistics industry has proven to be feasible, however hesitancy in its adoption exists possibly attributed to a lack of understanding.

Keywords: Logistics, Smart contract, IoT, Last mile delivery, Proof of delivery.

1. Introduction

Growth in the e-commerce industry has put additional pressure on the logistics sector with the last mile delivery taking up to 53% of the total cost. This can severely impact the customer satisfaction for various reasons and thus the importance of innovation for the proof-of-delivery (PoD) in a seamless, efficient, and secure manner is felt.

The objective of this research is to provide a solution for missed deliveries of parcels that require a physical signature from the owner. The inconvenience of a missed delivery is troublesome for both the owner of the parcel and the logistics company with its busy schedule. The focus is on potential use of blockchain technology as a solution, motivated by the limited progress in adoption for this sector. A blockchain solution offers a different view of this industry and given the lack of PoD systems using blockchain, developing a solution that demonstrates blockchain is applicable in this sector, particularly in last-mile delivery, could lead to further studies that could be influenced by the solution presented and this research.

The proposed solution does not aim to replace the delivery process, as other researchers have suggested with their solutions, but will rather use blockchain to improve certain aspects of the delivery process without affecting the delivery process or causing a major disruption. It would also be easier for logistics companies to adopt a feasible blockchain solution into their system. Finally, by exploring a feasible blockchain solution, logistics companies can stimulate their interest in using blockchain technology for their day-to-day operations. Although the solution presented in this study is a prototype, it has great potential for improvement that could lead to blockchain being seamlessly integrated into the delivery process in this industry.

2. Background

Blockchain technology uses a peer-to-peer (P2P) network with cryptographic encryption, consisting of multiple devices that serve as nodes in the network, making it increasingly difficult to modify a block in the blockchain. The P2P architecture allows each node on the blockchain to store and share files globally without involving intermediaries or using a centralized system.

2.1. Investment in Blockchain

According to [11], market research firm International Data Corporation (IDC) estimates that companies invested nearly $3 billion in blockchain-related technology globally in 2019. [11] referred to an IDC report in which nine out of ten financial institutions invested in blockchain solutions for individual customers, while 15% were developing industrial blockchain applications. According to the latest IDC report, companies will have spent $6.6 billion on blockchain solutions in 2021, a 50% increase from 2020. Furthermore, companies will invest $19 billion in blockchain solutions between 2020 and 2024, a massive increase from previous years. Over time, Blockchain technology has proven to be secure, dependable, and trustworthy.

2.2. Transaction Auditing with Smart Contracts

The possibility to allow a company to have control of their own auditing process has proven to be the main problem detected in the auditing process. Allowing companies to conduct their own auditing system gives them the ability to perpetrate fraud and makes it harder

to demonstrate complete transparency. According to [6], the use of blockchain technology in auditing has several advantages, including immutability and transparency. The usage of blockchain can be beneficial in a variety of situations, including when a transaction requires proof of ownership, identity, existence, or nonexistence. Blockchain with the use of smart contracts offers many advantages, such as the elimination of paper, clear communication, encryption of transaction audit data, storage and backup of audit records, and a transparent audit process where business activities must adhere to the rules of the regulator. Furthermore, [6] stated that using blockchain and smart contracts to verify reported transactions will remove the need for intermediaries, such as a bank, in the transaction.

2.3. Blockchain for the Logistics Sector

According to [10], [6] and [5], the use of blockchain would improve important areas in the logistics industry, such as better communication of the transaction between parties, complete elimination of paperwork, open access to information within the supply chain, end-to-end traceability of goods and storage of information in the form of digital assets such as warranties, copyrights, serial numbers and more. [6] and [5] identified logistical challenges such as delivery delays, loss of documents, unclear product origin, errors and more. The existing challenges in the logistics industry could be mitigated or avoided with blockchain technology. Blockchain would improve product and inventory management, increase sustainability, reduce errors and delays, lower transportation costs, resolve errors faster as well as increase customer and partner trust. Furthermore, [5] emphasise that legislative and regulatory measures, as well as existing infrastructure, organisational processes, and capabilities, are needed to realistically see the implementation of blockchain solutions in this sector. According to [1] the existing PoD system lacks transparency, traceability and credibility as PoD services rely on signed papers or documents to authenticate the owner of the parcel.

2.4. Blockchain Limitations

Blockchain, with all the advantages that this technology offers, requires many nodes to maintain this network. Crypto miners consume a lot of computing power to verify transactions, which requires an immense amount of energy, which has a negative impact on the environment [10]. According to [8], despite the high energy consumption for mining and verifying a transaction, there is no evidence that the system is sustainable, and the trend of crypto mining does not resemble that of a finite resource such as a commodity. This is one of the motivations for the Ethereum network to have shifted from the Proof-of-Work model to the Proof-of-Stake model. Despite the lack of evidence of limiting factors in crypto mining, [8] mentioned that the International Energy Agency estimated that bitcoin mining consumed less than $1/40^{th}$ of 1 % of global electricity consumption in 2016. Moreover, there are a lot of security concerns related to smart contracts. [9] highlighted a concept for criminal smart contracts (CSC). The CSC would have a list of malicious acts such as leaking confidential information, theft of cryptography keys or committing real-world crimes such as murder, terrorism and more. Although, [9] added that it is difficult to monitor malicious behaviour in smart contracts due to the lack of standards and regulations in the blockchain.

3. Research Methodology

In this research, the hypothesis being addressed is the use of an Internet of Things (IoT) device acting as a locking/unlocking mechanism for a storage compartment such as a locker can be fully automated and audited with a blockchain-based system. This research is addressing the hypothesis: the use of an IoT device acting as a locking/unlocking mechanism for a storage compartment such as a locker can be fully automated and audited with a blockchain-based system. To address said hypothesis the following research questions are presented:

- How is blockchain used in mail delivery service?
- What is the role of blockchain, why do we need it?
- What are the challenges in mail delivery systems and what is being done?
- What are the challenges this relatively new technology brings to the logistics sector?
- What kind of evaluation is done for blockchain enabled systems in the logistics sector?

3.1. Proof-of-Concept Prototype

The presented system consists of 3 parts, the smart contract, the custom-made device, and the Android mobile application developed in Java. A smart contract has been deployed on the Goerli's test network, in which it is handling the interaction between the courier and the owner of the device with the device itself, logging and verifying each transaction. The device used was a Raspberry Pi 3, on which a custom device was built to control the lock and unlock function of the device through a built-in server that uses Bluetooth to handle multiple connections and was developed using Python, while an Android application was developed to allow users to interact with the smart contract and the device. In addition, an API was developed using PHP to process information that does not need to be stored on the blockchain but is required for the Android application. Therefore, a central database was set up on a web host to store information that does not need to be stored on the blockchain, such as the owner's credentials. Before users can interact with the smart contract, they must provide a private key of their

crypto wallet to perform an operation that uses a function of the smart contract.

The system uses blockchain technology (through smart contracts deployed on an Ethereum test network, Goerli) and can be used in a variety of scenarios: The owner could be a logistics company that owns multiple devices such as a locker and whose couriers can access the locker to deposit the owner's packages; the owner could be a homeowner whose device is a post box or a locker that a courier can access to deposit the owner's package, or the owner could be a private company that provides a service to logistics companies where a courier could deposit a package in a particular location where a particular logistics company does not provide a pickup service and would like to expand without incurring expensive costs to expand in such locations. Several experiments were undertaken to test all possible last mile delivery interactions, blockchain transactions and fees.

3.2. Business Point of View

An interview was conducted with Mr Stathopoulos, who has worked in the logistics industry since 2004 and has held the role of operations manager at C&C Express Ltd in Malta since 2015, which serves as a FedEx branch. His insight into the industry and his opinion of the prototype provided important insights into the potential use of the presented system in the industry.

3.3. End-User Point of View

A survey was created to gather an overview of public perception on the quality of service of last mile delivery. A description of the prototype was provided which the participants used to evaluated and provide feedback. A total of 100 respondents were gathered.

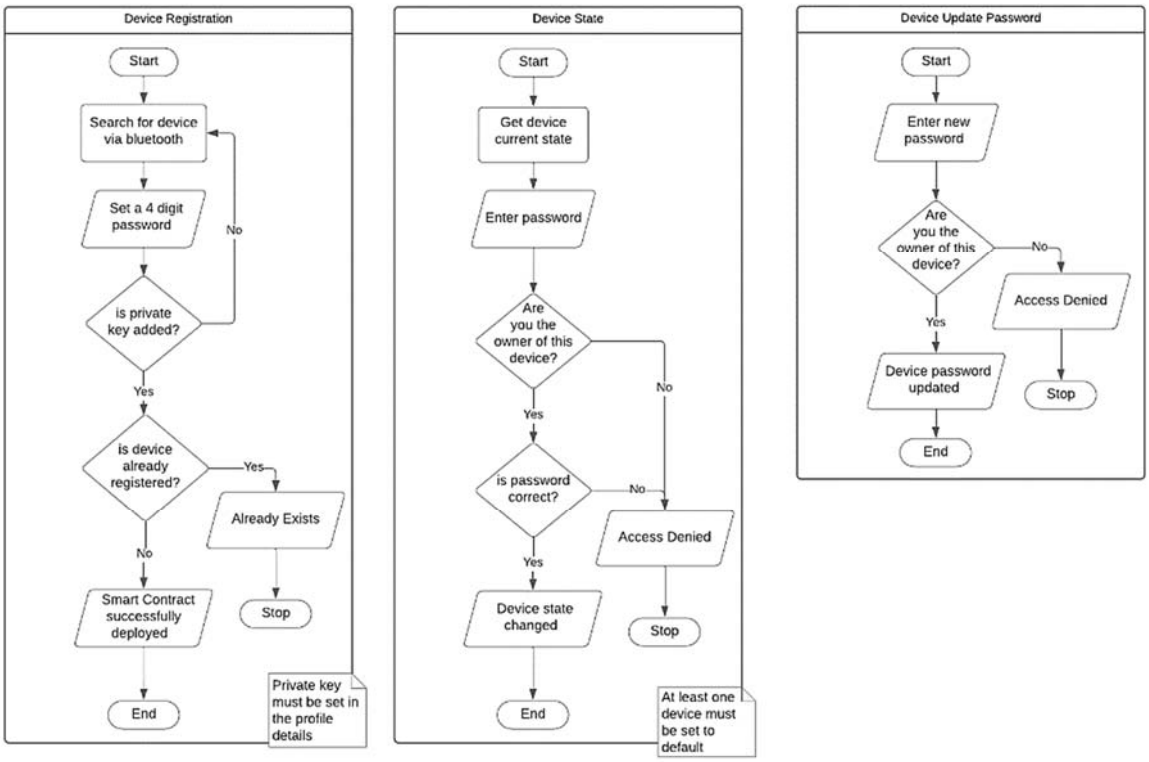


Fig. 1. Device owner interaction.

4. Results

4.1. Prototype

Phase one focused on developing a smart contract that provides proof of concept while showing the interaction between the IoT device owner and the courier. In phase two, the prototype demonstrated that the use of a mobile application and a custom-built device that acts as a locking mechanism to lock/unlock the locker reinforces and validates the work achieved in phase one. In addition, the prototype demonstrated that the system can also be used for pick-up service, showing the versatility of the application of this prototype. When comparing the concept of the developed system with the concept presented by [10], the biggest difference is in the way the system is used. [10] proposed a system where both the owner of the item and the courier(s) handling the package are verified until the package reaches the buyer, who then becomes the new owner of the item. The concept of the system presented here focuses on last mile delivery

and targets users who are homeowners and have a drop box such as a post-box or locker in their residence. The courier could use a purpose-built IoT device to interact with said device to unlock/lock it, rather than asking the owner for a physical signature, as an alternative must be physically at home to sign for the package when it is delivered, as the transaction is verified on the Ethereum network. [10] are using two smart contracts for their proof of concept while for the concept of the system presented is using one smart contract for every device registered by the owner. Initially, one smart contract was planned to be used in the presented system for all devices registered by all the owners using the system, so that all transactions of each registered device in the network would be publicly available under one smart contract. Hence, the concept was changed to use one smart contract for each device registered by the owner, which simplifies matters for all entities using the system. The change in concept was made after reviewing the approach of [10], who decided to focus on two smart contracts for each package and the courier(s) of the package rather than focusing on all the packages and all their couriers delivering those packages to the buyers. Moreover, [10]'s concept would be able to track every moment of the package and know who is in possession of the package at any given moment. However, they did not develop a prototype to validate their proof of concept, whereas in the system presented, a prototype was developed to validate the proof of concept, and in the process of developing the prototype, some initial ideas in the concept had to be changed to obtain a functional prototype. In addition, [11] has pointed to an experiment by Maersk and IBM, which developed a blockchain solution to digitise trade operations for shipment tracking. Their concept was to reduce the cost of processing documents by uploading the processing documents through a blockchain based online platform, which is then verified by multiple entities for clearance as it travels until the container arrives at the port of destination. Therefore, this solution provides an end-to-end tracking of the container and the entities that interact with the platform to move the container to its next destination. This concept is similar to [10], who refer to end-to-end tracking of the package, although Maersk and IBM have validated their concept with a functional prototype.

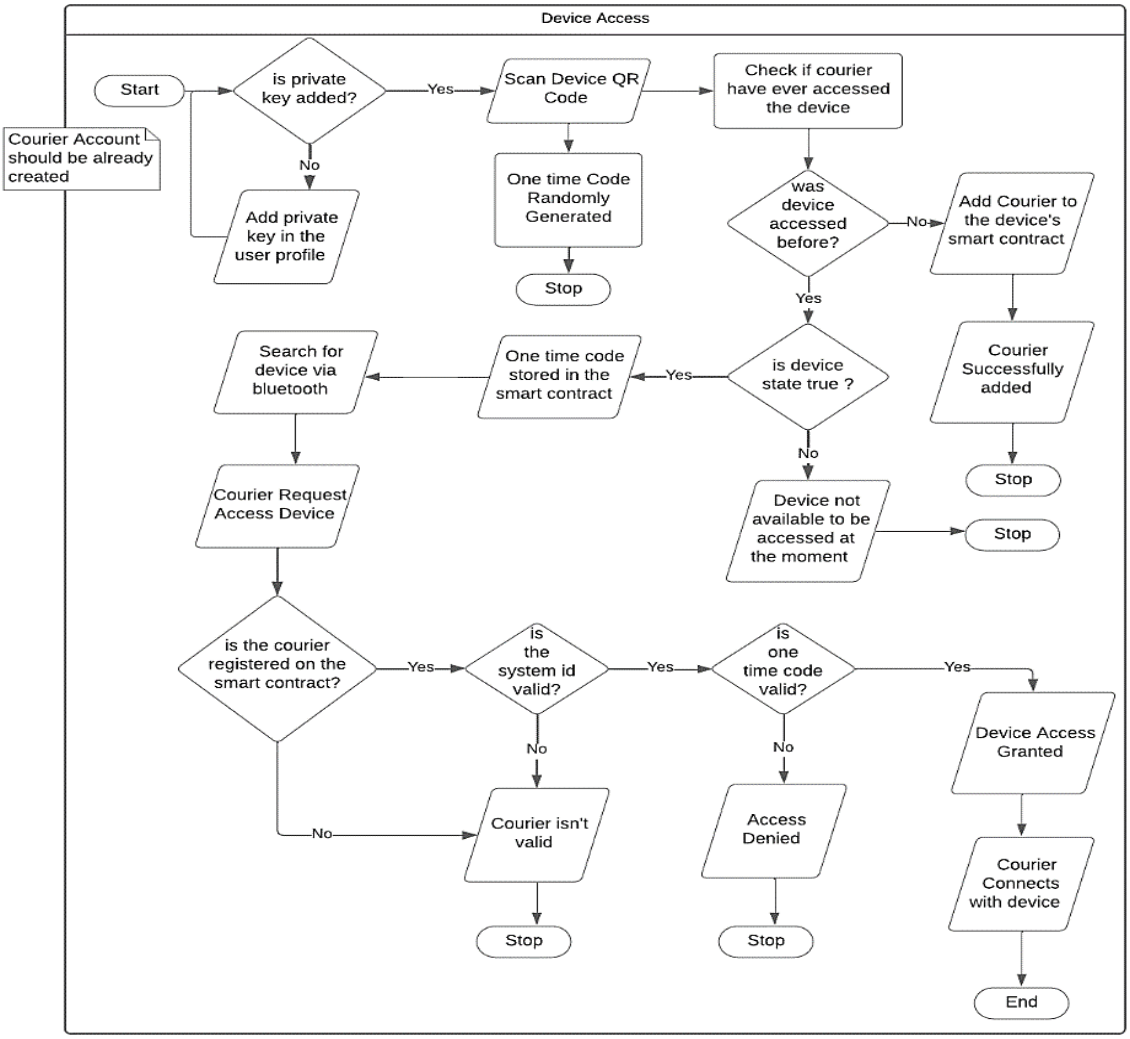


Fig. 2. Courier Interaction.

Ownership and identity verification is recorded on the blockchain, as well as every transaction made during the process, with a total of 7 smart contract transactions. Each transaction was tested for 5 times and the average gas consumption calculated. The highest being of 1,119,803 which corresponds to an average transaction fee of 2.463566 6 × 10^{-2} ETH. Each transaction took at most 15 seconds to complete.

4.2. Business Insights

From the interview with Mr Stathopoulos important insights into the potential use of the presented system in the industry were provided. When asked about the current challenges when it comes to PoD, Mr Stathopoulos highlighted that due to the Covid it has been challenging to obtain the physical signature from the client when the package is presented at the door. To overcome this challenge, Mr Stathopoulos explained the measures taken by obtaining the customer's ID number when the ID card is presented at delivery. A system update is then stored with the customer's name and ID number in case there is a dispute. When asked if there were any considerations to solve this challenge using blockchain technology, he emphasised that they were not aware of the potential applicability of a blockchain solution to solve this challenge. In addition, Mr Stathopoulos added that they act and operate according to their principal operation and that they cannot decide on their own. He added that there are rules and policies that as a FedEx branch in Malta they must follow as it goes to all the other FedEx branches worldwide. During the interview, a research paper was mentioned. The research paper by [7] highlighted an experiment by FedEx in which a blockchain solution was developed to track high valued cargo, and the company planned to extend this functionality to almost all its shipments. When asked if this system was currently being used in Malta, he stated that they were not aware of such a system and that it is not being utilised in Malta. Furthermore, when asked about if there were plans to introduce a self-pick-up service with lockers for customers in Malta and whether there were any considerations to use blockchain as a viable solution for this service, Mr Stathopoulos replied that there wasn't any consideration of providing such a service with a blockchain solution. He added that C&C Express Ltd currently has an online platform where the customer can log in and opt to pick up the package themselves from their office in Luqa instead of having it delivered. Therefore, the customer's package would be located and kept in the office until it is picked up. When asked if there had been discussions about a blockchain solution by experimenting with an alternative PoD, Mr Stathopoulos replied that there had been no discussions about experimenting with a blockchain solution for an alternative PoD. Finally, when asked if the prototype presented could be an improvement over the current proof-of-delivery system, Mr Stathopoulos replied that the prototype presented was an interesting idea and that the development of the prototype should focus on a specific area rather than focusing on the versatility of the prototype. Although it can be applied in many ways, it should be focused on a specific service. He added that their current system is efficient.

4.3. Client Insight

A survey was conducted among residents of Malta to explore their willingness to utilise the proposed delivery system as an alternative PoD. According to one hundred anonymous submissions through an online form, 28 % of the residents who completed this survey lived in an apartment, while 25 % of the residents lived in a maisonette. The remaining 47 % were split between residents living in a terraced house, house of character, a townhouse, and a penthouse. When asked about the frequency of parcel deliveries requiring a physical signature, 31 % of respondents said they receive a parcel requiring a signature occasionally, followed by once a month, which was indicated by 24 % of respondents. The remaining 45 % were split between once a week, more than twice a month and daily. Furthermore, when asked if they had ever had a missed delivery attempt, 88 % of respondents answered yes, while 12 % answered no. Those who answered yes were asked a follow-up question asking them how many deliveries they had missed in the past year. 55.6 % of respondents said they had between two and four missed deliveries attempts in the past year, while 20 % of respondents said they had between zero and one missed delivery attempt in the past year. 16.7 % of respondents indicated that they had between five and ten missed delivery attempts, while 7.8 % of respondents indicated that they had more than ten missed delivery attempts. In addition, those who had answered yes were asked another follow-up question about the time frame in which they would typically have these missed delivery attempts. The most common time frame with 69.3 % by respondents was between 8 am and 12 pm and 26.1 % of respondents said their missed delivery attempts occurred between 12 pm and 15 pm. The use of the proposed system could drastically reduce or eliminate the number of missed delivery attempts, as no human-to-human interaction is required when delivering a parcel. Moreover, when asked if they have ever used a self-collection service such as Easipik from Maltapost, 50 % of the respondents answered yes, while the other 50 % answered. A divided result shows that some of the respondents have taken an initiative to solve the problem themselves. When asked if they would be willing to use a locker or post-box where the courier can deliver their parcel, 76 % of the respondents answered yes, while 20 % of the respondents answered maybe indicating that they are interested but not yet convinced, and the remaining 4 % of the respondents answered no indicating that they would not be interested in such a service. Furthermore, a follow-up question was asked in which

some benefits were mentioned. Respondents were asked about their interest in the possibility of restricting the courier's access when a parcel is already inside. 80 % of respondents answered yes, meaning they are interested in the security feature mentioned, while 14 % answered maybe, meaning they are interested but not yet convinced, while 6 % of respondents answered no, meaning they are not interested in using such a. Finally, when mentioned the benefits of such a service that allows the IoT device in the locker or post-box to sign for the package on their behalf, 82 % of respondents answered yes, indicating that they would be interested in using the proposed system, while 12 % of respondents answered maybe indicating that they were interested but not yet convinced, while 6% of respondents answered no indicating that they were not interested in using such a service.

4.4. Security Analysis

When analysing the blockchain aspect of the system presented from the point of view of security, one of the most important points is the integrity that blockchain technology gives to the PoD system. Everything that is stored in the blockchain cannot be changed, so the data integrity of important information such as device details is guaranteed. The immutability of the blockchain enables the traceability of the courier's daily tasks, i.e. the monitoring of the courier's access. A courier will interact with the IoT device the most, and since the blockchain audits every transaction executed on the smart contract of every IoT device, anyone in a public ledger with the address of the smart contract can view these transactions and thus know exactly when an IoT device was accessed and by whom. Furthermore, one of the biggest security issues is smart contracts. In the Blockchain limitations section, several cases of smart contracts were cited, mostly due to poor programming. Thus, to avoid smart contract issues, a robust validation process has been introduced in each function to ensure that a specific parameter must be passed to execute the function. To avoid human input errors, the mobile application is retrieving selective data from the smart contract, e.g. the courier's data, which is automatically filled in without being able to be changed, so that the courier can only move on to the next activity to request device access. Moreover, while the security model which blockchain technology is equipped with is secure, the system presented does not prevent users from having their accounts stolen, thus exposing their private key of their crypto wallet. In addition, the blockchain does not have any mechanisms to prevent such a scenario of exposure. Finally, as already mentioned in the section blockchain limitations, a smart contract cannot be fixed if a fault is found in the smart contract. In the system presented, since deployment of a smart contract only occurs when an owner registers a new IoT device, in the event of a bug in the smart contract, a new patched version of the mobile app would solve any problems with future smart contracts, while for the smart contracts that have already been deployed, the user could choose to unlink the device and re-register the device to remove a faulty smart contract and start again, with the recommendation to download a CSV copy of the transaction records related to the faulty smart contract.

5. Conclusion

This study aimed to improve the current PoD system, especially last mile delivery, by proposing an alternative PoD system using blockchain technology. We have proven our hypothesis with a fully functioning complete prototype, as well as gathered interest within a logistics company and public support.

References

[1]. K. Sadouskaya, Adoption of blockchain technology in supply chain and logistics, Bachelor's Thesis, *South-Eastern Finland University of Applied Sciences,* 2017.

[2]. P. W. Abreu, M. Aparicio, C. J. Costa, Blockchain technology in the auditing environment, in *Proceedings of the 13th Iberian Conference on Information Systems and Technologies (CISTI),* 2018, pp. 1-6.

[3]. H. R. Hasan, K. Salah, Blockchain-based proof of delivery of physical assets with single and multiple transporters, *IEEE Access,* 6, 2018, pp. 46781-46793.

[4]. M. Kouhizadeh, J. Sarkis, Blockchain practices, potentials, and perspectives in greening supply chains, *Sustainability*, Vol. 10, Issue 10, 2018, pp. 3652.

[5]. M. Dobrovnik, D. M. Herold, E. F¨urst, S. Kummer, Blockchain for and in logistics: What to adopt and where to start, *Logistics*, Vol. 2, Issue 3, 2018, p. 18.

[6]. E. Tijan, S. Aksentijevi, K. Ivani, M. Jardas, Blockchain technology implementation in logistics, *Sustainability*, Vol. 11, Issue 4, 2019, pp. 1185.

[7]. M. Liu, K. Wu, J. J. Xu, How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain, *Current Issues in Auditing*, Vol. 13, Issue 2, 2019, pp. A19-A29.

[8]. R. L. Rana, P. Giungato, A. Tarabella, C. Tricase, Blockchain applications and sustainability issues, *Amfiteatru Economic*, Vol. 21, Issue 13, 2019, pp. 861-870.

[9]. S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F.Y. Wang, Blockchain-enabled smart contracts: architecture, applications, and future trends, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 49, Issue 11, 2019, pp. 2266-2277.

[10]. A. Batta, M. Gandhi, A. K. Kar, N. Loganayagam, V. Ilavarasan, Diffusion of blockchain in logistics and transportation industry: An analysis through the synthesis of academic and trade literature, *Journal of Science and Technology Policy Management*, Vol. 12, Issue 3, 2020, pp. 378–398.

[11]. D. Bonyuet, Overview and impact of blockchain on auditing, *International Journal of Digital Accounting Research*, Vol. 20, 2020, pp. 31–43.

(004)

Computation Independent Model in MDA-based Smart Contract Development

M. Jurgelaitis, L. Čeponienė, R. Butkienė and T. Valatkevičius
Faculty of Informatics, Kaunas University of Technology, Studentų str. 50, Kaunas, Lithuania
E-mail: mantas.jurgelaitis@ktu.lt

Summary: In Model Driven Architecture, a Computation Independent Model is used to describe business process, but is largely ignored in supporting model driven software development of blockchain technology-based systems. In this paper, we propose a CIM that encompasses business process, use case, and domain model specifications to support the application of MDA in blockchain technology-based system development. The proposed CIM can be employed for communication purposes and to outline the blockchain/smart contract role in an overall system design and ultimately be utilized in smart contract code production.

Keywords: MDA, UML, CIM, Software requirements, Smart contract.

1. Introduction

The understanding of blockchain technology differs between stakeholders and developers: some see it just as a cryptocurrency that is used for financial purposes, circumventing central authorities like banks, while others see it as a buzzword and fail to recognize how the blockchain could be integrated in software development. As there is no common understanding of the principles of application of technology [1], an assessment of blockchain technologies must be performed to identify the applicability of a specific platform before developing the required functionality. This means that developers may waste time analysing specific details of a specific technology, even though the scope of a project is unclear. Although concepts overlap between blockchain technologies, the specifics of a particular platform could be confused with the general principles of blockchain.

Similarly, as in traditional software development, blockchain technology-based systems could also benefit from the model-driven approach, which facilitates the system development process. One of the model driven approaches is Model Driven Architecture (MDA) [2], which encompasses modelling in several layers of abstraction and transformations between them. Modelling provides a valuable abstraction of business processes or system requirements, which can then be used to communicate with stakeholders to achieve a common understanding of the blockchain and blockchain integration capabilities. Instead of relying solely on manual development, model transformations and code generation techniques are introduced in MDA thus extending and structuring the system development process. There are several attempts to apply the MDA principles in the development of blockchain-based systems [3] [4] [5]. Most of these proposals are based on transformations between the Platform Independent Model (PIM), the Platform Specific Model (PSM), and code. In a model driven architecture**,** a computation independent model (CIM), it is mostly used to describe business processes, but it can also be used to describe the requirements of the system under development. The step of CIM for blockchain development and its transformation to PIM is described in [3] [4], but it does not cover business process specification, requirement elicitation, and design in the context of a blockchain technology-based system, making the transition between the two relatively unclear. The aim of this paper is to propose and outline a CIM for the MDA-based blockchain system development process method. The identified business processes in CIM can be further utilized for eliciting software requirements and system design during the preliminary phases of development.

2. The Role of CIM in the MDA-based Blockchain Development Process

The overall process for MDA-based blockchain technology-based system development is presented in Fig. 1. The proposed CIM development and its transformation to the PIM approach (Fig. 2) is an excerpt of a broader system development method, proposed in [6].

During the proposed blockchain technology based system development process the developer outlines the various software models. The method encompasses three different abstraction layers, where CIM, PIM, and PSMs are developed using model to model and model to text transformations for producing a smart contract code for a specific blockchain platform. The method currently supports the transformations to smart contract model for Hyperledger Fabric and Ethereum platforms and ultimately results in production of chaincode in Go and smart contract code in Solidity.

The main steps of the process related to CIM development and transformations are presented in Fig. 2. And since the main focus of the paper is on the Blockchain CIM, the model structure and the proposed transformations are further elaborated upon in the upcoming sections.

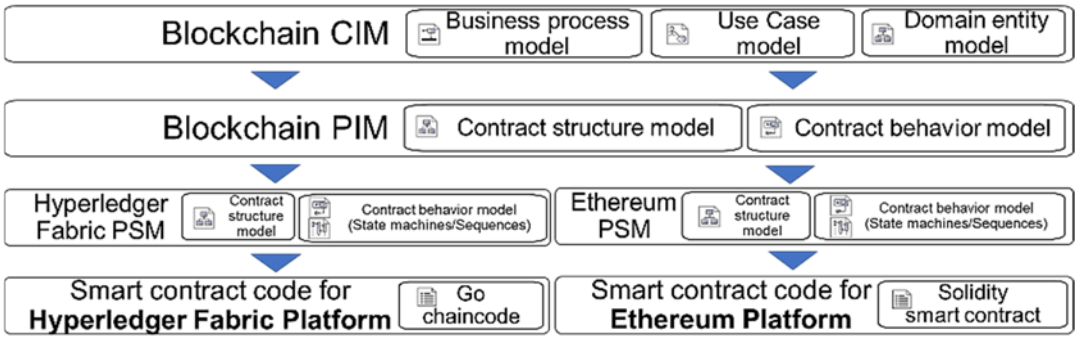


Fig. 1. General Principles of MDA-based Blockchain Technology-based System Development Method.

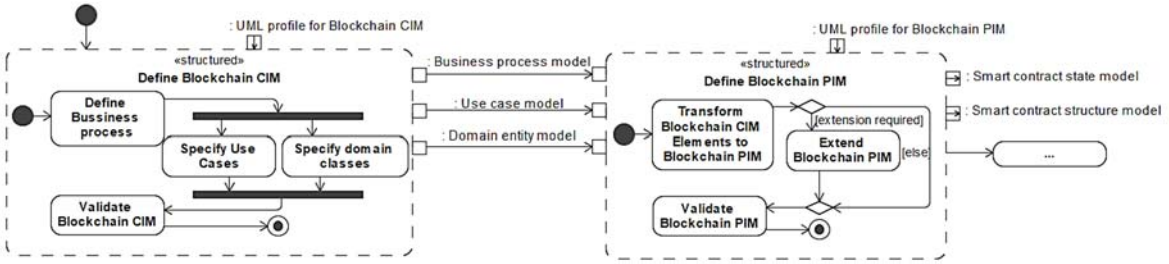


Fig. 2. Detailed Steps in CIM Development and Transformation to PIM.

2.1. The Proposed Structure of Blockchain CIM

The Blockchain CIM is proposed in this paper to describe not only the general principles of its development but also the identification of elements that can be implemented using blockchain technologies. Blockchain CIM encompasses the business process model, based on which use case and domain models are also specified. In the use case model, actors represent system users or the external systems communicating with the system under development. These external system actors can be specified as «blockchain» actors associated with the use cases in which the data from the blockchain is used or appended. For the specification of such actor, a stereotype «blockchain» is required, which is included in the Blockchain CIM profile (Fig. 3). Also, in the proposed Blockchain CIM, the domain model is used to specify the domain entities and to distinguish which data needs to be relocated to the blockchain (denoted using the stereotype «on-chain»).

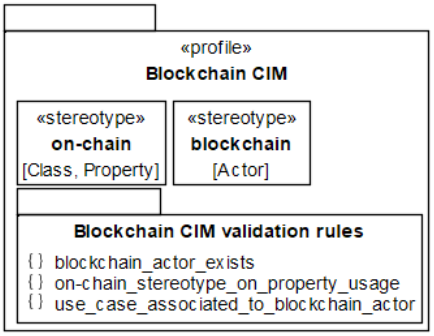


Fig. 3. Blockchain CIM Profile.

Once the CIM specification is done, the entire CIM is validated using the specified CIM validation rules, making sure that integrations with the blockchain are recorded, and the on-chain data entities or their properties can be successfully relocated to the smart contract model. The outlined Blockchain CIM contents, encompassing the business process, use case, and domain entity models, are used as inputs during the model transformation to PIM.

2.2 Transformation to Blockchain PIM

The next step of the proposed process is the definition of Blockchain PIM (Fig. 4). Some elements of Blockchain PIM can be automatically transformed from Blockchain CIM and others should be manually specified based on the information from CIM.

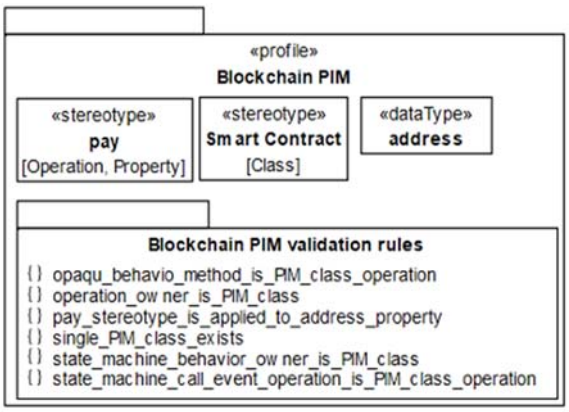


Fig. 4. Blockchain PIM Profile.

During the automatic transformation, using the specified domain and use case models, a smart contract class is produced. This smart contract encompasses data entities, their properties, and specific use case functionality recorded in the smart contract specification. Once the model to model transformation is complete, the Blockchain PIM can be manually extended with additional behavior models. Once the extension is complete, a model validation is performed. The result of the proposed transformation is Blockchain PIM, which is further used in the MDA-based blockchain technology-based system development method [6].

3. Conclusions

The paper contributes to broader research of model driven smart contract development process. Additionally, the proposed CIM also contributes to further outline the CIM role in the context MDA application for various domains, not only including the blockchain based solution and smart contract development. The proposed method compared to other proposed MDA based approaches explicitly outlines the CIM contents, and rules that could be used to facilitate the transition between requirement elicitation and design phases of development. The introduction of an MDA-based approach facilitates the development of blockchain technology-based systems, providing a general and more structured approach, without burdening the developer with unnecessary details. The proposed method serves as an abstraction for blockchain technology-based systems, which can be utilized to produce smart contracts for multiple platforms, provided that specific metamodels and transformations are developed. The proposed Blockchain CIM also serves as a basis for communication between stakeholders and permits developers to specify the behaviour and structure of the system under development.

References

[1]. J. D. Kruijff and H. Weigand, Understanding the Blockchain Using Enterprise Ontology, in *Proceedings of the International Conference on Advanced Information Systems Engineering*, Essen, Germany, June 12-16, 2017, pp. 29-43.

[2]. O. Pastor and J. C. Molina, Model-Driven Architecture in Practice, *Springer*, 2007.

[3]. K. Hu, J. Zhu, Y. Ding, X. Bai and J. Huang, Smart Contract Engineering, *Electronics*, Vol. 9, Issue 12, 2020, pp. 2042.

[4]. K. Boogaard, A model-driven approach to smart contract development, Master's thesis, *Utrecht University,* 2018.

[5]. H. Syahputra and H. Weigand, The Development of Smart Contracts for Heterogeneous Blockchains, *Enterprise Interoperability VIII*, Vol 9, 2019.

[6]. M. Jurgelaitis, V. Drungilas, L. Čeponienė, R. Butkienė and E. Vaičiukynas, Modelling principles for blockchain-based implementation of business or scientific processes, in *Proceedings of the International Conference on Information Technologies (IVUS 2019)*, Kaunas, Lithuania, April 25, 2019, pp. 43-47.

(006)

Combining Self-Sovereign Identity with Digital Currencies to Enable Programmable Money

S. Sezer [1] and W. Prinz [1,2]
[1] Fraunhofer Institute for Applied Information Technology FIT, Schloss Birlinghoven
53757 Sankt Augustin, Germany
[2] RWTH Aachen University, Templergraben 55, 52062 Aachen, Germany
Tel.: +49 2241 14 3720
E-mail: selin.sezer@fit.fraunhofer.de

Summary: Blockchain technology has proven to be useful for programmable money applications to achieve conditional payments, but also in empowering the Self-Sovereign Identity paradigm to manage digital identities. In this paper, we propose incorporating SSI components into programmable money to allow for a blockchain-based larger-scale programmable money concept that allows for increased trust over the use of payments among reduced possibility for misuse, data sovereignty for users, increased decentralization, and unified and flexible representation for various spending conditions. We illustrate different ways of utilizing verifiable credentials in this context by looking at what, who, when, and where questions. The aim of this paper is to examine and discuss the role of self-sovereign identity for a large-scale programmable money ecosystem and to lay the foundations for new payment opportunities with embedded spending conditions.

Keywords: Blockchain, Programmable money, Conditional payments, Self-sovereign identity, Verifiable credentials.

1. Introduction

We witness in the last decade that the ubiquity of the Blockchain platforms has transformed the existing concepts and processes, especially by encouraging us to rethink existing digital or non-digital structures and possibly redefine them during this transformation. The financial services industry is one of the areas where various incremental developments have been realized through Blockchain technology with even more revolutionary infrastructure changes on the way [1]. Inspired by the popularity of crypto-assets and their underlying technology, an increasing number of institutions like central banks, banks, and private businesses are trying to build initiatives to form advanced technological infrastructures. Existing projects include stable coins (Diem [2], commercial bank money tokenized on Blockchain, etc.) and possibly central bank digital currencies (CBDC) [3]. These initiatives present us with different opportunities to rethink and redefine what we can do with the concept of money. One such opportunity, although it is originally not new [4], is the idea of modifying the use of money. In today's emerging programmable world, in which more digital assets are utilized and exchanged by becoming programmable and linked to each other [1], why shouldn't we be able to program our money to reflect our preferences in a tightly controlled and transparent manner?

Digital Identity Management Systems are another area for which Blockchain technology will impose an important transformation toward the self-sovereign identity paradigm. Improvements in client onboarding and Know Your Customer (KYC) processes in terms of speed, cost, and customer convenience in addition to compliance with GDPR requirements are some of the benefits that blockchain-based self-sovereign identity can bring into the finance sector [5, 6]. Consequently, making the user both in charge of her money and her identity can also open further doors, not only by improving the traditional conditional payment use cases like donations, funding, and social welfare programs but also by providing possibilities for flexible modifications to existing payment processes like personal money transfers, management of project budgets, etc.

This paper aims to examine and discuss the role of self-sovereign identity in a large-scale programmable money ecosystem with embedded spending conditions. It is structured as follows: In the Background section, we explain the concept of programmable money and the general foundations of self-sovereign identity. In Related Work, we summarize the studies conducted on the programmable money concept. Based on these, we discuss in the Opportunities & Use Cases section the potential role that the self-sovereign identity can play for programmable money with Blockchain being the enabler technology. Finally, we provide the requirements and challenges of the suggested concept in the Implications section and conclude with a summary and future work in the Conclusion section.

2. Background

2.1. Programmable Money

There are several descriptions for the term "programmable" or "smart" money in the literature like differentiating different digital forms of money [7], tokens [8], programmable payments that make use of smart contracts and/or cryptocurrencies [9, 10], or other automation systems that can be adapted to

existing banking infrastructures [11]. In this paper, programmable money refers to a digital currency with embedded spending conditions. This implies that the currency is only transferable once the conditions embedded into it are fulfilled [12]. These conditions can be propagated further within the money life cycle since the behavior is embedded directly into the money rather than any system that manages it or can be updated dynamically depending on the use case.

2.2 Self-Sovereign Identity

The steady increase in the number of online services and the people using them has reflected greatly on the interest to manage digital identities that allow people to demonstrate digitally who they are and make a distinction between different entities [13]. These identities are not limited to the credentials required to utilize certain services, but can also involve the attributes that can be used to identify us in the real world [14].

Over time the Identity Management Systems evolved based on the technological developments and requirements of different use cases but most of the existing systems put the (service) provider in the center, making it hard for the users to manage and control their data in various services. On the other hand, the emerging concept of the Self-Sovereign Identity (SSI) differentiates itself from these systems by separating the user's digital existence from any provider [15] and providing the users the infrastructure to allow them to own and fully control their digital data among being the ultimate decision maker in terms of who has the access and processing rights of their personal information [16].

Although various definitions and properties have been suggested for SSI [17, 18, 19], it is still an emerging technology, and global standards and tools for the SSI enabled digital interactions have not yet been established [20].

In the SSI ecosystem, there are three entities that interact with each other. First, the issuer who issues (and revokes) the Verifiable Credentials (VC) with previously specified attributes. Independently provable claims confirmed by a party with the help of cryptographical signatures form VCs [21]. Second, the identity owner/holder who stores, manages, and presents VCs to the verifier. Finally, the verifier who validates whether the VC attributes conform to the specific requirements. Since the proof request is directed to the identity owner without communicating with the issuer, the owner of the credential can control the shared information [22].

Decentralized Identifiers (DID) [23] enable the interaction between entities in this ecosystem by referring to the information in the form of verifiable credentials provided by third parties. Thus, DIDs are suitable means for being used as an identity scheme for programmable money while verifiable credentials will provide trusted assertions for being used in the definition of spending conditions.

3. Related Work

Programmable payments empowered by smart contracts have been a major focus point since the emergence of the Blockchain technology [24, 25], however, the programmable money as the concept referred to in this paper has gained attention only recently, and therefore, the number of practical examples in the literature is limited.

Stadjerspas [26] is a Blockchain-enabled system offered by the Municipality of Groningen in the Netherlands since 2016 to support the low-income citizens to use services provided by the private sector that are hard to access (e.g., sports clubs, cinemas, solar panel subsidization). A voucher can be issued by the municipality or a partner company with certain eligibility conditions such as user profile details like residence district, income, number of children, etc., or spending conditions like eligible service providers and different usage restrictions. These conditions can be built into a smart contract and therefore ensures for the municipality that the allocated public money is utilized for the desired purpose by the targeted profile of beneficiaries. The eligibility checks on the applying citizens is handled by the municipality by a database check, if successful, followed by an issuance of a QR code that links the eligible citizen to a unique ID with assigned smart vouchers.

Another study [27, 7] shows in depth how welfare support for people with disabilities in Australia (National Disability Insurance Scheme (NDIS)) can benefit from programmable money where highly customizable spending rules determined for each participant by the National Disability Insurance Agency (NDIA) are implemented in token representations with dynamic policies attached to them. Once the participants receive their tokens, they can utilize them for desired services in eligible service providers who can then demand payment from NDIA in return. The eligible service providers are handled in separate registry smart contracts whereas the participant identity information and their Ethereum address mappings are stored off-chain.

Rehabilitative psychotherapy is another area where an application of programmable money is evaluated by cooperation involving different public organizations and private companies in Finland [28]. Electronic vouchers created within the system are issued for one time use only and unlike traditional digital money cannot be divided into smaller denominations. The merchants participating in the system are provided with merchant credentials by a participating Merchant wallet provider that involved business information like name, category code, and list of accounts among allowed and not allowed product categories.

Conditional payments based on Blockchain have also been investigated by [29] in cooperation with multiple partners with respect to the simplification of the issuance and verification processes of different payment promises such as vouchers for lunch and transportation benefits. Dynamic policies that could be coded into a token and be enforced during the spending

involved various properties like an upper limit of the money that can be spent on a specific product, a list of approved service providers, token validity, etc.

This review indicates that current methods are based mainly on a voucher-based approach and that the emerging concept of SSI has not yet been applied to secure both the participating identities as well as credentialling of spendings conditions. We believe that our work contributes to a new approach to addressing this research.

4. Opportunities & Use Cases

Utilizing a programmable money ecosystem brings various benefits. Different funding cases such as donations, grants, loans, and social welfare programs can benefit from **reduced risk of misuse** with the help of programmable money. Another advantage is having **improved control over money**. Vouchers and personal conditional money transfers like pocket money provided by parents to their children [4] or last will that declares certain use of money are some example use cases that strongly derive benefit from this category. In the case of project budgets, **automated auditing** can be achieved by determining for what the money is allowed to be spent beforehand. Various applications like customer incentives and loyalty programs can benefit from **better data analytics** on user behavior. Finally, the provision of **incentives for behavior change** to achieve desired social, environmental, or political goals (e.g., complementary currencies) can be provided by limiting the use of money. As an example, governments can initialize funding for their citizens that can only be used to buy green energy as an action against climate change.

At the time of writing the representation of digital identities in all existing programmable money implementations according to our knowledge represented in the Related Work Section require an additional maintainer actor in the system who is responsible for registration and management. This manual management of different entities (whether it is the spender of the money or the receiver) conforms to the size and context of these studies, however, a larger-scale programmable money ecosystem would require a more automated and self-sufficient approach to manage various identities and/or events that define identity-related attributes. In this context, in contrast to the current oligopolistic structure of digital identity management systems that are almost completely handled by a handful of big tech companies [30], the concept of self-sovereign identity can bring many benefits to a potential large-scale programmable money ecosystem by distributing the management task of identities to the participants of the ecosystem, incorporating additional trust by involving trusted institutions in the process, providing data sovereignty for the users, creating a secure decentralized structure that does not depend on third parties, and allowing a unified representation for various spending conditions based on identities.

These benefits can be analyzed better once the underlying components namely decentralized identifiers and verifiable credentials are investigated within the context of programmable money. DIDs provide continuous availability for the verification of the credentials which can become crucial considering the time sensitive nature of financial services. It will furthermore allow for selective disclosure of the data for the users by the use of different DIDs and avoid profiling in their transactions. The direct verification of the credentials without reliance on the service of a third party and the secure data exchange channels make it possible to create a fast, secure, and reliable system for exchanging personal information. Furthermore, the issuance of the VCs by trusted institutions and the tamper proof structure of these credentials with the help of cryptographic tools make it possible to increase the trust in the system and decrease the possibility of a misuse that might occur. Therefore, this makes it possible for the issuer/giver of the money to delegate the trust it has for certain institutions to the spender through the use of the credentials and add an additional trust layer next to the trust achieved by the “code is law” principle. Finally, since the VCs are portable and not enclosed within the issuer organization, they can be reused and allow for even more advanced cross references between different services that might involve conditional money exchange.

In practice, the desired attributes for the VCs together with the trusted institutions that can issue these credentials can be provided as a spending condition by the issuer of the programmable money. The receiver should provide these credentials meeting the predefined criteria to be able to send or receive the programmed money, depending on the requirements of the use case. To illustrate how differently VCs can be utilized for the concept, we can have a look at the following. A wide range of spending conditions can be expressed in the form of answers to the following generic questions:

- Who is allowed to spend the money?
- For what can it be spent?
- When can it be spent?
- Where can it be spent?

Based on these questions, we propose that there are four distinct awareness requirements that different use cases can be broken into:

a) Commodity-awareness: The money should be able to differentiate the type of products or services it is used to purchase. In addition to the question of what, additional product/company characteristics (e.g., vegan, climate-neutral, cruelty-free, etc.) also falls into this category. Differentiation of different products and services requires a semantic model to be built but in the case of a product or service that is not possible to represent within this semantic model verifiable credentials can be utilized to describe these. They can also be used attached to the semantic model to describe different characteristic requirements mentioned above.

Example: *A company issues gift coupons for its employers that can only be used on carbon-neutral*

products. A credential issued by a trusted carbon-neutral certification institution defined by the company is provided in addition to the product information and verified to realize the purchase transaction.

b) Identity-awareness: The money should be able to identify different attributes related to the identities which can belong to the sender and/or the receiver.

Example: *Alice wants to provide a one-time grant for a student that is from her hometown and below 18 years old. Somebody interested in the grant needs to include a credential issued by a trusted institution defined by Alice that shows that he/she is a student, comes from the same hometown, and is below 18 years old to request and receive the allowance.*

c) Temporal-awareness: The money should be able to comprehend different points in time and/or events. Although temporal boundaries with known points in time can be easily handled in a computational environment, representation of events with temporal uncertainty can be where the verifiable credentials might be appropriate.

Example: *Bob wants to motivate his skeptical son, Carl, to get a Corona vaccination by offering to pay a certain amount of money. The money can only be spent by Carl only when he shows that he got all his vaccinations. Bob sends the money to Carl and Carl uses credentials issued by a trusted institution defined by Bob to prove that he has been vaccinated to be able to use the money at the time of purchase.*

d) Spatial-awareness: that can identify the location where the transaction takes place.

Example: *A supermarket issues vouchers for its customers that can only be spent on chosen branches. The vouchers can be claimed at any time but cannot be used if the location requirements are not satisfied. The customers that enter those branches can get a credential issued by the market with the help of a QR code that shows that they are there for a certain period of time and they can attach these to the payment request to use the vouchers to shop.*

Although these examples illustrate the application of a single requirement, we expect that a real-life use case is more likely to have a combination of these.

Blockchain technology has empowered the digital transformation of various domains since its early days and can also be the enabling technology for building such a programmable money ecosystem supported by the self-sovereign identity paradigm. On the one hand, Blockchain technology has been often proposed as an outstanding choice for decentralized, tamper-proof digital identity solutions [16] and shows compliance with the essential properties of SSI. First, it is a decentralized platform that is not under the influence of a single institution and any authorized party can access data recorded in it. An owner of personal data has complete control over it, may govern how such data is shared with other Blockchain users, and can even build more fine-grained governance rules with the help of smart contracts. Data immutability, provenance tracking, distributed control, liability, and transparency are the additional features where a blockchain-enabled system differs from traditional systems [18]. On the other hand, Blockchain technology forms a solid foundation for highly customizable transfers of digital assets that can be abstractly defined in smart contracts. Compared to a centralized system, Blockchain technology provides certain benefits in terms of building a trusted environment between multiple entities in a trustless manner. In a larger-scale programmable money ecosystem with multiple entities, it can help avoid interaction with different systems for different use cases and facilitate the easy connection of different use cases [7].

5. Implications

In the previous section, we have demonstrated the possibilities that can be realized with the help of incorporating SSI concepts into programmable money. In order to realize this concept, technical requirements and risks should be investigated thoroughly.

Although the concept provides a wide range of possibilities to implement, the use of identity-related personal data as input should be handled in a privacy-preserving manner according to the related regulations. Different design choices like handling sensitive data off-chain or providing as an input to a smart contract on Blockchain have different implications on the trust the system provides. An off-chain approach might be easier to comply with privacy requirements but it might cause disadvantages in terms of where the trust in the system lies and how the verification of the credentials occurs according to the spending rules. In contrast, smart contracts provide much higher trust but compliance with privacy requirements as well as governance rules on access to this data might be complicated. Furthermore, the availability and use of personal data might be an issue that might affect user acceptance. Therefore, the system design must consider these aspects and be transparently implemented.

How persistent the spending conditions should be is also a question that impacts the system design and should allow for flexible modifications. Since real-life situations pose dynamic changes, the conditions might be open for changes over time, unless it is not requested to be otherwise. In these cases, it should be clear who should participate in the consensus to change any condition attached to the money.

A sustainable Blockchain-based infrastructure for the concept requires a trusted consortium to be built. Governance must be established that distinguishes between the applications of the presented concept in a public or permissioned manner. This would be informed by an analysis of the stakeholders and their socioeconomic interests and as well as the added value different approaches bring in.

The existing technical landscape of SSI brings further challenges. To enable multiple use cases and possible cross-links between them, standardization and interoperability need to be established. Furthermore, one natural consequence of using SSI is that the verifier is the one who decides whether the presented

credential is issued by a party it trusts. Within the programmable money concept, this means that the issuer of the money with certain constraints is responsible to define trusted institutions that can issue the type of credential it requires for the use of money. On one hand, this can help increase the trust provided by the system as explained in the previous section, on the other hand, it might become impractical for the user to cover all the possible institutions depending on the use case. Therefore, defining certain institutions that can be trusted with certain types of credentials can be helpful to ease this process. However, it should be eventually the choice of the issuer to rely on these.

As a potential factor that might increase user acceptance, building the concept on top of a digital currency with a stable value that is backed by trusted institutions should be considered. This would also enable building much easier cross-links between different use cases. The optimal type of digital currency in that regard needs to be investigated, but both the programmability feature and use of self-sovereign identity might then bring in certain added values to the currency itself. Finally, ethical concerns about the misuse of programmable money should be taken into consideration. Restricting the use of money based on identity information is open for exploitation and in the wrong hands might cause discriminating actions on personal, organizational, or even governmental levels. Therefore, necessary regulatory frameworks should be investigated and established by the regulators.

6. Conclusion

Increasing global interest in the issue of a digital currency provides an opportunity to review current payment infrastructures and think about new ways to handle our money. Programmability can become one of the new features that can increase the control and trust over the money. We propose that the self-sovereign identity paradigm can bring different benefits once it is incorporated into a programmable money ecosystem. These include increased trust through trusted institutions, provision of data sovereignty for the users, decentralization, and unification for flexible spending conditions. Verifiable credentials can be utilized to provide awareness to the programmable money in different dimensions. In addition to compliance with the essential properties of SSI, Blockchain technology offers a platform for realizing such a programmable money ecosystem that can allow trusted and easy transactions between multiple parties. We believe that the proposed concept may yield new opportunities for the development of trusted payment processes and as a consequence also for the creation of DAOs.

References

[1]. M. Avital, R. Beck, J. L. King, M. Rossi, R. Teigland, Jumping on the blockchain bandwagon: Lessons of the past and outlook to the future, in *Proceedings of the 2016 International Conference on Information Systems, (ICIS 2016)*, Dublin, 11-14 December 2016.

[2]. Diem Project Website (https://www.diem.com/).

[3]. P. G. Sandner, J. Gross, L. Grale, and P. Schulden, The digital programmable euro, libra and cbdc: Implications for european banks, 2020.

[4]. M. Avital, J. Hedman, L. Albinsson. Smart money: Blockchain-based customizable payments system, *Dagstuhl Reports*, Vol. 7, Issue 3, 2017, pp. 104–106.

[5]. R. Soltani, U. T. Nguyen, A. An, A new approach to client onboarding using self-sovereign identity and distributed ledger, in *Proceedings of 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1129–1136.

[6]. V. Schlatt, J. Sedlmeir, S. Feulner, N. Urbach. Designing a framework for digital KYC processes built on blockchain- based self-sovereign identity, *Information & Management*, Vol. 59, Issue 7, 2022, p. 103553.

[7]. I. Weber, M. Staples, Programmable money: Next-generation conditional payments using blockchain, in *Proceedings of the 11th International Conference on Cloud Computing and Services Science (CLOSER)*, 2021, pp. 7–14.

[8]. J. Lund, J. McCaleb, M. Kennedy, N. Drury, Charting the evolution of programmable money, *IBM Institute for Business Value,* 2019.

[9]. M. J. Casey, P. Vigna, In blockchain we trust, *MIT Technology Review*, 2018.

[10]. A. Chepurnoy, A. Saxena, On contractual money, 2019.

[11]. C. Elsden, T. Feltwell, S. Lawson, J. Vines. Recipes for Programmable Money, in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–13.

[12]. D. Karakostas, A. Kiayias, Filling the tax gap via programmable money, 2021, *https://arxiv.org/abs/2107.12069*.

[13]. A. Mühle, A. Grüner, T. Gayvoronskaya, C. Meinel. A survey on essential components of a self-sovereign identity, *ArXiv*, 2018.

[14]. M. G. Shashank, V. Sangeetha, H. Shilpa, An exploratory study on self-sovereign identity powered by the blockchain technology, *EasyChair,* 2021 Preprint no. 5484.

[15]. A. Tobin, D. Reed, The inevitable rise of self-sovereign identity, White paper, *Sovrin Foundation,* 2016.

[16]. A. Grech, I. Sood, L. Ariño, Blockchain, self-sovereign identity and digital credentials: Promise versus praxis in education, *Frontiers in Blockchain*, Vol. 4, 2021.

[17]. C. Allen, The path to self-sovereign identity, 2016.

[18]. M. S. Ferdous, F. Chowdhury, M. O. Alassafi, In search of self-sovereign identity leveraging blockchain technology, *IEEE Access*, Vol. 7, 2019, pp. 103059–103079.

[19]. J. Andrieu, A technology free definition of self-sovereign identity, in *Proceedings of 3rd Rebooting Web Trust Design Workshop*, 2016, p. 4.

[20]. G. Laatikainen, T. Kolehmainen, P. Abrahamsson, Self-sovereign identity ecosystems: benefits and challenges, in *Proceedings of the 12th Scandinavian Conference on Information Systems*, 2021.

[21]. J. Strüker, N. Urbach, T. Guggenberger, J. Lautenschlager, N. Ruhland, V. Schlatt, J. Sedlmeir, J.-C. Stoetzer, and F. Völter, Self-sovereign identity - foundations, applications, and potentials of portable digital identities, Project Group Business & Information Systems Engineering, *Fraunhofer Institute for Applied Information Technology FIT*, Bayreuth 2021.

[22]. K. Schmidt, A. Mühle, A. Grüner, C. Meinel, Clear the fog: Towards a taxonomy of self-sovereign identity ecosystem members, in *Proceedings of 18th International Conference on Privacy, Security and Trust (PST)*, 2021, pp. 1–7.

[23]. M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, C. Allen, Decentralized identifiers (dids) v1.0: Core architecture, data model, and representations, *W3C,* 2021.

[24]. H. Wang, H. Qin, M. Zhao, X. Wei, H. Shen, W. Susilo, Blockchain-based fair payment smart contract for public cloud storage auditing, *Information Sciences*, Vol. 519, 2020, pp. 348–362.

[25]. X. Ye, K. Sigalov, M. König, Integrating bim- and cost-included information container with blockchain for construction automated payment using billing model and smart contracts, in *Proceedings of the International Symposium on Automation and Robotics in Construction*, Vol. 37, 2020, pp. 1388–1395.

[26]. D. Allessie, M. Sobolewski, L. Vaccari, F. Pignatelli. Blockchain for digital government, *Publications Office of the European Union*, 2019.

[27]. D. Royal, P. Rimba, M. Staples, S. Gilder, A. B. Tran, E. Williams, A. Ponomarev, I. Weber, C. Connor, N. Lim, Making money smart - empowering NDIS participants with blockchain technologies, 2018.

[28]. Kela, Smart money specification document v1.0, *tietoEVRY,* 2020.

[29]. T. Kolehmainen, G. Laatikainen, J. Kultanen, E. Kazan, P. Abrahamsson, Using blockchain in digitalizing enterprise legacy systems: An experience report, in Klotins, E., Wnuk, K. (eds.) Software Business. ICSOB 2020. Lecture Notes in Business Information Processing, Vol 407, *Springer*, 2021, pp. 70–85.

[30]. U. Der, S. Jähnichen, J. Sürmeli, Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution, *arXiv:1712.01767*, 2017.

(008)

The Missing Piece of Blockchain Governance: Information Governance and its Transition to a Decentralized World

Trinh Nguyen-Phan
University of British Columbia, Vancouver, Canada
Tel.: + 16046189719
E-mail: trinh@student.ubc.ca

Summary: Blockchain governance is considered a fundamental aspect of in blockchain design. The literature on blockchain governance has chiefly focused on social and technical governance, whereas information governance has been subordinated to a product of technical governance. Using the three-layer model of blockchain that perceives blockchains as socio-informational-technical systems and a systematized literature research method, this paper posits that information governance (IG) deserves an equivalent discourse as is given to social and technical governance. Information governance informs the technical governance and adjusts the social governance aspects of blockchain. The differences in the core values of IG between the traditional (centralized) model and the contemporary (decentralized) model suggest that, in order to harvest the full potential of blockchains, we need to re-imagine IG principles for a more decentralized world or re-engineer blockchains to enhance their compatibility with traditional IG principles, or both.

Keywords: Blockchain, Blockchain governance, Information governance, IG, Decentralization.

1. Introduction

As a platform that connects multiple independent parties, the role of governance in blockchain technology, which is necessary to achieve coordination among participating parties, can hardly be overstated [1]. Yet blockchain governance research remains nascent and a source of confusion [2]; this also presents additional challenges in the integration of blockchain with existing information systems [3].

To understand blockchain governance, we must understand what blockchain is. The extant literature is replete with definitions emphasizing blockchain's technical constructs and social impact perspectives. These two themes usually go hand in hand and signify the focus of the research community on the socio-technical aspects of blockchain.

There is not yet a consensus on what blockchain governance means except the general reference to the process of decision making and collaboration of the stakeholders in a given blockchain [4], [6]. This paper will draw upon an international standard definition to understand it as a *"system for directing and controlling DLT systems including the distribution of on-ledger and off-ledger decision rights, incentives, responsibilities, and accountabilities"* [5].

Notwithstanding the importance of existing definitions of blockchain technology and blockchain governance, they overlook a crucial aspect of blockchains: information. This paper therefore adopts Lemieux and Feng's [6] three-layer model, which conceptualizes blockchains as socio-informational-technical systems [1], [3], [7]. We assert that the discourse of blockchain governance has overlooked the informational aspect of the blockchain ledger. This paper aims to problematizes the deficit of information governance (IG) consideration within blockchain governance and examines the challenges of migration of IG from the traditional centralized paradigm to the decentralized blockchain paradigm.

This paper raises three considerations. First, it highlights a blind spot in blockchain governance research, being IG. Second, it promotes understanding of IG, which is a relatively new research area needing understanding and consensus concerning its scope, definitions, and development. Third, it directs attention to the decentralized governance powered by blockchain technology. Understanding the transformation from a centralized to a decentralized model vitally affects organizational collaboration and, concomitantly, IG.

2. Methodology

Due to the lack of research at the intersection of IG and blockchain governance, this paper surveys the literature using a systematized literature review method [8]. The research was conducted in a systematic, traceable, and reproduceable way. Search terms, database, and search limitations were recorded along with the search results, number of items, abstracts, and their relevance.

The search was conducted in academic databases (LISTA), Google scholar, and Google. To search for IG literature on LISTA, we used the search string *"information AND governance AND models AND framework OR model OR theory"* and limited the research to academic publications from 1977 to 2021. The LISTA search resulted in 433 results. After skimming their title and abstract, we filtered 26 relevant articles, with relevance determined based on a qualitative assessment. The search for literature on *"blockchain governance"* in LISTA returned nine

results. A close reading filtered six studies directly relevant to blockchain governance [4], [6], [9–12]; the other results included blockchain use case research [13, 14] and one book review [15].

2. Findings

2.1. Blockchain Governance Primarily Focused on Technical and Social Governance

Most publications on blockchain governance that were retrieved during this study propose frameworks to assess or mitigate the challenges in blockchain governance from a socio-technical perspective. This is unsurprising given the past emphasis on the blockchain technical construct and social impact. For instance, [4], [6] described a blockchain governance model that emphasizes the social aspects; [10] proposed a technical solution for a policy-based on-chain governance model; [11], [12] look at blockchain governance from a combination of technical and social lenses. The socio-technical governance model generally refers to the technical infrastructure and the institutional framework surrounding a blockchain. [9] is the only study looking at the intersection between blockchain and IG from the perspective of the General Data Protection Regulations (GDPR).

Even though most studies seemingly overlooked the informational aspect of blockchain governance, they indirectly mention the imperative role of information management in blockchain via key concepts of IG such as “security”, “genuineness of a transaction”, “transparency”, and “accountability”. This speaks to the implicit role of IG in the design of blockchains and that the need to explicitly consider IG as a part of blockchain governance might not be fully acknowledged by researchers outside of the discipline of records and information management.

2.2. Traditional IG is Conceived of as a Function Performed within a Single Organization

The scholarship on IG is characterized by various definitions, models, and standards. The consensus, though, is that IG is an emerging research subject and that its growing popularity is driven by an exponential increase in the amount of data that organizations capture and manage.

Traditional definitions of IG focus on the managerial aspects of information flow, high-level strategic and methodological approaches to IG, and the normative aspects of using information. Despite these different perspectives, these definitions assure IG is a function performed within a single organization.

2.3. Traditional IG is being Decentralized

Empirical examples suggest that IG exceeded focal organization boundaries even before the adoption of blockchain and other distributed ledger technology. For example, cloud data storage is considered a hybrid model for record keeping, bridging between the traditional centralized model and a fully decentralized model [16]. It is no longer a question of whether decentralized governance will disrupt organizations and society, but how [16].

3. Discussion

In this paper, IG is anchored on eight principles of the Generally Accepted Recordkeeping Principles which consists of *Accountability, Transparency, Integrity, Protection, Compliance, Availability, Retention*, and *Disposition* [17]. We note that these principles have been designed with centralized record keeping in mind and thus there is a need to consider their applicability and suitability in the context of decentralized ledgers.

Reflecting on these eight principles and their relationship to blockchains, the decentralized governance of blockchain emphasizes integrity, security, availability, and retention of information recorded in the ledger. Blockchain governance references a topic that traditional IG models seem to lack: resilience. Blockchain governance, however, leaves open concerns for accountability, compliance, and disposition of records. Due to its decentralized nature, there is also no central trusted party to be held accountable for the records on the blockchain. This distributed, or even lack of, accountability is considered a major area of risk when organizations migrate their traditional IG to blockchain [16].

4. Conclusions

The discourse on blockchain governance and IG is emerging, and there is little consolidation of existing understanding. This study suggests that there are discrepancies between the core values of IG in a traditional centralized model and the emerging decentralized models of blockchain governance. This insight suggests that in order to harvest the full potential of blockchain, we either need to re-imagine existing IG principles or re-engineer blockchain to enhance its compatibility with those principles – or perhaps even both.

References

[1]. M. Zachariadis, G. Hileman, and S. V. Scott, Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services, *Information and Organization*, Vol. 29, No. 2, pp. 105–117, Jun. 2019.

[2]. V. Zamfir, Blockchain Governance 101, *blog.goodaudience.com*, 2018. https://blog.goodaudience.com/blockchain-governance-101-eea5201d7992 (accessed Dec. 02, 2021).

[3]. D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, A Survey on Blockchain for Information Systems Management and Security, *Inf. Process Manag*, Vol. 58, No. 1, Jan. 2021.

[4]. K. Jones, Blockchain in or as governance ? Evolutions in experimentation, social impacts, and prefigurative

practice in the blockchain and DAO space, *Information Polity*, Vol. 24, 2019, pp. 469–486.

[5]. ISO/TS 23635:2022, ISO/TS 23635:2022(en) Blockchain and distributed ledger technologies — Guidelines for governance, *ISO*, 2022. https://www.iso.org/obp/ui/#iso:std:iso:ts:23635:ed-1:v1:en (accessed Oct. 16, 2022).

[6]. R. van Pelt, S. Jansen, D. Baars, and S. Overbeek, Defining Blockchain Governance : A Framework for Analysis and Comparison, *Information Systems Management*, Vol. 38, No. 1, 2021, pp. 21–41.

[7]. V. L. Lemieux and C. Feng, Conclusion : Theorizing from Multidisciplinary Perspectives on the Design of Blockchain and Distributed Ledger Systems (Part 2), in Building Decentralized Trust, *Springer*, 2021, pp. 129–163.

[8]. M. J. Grant and A. Booth, A typology of reviews : an analysis of 14 review types and associated methodologies, *Health Info Libr J*, Vol. 26, No. 2, 2009, pp. 91–108.

[9]. D. Hofman, V. L. Lemieux, and A. Joo, The margin between the edge of the world and infinite possibility, Blockchain, GDPR and information governance, *Records Management Journal*, Vol. 29, No. 1/2, 2019, pp. 240–257.

[10]. T. Dursun and B. B. Üstünda, A novel framework for policy based on-chain governance of blockchain networks, *Inf. Process Manag*, Vol. 58, No. March, 2021.

[11]. E. Tan, S. Mahula, and J. Crompvoets, Blockchain governance in the public sector : A conceptual framework for public management, *Gov. Inf. Q*, Vol. 39, No. 1, 2022, p. 101625.

[12]. O. Rikken, M. Janssen, and Z. Kwee, Governance challenges of blockchain and decentralized autonomous organizations, *Information Polity: The International Journal of Government & Democracy in the Information Age*, Vol. 24, 2019, pp. 397–417.

[13]. K. Behnke and M. F. W. H. A. J. Marijn, Boundary conditions for traceability in food supply chains using blockchain technology, *Int. J. Inf. Manage*, Vol. 52, No. March 2019, 2020, p. 101969.

[14]. G. Schwabe, The role of public agencies in blockchain consortia : Learning from the Cardossier, *Information Polity*, Vol. 24, 2019, pp. 437–451.

[15]. J. Savirimuthu, Blockchain Regulation and Governance in Europe, by Michèle Finck The Blockchain and the New Architecture of Trust, by Kevin Werbach, *International Journal of Law and Information Technology*, Vol. 27, No. 3, Sep. 2019, pp. 306–309.

[16]. V. L. Lemieux, C. Rowell, M. L. Seidel, and C. C. Woo, Caught in the middle ? the era of blockchain and distributed trust, *Records Management Journal*, Vol. 30, No. 3, 2020, pp. 301–324.

[17]. ARMA.org, The Principles®. https://www.arma.org/page/principles

(009)

A Primer on Bitcoin

Md Abir Hossain [1] and Nazir Ullah [2*]
[1] Nanjing University, School of Business, Department of Marketing, Nanjing, China
E-mail: abirxhossain@hotmail.com
[2] Nanjing University, School of Management, Department of Management Science and Engineering, Nanjing
Tel.: +8613072553011
[*] E-mail: nazirabaz@gmail.com

Abstract: No one can neglect the great contribution of cryptography researcher David Chaum who used cryptographically signed tokens. The primary goal of bitcoin's creation is to address flaws in monetary standards, particularly the assurance that its supply will not be subject to policymakers' whims, and one that relies on transparency. However, bitcoin's radical nature provides no revenues, money streams, or income, there is yet no undeniable theory depicting how it should be priced. Bitcoin prices have a lot of short-term volatility, which makes it difficult for them to be used as a reliable unit of account. Various conditions can be altered in the future as a result of non-state actors' political, operational, and economic contributions to the use of virtual currency.

Keywords: Bitcoin, Digital, Currencies, Crypto, Risks.

1. Background of a Study

Virtual currencies bring many potential benefits in this competitive era, like greater speed and efficiency, especially in cross-border transactions, ultimately promoting financial inclusion. Developing virtual currencies from scratch requires high computational infrastructure, technological sophistication, and extensive networking. However, at the same time, virtual currencies pose considerable risks as a potential vehicle for terrorism, money laundering, fraud, and tax evasion [1]. The topic of Bitcoin actually includes the terms "Bitcoin, Bitcoin, Bitcoins, Bitcoin Mining, Bitcoin Exchange, Bitcoin Value, and Bitcoin Price". On 3rd January 2009, the first 50 blocks, known as "Genesis Block", Satoshi Nakamoto sent 10-bit cryptography nine days later. With the growing conversation about bitcoin, interest in digital currencies has dramatically increased. Its key features include; easy to use in daily life with a volatile exchange rate, easily measurable and divisible, reduced cross-border transaction costs, and no need for a central authority to safeguard its value, called completely decentralized authority. Bitcoin is pseudonymous in nature; each user is represented randomly, cryptographically string of digits that doesn't disclose the real identity of any user. The study of Eric Lockard [2] explained that the utilization of Bitcoin, while not yet standard, is developing past the early devotees. We anticipate that this development will proceed, and enabling individuals to utilize bitcoin to buy our items now enables us to be at the front edge of that pattern. The study of Yelowitz and Wilson [3], for the first time, systematically examined the determinants of interest for Bitcoin users by analysis of Google search. The study findings confirm that computer programming and illegal activity search terms significantly influence the bitcoin interest; however, libertarian and investment terms show no effect on bitcoin interest. The study of Baek et al. [4] investigated bitcoins as a speculative vehicle, and the study findings showed strong indication to suggest that uncertainty of bitcoin is inside due to (buyer and seller) so driving leads to the conclusion that the digital currency market is very speculative. The external factors have less impact on the market returns; bitcoin currency is 26 times more speculative than standard and has poor 500 indexes. The study of Healy et al. [5] analyzed that Twitter is an intriguing case of a judgment gadget in the bitcoin market, which can be delegated as cicerone that gives a field to faultfinders and pundits to remark on and endeavor to coordinate the market.

The main purpose of bitcoin creation is to overcome the deficiencies of the monetary standards, particularly on the assurance that its supply won't be at the instinct of regulators, and one that depends on transparency. The safety of its supply originates from an expected to be uncrackable algorithm. To upgrade and strengthen trust in the unwavering quality of the block chain, a Secure Hash Algorithm (SHA) formula is incorporated as a component of the calculation. The SHA is designed by the US National Security Agency and produced a long value (hash) for all purposes, one of a kind, yet with the extraordinary characteristic that, notwithstanding knowing the specific formula and the outcome, it can't be figured out to distinguish the factors utilized (one-way work). There have been various renditions of the SHA produced for various purposes. Bitcoin has embraced SHA256, which utilizes 256-piece encryption. The calculation of each block (mining) is greatly memory-concentrated and requires the intensity power of various PCs. Subsequently, the individuals who commit their opportunity and their PCs to this undertaking share in a reward that is paid, obviously in bitcoins [6].

1.1. Peer to Peer Technology Development

The first step regarding the development of bitcoin took place by Napster and Gnutella technology. Later, BitTorrent did a great job. They allow users to access information by connecting with anonymous on the Internet for the exchange of data. There are three simple ways you can obtain bitcoins. The first and most widely accepted is to buy it online from the marketplace; the second way is to accept them as payment for goods and services. The third way is to mine for bitcoins using supercomputers to solve cryptographic algorithms underlying the bitcoin protocol, producing new bitcoins. The most important characteristic of bitcoin is a store of value. The network or scene around bitcoin apparently has little connection with the lumpy social reality of numerous developing economies [7]. In 2014, NASDAQ launched its Private Equity Exchanged to provide key functionalities like investor relationship management and capability for the pre-initial public offering (IPO) or private companies. On 29th May 2014, the Dish network announced the bitcoin for satellite service to give the currency its well-known seller to date. On 26th January 2015, New York Stock Exchange approved the establishment of the Bitcoin Exchange. In June 2015, New York financial services released the Bit License. Later in June 2016, the US Department of Homeland Security is committed to six block application development company subsidies to allow companies to research data analysis, connected devices, and blockchain. On January 2016, the British government, for the first time, released a research report, "block chain: books distributed technology". In early 2016, Japan's financial service agency submitted a bill with regard to domestic economic management for Japan's national legislature off change brings. It allows bitcoins to become an asset, which gives the exchange the introduction of anti-money laundering and KYC rule. Later on, in May 2016, Japan approved the first digital currency regulation bill and is defined as a property bill. In March 2016, Australia Post began to explore blockchain technology applications in identity recognition. In 2017, Australia Government used blockchain technology for electronic voting purposes. The National Bank of Australia has successfully transferred money to the Canadian Imperial Bank of Commerce by using ripple technology ($10 transaction from one employee account in another within 10 seconds). The realization of bitcoin has fetched ahead the introduction of new cryptocurrencies and a powerful framework for decentralized applications. The study of Gupta et al. [8] explained that the US central bank created a blockchain-based chain digital coin called "Fed coin". As it has a legal tender along with the International currency of the US Dollar, so fed coin has been considered as "good money", in that it can have a short-run rate of return and long-run store of stable value as secured by fed imposing a 1:1 exchange rate with the American dollar. In Singapore, more than 15000 customers have invested in the famous Coinbase Business. The famous cryptocurrencies companies are Coin Pip, BitX, Tembusu System, and Coin supermarkets, that effort on a fuzzy idea from bitcoin still with minor changes.

2. Key Challenges

There is still no undeniable theory portraying how bitcoin ought to be priced since, by its extreme nature, it yields no profits, money streams, or income. Bitcoin prices exhibit a high degree of short-term volatility, limiting their ability to serve as a successful unit of record. Bitcoin's regular volatility will result in direct and indirect costs for businesses and consumers. Firms that use bitcoin must adjust costs on a regular basis, or they risk experiencing a drop in profits or a lack of competitiveness. This is particularly troublesome for organizations trading bitcoin yields when paying for creation factors and moderate contributions to nearby standard currency such as the British Pound, US dollar, Euro, Yen, resulting in errors in relative yield costs and contributions to the nearness of high bitcoin value unpredictability. Numerous fluctuation thusly winds up befuddling to buyers, as it turns out to be harder to identify the genuine prices of products. The Study of P. C. Phillips et al. [9] contends that bubble expansion can be seen as somewhat unstable conduct.

2.1. Crytographic Risk

Engineers composing their own software have regularly wound up losing cash because of mistakes in their transactions code. At the time, the MtGox, an extensive bitcoin trade, once lost more than 2000 bitcoins by incidentally transferring them to invalid un-spendable targets. The Blockchain.info, an online information and bitcoin wallet supplier, had an unobtrusive cryptographic error in its exchange, creating code that reused definite parts of the key to uncover the client's mystery keys enabling anybody to take their coins [10]. Throughout the Years, the developers and business network had become more mindful of these risks; anyway, concerning each venture, secure plan improves still regularly take a rearward sitting arrangement to rapidly pushing out a client confronting item, an approach that winds up costing beyond a reasonable doubt.

2.2. Security Risk

If e-commerce applications have a security issue may lead to many costly effects, but not to the complete loss of funds. While in bitcoin, having the possessions of a digital equivalent of physical cash-once lost couldn't be recovered. Bitcoins on a web-associated gadget build the severity of loss, subsequently ensuing to framework penetration by lawbreakers by different viruses. Statistics suggest that anywhere in the range of 30% and 50% of all is simply

not a secure place to store bitcoins. A digital wallet provides service to users, such as an online bank account, obviously moving a great part of the burden of safety onto the wallet developer. Be that as it may, the trust in these service providers was frequently lost; the same number of wallet providers lost client coins to these same problems because of insufficient privacy practices. No one can forget the five major incidents of the Bitcoin market; on 19th June 2011, Mt. Gox famous Japan based-Bitcoin Exchange (Amount Hacked: 2609 BTC | +750,000 BTC), on September 2012, BitFloor (Amount Hacked: 24,000 BTC), on 4th March 2014, Poloniex (12.3% of all BTCs (97 BTC), on 4th January 2015, Bitstamp (Amount Hacked: 19,000 BTC) and on August 2016, Bitfinex (Amount Hacked: 120,000 BTC) [11].

2.3. Government Regulatory Risks

In the early years, developers were working on a best-figure premise in light of the fact that there was no governing direction about which guidelines apply to bitcoin and what governing agencies will assert this region as their own [12]. There was also a sensible dread that governments may turn out with decides that will extremely handicap advancement by setting substantial consistence loads on businesses working in this space, by expanding existing managing an account/banking cash services controls to bitcoin services.

2.4. Counter Party Risks

The cash-like nature of bitcoin needs a great deal of trust with respect to the customer for the business that is receiving payment. The risk of loss because of the deceptive nature on the part of the trader, either in neglecting to deliver the guaranteed items, supplying the bad quality or the broken goods is significantly higher without the liability security and safety afforded by the traditional payment methods such as credit cards [13].

2.5. Personal Information Risks

Numerous bitcoin specialists require noteworthy personal information regarding their customers to consent to AML and KYC controls [14]. This constraint raises the risk of the potential loss of safety protection or agreement of individual private data, an issue that has tormented outdated merchant systems and monetary services in a few salient system negotiations in recent years.

2.6. Bad Reputation in the Eye of Be-Holder

The bitcoin protocol has several built-in limitations; among them, the main problem is each block's size, the number of signature operations, the total number of bitcoins, block reward structure, and average time per block. In developing countries and some emerging markets, many people don't have access to technology, scalability issues (e.g., data retention, delayed transaction confirmation, and communication problems), loss/theft of bitcoins (accidental loss, malware attacks), and structural problems like deflationary spiral. Many economists have ignored bitcoin because they feel that bitcoin is fairly new and its risk cannot be accurately quantified, so it's better not to use bitcoin. The experiment at MIT highlights the issues ahead of virtual exchange systems. In 2014, Bitcoin Club delivered every of MIT's 4,494 undergraduate students with $100 in bitcoin. Intriguingly, thirty percent of apprentices even didn't sign up for free currency. Within a few weeks, twenty percent of students converted their bitcoin into cash. Another best example can be Scotland, which has issued Scotcoin but couldn't get proper support in the market. Most insurgent organizations lack the basic skills necessary to deploy a cryptocurrency, like low physical infrastructure in politically contested territories and penetration of communication technology platforms (such as smartphones). In contrast, famous payment innovators (PayPal, Stripe, Payoneer, Alipay, WeChat, Samsung Pay, Apple Pay, Square, Google Wallet, etc.) especially Easy Paisa a mobile money transfer system in Pakistan and M-Pesa system in Nigeria works well, have convenience mechanism and require low technology as compare to crypto currencies [15]. There are as yet numerous deterrents in the way forward for bitcoin, in any case. Maybe the greatest one is the legitimate status of digital money, with a few nations keeping up an out-and-out boycott and others intensely confining it utilizes. The implementation of any new currency and users' trust in new digital currencies is very low. It entails large economic, logistic, and technological changes. The financial guidelines underlying a cryptocurrency need to be identified and sustained for the long term. Privacy is one of the significant assets of any exchange while investigating a digital currency is crucial because neither the seller nor buyer requires knowledge of its history. The speculators, money-related writers, and different members in the bitcoin market have been stating – that bitcoin has been on the rise over its generally short presence. Their outcomes offer belief to the case that the biggest one bubble had for sure blasted, and this may have been in charge of the end of bitcoin's greatest exchange– Mt Gox. In August 2016, bitcoin worth $72 million was stolen from the Hong Kong bitfinex exchange, which exposed security issues on BCT applications. The Bitcoin 40 famous exchanges had found that 18 had been shut down after digital assaults. Many Marijuana addicts were using bitcoin for buying buds from bitcoin vending machines. Bitcoin-based frameworks were used for tax evasion (money laundering) and financing psychological oppressors (terrorists), underground remittance systems in developing countries like Hawala. In January 2016, Netherland

state Dutch police detained ten persons as part of an international investigation by large bitcoins transfers. In 2013, US marshals directed an auction of 30,000 bitcoins detained from transactions in Silk Road network market, which was closed by the US state mediators in the fall of 2013. Utilizing digital forms of money to purchase legitimate genuine products would absolutely be one approach to restore criminal continues. Various national specialists particularly point to web-based betting services and even to the obtaining of tokens in internet diversions (online games) in such manner.

Blockchain-based cryptocurrencies present numerous lawful and administrative difficulties, including buyer insurance instruments, implementation strategies, and potential outcomes for taking part in illicit exercises, such as tax avoidance and the offer of unlawful products. They likewise present a few potential advantages for nationals, including decreased costs, enhanced security, and a more open and creative money-related framework. These and different issues were perceived in an ongoing movement at the European Parliament, which also featured the more extensive capabilities of blockchain innovations beyond the financial sectors and required a proportionate administrative methodology and the improvement of suitable limit and mastery at the Europe Union level.

4. Conclusion

In the future vary situations can be changed through the role of non-state actors politically, operationally, and economically towards virtual currencies usage. Non-state actors created secure cyber services like encryption platforms. Aurora coin can be the best example of political cases motivated and deployed in Iceland by Baldur Odinsson (March 2014) as an alternative fiat currency that could be less susceptible to inflation and are not subject to the Iceland government rules. Central authority can play a key role in the development and value of virtual currencies, which ultimately could bring a significant role in building and maintaining communities. The best examples of community currencies can be Salt spring dollars, Ithaca Hours, Ora currency, frequent flier miles, and Totness Pounds system. For regulation of currency software, developers would have to design some software. Just like miners can be the best example for decentralized bitcoin currencies. IP masking techniques such as Tor would have to build into digital currency software for the prevention of HUMINT methods and cyber-attacks (Mt. Gox, Gold finger, and DDoS attack). The key components that require development in the future include cryptocurrency itself, containing several significant design choices; the means of acquiring, maintaining, and transferring digital currencies as part of international physical means capable of supporting such transfers like smartphones. To support all these services securely, sufficient back-end services and a front-end payment processing system are required. While observant examination can reveal those that utilization various arrangements of open keys to complete transactions, new services such as, Bitcoin Fog and Dark Wallet proposed to improve the obscurity of exchanges by enabling unlawful exchanges to carefully piggyback on non-illegal exchanges– this is like the blending of assets of funds that is regular in tax evasion. Due to the verification of transactions, the high-cost problem can be unraveled through the issuance of a national bank electronic cryptocurrency, 24x7, international currency named, and enthusiasm was bearing access to a national bank's balance sheet. No matter what the context, it can be deemed acceptable and have a strong possibility that Blockchain will disrupt your organization. Indeed, the very big question is "When". In the next ten to twenty years, what other technologies do we have to anticipate? However, still more work to be done.

References

[1]. K. John, M. O'Hara, and F. Saleh, Bitcoin and beyond, *Annual Review of Financial Economics*, Vol. 14, 2021.

[2]. M. Polasik, A. I. Piotrowska, T. P. Wisniewski, R. Kotkowski, and G. Lightfoot, Price fluctuations and the use of bitcoin: An empirical inquiry, *International Journal of Electronic Commerce*, Vol. 20, No. 1, 2015, pp. 9-49.

[3]. A. Yelowitz and M. Wilson, Characteristics of Bitcoin users: an analysis of Google search data, *Applied Economics Letters,* Vol. 22, No. 13, 2015, pp. 1030-1036.

[4]. C. Baek and M. Elbeck, Bitcoins as an investment or speculative vehicle? A first look, *Applied Economics Letters,* Vol. 22, No. 1, 2015, pp. 30-34.

[5]. K. Healy, M. Hutter, and W. N. Espeland, Lucien Karpik Valuing the Unique: The Economics of Singularities. Princeton, Princeton University Press, 2010, *Socio-Economic Review,* Vol. 9, No. 4, 2011, pp. 787-800.

[6]. N. Arnosti and S. M. Weinberg, Bitcoin: A natural oligopoly, *Management Science,* 2022.

[7]. S. A. Sarkodie, M. Y. Ahmed, and P. A. Owusu, COVID-19 pandemic improves market signals of cryptocurrencies–evidence from Bitcoin, Bitcoin Cash, Ethereum, and Litecoin, *Finance Research Letters,* Vol. 44, 2022, p. 102049.

[8]. S. Gupta, P. Lauppe, and S. Ravishankar, A Blockchain-Backed Central Bank Cryptocurrency, *Yale University*, 2017.

[9]. P. C. Phillips, S. Shi, and J. Yu, Testing for multiple bubbles: Historical episodes of exuberance and collapse in the S&P 500, *International Economic Review,* Vol. 56, No. 4, 2015, pp. 1043-1078.

[10]. B.-J. Park, The COVID-19 pandemic, volatility, and trading behavior in the bitcoin futures market, *Research in International Business and Finance,* Vol. 59, 2022, p. 101519.

[11]. E. S. Pagnotta, Decentralizing money: Bitcoin prices and blockchain security, *The Review of Financial Studies,* Vol. 35, No. 2, 2022, pp. 866-907.
[12]. C.-C. Wu, S.-L. Ho, and C.-C. Wu, The determinants of Bitcoin returns and volatility: Perspectives on global and national economic policy uncertainty, *Finance Research Letters,* Vol. 45, 2022, p. 102175.
[13]. A. H. Elsayed, G. Gozgor, and C. K. M. Lau, Risk transmissions between bitcoin and traditional financial assets during the COVID-19 era: The role of global uncertainties, *International Review of Financial Analysis,* Vol. 81, 2022, p. 102069.
[14]. S. Choi and J. Shin, Bitcoin: An inflation hedge but not a safe haven, *Finance Research Letters,* Vol. 46, 2022, p. 102379.
[15]. S. Jiang, Y. Li, Q. Lu, S. Wang, and Y. Wei, Volatility communicator or receiver? Investigating volatility spillover mechanisms among Bitcoin and other financial markets, *Research in International Business and Finance,* Vol. 59, 2022, p. 101543.

(010)

Wood Traceability System using Blockchain and Zero-knowledge Proof

K. Shibano [1], T. Nakajima[2] and G. Mogi [1]
[1] Department of Technology Management for Innovation, The University of Tokyo, Tokyo, Japan
[2] Department of Forest Science, The University of Tokyo, Tokyo, Japan
E-mail: shibano@tmi.t.u-tokyo.ac.jp

Summary: The system proposed in this study uses zero-knowledge proof (ZKP) to verify the traceability of wood recorded in a public blockchain. Wood is a byproduct of several states, ranging from standing trees to logs, lumber, and wood products (hereinafter "wood objects"). The advantage of using the blockchain for record keeping is that participants can freely record the information at their discretion, without any restrictions. However, the openness of the blockchain may allow a malicious third party to introduce disinformation. In this study, we employ ZKP and near-field communication (NFC) chips to eliminate the possibility of disinformation introduction. ZKP is used to prove/validate changes in the state of wood objects, and the unique nonce associated with that state is encrypted and recorded on an NFC chip. The nonce is concealed and id of the wood object is defined as hash value of this nonce. We developed a prototype system based on an Android application and an Ethereum smart contract. We confirm that wood traceability and verification can be performed using the prototype system.

Keywords: Blockchain, Traceability, Supply chain management, Zero-knowledge proof, NFC, Wood, Logs, Lumber.

1. Introduction

In this study, we propose a traceability system for trees, logs, lumber, and final wooden products based on a public blockchain and zero-knowledge proof (ZKP). The blockchain has the advantage of allowing any user to keep records on it without restrictions. Furthermore, because records can be kept semi-permanently, it is possible to avoid the loss of existing tree records. However, because anyone can input a record on the blockchain, there is a possibility that third parties will record malicious disinformation. For example, if there is a very expensive tree, a person may wish to mislead others by claiming that his log was generated by that tree. ZPK can be used to verify which trees are used to make wood and which wood products are made from which wood, eliminating the possibility of disinformation. This can be done by using only the records on the blockchain. We have developed a prototype system using an Android application and an Ethereum smart contract to verify its operation.

End users will be able to confirm the origin of wood products using the proposed system. This may provide high added value that could not be realized until now. For example, a good-luck charm for academic success in school made from a tree on the campus of the same university may have a high added value. It would also help to reduce illegal timber.

2. Related Studies

Several wood traceability systems that use blockchain have been proposed. Figorilli et al. (2018) use RFID, the blockchain, and a client-server application to implement a wood traceability system [1]. Cueva-Sánchez et al. (2020) propose a system that uses Hyperledger Fabric to eliminate illegal wood in the wood supply chain. They developed web and mobile applications [2]. There exists wood traceability system using not only blockchain but also ZKP. Xue et al. (2022) propose ZKP for a public blockchain-based system to prove transactions while ensuring privacy protection [3]. Baliyanet et al. (2021) propose a highly transparent system that utilizes blockchain and RFID for general supply chain management systems. It prevents fraud by having the Law Enforcing Agency assess transactions. They mention wood traceability as an area of application [4]. Further details on blockchain-based wood traceability systems can be found in He and Turner (2022) [5]. The novelty of this study is that it uses ZKP to prove traceability. Traceability can be verified by the information in the blockchain only.

3. Zero-knowledge Proof

ZKP is a protocol that allows a prover to tell a verifier that a proposition is true without conveying any knowledge other than that the proposition is true. We use zkSNARKs, a noninteractive zero-knowledge proof protocol used in many blockchain applications. The process to be proven has inputs and outputs and is converted into a circuit. Then, a trusted setup ceremony is performed to generate proving and verification keys. The prover generates a witness using the circuit, the proving key, and input. The verifier can confirm that the prover used the correct value for the private input using the verification key for the proof and public output. The public output is the output of the process and the value of the public input.

4. System Overview

In this system, historical state records of wood supply chains, such as trees, logs, lumber, and wood products (hereinafter "wood objects") can be verified by referring to only blockchain records. A supply chain record has a tree structure and the state changes in one

direction. We assume there are two users of the proposed system: a prover and a verifier. The prover is a wood object producer or processor, and the verifier is a consumer. The prover uses an Android application to record unique information of the wood object on a near-field communication (NFC) chip and generate a proof of ZKP. The NFC chip is attached to the corresponding wood object, and a proof of ZKP is simultaneously recorded to the blockchain when information is recorded on the NFC chip. The verifier can verify the wood object's traceability by verifying the proof. When writing to the blockchain, the signature is also recorded, allowing verification of who wrote the record. The key pair of the private and public keys of elliptic curve cryptography is stored in the Android application and can be used for signing and encryption/decryption. The Elliptic Curve Digital Signature Algorithm (ECDSA) is used for signatures, and the Elliptic Curve Integrated Encryption Scheme (ECIES) is used for public key cryptography.

5. Design of Android Application and Developing Environment

The prototype system comprises an Android application, an Ethereum blockchain, and an NFC chip.

In this system, we use circom and snarkjs [6] for ZKP as libraries to implement. Snarkjs [6] is used in the Android application to generate proof. The circuit and proving key data loaded in snarkjs are generated previously in the PC using circom, whose ZKP scheme is Plonk. Since it is a JavaScript library, it cannot be run directly in the application. A web server is set up within the application and accessed via WebView. web3j [7] connects to the Ethereum blockchain.

Key pairs associated with Ethereum's externally owned accounts are used for keys related to ECDSA and ECIES. The private key is stored in the application's storage area, bouncycastle [8] is used as the ECIES library, and web3j is used for the ECDSA library.

The Ethereum smart contract only records data for which the ECDSA signature and the proof of ZKP have been verified, and the ZKP verification contract is the snarkis output.

The development environment is Ryzen 3600, 16 GB RAM (Windows 10), the Android device is Pixel3a (Android 12), the Ethereum blockchain is built locally using Ganache [9], and the NFC chip is MIFARE Classic 1k. Fig. 1 shows the Android device and NFC chip used in the development.

6. Proof of Traceability by Zero-knowledge Proof

A random number called "nonce" is encrypted and recorded on the NFC chip with its id. Each wood object w has a unique id created, as expressed in (1),

$$id_w = hash(nonce_w). \quad (1)$$

Fig. 1 Android device and NFC chip

Ids are used to identify wood objects and are related to other metadata in or outside the blockchain. When running a proof/verification process, an error occurs if the id and nonce of the previous wood object state p is not available. In this process, the public input is the id of p, the private input is p-nonce and w-nonce, the main process is the calculation of the hash value, and the output is the id of w. The flow of the process is shown in (2). If w is a tree, p-nonce is assigned to 0, and p-id is assigned to a hash value of 0. Process (2) is converted into a circuit using circom [6]. Proving and verification keys are generated based on the circuit. The circuit data and the verification key are built into the Android application. The verification process using the verification key can be performed using an Ethereum smart contract.

```
function CalculateID (
  public input p_id,
  private input p_nonce,
  private input w_nonce) {
  p_hash = hash(p_nonce);
  p_eq = p_hash == p_id;
  w_hash = hash(w_nonce);

  return w_hash * p_eq;
}
```

(2)

After a nonce is generated using the prover's Android device, it is recorded on an NFC chip and then discarded. ECIES encryption is performed using the public key in the device, and the encrypted nonce is recorded on the NFC chip with the id. Therefore, once a nonce is written on the NFC chip, only the prover can decrypt it by reading the NFC chip. To generate an id of wood objects without trees, the parent's nonce is required. The device that recorded prestate in the NFC chip can read and decrypt nonce on that NFC chip. That nonce is received separately from that device, and along with its generated nonce, the public output and proof are generated in the process (2) and recorded in the blockchain. A QR code is used for transmitting the previous id and nonce between Android devices.

The sequence of all process is shown in Fig. 2. This shows an example that a log is generated from a tree. The first row shows initial setup procedure on PC.

Output results are a circuit file and proving and verification keys. The circuit file and proving key are built-in Android application. The verification key is used for smart contract in the blockchain. The second and third rows show how to record the information of the wood objects in the blockchain using Android application.

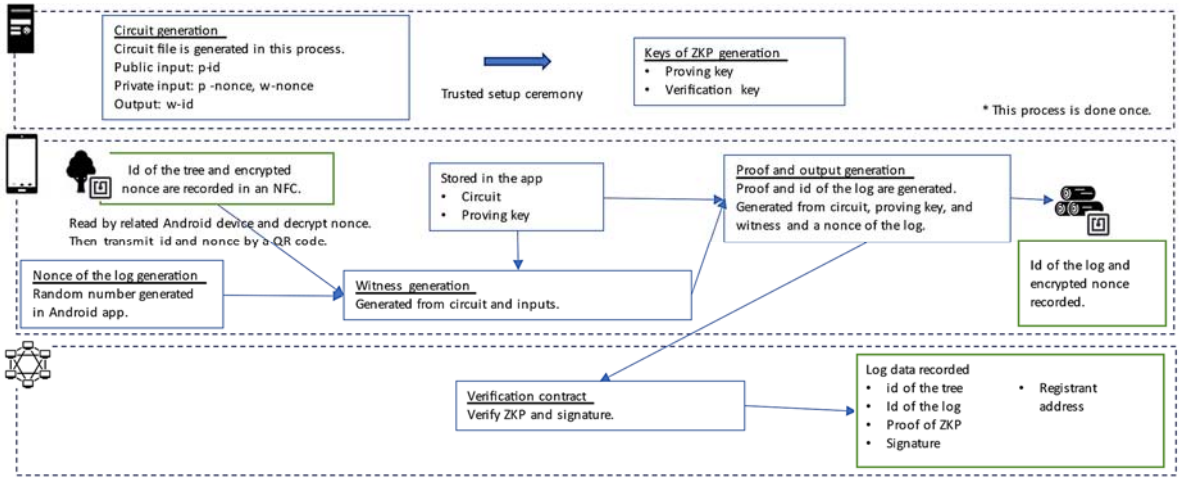


Fig. 2. Schematic of the process flow, from tree to log.

7. Prototype Experiment

We confirmed that the developed prototype system works correctly. We have simulated a scenario where we cut down a tree and generated a log from it. We conducted two tests: (A) whether the NFC chip can be attached to an actual tree and remain without peeling off over a long period of time and (B) whether verification using the application worked properly.

(A) To check whether it is safe to leave the NFC chip on the tree, it was taped to a tree in a forest managed by the University of Tokyo. We confirmed that it remained there for 6 months without incident (Fig. 3).

Fig. 3. A tree with an NFC chip.

(B) Next, we confirmed that only records verified by ECDSA signature and ZKP are recorded in the Ethereum blockchain. There are two Android devices: one for the tree and another for the log. The device for the tree read data from the NFC chip, decrypts nonce, and transmitted the tree nonce to the device for the log by a QR code on the app. The log device generated a new nonce and id of the log. Then, this device generates an id and an encrypted value of the new nonce to a new NFC chip. The proof and public output were recorded in the blockchain.

Table 1 shows data recorded in the blockchain. Each record contains w-id, id of its previous wood object, or p-id, the proof of ZKP, ECDSA signature, and address of Ethereum. In the first row, the value of p-id is a hash value of 0. w-id of the first row and p-id of the second row is the same. For these two records, the verification of ZKP proof and the ECDSA signature was confirmed in the smart contract, proving that the nonce value of the previous wood object is known to the recorder when generating the second line's record. The ECDSA signature guarantees that the owner of the address performs this process. In other words, it verifies the traceability of a tree object and the recorder's address using only the information recorded in the blockchain.

Generally speaking, ZKP proof generation requires much computation and is time-consuming. In the circuit of this study, the number of constraints is 731. We measured the time required to generate proof on an Android device and found that the average time for ten trials was 5,858.6 milliseconds. Pixel3a is a middle-class device several years old, and this time is considered sufficient for practical use.

The gas consumption for the smart contract was 1,030,996 [gas], 10 trials on average, approximately 40.2 USD in terms of gas prices in October 2022 (1 gas = 30 gwei, 1 Ether = 1,300 USD) [10, 11]. The transaction cost is high because of the many processes involved in the smart contract, such as verifying ZKP and signatures and registering information.

Table 1. Examples of records recorded in the blockchain.

w-id	*p*-id	Proof of ZKP	Signature	Registrant
370043348911802728 70661006398477818 47103961878055352 65523417069132915 9298675	11730251359286723 73114146609570990 14501703690945782 88842486979042586 033922425	0x1442dc394b656ea374badd091dfbfd97f4f33dd5169a2011024fa6cb572dd1f417ac1a4c6cd7a9116a1db945ef7abe6daf4ff28d24fa9500 28032d6a3cdbee652e48db375c34b66021969ff6e5947880cedc60dbc143eafb3ccbc56c0bb9bd7e18fdac8731746f68fb981bcaf336e93229 2c6ed4651cd3051595af1a466331e214e1e92e22d440fa39f862a70eab3c9d185ab2b418cf1240b0153d7a8cea5a2a2b429c4f4566234b4d9 92b4ebc5cb004ed9bf90af689669c29700ffb2dcb0534915a2f7374c96da26ec3e6ab403c4eea885a07fed8ba3c7add1936665fc534df912095 dd0709c363b47fa00cd6939f6f9883ed7e0dac90f77f9e95a01981fa77891da585e5f7d4fdc1dc5897a85cb8c087c7f68ab4adebff9259696d4 cb19513c11c780ede61a29d7e0bb6caf55201a45e128ce47f885a8c36e7370833b4c718ba11e5ffea03e47897152e1eac6487a9a5ffccf6243 b872e18b9aa6c86b8356360f05204553de4fdbf0e1e478e26eebe4896351ab2c1e29f572401a2aa35b4def9e2cb7fb242a833ff1bb5ae94f35b 7b02e91468c05a08e3dcdd2ba57765cff7114244b6c06df88b453b02fbf8766e7aae58456024c8f47ab00297998e5a335b8672ddde1d14e9f fb17fcb6344fea9126fca4b84da2b95f2a43ed1c40a2d1cd450c904a41568c4aa4779a0bdf92f744ea75602c9c8ba55a1c682d7b1b762cdec9c 141799554a867d1226a33296333debc223a50e7d2265ca2459a704b8222c8439611e5fe6265253130420a8ba66a6c9b8be47b3afc05a201d f8a961bbb99433b5fc18288608379a62935f042e51bf3bd72c20443721bb52ba3dfe177932aaa06da714eda9c3e08a3f59bc6f28059b33b32 39e628eb70aa2b4a2634ec3662c6fe66e24c8fc8e3c4ad92b81d2dd659ac348b2726bd52aa1d73bfc1f2d323b6cc8145220acbf20046736fc 75a6bf0bf984f2cb9df497b15547b534ae2cf8bf54c9ee6a0abc28a8463ef19d93b6a1f5eb5c43892f167467623417a6a9c1f28f79687e011d6 3b48d3c3d3b38829db2306d0ae9bdfd6a3213e67ac650293a8f04c66f480704034e0b0cf764e08cd557828063b00e2c98180d9eb829dc3c4 3db91172b9a59	0xa9f3dc7267e499aa7b435b92c0896 374a6c9cae2af279c84fdb590b7cfe5c e894d9135ece3ccf016efcb34c7ded4c cec9f51dbb4d43cdc8a78ec28f055ce1 ff11c	0xed883ff9caf287b84e4adc7d3d 5587d5532b7e4e
190607493880360917070689790927013619637925790995905 713116413289679611404985 38	370043348918027287066100639847781847103961878055352 65523417069132915 9298675	0x23fb2a027ead674e5a7dd9d48f667974d8764f9380e5cd1f4c634f5e8824e7ee110e754f75216b6d066b3faa3a10f31a3aba4613f09302e5 e0514752dc6927bb17c3e0f2be90dbcfabaefbaed0c61824a7f512bacd5bb35e6d41953172a91492026b57898e05de01f0849b9b179b40d33 068e8fbb2ff6114099 1a6f4b1ae54a21ae04d2d15d46cf7013412 5f588cb772df6c1535d133cfc53c5690f6f9bcbbf41257c32482cb63b1e89b 78885674ea96f8bf40dc96ac7039cbcc16f5df1dfda3d1a0bfa19769da0b9ed56226ae7359bf74d937ebc4206604048ce38f182b998ec2c991 8d649dbce7c82b72483b0bc0e8cb695053422ea1793183dac4ad3c500952f62344ae0a8c322ce2cb8bd1450bb9968060ff6a71b7b665d6a4 501c4f09a1a01e5701dfd5972e8badaa7c256f40cd9bfacd5201d1b0de8ab6d6cea2c917cee12f77396daeb3c084f66899c348989e9f482178 e78d0f47d8fc4b21475608fc31aa0fc53570ea50f5ebd666777f5512fdcf32915d8c5b7fd4f836746b06524ca02abe57eb712991ae187b2e74 2ffba1c12d3c663500850b08ccce82bf49cb5a22fb5f7fefd2c8bba79e566687ee524b801d64e3ff3ca44baffdf6f58e2dde58a2268e04c8774f1 5fdf4948c4d5ef6cebd004d51361ceaa31ef1446ec7ee0211731cdc4a92e229f59562072201c956c38f23cd58e90876474b8de4b1ece0279ec 614334ac094d00151c080b415811b69ed48fa145ea555501bf00e48bc7232e0e1f2822412558c755bad13a3ad0ea6f6efb42cde45f2952a1e 38ce992c8f20abd9100558002797dffb92499f8ccd5d5044a75bfe01a9212f24536d342264d3fbb85277bb96a4241d4e222d8fa979b917fab8e 115ca5be3877e2bc81cf105098dea8d078971140673077 7f086cd6541e6d78407e4429051f42d16ef899c83f2066cb62310f24124efcc0ca7 e8c9f9ec93e411bebd9b9458c4cbd31c5d6a469f5f70131728990a868e5c619b1ebc32c219eb067b150b4dca8b8b62f7f76fbadc1a0096279 21d895346c29add236c77175bfca19fc248055b0fb1a2f5949af49677b7b22602a88d26e89d229407309526a9b9d803e9515db965f917f32 a131f1421a3e1	0x68ce9d0326660610bbccdc3767fea c7f7a23203c2df8898148fc5f9a07f4 21e35d9086f9c3f771984e90e7563f6b abf431b193bf121a0db08a1f3927f989 67e41c	0xab00c6d62d94976e506d602c 31908fb89d8651e2

8. Future Work

This study's system only records the traceability relationship of wood objects in the blockchain. However, it is crucial to record additional information associated with each *w*-id; for example, GPS location information, pictures of wood objects, and tree species. Adding such information to traceability will increase its utility. To make it persistent, we plan to record additional information in a distributed database, such as IPFS.

To reduce transaction costs, we consider using another blockchain compatible with EVM.

We should also confirm whether this system can be used without problems for actual lumber processors. We plan to assess this with Japanese companies.

Although this system is applied to the traceability of wood in this study, it can be applied to the traceability of all products with the same relationships. We study what products and goods the system can be applied to and what value it might generate.

9. Conclusions

In this study, we proposed a method for verifying wood traceability using blockchain, NFC chips, and zero-knowledge proof. We constructed a prototype system and confirmed that wood traceability verification can be performed accurately. This system is a sample application of ZKP using an Android application and the Ethereum blockchain, and we hope this study's results will help develop applications using ZKP.

Acknowledgments

This work has been supported by Endowed Chair for Blockchain Innovation and the Mohammed bin Salman Center for Future Science and Technology for Saudi–Japan Vision 2030 (MbSC2030) at The University of Tokyo.

References

[1]. S. Figorilli, et al., A blockchain implementation prototype for the electronic open source traceability of wood along the whole supply chain, *Sensors,* 18, 9, 2018, 3133.

[2]. J. J. Cueva-Sánchez, A. J. Coyco-Ordemar and W. Ugarte, A blockchain-based technological solution to ensure data transparency of the wood supply chain, in *Proceedings of the 2020 IEEE ANDESCON Conference*, 2020, pp. 1-6.

[3]. Y. Xue, and J. Wang, Design of a blockchain-based traceability system with a privacy-preserving scheme of zero-knowledge proof, *Security and Communication Networks* Vol. 2022, 2022, p. 5842371.

[4]. A. Baliyan, K. S. Kaswan, Akansha, and N. Mittal, Blockchain assembled supply chains to foster secure trading using distributed ledger, in *Proceedings of the 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO*), 2021, pp. 1-5.

[5]. Z. He, and P. Turner, Blockchain Applications in forestry: a systematic literature review. *Applied Sciences,* 12, 8, 2022, 3723.

[6]. Iden3 docs, (https://docs.iden3.io/)

[7]. Web3j: Web3 Java Ethereum Dapp API, (https://github.com/web3j/web3j)

[8]. Bouncycastle, (https://www.bouncycastle.org/java.html)

[9]. Ganache, (https://trufflesuite.com/ganache/)

[10]. Etherscan Ethereum Gas Tracker (https://etherscan.io/gastracker)

[11]. Coinmarketcap Ethereum (https://coinmarketcap.com/currencies/ethereum/)

Blockchain-Based Access Control Mechanism for Internet of Things

A. Kul [1], O. Demirörs [1] and Y. M. Erten [2]
[1] Izmir Institute of Technology, Urla İzmr Turkiye
[2] Izmir University of Economics, Balçova, İzmir, TurkiyeTel.: + 905322623550
E-mail: yusuf.erten@izmirekonomi.edu.tr

Summary: In this study, Context-Aware Operation-Based Access Control Algorithm (CA-OBAC), which is proposed to create a reliable access mechanism in the Internet of Things environment, is developed on Blockchain using smart contracts to manage the access control mechanism. Thus, it is aimed to ensure the reliability of system access control processes and to keep all access request and result logs of access control processes in an unchanging structure.
Keywords: Context Aware Rule Based Access Control, Smart contract, Internet of Things, Blockchain, IOT,

1. Introduction

Access control can be defined as access to an object only by authorized parties. Various access control algorithms have been proposed in the literature, ranging from role-based access control to attribute-based access control. Adapting standard algorithms for IoT systems with a wide variety of environment variables and produced by different types of manufacturers is difficult as it requires adapting rules and specifications to this large and dynamic structure with many devices communicating with each other. On the other hand, the absence of software to ensure security on the device due to memory and power limitations increases the necessity of studies to meet security needs [1].

In this study, Context-Aware Operation-Based Access Control Algorithm (CA-OBAC), which was proposed in [2] was used in accordance with the IoT environment structure to ensure that the access rules and operation in a secure environment are immutable. It has been implemented using blockchain technology, which has features such as public key infrastructure and peer-to-peer networking, decentralized consensus, smart contracts, and data integrity, which is one of the basic security principles by cryptographically linking each block to the previous block [3].

With this study, while evaluating the rules in access control with smart contracts which are created on the blockchain, critical data such as the user requesting access, the device requested to be accessed, the transaction to be performed, the approval or rejection result information are stored in the blockchain, thus ensuring that the entire accessprocess record is kept reliably and attempted to operate.

2. Background

The Rule Based Access Control (RBAC) and Attribute Based Access Control (ABAC) are two types of access control methods commonly used. In RBAC, users cannot access resources directly. Instead, they can access depending on their role. ABAC, on the other hand, considers user, resource, and environment properties to provide access rights [4].

Since the IoT environment consists of too many variable components and environmental context, the access control models mentioned above are insufficient here. CA-ORBAC was proposed to provide access control for IoT environments. It is a model consisting of the combination of CA-RBAC and ABAC. In this study blockchain and smart contract support are added to it [5].

	RBAC	ABAC	CA-IRBAC
Method	Role based	Attribute Based	Context aware – rule based
Management	Role managing is a problem for huge organizations	Management is difficult	It overcomes the role explosion problem.
Flexibility	Roles, users and operations are tightly bound, not flexible	Flexible because of attributes.	Flexible because of attributes and associating with them instead of operations.

Fig. 1. Access Control Algorithm Comparison.

3. Proposed Model

The aim of this study is to strengthen the CA-OBAC with a system where the data is kept in a blockchain and accessed via smart contracts, so access permission, authorization and control are secured this way. It is aimedto provide a reliable access control, both suitable for the IoT structure and by making use of the Blockchain technology [6].

By ensuring that the access control process is carried out through smart contracts, a security weakness that mayoccur at this stage is prevented and the immutability ofthe access control process is also ensured.

The system is built over four smart contracts. The Smart System contract is used to create smart environments. Object contract, defines objects which are to be associated with the smart system. Users who will use the smart system are defined using the subject contract, which is managed by the system super admin. Finally, the Access Control contract is used by the system to evaluate the incoming request in the context evaluation phase of the CA-ORBAC algorithm and to grant accessto the authorized user when a request is received.

Smart Contract codes are written using Solidity language. Truffle was preferred as the development environment. The Ganache program was used to establish an Ethereum Blockchain locally to test Solidity Smart Contracts The Metamask interacts between Ganache Ethereum Blockchain and web3.js on the client side.

The formulas used when calculating the access control system complexity are given below.

Permissions (P) defines the operation permissions thatcan be performed for each object. It is given as the product of number of objects (N_{OB}) and number of operations (N_{OP}) as shown in equation 1.

$$P = N_{OB} * N_{OP} \quad (1)$$

Security Policies (SP) represent the sum of the security policies that will be operated on the basis of valid contexts with each valid authentication method of each role. It is given as the product of roles (N_R), policies (N_P) and contexts (N_C) (Equation 2).

$$SP = N_R * N_P * N_C \quad (2)$$

A smart home application has been proposed to verify this approach. The flow in the CA-OBAC algorithm has been modified as shown in Fig. 3 in order to introduce the smart contracts.

4. Application of the Model

There are certain objects that are relatively unchangeable compared to other components in the designed smart system or any IoT environment, and it is desired that these objects continue to work according to the rules defined from the beginning and that the access to these devices is carried out smoothly according to the determined rules. It is aimed to create a reliable access control mechanism that cannot be changed by creating a smart contract for each object in order to ensure access control, since it is the main goal that the objects work according to a certain policy and that their accessibility is reliable due to the data they carry.

In the smart home scenario, there are subjects like the parents, children and e.g., babysitter. There are also objects like the main door, household appliances etc.

Each of the subjects has permissions to interact with the attributes of the objects, such as “the parent is authorized to open the door”. The number of the subjects,objects and the rules defining the interaction among them determine the complexity of the system.

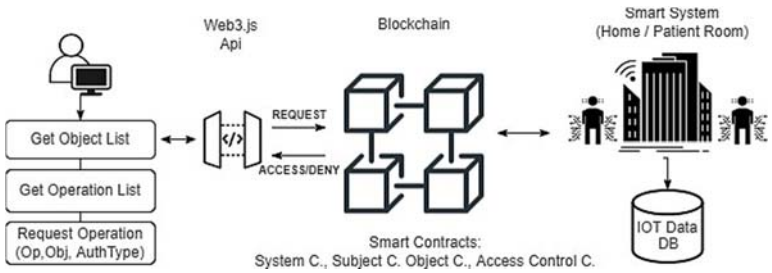


Fig. 2. General structure of system design.

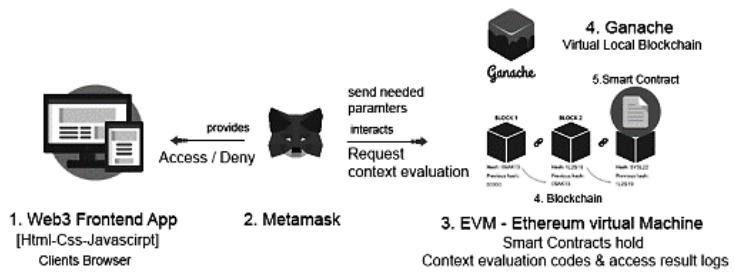


Fig. 3. Detail of Platforms.

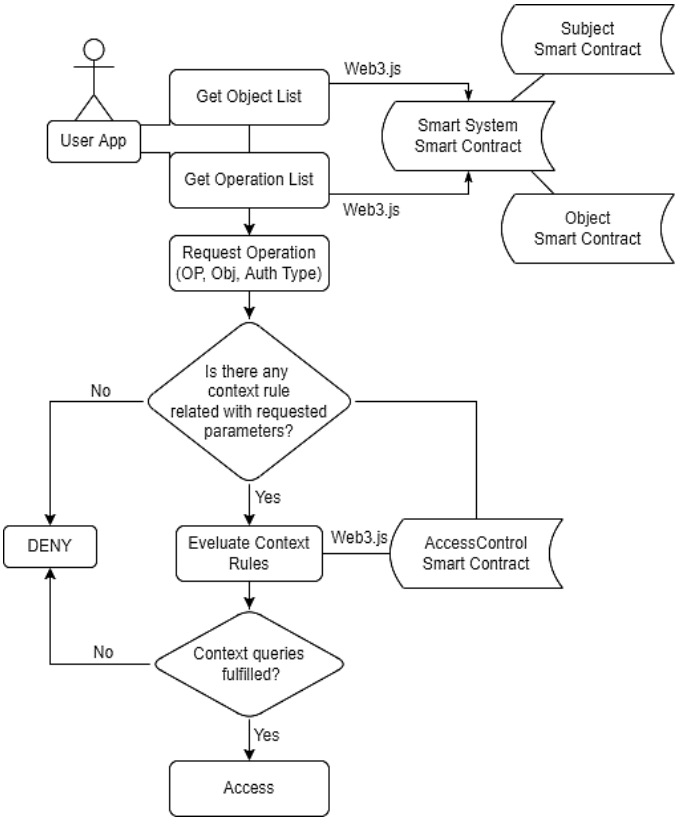


Fig. 4. The Modified CA-OBAC Algorithm.

Table 1. Access Control System Variables.

Authentications	2	Biometric, Mobile Device
Number of Object Attributes	4	Smart Door, Camera, Household Appliances, Wearable Devices
Number of Contexts	16	Subject Attributes: Parent, Children, Babysitter, Home app. Healthcare app. Distance Parents' Approval: yes, no Sb. In front of door: yes, no Location: inside house, outside Time: working hour, school hour Emergency: yes, no
Number of Operations	3	Date: Read, Open, Turn off

The complexity of scenarios are compared in Table 2 for different access control algorithms.

In the proposed algorithm where the blockchain is involved, the number of operations is the same as CA-OBAC, but access request and evaluation of these request are kept in the blockchain, hence an extra burden will be introduced in terms of processing time. In our test environment, a smart contract function returns results on average in 150 seconds, and block generation takes an average of 3 seconds.

The validated transactions per second can be maximized by using proof of authority instead of proof of work which will improve the performance.

Smart Contract Contribution: According to the security policy created for each object in the project, the decision mechanism of evaluation transactions is on the Smart Contract. In addition to the implemented access control algorithm referred from [2] to in this study, the security policies of each object are controlled by Smart Contracts. Smart Contracts of objects are assumed to be deployable to the Ethereum private network by the authorized user. Object Smart Contracts are stored in an encrypted and secure shared ledger.

The features, restriction of IoT environments and the contribution of the used technologies and the algorithms are given on the Tables 3 and 4.

Table 2. Complexity of different algorithms for smart home scenario.

	RBAC	**ABAC**	**CA-OBAC**
Complexity	1170	780	384

Table 3. IoT and Standard Access Control Algorithms Features and Restriction.

Features and Restrictions	
IoT	**Standard Access Control Algorithms**
Centralized	
Limited Bandwidth and Resource	Role, rule numbers etc. increase cost for IoT
Large Number of Devices	Complex for IoT
Security Problem	
Scalability is low and expensive	Not flexible

Table 4. Blockchain, Smart Contract and CA-IRBAC Contributions to the System.

Contributions		
Blockchain	**Smart Contract**	**Context Aware Access Control Algorithm**
Decentralized	Autonomy	Dynamic
Cost Saving	Trust	Flexible
Immutability	Security	Reduce Complexity
Security	Transparency	
Scalable		

The main security gains can be listed as follows.

Privacy: It was tried to ensure that policy changes can only be made by the authorized person, and the security of access to IoT devices was ensured by preventing outside interventions.

Immutability: During the context evaluation, all necessary access parameters and the evaluation result are stored on the smart contract, and an immutable log information is automatically kept for access requests.

Single Point of Failure: Our model uses a distributed access control points, which eliminates the single point of failure.

Another scenario has been tested to see how the CA-IRBAC algorithm can be used in non-IoT environments. The system is designed as an appointment tracking system where doctors who want to provide personalized online counseling services and those who want to get counseling from them can create and manage online appointments.

An appointment that can be controlled (created, cancelled, etc.) according to different user types, such as objects in the IoT environment, and has different states is accepted as an object. Users can be people and applications like in IoT applications. In order to perform an operation related to the appointment, it is important who the user is, the time and the current status of the appointment. These take the place of attributes in IoT applications.

5. Conclusions

A solution was proposed to secure access control using blockchain to hold the components and smart contract to hold the rules. The proposed solution improves the security of the system and does not increase its complexity. It also eliminates the single point of failure through the blockchain and smart contracts. It, however, introduces some processing overheads as expected.

The system has also been implemented for a patient monitoring systems and a medical appointment system and similar results were obtained.

References

[1]. Liang, Wenbing & Ji, Nan, Privacy challenges of IoT-based blockchain: a systematic review, *Cluster Computing,* 25, 2022, pp. 2203–2221.

[2]. D. Genç, E. Tomur and Y. M. Erten, Context-Aware Operation-Based Access Control for Internet of Things Applications, in *Proceedings of the International Symposium on Networks, Computers and Communications (ISNCC),* 2019, pp. 1-6.

[3]. Marc Pilkington, Blockchain Technology: Principles and Applications, Research Handbook on Digital Transformations, *Edward ElgarPublishing*, 2016.

[4]. D. Kulkarni and A. Tripathi,Context-aware role-based access control in pervasive computing systems, in *Proceedings of the 13th ACM Symposium on Access Control Models and Technologies*, 2008, pp. 113-122.

[5]. R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, Blockchain-the gateway to trust- free cryptographic transactions, in *Proceedings of the 24th Eur. Conf. Inf. Syst. (ECIS)*, Istanbul, Turkey, 2016, pp. 1–15.

[6]. R. Mahlous and A. Ara, The Adoption of Blockchain Technology in IoT: An Insight View, in *Proceedings of the 6th Conference on Data Science and Machine Learning Applications (CDMA),* 2020, pp. 100-105.

(012)

A Reward-based Blockchain Platform for Exchanging Goods and Services

M. Fiore, F. Nocera and M. Mongiello
Department of Electrical & Information Engineering, Polytechnic University of Bari, Bari, Italy
E-mail: name.surname@poliba.it

Summary: Blockchain technologies have been spreading since their first financial implementation in 2008. Lots of new platforms were born in the last decade, with the aim of creating new tools to produce wealth in the digital world. Bitcoin miners, for example, can profit by solving the Proof-of-Work consensus protocol challenge that is very expensive in terms of computational resources. Hence nowadays achieving richness in the digital world requires high quality hardware. This proposal aims to develop a platform to generate new richness without the need for the users to possess high and expensive computational resources; everyone can get the same amount of coin rewards by just joining the platform. Coins can be used for exchanging goods and services but they will not come out of the platform, so there will be a meritocratic focus and real-world daily routine transactions, rather than crypto exchange transactions.

Keywords: Blockchain, Barter, Exchanging goods and services, Proposal, Architecture.

1. Introduction

Blockchain technology first appears in 1991 as a cryptographically secured chain of blocks, with timestamps that could not be modified [1]. Its main diffusion takes place in 2008 thanks to Bitcoin. Cryptocurrencies are meant to generate a new kind of richness in an untrusted environment and without the need of a centralized third party. One way to generate new coins is through mining: with the Proof-of-Work consensus protocol, miners can receive a reward in coins when they accomplish their goal that is to find a correct hash for the new block. Nowadays, this procedure has become computationally expensive: if a user doesn't have enough computational power, he can not take benefits from the mining process.

This paper aims to overcome the difficulties of starting from a non rich situation, thus spreading a meritocratic concept of a Blockchain network. In the proposed platform, all users start with the same initial amount of coins that can be used to buy goods and services from other users. In this way, the more the user sells his own services, the more he can obtain in terms of coins. All users start with the same purchasing power and it is responsibility of the single participant to stay alive in the network. No coins will be mined or be exchanged with real money.

The paper is organized as follows: Section 2 shows some related works with a goal similar to the proposed platform one, Section 3 presents the system design with a particular attention to entities and some considerations on the target market, with two possible approaches, namely, Stablecoins and a self-levelling market, and their risks. Conclusions close the paper and set some future developments for further improving the platform design and implementation.

2. Related Work

In this section we present some related work in the field of barter applied to Blockchain.

The authors of paper [2] propose a novel economic system to exchange goods without the need of money, using Blockchain as the underlying technology. This proposal avoids the use of Proof-of-Work consensus protocol and is focalized on exchanging goods. However, it does not take into account the possibility to share services and to generate new forms of richness. Compared with this approach, our proposal aims to use coins that do not derive from mining but from offering someone's service.

Decathlon brand [3] has created a blockchain-based rewards program. It was launched in March 2019 in some test nations (Slovenia, Croatia and Serbia) with the name of Decathlon Team.

Here's an example of how the program works: A customer enters a Decathlon store to buy products, for example some football shoes. By the time she leaves the store, she can check her profile on the store app that runs on Blockchain on her smartphone to see how many medals (virtual coins) she has earned and the total number of medals credited to her account. As soon as she has enough medals, she can redeem some of her medals to receive a benefit, let's say, a two-hour lesson with a football instructor. That instructor earns the medals from the customer and can spend them to buy football-related goods from a Decathlon store.

This implementation is similar to our proposal, but, due to its industrial focus, it is based on spending real money to earn coins, so the starting point cannot be equal for anyone because it depends on how much money a customer can spend. This approach will not follow the main goal of the proposed platform, that is, no real money will be spent during the entire process.

3. System Design

The main idea of our proposal is described hereby. The user who wants to join the Blockchain can register to the platform, using a username to guarantee the pseudonimity of the Blockchain. It is important to

reach sybil resilience, so to use a mechanism to ensure that the same user will not create more than one account, otherwise he or she will get more coins than thought. A possible approach is to use a unique identifier such as the Social Security Number in America or the eIDAS ID in Europe [4], or by using the biometric techniques [5]. During the registration process, the user receives a certain amount of coins to start buying basic services. The coins available in the network depend on the number of users joining that network following the equation:

$$T = M * N = \sum_i C_i, \quad (1)$$

where T is the total available coins in the platform, M the number of registered users, N the number of initial coins per user and C_i the coins of user i. The mean of coins per user will be equal to the number of starting coins in the platform.

Fig. 1 shows a sample platform with M=10 registered users, each one starting with N=100 coins.

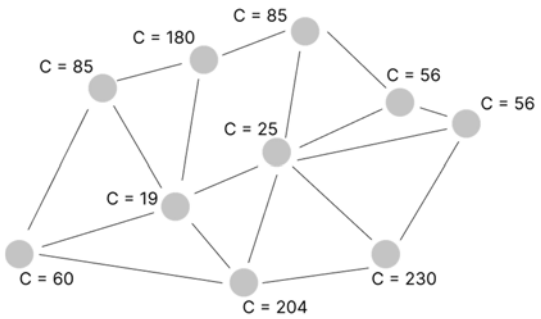


Fig. 1. Network example with 10 nodes, each one starting with 100 coins.

When a user buys a service, he or she makes a transaction in the chain that will be encrypted using the user's key. The transaction is then signed and sent to the network. Anyone can see that this transaction has been done and that the amount of coins needed for the service will be sent after the service is done.

The user cannot buy or mine new coins, so his computational power has no effect on the network; he can instead sell some goods or services to earn new coins and buy new services. This mechanism can prevent rich users from increasing their wealth in a short time or users with expensive hardware platforms from becoming richer.

3.1. System Analysis

A workflow sample is presented in Fig. 2.

User A (the buyer) makes an offer on some good or service to User B (the seller). They can use an in-app text chat to communicate, make offers and counter offers, until they reach an agreement on the price (in coins) of the selected product. After the agreement, the seller makes a request to the app to make the transaction and sign it in the Blockchain platform. The app forwards the request to the Blockchain that uses some predefined smart contracts to execute the transaction and takes the defined amount of coins from the buyer. The result of the transaction is sent to the app and back to both the buyer and the seller. After that, User A receives the good or service, she/he can declare to the app that the transaction can be completed successfully. The app will communicate with the Blockchain that will release the taken coins and give them to the buyer. The transaction is now concluded and registered to the platform.

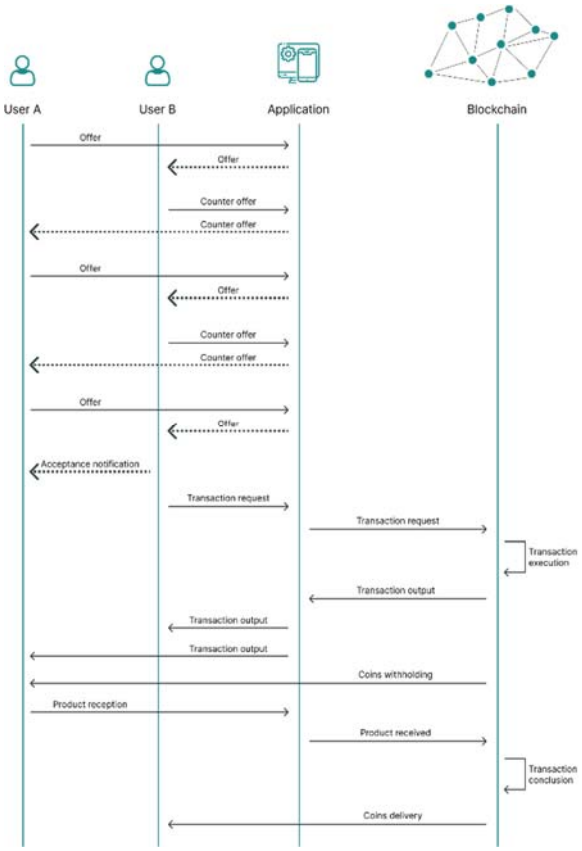


Fig. 2. Platform workflow.

In order to reach the desired goal, smart contracts will be used. Further studies will be conducted to understand if a public Blockchain (such as Ethereum) or a private one (such as Hyperledger Fabric) best fits the platform.

Ideally, participants in the network can also be the miners in the Blockchain; the more participants are in the network, the more the system becomes decentralized and, therefore, secure. Below is an example of a smart contract written in Solidity language with a basic transaction consisting of the sender's address, the recipient's address and the amount of money to purchase a good or a service (with its name and description). All transactions can be retrieved using the good or service ID through the retrieve function.

```
pragma solidity ^0.6.0;

   contract Exchange {

      struct ExchangeGood {
         address senderAddress;
         address receiverAddress;
         uint256 coinsAmount;
         string goodName;
         string goodDescription;
      }

      ExchangeGood[] public transactions;
      mapping(string => ExchangeGood) public
                        findTransactionFromID;

      function add(
         address _senderAddress,
         address _receiverAddress,
         uint256 _coinsAmount,
         string memory _goodName,
         string memory _goodDescription,
         string memory _goodID
      ) public {

         transactions.push(ExchangeGood({
            senderAddress: _senderAddress,
            receiverAddress: _receiverAddress,
            coinsAmount: _coinsAmount,
            goodName: _goodName,
            goodDescription: _goodDescription
         }));
         findTransactionFromID[_goodID] =
                        ExchangeGood({
            senderAddress: _senderAddress,
            receiverAddress: _receiverAddress,
            coinsAmount: _coinsAmount,
            goodName: _goodName,
            goodDescription: _goodDescription
         });
      }
   }
```

Fig. 3 shows the execution of the smart contract in a simulated environment: a user with address 0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2 buys from another user, with address 0xd9145CCE52D386f254917e481eB44e9943F39138, a good with name "Test product" and description "Used only few times". He spends 30 coins for that item. The transaction is stored in the Blockchain and is notarized, so anyone can check the existence of that transaction searching the good ID "TestID42".

The platform is composed by the following entities, namely:

User. A person who joins the network and receives the initial amount of coins to start buying and selling goods and services. A User can be both a Seller and a Buyer.

Product. A good or service inserted by a user that can be sold or bought.

Transaction. A record on the platform that keeps track of the two users involved, the amount of coins exchanged and a timestamp.

An overview of the relationship of the entities is shown in Fig. 4.

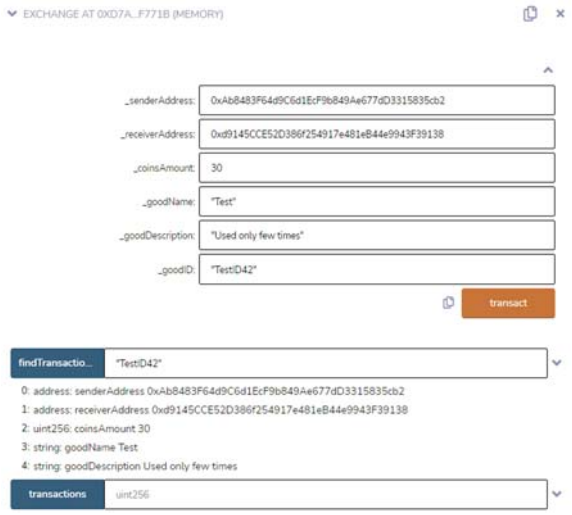


Fig. 3. Smart contract execution in a simulated environment.

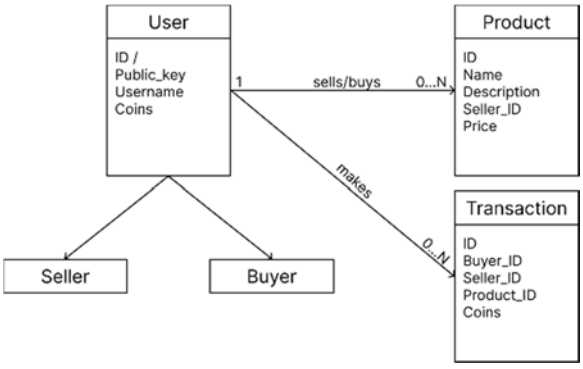


Fig. 4. Entity relationships basic scheme.

3.2. Economics Considerations

From an economic point of view, some doubts could emerge on the value of a coin in the platform. Two main approaches have been identified to address this issue:

Stablecoin approach [6]. Stablecoins are cryptocurrencies that follow the real world market, so there is no risk of speculation and no alternative markets with prices that differ from a real world situation. These kind of coins exist in the Blockchain topic; the most well-known one is Tether, a coin mainly used for payments.

Self-levelling market approach. The more challenging way is to not impose a value on a platform coin, but to let people organize by themselves on how much a coin is worth. The market will stabilize by itself after a certain number of successful transactions:

this approach will avoid to fix the price of a service (that is a consequence of fixing a starting value for a coin) and it will carry new results in the market. This self-levelling market approach at a starting point will make people sell and buy under or overpriced services, anyway this situation has a drawback.

The stablecoin approach is the simpler and safer one, but it's less innovative and challenging than the second proposal. For this reason, it could be more interesting (and risky) to follow the second idea and analyze the market transformation as quickly as customers increase. Obviously, people could sell and buy under or overpriced services in a first time, but there always is a limit at this situation.

For example, for the first two customers in the whole platform, every actor knows that the other one has a maximum amount of, let's say, 100 coins, so he would never try to sell a service for 100 coins or more, because it would be unacceptable by the other user.

From an economic point of view, the objective is to understand how the digital society will react to a kind of market similar to what was available centuries ago, when money did not have a fixed value. For this reason, validations will be analyzed after a certain number of transaction has happened in the developed platform.

4. Conclusion

In this article, we presented a proposal on a new Blockchain-based platform for exchanging goods and services. We provided a first analysis and design of the system. Some market analysis has been done in order to understand the better and most innovative approach to solve the issue of assigning a starting value to a platform coin. The impossibility to mine coins or convert them to real money makes the platform meritocratic and robust: anyone can join independently from his real-life economic situation.

Future developments of the platform are proposed as follows: implementing the platform using a public or private Blockchain, based on the defined needs; deploying new smart contracts to easily register every transaction happening on the platform and keep track of all of them; developing a cloud-based app to connect to the back-end: avoiding multiple accounts for the same person (who could register multiple times to obtain more coins); this task will be reached after the definition of the user registration process.

Acknowledgements

This work was funded by the TRACECOOP Research project (Italy) (B96G21000060005).

References

[1]. S. Haber, W. Stornetta, How to time-stamp a digital document, Conference on the Theory and Application of Cryptography, *Springer*, Berlin, Heidelberg, 1990.

[2]. K. Ikeda, M. N. Hamid, Applications of blockchain in the financial sector and a peer-to-peer global barter web, *Advances in Computers*, Vol. 111, 2018, pp. 99-120.

[3]. Oracle Blockchain Blog (https://blogs.oracle.com/blockchain/post/retailer-decathlon-sprints-to-the-finish-line-with-blockchain).

[4]. L. Argento, et al., ID-service: A blockchain-based platform to support digital-identity-aware service accountability, *Applied Sciences*, 11, 1, 2021, 165.

[5]. N. Khalili, Design and Implementation of a Blockchain-based Global Authentication System Using Biometrics and Subscriber Identification Module, Diss., *Université d'Ottawa/University of Ottawa*, 2022.

[6]. M. Mita, et al., What is stablecoin?: A survey on price stabilization mechanisms for decentralized payment systems, in *Proceedings of the 8th International Congress on Advanced Applied Informatics (IIAI-AAI)*, IEEE, 2019, pp. 60-66.

(013)

Proposal of the Technical Implementation of 3D Printers in a Blockchain-based Exchange of Capacity

N. Große[1], P. Stuckmann-Blumenstein[1], D. McInnis[2] and Y. Qiao[3]
[1] Chair of Enterprise Logistics, TU Dortmund University, Germany
[2] University of Michigan, Michigan (US)
[3] Northwestern University, Illinois (US)
Tel.: +(49)2317556347
E-mail: nick.grosse@tu-dortmund.de

Summary: Blockchain technology receives attention in research as it helps to overcome challenges evoked by information asymmetries. This offers new ways for the decentralized exchange of capacities. However, how technical assets can be connected to the blockchain remains unclear. This paper proposes a draft for the technical implementation of 3D printers as network entities for decentralized capacity exchange. By creating and deploying four smart contracts, we built a streamlined service that matches 3D printing requests between customers and printers, guaranteeing the safe transaction of payments and delivery of printed products. The goal of the service is to create a simple, transparent, and trustworthy process that can improve the customer experience of completing a printing task. Researchers and practitioners with technical backgrounds are provided with hard- and software modules necessary for technical implementation.

Keywords: 3D Printer, Transaction-lifecycle, Blockchain, Smart contract.

1. Introduction

Since supply chains are suffer from increasing dynamics and result in decentral systems controlled by cyber-physical systems (CPS), manufacturers must focus on interconnecting their production resources as cyber-physical production systems [1]. The demand for utilizing resources and avoiding uncertainties is closely linked to CPS's emergent and real-time interplay in creating new process chains in versatile value-adding networks [1].

To overcome challenges that are evoked by information asymmetries, lock-in effects and single of failures in centralized architectures, blockchain is seen as promising technology due to its potential to establish security and trust in a decentralized network [2]. Smart contracts have the potential to contribute to this solution, especially in decentralized markets [3].

Since supply chains in production may inherit sensitive data and high thresholds for implementation [4], trials are preferably conducted on small-scale transparent supply chains. Thus, a minimalistic supply chain represented by 3D printers enables a practice-oriented and transparent experimentation environment for the usage of such a platform based on a blockchain. As customers may not know all participants in a 3D printer network, platforms must provide mechanisms ensuring security for all participants and suppressing opportunistic behavior. Participants hence can request or offer capacities on a secure and reliable base.
Against that backdrop, the underlying research question is: "How to implement 3D printer into a blockchain-based capacity exchange platform?"

The contribution provides the researcher and platform designer a proposal of technical components for implementing 3D printers in blockchain-based capacity exchange platforms.

2. Related Work

Since we emphasize technical implementation, terms such as blockchain, smart contracts, and oracles are introduced and enriched with information on related work. Generally, a transaction passes four stages of a transaction lifecycle [5]: information, negotiation, settlement and after-sales. Smart contracts are limited programs running on decentralized systems, such as a blockchain, which is a practically immutable and decentralized database [6]. The interplay between on- and off-chain data is enabled by oracles as brokers for gathering 3D printer data serving as input for smart contracts [7].

3. Proposal of an Interface for Docking 3D Printer

To locate our research, we refer to the blockchain framework proposed by [8], which consists of an environmental, infrastructure, application, agent, and behavioral layer, followed by a trust frontier separating the agent and behavioral layer. Due to the technical focus set on our contribution, a particular emphasis is made on the application and infrastructure layer, which is depicted in Fig. 1. On the infrastructure layer, there are the 3D printer, which are connected to the API on the protocol layer. Furthermore, an Ethereum-based testnet, including four smart contracts, has been set up.

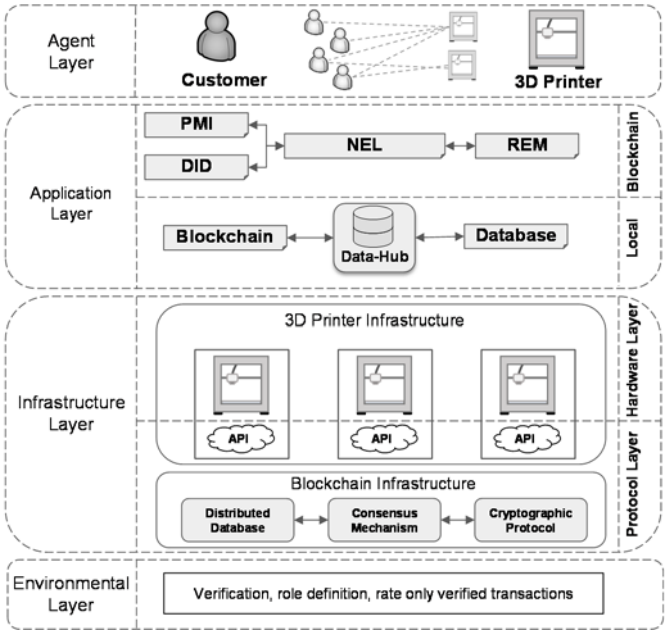


Fig. 1. Locating the interface in the blockchain framework proposed by [8].

On the protocol layer, off-chain data from the 3D printers and the corresponding API is stored by the data-hub in a local database. Each data-hub connects the local databases to the decentralized system. Hence, the network consists of centralized data-hubs forming a decentral network, whereas its interplay represents a federal system. This data-hub establishes a connection between the capacity exchange platform and the 3D printers. This ensures that only user-approved data is released to the blockchain. In particular, every supplier should operate at least one data-hub connecting the printer to the platform.

The blockchain-based capacity exchange platform consists of four interdependent smart contracts: Printer Model Identifier (PMI), Decentralized Identifier (DID), Negation Logic (NEL) and Reputation Mechanism (REM).

PMI, as a decentral database for printer specifications. Information like layer height or dimensions is stored, which are used in the DID and NEL to filter service providers without required resources. This system can also access status-related information from the data-hub. DID provides functionalities for role management (provider and demander) and linking the associated 3D printer to owner identities. This contract also ensures that the users cannot stay anonymized and can perform liquidity checks without making the assets transparent for clients. NEL forms the logic behind the system, including functionalities for specifying the demand, displaying suggestions of offers, fulfilling the task allocation and for initiating and controlling the payment. Demands can be defined with specific requirements on the platform and suppliers with the ability to fulfil the request can place an offer. REM provides the demander and supplier functionalities for rating each other after the fulfilled transaction. The score serves as a trust-enabling basis since it only allows verified users to rate a transaction. Moreover, the immutable storage and traceability of the rating encourage both participants to rate honestly.

4. Conclusions

Recent research shows the first attempts at how 3D printers are connected to smart contracts to be part of the transaction lifecycle. Besides knowledge about the appropriate design of smart contracts, a technical understanding of docking real assets remained unclear. Against that backdrop, our proposed interface shows how 3D printers can be technically connected to a blockchain-based capacity exchange platform. In an extended paper, we plan to include governance concepts and evaluation patterns to provide researchers and practitioners better guidance for their blockchain-related economic analysis in terms of transaction costs.

Acknowledgments

This research is funded by Blockchain Europe (funding code: 005-2003-0071) and Deutsche Forschungsgemeinschaft (DFG) - 276879186/GRK2193'.

References

[1]. M. ten Hompel and M. Henke, Logistik 4.0 – Ein Ausblick auf die Planung und das Management der zukünftigen Logistik vor dem Hintergrund der vierten industriellen Revolution, in Handbuch Industrie 4.0 Bd.4, *Springer Vieweg*, Berlin, Heidelberg, 2017, pp. 249–259.

[2]. N. Grosse, T. Guerpinar, and M. Henke, Blockchain-Enabled Trust in Intercompany Networks Applying the Agency Theory, in *Proceedings of the 3rd Blockchain*

and Internet of Things Conference, Ho Chi Minh City, Vietnam, 2021, pp. 8–14.

[3]. T. Gürpinar et al., Blockchain Technology in Supply Chain Management – A Discussion of Current and Future Research Topics, in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Science and Technologies for Smart Cities, S. Paiva et al., Eds., *Cham: Springer International Publishing*, 2022, pp. 482–503.

[4]. F. Kache and S. Seuring, Challenges and opportunities of digital information at the intersection of Big Data Analytics and supply chain management, *IJOPM*, Vol. 37, No. 1, 2017, pp. 10–36.

[5]. J. Gebauer and A. Scharl, Between Flexibility and Automation: An Evaluation of Web Technology from a Business Process Perspective, *Journal of Computer-Mediated Communication*, Vol. 5, No. 2, 1999, JCMC525.

[6]. DIN SPEC 16597, Terminology for blockchains, Text in English, *Beuth Verlag*, Berlin, 2018.

[7]. A. M. Antonopoulos and G. A. Wood, Mastering Ethereum: Building smart contracts and DApps, *O'Reilly*, Beijing, Boston, Farnham, Sebastopol, Tokyo, 2019. [Online]. Available: https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=5594049

[8]. F. Hawlitschek, B. Notheisen, and T. Teubner, The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy, *Electronic Commerce Research and Applications,* Vol. 29, 2018, pp. 50–63.

(014)

Towards a Multidimensional Blockchain Governance Taxonomy

S. Brüning [1], D. Bons [2], H. Schulz [1], T. Gürpinar [2] and P. Keitzl [2]
[1] Fraunhofer-Institute for Material Flow and Logistics,
2-4 Joseph-von-Fraunhofer-Str., 44227 Dortmund, Germany
[2] TU Dortmund University, Chair of Enterprise Logistics,
5 Leonhard-Euler-Str., 44227 Dortmund, Germany
Tel.: + 49-231-9473-417
E-mail: sebastian.bruening@iml.fraunhofer.de

Abstract: Blockchain governance currently is a relevant topic for both practice and research. To date, there is no task-based guidance for companies on how to implement and govern blockchain networks while combining influences of all relevant governance approaches. Based on a systematic literature review, in this paper, a first draft of a taxonomy is developed that identifies and structures the tasks for establishing a multidimensional blockchain governance. By identifying the relevant tasks in building and operating blockchain networks, the taxonomy supports companies in dealing with respective challenges. Finally, the taxonomy adds on the mainly technological oriented discussion of blockchain governance by the introduction of further tasks from an organizational, economical, and legal perspective.

Keywords: Blockchain technology, Blockchain governance, Literature review, Taxonomy, Dimensions, Holistic approach.

1. Introduction

Blockchain governance is a topic that is of great practical relevance and where there is an immense need for research. To date, no clear definition of the term blockchain governance exists in the scientific literature.

In this paper, the definition of *LAATIKAINEN ET AL.* (2021) is used: *"Blockchain governance encompasses technical and social means to make decisions [...] related to [...] business, technological, legal, and regulatory aspects of a blockchain system during its whole lifecycle"* [1, p. 72]. *LAATIKAINEN ET AL.* include five different governance approaches in their definition: corporate, IT, internet, platform, and open-source governance [1].

While blockchain governance combines multiple aspects of all these governance theories on the one hand, it also stands out from them in key respects due to the unique combination of their characteristics. To date, there is no task-based guide for companies to implement a multidimensional blockchain governance. Therefore, a multidimensional blockchain governance taxonomy is developed and proposed that includes a variety of tasks and sets companies up to face governance challenges arising throughout a blockchain system's lifecycle.

2. Methodology

Therefore, in this paper, based on a systematic literature analysis according to *VOM BROCKE ET AL.* [2], a first draft of a taxonomy is developed to answer the following research questions (RQ):

RQ1: Which tasks are necessary for setting up and operating blockchain networks?

RQ2: What dimensions build the base for a holistic blockchain governance?

For this purpose, the search string *(Blockchain AND Governance) OR (Blockchain AND Governance AND (Components OR Dimensions OR Layers))* was applied to the parameters Title, Abstract, and Key Words in the databases Science Direct, Scopus, SpringerLink, AIS eLibrary, and ACM Digital Library. This search resulted in 116 hits, which were narrowed down to 100 results after removing duplicates and then to 36 relevant sources after content analysis. These were enriched by additional sources after performing a backward and forward search and serve as a basis for the taxonomy development process of *NICKERSON ET AL.* [3] that is already established in the blockchain domain [4]. The resulting taxonomy draft was subsequently evaluated and refined ex-ante through expert interviews.

3. Blockchain Governance Taxonomy

In response to the two research questions posed, a total of 21 tasks of a multidimensional blockchain governance were identified (RQ1). After several iterations, these were classified into a total of six dimensions (see Table 1) that are assigned to the four meta-dimensions of organizational, technical, economical, and legal (RQ2).

The *organizational* part comprises those tasks that create the organizational conditions for multiple actors to collaborate within a blockchain network and therefore structures the collaboration. Its meta-dimension can in turn be broken down into three dimensions: network structure, network processes, and network participants. The network structure dimension comprises tasks whose goal is to make fundamental decisions regarding the blockchain network to be set up. The network processes dimension is oriented towards the process structure planning of an

organization. The goal of this dimension is to determine the useful and supporting processes.

In the network participants dimension that is modeled based on organizational structures, the processes previously defined in the process structure planning are transferred to areas of responsibility and defined subsequently.

The *technical* meta-dimension of blockchain governance encompasses those tasks that create the technical conditions for multiple actors to collaborate within a blockchain network. In the general understanding of a digital blockchain network, this includes both the software and hardware aspects [5].

Building or operating a blockchain-based network requires resources, but also generates added values. The equitable distribution of these factors is addressed with the *economical* meta-dimension as well as its associated tasks.

During the lifecycle of a blockchain network, jurisdictional challenges may also arise and take influence on its design [6]. The *legal* meta-dimension, therefore, includes those tasks that create or take into account the legal requirements for the operation of the blockchain network and in this way ensures their compliance on a permanent basis [7, p. 6 f.].

Table 1. Blockchain governance taxonomy draft.

Meta-Dimension	Dimension	Tasks				
Organizational	Network structure	Definition of power decentralization	Definition of access requirements	Definition of a transparency level	Identification of external relationships & dependencies	
	Network processes	Identification of business processes	Definition of standard processes	Establishment of communication channels		
	Network participants	Identification of actors (internal) and stakeholders (external)	Definition of roles (incl. rights & responsibilities)	Allocation of roles to actors		
Technical	Technical network aspects	Determination of a suitable framework	Agreement on data storage & data management	Determination of a necessary cyber-security level	Definition of required hardware and software resources	
Economical	Economical network aspects	Identification & allocation of costs	Identification & allocation of revenues	Instantiation of incentive mechanisms	Fund raising & investments	Clarification of ownership
Legal	Legal network aspects	Identification of obligatory laws & regulations		Clarification & control of compliance with obligatory laws & regulations		

4. Conclusion

In the course of this publication, the topic area of blockchain governance is comprehensively studied and structured. By highlighting the relevant tasks in the context of setting up and operating blockchain networks, companies are supported in dealing with them. It was determined that in addition to the purely technological introduction of a blockchain solution, tasks from an organizational, technical, economical, and legal perspective must also be dealt with as part of a multidimensional blockchain governance. The chosen form of structuring the tasks and dimensions enables comparison or combination with other, adjacent models like the Dortmund Management Model [8] or the Blockchain Integration Model [9]. These models describe a process that existing structures go through in order to adapt to new circumstances in general [8] or when integrating blockchain solutions in specific [9].

Since the presented taxonomy draft outlines tasks companies face when setting up a holistic blockchain governance that spans the whole lifecycle of a blockchain network, potentials for mutual complementation are to be expected.

Acknowledgements

This research is funded by Blockchain Europe (funding code: 005-2003-0071).

References

[1]. G. Laatikainen, M. Li, P. Abrahamsson, Blockchain governance: A dynamic view, in *Proceedings of the 12th International Conference on Software Business (ICSOB),* 2021, pp. 66-80.

[2]. J. vom Brocke, A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, A. Cleven, Reconstructing the giant: On the importance of rigour in documenting the literature search process, in *Proceedings of the 17th European Conference on Information Systems (ECIS),* 2009, 161.

[3]. R. C. Nickerson, U. Varshney, J. Muntermann, A method for taxonomy development and its application in information systems, *European Journal of Information Systems,* 2013, pp. 336–359.

[4]. T. Gürpinar, M. Austerjost, J. Kamphues, J. Maaßen, F. Yildirim, M. Henke, Blockchain technology as the backbone of the internet of things - A taxonomy of blockchain devices, in *Proceedings of the 3rd Conference*

on Production Systems and Logistics (CPSL), 2022, pp. 733-743.

[5]. R. Ziolkowski, G. Miscione, G. Schwabe, Exploring decentralized autonomous organizations: Towards shared interests and 'code is constitution', in *Proceedings of the 41st International Conference on Information Systems (ICIS),* 2020, p. 2319.

[6]. ISO/TS 23635:2022: Blockchain and distributed ledger technologies – Guidelines for governance, *ISO Standard,* 2022.

[7]. M. Schwarzer, T. Gürpinar, M. Henke, To join or not to join? – A framework for the evaluation of enterprise blockchain consortia, *Frontiers in Blockchain*, 5, 2022, 935346.

[8]. M. Henke, C. Besenfelder, S. Kaczmarek, M. Fiolka, A vision of digitalization in supply chain management and logistics, in *Proceedings of the 1st Conference on Production Systems and Logistics (CPSL),* 2020, pp. 277-286.

[9]. T. Gürpinar, S. Harre, M. Henke, F. Saleh, Blockchain technology - Integration in supply chain processes, in *Proceedings of the Hamburg International Conference of Logistics (HICL),* 2019, pp. 153-185.

(015)

Blockchain Research from the Perspective of Open Source Constructs - a Literature Review

F. N. Paffrath, J. Brinkmeyer, A. Gabriel and A. Mojtahedsistani
TU Dortmund University, Chair of Enterprise Logistics, Leonhard-Euler-Straße 5, 44227 Dortmund, Germany
Tel.: +49 (231) 755- 5909,
E-mail: florian.paffrath@tu-dortmund.de

Summary: Blockchain technology and the open source movement are two highly discussed topics in scientific literature. The connection of blockchain technology with open source can be seen in many open source blockchain platforms such as the open source Hyperledger Fabric. However, the interaction between both of these technologies is only occasionally discussed in science. Therefore, a systematic literature review to provide an overview of the existing knowledge on this connection was conducted. The results show how the effects of open source on blockchain projects can be visualized by considering open source as a concept of organization. Using the Inputs-Mediators-Outputs-Inputs (IMOI) model as a basic framework, the identified scientific investigations on this topic were structured in multiple categories according to stages of team projects. Furthermore, we identified several ways in how blockchain solutions can improve open source processes by addressing specific challenges of open source development.

Keywords: Open source, Blockchain.

1. Introduction

The phenomenon of open source changes the principles of how software code is developed fundamentally. The conditions, that software is considered as open source, are zero price, redistributable, unlimited users and usage, source code availability and modifiability [1]. The results of open-source innovations can be seen through many examples such as software development (e.g., Linux, Apache), content creation projects (e.g., Wikipedia, Open Street Map) or the development of hardware (e.g., Arduino) [2]. Additionally, in times of industry 4.0, open source can play an important role as an enabler for many other information and communication technologies – including blockchain networks that are dependent on open communities willing to share their data [3, 4].

Blockchain technology, as a distributed, immutable, privacy-preserving and verifiable possibility of data storage, has well-known connections to the phenomenon of open source [5]. Many blockchain projects are developed by open source communities and can be found, for example, on GitHub. One of the most popular examples is the open source blockchain framework Hyperledger Fabric which enables the open source development of applications and solutions. The open source development of blockchain projects can lead to a higher project's success for different reasons. For example, they can benefit from high code standards and continuous growth of the projects [6] and open source projects tend to be more secure as many developers can verify security [16].

Even though the phenomena of open source is a well-known enabler of blockchain development as well as blockchain research, the connection of both research areas is only occasionally discussed. Moreover, open source seems to be a natural appearance within blockchain research, without further discussing the effects of open source and community-based software development. However, seeing open source as a new form of organization in software development projects, organizational changes are going beyond the development of single processes, methods or models [2, 7]. Therefore, to understand the results of open source blockchain projects within blockchain research, also, we need to understand the effects of open source as a type of organization.

This paper addresses this gap by giving an overview of existing literature on open source within blockchain research. The goal is to determine factors as well as effects of community-based open source development within blockchain projects. On the other hand, the goal is to identify blockchain applications to enhance open source development. The following two research questions will be addressed.

RQ1: What do we know from scientific literature about open source blockchain projects regarding community-based open source development?

RQ2: What do we know from scientific literature about the ability of blockchain technology to support open source projects?

In this paper, we define all software projects that are working on implementing a blockchain as blockchain projects. Both blockchain platforms (e.g. Ethereum or Bitcoin) as well as general blockchain software are included within this definition [6].

This paper is structured as follows. Firstly, the conceptualization to understand the organizational perspective of open source and the constructs used to review relevant literature is introduced. Then, we explain our methodology of research which is followed by the presentation and explanation of our results. In

the end, we provide a conclusion by discussing the connection between blockchain research and open source research.

2. Conceptualization

The open source movement has been emerged within the last decades and opened the opportunity to bring out famous examples of open source projects such as Mozilla, Linux or Apache. This movement results in different kinds of innovations that can be grouped into four categories *legal innovation*, *process innovation*, *tool innovation* and *business model innovation* [40]. The process innovation underlines the idea of collaboration as well as open communication within the software development process. Seeing open source as a new form of organization, we are especially considering the process innovation within this paper. In line with this definition, open source projects are associated with an ecosystem of virtual connected human beings who develop interactively and efficiently solutions for processes and products. Open source ecosystems initiate a process to create solutions in cooperation with inter-organizational or independent developers. These open source communities are constituted by their democratic, voluntary and non-proprietary character. Different incentives are moving participants within open source projects such as time savings, a decrease in development costs, know-how availability, community affiliation, company promotion, a better competitive standing and human-resource opportunities drive the contribution to open source developments [2].

Within open source communities, individuals are getting together for a common goal (e.g., the development of a software product). This leads to the assumption that an open source community passes through elements of all stages which define a team [10]. The forming stage is the first step of building a group for a purpose in which confidence in the team is established, the development process is fixed and the organization is done. At the next stage, the functioning stage, team members need to feel cohesion in the group, they do adjustments towards the task and increase their knowledge by being part of a group. The last phase is the finalization which leads to the dissolution of the team. After passing all stages, a new development iteration starts, which includes new and possibly different conditions. The *inputs-mediators-outputs-inputs* model (IMOI) from llgen et al. describes this structure of a team project by extending the common input-process-output model (e.g., [12]) using a broader driving factors' definition, which is called mediators instead of process, and the influence of development cycles at the start of a new iteration[11]. The structure of the model is visualized in Fig. 1.

Crowston et al showed how this model can be used to analyze literature on open source development [10]. In this paper, we adopt this concept to answer the first research question focusing specifically on blockchain research. However, as the model focuses on organizational aspects, the model is not useful to structure applications of blockchain technology. That is why we invent new categories to answer the second research question by focusing on the process-related application of blockchain solutions.

Fig. 1. IMOI Model [10, 11]

3. Methodology

To conduct the research, a systematic literature review was performed according to the guidelines of Kitchenham and Charters that are commonly used in similar research approaches (e.g. [9]) [8].

As a first step, the search strategy was developed based on the defined research questions. Therefore, considering the aim of the paper, we used the following search string to involve articles on open source and blockchain.

KEY ("open source") AND KEY (blockchain OR bct OR dlt OR "distributed ledger technology")

The search string was applied to the Scopus database and therefore results are limited to peer-reviewed articles. In the next step, inclusion and exclusion criteria were defined by considering the research questions. Many articles name open source blockchain platforms without discussing the relationship between both technologies. Therefore, we only included articles that provide new knowledge on the interface between open source and blockchain. Using this inclusion criterion, we excluded articles that describe the use of basic open source tools during their research on blockchain without specifically mentioning the effect of open source. Also, this criteria excluded many articles that mentioned open source platforms only for data acquisition or validation purposes. Two scientists screened 263 articles according to the defined criteria. After screening the first wave of 50 articles, the results were compared to validate the clarity of the inclusion criteria.

To structure the literature qualitatively, firstly, two scientists analyzed the articles and coded the identified constructs studied in the literature. Then, the identified codes were sorted into groups in a workshop with multiple scientists involved. To conduct the review regarding the first research question, we involved the methodical approach from Crowston et al. on how to structure open source research [10]. Specifically, we adopt the IMOI model by sorting the groups of codes deductively into this model. The developed framework was evaluated iteratively considering the results from the continued screening process. To answer research question two, we inductively built categories by underlying the respective value of blockchain applications for open source projects.

4. Results

4.1. General Findings

In sum, we identified 34 relevant papers according to our search strategy. We found that papers only provide knowledge contribution to one of two research questions. As a result, 22 papers address the first research question and 12 papers address the second research question. Relevant papers were published between 2017 and 2022. Fig. 2 visualizes the number of identified papers regarding the year of publication and the addressed research question.

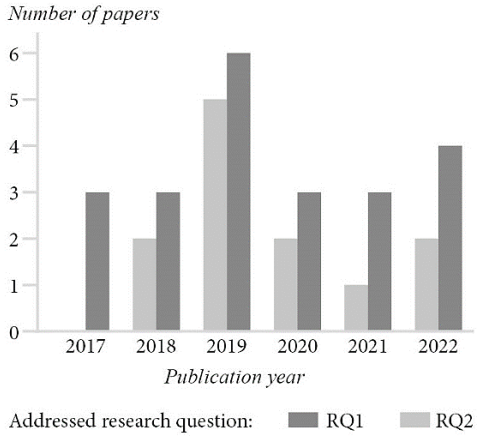


Fig. 2. Number of relevant papers published.

4.2. First Research Question

The results show that the investigated literature provides findings along each IMOI model category according to the first research question of how the effects of open source development are addressed in blockchain research.

The first construct, named *inputs*, is characterized as the circumstantial situation of a team at the beginning of their interaction. This could be the involved person's character or the aim of their get-together, e.g., a software development project [10]. Crowston et al. suggest three subcategories for this construct: *Member characteristics, project characteristics and technology use.* In our findings, we identified two papers that address the input construct specifically. The first paper examines the different member characters between open source blockchain projects and other open source projects. Therefore, it contains insights into member and project characteristics at the same time [13]. The second paper depicts the dynamic of different development aims of individuals within an open source blockchain community focusing especially on bitcoin [14]. We did not find any articles which belong to the subcategory *technology use.* So technologies to provide good code or tracks the development progress, e.g. scrum tools, are not investigated well considering the effects on open source organization.

The *mediator* category consists of the reason for influence on groups' productiveness and persistence [11]. Two major mediator categories are *processes* and *emergent states*. The process category unites all factors which target the active interconnections between the involved individuals. Following Crowston et al., three can be identified: *Social Processes, Software Development Practices and Firm Involvement Practices.* Our findings show that most articles investigate social processes. Collaboration, as one part of social processes, was highly investigated by the scientific community. The topics surround exemplary the participants' commitment to open source cryptocurrency projects [15], the interaction between blockchain developers on open source platforms [16] and the influence of open source repertoires on the blockchain social movement [17]. Further social process aspects deal with the governance and leadership in the open source supports blockchain context. The governance element depicts different organizational structures of decentralized open source blockchain projects [18, 19]. The social process aspect of leadership focuses, exemplary, on the characterization of leadership behaviors in open source blockchain communities [20]. Social Development process articles concentrate, for example, on the defect investigation of open source smart contract codes and how contributors check the quality of their code [21].

Surprisingly, we did not find any literature addressing the category *firm involvement practices*. Generally, the potential for industries within the involvement of open source blockchain projects has been investigated (e.g. [4], [9]). However, the involvement of open source projects has been identified as a challenge for companies (e.g. [39]) that should be addressed within blockchain research as well. Thus, at this point, there is a potential to do some further investigation.

The *emergent states* construct includes the characterizing properties of the team or the community [10]. Considering this category, we identified two special constructs – the *forks* of open source blockchain code and *operational risks*. In the category *forks*, some literature investigates the contributors' perspective on the differences between blockchain forks and other open source software forks [22] and, also, the influence of forking within the blockchain infrastructure on the open source community [23].

Operational risks are the second category of the emergent states construct. On the one hand, the authors investigate the open source characteristic of blockchain applications on their security against malicious attacks [24, 25]. On the other hand, the literature presents operating risks through the usage and further development of open source blockchains [26]. Thus, operational risks rise out of intentional malicious acting or accidental dysfunctions of the community.

Output constructs include all the outcomes or signs of progress toward the teams' target. The general subcategories for open source research are *software implementation, team performance and evolution.* [10]

Regarding the category *team performance*, the literature aims on comparing open source and proprietary blockchains or blockchain applications in terms of performance indicators like user activity, profitability, number of users [27] or the quality of the code [28]. A further investigative direction at the team performance layer portrays the success of different kinds of leaders, which differ in terms of dimensions like their way of acting, organization or cognitive abilities in open source blockchain communities [29].

The subcategory *evolution* encompasses the change process of the team and of the target development itself. The literature compares the progress of open source blockchain projects with other open source projects [30]. Furthermore, the influence of entrepreneurial action in open source blockchain communities and their infrastructure over time is addressed [31]. Lastly, the literature investigates open source blockchains considering them as networks that do not only evolve through their software development but as well through their users and their application of it [32].

In line with missing research on firms' involvement practices, our research does not discover any articles on open source blockchain software implementation in monetary and competitive environments that focus on the outcome effects of open source.

Our findings suggest an additional subcategory that depicts the impact of open source projects' output on blockchain. Papers within this category *impact on blockchain* are characterized by a broader discussion on the scientific or practical impact of open source research within blockchain research or blockchain projects' *impact on blockchain*. Addressing the cyclic character of the IMOI model, the literature emphasizes the impact on the characteristics of the whole project in general. One concrete example within this category highlight open source as one of the main enabler for information and communication technologies in times of industry 4.0 such as blockchain [33].

4.3. Second Research Question

Open source software provides plenty of opportunities, but also entails challenges. The literature review found four different ways, in which blockchain technology was able to facilitate facing these challenges: as part of compliance management, to enhance coordination, for minimization of operational risks and the creation of incentive mechanisms for participation. In the following section, examples of the support functions will be illustrated.

By definition, open source can be used by anyone for any purpose. However, in most companies, software needs to comply with certain policies. To ensure compliance, the development of a blockchain-based compliance platform, which automatically evaluates events in the development process is demonstrated [34]. One event triggers the creation of a new event-block and smart contracts assess compliance.

One possibility to enhance the coordination of open source projects is to provide an overview of the software provenance to all stakeholders on a blockchain [35]. Thus, relevant information about the software is easily available and accessible. A license management tool based on blockchain is another tool to support coordination [36].

Operational risks posed to open source projects can be limited through a blockchain-based ecosystem for security auditing [37]. One benefit of the system is for example the mitigation of malicious software distribution.

As open source software relies on continuous contributions of the development community, one way to support the open source concept is to provide incentives to the community by implementing a token-based incentive mechanism which reported great success [38].

5. Conclusions

In this paper, we built on the definition of open source as a way of organizing software development to review blockchain research from the perspective of open source effects. To find a structure of existing literature within this research field, the differentiation of two perspectives of blockchain research was needed to include all articles. On the one hand, open source blockchain projects are investigated to determine the organizational factors on different levels considering open source characteristics. On the other hand, literature identified the connection between open source and blockchain by identifying blockchain applications as a solution open source projects' challenges. These two perspectives are reviewed separately according to two research questions.

To answer the first research question, we built categories using an existing structure out of the open source research field. By using the structure of the *inputs-mediators-outputs-inputs* model, we could analyze the effect of open source within different levels of blockchain projects. Also, it was possible to compare results on blockchain research with general results on open source projects and reveal missing knowledge contributions within blockchain research.

Considering the second research question, we were able to detect different fields of blockchain solutions to improve open source projects. Therefore, we focused on challenging process steps within open source projects to address blockchain solutions. As a result, we found blockchain solutions to support compliance management, coordination, minimization of operational risks and creation of incentive mechanisms for participation.

Overall, the results suggest that the connection of both research fields *blockchain research* and *open source research* is promising to extend the knowledge base on both research fields. Moreover, understanding both research fields is crucial to recognize and interpreting results within one of these research fields comprehensively. Understanding the impacts of open

source and blockchain correctly, both innovations can play the role of an enabler for the other innovation. Considering the identified lack of research in this field, we hope to support the development of more knowledge contributions in the future. Furthermore, other perspectives on open source such as business model innovations or tool innovations could be a promising research area within blockchain research.

References

[1]. J. Feller, B. Fitzgerald, A framework analysis of the open source software development paradigm, in *Proceedings of the Twenty First International Conference on Information Systems*, Brisbane, Queensland, Australia, January 2000, pp. 58-69.

[2]. C. Burtet, A. C. Bittencourt, J. R. Verschoore, Open source innovation: what makes it move?, *International Journal of Business Innovation and Research*, Vol. 16, Issue 3, 2018, pp. 324-341.

[3]. G. Aceto, V. Persico, A. Pescapé, A Survey on Information and Communication Technologies for Industry 4.0: State-of-the-Art, Taxonomies, Perspectives, and Challenges, *IEEE Communications & Tutorials*, Vol. 21, Issue 4, 2019, pp. 3467-3501.

[4]. T. Gürpinar, S. Harre, M. Henke, S. Farah, Blockchain technology – integration in supply chain processes, in *Proceedings of the Hamburg International Conference of Logistics (HICL),* Hamburg, Vol. 29, 2020, pp. 153–185.

[5]. Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, in *Proceedings of the IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, USA, 25-30 June 2017, pp. 557-564.

[6]. S. Porru, A. Pinna, M. Marchesi, R. Tonelli, Blockchain-oriented Software Engineering: Challenges and New Directions, in *Proceedings of the IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)*, Buenos Aires, Argentina, May 2017, pp. 169-171.

[7]. P. Puranam, O. Alexy, M. Reitzig, What's "New" About New Forms of Organizing?, *Academy of Management Review*, Vol. 39, No. 2, 2014, pp. 162–180.

[8]. B. Kitchenham, S. Charters, Guidelines for performing Systematic Literature reviews in Software Engineering Version 2.3, Technical report EBSE-2007-01, *Keele University and University of Durham,* 2007.

[9]. T. Gürpinar, G. Guardiana, P. Asterios Ioannidis, N. Straub, M. Henke, The Current State of Blockchain Applications in Supply Chain Management, in *Proceedings of the 3rd International Conference on Blockchain Technology*, March 2021, pp. 168–175.

[10]. K. Crowston, K. Wei, J. Howison, A. Wiggins, Free/Libre Open-Source Software Development: What We Know and What We Do Not Know, *ACM Computing Surveys*, Vol, 44, No. 7, 2012, pp. 1-35.

[11]. D. R. Ilgen, J. R. Hollenbeck, M. Johnson, Teams in Organizations: From Input-Process-Output Models to IMOI models, in *Annual Review of Psychology*, Vol, 56, 2005, pp. 517-543.

[12]. J. R. Hackman, C. G. Morris, Group tasks, group interaction process, and group performance effectiveness: A review and proposed integration, *Advances in Experimental Social Psychology*, New York, USA, Vol. 8, 1975, pp. 45-99.

[13]. A. Bosu, A. Iqbal, R. Shahriyar, P. Chakraborty, Understanding the motivations, challenges and needs of Blockchain software developers: a survey, *Empirical Software Engineering*, Vol. 24, Issue 4, 2019, pp. 2636-2673.

[14]. Y. M. Kow, C. Lustig, Imaginaries and crystallization processes in bitcoin infrastructuring, *Computer Supported Cooperative Work (CSCW)*, Vol. 27, Issue 2, 2018, pp. 209-232.

[15]. S. Sarkintudu, I. Huda, A. A. Wahab, Antecedents of Developers' Commitment in Cryptocurrency Projects, in *Proceedings of the Twenty-fourth Pacific Asia Conference on Information Systems*, Dubai, UAE, 2020, p. 111.

[16]. A. Das, G. Uddin, G. Ruhe, An Empirical Study of Blockchain Repositories in GitHub, *arXiv preprint arXiv:2205.08087*, 2022.

[17]. C. I. Bogusz, J. V. Andersen, Open or just Fragmented? Mobilization through Open Source Action Repertoires in the Social Movement of Bitcoin, in *Proceedings of the 54th Hawaii International Conference on System Sciences*, University of Hawai'i at Manoa, 2021, pp. 6390-6399.

[18]. R. Ziolkowski, G. Miscione, G. Schwabe, Exploring decentralized autonomous organizations: Towards shared interests and 'code is constitution', in *Proceedings of the Forty-First International Conference on Information Systems*, India, 2020, p. 2319.

[19]. G. Miscione, T. Goerke, S. Klein, G. Schwabe, R. Ziolkowski, Hanseatic governance: understanding blockchain as organizational technology, in *Proceedings of the Fortieth International Conference on Information Systems*, Munich, 2019.

[20]. W. Mu, Y. Bian, J. L. Zhao, The role of online leadership in open collaborative innovation: Evidence from blockchain open source projects, *Industrial Management & Data Systems*, Vol. 119, Issue 9, 2019, pp 1969-1987.

[21]. L. Palechor, C.-R. Bezemer, How are Solidity smart contracts tested in open source projects? An exploratory study, in *Proceedings of the Third ACM/IEE International Conference on Automation of Software Test (AST 2022)*, Pittsburgh, USA 2022, pp. 165–169.

[22]. N. Islam, M. Mäntymäki, M. Turunen, Understanding the role of actor heterogeneity in blockchain splits: An actor-network perspective of bitcoin forks, in *Proceedings of the 52nd Hawaii International Conference on System Sciences,* 2019, pp. 4595-4604.

[23]. J. V. Andersen, C. I. Bogusz, Patterns of Self-Organising in the Bitcoin Online Community: Code Forking as Organising in Digital Infrastructure, in *Proceedings of the 38th InternationaI Conference on Information Systems (CIS)*, Seoul, South Korea, 2017, pp. 1-21.

[24]. M. Sasabe, M. Yamamoto, Y. Zhang, S. Kasahara, Block diffusion delay attack and its countermeasures in a Bitcoin network, *International Journal of Network Management*, Vol. 32, Issue 3, 2022, p. e2190.

[25]. N. Lu, B. Wang, Y. Zhang, W. Shi, C. Esposito, NeuCheck: A more practical Ethereum smart contract security analysis tool, *Software: Practice and Experience*, Vol. 51, Issue 10, 2021, pp. 2065-2084.

[26]. A. Walch, Open-source operational risk: should public blockchains serve as financial market infrastructures?,

Handbook of Blockchain, Digital Finance, and Inclusion, Vol. 2, 2018, pp. 243-269.

[27]. X. Chen, Q. Kong, H. N. Zhu, Y. Zhang, Y. Huang, Z. Jiang, Deciphering Cryptocurrencies by Reverse Analyzing on Smart Contracts, in *Proceedings of the International Conference on Blockchain and Trustworthy Systems*, Springer, Singapore, 2020, pp. 532-546.

[28]. Z. Wan, D. Lo, X. Xia, L. Cai, Bug characteristics in blockchain systems: a large-scale empirical study, in *Proceedings of the 2017 IEEE/ACM 14th International Conference on Mining Software Repositories (MSR*), IEEE, 2017, pp. 413-424.

[29]. Y. Bian, W. Mu, J. L. Zhao, Online leadership for open source project success: Evidence from the GitHub blockchain projects, in *Proceedings of the Twenty-Second Pacific Asia Conference on Information Systems,* Japan, 2018, p. 189.

[30]. J. Cao, X. Wang, Z. Li, Q. Gu, Z. Chen, The evolution of open-source blockchain systems: An empirical study, in *Proceedings of the 11th Asia-Pacific Symposium on Internetware*, Fukuoka, Japan, 2019, pp. 1-10.

[31]. K. Jabbar, P. Bjørn, Growing the Blockchain information infrastructure, in *Proceedings of the 2017 CHI Conference on Human Factors in Computing System*s, Denver, CO, USA 2017, pp. 6487-6498.

[32]. P. Nerurkar, D. Patel, Y. Busnel, R. Ludinard, S. Kumari, M. K. Khan, Dissecting bitcoin blockchain: Empirical analysis of bitcoin network (2009–2020), in *Journal of Network and Computer Applications*, Vol. 177, 102940, 2021.

[33]. G. Aceto, V. Persico, A. Pescapé, A survey on information and communication technologies for industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges, in *IEEE Communications Surveys & Tutorials*, Vol. 21, Issue 4, 2019, pp. 3467-3501.

[34]. K. Singi, P. D S (Pradeepkumar D S), V. Kaulgud, S. Podder: Compliance Adherence in Distributed Software Delivery: a Blockchain Approach, in *Proceedings of the 13th International Conference on Global Software Engineering,* Gothenburg, Sweden, 2018, pp. 126-127.

[35]. R. P. J. C. Bose, K. K. Phokela, V. Kaulgud, S. Podder, BLINKER: A Blockchain-enabled Framework for Software Provenance, in *Proceedings of the 26th Asia-Pacific Software Engineering Conference (APSEC),* Putrajaya, Malaysia, 2019, pp. 1-8.

[36]. A. Kumar, A. Gupta, L. M. Sanagavarapu, Y. R. Reddy, An approach to open-source software license management using blockchain-based smart-contracts, in *Proceedings of the 15th Innovations in Software Engineering Conference (ISEC' 2022)*, Gandhinagar, India, 2022, pp. 1-5.

[37]. Q. Hu, M. R. Asghar, S. Zeadally, Blockchain-based public ecosystem for auditing security of software applications, *Computing (Springer)*, 2021, pp. 2643–2665.

[38]. S. Liu, Research on Token Incentive Mechanism of Open Source Project - Take Block chain Project as an Example, *IOP Conference Series: Earth and Environmental Science,* 2019, pp. 1-7.

[39]. F. N. Paffrath, M. Henke, The relevance of strategic procurement within strategies for using open source as an outsourcing alternative – a structured literature mapping, in *Proceedings of the 13th International Purchasing and Supply Education and Research Association Conference*, April 2022.

[40]. D. Riehle, The innovations of open source, in *Computer*, Vol. 52, No. 4, 2019, pp. 59–63.

(016)

High-Frequency Spillover Analysis of Cryptocurrency in the Exchange Listings

Husam Bukhary, Kyohei Shibano and Gento Mogi
Department of Technology Management for Innovation, School of Engineering,
The University of Tokyo, Tokyo, Japan
E-mail: bukhary-husam320@g.ecc.u-tokyo.ac.jp

Summary: This working paper examines the cryptocurrency's exchange listing influence on intraday interdependencies of cryptocurrencies using the methodology of Diebold and Yilmaz to the 5-min return spillovers. We calculate the averaged spillovers for each pre- and post-announce exchange listing's spillovers. The empirical results show that there is no significant change in return spillover due the listing announcement in a 4-hours sample period. But the listings from the biggest exchanges showed changes; from BTC to other coins. It may be the case that big exchanges announcements are considered a shock to cryptocurrencies, hence time-varying spillover could yield interesting results regarding the cryptocurrency's connectedness in intraday.

Keywords: High-frequency data, Spillover index, Cryptocurrency.

1. Introduction

Risk management of cryptocurrencies has been highly demanded due to the increase of its market capitalization in recent years. Cryptocurrencies are known for their high volatility and correlation as Bitcoin price fluctuation contributes to the whole market. In this paper we investigate the general effect of exchange listings to understand the interconnectedness and the shock transmission in the cryptocurrency market where the exchange listing is a recurring event in multiple exchanges and understanding it would be able to gain insight into how cryptocurrencies behaves with its associated price spikes in intraday.

2. Existing Studies

The studies on cryptocurrencies spillover have mainly occurred conducted on Bitcoin and other markets where Bitcoin is the biggest transmitter [1]. The common nominator of these studies is based on daily prices. On the other hand, the studies of the intraday spillover are still limited. On the long horizon Bitcoin was and still likely the most important transmitter. However, the high volatility of cryptocurrencies could show a difference in intraday. Thus intraday spillover studies are mostly associated with big pre-and post- big events [2]. As an example, the interconnectedness between the cryptocurrencies are during the COVID-19 prices using hourly data [3].

The spillover index proposed by Diebold and Yilmaz [4] is widely used in the literature to analyze returns and volatility spillovers among different financial markets as it quantifies spillover risk at the pairwise directional level.

3. Diebold Spillover Index

We use Diebold and Yilmaz methodology to measure the spillover. This methodology is based on a VAR modeling technique which involves a subsequent estimation of variance decomposition used to measure interdependencies among cryptocurrencies log returns. It constructs spillover tables to show which currencies transmit (receive) spillovers to (from) others and in what relative proportions.

4. Data and Methodology

In this study, we gathered exchange listing announcements through Twitter links of multiple exchanges, which include the exact timing of the announcement in minutes, from Jan 19, 2019 until July 11, 2022 for a total of 846 exchange listing events.

We used 5 min aggregate price data of multiple markets of 8 fixed cryptocurrencies and the listed coin to calculate the spillover index. Listed coin stands for the announced cryptocurrency in the tweet link which is to be listed of each exchange listing event. The spillover index is calculated using log returns with variance decomposition based upon VAR of order of 1 and forecasting horizon of 10 periods pre- and post-announcement to investigate the interdependencies change of the exchange listings. Finally we average all the calculated tables to get a general view on the spillover changes.

Table 1 and Table 2 show the averages of spillover tables of all listing events for 4 hours pre-and post-announcement.

Table 1. All Announcement Log Returns Spillover.

	BTC	ETH	ADA	BNB	XRP	TRX	LTC	XLM	Listed Coin	From Others
Panel A: Pre-Tweet (n = 827)										
To Others	32.3	6	4	3.2	3.2	2.6	2.4	2.2	1.8	
Net (to - from)	27.1	3.8	-3.7	-2.8	-3.4	-4.6	-4.7	-6.1	-5.3	Total Spillover
Bidirectional (TO + FROM)	37.4	8.3	11.8	9.3	9.9	9.9	9.7	10.6	8.9	58.1
Panel B : Post-Tweet (n = 827)										
To Others	31.1	6.2	3.9	3.2	3.1	2.8	2.4	2.2	2	
Net (to - from)	26.1	3.9	-3.8	-2.8	-3.3	-4.3	-4.6	-6	-5	Total Spillover
Bidirectional (TO + FROM)	36.1	8.5	11.6	9.2	9.6	10.1	9.6	10.5	9.1	57.2

Table 2. Exchanges Log Returns Spillover.

	BTC	ETH	ADA	BNB	XRP	TRX	LTC	XLM	Listed Coin	From Others
Panel A: Binance Exchange Pre-Tweet (n = 10)										
To Others	28.6	5	2.7	3.3	2.6	3.4	2.2	2.1	6.7	
Net (to - from)	24.8	2.4	-5.6	-2.7	-3.3	-4	-4.5	-6.1	-0.7	Total Spillover
Bidirectional (TO + FROM)	32.5	7.6	11.1	9.3	8.6	10.8	9	10.4	14.2	57
Panel B : Binance Exchange Post-Tweet (n = 10)										
To Others	32.9	4.7	3.2	3.5	5	3.2	3.1	1.8	1.1	
Net (to - from)	28.7	2.2	-4.8	-2.7	-2.2	-4	-4.2	-7.1	-5.6	Total Spillover
Bidirectional (TO + FROM)	37	7.3	11.4	9.9	12.4	10.5	10.5	10.8	8	59
Panel C: FTX Exchange Pre-Tweet (n = 5)										
To Others	39.3	4.4	3.4	3.2	2.3	1.4	1.7	2	1.7	
Net (to - from)	34.8	3	-5.7	-2.5	-5.3	-6.8	-5	-6.5	-5.7	Total Spillover
Bidirectional (TO + FROM)	43.7	5.9	12.6	9.1	10	9.6	8.5	10.5	9.2	59.2
Panel D: FTX Exchange Post-Tweet (n = 5)										
To Others	30	5.5	5.6	4	2.9	2.9	2.5	3	3.2	
Net (to - from)	24.6	2.2	-2.1	-1.8	-5.3	-5.8	-4.4	-4.3	-2.8	Total Spillover
Bidirectional (TO + FROM)	35.5	8.8	13.4	9.9	11.1	11.8	9.6	10.5	9.3	60.2

5. Results

Table 1 shows the average results of all exchange listing averages. Because of inadequate space we removed pairwise direction spillover of the coins and no significant changes of their values. Next, we tried calculating the average of each exchange separately. Table 2 show the results of Binance and FTX exchange. The Bitcoin spillover To Other crypto had increases from 28.8 % to 32.9 % and Listed coin also spillover To Other decreased from 6.7% to 1.7 % in Binance case. However, Bitcoin spillover To Other decreased from 39.3 % to 30 % in FTX exchange.

6. Discussion

Cryptocurrencies landscape has gone through big changes in both market capitalization and top coins since 2019. Even though Bitcoin still dominates the market movement, projects such as SOL, AVAX and DOT have a significant proportion of the current

market. We used old cryptocurrencies to see intraday spillover throughout 3 years but the importance of those coins has decreased gradually due the emergence of newer cryptocurrencies with high market capitalization.

The overall spillover changes are lacking in current results. A normal exchange listing announcement isn't considered a shock to the cryptocurrency. However, big exchanges show changes in the pre- and post-results. It could be due; (i) the listed coins type and its market capitalization hold importance. The sample of cryptocurrencies gathered are top 500 cryptocurrencies according to coinmarketcap.com. However, not all of them have enough trading volume or strong impact on crypto interconnectedness. As the price movements are stagnating even due a listing announcement. (ii) Both Binance and FTX result assert that listing's exchange holds importance in the amount of change. The listing in these exchanges would cause a spike in prices where the interconnectedness changes momentarily. However, the sample size is too small to assert.

7. Conclusions

In this study, we apply Diebold Yimaz static spillover on 5-min data over 4 hours pre- and post exchange listing announcement. In general, there is no sudden change in spillover for those pre- and post-announcement. However, analyzing the big exchanges spillover tables, a change of value Bidirectional change has occurred. It could be argued that the exchange listing of top exchanges is considered as a shock for the cryptomarkets. In order to clarify we need to look into time-varying spillovers for such events to examine how the changes through time.

Acknowledgments

This work has been supported by Endowed Chair for Blockchain Innovation and the Mohammed bin Salman Center for Future Science and Technology for Saudi–Japan Vision 2030 at The University of Tokyo (MbSC2030).

References

[1]. George Moratis, Quantifying the spillover effect in the cryptocurrency market, *Finance Research Letters*, Vol. 38, 2021, 101534.

[2]. Yusaku Nishimura, Bianxia Sun, The intraday volatility spillover index approach and an application in the Brexit vote, *Journal of International Financial Markets, Institutions and Money*, Vol. 55, 2018, pp. 241-253.

[3]. Paraskevi Katsiampa, Larisa Yarovaya, Damian Zięba, High-frequency connectedness between Bitcoin and other top-traded crypto assets during the COVID-19 crisis, *Journal of International Financial Markets, Institutions and Money,* Vol. 79, 2022, 101578.

[4]. Francis X. Diebold, Kamil Yilmaz, Better to give than to receive: Predictive directional measurement of volatility spillovers, *International Journal of Forecasting*, Vol. 28, Issue 1, 2012, pp. 57-66.

(017)

A Taxonomy Characterizing Blockchain-Empowered Services for the Metaverse

Anjali Vaghani, Tan Gürpinar and Nick Große
TU Dortmund University, Chair of Enterprise Logistics, 5 Leonhard-Euler-Str., 44227 Dortmund, Germany
Tel.: +49 (231) 755 – 5771
E-mail: Anjali.vaghani@tu-dortmund.de

Summary: Supply Chain 4.0 ensures intelligence infrastructure, machine-to-machine communication, real-time analysis of data synchronization of the manufacturing process, and smart maintenance-based data-driven decision-making. This digitization of manufacturing processes has made the possibility of adapting digital twins. A digital twin, which assists in maximizing business performance, is a virtually real-time digital representation of a physical product or process. However, the objective of this paper is to explore how digital twins can be fitted into the metaverse to optimize supply chain processes. Developments of the metaverse are on the rise and offer links to multiple decentralized applications, such as Fungible Tokens and Non-Fungible Tokens (NFT). In this paper, we perform a structured literature review and develop a taxonomy to characterize the above-mentioned phenomenon and deliver both a theoretical and practical contribution by transferring our taxonomy into an easy-to-handle guideline for organizations that plan to offer metaverse services.

Keywords: Metaverse, Blockchain technology, Digital twin, NFT, Systematic literature review, Taxonomy.

1. Introduction

From recent crises such as COVID-19 or the war in Ukraine, we have seen disruptions in the operations of worldwide supply chain infrastructures. Key manufacturing industries, transporting goods, and suppliers are targeted in this context. Businesses must not only figure out how to get by in the here and now, but also how to get back to a new normal. It is improbable that anyone will be able to resume their previous activities prior to the epidemic. Currently, it is anticipated that the future smart supply chain should include essential components like traceability, sustainability, resiliency, and effectiveness in order to enhance the overall supply chain networks from end to end. Manufacturers must prepare for the now, the future, and beyond [1]. However, manufacturers can avoid possible pitfalls with the aid of a digital twin. Additionally, it can aid in creating a supply chain that is more robust to future disruptions. With a digital twin, simulations may be conducted with various variables changed to see the full effects of any number of situations, including supplier bankruptcy, manufacturing shutdowns, shipment delays due to shipping port congestion, or an unexpected increase in product demand. One step ahead, the metaverse will open up 3D and virtual technologies for the participants participating in the supply chain. That may spark a creative and design explosion, also, accelerating the mass customization trend. For example, Siemens and NVIDIA teamed up to enable Industrial Metaverse to achieve flexibility and transform businesses by combining the real and digital worlds [2, 3].

2. Methodology

To address the below research questions we have developed a taxonomy for characterizing blockchain-empowered Services for the metaverse which is based on a structured literature review.

1. Which role/applications does blockchain technology have in a metaverse context?
2. How can supply chain networks benefit from using the metaverse (Digital twin and NFT)?

For this purpose, we utilized state-of-the-art techniques to obtain reliable references. At first, we applied the keywords blockchain and metaverse with supply chain and digital twin in different combinations to form search strings. Then, this search string was applied to data sources such as Google Scholar and ScienceDirect not restricted to publication periods. This search resulted in 184 hits, which we then narrowed down to 86 relevant papers. After screening processes, the final sample consists of 49 publications and applied the taxonomy-building process following Nickerson et al. [4].

3. Metaverse Taxonomy

We developed a taxonomy that is necessary to construct the blockchain-empowered metaverse with the procedure (Section 2) including a total of 4 layers, 10 dimensions and a total of 35 characteristics were identified (see Table 1).

The platform layer comprises dimensions that provide various immersive services such as immersive events (Virtual Reality, Augmented Reality, Mixed

Reality, Extended Reality, Speech communication), metaverse applications (Marketing, Simulation, and Office meetings), and virtual world (Collaborative Virtual Environment, and Digital Twin). AI can also contribute to the creation of the metaverse and the way to improve users' immersion in the virtual world [5].

In the metaverse, avatars act as our digital natives. Therefore, in the social layer, dimensions included are Digital Identity (or avatar in the context of the metaverse), and Education/Onboarding [8]. For social interaction (especially in the case of the Industrial Metaverse) example, Education or Onboarding of the new trainee), can further be characterized as technical training and non-technical training.

The development layer includes the technology dimensions to further characterize the metaverse based on infrastructure, data, user experience, and security. The technology it uses is AI, IoT, VR tools, and Human-Computer Interaction [6, 7]. Well, users of the metaverse would be also able to share 3D worlds more easily without being hindered by teleoperation across various blockchain systems thanks to standardized scalability and interoperability [8].

Table 1. Blockchain services for Metaverse Taxonomy.

Layer	Dimension	Characteristics				
Platform	Immersive Events	VR (Virtual Reality)	AR (Augmented Reality)	MR (Mixed Reality)	XR (Extended Reality)	Speech Communication
	Application	Marketing	Simulation			Office
	Virtual World	Collaborative Virtual Environment			Digital Twin	
Social	Digital Identity	Digital Humans			Avatar	
	Education/On-boarding	Technical Training			Non-Technical Training	
Development	Connected Technologies	Artificial Intelligence (Automation)	IoT Devices		VR tools	Human Computer Interface
	Interoperability	Cross Chain	Cross Platform/App			Cross Web2 & Web3
Blockchain	Asset Tokenization	Digital Art	Real Estate	Intellectual Property		Venture Capital Funds	Commodities
	Marketplace Types	NFTs	E-commerce	Art Gallery	Auctions	Advertisement	Branding
	Crypto Services	Payment Services		Incentive Mechanisms		Decentralized Finance	

Finally, for the blockchain layer, we have provided blockchain-empowered services such as asset tokenization, different marketplace, crypto services such as payment services and decentralized finances, and last trust enabled by blockchain will provide the advantage of verification, security, distributed ledger, etc.

4. Conclusions

The supply chain participants will have access to 3D and virtual technology because of the metaverse. This could also unleash a creative and design revolution, pushing the trend toward mass customization. The primary objective of the paper is a taxonomy that describes the relevant characteristics of blockchain-empowered services for the Metaverse, especially in the domain of supply chain, and is supported scientifically by literature research. The topic of the metaverse has been carefully examined and addressed. A total of 4 layers, 10 dimensions, and 35 characteristics were identified. Where the first layer (platform) addresses the user's immersion and application into the virtual world. The second layer explores the virtual representation of human or digital natives. The third layer comprises the technology and infrastructure needed to operate the metaverse. And the final layer provides the blockchain services such as asset tokenization and crypto services.

Acknowledgments

This research is funded by Deutsche Forschungs-gemeinschaft (DFG) - GRK2193.

References

[1]. T. Gürpinar, N. Große, M. Schwarzer, E. Burov, R. Stammes, P. A. Ioannidis, L. Krämer, R. Ahlbäumer and M. Henke, Blockchain Technology in Supply Chain Management–A Discussion of Current and Future Research Topics. in *Proceedings of the International Summit Smart City 360°,* 2022, pp. 482-503.

[2]. J. Goldston, T. J. Chaffer, and G. Martinez, The Metaverse as the Digital Leviathan: A Case Study of Bit. Country, *Journal of Applied Business & Economics,* 24, 2, 2022.

[3]. R. Lebardian, The Metaverse Goes Industrial: Siemens, NVIDIA Extend Partnership to Bring Digital Twins Within Easy Reach, *NVIDIA,* 2022.

[4]. R. C. Nickerson, U. Varshney, J. Muntermann, A method for taxonomy development and its application in information systems, *European Journal of Information Systems,* 2013, pp. 336–359.

[5]. T. Huynh-The, Q. V. Pham, X. Q. Pham, T.T. Nguyen, Z. Han, and D.S. Kim, Artificial Intelligence for the Metaverse: A Survey, 2022, *arXiv preprint arXiv:2202.10336.*

[6]. S. -M. Park and Y. -G. Kim, A Metaverse: Taxonomy, Components, Applications, and Open Challenges, *IEEE Access*, Vol. 10, 2022, pp. 4209-4251.

[7]. T. Gürpinar, M. Austerjost, J. Kamphues, J. Maaßen, F. Yildirim, M. Henke, Blockchain technology as the backbone of the internet of things - A taxonomy of blockchain devices, in *Proceedings of the Conference on Production Systems and Logistics (CPSL' 2022),* Hannover, 2022, pp. 733-743.

[8]. M. Xu, W.C. Ng, W.Y.B. Lim, J. Kang, Z. Xiong, D. Niyato, Q. Yang, X.S. Shen, C. and Miao, A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges, 2022, *arXiv preprint arXiv:2203.05471*.

(019)

Geospatial Blockchain for Land Registration and Cadastral Data Management using Geographical Information System – A Theoretical Framework

O. O. Lawal [1], N.O. Nawari [1] and B. W. Alem [2]
[1,] Department of Architecture, University of Florida, Gainesville, USA
[2,] Department of Anthropology, University of Florida, Gainesville, USA
Tel.: +1 (352)-392-0205, fax: +1 (352)-392-4606
E-mail: o.lawal@ufl.edu, nnawari@ufl.edu, belayalem@ufl.edu

Abstract: The accuracy of cadastral information often relies on a centralized catalog of municipal records and distribution of duplicate copies to property owners. For many years, the analogue centralized records are the only repository of accurate information of land ownership and are yet not tamper-proof but highly susceptible to alterations. In recent years, scholarly contributions in the deployment of blockchain technology in land registration has been well documented. Blockchain-enhanced Geographical Information System (GIS) has also found several use cases in areas such as supply chain, healthcare and border violation detection. This research proposes a new framework that redefines the concept of trust by leveraging three unique well established concepts namely, GIS, Blockchain and Land Registration to provide immutable, decentralized ownership records. The immutability and decentralized information strata of blockchain technology is explored to develop a crypto-spatial coordinate system of land registration, which is absent in earlier blockchain-based land registration system. Geocoded description of land, its location on the earth surface and its ownership information is combined with georeferenced maps of every parcel and these geographical data are cryptographically secured in a distributed ledger.

Keywords: Blockchain technology, GIS, Land registration, Crypto-spatial coordinate system, Distributed ledger.

1. Introduction

Land is one of the most significantly valued assets of an individual [1]. The physical representation of land boundaries is the most common way to store cadastral records. These records are stored centrally within a municipal repository with each stakeholder having a duplicate information pertaining only to their own asset, without any knowledge of other neighboring assets. Land is an important aspect of human history [2, 3]. It is a pillar aspect of wealth; it is also a means for power and political representation of a certain political community. Moreover, it has cultural significance in a given society [4]. In any jurisdiction, immovable property such as land is registered and regulated more stringently as compared to other movable properties [5]. However, registration and the entire regulation of land has been subject to multifaceted vices because of the technical matters it involves in the registration process. Manual paper-based registration that has been practiced in many countries has made registration susciptible to fraud and other deceitful land management and transaction practices. Blockchain is an immutable data ledger that distributes information across different nodes, making the system less prone to malicious attacks contrary to the single point of control in practice currently. They may be private, consortium or public blockchains, depending on their degree of centralization [6]. The entries in the databases are transparent and most importantly, the integrity of the system is guaranteed by the application of cryptographic means of securing information [7].

2. Background to the Study

Land is a ubiquitous resource widely regarded as an asset with an increasingly high yield in time. It is generally accepted that an efficient, formal land registration system is an essential prerequisite for the operation of a formal land market [8]. As with all forms of asset management, the deployment of Blockchain Technology (BCT) to enhance efficiency is near inevitable. One of the early adoptions of the BCT and Distributed Ledger Technology (DLT) in the public sector is in land administration [9].

2.1. Intricacies in Traditional Land Registration

In the earliest times people have been seeking security for those who have rights or wish to have rights or intend to rely on immovable objects of property, particularly of land. Dunning (1967) observed that for centuries, ways have been sought to provide security at least for rights over immovables, which by their nature are more susceptible to identity-related fraud than movables [10]. He further argues that in the earliest times, security was provided by the performance of public acts on the immovable, for example the handing over of a piece of earth or other symbol of the land by a seller to a buyer in the presence of the assembled neighbors. Assembled neighbors served as a witness [10].

When the use of documents became more widespread, security was achieved by giving publicity to those documents, by allowing or requiring that the originals or copies thereof be filed in public institutions

such as court houses or land registration offices or public notary offices. Since the 20th century, security has continued to be achieved in many jurisdictions by the establishment of comprehensive registers, public office. Basic processes of land records management include registration of ownership, regulation of transactions pertaining to use and ownership of the land. The use of traditional technologies in supporting these activities may lead to erroneous updating of ledger, duplication of records and tempering with ledger [11].

Geographical Information System (GIS) - based BCT is a suggestive substitute to traditional paper-intensive land registration system to reduce, and possibly eliminate land disputes that arise from archaic land registration and any kind of transactions (mortgage, sale, usufruct, lease etc.) related to land. GIS-BCT land registration can give a unique identity code of a certain expanse of land on the earth's surface. It can also be used for both land documentation and title registration depending on geographical peculiarities of various locations, giving stakeholders better insight on the nature of transactions pertaining to the land.

2.2. Land Administration & Governance

According to the 2011 UN report, low levels of transparency, accountability and the rule of law results to weak land governance, which strains "the rules, processes and institutions that determine which land resources are used, by whom, for how long, and under what conditions." [12]. Therefore, the immutability of blockchain can provide the necessary transparency in Land Registration.

Faniran & Olaniyan (2016) suggested that adopting GIS-based applications in land administration by state governments across Nigeria can reduce the number of slum dwellers [13]. Similarly, Biswas et al (2021) proposed a blockchain-based platform to significantly cut down the time taken in land transactions, prevent fraud and provide secured ownership in Bangladesh while also enhancing government revenue collection [1]. Mishra et al (2021) cited immutability, consensus and distributed information as the most attractive features of their technology to facilitate direct interaction between property buyers and sellers in India [14].

One of the earliest records in the use of blockchain to solve the problem of irregularities and counterfeiting in land registration was in Honduras between 2016 and 2017. Other areas where blockchain-based solutions for land registration include Brazil, Ukraine, Sweden and India [15]. Border Violation Detection is another urban blockchain use case, which is also within the land registration domain. This is a hierarchical model that maintains consistency of demarcation between cadastral surveys by ensuring stakeholder agreement for any alteration to surveys [15].

Torun (2017) explored the use of a CAD/GIS enabled data structure in a blockchain model to solve the disparity issues between two boundaries belonging to the same cadastre boundary data. The study proposed a prevention to mistakes in cadastre survey by developing a blockchain platform wherein the landowners can participate as equity partners in the decision-making process [16].

Blockchain and GIS have also been uses outside of land administration. Sandaruwan et al (2020) proposed a platform for the efficient and secure management of blood banks using a number of novel concepts including GIS and blockchain [17]. Farizi & Sari (2021) proposed a blockchain-based e-waste (electronic waste) management application which is a data repository for collecting electronic waste in Indonesia [18].

The integration of multiple technologies with GIS is essential for smart cities where data from both assets and environment are required [19]. Ma & Ren (2017) documented a number of evidences for integration of Building Information Modeling (BIM) and GIS in planning and design, Operations and Maintenance, Infrastructure and Urban Districts. Mingard and Christophe (2014) attempted to bridge the gap between GIS and BIM by developing a facility management platform to capture urban elements. An Urban Information Model (UIM) was created to enable modelling of information of city to allow facility managers to support the lifecycle of an urban environment [20].

3. Proposed Framework

This study explores a knowledge gap by testing the hypothesis that BCT-based land registration framework can provide higher efficiency and accuracy with geo-specific cadastre information to provide secured land ownership with decentralized and immutable records. This research uses simulated data to develop a theoretical framework for a tamper-proof land record, leveraging a technology that substitutes the need for a third-party or central authority with a redefined concept of trust using blockchain. The framework can be broadly categories under two main headings namely; data gathering and processing, and model development.

Fig. 1 illustrates the conceptual framework of a blockchain-enabled land registration with smart contracts as an integral component for validating and recording transactions immutably.

3.1. Data Gathering and Processing

This phase entails the collation of information which often exists in analogue formats and can be found in municipal archives. Data on land and landowners are collated and tabulated as shown in the Table 1. The table contains land locations, coordinates, land sizes, acquisition dates, previous owners and current ownership information. In this study, we simulate data on five (5) parcels of land of different uses within the city of Gainesville, Florida.

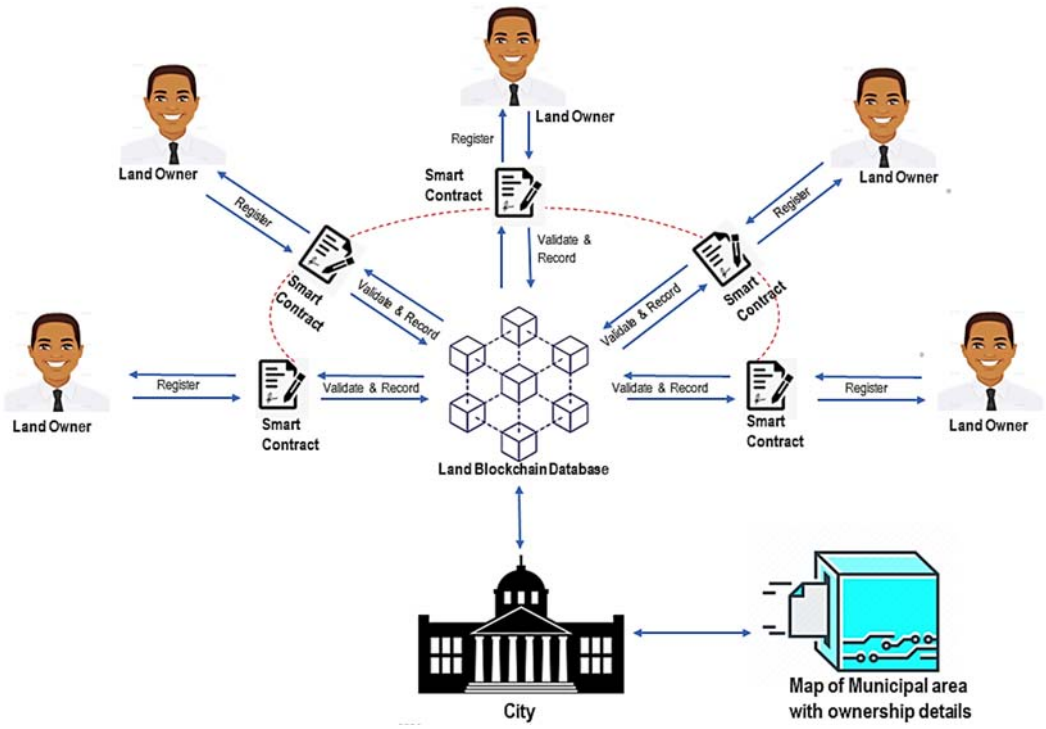


Fig. 1. Blockchain-based Land Registration Framework.

Table 1. Database of Land Owners.

Owner	Description	Location	Lat DD	Long DD
Owner A	Commercial Parcel	210 SE 6th Str. Gainesville FL	29.65006683	-82.31 962274
Owner B	Recreational Parcel	428 SE 12th Str. Gainesville FL	29.64765701	-82.31 059335
Owner C	Residential Parcel	1723 NW 14th Avenue, Gainesville FL	29.66501007	-82.34 507267
Owner D	Industrial Parcel	2605 NE 9th Str., Gainesville FL	29.67687138	-82.31 399958
Owner E	Institutional Parcel	1250 NW 33rd Avenue, Gainesville FL	29.68331726	-82.33 822644

This information is geocoded into a GIS application as shown in Fig. 2 thereby creating a map of the locations of these sites. The longitude and latitude information provides a unique identification for each land to avoid double registration of the same parcel of land. The geocoded data is added to a base map to show the location of selected lands of study. Symbology and labels are used to analyze land information quantitatively with respect to land sizes, quantities per owner etc.

The above information in Table 1 and Fig. 2 below are stored in the back-end of the municipal blockchain repository, and it is only accessible by authorized statutory officials. However, all transactions on existing lands recorded in the blockchain will be validated by the municipal records and updated. Each participant or landowner will be able to retrieve their copy of the ownership documents pertaining to their lands.

3.2. Model Development

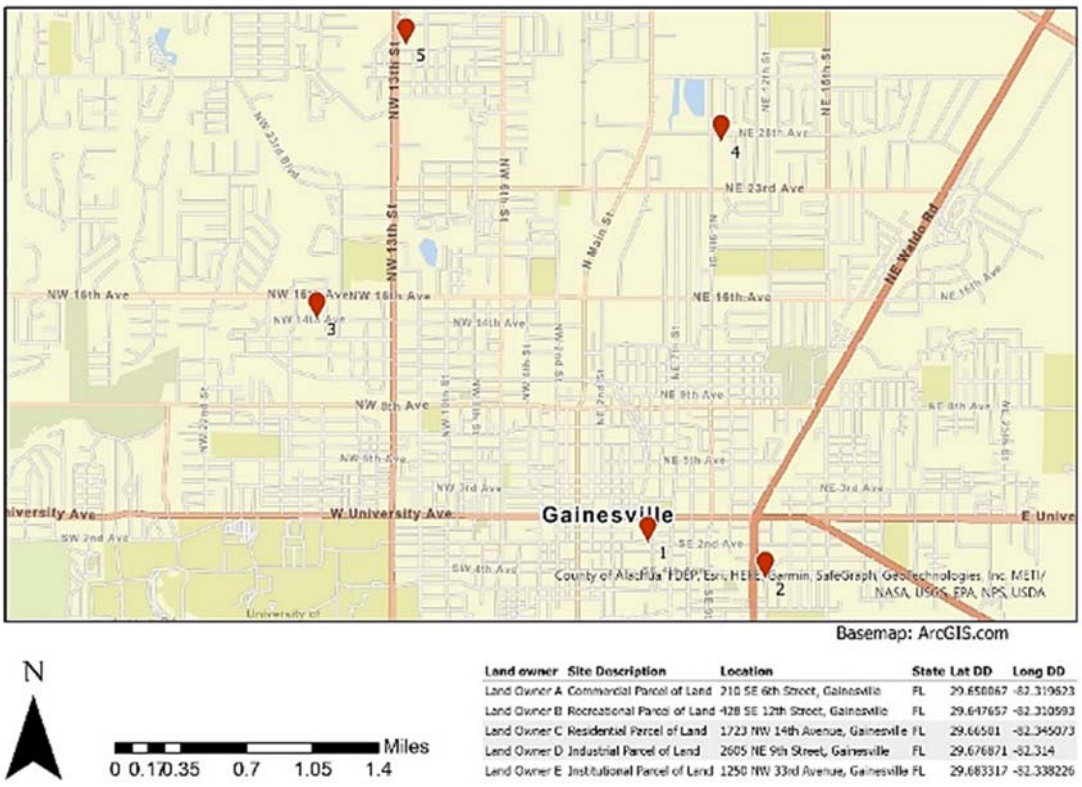
In this phase, a private blockchain network with nodes to represent all landowners is developed. This network uses a Hyperledger fabric as its DLT. All maps developed earlier and their ownership information are added into the distributed ledger of the blockchain. This enables all recorded geospatial information to be cryptographically recorded in blocks of immutable data. This blockchain is managed by the municipality and all entities added to the network are guaranteed to remain as such. Any alteration to a cadastral information will be visible to the entire network and a consensus will have to be reached by more than 50 % of the network for the alteration to be added to the ledger.

As illustrated in Fig. 3, each participant registers unto the blockchain network with a *unique identification* key. Upon registration, the network prompts the land owners to enter information regarding their land or asset(s). Copies of survey maps and ownership deeds are input. This information is validated by the private blockchain network via a consensus mechanism involving other stakeholders. This consensus provides the novel transparency. For validation to be successful, in addition to the consensus, the information from the land owner is cross-referenced with municipal records to ensure that

the GIS-generated information is in consonance with that of the city database in terms of geo-spatial descriptions.

Upon validation, electronic confirmation of ownership is issued to the landowner via automated smart contracts.

Successful registration and validation make up a block in the blockchain, encrypted by a hash and a time stamp, and subsequent transactions regarding that land will be represented in a separate block, linked to the hash of the previous block, to ensure a continuous chain of ledgers. All of this information is accessible to any other member of the network upon authorization of the municipality, which plays the role of an administrator of the network.



Land owner	Site Description	Location	State	Lat DD	Long DD
Land Owner A	Commercial Parcel of Land	210 SE 6th Street, Gainesville	FL	29.650867	-82.319623
Land Owner B	Recreational Parcel of Land	428 SE 12th Street, Gainesville	FL	29.647657	-82.310593
Land Owner C	Residential Parcel of Land	1723 NW 14th Avenue, Gainesville	FL	29.66581	-82.345073
Land Owner D	Industrial Parcel of Land	2605 NE 9th Street, Gainesville	FL	29.676871	-82.314
Land Owner E	Institutional Parcel of Land	1250 NW 33rd Avenue, Gainesville	FL	29.683317	-82.338226

Fig. 2. Map of 5 geolocated sites.

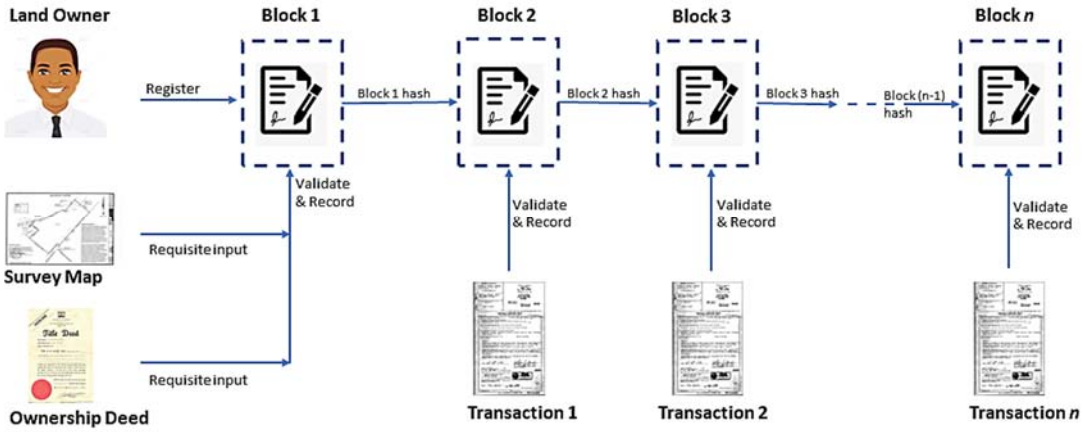


Fig. 3. Blockchain-based WorkFlow for Transactions.

The above survey map shows Land Owner E's asset and it is stored on the municipal records in the blockchain network. These maps are synchronized with the layout of all land owners in Gainesville Florida to ensure that information available to the public about their assets is in accordance with the municipal records.

The above process leverages on research which indicates that GIS techniques can provide a powerful tool for land use planning and management of information. The system can meet the needs to manage land use, significantly raise the working efficiency, avoid massive duplication of mechanical work, and greatly facilitate planning data sharing [21].

Fig. 4: Map showing Property of "Landowner E".

4. Conclusion

Previous studies have either shown how blockchain technology can be introduced to land registration or how GIS can be deployed for land resources management. In this research, the tripod relationship between GIS, Blockchain and Land Administration has been explored. This is to not only provide immutable, tamper-proof land database, but to also unify cadastral management across the globe through GIS, thereby eliminating the potentials for erroneous description of any portion of the earth surface through geolocation.

However, GIS-BCT land registration requires a technologically literate society. Sufficient training on the use of computers or smart phones to manipulate stored data and information in the blockchain helps to realize the effectiveness of this study. It is also worthy of mention to note that such revolutionary technology should be applied on a need's basis and to the peculiarity of the case in a specific region. Technology has a vital role to play in land titling for example, but it must be looked at within the overall objective of establishing a land administration system [22].

References

[1]. Biswas, M., Al Faysal, J., & Ahmed, K. A, LandChain: A Blockchain Based Secured Land Registration System, in *Proceedings of the International Conference on Science & Contemporary Technologies (ICSCT' 21),* 2021, pp. 1-6.

[2]. Fairweather, J., A common hunger: Land rights in Canada and South Africa (No. 3), *University of Calgary Press,* 2006.

[3]. Cantu, F, Human History and the Hunger for Land, *The Newyorker,* 2021.

[4]. Hann, C., Property relations: renewing the anthropological tradition, *Cambridge University Press*, 1998.

[5]. Shahnoosh, F., Jurisprudential considerations of registration in the acquisition of immovable property, *Journal of Islamic Jurisprudence and Law*, *14,* 27, 2021, pp. 64-83.

[6]. Zheng, R., Jiang, J., Hao, X., Ren, W., Xiong, F., Ren, Y, bcBIM: A Blockchain-Based Big Data Model for BIM Modification Audit and Provenance in Mobile Cloud, *Mathematical Problems in Engineering,* 2019.

[7]. Kaczorowska, M, Blockchain-based Land Registration: Possibilities and Challenges, *Masaryk University Journal of Law and Technology*, 2019, pp. 339-360.

[8]. Brits, A.-M., Grant, C., & Burns, T., Comparative study of land administration systems, *Regional Workshops on Land Policy Issues-Asia Program*, 2002.

[9]. Konashevych, O, 'GoLand Registry' Case Study: Blockchain/DLT Adoption in Land Administration in Afghanistan, in *Proceedings of the 22nd Annual International Conference on Digital Government Research* (*DG.O' 2021)*, 2021, pp. 489-494.

[10]. Dunning, H, Property Law of Ethiopia: (materials for the study of Book III of the Civil Code), 1967.

[11]. Aquib, M., Dhomeja, L., Dahri, K., & Malkani, Y. A, Blockchain-based Land Record Management in Pakistan, in *Proceedings of the 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET),* 2020, pp. 1-5.

[12]. Corruption leading to unequal access, use and distribution of land, *UN Report,* 2011.

[13]. Faniran, S., & Olaniyan, K, From slums to smart cities: addressing slum-dwelling in Nigeria through e-land administration, in *Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance,* 2013, pp. 189-189.

[14]. Mishra, I., Sahoo, A., Anand, M., & Supriya, Digitalization of Land Records using Blockchain Technology, in *Proceedings of the International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE' 2021)*, 2021, pp. 769-772.

[15]. Mendi, A., Cabuk, A, Blockchain applications in geographical information systems, *Photogrammetric Engineering & Remote Sensing*, 1, 86, 2020, pp. 5-10.

[16]. Torun, A, Hierarchical blockchain architecture for a relaxed hegemony on cadastre data management and update: A case study for Turkey, in *Proceedings of the UCTEA International Geographical Information Systems Congress*, Adana, Turkey, 2017, pp. 15-18.

[17]. Sandaruwan, P., Dolapihilla, U., Karunathilaka, D. W., Wijayaweera, W., Rankothge, W., Gamage, N, Towards an efficient and secure blood bank management system, in *Proceedings of the IEEE 8th R10 Humanitarian Technology Conference (R10-HTC)*, 2020, pp. 1-6.

[18]. Farizi, T. S., & Sari, R. F, Implementation of Blockchain-based Electronic Waste Management System with Hyperledger Fabric, *ICT for Rural Development (IC-ICTRuDev),* 2021, pp. 1-6.

[19]. Ma, Z., & Ren, Y, Integrated Application of BIM and GIS: An Overview, in *Proceedings of the Creative Construction Conference (CCC 2017),* Primosten, Croatia, 2017, pp. 1072 – 1079.

[20]. Mingard, C., & Christophe, N, Merging BIM and GIS using ontologies application to urban facility

management in ACTIVe3D, *Computers in Industry*, 2014, pp. 1276-1290.

[21]. Cao, Y., Liu, H., Xu, J, Design of Land-Use Planning Management Information System Base on ArcGIS, in *Proceedings of the WRI World Congress on Computer Science and Information Engineering*, 2009, pp. 359-363.

[22]. Burns, T, International experience with land administration projects: A framework for monitoring of pilots, in *Proceedings of the National Workshop on Land Policies and Administration for Accelerated Growth and Poverty Reduction in the 21st Century*, 2006, 5.

(024)

Use of Blockchain for Request Management Medication by Court

M. A. S. do A. Divino, A. E. S. Freitas
Federal Institute of Education, Science and Technology of Bahia (IFBA), Professional Master's Degree in Systems and Product Engineering Program (PPGESP)
R. Emídio dos Santos, IFBA, sala A-307, 40.301-015, Salvador, Brasil
E-mails: marioaugustosantos@gmail.com, allan@ifba.edu.br

Summary: Judicial demand for medication overloads the Brazilian Unified Health System, and duplicate requests may occur due to different possibilities in the care flow. Blockchain may provide better traceability. That makes request management decentralized, secure, resilient, and auditable, providing the economy and transparency necessary for the process. The proposed system works through a smart contract that will manage tokens associated with the lawsuits on screen. We provide a proof of concept simulating an entire scenario validated with specialists from the Health Department of Salvador. Those specialists indicate that using of the system can provide better control of the movement and management of the medication request with significant gains to the Brazilian Unified Health System process.

Keywords: Drug traceability, Drug through court, Private and permissioned blockchain, Blockchain audit.

1. Introduction

In Brazil, patients from the Unified Health System (named SUS, after "Sistema Único de Saúde") who have a medical prescription can obtain the medication immediately if it is available in municipal or state health units. The problem is that the list of drugs goes through constant adjustments. With this dynamic, some drugs are unavailable in the assistance network. However, they can be irreplaceable for the effectiveness of treatments. This unmet demand goes against the right to health, present in the Brazilian constitution, thus requiring special treatment by the law bodies.

In order to comply with the right mentioned above, the state allows the citizen to enter justice with individual action, filing a public civil action. After opening the process, the patient requests the medication from one of the health departments, which is then responsible for the logistics of purchasing and delivering the medical supplies [1].

The lack of integration between the entities' information systems was a problem raised in an interview with the pharmaceutical manager of the city of Salvador. Without integration, requests can be handled by more than one secretariat, generating duplicate requests and loss of revenue for the state. Different policies are subject to inconsistencies, making traceability difficult and making the audit of the judicial process fragile.

Blockchain is suitable for developing solutions related to traceability, as transactions are immutable, data travels in a secure and decentralized way, and offers reliable auditing [2]. Transaction immutability is attractive for healthcare applications as it creates full audit trails. Unlike systems that use centralized databases, it keeps data distributed among network participants. It uses consensus algorithms to ensure that all machines are synchronized and have the same information. This work aims to present a blockchain system to integrate institutions, strengthening traceability and transparency in the Brazilian public service.

2. Related Work

Our prior study found no work directly related to the context of lawsuits related to medicines. For the analysis, a study was carried out aimed at the traceability of materials using blockchain technology in general, and they are presented below.

The proposal brought by [3] uses blockchain to prevent unregulated or counterfeit products from entering the US supply chain. According to the author, there is an increasing number of counterfeit medicines produced and marketed. The FDA (Food and Drug Administration) regulatory authority established the Medicines Quality and Safety Act which requires the adoption of safer mechanisms for drug traceability.

Company MODUM.IO AGO produced a blockchain to monitor the temperature of medicines during transport [4]: immutable monitoring data validate the optimal temperature supply contract for the package in transit. Finally, a mobile application reads the thermal sensors attached to the packages and sends the data to the Blockchain based on the Ethereum platform [5].

In the work of [6], a blockchain system called Drugledger tracks the drug supply chain from production to arrival at the pharmacy. The system does the traceability in a non-synchronized way with the physical flow of the drug. In this work, there is a concern with the financial privacy of transactions to avoid unfair competition and commercial advantages for any participant. With source and destination keys, it only allows the next transaction if the following key is that of the expected recipient. This work distinguishes itself from the others by bringing a strategy to control the growth of transaction blocks.

In [7], the authors conceived the Gcoin blockchain for drug tracking to combat counterfeiting. This work differs from other proposals because the government has a regulatory role and provides licenses to the organizations.

In the case study in [8], the author analyses the use of the blockchain developed for food tracking with the retailer Walmart. According to the author, the retail store is in 28 countries and has almost 12,000 stores with approximately 260 million customers. The objective is to solve problems frequently faced, such as the deterioration and falsification of products. The author relates a proof of concept in a pilot project that reduced the time of locating lots on the network from 6 days to 2 seconds.

2.1. Comparison with the Proposed Solution

We compare the technical requirements that motivate our proposal with these previous works. As far as we know, no alternatives specifically dealt with legal requests for medicines and their traceability for public care systems. The analyzed works consider the final customer and approach those who can pay for the product at the moment of its need. The SUS client or patient depends on the logistics of public agencies to obtain the medicines; because of this, the safety of the process and the time of service are great allies in health care and the preservation of life. Table 1 numbered these works compared in Table 2.

Table 1. Related work.

Nr.	Related Work
1	Trace and Track: Enhanced Pharma Supply Chain Infrastructure to Prevent Fraud
2	Blockchains Everywhere - A Use-case of Blockchains in the Pharma Supply-Chain
3	Drugledger: A Practical Blockchain System for Drug Traceability and Regulation
4	Governance on the Drug Supply Chain via Gcoin Blockchain
5	A New Era of Food Transference Powered By Blockchain

Table 2. Comparative table with correlated work.

Product Requirements	Proposed System	1	2	3	4	5
Private Blockchain	YES	YES	YES	YES	NO	YES
Permissioned Blockchain	YES	NO	NO	YES	YES	YES
Provides Audit	YES	YES	YES	NO	YES	YES
Traceability to the End Customer	YES	YES	NO	NO	YES	NO
Serves Public System User	YES	YES	NO	YES	YES	NO
Meets Judicial Request for Medication	YES	NO	NO	NO	NO	NO

3. Method Used

Through interviews with the pharmaceutical manager of the city of Salvador, we identify that the lack of integration between public agencies regarding judicial requests for medicines is a significant problem to be solved. A basic questionnaire was applied to consolidate the requirements. We map the business rules and validate them with the management staff. In the implementation phase, we develop the proposed blockchain platform. Finally, we run a simulated environment with the following nodes representing actors in this process: the Municipal Health Department, the Public Ministry, and the Secretary of State Health.

With the platform's development, we evaluate execution time and functionality for digital intelligent contracts in the deploy environment. The simulated environment comprises a representation of the Health Department of the Municipality of Salvador, the Public Ministry, and the Health Department of the State of Bahia.

4. Court Case Flow

Fig. 1 shows the flow of the judicial process. The patient travels to the health unit in search of the medication and, if found, will be attended by the unit's pharmacy; otherwise, it goes to the judicial body to open a court order, which initiates the interaction with the Blockchain system. Upon receiving the citizen, the agency's court verifies the medical report. It opens the petition, forwarding the process to the blockchain and making it a digital asset for the network, accessible to all public bodies in the consortium. With the process

open, the patient goes to one of the secretariats, who then checks it on the blockchain and takes over the process for care, requesting to purchase the medication. With all operations sent to the blockchain system, citizens may monitor the movements until the drug arrives.

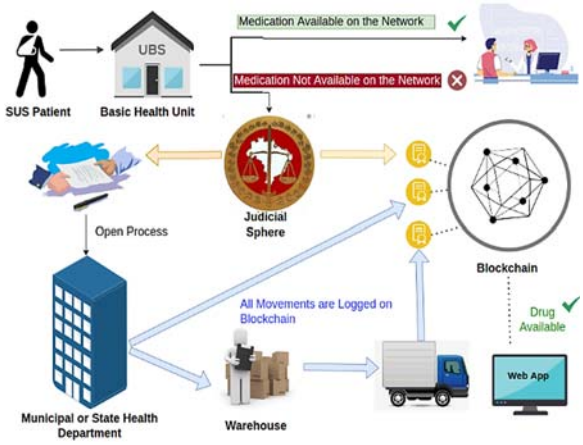


Fig. 1. Big picture with the flow of the whole process until the movements in the blockchain.

5. System Presentation

For the development of the system, we use the frameworks Hyperledger Fabric [9] and Minifabric [10], where all peers are clients and servers, thus not allowing the centralization of information in any institution. The control between the entities occurs without any technological or institutional hierarchy, obeying only the business rules present in the smart contract.

Managers or citizens can check and monitor the entire flow (for example, movements until the arrival and withdrawal of the drug), which gains transparency in public service management.

The network scripts and artifacts were generated through the Minifabric framework, such as organization configuration, connection files, and cryptographic materials that are the access credentials for each node on the network. Through the execution of the scripts occurs the creation and configuration of the network with all the artifacts.

The consensus algorithm implemented is Raft [11] which allows fault-tolerant replication, except for Byzantine faults. The protocol is used in distributed systems to manage and maintain the log consistency that records messages replicated between nodes in the network [11]. In the blockchain system, there is one ordering node in each one of the organizations, forming the group that participates in the consensus.

Dynamically by quorum/vote, the protocol chooses the leader node (which can be any of the organizations) to coordinate the consensus. The follower nodes receive "heartbeat" messages from the leader informing them that it is active. Suppose the leader fails to send these messages; in that case, the followers initiate a new election, and one becomes the leader, thus applying fault tolerance.

The leader receives an entry for the transaction log and sends it to the other follower nodes for verification; after checking, the followers send the result to the leader, and the most consistent result, according to the majority, is confirmed.

Globally, each sort node maintains a finite state machine [11] that collectively evaluates incoming inputs, ensuring that the sequence is consistent across all nodes. Raft promotes determinism by preventing forks or parallel branches of data blocks from existing on the network.

For it to work, most nodes must be up and running. In the case of the blockchain system, with three participants initially, at least two organizations need to be active. When a lawsuit starts, all organizations verify that the transaction signature is from the author who created it, then everyone endorses and confirms the process on their local blockchain.

The process opened in the judicial body is the asset controlled in the ledger. All transactions are included, such as the creation and movement of the process. The channel shared between the institutions works as a consortium where only the allowed participants may operate on the ledger. The channel also ensures a unified and private view of the data between organizations.

Each movement is registered and communicated to all parts, allowing subsequent auditing. The operations are made available and controlled by the smart contract [12] through the specific permissions for each integral part, such as the request for medication, which can only be carried out by one of the health departments.

The blockchain system comprises the Fabric network with a chaincode (smart contract) in Node.js [13], a Web API that provides blockchain operations, and a web application that consumes the Web API and makes the operator interface. Access is allowed from each institution with respective asymmetric cryptographic keys (public and private). The implemented smart contract controls all operations and permissions according to institutional roles.

No personal information is stored on the blockchain, it remains in the originating institutions, and no sensitive data is persisted and is required. Blockchain adheres to the Brazilian General Data Protection Law.

5.1. Code to Create a Legal Proceeding as an Asset on Blockchain

The chaincode in Fig. 2 demonstrates the asset registration on the blockchain. Line 53 checks if the law process already exists. It avoids duplication of law processes in the blockchain. The requester must belong to an organization with credentials for the petition, such as, for example, the Public Ministry. After validation, the asset is created on line 64 and sent to the blockchain through the putState function on line 75.

```
async CriarAtivoProcessoJudicial(ctx, id, numAnvisa, nomeComercialMedicamento, instancia, status, operador) {

    var data = new Date();
    const exists = await this.AssetExists(ctx, id);
    const cid = ctx.clientIdentity;
    let MSPID_ORIGEM = cid.getMSPID();

    if (exists) {
      throw new Error(`O  processo de número ${id} já foi cadastrado e não pode ser repetido.`);
     return;
    }

    if ( MSPID_ORIGEM !='sms-ba-gov-br') {
       throw new Error('Usuário você pertence a organização  ${MSPID_ORIGEM}
                        apenas usuários do Ministério Público podem cadastrar um processo judicial.');
    return;   }

    else {
     const asset = {
        ID: id,
        NumAnvisa: numAnvisa,
        NomeComercialMedicamento: nomeComercialMedicamento,
        Instancia: instancia,
        Status: status,
        TipoOperacao:'Cadastro',
        Operador: operador,
        Data: data.toString(),

     };
        ctx.stub.putState(id, Buffer.from(JSON.stringify(asset)));
        return JSON.stringify(asset);
  }}
```

Fig. 2. Registration of the Judicial Process - Chaincode.

5.2. Web Application

The web application was developed in Node.js on the back end and Vue.Js on the front end. This front-end provides interfaces for registering and moving legal proceedings, monitoring, auditing, and a dashboard.

Transactions are sent to the chaincode through API requests on the web server Express.Js and published on the institution server.

Mandatory fields are validated and checked on the client side. All business rule validations are performed in chaincode with returns of success or error when submitting transactions.

The Dashboard in Fig. 3 demonstrates example data that can be useful for management. In this simulation, we have many law processes created in the legal sphere; however, only half reached the secretariats, and few processes were completed. It also presents a ranking of the most requested drugs. This data can generate actions for improvements in all public management.

5.3. Deployment

Our environment consists of a node with Ubuntu 21.10 operating system and the following software: Hyperledger Fabric, Minifabric, Docker, and Express.Js web server.

The docker containers are the peers that do the communication and operations on the network, the transaction blocks containing the ledgers, and the NoSQL CouchDB database.

The API and the web application are deployed on the Node Espress.Js web server. With the case number, the SUS patient accesses the system through a web browser and follows the petition. Fig. 4 shows the deployment diagram.

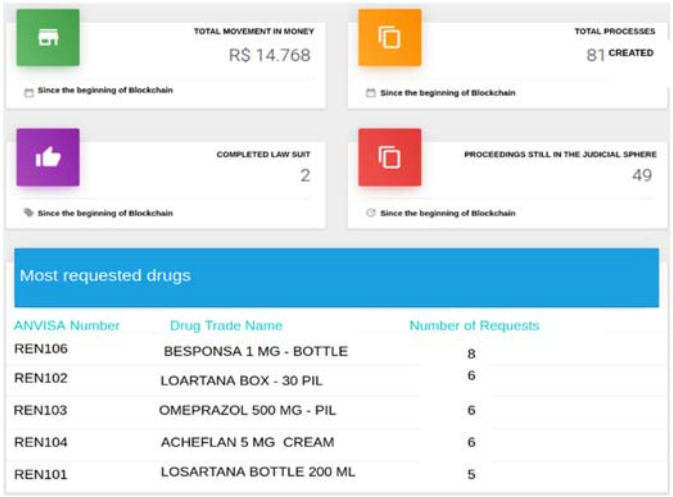


Fig. 3. Dashboard example with data for management assistance.

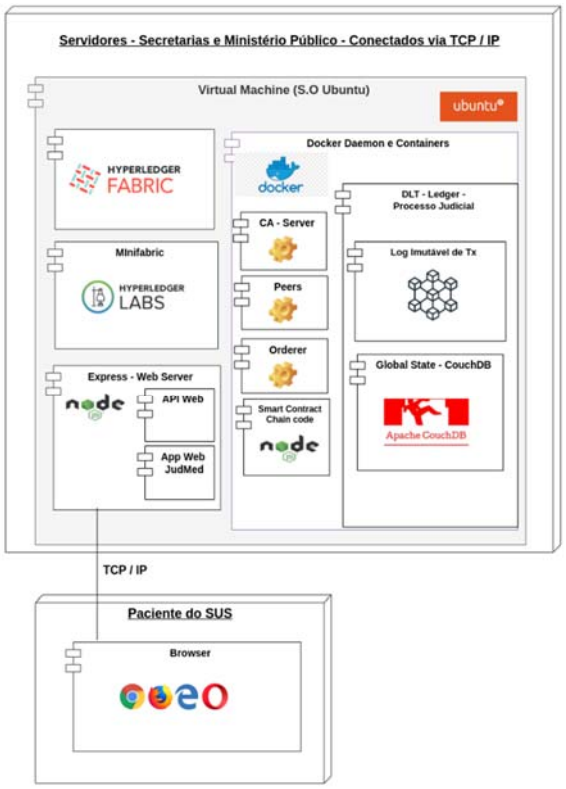


Fig. 4. Deployment Diagram.

6. Proof of Concept

Validation took place through a proof of concept. We proceed to validate blockchain functioning and, after, to reproduce the business process: we use fifteen actual processes from the open data portal of the Court of Justice of the State of Bahia. We reproduce their flow, validated by a pharmaceutical manager and a business analyst of Salvador's municipal public health management.

The following validations took place in a simulated environment: private consortium and respective authorized entry, transactions for creation and movement of processes, organization roles, consensus to validate the submission and make the information persistent, and data recovery for audit.

After configuring the spec.yaml files on the machines in a simplified way, the network initialization was executed with Minifabric, starting all docker containers with a total of 1 minute and 40 seconds on each host, leaving the network operational. That execution time may be reduced in a more robust configuration execution environment. The initialization generates all files and scripts necessary to operationalize the network, such as the channel configuration and the cryptographic material of each entity.

In a practical and organized way, everything was arranged in the "mywork" working directory. After starting the network, it was necessary to manually carry out the following steps: placing the organizations on the same channel, configuring the host information of the State Health Department on the network channel, discovering and approving the new entity, reading, writing, and approving transactions.

The entire flow after the creation of network nodes was manual, performing commands or exchanging files between organizations, as seen before. This aspect can be improved in the future by reducing manual steps and speeding up the entry of new organizations.

In the judicial process managed on the blockchain, the number in the Public Ministry, the data related to the drug, and information about the asset movement without storing or exposing sensitive patient data.

There was control over who could access and execute each function, demonstrating the effectiveness of chaincode, called by the API and executed by the web application. By verifying the existence of the same judicial process on the blockchain by the process number, duplicity was also avoided, barring a new request.

The submitted transactions took, on average, 5 seconds to be confirmed after consensus with the Raft protocol between organizations, which can also be optimized when deployed on a server machine with more infrastructure resources. The search function was performed for the audit, retrieving all the information from the audited judicial process. For the SUS patient, the monitoring screen brings the current state of the process.

7. Final Remarks

Integrating organizations with blockchain bring the benefits of decentralization, transparency, resilience, and irrefutability. That contributes to institutions and people who depend on logistics for health care and treatment through pharmaceuticals. The follow-up makes it possible to obtain agile data, and data analysis through the dashboard should provide a continuous improvement in the entire flow of material acquisition. In this paper, we show how blockchain may help govern public health systems by providing effective mechanisms for drug delivery.

Acknowledgments

The authors thank the Dean of Research, Graduate Studies and Innovation (PRPGI) and the Federal Institute of Education, Science and Technology of Bahia for their financial support for the publication and presentation of the work.

References

[1]. Macedo, E. I. D., Lopes, L. C., Barberato-Filho, Análise técnica para a tomada de decisão do fornecimento de medicamentos pela via judicial (“Technical analysis for decision-making on the supply of medicines by judicial means.”), *Revista de Saúde Pública,* 45, 2011, pp. 706-713.

[2]. Zhang, J., Xue, N., and Huang, A secure system for pervasive social network-based healthcare, *IEEE Access,* 4, 2016, pp. 9239-9250.

[3]. Alangot, B., and Achuthan, K., Trace and track: Enhanced pharma supply chain infrastructure to prevent fraud, in *Proceedings of the International Conference on Ubiquitous Communications and Network Computing,* 2017, pp. 189-195.

[4]. Bocek, T., Rodrigues, B. B., Strasser, T., and Stiller, B., Trace and track: Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. in *Proceedings of the IFIP/IEEE Symposium on Integrated Network and Service Management (IM),* 2017, pp. 772-777.

[5]. Dannen, C., Introducing Ethereum and solidity, Apress, Berkeley, 2017, Vol. 1, pp. 159-160.

[6]. Huang, Y., Wu, J., and Long, C., Drugledger: A practical blockchain system for drug traceability and regulation, in *Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),* 2018, pp. 1137-1144.

[7]. Tseng, J. H., Liao, Y. C., Chong, B., and Liao, S. W., Governance on the drug supply chain via gcoin blockchain, *International Journal of Environmental Research and Public Health*, 15, 6, 2018, 1055.

[8]. Yiannas, F., A new era of food transparency powered by blockchain, *Innovations: Technology, Governance, Globalization*, 12, 1-2, 2018, pp. 46-56.

[9]. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., and Yellick, J., Hyperledger fabric: a distributed operating system for permissioned blockchains, 2018, *arXiv preprint arXiv:1801.10228*.

[10]. Lodi, G. C, Sistema de monitoramento dos processos de manutenção e vida de produto utilizando a tecnologia blockchain ("Maintenance Processes and Product Life Monitoring System Using Blockchain Technology"). Master's thesis, *Universidade Tecnológica Federal do Paraná*, 2021.

[11]. Hu, J., and Liu, K., Raft consensus mechanism and the applications, *Journal of Physics: Conference Series,* Vol. 1544, No. 1, 2020, pp. 012079.

[12]. Li, W., He, M., and Haiquan, S., An overview of blockchain technology: applications, challenges and future trends, in *Proceedings of the 11th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC)* 2021, pp. 31-39.

[13]. Hahn, E., Express in Action: Writing, building, and testing Node.js applications, *Simon and Schuster,* 2016.

(026)

Investigate the Blockchain APP for Distributed Energy Resources with Energy Blockchain Point-to-Point Transaction

A. J. Jin [1], J. Tan [2 *] and C. Li [3]
[1] The Maritime Faculty, Ningbo University, Ningbo, China
[2] School of Computing and Data Engineering, NingboTech University, Ningbo, China
[3] College of Artificial Intelligence, Nanjing University of Information Science and Technology, Nanjing, China
E-mail: jt@nit.zju.edu.cn

Summary: This article studies the broad methodology and major application of smart distributed energy resources (DER) in terms of energy generation, consumption, and transaction. This article simplifies a general DER system into a generic type of integrated DER model with three input parameters and three critical output functions. The combination of both DER and blockchain is a type of energy blockchain (EBC) and will receive significant added values. Smart DERs are enabled by computerized decision where a computer collects various data in entire processes. Authors demonstrate valuable EBC features as follows. First of all, the best solutions can meet power demand, offer economic advantage, and have low carbon footprint for consumers. Moreover, several network blockchain options are discussed. Finally, the exergy is discussed that can be possibly achieved for the smart DER systems. EBC and DER is advantageous over the exergy that is a market driver of the so-called intelligent power technology.

Keywords: Distributed energy resources, Renewable energy, Energy blockchain, Keyless blockchain-as-a-service, Exergy.

1. Introduction

With the aim to address an increasing trend of carbon emission and climate changes, the world has made a significant agreement to curb this trend. The field of distributed energy resource (DER) has become very interesting and has attracted huge attention of researchers [1]. Following the goals defined by the Paris Agreement, multiple sectors have been putting tremendous effort into finding efficient and effective ways of addressing the issue of climate change. The carbon greenhouse gas emission of energy can lead to climate anomalies, so there is an urgency to reduce the carbon-emission [2-3]. Because greenhouse gas increases solar irradiance absorption, which leads to rapid glacier melting and disruption of fragile ecosystems, a climate emergency has been declared.

Carbon pricing scenarios include a wide range of low-cost and/or cost-saving options associated with high energy efficiency, schedule optimization, alternative energies, energy storage, and a transition from less environmentally friendly energy sources to more renewable energy sources. Recent growth in energy consumption has resulted in a dire need to identify renewable energy sources that can operate at large scales. To date, there have been many valuable advances in the commercial application of energy technologies [4-7]. However, upscaling renewable energy operations is problematic for many reasons, and power production could become unstable on a daily basis. For instance, solar energy cannot be generated at night, and the generation of wind power depends on daily and seasonal weather conditions. Despite these challenges, many countries have developed advanced technologies that allow them to use renewable energy sources [8-14].

Toward research on extensive renewable energy systems, discussions of renewable energies effect on load forecasting and on carbon economy or pricing, these have been studied separately recently in literature [15-17]. The combination of both distributed energy resources and blockchain will receive significant added values for the market. Among various approaches, authors have investigated the first approach of its kind, to study both EBC and renewable energies [1, 6]. This approach has significant impacts on critical output functions. A smart micro grid is value-added and beneficial for users and EBC community.

2. Smart Distributed Energies

As it is shown in Fig 1, the smart distributed resources, the smart DER has prosumers with power generation capability who possibly connect to energy storage and grid power with computerized energy management system.

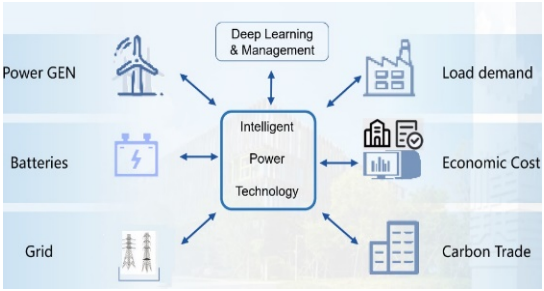


Fig. 1. An energy management system of distributed energies with EBC for commercial transaction with power prosumers with power generation, energy storage, and grid power.

The researchers have discovered valuable knowledge about the recent use of renewable energies and distributed energy technologies. A financial model is demonstrated in an equation as follows.

$$Fin(t) = \int dt\{[PG * a_1(t) - CP * a_2 + ES \times a_3(t) \times \Delta p - GP * a_4(t) \times p(t)\} \quad (1)$$

In the valued dependency model, Eq. 1, Fin is illustrated in a mathematical model at the top right. PG is an input parameter, e.g., of the total solar PV generation (from specification); with a1 being an ambient power coefficient that has a range of (0, 1) and varies with time during the day. p(t) is a scheduled price from utility provider.

CP is an input parameter dictated by a prosumer who decide how many in total household power to use for what time in which day. In Eq. (1), CP is multiplied by a2 where a2 is a parameter that ranges (0, 1) for the distributed power deployment or that may be a customer's specification.

Normally the ES charges energy at the night and discharges in the day. The energy level of ES ranges by the manufacturer's spec, e.g., between 10 % to 95 % during a discharge-charge cycle.

The coefficient a3 in ES is the effective charge-discharge rated coefficient that ranges (-1, 1). Its actual range may depend on the manufacturer's specification.

GP represents the grid power input that is a parameter for prosumer to decide. In the equation, the term GP is as a4 * GP, max; where a4 is an ambient power coefficient that ranges from 0 to 1. A smart meter connects EBC to the external grid. p(t) is the price-schedule of electricity.

This financial model enables mechanism such as forward contracts or futures contracts implemented with blockchain technologies to make energy supply-demand more balanced by compensating predictable energy generation and consumption.

Authors have investigated commercial applications by employing eq. (1). In a typical system with wind and solar power generation, along with ES and grid power, the grid power has a specific pricing schedule that differentiates peak, valley, and average hours. Moreover, the hardware configuration is as follows.

The inputs involve wind power and solar power specified at a spec of 500 kW. The ES is set at 300 kWh. The computer simulation resulted in favourable outputs, as shown in Tables 1. Table 1 shows that the cost results favour the case of wind-solar light with an ES complementary microgrid and that the peak load in this case demands significantly less of the grid. The load at valley time for traditional wind-solar-without ES has a negative value, where the microgrid outputs power to the grid. The configuration with wind-solar-and-ES demonstrates economic income, as shown by negative value(s). It has net power output during the peak hours leading to financial gains, and it has net power input during the valley hours for overall financial benefit.

Simulation are studied for three different configurations where the conversion 1 Yuan equals to $0.14 USD with table at below. It obviously exhibited the advantages of utilizing the wind-light complementary microgrid with ES.

Table 1. Simulation results are enlisted.

Methods	Base load	Traditional wind-light complementary microgrid	Wind-light complementary microgrid (with ES)
Cost (yuan)	9125	78	-510
Peak load (KWh)	6908	40	-1289
Valley load (KWh)	2608	-398	22

3. Energy Blockchain Among Networks

In a decentralized energy system, energy supply contracts can be directly constructed between producers and consumers. Enabling energy blockchain can result in a considerable number of direct interactions and transactions between local energy producers and consumers.

3.1. Permission-based Blockchain Networks

One can set up a private EBC network, which is a type of permission based blockchain network differed from a general setup. A consortium blockchain represents an ideal solution for companies where all participants need to be permissioned and have a shared responsibility for the blockchain.

Blockchain networks build in security risk management systems. When building an enterprise blockchain network, it is important to have a comprehensive security strategy that uses cybersecurity frameworks, assurance services, and best practices to reduce risks against attacks and fraud.

When building an enterprise blockchain network, it is critical to have a comprehensive and holistic view for security. A proper security strategy should adopt fitting cybersecurity frameworks, assurance services, and best practices to reduce attacks and fraud risks.

There are many types of energy blockchain such as private BC network, permission-based BC network; keyless BC as a service BC.

The power transaction may be enabled/ performed with currency known as tokens. E.g., these tokens can be independently traded outside the platform as a digital asset on eligible exchanges. For example, to access the Power Ledger platform, a bond has to be obtained and must be paid in the form of power tokens. Power Ledger platform provides a market mechanism that encourages people to install battery systems that can stabilize the grid and stay connected to the grid. In

the past, batteries were installed by consumers to self-supply and be less reliant on the grid. The decrease in the price of solar panels and batteries has stimulated their usage without government subsidies. Connecting them to the Power Ledger platform enables consumers to trade and achieve a certain income.

3.2. An Energy Blockchain Architecture

As it is shown in Fig. 2, a flowchart of the proposed architecture for EBC is presented that basically has three layers of structure. The blockchain APP executes a list of transaction as agreements or notes where the ledger is recorded as a part of algorithmic application. For the distributed renewable energy resources, combination of EBC and smart grid is powerful to meet the power supply and demand ecosystem.

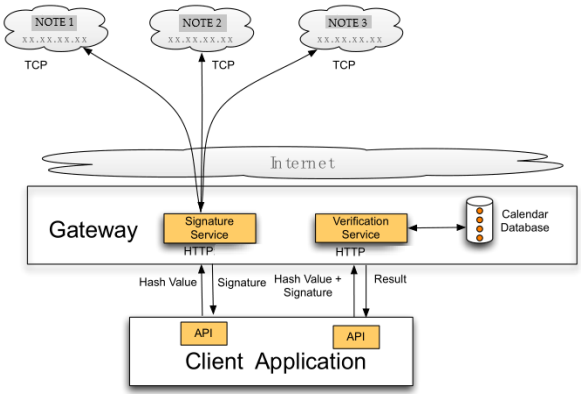


Fig. 2. The figure illustrates an architecture of a blockchain APP with a list of agreements or notes.

4. Discussions

Through works that are established at above, the EBC has promised a tremendous potential for the high technology commercial application with smart DER. In this article, authors have highlighted the research breakthrough in terms of configurations in hardware, software, and mathematical model with big data apps. These configurations are tested and simulated.

As it is shown in Fig. 3, it illustrates that there are many players in the area of energy blockchain market. Based on our research findings, no player is dominating the field and each one has sufficient rooms to grow big with EBC.

The digital electricity helps mankind to control the climate warming and to achieve rapid and far-reaching transition from fossil-based fuels to renewable energies. Tokenization of energy has been provided by various vendors as shown in Fig. 3. This illustrates that there are many players in the area of energy blockchain market. Based on our research findings, no player is dominating the field and each one has sufficient rooms to grow big with EBC. Many players endeavor to succeed in the tokenization of energy; the research in the field shows that the key apps of smart DER or EBC is not huge yet and should grow huge. There are many players in the area of energy blockchain market, no player is dominating the field and each one has sufficient rooms to grow big with EBC.

Fig. 3. The figure illustrates many developers in EBC. No player is dominating the field and each one has sufficient rooms to grow big with EBC.

5. Conclusions

At microgrid energy transaction level, a peer-to-peer transaction mode based on blockchain can promote energy transactions with low marginal costs characterized by immutability and high transparency.

The critical output functions are derived from the input parameters in distributed energy resources through power utility matrix solutions.

The computer algorithm collects various energy related data that is fed into computer for deep learning and the computer makes intelligent decision in order to meet both expected and unexpected demands for power and to provide users with smart DER solutions in a stable, safe, and cost-efficient fashion.

Energy blockchain is advantageous over driving carbon peak and carbon neutrality that cuts down the carbon emission effectively. Smart DER and EBC can be exploited to extract maximal useful work.

Acknowledgment

The authors are appreciative of Z. Li, Q. Meng, S.W. Gao and D. Liu for their valuable discussions and special support.

References

[1]. Jin, A. J., Li, C., Su, J., Tan, J. Fundamental Studies of Smart Distributed Energy Resources Along with Energy Blockchain, *Energies,* 2022, 15, 27 October 2022, pp. 806701- 806712.

[2]. Arantegui, R., Jager-Waldau, A., Photovoltaics and wind status in the European Union after the Paris Agreement, *Renew. Sustain. Energy Rev.,* 81, 2017, pp. 2460–2471.

[3]. Shivakumar, A., Dobbins, A., Fahl, U., Singh, A., Drivers of renewable energy deployment in the EU: An analysis of past trends and projections. *Energy Strategy Rev.,* 26, 2019, 100402.

[4]. Morstyn, T., Mcculloch, M. Multi-class energy management for peer-to-peer energy trading driven by prosumer preferences, *IEEE Trans. Power Syst.,* 34, 2019, pp. 4005–4014.

[5]. Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities, *Renew. Sustain. Energy Rev.,* 100, 2019, pp. 143–174.

[6]. Li, Z. H., Su, J. P., Jin, A. J. Perspectives on Published Energy Sources and Smart Energy Supplies, *Adv. Mater. Lett.,* 12, 2021, 21031607.

[7]. Su, J., Li, Z., Jin, A. J. Practical Model for Optimal Carbon Control with Distributed Energy Resources, *IEEE Access*, 9, 2021, pp. 161603-161612.

[8]. Supasa, T., Hsiau, S. S., Lin, S. M., Wongsapai, W., Chang, K. F., Wu, J. C., Sustainable energy and CO2 reduction policy in Thailand: an input–output approach from production- and consumption-based perspectives, *Energy Sustain. Dev.,* 41, 2017, pp. 36–48.

[9]. Heydaria, A., Garcia, D. A., Keyni, F., Bisegna, F., De Santoli, L. A novel composite neural-network based method for wind and solar power forecasting in microgrids, *Appl. Energy,* 251, 2019, 113353.

[10]. Meng, X., Niu, H., Jia, D., Zhang, X., Luo, X., Yang, M., Real-time energy optimal dispatching method for microgrid based on energy storage Soc day-ahead plan, *J. Agric. Eng*., 32, 2016, pp. 155–161.

[11]. Fan, W. User-Side Microgrid Energy Management Method Based on Online Optimization, Graduate Thesis, *North China Electric Power University,* Beijing, China, 2017.

[12]. Long, M. X., Research on Optimal Dispatching of Residents Load in Smart Communities Considering New Energy Grid-Connected, in Energy Transfer, *Hunan University*, Changsha, China, 2018.

[13]. Park, L. W., Lee, S., Chang, H., A Sustainable Home Energy Prosumer-Chain Methodology with Energy Tags over the Block-chain. *Sustainability,* 10, 2018, 658.

[14]. Ding, W., Wang, G. C., Xu, A. D., Research on key technologies and information security issues of energy blockchain, *Proc. CSEE*, 38, 2018, pp. 1026–1034.

[15]. Sabounchi, M., Jin, W., Towards resilient networked microgrids: Blockchain-enabled peer-to-peer electricity trading mecha-nism, in *Proceedings of the IEEE Conference on Energy Internet & Energy System Integration*, Beijing, China, 26–28 November 2017, pp. 1–5.

[16]. Tai, X., Sun, H. B., Guo, Q. L., Blockchain-based power transaction and congestion management method in the energy internet, *Power Grid Technol. China*, 40, 2016, pp. 3630–3638.

[17]. Mylrea, M., Gupta Gourisetti, S. N., Bishop, R., Johnson, M., Keyless Signature Blockchain Infrastructure: Facilitating NERC CIP Compliance and Responding to Evolving Cyber Threats and Vulnerabilities to Energy Infrastructure, in *Proceedings of the 2018 IEEE/PES Transmission and Distribution Conference and Exposition (TD)*, Lima, Peru, 18–21 September 2018, pp. 1–9.

(027)

Heterogeneous Models Inference Using Hyperledger Fabric Oracles

V. Drungilas, E. Vaičiukynas, L. Ablonskis and L. Čeponienė
Faculty of Informatics, Kaunas University of Technology, Studentų str. 50, Kaunas, Lithuania
E-mail: vaidotas.drungilas@ktu.lt

Summary: The implementation of distributed machine learning using blockchain technologies is frequently complicated by computationally intensive calculations and limitations of smart contract languages supported by the blockchain network. In this study, we present a distributed machine learning architecture that supports heterogeneous machine learning models using blockchain oracles for model inference calculations. The proposed architecture allows collaborative network participants to upload machine learning models and validation data to the blockchain and obtain model inference results using oracles. The models can then be combined into a collaboratively developed ensemble. Overall, this architecture produces trusted inference results on shared data for each uploaded model simultaneously.

Keywords: Machine learning, Blockchain oracle, Chaincode, Hyperledger fabric.

1. Introduction

In recent years there has been an increase in research interest in the fields of distributed machine learning (ML), such as federated learning [1] or privacy-preserving learning [2], which allows distributed parties to participate in machine learning collaboratively. Propositions to apply blockchain technology to empower distributed machine learning systems are being explored [3], [4]. When moving from a centralized ecosystem to a decentralized one, there are benefits and drawbacks to consider. While blockchain introduces immutable ledger and transaction logging, it can also bring increased computation costs in the form of the overhead of consensus algorithms and increased system response times due to the size of a blockchain network. To facilitate the creation of a blockchain based distributed machine learning implementation, we propose: a) a novel system architecture that utilizes Hyperledger Fabric (HF) network where each participating node features separate blockchain oracle services and b) a distributed learning web application.

Blockchain oracles are traditionally used to retrieve information from third parties or perform complex computations outside of a blockchain network [5]. The architecture presented here is a continuation of the findings of our previous research [6]. In our solution, the introduction of blockchain oracles allows the network participants to collaborate by using a wider range of programming languages instead of using only the ones supported by the smart contract implementation. The use of blockchain oracles also allows for model inference calculations and enables more complex machine learning models than those that can be implemented purely within the blockchain network.

2. System Architecture for Heterogeneous Machine Learning Inference

Our proposed architecture (Fig. 1) is built on the HF blockchain network. The unique set of features that HF provides for our solution are modular architecture, less computationally demanding consensus algorithm, and ability to perform calls to blockchain oracles from the chaincode. The blockchain network should contain at least two participating organizations with their own separate certificate authorities, an ordering service, and any number of peers. The model inference chaincode is deployed to each communication channel existing between the participating organizations. The distributed learning (DL) web application should be installed in the environment of each network peer. This web application implements calls to API of chaincode.

The purpose of the DL web application is to provide a web interface for users of the blockchain network that allows one to upload model and data files and utilize the model inference results. The model validation and inference are performed by blockchain oracles. The blockchain oracle services are provided by each organization and deployed to each peer that joins the required chaincode. It is recommended to have a separate chaincode for every distinct oracle implementation.

In Fig. 1, we present an example prototype network containing two organizations. The components of a peer network node are presented in Fig 2. A network peer node must contain a separate oracle for each different machine learning technology utilized in the participating organization.

3. Model Inference Chaincode

To obtain model inference results in a blockchain network, a chaincode for model deployment and

validation must be developed. Model inference calculations have two basic prerequisites: a) data and b) a machine learning model capable of producing predictions. We suggest storing both prerequisites in HF supported CouchDB database. The data should be transformed into JSON format and uploaded to blockchain. Native ML model representations are usually stored in more complex file-based structures. We suggest that the contents of the model file produced by a machine learning library be archived in a single .zip package and encoded using the BASE64 algorithm before the upload. This reduces the size of the model representation and enables it to the blockchain network. To validate and calculate model inference, both data and encoded model file will be transferred from blockchain data storage to a peer hosted blockchain oracle. The selected oracle will decode and extract the model file for validation of file format and data structure. If the file and data structure are found to be valid, the model file is used to run the inference step and returned values are stored on the blockchain. The proposed model and data upload process produces data entries for each data type, model, and model inference.

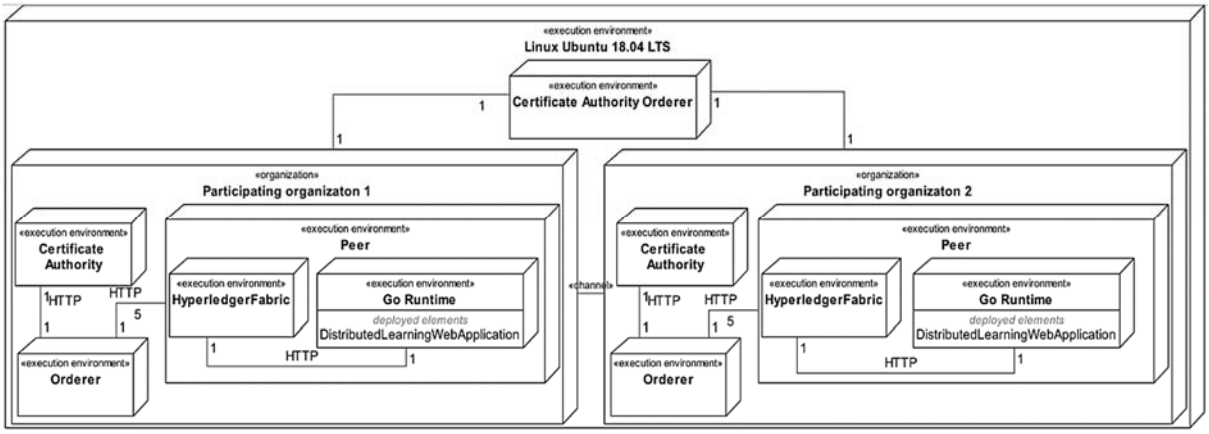


Fig. 1. Configuration of the network used in proof-of-concept implementation.

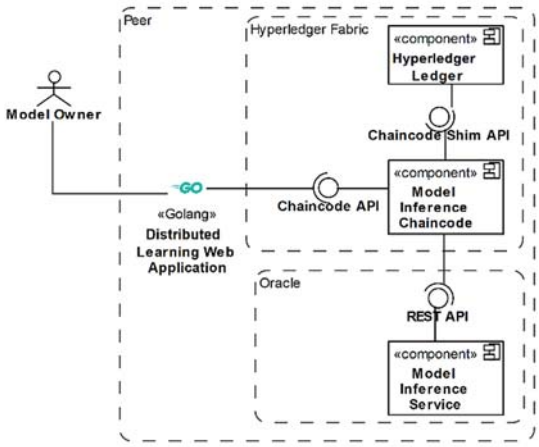


Fig. 2. Components of a network peer node.

4. Proof-of-concept Implementation

To validate the proposed architecture, we have developed a prototype HF network. This HF network was implemented using containerized HF components using configuration described in Fig. 1. This network allows model inference calculations by using blockchain oracles for two languages: Python and R. The blockchain oracles were created as individual components that implement model validation and model inference functions. Blockchain oracle powered by Python was implemented using Flask and PySpark libraries. R language oracle was utilized Plumber and MLR3 libraries. The distributed learning web application was created using Golang and supports uploading of the model and data from .zip and .csv files, respectively. The system was tested by performing model inference on all uploaded models. We have used logistic regression and decision tree ML models in R and Python and a dataset containing 32 000 rows with 14 features. The data sets, model representations were uploaded to blockchain network and successfully produced model inference.

5. Conclusions

The proposed architecture enables organizations to perform heterogeneous model inference calculations using the Hyperledger Fabric blockchain. The results can be combined via model ensembles or meta-learning (or aggregated teacher in student-teacher learning) to achieve a stronger learner collectively. The blockchain oracles in our solution expand the list of compatible ML technologies from those supported by the blockchain chaincode only to the generic set more commonly used in a field of machine learning. The proposed architectures performance was tested by creating proof-of-concept implementation that used multiple model types with multi-oracle setup.

References

[1]. L. Li, Y. Fan, M. Tse and K.-Y. Lin, A review of applications in federated learning, *Computers & Industrial Engineering*, Vol. 149, 2020, 106854.

[2]. X. Runhua, B. Nathalie and J. James, Privacy-Preserving Machine Learning: Methods, Challenges and Directions, *arXiv:2108.04417*, 2021.

[3]. D.C. Nguyen, M. Ding, Q.-V. Pham, P. N. Pathirana, L. B. Le and A. Senevirtavatine, Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges*, IEEE Internet of Things Journal*, 8, 16, 2021, pp. 12806-12825.

[4]. L. Yuzheng, C. Chuan, L. Nan, H. Huawei, Z. Zibin and Y. Qiang, A Blockchain-Based Decentralized Federated Learning Framework with Committee Consensus, *IEEE Network*, Vol. 35, No. 1, 2021, pp. 234-241.

[5]. K. Mammadzada, M. Iqbal, F. Milani, L. García-Bañuelos and R. Matulevičius, Blockchain Oracles: A Framework for Blockchain-Based Applications, in *Proceedings of the Business Process Management: Blockchain and Robotic Process Automation Forum, BPM 2020 Blockchain and RPA Forum,* Seville, Spain, September 13–18, 2020, pp. 19-34.

[6]. V. Drungilas, E. Vaičiukynas, M. Jurgelaitis, R. Butkienė and L. Čeponienė, Towards Blockchain-Based Federated Machine Learning: Smart Contract for Model Inference, *Applied Sciences,* Vol. 11, No. 3, 2021, 1010.

(028)

Correlations between Cryptocurrencies and Traditional Financial Markets during Turbulent Periods

M. Wątorek[1], J. Kwapień [2] and S. Drożdż [2,1]
[1] Cracow University of Technology, ul. Warszawska 24, 31-155 Kraków, Poland
[2] Complex Systems Theory Department, Institute of Nuclear Physics, Polish Academy of Sciences, ul. Radzikowskiego 152, 31-342 Kraków, Poland
E-mail: marcin.watorek@pk.edu.pl

Summary: In the paper the correlations between the cryptocurrency market represented by the two most liquid and highest capitalized cryptocurrencies: bitcoin and ethereum versus traditional financial markets: stock indices, Forex, commodities are measured in the period: Jan 2020 - Jul 2022. By calculating the q-dependent detrended cross-correlation coefficient on high frequency 10s data in the rolling window, the dependencies on various time scales, different fluctuation magnitudes, and in different market periods are examined. There are strong indications that the dynamics of bitcoin and ethereum price changes since March 2020 Covid panic is no longer separated, but it is related to changes in traditional financial markets. This is especially visible in the first half of 2022 in bitcoin and ethereum relation to US tech stocks when joint declines are observed.

Keywords: Financial markets, Cryptocurrencies, Cross-correlations, Multiscale, Hedge.

1. Introduction

Financial markets are characterized by an enormous network of connections and factors that can influence the structure and dynamics of the system [1]. One of the youngest parts of the modern financial markets are cryptocurrencies [2, 3]. Since the invention of Bitcoin in 2009 [4], the cryptocurrency market has experienced striking development in recent years, from being entirely peripheral to being a part of world financial markets [5].

2. Data and Methods

In the study, the cross-correlations between the cryptocurrency market represented by the two most liquid and highest capitalized cryptocurrencies: bitcoin (BTC) and ethereum (ETH) versus traditional financial markets: stock indices (Nasdaq 100 - NQ100, S&P500, Dow Jones - DJI, Russell 2000 - RUSSEL, and DAX), Forex (Australian dollar - AUD, Canadian dollar - CAD, Swiss franc - CHF, Chinese juan - CNH, euro - EUR, British pound - GBP, Japanese jen - JPY, Mexican peso - MXN, Norwegian krone - NOK, New Zealand dollar - NZD, Polish zloty - PLN, and South African rand - ZAR) and commodities (WTI crude oil - CL, high grade copper - HG, silver - XAG, and gold - XAU) are measured. All these instruments are expressed in USD and their quotes cover a period from Jan 1, 2020 to Jul 1, 2022. Each week the quotes were recorded from Sunday 22:00 to Friday 20:15 with a break between 20:15 and 22:00 each trading day (UTC). The original price changes, sampled every 10s, were transformed into logarithmic returns: $r(t_m) = ln\ P_i(t_{m+1}) - ln\ P_i(t_m)$, where $P_i(t_m)$ is a price quote recorded at time t_m (m=1,…,T) and i represents a particular financial instrument. The standardized prices of all the instruments considered are plotted in Fig. 1 against time.

The Pearson correlation coefficient [6, 7] may not be well suited to the high-frequency data of the cryptocurrency market, since these data are characterized by high volatility and, thus, nonstationarity. This is why cross-correlations will henceforth be measured using an alternative method: the q-dependent detrended cross-correlation coefficient $\rho_q(s)$, which allows tio lift the assumption of data stationarity [6]. The values of $\rho_q(s)$ calculated for BTC and ETH versus the traditional instruments in the first half of 2022 are shown in Fig. 2. One can immediately notice two properties: (1) the correlation strength increases with scale s for most financial instruments, and (2) the correlation strength is lower for q=4 (i.e., for large fluctuations) the strongest cross-correlations measured by $\rho_q(s)$ for q=1 are BTC and ETH versus the stock indices NQ100 and S&P500. By calculating the $\rho_q(s)$ in a 5-day rolling window with a 1-day step was, the dependencies on two time scales: s=12 (2 min) and s=360 (60 min) in different market periods are examined - Fig. 3. During Period I a significant positive cross-correlation for BTC and ETH versus the risky assets such as the stock indices, CL, HG, and the commodity currencies can be observed. What is more interesting is the appearance of the even stronger positive cross-correlations for BTC and ETH versus almost all the other instruments except for JPY in the second half of 2020. The third period of the significant cross-correlations for BTC and ETH versus the other instruments starts at the beginning of Dec 2021 after the Nov. 2021's all-time highs on both the cryptocurrency and the US stock markets occurred.

3. Figures

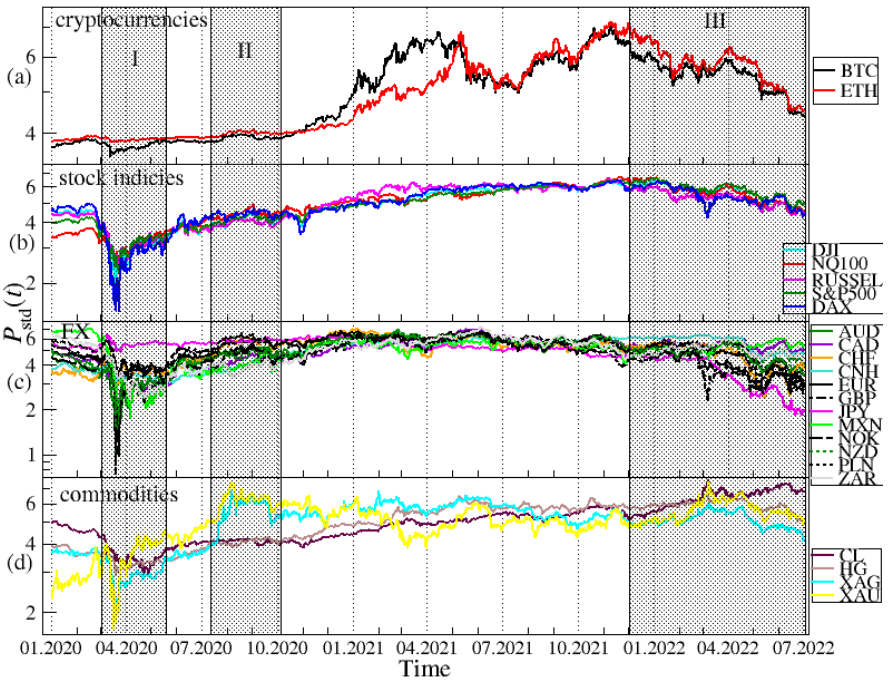


Fig.1. Evolution of the standardized price of the cryptocurrencies (a), the stock market indices (b), the fiat currencies (c), and the commodities (d) over a period from Jan 1, 2020 to Jul 1, 2022. The periods for which significant correlations between the cryptocurrencies and the US stock indices are distinguished by grey vertical strips. The most characteristic events are denoted by Roman numerals: a Covid-19-related crash in Mar 2020 and a quick bounce in Apr-May 2020 (event I), new all-time highs of NQ100 and S&P500 and a Sep 2021 correction (event II), and a bear phase in the cryptocurrency and stock markets since Nov 2021 (event III).

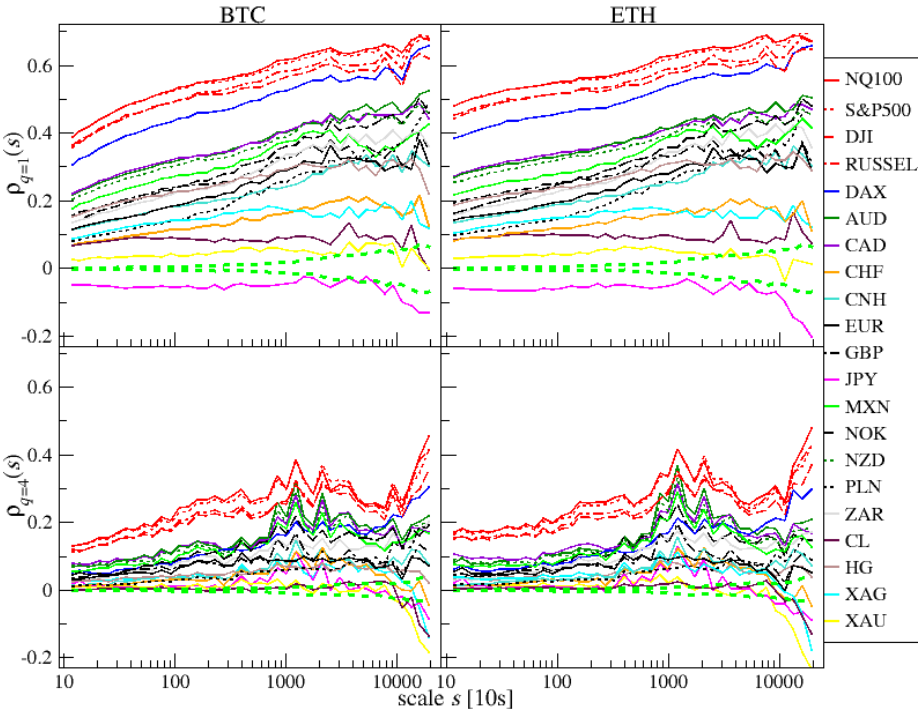


Fig.2. Correlations measured by the q-dependent detrended cross-correlation coefficient $\rho_q(s)$ in the first half of 2022 between BTC (right) and ETH (left) versus selected traditional financial instruments for q=1, which does not favor any specific amplitude range (top), and for q=4, which amplifies large return contributions (bottom). The region of statistically insignificant correlations (dotted green line) is given as the ±standard deviation of $\rho_q(s)$ calculated from 100 independent realizations of shuffled time series.

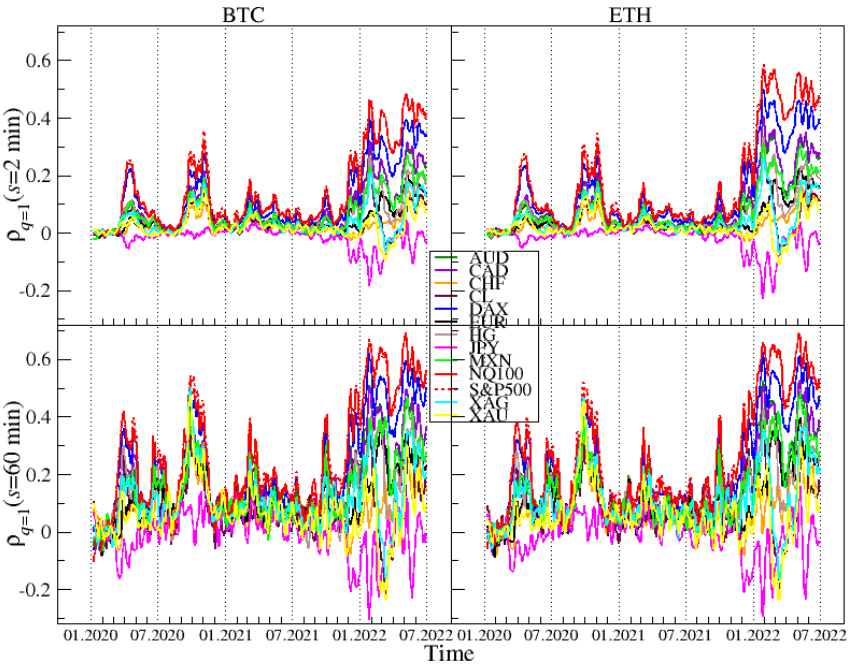


Fig.3. Evolution of the q-dependent detrended cross-correlation coefficient $\rho_q(s)$ with q=1 calculated in a 5-day rolling window with a 1-day step between Jan 1, 2020 and Jul 1, 2022 for the price returns of BTC (left) and ETH (right) versus the selected traditional assets expressed in the US dollar: AUD, CAD, CHF, CL, DAX, EUR, HG, JPY, MXN, NQ100 S&P500, XAG, and XAU. Two time scales are shown: s=2 min (top) and s=60 min (bottom).

4. Conclusions

Based on the multiscale cross-correlation analysis, it can be concluded that the dynamics of the cryptocurrency market has not been separated from traditional financial markets. Consistently, the most liquid cryptocurrencies, BTC and ETH, cannot serve as a hedge or safe haven for the stock market investments, especially during the turbulent periods like the Covid-19 panic, but also during the recent bear market time on tech stocks, which has been accompanied by the parallel bear market on cryptocurrencies. Many observations show that the Covid-19 pandemic may have changed the paradigm that the cryptocurrency market is largely independent from the other financial markets. Recent market turmoil and the strong US dollar additionally increase the strength of cross-correlations for BTC and ETH versus the US tech stocks. This is a strong indication that, after 12 years of the maturation process, the cryptocurrency market has finally become a connected part of the global financial markets.

References

[1]. J. Kwapień, S. Drożdż. Physical approach to complex systems, *Phys. Rep.,* 515, 2012, pp. 115–226.

[2]. S. Corbet, A. Meegan, C. Larkin, B. Lucey, L.Yarovaya. Exploring the dynamic relationships between cryptocurrencies and other financial assets, *Econ. Lett.,* 165, 2018, pp. 28-34.

[3]. S. Corbet B. Lucey A. Urquhart L. Yarovaya, Cryptocurrencies as a financial asset: A systematic analysis, *Int. Rev. Financ. Anal.*, 62, 2019, pp. 182-199.

[4]. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. (https://bitcoin.org/bitcoin.pdf)

[5]. M. Wątorek, S. Drożdż, J. Kwapień, L. Minati, P. Oświęcimka, M Stanuszek, Multiscale characteristics of the emerging global cryptocurrency market, *Phys. Rep.,* 901, 2021, pp. 1-82.

[6]. J. Kwapień, P. Oświęcimka, S. Drożdż, Detrended fluctuation analysis made flexible to detect range of crosscorrelated fluctuations, *Phys. Rev.,* E 92, 2015, 052815.

[7]. K. Pearson, Note on regression and inheritance in the case of two parents, *Proc. R. Soc. Lond.*, 58, 1895, pp. 240–242.

(030)

How to Build Self-Sustaining Tokenomics

O. Letychevskyi, V. Peschanenko, M. Poltoratskyi and Yu. Tarasich
GARUDA.AI, Ltd., 19-H Vysokosna str., 73035, Kherson, Ukraine
Tel.: + 380502665872
E-mail: tokenomics@garuda.ai

Summary: The development and launch of blockchain products based on a safe and self-governing token economy that satisfies all the desired properties of the blockchain market remains an open and painful issue for startup/active project owners and investors. The tokenomic model must provide economic equilibrium in its functioning for the project authors to obtain a predictable profit. Thus, the project owners need to develop and offer a quality product. The only algebraic formal approach and creation of the relevant tool allow for resolving these issues.

The main idea of the article is to present the algebraic approach and description of the authors' own unique tokenomics modeling tools. The Tokenomics Constructor and Model Creator tools' main features were introduced. The proposed approach is successfully used for Tokenomics Models verification. In addition, it allows project owners to use the outcome data to improve their initial token economy idea in a way it will become long-lasting, balanced, and self-sustainable.

Keywords: Token economy, Behaviour algebra, Formal methods, Symbolic modelling, Insertion modelling, Tokenomics Constructor, Model creator.

1. Introduction

Today the whole world is experiencing a mass blockchain adoption boom in all spheres of human activity. As a result, new projects and services evolve daily, creating a new ecosystem of crypto-related platforms and products that utilize cryptocurrencies and tokens. But creating a self-governing economy is still very difficult, requiring much effort, knowledge, and provision.

If we analyze the current situation in the blockchain products market, it's easy to see that most creators, even if they have a profound whitepaper and seem to have quite a thoughtful token economy, intuitively build pyramid-like structures with a lack of real token utility and stakeholders motivation to hold and most important - use their tokens in daily activities within the platform. As a result, we have most projects that will never reach a system balance and become too dependent on whale investors' speculations.

Is there a simple and efficient way to help blockchain project creators to avoid mistakes and create self-sustainable token economies right at the stage of white paper and MVP development? The answer is - math and formal methods. Modeling is a mandatory activity that shall be provided during Tokenomics creations. Algebraic modeling can help build and prove the economic equilibrium, analyze different undesirable properties like centralization or prevent the malicious actions of unscrupulous stakeholders.

Our approach is to use an algebraic modeling approach, implemented within the framework of the Insertion Modeling System IMS [1,2] that was developed at the Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine under the guidance of an Academician of the National Academy of Sciences of Ukraine, Professor A. A. Letichevsky. Insertion modeling is an approach for modeling complex distributed systems based on the theory of interaction between agents and environments. This theory has been successfully used in the last decade to verify software system specifications.

The software tools and systems that authors successfully use to formalize and verify tokenomics models (Algebraic Programming System (APS) [1, 2], Insertion Modeling System (IMS) [1, 2], Model Creator [3, 4], Tokenomics Constructor [5], etc.), in particular, Tokenomics Constructor tool, are presented in this article.

Them allows us to input the parameters of a future token economy, including ICO rounds data, predicted efficiency of the product, desirable token price, and profit after a period of product functioning. Using formal methods, the Tokenomics Constructor that works in pairs with our Algebraic Server can compute the initial parameters of Tokenomics that lead to desirable results and predict the possible troubles - the modeling algorithm is based on the historical data of exchange trading and the liquidity of tokens - that allows us to make accurate predictions and show possible outcomes.

2. Market Overview

Parallel to the rapid development of tokenomics in the last few years, we are also observing the market's saturation with various products and services that allow us to conduct some research in the field of blockchain and, in a certain sense, provide an opportunity to analyze tokenomics models.

One of the tools that are used for analyzing tokenomics models is the cadCAD tool. The example of using the cadCAD system to analyze the Insolar tokenomic model is presented in [6, 7]. The authors use differential game theory and stochastic modeling techniques. Supply and demand are modeled as stochastic dynamic systems.

The agent-oriented approach for the token economy simulation is realized in the Tokesim tool [8]. The tool was developed in Python programming language and created using the Mesa ABM and OpenRPC infrastructure. The tool allows developers to model interactions with smart contracts and tests smart contracts based on Ethereum.

A theoretical analysis method for estimating the profit of different roles in tokenomics and a root method for calculating the weights of indicators is proposed in [9]. The proposed algorithms were implemented in the Python programming language. The authors created a value creation network to analyze the main factors and proposed two economic models: a model of the hierarchical structure of the alliance and a new model of profit.

There are a lot of calculators that allow users to calculate the ROI for staking, token ROI, liquidity, an estimate of staking rewards, etc. [10-14].

For example, Uniswap V3 Fee Calculator [10] calculates specific token amounts as well as liquidity and uses the current swap volume and liquidity to create an estimate of future fee potential based on historical values. Ada Staking Calculator [11] helps users to calculate their possible staking rewards.

There are also special tools for the analysis of blockchain data, such as BlockSci [15], Blocksim [16], Simblock [17], etc.

But more of these tools only support specific use cases and can't be used for full-fledged tokenomics project modeling.

We present a general approach that may be used to build a formal tokenomics model in terms of behavior algebra. This makes it possible to apply a method such as algebraic modeling and provide proof of execution of the liveness and safety properties.

3. Tokenomics Constructor

The Tokenomic Constructor is a special Web interface for modeling and evaluating tokenomics projects (Fig.1). It is based on the AVM (Algebraic Virtual Machine) [18] system and allows for automating the creation of the algebraic representation of tokenomics models for the Model Creator tool.

The main features of the tokenomic constructor are:

1. Creation of multiple scenarios and token lifecycles;
2. Aid in model creation with different levels of abstraction;
3. Use of external scenarios for liquidity & market activity changes;
4. Behaviour algebra specifications for token economy modeling;
5. Verification of the model for undesirable properties such as centralization or token leakage.

The project owner can define the needed exchange functions and enter specific data planned for the project – the total number of tokens, a list of the agents of the tokenomics model and rewards data, needed pools data, and the marketing functions for planned project services (farming, staking, etc.) (Fig. 2, Fig. 3).

After entering the desired data, the algebraic server [4] will be queried for the simulation. In this case, when all data were received from the Tokenomics constructor, we get the specific model. It allows us to build the chart of the agents' tokens distribution and calculate the token price depending on the time, such as a monthly duration. Other charts and special properties also can be specified during the query to the algebraic server.

After receiving the file with the algebraic model, we can view, simulate and change the model in the Model Creator tool. This system provides an interface for creating appropriate agents and environments and modeling the entire system with the output of graphs and corresponding scenarios in the form of message sequence chart traces. A brief description of it is given below.

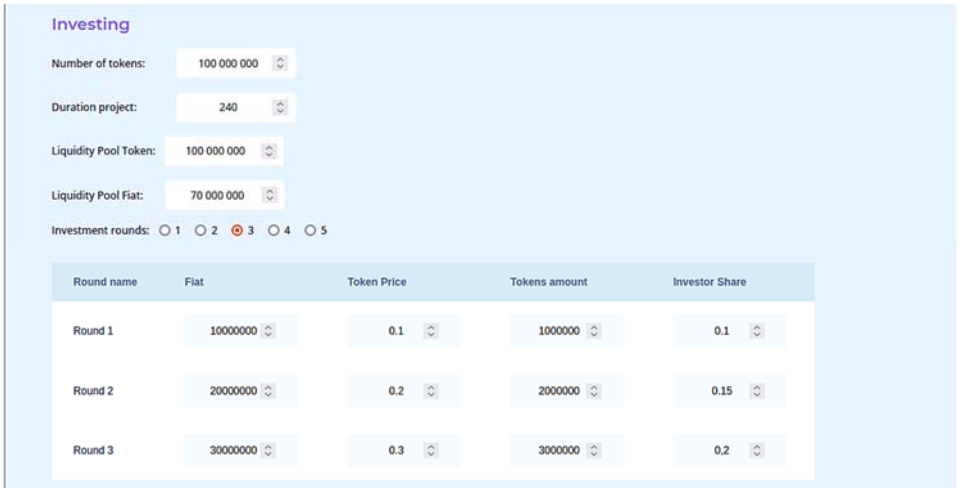


Fig. 1. Fragment of the Tokenomic Constructor. Investing Process Data.

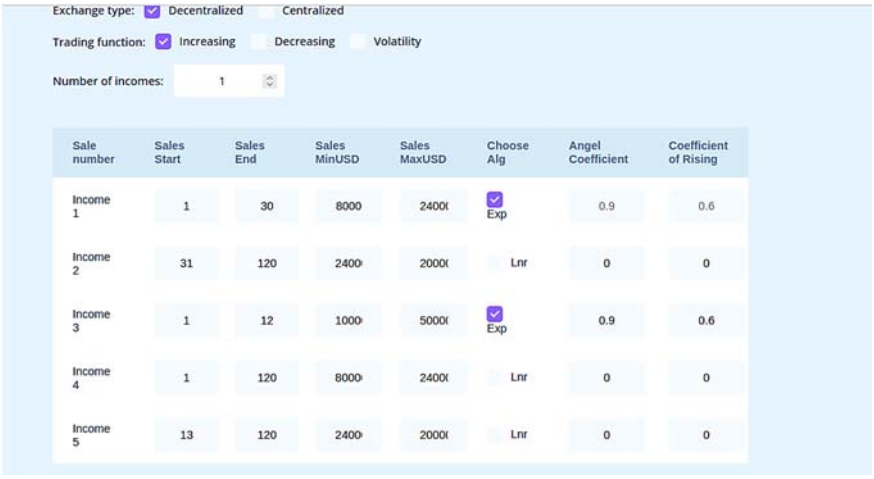


Fig. 2. Fragment of the Tokenomic Constructor. Incomes Data

Fig. 3. Fragment of the Tokenomic Constructor. Vesting and Unloking.

4. Model Creator

Model Creator is a system that uses symbolic modeling techniques, including algebraic and deductive-formal methods, for solving complex problems.

The platform's key features are testing technology, model-based development, supporting the development process of a critical system or quality of service (QoS) system, verification and validation, and cybersecurity.

The Model Creator includes several systems and libraries for implementing formal algebraic methods and integrating them with other software systems.

An example of the implementation of the model in the system is shown in Fig.4.

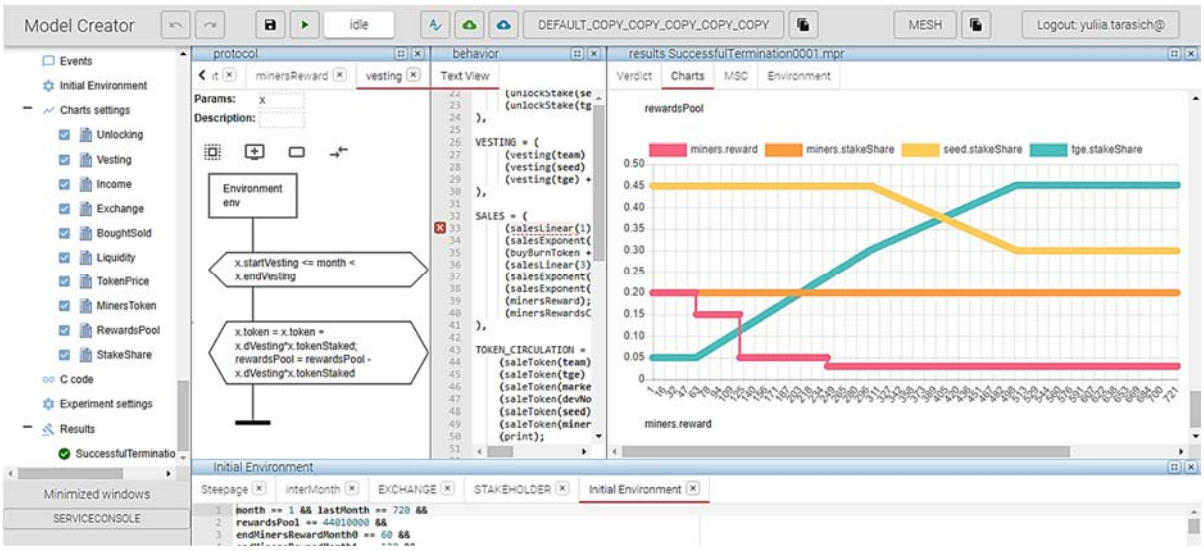


Fig. 4. Model Creator.

5. The Theory of Agents and Environments. A Brief Review

The basic idea is the interaction of agents in a certain environment. The environment may also be an agent that interacts with similar agents in a higher-level environment and so on. Thus, having the multilevel in the formalization of knowledge, we can operate with objects at different levels.

We consider agents as entities that change their state in the process of evolution. The state of the agent is determined by its attributes, which are typed, i.e., determined by a certain theory with operations and predicates in it. For example, linear arithmetic with arithmetic operations and such predicates as equalities and inequalities, or byte theory, where operations are the copying of bytes and predicates are comparing of their contents. In tokenomics, agents are participants in a tokenomic game, and the attributes are the number of tokens and the amount of fiat money, which are determined by arithmetic over floating-point numbers. Boolean functions, such as disjunction, conjunction, and negation, are also used to express attribute statements.

The environment also contains attributes that are available to all agents. In turn, only their attributes are available to agents. The states of all agents and the values of the attributes of the environment constitute the general state of the environment, which formulas can express over the attributes that may relate to different theories. Each agent can perform certain actions that change its state, such as changing the values of the attributes of the agent. Each action consists of a precondition and a postcondition, and they are also formulas from the theories defined in the model. The precondition determines that it is compatible with the state of the environment, and that its conjunction is satisfiable. Also, the postcondition determines how the state of the environment will change after the action.

Example of action in tokenomics (agent x purchases N tokens):

```
buy(x,N): (exchange.token > 0) ->
(exchange.token = exchange.token - N;
exchange.fiat = exchange.fiat + N*tokenPrice;
 x.token = x.token + N)
```

An assignment operator is used in action formulas that show how the environment is changing. The general formula of the environment will be used and changed according to such operators when modeling tokenomics.

Expressions of behavioral algebra are the behavioral operations of the actions of agents. Operation “.” (prefixing) a.S determines the execution of action a under the behavior S. Another operation "+" (alternative choice) defines the branching of two behaviors. These behaviors can be performed non-deterministically or take into account the precondition of the action.

The behavioral equation can contain parallel or sequential compositions of behaviors. The expression of behavioral algebra consists of the actions, behaviors, and operations of behavioral algebra, and of corresponding compositions. The behavioral equation contains a unique identifier of behavior on the left part and a behavioral algebra expression on the right part.

6. Internet of Things Project Tokenomics Model. Formalization and Simulation Results

The example considers the using formal methods and an algebraic approach to create a tokenomics model for a project built on the IOTA platform.

It demonstrates the equilibrium of the token life cycle and initial parameters of Tokenomics that were defined using algebraic modeling.

The model was used to establish a forecasted scenario, including conservative values for parameters of interest such as Token Price, Liquidity, amount of Burned Tokens, and Distribution of tokens towards traders, miners, investors, and cryptocurrency exchanges.

The project involves the deployment of a network of antenna devices to enable connectivity for the Internet-of-Things (IoT). This service functions on the IOTA Tangle using the project own token. This token is used to pay for traffic by Users. The service also introduces an additional token, which is linked to the dollar exchange rate and is used to determine the cost of traffic. Owners (miners) of purchased antenna devices (nodes) receive rewards for providing coverage and using the service.

The tokenomics of a project consists of two parts/stages. The first part - the pre-production stage, during which service development takes place, involves the open sale of tokens along with marketing activities for the operation. During this period, the sale of nodes begins. Purchased devices are involved in the test period and the owners of antenna devices (miners) are rewarded.

The product stage is defined by the functioning of the product and forms a self-managed sustainable system of tokenomics. During the product stage, IoT devices are sold and connected to the service network. Device owners buy tokens on a cryptocurrency exchange to pay for traffic. Investors, the team and miners receive tokens as rewards. Tokens shall be listed on the cryptocurrency exchange at the beginning of the product period.

For this model we define the next agents:

- Investor (tge and seed agents) buys tokens. The fiat proceeds from the sale of tokens to the Investor goes into the budget for development, marketing, and other expenses. Investors can sell tokens on the cryptocurrency exchange, receiving fiat as well as receiving tokens as profit for blocked tokens.

- Team receives tokens as profit from the project's service from Platform (general tokens pool). The team sells tokens on the cryptocurrency exchange.

- Miners receive a reward from the Platform (Reward Pool) for covering the network, as well as a

reward for transmitting data. Miners sell tokens for the Exchange.

- Exchange sells Speculant tokens and buys tokens from Speculant, Team, and Investor.

Speculant buys and sells tokens from the cryptocurrency Exchange.

- Marketing receives tokens from the general tokens pool. Marketing sells tokens for the Exchange.

- devNoperations receive tokens from the general tokens pool. devNoperations sells tokens for the Exchange.

We consider listing a company on a decentralized exchange, so a new token price will be formed each time the number of tokens bought or sold changes.

The top-level main equation as a sequential composition of the five parts of IoT tokenomics is presented as:

```
B1 = (  (UNLOCKING); (VESTING); (SALES);
     (TOKEN_CIRCULATION); (STAKING);
     (nextMonth.B1 + !nextMonth.Delta))
```

Let's consider the equations that represent the SALES and TOKEN_CIRCULATION parts more detail:

```
SALES = (
    (salesLinear(1) + !salesLinear(1));
    (salesExponent(2) + salesExponentInter(2) +
noSales(2));
    (buyBurnToken + !buyBurnToken);
    (salesLinear(3) + !salesLinear(3));
    (salesExponent(4) + salesExponentInter(4) +
noSales(4));
    (salesExponent(5) + salesExponentInter(5) +
noSales(5));
    (minersReward); (minersRewardsChanging +
!minersRewardsChanging)),
```

The behavior describes several types of token sales - linear and exponential - actions salesLinear(n) and salesExponent(n), n=1,…,5. Thus, in order to model the possibility of transitions between types of sales, 5 different sales time intervals are considered. Behavior also includes actions of tokens burning and rewarding miners.

```
TOKEN_CIRCULATION = (
    (saleToken(team) + !saleToken(team));
    (saleToken(tge) + !saleToken(tge));
    (saleToken(marketing) + !saleToken(marketing));
    (saleToken(devNoperations) +
!saleToken(devNoperations));
    (saleToken(seed) + !saleToken(seed));
    (saleToken(miners) + !saleToken(miners));
    (newLiquidity + !newLiquidity);
    (newPriceDelta + !newPriceDelta)),
```

Behavior describes the processes of selling tokens by various agents, including the actions of recalculating the price change and liquidity of the token.

Each agent's action describes the transition in the tokenomics system from one state to another when the token distribution changes.

For example, **buyBurnToken** action describes the processes of buying and burning tokens.

```
buyBurnToken =((exchange.token > 0) ->
("Environment#env:action 'Buy and Burn Token' ")
(exchange.token = exchange.token -
totalFiatIncome/tokenPrice;
exchange.fiat = exchange.fiat + totalFiatIncome;
BOUGHT_TOKEN = BOUGHT_TOKEN +
totalFiatIncome;
rewardsPool = rewardsPool +
totalFiatIncome/tokenPrice; totalFiatIncome = 0)),
```

The number of tokens purchased by agents is deducted from the exchange and added to the reward pool. The amount of exchange's fiat received from sales increases.

Having a formal description of the parallel composition of behaviors together with actions, we can analyze the properties of tokenomics, in particular, constructing charts of different behaviors or algebraic charts for arithmetic data.

Property analysis was performed using modeling, both concrete (or simulation) and symbolic. If we determine all the initial conditions and criteria of behaviors on the stock exchange and the marketing plan, it is possible to build a chart of the token price as an indicator of equilibrium.

This system was simulated with the following conditions:

- The effect of trading activity on token liquidity 10-40 %;

- A positive trend in marketing with regard to market saturation and coverage was considered. An unsuccessful outcome was not considered;

- Volatility was considered with different starting number of tokens when listing the exchange, with different distribution of marketing, with different initial number of buyers;

- Sensitivity is observed in more than 5 years in the case of a shortage of tokens for the exchange settlements with the increase in consumers. To eliminate this, the required (larger) number of tokens for the listing is calculated.

The examples of obtained results for concrete modeling are presented below (Figs. 4-5).

7. Conclusions

Using the proposed approach and tools provides an opportunity to create self-sustaining tokenomics for projects in various subject areas. Today we've successfully used it to create and verify tokenomics models for education, the Internet of Things, cryptocurrency exchange projects, etc. [3, 19]. Tokenomics Constructor doesn't require serious mathematical knowledge, so it's able for mass use and can be used to find the most prevalent tokenomics projects' problems. In addition, all models can be extended and verified in the Model Creator.

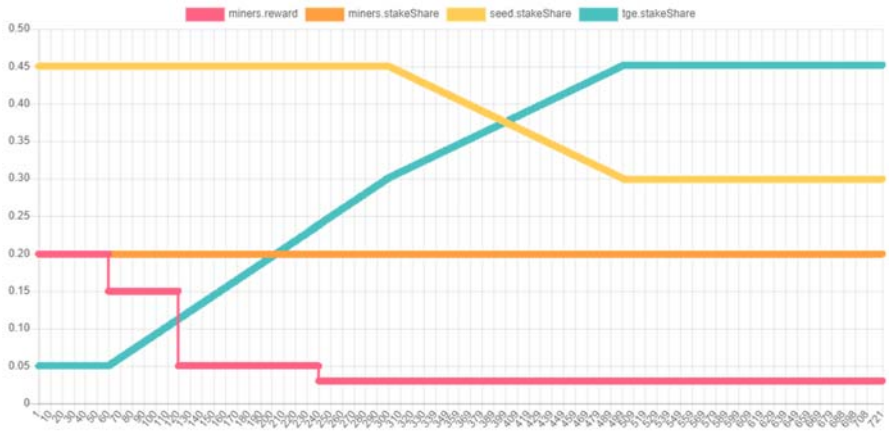


Fig. 4. Burning and Rewards.

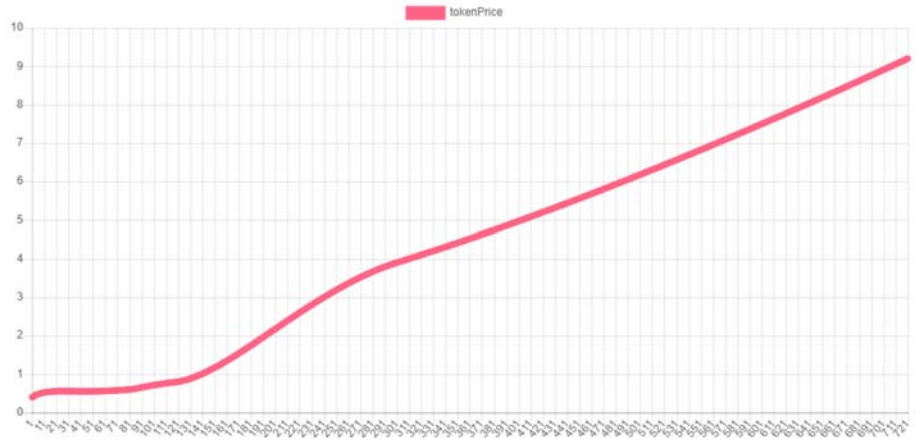


Fig. 5. Token Price.

References

[1]. APS & IMS (https://apsystems.org.ua/index.php)

[2]. A. Letichevsky, O. Letychevskyi, V. Peschanenko, Insertion Modeling and Its Applications, *Computer Science Journal of Moldova,* Vol. 24, No. 3, 2016, pp. 357-370.

[3]. O. Letychevskyi, V. Peschanenko, M. Poltoratskyi, Y. Tarasich, Platform for modeling of algebraic behavior: Experience and conclusions, in *Proceedings of the CEUR Workshop*, Vol. 2732, 2020, pp. 42–57.

[4]. Model Creator (https://rd.litsoft.com.ua/)

[5]. Tokenomics Constructor (https://tokenomics.litsoft.com.ua/)

[6]. Z. Zhang, Engineering token economy with system modeling. (https://arxiv.org/ftp/arxiv/papers/1907/1907.00899.pdf)

[7]. cadCad (https://github.com/cadCAD-org/cadCAD)

[8]. Tokesim (https://github.com/tokesim/tokesim#about-the-project)

[9]. C. Guo, P. Zhang, B. Lin, J. Song, Dual Incentive Value-Based Paradigm for Improving the Business Market Profitability, *Blockchain Token Economy. Mathematics,* Vol. 10, 2022, p. 439.

[10]. Uniswap V3. Calculator & Simulator (https://www.metacrypt.org/tools/uniswap-v3-calculator-simulator)

[11]. Ada Staking Calculator (https://cardano.org/calculator/?calculator=delegator)

[12]. Custom token ROI calculator (https://pulse.enecuum.com/#!/token-roi)

[13]. Staking rewards (https://www.stakingrewards.com/calculator)

[14]. Cryptolek. Rewards calculators (https://cryptolek.com/staking)

[15]. H. Kalodner, et al. {BlockSci}: Design and applications of a blockchain analysis platform, in *Proceedings of the 29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 2721-2738.

[16]. M. Alharby, A. Van Moorsel, Blocksim: a simulation framework for blockchain systems, *ACM SIGMETRICS Performance Evaluation Review*, Vol. 46, Issue 3, 2019, pp.135-138.

[17]. Yu. Aoki, et al., Simblock: A blockchain network simulator, in *Proceedings of the -IEEE Conference on Computer Communications Workshops (Infocom 2019)*, 2019. pp. 325-329.

[18]. A. Letychevskyi, V. Peschanenko, V. Volkov, Algebraic Virtual Machine Project, in *Proceedings of the Communications in Computer and Information Science Workshops (ICTERI' 2021)*, Vol. 1635, 2022, pp. 353–364.

[19]. O. Letychevskyi, Creation of a Self-Sustaining Token Economy, *The Journal of the British Blockchain Association*, February 2022.

(031)

The Art NFTs and Their Marketplaces

Lanqing Du [1], Michelle Kim [2] and Jinwook Lee [1*]

[1] Drexel University, Philadelphia, PA 19104, USA
[2] Horace Mann School, Bronx, NY 10471, USA
* E-mail: jl3539@drexel.edu

Abstract: Non-Fungible Tokens (NFTs) are crypto assets with a unique digital identifier for ownership, powered by blockchain technology. Technically speaking, anything digital could be minted and sold as an NFT, which provides proof of ownership and authenticity of a digital file. For this reason, it helps us distinguish between the originals and their copies, making it possible to trade them. This paper focuses on art NFTs that change how artists can sell their products. It also changes how the art trade market works since NFT technology cuts out the middleman. Recently, the utility of NFTs has become an essential issue in the NFT ecosystem, which refers to the owners' usefulness, profitability, and benefits. Using recent major art NFT marketplace datasets, we summarize and interpret the current market trends and patterns in a way that brings insight into the future art market.

Keywords: Non-fungible tokens (NFTs), Digital art, NFT marketplace, Machine learning, Principal component analysis.

1. Introduction

1.1. NFTs and the Art World

In April, 2022, Sotheby's sold a small receipt paper of the 1959 project called "Zone of Empty Space" by Yves Klein, the French conceptual artist, for $1.2 million. It was a part of the ledger where Klein recorded all sales and resales of the 1959 artwork ([1]). More than a half-century later, thanks to the blockchain technology and NFTs, this ledger-keeping has become an essential part of the art industry ([2, 3]).

The phrase "NFT art," we believe, is not the most accurate phrase. NFT itself is not the art, it is simply a technology that increases the utility of the art, by functioning as a proof and traceability of the ownership ([4-6]). Thus, throughout the rest of the paper we will be using the phrase "art NFT" as opposed to "NFT art."

There are three types of art NFT: digital art (stand-alone), PFP (generative art), and Phygital art (linking physical art with the NFT) ([7, 8, 9]). The very brief history of NFTs begins with digital art and its pioneer Kevin McCoy ([10, 11]). In 2014 McCoy and Anil Dash created the first stand-alone NFT, *Quantum* ([12]). Prior to *Quantum*, digital artworks were "fungible," meaning that there were multiples of the same artwork. Following McCoy, artists like Mike Winkelmann, better known as Beeple, and companies like Larva Labs, creator of CryptoPunks, took center stage on the NFT market.

The launch of CryptoPunks marked the creation of a new category of art NFT: PFP (Profile Pic) created using a technology called generative art. PFP art including CryptoPunks, Bored Ape Yacht Club (BAYC), Doodles, and recently Clone X doubled as a form of art and a status symbol on various social media platforms. In the last couple years, BAYC became widely popular within the NFT community and beyond, with the most expensive piece, #8817, selling for $3.4 million in 2021. ([13]) Yuga Labs, the creator of BAYC, have fully experimented with and implemented business strategy models like token-gating.

Token-gating is a way of adding value to an NFT by granting the holder exclusive access to content, community, events, and physical products, additional to the digital token ([14]). BAYC was also the first art that granted full commercial rights to the Intellectual Property (IP) to its holders, who were now able to commercialize their Bored Apes. Unsurprisingly, popularity factors for BAYC include commercial rights and exclusive access to spin-off collections like Bored Ape Kennel Club (BAKC) and Mutant Ape Yacht Club (MAYC) both of which have high resale value as well access to off-line events including the annual Ape Fest.

If commerce platforms like Nifty Gateway and Superway became well-known for their curation of digital art, marketplaces like OpenSea became highly successful from their listing of PFP art, such as the BAYC. While digital art centers around individual artists, like McCoy and Beeple, PFP centers around companies, Yuga Labs and Larva Labs being the most notable, where they curate communities, introduce roadmaps, and coordinate on and offline events and launches.

There are not yet any notable cases of the third type of art NFT, Phygital art (Physical and Digital art). Yet, by linking NFT (digital proof of authenticity) with the physical art, it will revolutionize both the NFT and the traditional art market. The prime challenge is finding an optimal method of linking the two; Quick Response (QR) codes, Radio Frequency Identification (RFID) and Near Field Communication (NFC) are a few ways.

Art NFT is changing the landscape of the art market and its players including, the artist, buyer, and platforms (galleries, online commerce platform). While in the traditional art market, galleries and auctions and its agents, functioned as an intermediary

between the artists, the artwork and the customers, the emergence of NFTs have bridged the gap between the three. Now the artist or the creator can list and mint their artwork directly on an online platform (with little to no commission fee) and oftentimes connect directly with their buyers. Though there are still technical, ethical, and sometimes legal issues associated with art NFT, it will shift the dynamic between the artist and the buyer, the role of the intermediaries (auctions, galleries, online platforms), and most notably the trends and value surrounding art.

1.2. Data Collection and our Key Findings

Our data collection is as follows: 11 marketplaces datasets from NonFungible.com ([15]): ArtBlocks, Azuki, BoredApeYachtClub, CloneX, CoolCats, CrypToadz, CryptoPunks, Meebits, TheSandbox, VeeFriends, and WorldofWoman. This is daily NFT marketplace datasets with one-year multivariate time series datasets from 09/13/2021 to 09/12/2022.
Each dataset contains the following ten features: (1) the number of sales (transactions), (2) total sales (USD), (3) average sales (USD), (4) the number of active market wallet, (5) primary sales, (6) secondary sales, (7) primary sales (USD), (8) secondary sales (USD), (9) unique buyers, and (10) unique sellers. Note that null values <0.05% of the entire dataset are removed in the given dataset.

2. Machine Learning on the NFT Marketplace Datasets

The principal components of data matrix are its singular vectors. Using the SVD (Singluar Value Decomposition), Principal Component Analysis (PCA) finds the largest singular values to extract the most important information from the data (with the largest variance) by solving perpendicular least squares (i.e., orthogonal regression) (see, e.g., [16]).
Note that, in the given datasets, each feature has a scale with a varied magnitude, thus normalization is performed first before passing the dataset to PCA. *Python* 3 (version 3.7.14) is used as the programming language and *sklearn.decomposition.PCA* function from Scikit-learn package (version 1.0.2) ([17]) is applied.

2.2. Numerical Results

Number of principal components (PCs) for each art NFT are presented in the Table 1.

Table 1. Number of principal components (PCs) for each art NFT.

ArtBlocks, BoredApeYachtClub, CloneX, CoolCats, Meebits, TheSandbox, VeeFriends, WorldofWoman.	2 PCs
Azuki, CrypToadz	3 PCs
CryptoPunks	4 PCs

In Fig. 1, for the NFTs with different number of PCs, the linear combinations for each PC are different.

In Fig. 2, the linear combinations for each PC in the NFTs (with 2 PCs) are comparable. From top left to top right: ArtBlocks, BoredApeYachtClub, CloneX, CoolCats. From bottom left to bottom right: Meebits, TheSandbox, VeeFriends, WorldofWoman.

In Fig 3, each heatmap represent the coefficient for a single art NFT (with 3 PCs). From left to right: Azuki, CrypToadz.

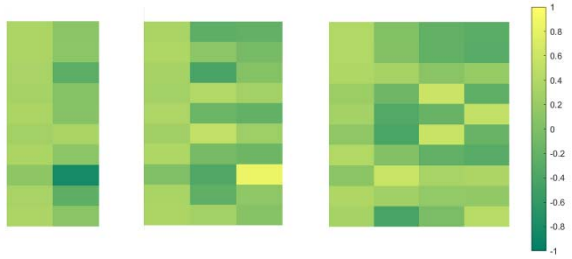


Fig 1. Principal component (PC) coefficient heatmap for NFT with two, three, and four PCs. From left to right: BAYC, Azuki, CryptoPunks.

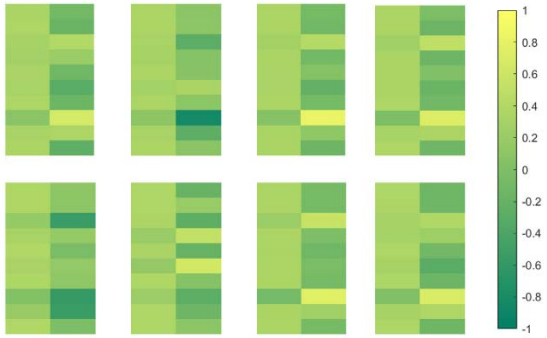


Fig 2. Principal component (PC) coefficient heatmap for NFT with two PCs. Each heatmap represent the coefficient for a single art NFT (with 2 PCs).

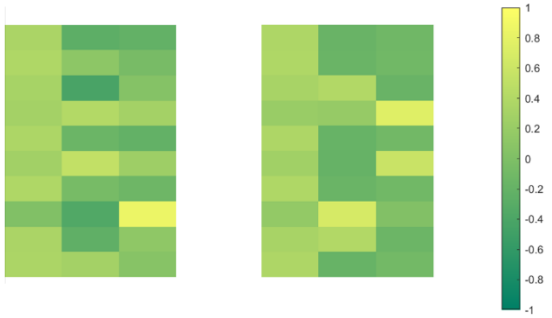


Fig 3. Principal component (PC) coefficient heatmap for NFT with three PCs.

2.3. Interpretation and Inferences

CryptoPunks, the only NFT marketplace which needs at least four PCs to reach 90 % cumulative proportion of variance explained, shows different behaviors from the other NFT marketplaces. For our PCA interpretation, we choose the linear combination of

features only that significantly contributes to the model. This is because we want to comprehend each major component with others not contributing to more than one component. Taking CryptoPunks as a special example, due to its relatively stable yet massive transaction amounts, we can write the following linear combination for each principal component:

$$PC1 = 0.38 \times SalesUSD + 0.39 \times ActiveMarketWallets + 0.37 \times SecondarySalesUSD + 0.39 \times UniqueBuyers + 0.39 \times UniqueSellers \quad (1)$$

$$PC2 = 0.58 \times AverageUSD \quad (2)$$

$$PC3 = 0.57 \times PrimarySales + 0.59 \times PrimarySalesUSD \quad (3)$$

$$PC4 = 0.43 \times NumberOfSales + 0.52 \times SecondarySales \quad (4)$$

Note that from Eq. 4 we can see that the features of SecondarySales and NumberOfSales make a significant contribution to the fourth principal component of CryptoPunks. On the other hand, it is not the case for BAYC. From this observation, we can say that CryptoPunks is a relatively more stable market, where the secondary transaction trading sizes are substantially larger based on PCA results.

3. Conclusions

NFTs are a new digital asset in the blockchain network. Its utility features and marketplaces are still in the process of reaching a point where users can find a more healthy and safe trading experience on digital assets. Sooner than later, NFTs may be linked to some physical counterparts (as utility NFTs). This paper finds some trends and patterns from the selected NFT trading marketplaces. Based on our data collection and analysis, the number of secondary sales is much higher than that of the primary sales. In other words, the art NFTs are still trading assets, bought and sold for short-term objectives, rather than long-term investments. Among our selected NFT marketplaces, CryptoPunks showed a unique pattern: (i) much fewer transactions; (ii) higher average sales amount. CryptoPunks is the only marketplace with four principal components for the PCA, explaining 95% of the total variation. In contrast, other marketplaces have two or three PCs with a similar explanation level of the variation. We hope our research delivers useful summaries and insights into the art NFTs as well as their unstable yet rapidly converging marketplaces.

References

[1]. The original NFT? Sotheby's to offer a receipt for an invisible work by Yves Klein for €500,000 (https://www.theartnewspaper.com/2022/03/22/sothebys-selling-receipt-invisible-yves-klein-work-paris).

[2]. D. Das, et al., Understanding Security Issues in the NFT Ecosystem, *arXiv preprint, arXiv:2111.08893.*

[3]. ERC-721 Non-Fungibal Token Standard (https://eips.ethereum.org/EIPS/eip-721)

[4]. M. Nadini, et al., Mapping the NFT Revolution: Market Trends, Trade Networks and Visual Features, *Scientific Reports*, Vol. 11, 2021, pp. 1-11.

[5]. F. Regner, et al., NFTs in practice – non-fungible Tokens as core component of a blockchain-based event ticketing application, in *Proceedings of the International Conference on Information Systems Conference (ICIS' 19),* 2019, p. 1479.

[6]. The fast growing NFT Market is problematic yet promising (https://www.coindesk.com/business/2020/09/21/thefast-growing-nft-market-is-problematic-yet-promising/).

[7]. Art Blocks (https://artblocks.io/)

[8]. D. Joselit, NFTs, or The Readymade Reversed, *October*, Vol. 175, 2021, pp. 3-4.

[9]. N. Lambert, Beyond NFTs: A Possible Future for Digital Art, *ITNOW*, Vol 63, Issue 3, 2021, pp. 8-10.

[10]. B. L. Frye, NFTs and the Death of Art, *Available at SSRN 3829399*, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3829399

[11]. M. D. Murray, NFTs and the Art World – What's Real, and What's Not, *UCLA Entertainment Law Review*, Vol 29, 2022.

[12]. The Birth of a New Discipline: The History of NFT art (https://art.haus/history-of-nfts/).

[13]. Top 11 Most Expensive Bored Ape Yacht Club NFTs (https://www.cryptotimes.io/most-expensive-bored-ape-yacht-club-nfts/).

[14]. A Retailer's Guide to Tokengating and NFTs (https://www.shopify.com/retail/token-gating).

[15]. Market tracker: NFT sales history & trends. NonFungible.com (https://nonfungible.com/market-tracker).

[16]. B. Everitt, T. Hothorn, An introduction to applied multivariate analysis with R, *Springer Science & Business Media*, 2011.

[17]. F. Pedregosa, et al., Scikit-learn: Machine Learning in Python, *Journal of Machine Learning Research*, Vol. 12, 2011, pp. 2825–283.

(033)

Blockchain Assisted Near-duplicated Content Detection

A. Moreaux and M. Mitrea
ARTEMIS Department, SAMOVAR Laboratory, Telecom SudParis – Institut Polytechnique de Paris, Palaiseau, France
E-mail: alexandre_moreaux@telecom-sudparis.eu

Summary: This paper presents a study on the possibility of coupling blockchain solutions to multimedia tracking applications. The challenge lies in accommodating complex operations such as visual fingerprint extraction and management, which usually occur on general-purpose computing machines, under the blockchain framework. The advanced solution features a load-balancing architectural framework combining a multimedia app, its database, a Smart Contract, and a Token Contract. Thus, we bring forward the proof of concept for the tokenization of multimedia assets using this architecture. We also provide a resource utilization analysis for two use cases involving a robust video fingerprinting method and the International Standard Content Code, respectively. Thus, we demonstrate the mutually beneficial association of offchain and onchain applications for visual content tracking.

Keywords: Blockchain, Visual fingerprint, Load-balancing, Tokens.

1. Introduction

This paper falls under the scope of the relationship between blockchain and multimedia technologies.

On the one hand, blockchains are peer-to-peer anonymous networks of nodes producing a sequence of cryptographically linked blocks, containing information about the transactions that have occurred in that network [1]. Their mainly act as a trusted third party in the exchange of assets and information between untrustworthy actors. Since their inception, blockchains have evolved to support a large area of applicative domains thanks to automated pieces of code called Smart Contracts. Smart Contracts are written in different languages for different blockchains (e.g., Solidity for Ethereum) and run exactly as they are programmed, with no possibility of change or influence from any central authority. Decentralized applications use Smart Contracts as backends serving frontend user interfaces to offer a wide array of services, including decentralized finance (DeFi), marketplaces, etc. The digital assets that are meant to be owned and exchanged are referred to as tokens, and can be fungible (interchangeable and splitable, as per legal tender) or non-fungible (representing unique assets and being undividable). Non-Fungible Tokens (NFTs) often serve as the representation of digital art and constitute a 4 billion USD market in 2021, projected to reach 200 billion USD by 2030 [2]. Yet, the environment is riddled with fraudulent content. The biggest NFT selling platform in the world [3], *Opensea*, observed that over 80% of the assets being flagged as plagiarized works, fake collections, and spam were created with their simplified "lazy minting" process, accessible to all [4]. This serves as an example to illustrate that NFT abuse can be easy, accessible, and rampant [5].

On the other hand, multimedia content represents one of the highly valuable assets on the market today. From video content for cinemas to audio analysis for military applications, nearly every sector benefits from advancements in multimedia content services. Being an asset so valuable, its protection is naturally at very high stakes, be it in academic or industrial settings. Various approaches allow to control the flow of data by hiding it (data encryption), identifying its owners (digital signatures), or tracking the content itself (digital watermarking and fingerprinting). Specifically, near-duplicated content protection (also referred to as visual fingerprinting) is a technology able to identify slightly modified versions of multimedia content. Fingerprinting is a technique that summarizes the perceptual characteristics of a digital contents into a semantically invariant digest. This technique differs from cryptographic hashing in that it retains semantic information about the input; this way, we can not only check if two fingerprints are strictly equal, but also how similar they are.

Visual fingerprinting does not feature any intrinsic trust property and blockchain is an appealing solution to this problem. Coupling blockchain to multimedia content presents no conceptual contradictions. For instance, some forms of multimedia content do appear on blockchains (e.g., NFTs). Yet, in a more general sense, the association between the two is limited by the lack of methodological bridges. Indeed, multimedia content processing is often prohibitively complex to be executed onchain.

This paper studies the use of fingerprinting techniques in blockchain environments. The main contribution is a load-balancing architecture that combines the trust and asset management of blockchains to precise content identification of fingerprinting. This way, the semantic unicity of entries in a database can be ensured. Each time a piece of multimedia content is candidate to be registered into a blockchain-authentified database, its fingerprint is compared to the previously recorded fingerprints. Upon acceptance, new entries are tokenized into NFTs that validate the good standing of the original content.

These NFTs can subsequently be exchanged or sold as per standard usage. We provide a proof-of-concept of this architecture for the Ethereum blockchain.

This paper is focused on providing the governance mechanism allowing the blockchain to accommodate fingerprinting applications. Fingerprinting methods themselves, database exploitation, and security concerns are out of our scope.

This paper elaborates on the topic with the following organization. We discuss the current state-of-the-art of blockchain-assisted applications in Section 2 before introducing our methodology in Section 3. In Section 4, we analyze the performance of our architecture, before concluding and discussing future work in Section 5.

2. State-of-the-art

Although theorized in 1994 [6], the concept of Smart Contracts gained popularity with Ethereum [7]. The capacity to enforce agreements between parties without the involvement of a trusted third-party enabled Smart Contracts to gain massive traction in DeFi and notarization, as summarized in [8]. Although legal gray zones and security threats undermined the boom, Smart Contracts quickly spread to other use cases (healthcare, could computing, energy, etc.) and the activity of scientific literature in the field suggests that opportunities are still being investigated for various industries [9]. Smart Contracts are often used as the backend to decentralized applications (dApps e.g., exchanges, marketplaces, etc.) in which case they interact with an offchain frontend User Interface. More specialized approaches, limited by the computing capacity of blockchains, tended to use Smart Contracts as complements to legacy applications such as wireless systems [10]. When it comes to multimedia content, blockchain can and has served the security, integrity, accessibility, and distribution of content, most through NFTs. Multimedia processing itself can be enhanced via blockchain technology as part of the process [11] or hand in hand with offchain technology [12]. The joint uses of content protection techniques and blockchains are summarized in [13]. This holistic survey cites encryption, watermarking and transaction tracking fingerprinting and indicates that near copy detection using visual fingerprinting techniques has not yet been associated with blockchain. When it comes to databases being used alongside blockchain, the IoT use case was analyzed in [14] and cloud computing in [15]. To the best of our knowledge, the replicated hashed onchain database as an integrity verifier brought forward in this paper is novel. The idea of a load-balancing architecture for blockchain-enhanced applications we used in this paper was brought forth in [16].

3. Methodology

In this section, we detail the architectural framework we designed for serving the needs of coupling blockchain to visual fingerprinting. We will start by explaining our method in a general sense, before detailing each of the blocs constituting the architecture.

3.1. General Architecture

This architecture, illustrated in Fig. 1, is designed as to ensure the processing and the data exchange among four entities: an offchain database, an offchain app, a Smart Contract, and a Token Contract. The first three entities represent the pillars of the solution while the Token Contract is called upon the successful processing of an input and does not interfere with the inner workings of the solution.

Before we delve into each one specifically, the execution workflow is presented. The initial setting up of the database and deployment of the Smart Contract is done by a qualified blockchain expert. Once setup, an unqualified operator can use the architecture, only ever needing to interact with the app.

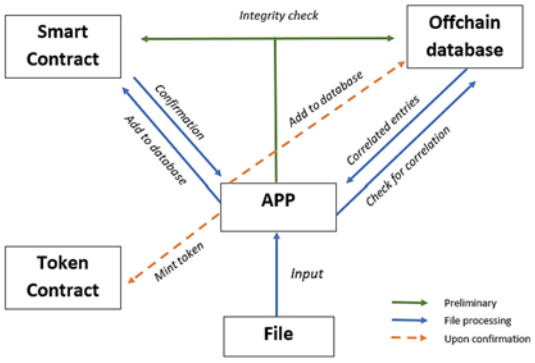


Fig. 1. General architecture.

The process starts with multimedia content being fingerprinted, and these fingerprints being stored on a database. They are then initialized on the blockchain via the Smart Contract, which serves as a pseudo database. This tamperproof (because onchain), redundant database allows the Smart Contract to serve as an arbiter ensuring the database has not been tampered with. It intervenes before the app compares an input (be it a new piece of content or a suspected copy) to each of the offchain database entries. Three results are possible:

- The input is detected as a copy of existing content (i.e., the fingerprint is identical to an entry of the database), the operator is informed as such and the process stops.
- The input is detected as a near copy of one of the entries according to the designating threshold (cf. Section 4) and the operator may decide to consider the input as a copy or not.
- The content is not detected as the copy of existing entry. The operator may add it to the database by answering a prompt.

Upon its arrival into the onchain database, the entry is minted as an ERC721 Non-Fungible Token [17] and sent to the wallet of the initiator of the transaction. This process is illustrated in Fig. 1 and Fig. 2.

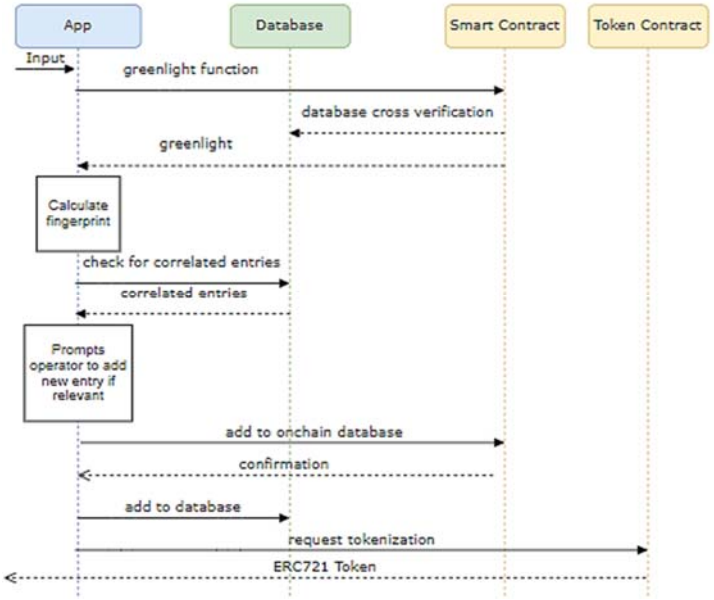


Fig. 2. Step-by-step addition of a new entry in the database.

3.2. The Offchain Database, App, and Token Contract

The proposed architecture does not worry itself with the exact technology managing the database. In fact, it only has light lifting to do, as it only needs to hold the fingerprints of the multimedia content and to pass that information on to the app when requested. Although it would be possible to hold the content itself in the database and fingerprint it upon retrieval, a lighter and more private database allows for faster processing and less potential privacy concerns.

The app has a central role in the process. Not only does it interact with both databases, but it is also the only point of contact for the operator. As such, the visual interface can be designed to make the process intuitive and easy to operate. In the context of a proof-of-concept, we did not develop any graphical interface and interacted with the app using a command prompt.

The app is given a file (.jpg, .mp4, .pdf depending on the use case) and an optional threshold (that defaults to a recorded value) as input parameters and begins by establishing a connection with the Smart Contract and invoking a greenlight function. This function returns True, allowing the process to continue, if and only if the offchain and onchain databases match. It does so by getting the size of the map of hashes and by using the compare function of the Smart Contract (Subsection 3.3) for each one of the entries of the offchain database. This process is expedited by the fact that the database contains fingerprints that need not be reprocessed systematically. The greenlight returning False will interrupt the process and inform the operator that the database has been tampered with.

Once this important control passed, the app calculates the input file's fingerprint and compares it to all the entries in the offchain database. As explained in Subsection 3.A, three possible results are presented to the operator: copy, near copy, or no copy. In the latter two cases, the operator may prompt the app to add the input to the database. The app then transactions the Smart Contract via the deployer wallet to add the hash of the new fingerprint to the onchain database, before adding the fingerprint (identified by its hash) to the offchain database. Note that the fingerprint is hashed before being stored in the Smart Contract because of size and format concerns (e.g., matrices are not supported). If the fingerprint in context happens to output short identifiers the hashing step may be skipped as it is not essential to the proper functioning of the code but could still be used to add a layer of privacy to the information.

Once the transaction that added the new entry to the Smart Contract is validated, the app queries the minting of a unique NFT. Our work being on Ethereum, we selected the popular ERC721 standard in which we put the hashed fingerprint of the file.

This NFT could be made more thorough, but its usage largely depends on the use case. If this architecture were used to certify content before it is sold as original, one could imagine additional information being present in the token to ensure the good standing of the content the token represents. Such additional information may relate to the transaction number of the initial admission of the entry in the database or the electronic signature of the issuing body operating the database.

In our example, the token is sent to the deployer wallet as it is the central entity of the use case. These tokens can then stay in this wallet or be sent manually or automatically to addresses belonging to the Intellectual Property Rights (IPR) holders, for example. It would be simple enough for the operator to indicate the address of the content provider for the token to be distributed directly upon validation.

3.3. The Smart Contract

As explained in Subsection 3.B and Fig. 2, the Smart Contract is used on two occasions: to provide information to the greenlight function and to process a new entry. The former does not require input data whilst the latter requires a hash and an optional string of general information concerning the entry. It maps these two entities into a structure containing a Boolean to indicate the existence of the hash and an optional string containing general information. In addition, it implements six functions.

Three of these functions are of "get" type and allow to communicate information about the onchain database to the app. They return the size of the map, the Boolean associated with a hash, and the information associated with a hash, respectively. The other three functions manage database entries, respectively providing the addition, deletion, and comparison of entries. The addition function verifies prior inexistence of the entry in the database, indexes relevant information (if present in the parameters), adjusts the size of the map and returns a Boolean to indicate successful processing. The deletion function checks if the entry already exists and adjusts the size of the map if needed before returning a Boolean. Finally, the comparison function returns the Boolean associated with the hash given as a parameter, indicating whether it is indexed or not.

Please note that within this proof-of-concept, the burning (or deletion) of the token that was created alongside the inclusion of the entry in the database does not occur. Also, the addition and deletion functions can only be called by the address that deployed the Smart Contract. If a use case requires multiple addresses to call the Smart Contract, a whitelist can replace the "only deployer" approach.

4. Experimental Illustration

Our experiments ran on two blockchains: a 3-node, Hyperledger Besu EEA (Enterprise Ethereum Alliance)-compliant [18] PoA private blockchain deployed on an AWS server, and the Rinkeby Ethereum testnet through the Infura node cluster.

4.1. Fingerprinting Methods

Although the method used to identify content is the core of the application, the general architecture in Section 3.A is independent of it. The ins and outs and optimization of fingerprinting methods are out of the scope of this paper. The role of the fingerprinting method is twofold. First, being the first step of the process, it defines what the inputs are. Near copy detection has use cases using a variety of data formats (images, video, text, etc.) some of which might focus on semantic content whilst others could include metadata or instance data. Second, the near copy detection can only be as precise as the specific fingerprinting method permits. As opposed to having a universal solution, appropriately selecting a fingerprinting method on a case-by-case basis will yield the best results.

4.2. Use Cases and Parameters

The proof-of-concept is instantiated with two use cases. The first simulated a museum wary of multimedia content posted online being copied. We used a database comprised of sequences extracted from the virtual visit of six rooms offered by the Louvre Museum in Paris during the COVID-19 pandemic [19]. We used these images for strictly academic and non-commercial purposes and do not intend any infringement of the Louvre's IPR. Test videos were sampled to 1 frame per second, the fingerprints were computed according to [20] and were compared using a normalized correlation method.

The second use case constituted a more generic database identified using International Standard Content Codes (ISCC) [21] and a collection of twenty JPG images of various sizes taken from the mirflickr25k set as our database entries. We focused on the "Content Code" portion of ISCC and a database of images, but it could very well be used to compare metadata and instance information of text files. The codes were compared using Hamming's distance. Given that ISCC codes are short (between 13 and 55 characters), the hashing of the fingerprint is not necessary.

The thresholds used to detect near copies also depend on the use case. If the objective is only to detect very close copies of the content in the database, we would set our normalized correlation threshold close to 1, or our maximum Hamming distance very small (in the range of 0 – 3 bits). If we are more generally looking to detect the same semantic content after alteration, we would set our normalized correlation threshold between .6 and .8, or our maximum Hamming distance between 8 and 12. For our demonstrations with a goal of general detection, we used a threshold of 0.7 for the normalized correlation and a maximum Hamming distance of 10 for general detection purposes. For both use cases, the inputs we fed into the algorithm were altered versions of content held in the databases we subjected to standard image processing attacks, namely: conversion to black and white, brightness increases, cropping (50%), JPEG compression at a quality factor of $Q = 90$ and resizing to 600x400. Given that the detection performance solely relies on the specific fingerprinting method in use, and that the architecture put forward in this paper has no effect on the performances of said method, we will not dwell on them here. Extensive performance analysis for these respective methods are available in [19] and [20] and were corroborated by our tests.

4.3. Examples of Execution

We find ourselves in the first scenario where six image sequences are fingerprinted in the database and the Smart Contract has been previously deployed on

the Rinkeby testnet alongside the Token Contract. Fig. 3 shows the results of us giving one of the original videos as an input, whose fingerprint appears as is in the database, as well as a near-copy case. We altered the sequence of another original video by cropping the top and bottom 25 % of each image and increasing their luminosity before feeding it to the app as a new input. One of the images of the sequence is illustrated alongside the results of the app in Fig. 3.

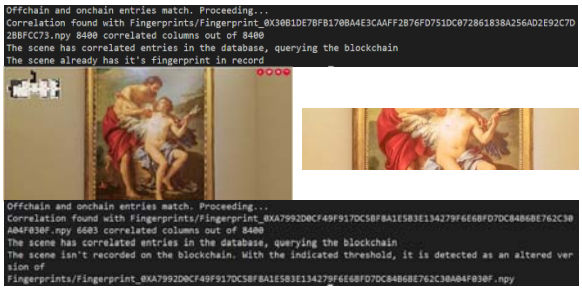


Fig. 3. A copy (top) and near-copy (bottom) sequence detection.

If a malicious actor were to gain access to the database and delete an entry from the records for their own entry to be perceived as original, the greenlight function would not permit the app to function, as shown in Fig. 4. The same thing cannot happen with the verification database, as is appears onchcain and is subsequently unalterable. We then compiled a random modified sequence of images from different videos to create a sequence that has no significance to the original database. If we run the app using this sequence as an input, we get a prompt illustrated in Fig. 4. If the operator wishes to add this input to the database, they may accept this prompt which transactions the Smart Contract and the Token Contract. The ensuing transactions are shown in Fig. 4 and may be cross checked using a Rinkeby explorer (such as rinkeby.etherscan.io). The ERC721 token created for the occasion is found in the deployer wallet and a subsequent execution of the app using this input yields the same result as the first image of Fig. 3.

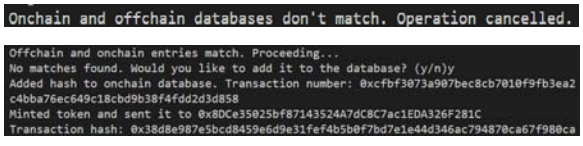


Fig. 4. A greenlight function failure (top) and the successful addition of a new entry in the database and its subsequent tokenization (bottom).

The Smart Contract and Token Contract we used for this test can respectively be found at 0xA75f207314C85F4891657a2D4f73b19b88b21dc9 and 0xAAFFfFF06a971b57ca87953010135d771B91f965.

4.4. Resource Usage

This architecture's objective is not to enable fast nor efficient processing of information, but to provide reliable and verifiable data integrity. The results we provide here must be taken with a grain of salt, as execution times and gas costs will vary significantly depending on the blockchain in context as well as the network traffic at the time of execution. The detail of the initial deployment of the onchain assets can be found in Fig. 5. It shows single block deployments (12 s) of the Smart Contract and Token Contract, respectively using 15.24 % and 61.45 % of gas limits (set by default at 4.5 million), for a total of 0.03451321ETH (for a gas price of 10 Gwei). Use cases not needing the tokenization of their assets can get away with a single lightweight Smart Contract.

Populating our database with 6 entries cost us 0.000114ETH and the tokenization 0.000226 ETH per entry (for a gas price of 1.5 Gwei). Although this step is the biggest resource sink in the entire process, it stays in the scope of a blockchain application. The gas and time spent scales linearly with the number of entries, so even databases of a few hundred to a few thousand entries could comfortably be processed in the span of a couple of hours.

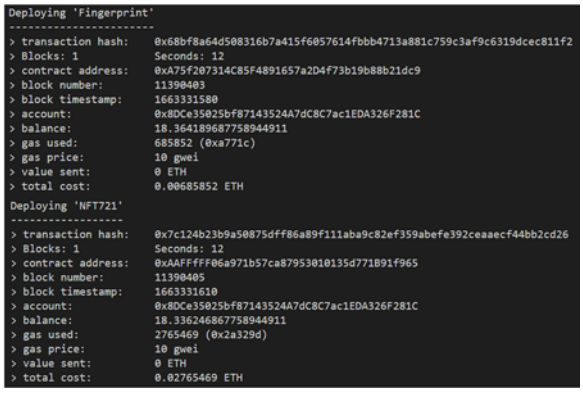


Fig. 5. Deployment figures to the Smart Contract (top) and Token Contract (bottom).

After the setup and for general use, the Smart Contract is only invoked at two specific moments. This leaves most of the processing up to the faster and more efficient app. The first use is the greenlight function. This instance does not constitute a transaction as it does not write any information on the blockchain. This call does not cost gas and is not limited by slow block rates. In our experience and with our testing setup, this step never added more than 2 seconds of execution to the processing of an input. The second use is in case a new entry is to be added to the database. This step is essentially the initial setup brought to the scale of a single entry. In fact, the transaction we executed to illustrate Subsection 4 cost the same amount of 0.000114ETH. As was our aim, this localized and minimal use of blockchain enables us to avoid long processing times and excessive gas fees.

5. Conclusion

This paper advances an architectural framework making it possible for multimedia tracking fingerprinting applications to be backboned by blockchain, while suffering minimally from excessive resource usage. With this design, the system is as safe as the app itself and its communication to the blockchain. A user has the freedom to slot in their preferred technological blocks to adapt this idea to specific use cases. Future work should investigate creating the Smart and Token Contracts for other development blockchains, ensuring the security of the links between the app and databases, and integrating this architecture into larger projects where intellectual property and content originality play important roles.

Acknowledgements

We acknowledge Titusz Pan and Sebastian Posth from the ISCC foundation for out fruitful exchange leading to the integration of ISCC into this methodology. We acknowledge Najah Naffah from Blockchain Secure for his insights in applicative blockchain environments.

References

[1]. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Cryptography Mailing list at https://metzdowd.com

[2]. Grand View Research portal (https://www.grandviewresearch.com/industry-analysis/non-fungible-token-market-report)

[3]. DappRadar Web portal (https://dappradar.com/nft/marketplaces)

[4]. Opensea Twitter post (https://twitter.com/opensea/status/1486843204062236676)

[5]. D. Das, P. Bose, N. Ruaro, C. Kruegel, G. Vigna, Understanding Security Issues in the NFT Ecosystem, in *Proceedings of the ACM Conference on Computer and Communications Security (CCS),* 2022.

[6]. N. Szabo, Formalizing and Securing Relationships on Public Networks, *First Monday,* Volume 2, Issue 9, 1997.

[7]. V. Buterin, A Next-Generation Smart Contract and Decentralized Application Platform, *Ethereum White Paper,* 2014.

[8]. V. Dhillon, D. Metcalf, M. Hooper, Blockchain Enabled Applications, *Springer*, 2017.

[9]. T. Hewa, Y. Hu, M. Liyanage, S. Kanhare, M. Ylianttila, Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research, *IEEE Access*, 9, 2021, pp. 87643 - 87662.

[10]. X. Li, P. Russell, C. Mladin, C. Wang, Blockchain-Enabled Applications in Next-Generation Wireless Systems: Challenges and Opportunities, *IEEE Wireless Communications*, Vol. 28, No. 2, April 2021, pp. 86-95.

[11]. R. Li, Fingerprint-related chaotic image encryption scheme based on blockchain framework, *Multimedia Tools and Applications,* Vol. 80, Issue 20, 2021, pp. 30583–30603.

[12]. F. Frattolillo, A Watermarking Protocol Based on Blockchain, *Applied Sciences*, Volume 10, Issue 21, 2021, 7746.

[13]. A. Qureshi, D. Megías Jiménez, Blockchain-Based Multimedia Content Protection: Review and Open Challenges, *Applied Sciences*, Volume 11, Issue 1, 2021, p. 1.

[14]. L. Tseng, X. Yao, S. Otoum et al., Blockchain-based database in an IoT environment: challenges, opportunities, and analysis, *Cluster Computing*, Vol. 25, 2020, pp. 2203-2221.

[15]. X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability, in *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, 2017*,* pp. 468-477.

[16]. M. Allouche, M. Ljubojevic, M. Mitrea, Visual document tracking and blockchain technologies in mobile world, in *Proceedings of the IS&T International Symposium on Electronic Imaging 2021, Imaging and Multimedia Analytics in a Web and Mobile World 2021,* Online, France, January 2021, pp.279:1-279:7.

[17]. W. Entriken, D. Shirley, J. Evans, N. Sachs, EIP-721: Non-Fungible Token Standard, *Ethereum Improvement Proposals*, No. 721, January 2018.

[18]. Ethereum Entrprise Alliance Specification portal (https://entethalliance.org/technical-specifications/)

[19]. Le Lovre online tours portal (https://www.louvre.fr/en/online-tours)

[20]. A. Garboan, M. Mitrea, Live camera recording robust video fingerprinting, *Multimedia Systems*, 22, 2016, pp. 229–243.

[21]. International Standard Content Code Foundation portal (https://iscc.foundation/iscc/)

(034)

Challenges of Blockchain Technology Adoption for Document Authentication in Universities: A Systematic Literature Review

A. Aman [1], N. S. Mohd. Satar [1*], Y. Adnan [1] and A. H. Morshidi [2]
[1] Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia
[2] Universiti Malaysia Sabah, Jln UMS, 88400 Kota Kinabalu, Sabah, Malaysia
Tel.: + 60122848697, fax: +60389256732
*E-mail: nurhizam@ukm.edu.my

Summary: Despite the fact that blockchain technology has several advantages for the higher education sector, universities have not yet embraced it broadly for document authentication. Therefore, this research aims to systematically review what obstacles and challenges deter universities from integrating blockchain with their document verification processes rather than offering more reasons to utilise blockchain technology. This systematic literature review followed the Preferred Reporting Items for Systematic Review and Meta-Analyses (PRISMA) guidelines. Our conclusions are based on 16 studies that have been carefully chosen and debated using the Technology, Organization, and Environment (TOE) framework and the Diffusion of Innovation (DOI) theory. Finally, the latest blockchain-based document verification application from the National University of Malaysia (UKM) is presented as an example of how this research will help universities figure out how useful blockchain technology is and pave the way for its wide use in the higher education sector.

Keywords: Blockchain, Document verification, Constraints, Universities, Malaysia, SLR.

1. Introduction

Blockchain technology is a technological advancement that is getting more complex every day, and they are being made to make life easier for people in every way [3]. However, the rapid rise of technology impacts increasingly sophisticated security, such as data theft or data falsification by internet data transfer that unauthorised individuals can alter [1, 4]. Standard applications of blockchain technology include the issuance and verification of academic credentials such as degrees, transcripts, competencies, achievements, and professional abilities that employers may confirm worldwide [2, 4]. As a result of blockchain technology's ability to speed up the certification process, the amount of time an employer needs to spend verifying academic results is reduced. It is helpful to the education industry because it provides a safe platform for transferring student data, which builds confidence, reduces costs, and increases transparency [2, 5].

2. Research Problem

The academic world has long struggled with the problem of fake document and credentials. Despite all of the advantages and opportunities that blockchain presents for universities, for example, because it is still in its infant phases of development, it is still considered a young and immature technology. In addition, there is apprehension regarding the challenges that may arise while integrating institutions' traditional information systems with blockchain technology [1, 2]. However, the obstacles colleges and universities may face in adopting blockchain technology have not yet been thoroughly examined [1, 2]. This study attempts to fill that gap in the research. Therefore, to fill in the gaps left by previous studies, this systematic review focuses on understanding what prevents universities from integrating blockchain technology with their document verification processes rather than offering more reasons to adopt the technology with the following research question.

3. Research Question

For a systematic review to be successful, it is vital to develop research questions that will be used to direct the search and extraction procedures. The first step in finding them is to locate studies pertinent to the research concerns that need to be addressed [4, 5]. The initial step for researchers is to identify the search phrases used. The research question was developed from two sources: first, ideas from past investigations by [6]. Issues were covered in each article. This approach made it easier for the authors to frame the study's principal research question, namely, what are the challenges of blockchain technology adoption in document authentication by universities?

4. Methods

The Preferred Reporting Items for Systematic Review and Meta-Analyses (PRISMA) were used to guide the conduct of this systematic literature review [6]. This SLR was aligned with the computer science domain using Kitchenham's in [6] standard guidelines. The methodologies used for this SLR are described in this methodology section. It entails developing research questions, establishing eligibility standards for choosing the most pertinent articles and conference papers, as well as knowledge sources, paper searches, study collecting, and data extraction, sources of information, study collections, and data extraction.

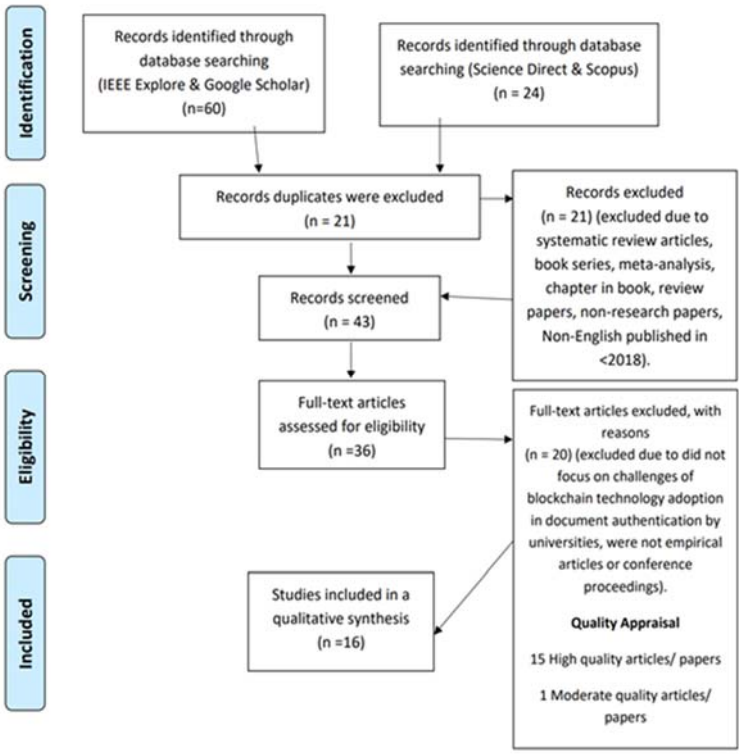


Fig. 1. PRISMA Flow Diagram [7].

5. Result and Discussion

The purpose of this SLR I is to review the challenges of blockchain technology adoption in document authentication by universities. Sixteen articles have been selected for the systematic review.

The emphasis is on the rules and laws in various nations for protecting personal information, which universities planning to embrace blockchain should take into account. They have outlined several obstacles to utilising blockchain technology for education, including data scarcity, scalability issues, cost issues, immutability, creating boundaries, trust issues, and the deterioration of traditional university certificates [2-4] Adopting blockchain technology comprises infrastructure costs, costs associated with managing large amounts of data, time costs related to sluggish transactions, and processing power costs. Every time new features were added, additional costs arose. Data leakage that could turn into a security concern can be caused by frequent upgrades and the addition of new functionality [4, 5].

Taking these challenges into consideration, Universiti Kebangsaan Malaysia, a prominent public university in Malaysia has embarked on an inclusive Blockchain Sandbox @ UKM HRMIS project. This initiative uses blockchain technology to reduce the issuance of bogus and fraudulent certificates. The UKM Certification Authentication Platform offers an Ethereum-based Blockchain solution to address the aforementioned problems. This solution includes employing a multi-signature scheme to improve certificate authentication; implementing a secure federated identification to ensure the identity of the university issuing the certificate; and enacting a safe revocation mechanism. The system that incorporates the aforementioned solutions will be designed and put into place as part of the project.

6. Conclusions

In a nutshell, this systematic review is seen to be an invaluable resource for academics and professionals trying to comprehend the challenges to blockchain adoption for document authentication in universities. Although blockchain technology has a number of advantages, its use in higher education is still in its early stages because of many difficulties. The results of the current study show that a number of obstacles have prevented blockchain technology from being widely used in universities for document authentication.

Acknowledgements

Funding: This research received funding from Univerisiti Kebangsaan Malaysia.

References

[1]. Haveri, P., Rashmi, U. B., Narayan, D. G., Nagaratna, K., Shivaraj, K., EduBlock: Securing Educational Documents using Blockchain Technology, in *Proceedings of the 11th International Conference on*

Computing, Communication and Networking Technologies (ICCCNT), 2020, July, pp. 1–7.

[2]. Kanan, T., Obaidat, A. T., & Al-Lahham, M., SmartCert blockchain imperative for educational certificates, in *Proceedings of the IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT),* April, 2019, pp. 629–633.

[3]. Saleh, O. S., Ghazali, O., & Idris, N. B., A New Decentralized Certification Verification Privacy Control Protocol, in *Proceedings of the 3rd International Cyber Resilience Conference (CRC),* January 2021, pp. 1–6.

[4]. Salau, O., Adeshina, S. A., Secure Document Verification System Using Blockchain, in *Proceedings of the 1st International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS),* 2021, July, pp. 1–7.

[5]. A. Mohammad and S. Vargas, Barriers affecting Higher Education Institutions' adoption of blockchain technology: A qualitative study, *Informatics (MDPI),* Vol. 9, No. 3, 2022, p. 64.

[6]. M. Shaffril, H. A. Samsuddin, and S. F. Samah, The ABC of systematic literature review: The basic methodological guidance for beginners, *Quality & Quantity*, Vol. 55, No. 4, 2021, pp. 1319–1346.

[7]. D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, Reprint-preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement, *Physical Therapy*, Vol. 89, No. 9, 2009, pp. 873–880.

(035)

Blockchain Technology Solutions for Small and Medium-Sized Enterprises Challenges

A. Amanollahnejadkalkhouran, B. Batiz-Lazo and C. Ochie
University of Northumbria, Department of Entrepreneurship, Innovation and Strategy, Newcastle, UK
E-mail: abolfazl.amanollahnejadkalkhouran@northumbria.ac.uk

Summary: Small and medium-sized enterprises (SMEs) are considered the backbone of most economies, and their survival is vital for a healthy society. SMEs must be strengthened in order to overcome current economic challenges. In particular, market friction impedes the exchange of assets for all businesses, and SMEs are no exception. The recent introduction of blockchain technology (BCT) is considered to be able to eliminate, or at least significantly reduce, various types of market friction that impact businesses in different industries. In the case of small businesses, there are several solutions that address information, interaction and innovation challenges. The study proposes that SMEs' key challenges determine their adoption of BCT. Cost-effectiveness, internalization, scalability, network size, information asymmetry and financing have been identified in the literature as reflecting the main challenges of SMEs. Given the arena's early stages of development, the paper relies on a qualitative analysis including SMEs literature and extant literature of BCT.

Keywords: Blockchain technology, Cost-effectiveness internalization, Scalability, Network size, Information asymmetry, and financing.

1. Introduction

The appearance of blockchain technology (BCT) as a trend in the information technology (IT) industry has attracted extensive consideration from national development authorities, practitioners, academics and researchers [14]. The notion of BCT has spread universally following the appearance of Bitcoin [30]. Since then, several blockchain based applications have been advanced [13] [40] generating opportunities for alternative enterprise models [10] [21] and enhanced performance [24]. BCT utilizes a decentralized network of nodes or participants to execute transactions [8] which are stored, verified and validated by consensus [21] [23]. BCT are developing rapidly in both the private and public sectors in numerous developed as well as developing nations. [15] [9]. It is estimated that 10% of the globe's gross domestic product will be saved and stored on BCT by 2027 [41]. In the last few years, BCT has been used in an extensive array of settings, such as healthcare [1] open manufacturing, and real estate [38].

In spite of growing relevance of BCT for both research and practice, very little is known about how and why SMEs are adopting and implementing BCT. Prior studies concentrated mostly on technical matters of BCT [36] or in large and multinational businesses [10]. This article conceptualizes the appropriateness of BCT for SMEs within six factors. These factors reflect the major challenges of SMEs when competing with large companies and which have been stressed in the existing literature.

2. Critical Literature Review

Blockchain technology in the business context is a new area of research [14]. Some studies take a broader perspective, and examine the difficulties and consequences of using BCT in firm administration [34]. Such studies provide academics and practitioners with an overview of how this new-fangled technology can be used either in research or business [34]. Another section of the literature studies blockchains from the perspective of business development administration. These studies highlight the potential advantages of shared ledgers for companies [14]. BCT provides a data-aware procedure for businesses that are looking for new ways to collaborate [20]. Distributed ledgers help businesses to track corporate procedures, while each task is performed by adopting a space-optimized data structure [34]. Moreover, BCT ensure transparency for investors in a business [2]. As no-one owns a BCT solution, they also provide data traceability, through the assessment of BCT records [26] [31]. On the other hand, some studies have looked at negative aspects, such as data storage and computation costs [2]. While all of the cited studies suggest that BCT is a valuable instrument for business solutions, its suitability for SMEs has not been considered.

Several theoretical frameworks – for example the Technology Acceptance Model [25] the United Theory of Acceptance Model [32] and the Technology-Organisation-Environment framework [40] have been developed to describe the adoption of technological innovations in businesses, and a few empirical studies have focused on the use of these models in SMEs [40]. These studies have identified some of the reasons for unsuccessful IT application in SMEs, and slow uptake. Firstly, many SMEs (at both managerial and non-managerial level) do not understand how to use new technologies. Secondly, there are many misconceptions about technology usage. And, finally, SMEs often lack an IT strategy, have few IT skills, and lack access to capital resources [40].

To overcome knowledge erosion, and optimally manage knowledge resources, SMEs must rely upon well-organized knowledge management systems.

Knowledge is an increasingly important strategic priority for all firms, regardless of size. SMEs that can find ways to manage knowledge are likely to enjoy a competitive advantage [18]. Knowledge management encompasses many organizational processes and structures, and the adoption of innovative technologies such as BCT is a key element [18].

This research addresses gaps in the literature in relation to: the innovative use of blockchain technology in SMEs; the factors affecting their use of blockchain technology; the effect of the innovative features of blockchain technology on the challenges faced by SMEs.

2.1. What Makes a Blockchain Technology Suitable for Business?

Blockchain technology for business is a private, permissioned network with recognized identities and without the demand for cryptocurrencies. To more understand how a BCT for enterprise works, and to gain its possible for transforming enterprise networks, It is needed to recognize the four important components of BCT for enterprise, shown in Fig. 1.

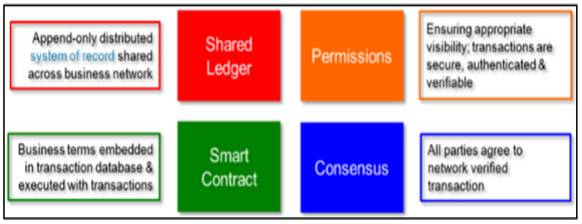


Fig. 1. Four key concepts of blockchain for business

Shared ledger

A shared ledger is an immutable record of all transactions on the business network, a record that all business network members can access. With a shared ledger, transactions are kept and recorded only once, removing the duplication of effort that's distinctive of conventional business networks [42]. BCT move the paradigm from data held by a single owner to a shared lifetime history of a transaction or asset [42]. Members of network can validate and authorize transactions and confirm ownership and identities without the requirement for third-party intermediaries [27]. All related data can be shared with others based on their access and roles privileges [27].

Permissions

With a permissioned BCT, each member of network has an exclusive identity, which qualifies the use of policies to restrict access to transaction details and network participation [27]. Permissioned BCT are also more efficient at controlling the consistency of the information that gets added to the BCT [27]. With the capability to limit access to transaction details, more transaction detail can be kept and stored in BCT, and members of network can specify the transaction data they're willing to permit others to view (With a public BCT, the level of transaction detail may be restricted to protect anonymity and confidentiality) [27]. BCT for enterprise network can be set up as a members-only club, where every member of network has an exclusive identity, and members must meet certain principles to conduct transactions [27]. Members of network can conduct transactions confident that the individual they're dealing with is who she/he claims to be [27].

Consensus

In a network where members are trusted and known, transactions can be committed and verified to the ledger through several means of consensus or agreement [28]. BCT adopts consensus algorithms to authorize and validate transactions. Members of business network can conduct business at a pace that is more in-line with the pace of their decisions [28].

Smart contracts

A smart contract is a set of rules or an agreement that rule a transaction; it's stored and kept on the BCT and is executed automatically as part of a business transaction [5]. These contracts may have several contractual sections that could be made fully or partially self-enforcing, self-executing, or both [5]. Their aim is to offer security superior to conventional contract law while decreasing the delays and costs related to conventional contracts [33].

2.2. Types of Market Friction

Several forms of market friction influence various industries in dissimilar ways. This part explains about the common forms of market friction that BCT is able of easing.

Information frictions

These frictions arise from the following restrictions:

Imperfect information: Members of networks in a transaction don't have access to the similar data, giving one side an unfair benefit. Data may besides be inconsistent or incorrect, leading to deficient delays or decisions while reconciling it [3].

Inaccessible information: The possible value of rich information is importantly limited by the technical challenges and barriers of analyzing, storing, sharing and processing it. Consequently, much data is not collected or remains inaccessible [3].

Information risks: Technological hazards to information, from identity theft to cybercrime and privacy concerns to hacking are on the growth. These incur rising expenses, as well as damage to brand standings and reputations [3].

Interaction frictions

These frictions happen when either the expense of transaction is too high or the degree of separation between parties is too enormous [17]. Transactions that take days and are expensive to handle via intermediaries are major candidates for disruption by competitors [17]. BCT's peer-to-peer architecture can

often decrease the number of parties or interactions demanded to execute a transaction, therefore decreasing the number of possible sources of interaction friction [16].

Innovation frictions

These frictions are external, internal or any conditions that compromise a business's capability to respond to marketplace changes, for example the following:

Institutional inertia: legacy systems and Internal bureaucracy accompanied by the human resistance to change can hinder a business's responsiveness [35].

Restrictive regulations: Whereas regulations may be needed to control industry behavior, they have the unexpected result of introducing delays and costs [35].

Invisible threats: Novel competitive enterprise models made probable by new technologies are threats for which businesses can't plan. For several, this increasing uncertainty will disrupt sustained business success. Both SMEs and larger ones will try innovative approaches, and however many will fail, some will redefine whole industries [35].

2.3. Blockchain Technology in SMEs Context

This study explores the consequences of the adoption of BCT by SMEs as a function of six factors. It has been identified in the literature as reflecting the key challenges SMEs face when in competition with larger businesses. In brief, they are: cost-effectiveness (cost reduction) [40] internalization [13, 14] network size [4] information asymmetry [39] and financing [6] (Fig. 2).

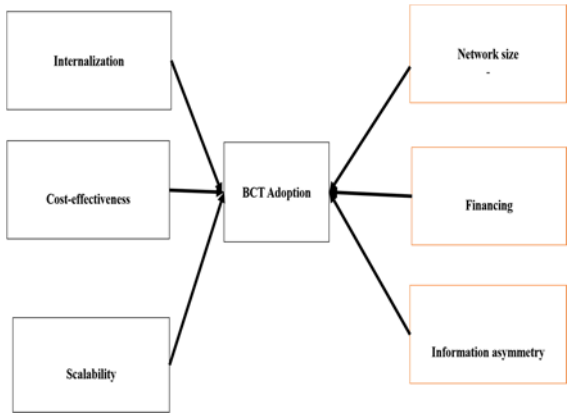


Fig. 2. SMEs' key challenges impact on BCT adoption.

2.3.1. Cost-effectiveness

Despite this progress, there is lack of studies that consider the impact of SME adoption of BCT on these factors, in order to provide insight into their effects on improving SME performance. The capacity of blockchain-driven SMEs can guarantee information security, tracking, and validity, along with intelligent contractual partnerships for a trustless world [33].

SMEs suffer frequently from resource constraints and restrictions [37]. One of the solutions BCT offers for SMEs is it eliminates intermediary for value transaction [33]. For SMEs, this intermediary might be a bank or a broker who secures the value transaction between trading counterpart and SMEs [33]. Relying on an intermediary inevitably enhances transaction expenses due to the fees the intermediary takes [29]. By using BCT, the SMEs can decrease their transaction expenses. These reductions enable for more effective practices, for instance the cost of verification reduction can have an instant influence on SMEs' business procedures [12].

2.3.2 Internalization

Another challenge of SMEs to increase their share in global markets is internationalization [22]. The concern of the loss of resources and capitals makes SMEs hesitate to do business with actors who have no credible and available trading record. This may cause lose the prospect of implementation of a possibly profitable business for small businesses [22]. BCT can benefits and helps SMEs shaped a reliable partnership between all parties in worldwide operations [33].

In this regard, smart contracts offer an opportunity for SMEs to do business and trade with untrusted parties [33]. It generates a business platform where peers do not require to trust each other. They can make secure value transaction even they have no former trading record [33]. The SME's adopting smart contracts can set random circumstances to execute operation and on condition that peers fulfil the fixed conditions, these contracts autonomously execute value transaction [27].

2.3.3. Scalability

Scalability is another challenge that should be considered to decide the suitability of BCT [34]. The higher business transaction speed might be a vital expectancy for SMEs while make decision to adopt BCT. For example, a speedy transaction might be central for an SME to make probable a fast payment system [34].

2.3.4. Network Size

The key benefit of BCT is it removes the dependence of peers to a central authority [17]. Its decentralized nature enhances the worth of network effect [17]. The possible advantages of BCT enhances as long as the size of the network grows [11]. Consequently, it becomes stronger to the outside attacks as it grows [7].

2.3.5. Financing

A commonly raised challenge of SMEs to understand their ambitions is their dearth of or access to financing [22]. In that sense, BCT provides SMEs a fundraising opportunity so-called Initial Coin

Offerings [22]. In an Initial Coin Offerings, the SME who possesses a project generates a certain amount of digital token and sells it to the possible investors [22]. These stakeholders buy these tokens in exchange for a service offered by the SME or growing demand on the token in crypto marketplaces that brings higher net profits [27]. This win-win state qualifies SMEs to acquire the needed funding, and it offers higher net profits to their stakeholders [27].

2.3.6 Information Asymmetry

The root cause of the SMEs financing challenges lies in the thoughtful information asymmetry that exists between financial organizations and SMEs [22]. Asymmetric information means that one side has access to critical information for decision making, while the other party is dearth of the appropriate information, or the information is no more than the other side has [19]. BCT ensures that all participants have access to all the data exchanged between them in the business network [17].

3. Conclusions

The interest over BCT in current years draws a promising picture that BCT can be a solution to numerous problems of small businesses. It may aid SMEs in various sectors and industries [11]. In theory, these statements have convincing points to overcome the mentioned challenges. Nevertheless, BCT is still in an early stage and a few years are demanded to see feasible applications of BCT in the SMEs context. It is recommended that SMEs who are keen on BCT and its application should carefully assess the challenges of BCT cynically and when they are completely sure, then, they should adopt and use it. They should also consider that those businesses who adopt and use BCT first will have a pioneering edge over their competitors.

References

[1]. Agbo, C. C., Mahmoud, Q. H. and Eklund, J. M, Blockchain Technology in Healthcare: A Systematic Review, *Healthcare,* 7, 2, 2019, pp. 56.

[2]. S. AhluwaliaaRaj V. Mahtob. M. Guerrero, Blockchain technology and startup financing: A transaction cost economics perspective, *Technological Forecasting and Social Change,* 151, 2020, 119854.

[3]. T. Allen, Information frictions in trade, *Econometrica*, Vol. 82, No. 6, November, 2014, pp. 2041–2083.

[4]. A. Amanollah Nejad Kalkhouran, B. Hossein Nezhad Nedaei. S. Abdul Rasid, S, The indirect effect of strategic management accounting in the relationship between CEO characteristics and their networking activities, and company performance, *Journal of Accounting & Organizational Change,* 13, 4, 2017, pp. 471-491.

[5]. S. Balasubramanian, V. Shukla, J. S. Sethi, N. Islam, R. Saloum, A readiness assessment framework for Blockchain adoption: a healthcare case study, *Technological Forecasting and Social Change*, 165, 2021, p. 120536.

[6]. S. Bakhtiari. Breunig, R., Magnani, Zhang, J, Financial Constraints and Small and Medium Enterprises: A Review, *The IZA Research, Discussion Paper Series,* 2020.

[7]. N. Bauerle, What is the Difference between Public and Permissioned Blockchains? 2017, Accessed 14th July 2018. https://www.coindesk.com/information/what-is-the-difference-betweenopen-and-permissioned-blockchains/

[8]. R. Beck, 2018, Beyond bitcoin: the rise of Blockchain world, *Computer,* 51, 2, pp. 54-58.

[9]. J. Berryhill, Bourgery, T. and Hanson, A, Blockchains unchained: blockchain technology and its use in the public sector, *OECD Working Papers on Public Governance*, No. 28, 2018, p. 53.

[10]. E. Bracci, Tallaki, M., Ievoli, R. and Diplotti, S., Knowledge, diffusion and interest in blockchain technology in SMEs, *Journal of Knowledge Management,* 26, 52022, pp. 1386-1407.

[11]. B. Carson, Romanelli, G., Walsh, P., Zhumaev, A, 2018, Blockchain beyond the hype: What is the strategic business value? 2018, Accessed 15th July 2018. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value

[12]. C. Catalini, Gans, S., Some Simple Economics of the Blockchain, Rotman School of Management Working, *MIT Sloan,* No. 5191-16, April 20, 2019, Paper No. 2874598.

[13]. Y. Chen, Blockchain tokens and the potential democratization of entrepreneurship and innovation, *Business Horizons*, Vol. 61, No. 4, 2018, pp. 567-575.

[14]. T. Clohessy. T. Acton, Investigating the influence of organizational factors on blockchain adoption, *Industrial Management & Data Systems,* 119, 7, 2019, pp. 1457-1491.

[15]. I. Giotopoulos. Kontolaimou, A., Korra, K. and Tsakanika, A, What drives ICT adoption by SMEs? Evidence from a large-scale survey in Greece, *Journal of Business Research,* 81, 2017, pp. 60-69.

[16]. M. Gupta, Blockchain, *IBM Limited Edition*, 2017.

[17]. L. Hashimy. Treiblmaier, H. and Jain, G, Distributed ledger technology as a catalyst for open innovation adoption among small and medium-sized enterprises, *The Journal of High Technology Management Research,* 32, 1, 2021, pp. 100405.

[18]. Hock-Doepgen, M. Thomas Clauss, Sascha Kraus, Cheng-Feng Cheng, Knowledge management capabilities and organizational risk-taking for business model innovation in SMEs, *Journal of Business Research,* Vol. 130, June 2021, pp. 683-697.

[19]. C. Huan, Y. When, Z. Liu, Analysis on Financing Difficulties for SMEs due to Asymmetric Information, *Global Disclosure of Economics and Business*, Vol. 3, 2, 2014, pp. 28-31.

[20]. R. Hull, Batra, V. S., Chen, Y. M., Deutsch, A., Heath III, F. F. T., Vianu, V, Towards a Shared Ledger Business Collaboration Language Based on Data-Aware Processes. In: Q. Sheng, E. Stroulia, S. Tata & S. Bhiri (Eds.), Service-Oriented Computing, *Springer,* 2016, pp. 18-36.

[21]. M. Iansiti. Lakhani, K. R, The truth about blockchain, *Harvard Business Review,* 95, 1, 2017, pp. 118-127.

[22]. E. Ilbiz. S. Durst, The Appropriation of Blockchain for Small and Medium-sized Enterprises, *Journal of Innovation Management*, 7, 1, 2019, pp. 26-45.

[23]. Y. Kano, Nakajima, T, A novel approach to solve a mining work centralization problem in blockchain technologies, *International Journal of Pervasive Computing and Communications*, Vol. 14, No. 1, 2018, pp. 15-32.

[24]. N. Kant, Blockchain: a strategic resource to attain and sustain competitive advantage, *International Journal of Innovation Science*, Vol. 13 No. 4, 2021, pp. 520-538.

[25]. S. Kamblea, A. Gunasekaranb. V. Kumarc. A. Belhadid. C. Forn, A machine learning based approach for predicting blockchain adoption in supply Chain, *Technological Forecasting and Social Change,* 163, 2021, 120465.

[26]. H. Kim, Laskowski, M, Towards an Ontolgy-Driven Blockchain Design for Supply Chain Provenance, *SSRN*, 2016, Accessed 28th July 2018, https://ssrn. com/abstract=2828369

[27]. D. Kimani. K. Adams. R. AttahBoakye. S. Ullah. J. Frecknall. Hughes. J. Kim, Blockchain, business and the fourth industrial revolution: Whence, whither, wherefore and how?, *Technological Forecasting and Social Change,* Vol. 161, December 2020, 120254.

[28]. B. Lewis, De Beers Turns to Blockchain to Guarantee Diamond Purity, available at https://www.reuters. com/article/us-anglo-debeers-blockchain/de-beers-turns-to-blockchain-toguarantee-diamond-purity-idUSKBN1F51HV; retrieved April 26, 2018.

[29]. A. Madhok Tallman, S, Resources, Transactions and Rents: Managing Value Through Interfirm Collaborative Relationships, *Organization Science*, 9, 3, 1998, pp. 326-339.

[30]. S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, 2008, available at: www.Bitcoin.org/ bitcoin.pdf, accessed February 28, 2018.

[31]. J. Orji I. Kusi-Sarpong, S., Huang, S W. and Vazquez-Brust, D., Evaluating the factors that influence blockchain adoption in the freight logistics industry, *Transportation Research Part E: Logistics and Transportation Review,* 141, 2020, 102025.

[32]. M. Queiroz. S. Fosso Wamba, Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA, *International Journal of Information Management,* 46, 2019, pp. 70-82.

[33]. S. Rakshit, N. Lam, S. Mondala, T. Paul, Influence of blockchain technology in SME internationalization: Evidence from high-tech SMEs in India, *Technovation,* 115, 2022, 102518.

[34]. T. Saheb, F. H. Mamaghani, Exploring the barriers and organizational values of blockchain adoption in the banking industry, *The Journal of High Technology Management Research,* 32, 2, 2021, pp. 100417.

[35]. D. Schonthal and J. Euchner, Understanding Innovation Friction, *Research-Technology Management,* Vol. 65, Issue 4, 2022, pp. 11-17.

[36]. A. Tandon. Dhir, A., Islam, N. Mäntymäki, M, Blockchain in healthcare: a systematic literature review, synthesizing framework and future research agenda, *Computers in Industry*, Vol. 122, 2020, p. 103290.

[37]. J. Thong, Resource constraints and information systems implementation in Singaporean small businesses, *Omega,* 29, 2, 2001, pp. 143-156.

[38]. J. Veuger, Trust in a viable real estate economy with disruption and blockchain, *Facilities*, Vol. 36, Nos 1/2, 2018, pp. 103-120.

[39]. R. Wang. Lin, Z. and Luo, H, Blockchain, bank credit and SME financing, *Quality & Quantity*, Vol. 53, No. 3, 2019, pp. 1127-1140.

[40]. L. W. Wong. Leong, L., Hew, J., Tan, G. and Ooi, K, Time to seize the digital evolution: Adoption of blockchain in operations and supply chain management among Malaysian SMEs, *International Journal of Information Management*, 52, 2020, 101997.

[41]. Deep shift: technology tipping points and societal impact, Survey Report, *World Economic Forum*, 2015.

[42]. Z. Zheng, Xie, S., Dai, H., Chen, X. and Wang, H, An overview of blockchain technology: Architecture, consensus, and future trends', in *Proceedings of the 2017 IEEE BigData Congress*, Honolulu, Hawaii, USA, 2017, pp. 557–564.

(036)

Key-pair Generation using Fingerprint-based Seed in Blockchain Systems

M. Fiore, F. Carrozzino, M. Mongiello and F. Nocera
Department of Electrical & Information Engineering, Polytechnic University of Bari, Bari, Italy
E-mail: name.surname@poliba.it

Summary: Blockchain technologies use key-pairs to sign and verify transactions. Users in a Blockchain system are anonymous and can create multiple wallets, but this can lead to problems such as the sybil attack, a kind of network attack in which a person tries to impersonate multiple identities to take over the network. This paper tries to model a sybil resistant Blockchain thus ensuring anonymity for users. After some preliminary steps such as feature extraction and hashing, biometric information is used to generate a key-pair that will be linked to one person. Even though information is related to a given person, her identity can not be retrieved. Biometrics can limit each user on the platform to have at most 10 wallets, but further considerations can be done to limit that number.

Keywords: Blockchain, Authentication, Fingerprint, Principal component analysis, Key-pair generation.

1. Introduction

The arrival of Blockchain technology constitutes a paradigm shift in the conception of databases, that now are conceived as decentralized and distributed. Blockchain carries lots of characteristics: it is anonymous and it uses wallets with key-pairs for authentication and signing processes. A user private key is used for signing transactions and a public key is used to verify their authenticity.

Blockchain also has some limitations and open challenges: the one analysed in this paper regards sybil resilience, that is, every user can activate multiple nodes to create multiple identities - wallets - at the same time. The possibility to operate more than one identity on a single entity could carry various attacks, such as the 51% attack or multiple fake reviews on e-commerce platforms. Online businesses can be damaged from frauds and sybil attacks make fraud detection hard to accomplish [1].

This paper proposes a new method to overcome the sybil attack using user fingerprints. In this way, each person in the world can have a limited number of wallets - one for each finger. To still guarantee anonymity, each fingerprint will go through a feature extraction and a hash function, so it would be impossible to go back from a hash value to the initial string. The main contribution of this proposal is that fingerprint data will not be collected but only used to generate a key-pair to limit user wallets, making the seed usage more scalable and more secure.

Section 2 proposes a background of the fundamental technologies used in the Blockchain-based architecture: fingerprint authentication and feature extraction. Section 3 analyses some related works and their pros and cons, Section 4 shows the proposed architecture and a basic workflow, finally Section 5 concludes the paper and indicates some future developments.

2. Background

2.1. Fingerprint Authentication

Fingerprint authentication is a form of biometric technology implemented in a system that allows to verify the identity of a user analyzing his fingerprint through image processing and grant him the access to the system. A fingerprint reader is needed to scan the user's fingerprint.

2.2. Feature Extraction

In image processing, feature extraction is a technique that, given a large set of data, is able to extract a smaller set of non-redundant data, so it allows to reduce the dimension of the data set.

There are several feature extraction techniques. A popular one is the Principal Component Analysis (PCA) that reduces the dimensionality of a data set preserving as much variability as possible, finding new variables that are linear functions of those in the original data set [2].

3. Related Work

In this section, an overview of related work regarding unique authentication in Blockchain is proposed. The idea of using a fingerprint-based authentication in a Blockchain system has been already showed in other publications. Various approaches have been applied in order to take advantage of the inner characteristics of the Blockchain joined to the fingerprint authentication. A simple but efficient idea is to use the Blockchain for secure and immutable storage of biometric data [3], storing encrypted fingerprint templates to avoid data deletion and manipulation [4]. Both these approaches do not rely on generating unique key-pairs.

Practical applications have also been proposed; in order to guarantee the uniqueness of a voter, an electronic voting system has been implemented using Blockchain and fingerprint authentication [5]. In IoT field, it has been used to unlock doors using a smartphone to protect against tampering of users information [6]. These are validation processes but do not regard the signup process of the user.

None of these approaches aim to really limit the number of wallets per user without vanishing the anonymity characteristic of Blockchain systems.

4. Architecture

The functionality of the proposal is represented in Fig. 1.

The user scans his or her fingerprint in order to generate a new key-pair. A Principal Component Analysis is applied to the result of the scan to identify some characteristics of the fingerprint, then these characteristics are hashed using a secure hash function to ensure that the fingerprint information is not accessible by anyone. For security reasons, the system only hashes the fingerprint features and does not collect the whole fingerprint data.

The novelty introduced in this architecture is about the obtained hash value, indeed it is used as a seed to generate the key-pair, composed by a public key and a private key.

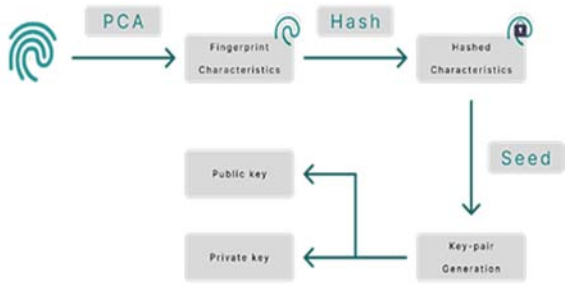


Fig. 1. Proposal architecture.

This kind of approach allows developers to design Blockchain-based platforms without the worry of sybil resilience, ensuring that every user can create a limited number of accounts – that is, one for each finger. Some approaches can be considered to further limit the number of wallets per user, for example recognizing the fingerprint and allowing the index finger only – 2 wallets per user.

5. Conclusions

There are several applications of the Blockchain technology, and in some cases it is mandatory to unambiguously identify the user to ensure that he or she does not create multiple wallets. Thanks to this biometrical approach, the proposed system is able to reduce the number of wallets binding their creation to user fingerprint data.

Differently from other approaches, several advantages can be obtained using the fingerprint data combined with the hash function in order to generate the seed for the key-pair generation. Since fingerprint data are not directly used for the authentication and they are not stored in the blockchain, the anonymity of the user is guaranteed.

Further studies will be done to understand how to further limit the number of wallets, for example scanning all 10 fingers, mixing their features to ensure anonymity, to get a wallet; another approach could be to identify only one finger per hand, limiting the number of wallets to 2 per user.

Acknowledgements

This work was funded by the TRACECOOP Research project (Italy) (B96G21000060005).

References

[1]. Y. Cai, D. Zhu, Fraud detections for online businesses: a perspective from blockchain technology, *Financial Innovation*, 2016, pp. 1-10.

[2]. I. T. Jolliffe, J. Cadima, Principal component analysis: a review and recent developments, *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374, 2065, 2016.

[3]. D. Pawade, et al., Implementation of fingerprint-based authentication system using blockchain, in Soft Computing and Signal Processing, *Springer*, Singapore, 2019, pp. 233-242.

[4]. M. A. Acquah, et al., Securing fingerprint template using Blockchain and distributed storage system, *Symmetry*, 12, 6, 2020, 951.

[5]. M. Ibrahim, et al. Electionblock: An electronic voting system using Blockchain and fingerprint authentication, in *Proceedings of the 18th IEEE International Conference on Software Architecture Companion (ICSA-C)*, 2021, pp. 123-129.

[6]. J. H. Huh, K. Seo, Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing, *The Journal of Supercomputing*, 2019, pp. 3123-3139.

(037)

Smart Card Based Offline Payment System for Central Bank Digital Currencies

Ali Doğan, Mustafa Takaoğlu, Taner Dursun and Ercan Ölçer
Informatics and Information Security Research Center, The Scientific and Technological Research Council of Türkiye, Kocaeli, Türkiye
E-mail: doganali@tubitak.gov.tr, mustafa.takaoglu@tubitak.gov.tr, taner.dursun@tubitak.gov.tr, ercan.olcer@tubitak.gov.tr

Summary: TÜBİTAK Offline Payment System (TOPS) is an offline payment method that has been proposed to be used in digital currency projects of central banks. There are various methods of offline payment solutions in the literature. Generally, solution proposals in which mobile phones are accepted as a trusted execution environment come to the fore. The method proposed by the researchers, prepared as a result of the joint work of E-Identity and Blockchain Laboratories under the roof of TÜBİTAK BİLGEM, allows offline payments by making use of the AKIS Smart Card Operating System and NFC technologies. AKIS runs on a microprocessor that provides security services and provides electronic signature, encryption, and security keys transport services. The TOPS allows the use of Turkish ID cards for offline payments, is an alternative to TEE-oriented solutions used in mobile phones, and is a highly secure method that can work on AKIS-compatible ID cards of any country. The TÜBİTAK Offline Payment System also has importance in that it is the first study in the world to be proposed using AKIS -compatible ID cards. In this study, only the cryptographic architecture of the proposed TOPS system is introduced.

Keywords: Offline payment, Digital currency, Central bank digital currency, Near field communication, Smart card operating system, AKIS, TEE.

1. Introduction

Central Bank Digital Currencies (CBDC) are national currencies developed to replace cash [1]. As a result of the interest in cryptocurrencies and the spread of blockchain technology [15, 16], especially in the field of finance, many central banks in the world are working on blockchain-based digital money to be used in digital payments [2]. Considering May 2022, 109 countries continue their studies on CBDC at various levels. China, Nigeria, Bahamas, Cambodia, and the Republic of the Marshall Islands are countries that have made progress in CBDC studies and have made them available [3].

When examining CBDC projects, three criteria usually come to the fore. The first of these is the ledger architecture of the CBDC project. A CBDC project can be single-ledger-based, distributed-ledger-based, or hybrid solutions purely according to the needs of central banks. In single-ledger-based systems, it becomes a target because the central bank runs the ledger itself. If the ledger under the control of the central bank cannot be reached due to cyber-attacks or various reasons, the financial system of a country may become unusable. In distributed-ledger-based systems, transaction records are shared among stakeholders in a distributed and transparent manner in accordance with the consensus used. Compared to the other method, it is more secure due to the use of a distributed architecture against cyber-attacks. In hybrid solutions, according to the central banks' requests, the system can have architectures that keep the ledger off-chain or transactions saved partially on the ledger, and the rest of the information can be saved in off-chain architectures. In CBDC projects where hybrid solutions are selected, system security should be handled in great detail and it should be developed against any kind of security breach that may be encountered. The second criterion is whether the CBDC system is permissioned or permissionless. In other words, the access authorization to the system is only for certain people or it is open to everyone. The third criterion is the direct-CBDC system where the central bank serves people as a service provider in CBDC projects or the indirect-CBDC system that makes use of intermediary institutions [4].

No matter what criteria the CBDC projects are developed, it has to meet all the functionality that the cash used today can do [5]. The offline payment capability is at the forefront of these functionalities that are focused on in this study. Since CBDC projects are internet-based services, internet connection is one of the most important requirements that users should have [6]. In addition, the ability to make payments, provided by cash and without the need for any infrastructural requirements, is a feature that should be practically provided in CBDC systems [7]. The possibility of accessing the internet is at different levels in every country in the world in proportion to the level of development. For this reason, the CBDC systems should be able to work and be usable by all segments of society even in environments where internet access is minimal or non-existent [17]. There are various studies in the literature on this subject and there are real-life applications that can be checked [8-11].

Security requirements in offline payment processes are provided with cryptology techniques and appropriate hardware. The prominent requirements for offline payment security are double-spending, unforgeability, non-repudiation, verifiability,

anonymity, and DDoS-proof [4]. The system proposed in this study meets all of the specified security criteria at different levels.

Technologies such as Trusted Execution Environments (TEE) [11], Near Field Communication-NFC [12, 13], Short Message Service (SMS), Quick Response (QR) Code, and Bluetooth are used in offline payment architectures [9]. TEE, which is available on most phones, tablets, and computers, is widely preferred in offline payment solutions. Because it tries to avoid double-spending by relying on digital signatures created by TEE. The study of Christodorescu et al. is a very good example of TEE-based systems [11]. Moreover, The TOPS system we proposed was inspired by the study of Christodorescu et al. However, since the reliability of the TEE environment will be at a level that will be provided by private companies that produce TEE, alternative solutions such as smart cards provided by more reliable authorities should be used in cases where national usage such as offline payment is required. For this reason, in the TOPS study, an offline payment system using mobile phone's NFC technology and the microprocessors in Turkish identity cards as a reliable environment without the requirement of TEE, thanks to AKIS Smart Card Operating System [14] developed under the roof of TÜBİTAK, has been proposed.

AKIS Smart Card Operating System

AKIS is a nationally developed smart card operating system. AKIS is designed to run on smart card microprocessors that have passed the Common Criteria CC EAL 5+ security assessment and it also has CC EAL 5+ certification. AKIS provides security services and provides electronic signature, encryption, and security keys transport services. In daily life, smart cards with AKIS are used for electronic signatures, electronic identity cards, credit cards, public transportation cards, etc. purposes.

Developed in compliance with ISO/IEC 7816 standards, AKIS smart cards are used as PKI cards with contacted or contactless interface that is compatible with ISO/IEC 14433A. Thus, the contactless interface can communicate securely with the NFC of mobile phones.

The most important advantage of the AKIS smart card is that the information stored in it can be protected against unauthorized access and tampering. Since the access to the data is only in serial way, the control of this door is done by the card operating system and the security mechanism. Under this security mechanism, confidential information can be written on the card and cannot be accessed by unauthorized persons. This information can be processed or used by the card processor as required by the application. In these processes, no information is leaked to the outside. In principle, various security measures can be taken by linking memory functions such as reading, writing, and deleting to certain hardware and software conditions.

The smart card operating system has security measures against various deeper attacks. For example, by fixing the processing times of the algorithms, with channel analysis and timing analysis disclosure of confidential information is prevented. Data important to security collection test data integrity is checked. When integrity is broken, the card protects itself.

Operations in algorithms by changing the order of the algorithm detection is made difficult. Operation with counters used in the side-channel analysis. The counter operation can be prevented by being detected and the power is cut off at that time. In counters, the attack can be prevented by resetting the counter to its old value. Requiring high-security experiments with a length limit on the data estimation is made difficult by the error method.

2. Proposed System

In the proposed system, an offline payment method based on running the specified functions securely is offered on AKIS Smart Card for CBDC offline payments. The functions that must be executed by the smart card are described below.

Table 1. Notations.

Variable	Description	Scope
(vk_A, sk_A)	Key pair for Client A	Global, Phone
(vk_s, sk_s)	Key pair for the server	Global, Server
$S.onBal_A$	Online balance of Client A	Server
$S.i_A$	The counter value of Client A executed by the Server	Server
C_A	A's secure execution environment is the smart card	Card
$(C_A.vk, C_A.sk)$	Key pair of C_A	Card
$cert_A$	Certificate generated by the server for vk_A	Global
$C_A.cert$	Certificate generated by the server for $C_A.vk$	Global
$C_A.i$	Counter value executed by the card of Client A	Card
$C_A.j$	"payment counter value" executed by Client A's card	Card
$C_A.bal$	Offline balance of Client A handled by the card	Card
$C_A.inPaymentLog$	List of offline payments	Card

Init: Generates a key pair for the smart card. Resets the balance and counter values. Generates the signature that the generated key was created by the card. This is the first function that needs to be run on the board.

CertInit: Verifies and saves the certificate received from the server. It is the second function to be executed, after this function other functions can be executed.

Deposit: Converts online balance to offline balance and increases offline balance.

Withdraw: Converts offline balance to online balance and increases online balance.

Pay: Generates offline payment value.

Collect: Increases the balance held by the card in the offline session.

In Fig. 1, the proposed system model is shared. Arrow 1 represents the *withdraw* function, arrow 2 represents the *pay* function, arrow 3 represents the *collect* function, and arrow 4 represents the *deposit* function.

Transactions performed in arrow 2 and arrow 3 are not one-time procedures. The client, who got paid in the offline payment system, can use this money for another offline payment without interacting with his online account. In other words, in the proposed system, offline payments can be made in large numbers without interacting with the online account.

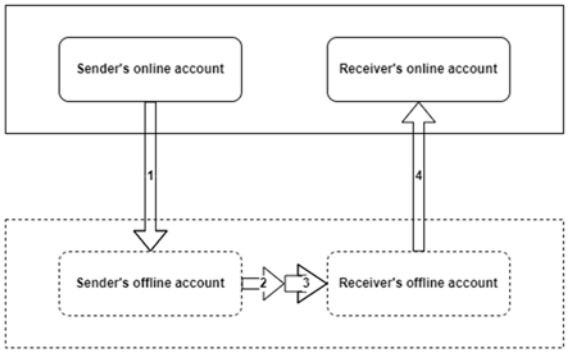


Fig. 1. Proposed system model.

3. Protocols of the System

There are 5 protocols in the offline payment system we have proposed. These are client registration protocol, smart card registration protocol, deposit protocol, withdraw protocol, and offline payment protocol. These protocols are explained in the following subchapters.

3.1. Client Registration Protocol

Purpose: Client A wants to create an account on Server S.
1. Client A sends [RegisterClient, vkA] values to Server S such that (vkA, skA) ← KeyGen()
2. After the server receives the [RegisterClient, vkA] request: **a.** If (aka) is registered, it cancels the request. **b.** (vkA, ∅) is added to the Recording List. **c.** S.onBalA ← 0 **d.** creates a certA and sends it to Client A.

The Client generates a signature key pair denoted by (vk, sk) to register with the server and sends the authentication key to the Server. After checking whether a record has been created with this key before, the server resets its online balance and creates a certificate for Client A and sends the certificate to Client A. The certificate is generated with the private key of the S server and contains the vk public key.

3.2. Smart Card Registration Protocol

Purpose: Client A wants to register its Smart Card (Client A's trusted execution environment) on the server.
1. A creates (C_A.vk, σ) ← C_A.Init() in card environment and sends [CardRegister, C_A.vk, vk_A, σ] values to Server.
2. After S Server gets [CardRegister, C_A.vk, vk_A, σ] values: **a.** If (vk_A, ∅) is not registered in the list or CardVerify(C_A.vk, σ) ≠ 1, it will cancel the request. **b.** i_A ← 0 **c.** Generates a certificate and sends it to Client A such that cert.vk ← C_A.vk **d.** Replaces the value (vk_A, ∅) in the list with (vk_A, cert.vk).
3. Client A runs the C_A.CertInit(cert) function.

Client A executes the Init() function by the card to register its Smart Card to the server. The init() function generates the key pair for the smart card. Resets offline balance and counter values. The Card.Prove(C.vk) function proves that the generated key is actually generated by the card. Mastersecretkey can be embedded in AKIS cards and c.vk keys can be signed with this secret. The function outputs (C.vk, σ) values. A sends the values [CardRegister, C_A.vk, vk_A, σ] to the server.

After the server receives the values, it checks if the client is in the list and checks that the generated key is generated by the card. It then resets the counter value and generates a certificate for the C_A.vk key generated by the Card. It sends the generated certificate to Client A.

Init () function:
1. (C.vk, C.sk)← KeyGen()
2. C.bal = 0, C.i = 0, C.j = 0
3. σ ← Card.Prove(C.vk)
4. Output: (C.vk, σ)

After Client A receives the certificate, it runs the C_A.CertInit(cert) function inside the card. The certificate is verified with the authentication key of the server previously installed in the card and the certificate is saved by the card.

CertInit (cert) function:
1. If CertVerify(cert, vk_s) ≠ 1, the function stops.
2. C.cert ← cert.

3.3. Deposit Protocol

Purpose: Client A wants to transfer x amount from its online balance (on the S Server side) to its offline balance (on the smart card side).
1. Client A sends a deposit request to Server S and the amount x it wants to transfer. [Deposit, x]
2. After S Server receives [Deposit, x] request: **a.** If $x > S.onBal_A$, it cancels the request. **b.** $S.onBal_A \leftarrow S.onBal_A - x$ **c.** $S.i_A \leftarrow S.i_A + 1$ **d.** The server sends the confirmation and values. [DepositConfirmed, x, $S.i_A$, σ] such that $\sigma \leftarrow Sign([C_A.vk, x, S.i_A], S.sk_s)$
3. Client A runs the C.Deposit(x, i, σ) function after receiving [DepositConfirmed, x, $S.i_A$, σ] values from Server S.

Client A, who wants to transfer x amount from their online balance to their offline balance, sends the [Deposit, x] request to the server. After identifying A's identity, the server checks whether he has sufficient funds. After this check, the Server will deduct x amount from its online balance, increase the counter value of A and generate a confirmation containing x amount. In addition to the amount, the confirmation includes the counter value and the digital signature issued by the Server. Having received the confirmation and values, Client A runs the Deposit function in its secure environment.

Deposit (x, i, σ) function:
1. If $i \neq i + 1$ or SignVerify([C.vk, x, i], σ, vk_s) $\neq 1$, the function stops.
2. C.bal ← C.bal + x
3. i ← i + 1

The deposit function checks whether the counter value is compatible and verifies the signature. It then increments the balance handled by the smart card and prepares the current counter value for other Deposit or Withdraw functions.

The counter value i is used to uniquely identify deposits and withdrawals, thus preventing a customer from using a particular deposit confirmation more than once. If the attacker tries to forge the i value, the digital signature will prevent such an attack.

3.4. Withdraw Protocol

Purpose: Client A wants to transfer x amount from its offline balance (on the smart card side) to its online balance (on the S Server side).
1. Client A sends [Withdraw, x, i, σ] values to Server S such that [x, i, σ] ← C.Withdraw (x)
2. After S Server receives the [Withdraw, x, i, σ] request: **a.** If $i \neq S.i_A + 1$ or SigVerify([x, i], σ, $C_A.vk$) $\neq 1$, it cancels the request. **b.** $S.onBal_A \leftarrow S.onBal_A + x$ **c.** $S.i_A \leftarrow S.i_A + 1$ **d.** The server sends the confirmation to Client A. [WithdrawConfirmed]

Client A wants to transfer the amount x from its offline balance to its online balance and runs the Withdraw function. The smart card checks the adequacy of its offline balance. It then replenishes its offline balance and prepares the current counter value for other Deposit or Withdraw functions. As with the Deposit Protocol, the signature is set to x and i values and sends them to Client A.

Withdraw(x) function:
1. If x > C.bal, the function stops.
2. C.bal = C.bal − x
3. i ← i + 1
4. Output: [x, i, σ] such that σ = Sign([x, i], C.sk)

The S server checks the counter value for compatibility and verifies the signature. Then, it increases the online balance of the relevant user by x amount, renews the counter value, and sends the confirmation to Client A.

3.5. Offline Payment Protocol

Purpose: Client A wants to transfer x amount of money to Client B offline.
1. Client B selects receiver←C_B.cert and forwards RequestPayment, x, receiver values, and request to Client A.
2. Client A sends P ← C_A.Pay(x, receiver) values to Client B after receiving the request.
3. After Client B receives the P values, it runs the CB.Collect(P) function on the smart card and sends the [ReceivedPayment] value to Client A.

Client B sends Client A a payment request specifying the amount and certificate. After Client A receives the request, it runs the Pay(x, receiver) function on its smart card. After the function checks the balance, the amount to be transferred decreases from the offline balance, and by increasing the counter used for offline payment; creates a digital signature containing quantity, recipient certificate, sender certificate, and counter value and sends these values to Client B.

Pay(x, receiver) function:
1. If x > C.bal or C.cert = ∅, the function stops.
2. C.bal = C.bal − x
3. j ← j + 1
4. P.amount ← x,
P.sender ← C.cert, P.receiver ← receiver,
P.index ← C.j,
5. P.sign ← Sign([P.amount, P.sender, P.receiver, P.index], C.sk)
6. Output: P

Client B runs the Collect(P) function on the board after receiving the values. With the PayVerify() function, it checks the signature accuracy, whether the amount has been created for itself and whether this transaction has been recorded before (to avoid double-spending.). It then adds the amount to the offline balance and adds the P to the Payment Records.

Collect(P) function:
1. If the following conditions are true, the process stops. **a.** PayVerify(P) ≠ 1 **b.** P.receiver ≠ receiver **c.** P ∈ B.inPaymentLog
2. C.bal = C.bal + x
3. Adds the P to the Payment Records.

4. Analysis of Proposed TÜBİTAK Offline Payment System

In offline payment systems suggested in the literature, as expected, blockchain integration is disabled, in other words, transactions cannot be recorded on the blockchain synchronously. Processes that interact with the blockchain include situations where online and offline wallets communicate with each other and digital currency exchanges occur between the user's wallets. A similar architecture has been developed in the TÜBİTAK Offline Payment System that was proposed in this study. AKIS - compatible smart cards (AKIS 3.0 Smart Cards) have infrastructural facilities to keep detailed records of offline payments and send these transaction records to the blockchain. Thanks to this feature, which will be added to the TOPS system in the future, it will provide a solution to the problem of tracking the money flow encountered in the literature, in a way that will not affect anonymity, as well as the possibility of recording offline payment transactions on the blockchain. However, the current version of the shared TOPS proposal does not provide solutions for blockchain interaction and money flow tracking features in offline payments.

TÜBİTAK Offline Payment System offers a smart card-based solution. It can provide the features provided by TEE, which is widely used today. TEE solutions are as secure as private sector companies that develop TEE can provide. Security vulnerabilities originating from the manufacturer are possible. In the TOPS proposal, smart card security in ID cards owned by each user and used in offline payment processes is under the protection and responsibility of the state. In this context, TOPS is a more reliable solution.

In the TÜBİTAK Offline Payment System, there is the amount of digital money sent, the sender's certificate, the recipient's information, the transaction counter, and the signature created by the sender using all these data. The receiver checks whether this information has already been found in the records. In this way, the reuse of used money is prevented. Certificate control and payment counter structure are mechanisms that were developed at TOPS to prevent double-spending.

TOPS' smart cards put themselves into protection mode and lock themselves in case of external intervention or attack on the card. This feature ensures the protection of the digital currency balance and other data that needs to be protected. Thanks to this feature, unforgeability is provided to the proposed system.

Each data that the user sends to the external environment by the card contains the signature of the card, in other words, the cryptologic signature of the user. This feature also provides non-repudiation to TOPS.

When offline payment is made in TOPS, the amount of money, sender certificate, recipient information, and transaction counter are stored in the card log. In this way, verifiability is provided to the system.

Transaction histories in offline payment at TOPS can be examined after AKIS officials obtain the necessary official permission from the relevant authorities and access to the physical card is provided. However, even if this information is accessed, TOPS in its current form does not keep the information of the users that would conflict with anonymity in the transaction records.

There are two accepted solutions to prevent DDoS attacks on blockchain systems. The first solution is to charge fees for transactions. Transaction fees reduce the risk of DDoS, as can be seen in the examples of AVAX and many other distributed ledger technology platforms. In the second method, a delay time is determined between transaction requests. In this way, the simultaneous transaction request is streamlined and DDoS attack from a single source is prevented. The AKIS cards that we used in our study have a delay period for transactions. In this way, hardware protection is provided by AKIS against DDoS attacks.

5. Conclusions

In the proposed study, only the cryptographic architecture of the TÜBİTAK Offline Payment System, which can work on Turkish ID cards with AKIS Smart Card Operating System compatible smart cards, has been introduced. TOPS has importance in that it is the first study in the world to be proposed using AKIS-compatible ID cards, and it can be an alternative method that can be easily applied in the Central Bank Digital Money projects today. TOPS is designed as an alternative to conventional TEE-based offline payments and is a highly reliable offline payment system with both the structural security layers provided by AKIS-compatible smart cards and the cryptologic security layers. There is no ledger architecture in TOPS proposed in the study. However, in addition to the capabilities that can be gained with AKIS 3.0, researchers are still continuing their studies

to integrate the ledger into the existing system with the help of smart contracts.

Acknowledgements

We would like to thank TÜBİTAK-BİLGEM for financing our TOPS study and also we would like to thank Ümit Aygül from Crypto Analysis Laboratory for providing support in cryptologic studies.

References

[1] G. Goodell, H. D. Al-Nakib, P. Tasca. A Digital Currency Architecture for Privacy and Owner-Custodianship, Future Internet, Vol. 13, Issue 5, 2021, pp. 130.

[2] H. Jung, D. Jeong. Blockchain Implementation Method for Interoperability between CBDCs, Future Internet, Vol. 13, Issue 5, 2021, pp. 133.

[3] Central Bank Digital Currency Tacker (https://www.atlanticcouncil.org/cbdctracker/).

[4] Y. Chu, J. Lee, S. Kim, H. Kim, Y. Yoon, H. Chung. Review of Offline Payment Function of CBDC Considering Security Requirements, *Applied Sciences*, Vol. 12, Issue 9, 2022, pp.4488.

[5] B. C. Su, L. W. Wu, Y. C. Yen, Antecedents and Consequences of Trust and Loyalty in Physical Banks Affecting Mobile Payments, *Sustainability*, Vol. 13, Issue 22, 2021, pp. 12368.

[6] B. Swoboda, A. Winters, Effects of the most useful offline-online and online-offline channel integration services for customers, *Decision Support Systems*, Vol. 145, Issue 2021, pp. 113522.

[7] A. M. Musyaffi, S. Mulyani, I. Suraida, C. Sukmadilaga. Lack of Readiness of Digital Banking Channel Acceptance: Study on TAM 3 and Technology Readiness, *Academy of Strategic Management Journal*, Vol. 20, 2021, pp. 1-18.

[8] Secure offline CBDC wallet (https://www.idemia.com/secure-offline-cbdc-wallet).

[9] Completely Offline Central Bank Digital Currency (https://www.whispercash.com/).

[10] D. Alexandra, N. David, Y. Moti. Secure Wallet-Assisted Offline Bitcoin Payments with Double-Spender Revocation, in Proceedings of the ACM on Asia Conference on Computer and Communications Security, Association for Computing Machinery, New York, USA, 2017, pp. 520–531.

[11] M. Christodorescu, W.C. Gu, R. Kumaresan, M. Minaei, M. Ozdayi, B. Price, S. Raghuraman, M. Saad, C. Sheffield, M. Xu, Towards a Two-Tier Hierarchical Infrastructure: An Offline Payment System for Central Bank Digital Currencies, *arXiv:2012.08003*, 2020.

[12] C. Thammarat, Efficient and Secure NFC Authentication for Mobile Payment Ensuring Fair Exchange Protocol, *Symmetry*, Vol. 12, Issue 10, 2020, pp.1649.

[13] N. K. Singh, Near-field Communication (NFC), *Information Technology and Libraries*, Vol. 39, Issue 2, 2020.

[14] National Smart Card Operating System, (https://akiskart.bilgem.tubitak.gov.tr/tr/akis-nedir.html).

[15] M. Takaoğlu, A. Özyavaş, N. Ajlouni, A. Alshahrani, B. Alkasasbeh, A Novel and Robust Hybrid Blockchain and Steganography Scheme, *Applied Sciences*, Vol. 11, Issue 22, 2021, pp. 10698.

[16] N. Ajlouni, A. Özyavaş, M. Takaoğlu. A Survey of Artificial Intelligence Driven Blockchain Technology: Blockchain Intelligence, *The Manchester Journal of Artificial Intelligence & Applied Science*, Vol. 2, Issue 2, 2021.

[17] J. Kiff, Taking Digital Currencies Offline. (https://www.imf.org/en/Publications/fandd/issues/2022/09/kiff-taking-digital-currencies-offline).

(003)

Hidden Markov Model for Price Clustering Bitcoin-Ethereum Trading

Fatma Hachicha
Department of Finance Institute of High Business Studies of Sfax, Sfax, Tunisia
Fatma.hachicha@ihecs.usfs.tn

Summary: Hidden Markov model (HMM) is a statistical prediction model, which has been widely used to predict economic regimes and stock prices. With the rapid growth of the cryptocurrency market, we applied this model to predict the phenomenon of price clustering. In this paper, we firstly propose the K-means approach (algorithm) in order to determine the efficient (real) number of states. Secondly, we applied the hidden Markov model, which is based on the transition matrix and emission matrix, to apprehend the relationship between price clustering Bitcoin/Ethereum and rational sentiment investor, volatility, price and economic policy uncertainty (EPU) variables. The proposed model facilitates capturing the uncertainties price clustering and the possible effects of the dynamics of the cryptocurrency market on the persistence of these regimes or states. Our results indicate that the Hidden Markov Model (HHM) with four states has the best one-step-ahead forecasting performance among all competing models for two series; the accuracy rate is 98 %.Moreover, the results of this paper gave new insights into the financial analysis of cryptocurrency market about the dynamic relationship between price clustering regimes and different states of the explanatory variable. Indeed, the impact of the rational sentiment investor and the prices and the EPU on predicting the price clustering was found to depend on the state of price clustering and the explanatory variable. These empirical findings provide important insight into portfolio management and policy implementation. In fact, the detection of the different returns on cryptocurrency market states improves the investment decisions for investors and particularly the risk of portfolio diversification. In addition, our finding proves the efficiency of Hidden Markov Model for our sample and provides a good predictability.

Keywords: Hidden Markov model, Predictability, Price clustering, Bitcoin, Ethereum, Rational sentiment investor, k-Means Clustering, Transition probability matrix, Emission probability matrix.

1. Introduction

Cryptocurrency markets have grown enormously since 2008. It is the first cryptocurrency that aims to decentralize the central banking system with an implemented blockchain and it was developed and introduced by Satoshi Nakamoto. There has been a growing interest in predictive studies of cryptocurrency returns [1-4], without forgetting the study of the stochastic volatility of this cryptocurrency [5-7]. Other researchers examined the volatility and market microstructure of bitcoin [8-10].

Following the spectacular growth of this virtual currency, several studies have shown that it is interesting to incorporate it into the investor's portfolio as a means of diversification and refuge [11-13].

Following the spread of this currency to the real sphere, a well-known behavioral phenomenon is observed in the literature known as price clustering, where prices tend to cluster around specific sets of values, usually whole figures. Price clustering is a frequently observed phenomenon in financial markets. It should be noted that this phenomenon was initially observed on stock markets [14-20], commodity markets [21, 22], foreign exchange market, [23, 24], and options markets [25].

In fact, during the past two decades, crypto-currency markets have experienced different episodes of crashes such as the covid-19 pandemic and the global financial crisis. Several techniques have been applied to predict the return of this virtual cryptocurrency such as learning models [26]; Bayesian framework [27], time-varying vector autoregression models [28].

More especially, in stochastic analysis, the hidden Markov model (HMM) is a probabilistic process that looks at the current state to predict the next one. It should be noted that HMM models have been applied in the cryptocurrency market to understand price bubbles by Phillips and Gorse [29].

As for the price clustering forecast, we note that few techniques have been applied like the profit model and the OLS [30]. For these reasons, it should be noted that it is interesting to present other techniques to help the investor better allocate their portfolio and manage their risk. Through this research paper, we will present the Hidden Markov Model technique to predict the price clustering.

This paper makes at least two contributions to the cryptocurrency market. First, we introduce a recent measure of sentiment rational of investor using the CPA with different factors in order to explain the price clustering. Second, it contributes to the cryptocurrency finance literature by using Hidden stochastic processes called Markov chains with four states to predict the price clustering. We applied the K-means in order to specify the efficient number of states. Moreover, we used the four explanatory variables and attributed two states for each variable (discretization). Hence, this paper uses the Hidden Markov Model (HMM) that could interpret the price clustering of two cryptocurrency Bitcoin and Ethereum using four explanatory variables (investor sentiment, economic

policy uncertainty, prices and volatility) and tries to find out the transition probability of regime change. Third, the present work seeks originality in the fact that such an analysis has not been conducted yet, in the context of financial cryptocurrency using the K-means.

Our paper aims to analyze the clustering of the cryptocurrency market like the Bitcoin and Ethereum based on the hidden Markov Model. After 2018, the cryptocurrency market has experienced a massive bull market. Notably, most of the cryptocurrencies exhibit extremely high correlations with the Bitcoin and Ethereum. Therefore, in this study, we attempt to estimate the price clustering Bitcoin–Ethereum for four states and analyze the market structure for different periods cases and also for the Pre- and Post-Covid 19 period.

The objective of this paper is to investigate the predictive effect of rational sentiment investor, volatility, price and EPU on price clustering cryptocurrency markets. We consider four price clustering states: the depressed price clustering (S0), the bullish price clustering (S1), the bearish price clustering (S2) and the bubble price clustering (S3). We propose an HMM based on the transition matrix to capture not only the relationship between the price clustering cryptocurrency and the four explanatory variables but also the uncertainties in the price clustering BTC/ETH.

Firstly, to the best of our knowledge, it is the first study to explore the HMM of clustering price BTC/ETH based on four explanatory variables, namely prices, volatility, investor rational sentiment and Economic policy uncertainty (EPU).

Our results showed that the use of K-means approach is efficient in choosing the number of states. After that, we identified *four states for the price clustering according to the market* namely the depressed, the bullish, the bearish, and the bubble. The probability of transaction matrix is very interesting in the sense that we can determine the probability of transition from one state to another state. We find that state 1 exists and persists for two series during totality period especially for Covid 19 period. The transition probability from the depressed state to the bubble state is very much lower, because the transition from the depressed state to the bubble state is only possible through the bullish and bearish states. Similarly, through the emission matrix, the higher state of the different explanatory variable can be said to directly influence the price clustering. In addition, through the emission matrix, it can be said that the higher state of the different explanatory variables directly influences the price clustering (the probabilities are high for the different states).

Furthermore, the detection of the different states of this phenomenon improves the investment decisions for investors and particularly the risk of portfolio diversification. Our finding proves that the HMM model is a very efficient model to estimate the price clustering. It identifies predictors with different conditions on the hidden states linear and effects on the cryptocurrency returns.

Overall, using the Markov chains as a stochastic analysis method in price clustering is considered the first research, and proved its efficiency at the predictability level.

The remainder of this paper is organized as follows. Section 2 details the empirical methodology by introducing first of all the price clustering and the explanatory variables and second of all the HMM model and the K-means approach. Section 3 presents the data and the variable analysis and Section 4 discusses the results. Finally, Section 5 concludes and provides practical implications of our findings.

2. Methodology

The following section presents the methodology used in this study. We start with the construction of price clustering of Bitcoin and Ethereum. Secondly, we present a brief introduction of two approaches using the K-means and the HMM.

2.1. Price Clustering of Bitcoin and Ethereum

We will opt for three daily measures of clustering: (1) round clustering (ROUND%), (2) strategic clustering (STRGY%), and (3) total clustering (CLUSTER%). These measures are calculated as follows:

$$\text{ROUND\%} = \frac{\text{Number of trades occurs at \$;0.10 increment(\$;X;Y0)}}{\text{Daily total numbers of trades}} \quad (1)$$

$$\text{STRGY\%} = \frac{\text{Number of trades occurs at \$;X.01 and \$;X.99}}{\text{Daily total numbers of trades}} \quad (2)$$

$$\text{CLUSTER\%} = \text{ROUND\%} + \text{STRGY\%} \quad (3)$$

2.2. The Explanatory Variables

2.2.1. The Rational Sentiment Measure

For our sentiment measures, we use the Verma and Soydemir [31] model below to capture the two components of investor sentiment — rational and irrational:

$$\text{Sent}_t = \gamma_0 + \sum_{j=1}^{n} \gamma_{j\text{FUND}_{jt}} + \vartheta_t \quad (4)$$

where Sent_t are investor sentiments respectively at time t. FUND_{jt} is the set of fundamental factors indicating rational investor expectations based on several risk variables which are commonly accepted and used to value asset prices in the literature. γ_0 is constant; γ_j are the parameters to be estimated; and $\vartheta_t$is the random error term.

To calculate these sentimental variables, we used the R software by applying PCA (Principal Components Analysis) while taking "Consumer Price Index", "month Treasury Bill, exchange rate and production index as fundamental factors.

Several macroeconomic factors are used in this study as being representative of U.S. market fundamentals. (See appendix 1).

2.2.2. The Volatility

Cryptocurrency, in an emerging market and due to many changes, has impacted the financial system; the market remains turbulent and the price of a currency can rise and fall rapidly. Harris [14] and Ikenberry and Weston [32] presented that stock-specific factors, such as market capitalization, business activity, and volatility, influence the level of clustering. However, Blau et al [33] showed that if volatility changes, the level of price clustering does not necessarily change and they even found that exogenous shocks to volatility do not cause changes in the level of clustering.

2.2.3. The Economic Policy Uncertainty

The EPU (Economic Policy Uncertainty) indicator was developed in 2012 by N. Bloom, Scott R. Baker and Steven J. Davis. It is an original and innovative tool that could become a reference in the measurement of uncertainty related to the conduct of economic policy. Baker and al. [34] showed that the Economic Policy Uncertainty index (EPU) is considered an important factor in the crypto-currency market. While Demir and al. [35] observed that uncertainty about government decisions can cause investors to lose confidence in their fiat currencies or worry about the global economy, especially after the 2008 financial crisis.

3. The K-Means

An important question is how to decide what constitutes good clustering, since it is commonly acknowledged that there is no absolute ‘best’ criterion which would be independent of the final aims of clustering. There are different types of clustering which have been extensively reviewed in the literature. Briefly, one approach is to group data in an exclusive way, so that if a certain item of data belongs to a definite cluster, then, it could not be included in another cluster. In our present work, we have chosen to use the k-means algorithm, as it is unsupervised and its algorithms complexity is linear. In this case, data will be associated to an appropriate membership value and choose the number of clusters in the runs of K-means with different value of K and calculate the sum of squared error SSE of the different clusters. The SSE is the sum of the squared distances between centroid and each member of the cluster. Thus, we seek to estimate a number of clusters K such that the selected clusters minimize the distance between their centers (centroids) and the observations in the same cluster. We are talking about minimizing the intra-class distance.

Data clustering techniques are descriptive data analysis techniques that can be applied to multivariate datasets to discover the structure present in the data. Data clustering can be a valuable tool especially when conventional second-order statistics (sample mean and covariance) cannot be used. It can also be said that data aggregation is a form of unsupervised classification. The k-means clustering technique is part of the grouping of partitioning-based techniques. They are essentially based on the iterative relocation of data points between clusters. Clustering can be viewed as an unsupervised procedure which classifies patterns into groups (clusters).

The clustering of K-means is very useful in exploratory data analysis in any research area. The computational efficiency has made them very popular compared to other clustering techniques such as hierarchical clustering.

3.1. Hidden Markov model (HMM)

A hidden Markov model (HMM) is a statistical model that can be used to describe the evolution of observable events that depend on internal factors, which are not directly observable. This model is introduced by [36]. We call the observed event a `symbol' and the invisible factor underlying the observation a `state'. An HMM consists of two stochastic processes, namely, an invisible process of hidden states and a visible process of observable symbols. The hidden states form a Markov chain, and the probability distribution of the observed symbol depends on the underlying state. The model has the following main assumptions

1. An observation at t was generated by a hidden state (or regime);
2. The hidden states are finite and satisfy the first-order Markov property;
3. The matrix of transition probabilities between these states is constant;
4. The observation at time t of an HMM has a certain probability distribution corresponding with a possible hidden state.

The Hidden Markov model is a probabilistic model about time series. It describes the process of generating a random sequence of unobservable states randomly from a hidden Markov chain and then, generating an observation from each state to generate a random sequence of observations. The key idea is that an HMM is a finite model that describes a probability distribution over an infinite number of possible sequences Eddy 1996.

The sequence of states randomly generated by the hidden Markov chain is called the state sequence; each state generates an observation, and the resulting random sequence of observations is called the observation sequence. Each position in the sequence can be regarded as a moment.

$Q = \{q_1, q_2, \ldots \ldots q_n\}$ denotes the set of all possible states and $v = \{v_1, v_2, \ldots \ldots v_M\}$ denotes the set of all possible observations.

Among them, N is the number of possible states, and M is the number of possible observations. Suppose $I = \{i_1, i_2, \ldots \ldots i_T\}$ is the state sequence of length T, and $O = \{o_1, o_2, \ldots \ldots o_T\}$is the corresponding observation sequence:

$A = [a_{ij}]_{N \times N}$ is the state transition probability matrix and $\pi = (\pi_i)$ is the initial state probability vector.

A, B, π are called the three elements of the hidden Markov model. The state transition probability matrix A and the initial state probability vector π determine the hidden Markov chain and generate an unobservable state sequence. The observation probability matrix B determines how to generate observations from the state, and the state sequence determines how to generate the observation sequence.

The HMM has four main algorithms: the forward, the backward, the Viterbi, and the Baum–Welch algorithms.

HMM is a regime-shift model that assumes that observation data were driven by hidden regimes. Given the time series of Islamic index returns and investor sentiment, we use hidden Markov chains that capture the movement of price clustering in terms of the transition probability matrix (TPM). We consider four states for the dependent variable and two states for each explanatory variable. In our study, we assume that the number of hidden states is discrete and finite. Here we characterize the movement of price clustering from one state to another at random.

4. Data and Variable Analysis

4.1. Data

For this study, two of the most important types of crypto-currencies were chosen (Bitcoin and Ethereum) because together they represent more than 50% of the current market of crypto-currencies. Bitcoin also represents the most common medium of exchange, followed by Ethereum in second place. At the time of data collection, all bitcoin exchanges were in dollars. We collect Bitcoin price and Ethereum price, from the website www.bitcoincharts.com from July 1, 2017 through August 21, 2020. In the form of open, high and low prices (as mentioned above, we ignore close prices) of various time frames (every 5 min). We employ daily data on the US EPU index, extracted from https://www.policyuncertainty.com/ EPU. The software applied is PYTHON.

4.2. Variable Analysis

4.2.1. Price Bitcoin, Ethereum

Fig. 1 plots the evolution of price Bitcoin/Ethereum from July 1, 2017 through August 21, 2020.

Fig. 1 plots the Bitcoin price and the Ethereum price evolution. For a price of 2,434.55 / BTC at the start of our sample, the price of bitcoin temporarily rose to $ 13,657.20 at the start of the first quarter of 2018, then fell back to $ 3,742.70 at the end of the same year.

During the months of 2018, the price of bitcoin exhibited a large fluctuation with a negative trend. In the second quarter of 2019, it rose again and reached 10,817.16 at the end of June. At the end of the sampling period, the recorded price of bitcoin was approximately $ 11,592.49.

Ethereum prices fluctuated widely, like bitcoin and all other cryptocurrencies. The Ethereum price crossed the $ 1,000 mark for the first time at the beginning of January 2018. It reached its historical peak which was equal to $ 1,448.18 but fell below this symbolic bar the following month.

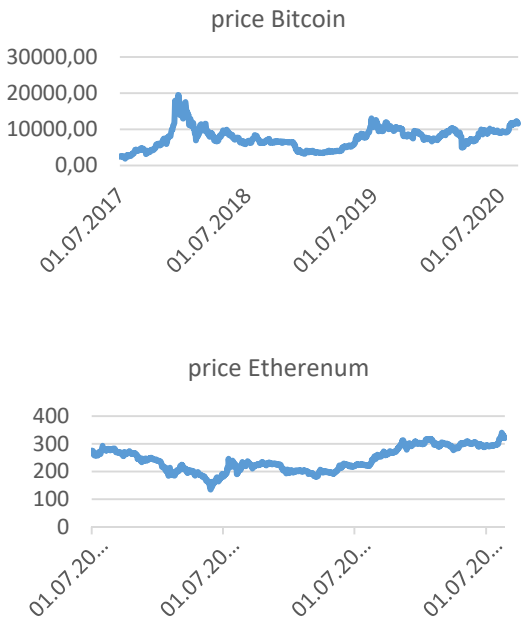


Fig. 1. Price evolution (Bitcoin/Ethereum).

4.2.2. Price clustering Bitcoin, Ethereum

Fig. 2 shows the evolution of price clustering Bitcoin/Ethereum from July 1, 2017 through August 21, 2020.

5. Results and Discussions

5.1. The K-means

The SSE (Sum of Squared Error) is used to evaluate which number of clusters is more optimum for our dataset, or find cluster fitness. Given two clusters, we can choose the one with the smallest error. In addition, the quality of created clusters rely on SSE in order to maximize the inter-class distance between the data points which cluster center. According to Fig. 3 the

optimal number of clusters K is 4, 5 or 6. We choose the K=4 because there is no big difference between 4, 5 and 6. Also, this solution will be supported by further analyses. Generally, the crucial point is that of the number of clusters from which the error is the minimum possible.

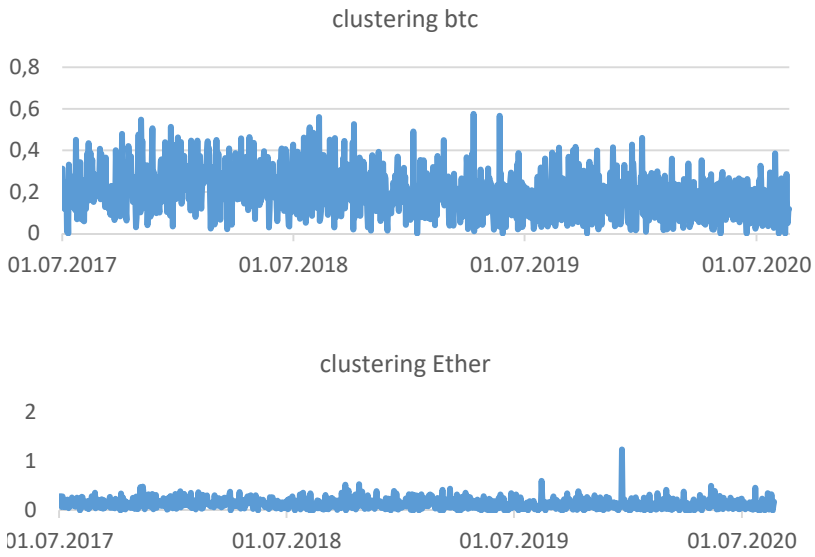


Fig. 2. Price Evolution clustering (Bitcoin/Ethereum).

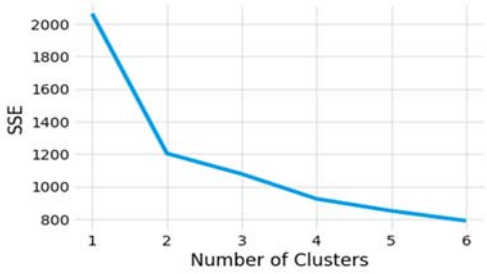


Fig. 3. Optimal number of clusters of Bitcoin.

The dispersion of bitcoin prices clustering is very large as it ranges from 0 to 0.575234. The price is also very disparate (from 1929.820 to 19497.40) with an average equal to 7611.508. Thus, the dispersion of Ethereum prices clustering is as large as that of Bitcoin, ranging from 0 to 0.597138, but its price is lower than that of bitcoin. It varies between 134.32 and 339.94 with an average equal to 242.9177.

For the STRGY variable, it is more important for bitcoin with a value of 0.478924 than that of Ethereum which has a value of 0.381145. On the other hand, for the variable ROUND, it is higher for Ethereum with a value of 0.597138 and a value of 0.536884 for bitcoin.

5.2. Estimation of the Transitional Matrix for Price Clustering BTC/ETHER

Table 1 presents the transition matrix of price clustering during the period from 2017 to 2020 of Bitcoin and Ethereum. The transition probability presents the possibility that the price clustering movements may stay in the original regime or switch to others. These probabilities of movements are presented in the form of the transition probabilities. The values on the diagonal represent the state persistence, which is the probability of remaining in a particular market regime. In fact, we have four-regime transition probabilities P_{11} , P_{22} , P_{33} and P_{44} with 0 = the depressed price clustering BTC/ETHER(S0), 1 = the bullish price clustering BTC/ETHER (S2), 3 = the bearish price clustering BTC/ETHER (S3), 4 = the bubble price clustering BTC/ETHER (S4).

From Table 1, we can examine the dynamic evolution of the transition probabilities and switching regime over time. The transition probability estimates for switching from the depressed market to the bubble market P_{03} (0.104418) are essentially low for Bitcoin. Although it was observed that in cryptocurrency market Bitcoin, the probability of switching from a bubble to a bullish clustering state P_{31} (0.370787) is higher than that of switching from a bullish to a bubble state P_{13} (0.136364). Moreover, the probability of switching from a bubble price clustering to a bearish state P_{32} (0.280899) is higher than the probability of switching from the bearish price clustering to the bubble state P_{23} (0.17284). In fact, the probability of switching from a depressed state to bubble state and conversely is low, and the switching is insignificant.

Table 1 displays a persistence of state 2 (bullish price clustering) in two cryptocurrencies Bitcoin and Ethereum. Indeed, the probabilities in the diagonal are 0.35 in Bitcoin, 0.38 in Ethereum. In contrast, states 0, 1, and 3 seem to be transitory. As can be seen from Table 1, regime switching can be predicted quite accurately because of the high transition probabilities. The persistence of the bullish regime is highly predictable.

Table 1. Transition matrix BTC/ETH.

Transition matrix for BTC				
	State 0 (depressed)	State 1 (Bullish)	State 2 (Bearish)	State 3 (Bubble)
State 0 Depressed	0.309237	0.341365	0.24498	0.104418
State 1 Bullish	0.244949	0.330808	0.287879	0.136364
State 2 Bearish	0.166667	0.354938	0.305556	0.17284
State 3 Bubble	0.117978	0.370787	0.280899	0.230337
Transition matrix for ETHER				
	State 0 (depressed)	State 1 (Bullish)	State 2 (Bearish)	State 3 (Bubble)
State 0 Depressed	0.283155	0.397638	0.212798	0.106436
State 1 Bullish	0.269381	0.347921	0.296112	0.086586
State 2 Bearish	0.208321	0.337261	0.327265	0.127153
State 3 Bubble	0.156329	0.383866	0.316725	0.143080

In summary, the results identify that the first bullish regime is the most persistent for Bitcoin and Ethereum cryptocurrencies. A possible explanation for this result is that a higher transition probability of the bull regime is associated with an increase of a positive rational investor's sentiment especially during the Covid 19.

5.3. Residual Error Test of the Price Clustering

From these two Figs. 4 and 5, we observe that the residual error of the price clustering variable is between (-2 ;2) for a risk level of 5 %. This proves the strength and effectiveness of our estimation approach. Then we obtain the accuracy rate equal to 98 %. This proves the efficiency and robustness of our applied model for this study.

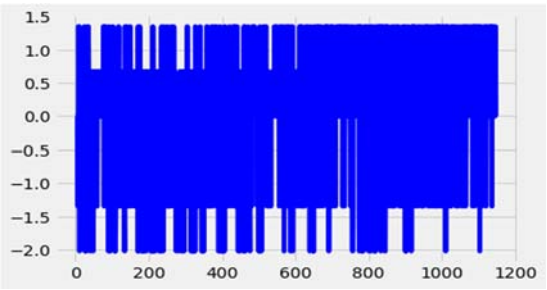


Fig. 4. Residual error of BITCOIN.

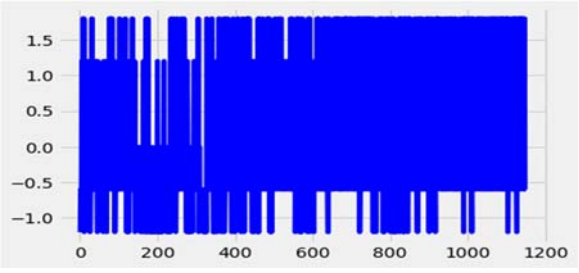


Fig. 5. Residual error of ETHER.

5.4. Predicted of the State Price Clustering

In order to test the efficiency and robustness of the HMM model to predict the price clustering, a modelling with new sample of 250 observations was taken. In this case, we estimated the different states of each observation for both cryptocurrency Bitcoin and Ethereum through the HMM model.

Fig. 6 illustrate the prediction of new sample for cryptocurrency BTC/ETHER. According to this fig, we note that most of the predicted states are positioned between the two states 1 and 2. Otherwise, there is a concentration of bitcoin price clustering at the level of bearish and bullish.

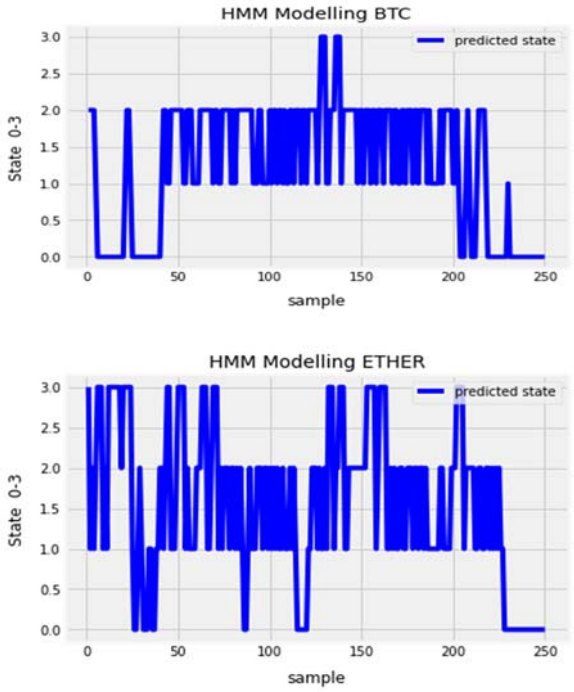


Fig. 6. HMM modeling a new sample.

The different patterns of price clustering for different states can be explained essentially by the psychology of the investor. Our finding joins the work of (Mitchell, 2001). High and low rational sentiment directly influences the price clustering. Similarly, high prices tend to cluster more at 9 and 8 than open and low prices, while low prices tend to cluster more at 1 and 2. This induces the concentration of price

clustering at the level of the two states 1 and 2 explaining the switching regime Bull and Bear.

This implies that the price at these moments is created by a surge in cryptocurrency prices that is driven by exuberant market behavior. In this situation the behavior of the investor will be different following the sentiment and more particularly the rational sentiment, which will induce a different behavior of investors compared to other states.

6. Conclusion

The main objective of this research work is to examine the predictive effect of the relationship between price clustering for two cryptocurrency Bitcoin/Ethereum and the rational sentiment investor, prices, volatility and EPU from July 1, 2017 to August 21, 2020.

We propose to use the K-means approach in order to detect the efficient number of states. We find that number four of the states is the best. *We attribute four states for the price clustering according to the market* namely the depressed, the bullish, the bearish, and the bubble. After this choice, we propose to use the HMM to estimate the transition matrix, the emission matrix and the derivation of SteadyState probabilities. In fact, the Markov chain provides a credible approach for a successful analysis and prediction time-series data that reflect Markov's dependency.

Our results have proven that state 1 exists and persists. Besides, it has the highest duration for the Bitcoin and Ethereum. Interestingly, the transition probability from the depressed state to the bubble state is very much lower. Because the transition from the calm state to the bubble state is possible only by going through the depressed, bullish and bearish states, these states are the transition states in price clustering. Therefore, the transition from the bearish state to the bullish state is absolutely possible.

Also, the transition from the bubble to the bearish is only by going through the bullish for the two cryptocurrency Bitcoin /Ethereum.

Indeed, the impact of the rational sentiment investor, the prices and the EPU on predicting the price clustering was found to depend on the state.

Similarly, through the emission matrix it can be said that the higher state of the different explanatory variable directly influences the price clustering (the probabilities are high for the different states).

Furthermore, the detection of the different stock market states improves the investment decisions for investors and particularly the risk of portfolio diversification.

Overall, using the Markov chains as a stochastic analysis method in price clustering is considered the first research, and approved its efficiency at the predictability level.

The implications of these findings for investment and portfolio choices have been highlighted. With this study, investors are better positioned to choose the best portfolio allocation while landing on the four states. Indeed, investors and policy-makers should pay heed to the price and volatility of explaining the price clustering, consider the rational sentiment investor and the EPU in the two states and the transition probabilities when they make portfolio investment decisions.

Reference

[1]. Aalborg, H., Molnar, P., de Vries, J., What can explain the price, volatility and trading volume of Bitcoin? *Finance Research Letters*, 29, 2019, pp. 255–265.

[2]. Bleher, J., Dimpfl, T., Today i got a million, tomorrow, i don't know: On the predictability of cryptocurrencies by means of google search volume, *International Review of Financial Analysis*, 63, 2019, pp. 147 – 159.

[3]. Kurka, J., Do cryptocurrencies and traditional asset classes influence each other? *Finance Research Letters*, 31, 2019, pp. 38–46.

[4]. Katsiampa, P., An empirical investigation of volatility dynamics in the cryptocurrency market, *Research in International Business and Finance,* 50, 2019, pp. 322 – 335.

[5]. Hachicha F, Hachicha.A, 2021, Analysis of the bitcoin stock market indexes using comparative study of two models SV with MCMC algorithm, *Review of Quantitative Finance and Accounting,* 2021, 56, pp. 647–673.

[6]. Dirk .G; .Baur, L .Hoang, M Zakir, H., Is Bitcoin a hedge? How extreme volatility can destroy the hedge property, *Finance Research Letters*, 2022.

[7]. Chuanhai Z., Zhanga, H., Chena Z, Does Bitcoin futures trading reduce the normal and jump volatility in the spot market? Evidence from GARCH-jump models, *Finance Research Letters*, 2022.

[8]. Urquhart, A., Zhang, H., Is bitcoin a hedge or safe haven for currencies? An intraday analysis, *International Review of Financial Analysis*, 63, 2019, pp. 49 – 57.

[9]. Blau, Benjamin M, Price dynamics and speculative trading in bitcoin, *Research in International Business and Finance*, 41, 2017, pp. 493–99.

[10]. Bariviera, Aurelio F, The inefficiency of bitcoin revisited: A dynamic approach, *Economics Letters,* 161, 2017, pp. 1–4.

[11]. Zhang X., Chen Q., Fang. P., Cluster-based aquaculture growth, *International Food Policy Research Institute IFPRI*, 2019. https://www.researchgate.net/deref/https%3A%2F%2Fdoi.org%2F10.1080%2F00036846.2011.610747

[12]. Bouri, Elie et al., Gold, Platinum and the Predictability of Bond Risk Premia, *Finance Research Letters*, 2020, p. 101490.

[13]. Platanakis, Emmanouil and Andrew Urquhart, Should investors include bitcoin in their portfolios? A portfolio theory approach, *The British Accounting Review,* 2019, p. 100837.

[14]. Harris, L., Stock price clustering and discreteness, *Rev. Financ. Stud*, 4, 1991, pp. 389–415.

[15]. Kandel, S., Sarig, O., Wohl, A., Do investors prefer round stock prices? Evidence from Israeli IPO auctions, J, Banking Finance 25, 2001, pp. 1543–1551.

[16]. He, Y., Wu, C., Is stock price rounded for economic reasons in the Chinese markets? *Global Finance J.*, 17, 2006, pp. 119–135.

[17]. Cai, B. M., Cai, C. X., Keasey, K., et al., Influence of cultural factors on price clustering and price resistance

in China's stock markets, *Accounting & Finance*, 47, 2007, pp. 623–641.
[18]. Brown, P., Mitchell, J., Culture and stock price clustering: evidence from The Peoples' Republic of China, *Pacific-Basin Finance J*, 16, 2008, pp. 95–120.
[19]. Narayan, P. K., Narayan, S., Popp, S., Investigating price clustering in the oil futures market, *Appl. Energy*, 88, 2011, pp. 397–402.
[20]. Davis, R. L., Jurich, S. N., Roseman, B. S., Watson, E. D., Short-sale restrictions and price clustering: evidence from SEC rule 201, *J. Financ. Serv. Res,* 54, 2018, pp. 345–367.
[21]. Ball, C. A., Torous, W. N., Tschoegl, A. E., The degree of price resolution: the case of the gold market, *J. Futures Markets*, 5, 1985, pp. 29–43.
[22]. Bharati, R., Crain, S.J., Kaminski, V., Clustering in crude oil prices and the target pricing zone hypothesis, *Energy Econ,* 34, 2012, pp. 1115–1123.
[23]. Lallouache, M., Abergel, F., Tick size reduction and price clustering in a FX order book, *Physica A,* 416, 2014, pp. 488–498.
[24]. Liu, H.-C., Timing of price clustering and trader behavior in the foreign exchange market: evidence from Taiwan, *J. Econ. Finance*, 35, 2011, pp. 198–210.
[25]. Sopranzetti, B. J., Datar, V., Price clustering in foreign exchange spot markets, *J. Financ. Markets,* 5, 2002, pp. 411–417.
[26]. Chen, Z., Li, C., Sun, W., Bitcoin price prediction using machine learning: An approach to sample dimension engineering, *Journal of Computational and Applied Mathematics,* 365, 2020, 112395.
[27]. Hotz-Behofsits, C., Huber, F., Zorner, T. O., Predicting crypto-currencies using sparse non-Gaussian state space models, *Journal of Forecasting,* 37, 2018, pp. 627–640.
[28]. Catania, L., Grassi, S., Ravazzolo, F., Forecasting cryptocurrencies under model and parameter instability, *International Journal of Forecasting,* 35, 2019, pp. 485 – 501.
[29]. Phillips, R. C., Gorse, D., Predicting cryptocurrency price bubbles using social media data and epidemic modelling, *IEEE Symposium Series on Computational Intelligence*, 2017, pp. 1-7.
[30]. Ahmed S, Baig, OmairHaroon, Nasim Sabah, Price clustering after the introduction of bitcoin futures, *Applied Finance Letters,* Vol. 29, Issue C, 2019, pp. 111-116.
[31]. Verma, R., and Soydemir, G., The impact of U.S, individual and institutional investor sentiment on foreign markets, *The Journal of Behavioral Finance,* 7, 3, 2006, pp. 128-14.
[32]. Ikenberry, D., & Weston, J, P, Clustering in US stock prices after decimalization, *European Financial Management,* 14, 2008, pp. 30–54.
[33]. Blau, Benjamin M, & Griffith, Todd G., Price clustering and the stability of stock prices, *Journal of Business Research,* Vol. 69, 10, 2016, pp. 3933-3942.
[34]. Baker, Scott R, and al., Measuring Economic Policy Uncertainty, *The Quarterly Journal of Economics,* Vol. 131, Issue 4, November 2016, pp. 1593–1636.
[35]. Demirand al., Does Economic Policy Uncertainty Predict the Bitcoin Returns? An Empirical Investigation, *Finance Research Letters,* Vol. 26, September 2018, pp. 145-149.
[36]. Baum, L. E, and Petrie, T., Statistical inference for probabilistic functions of finite state Markov chains, Ann, Math, Statist., 37, 1966, pp. 1554–1563.

Appendix

• Economic growth measured as the monthly change in the U.S. industrial production index (IIP) (Fama, 1970).

• Short-term interest rates measured as the yield on the one-month U.S. Treasury bill (Campbell, 1991).

• Inflation measured as the monthly change in the U.S. consumer price index (Fama&Schwert, 1977; Sharpe, 2002)

• Currency fluctuation (Elton & Gruber, 1991) measured as the change in the Turkish lira and U.S. dollar exchange rate.

• Business conditions measured as a default spread, which is the difference in yields on Baa and Aaa corporate bonds (Fama& French, 1988).

• Future economic expectation factor measured as the term spread, which is the difference in yields on tenyear U.S. Treasury bond and three-month T-bills (Fama, 1990).

• Excess return on the market portfolio measured as the value-weighted returns on all NYSE, Amex, and NASDAQ stocks minus the one month T-bill (Lintner, 1965; Sharpe, 1964).

• The premium on a portfolio of small stocks relative to large stocks (SMB) (Fama& French, 1993).

• The premium on a portfolio of high-book-to-market stocks relative to small stocks (HML) (Fama& French, 1993).

• The momentum factor, which is the average return on two high prior return portfolios minus the average return on two low prior return portfolios (Jegadeesh & Titman, 1993).

• Currency fluctuation (Elton and Gruber [1991]), measured as the changes in a fifteen-country trade-weighted basket of currencies.

(018)

Audit and Provenance Model for Transactions in Real Estate Markets through Blockchain-based Supply Chain Management.

O. O. Lawal and N. O. Nawari
Department of Architecture, University of Florida, Gainesville, USA
Tel.: +1 (352)-392-0205, fax: +1 (352)-392-4606
E-mail: o.lawal@ufl.edu, nnawari@ufl.edu

Abstract: The construction industry is one of the least advanced globally in the adoption of digital technology. When coupled with the lack of documentation prevalent in informal real estate markets, especially in developing regions, the result is a construction market where third party verification is unreliable and traceability of components is difficult. The advent of emergent technologies such as Building Information Modelling, Blockchain Technology, Artificial Intelligence, Internet of Things (IoT) - otherwise referred to as Industry 4.0 - have had significant impact on the built environment, leading to practicable real-life applications. There is a plethora of scholarly contributions in the application of blockchain in the built environment. One major aspect of the building and construction industry that is capitalizing on the unique attributes of blockchain is construction supply chain (CSC). This research leverages on recent advancements in blockchain-based supply chain management to propose an auditable provenance model. The concept of trust in a decentralized peer-to-peer transaction is redefined, thereby contributing to the regulation of informal property markets by providing stakeholders with the opportunity to verify the value of construction by-products.

Keywords: Blockchain technology, Construction supply chain, Provenance, Distributed ledger technology, Informal real estate market.

1. Introduction

The advent of new data and information protection laws to guide unsuspecting members of the public makes it imperative to have an accurate system of as-built audit of construction projects. In this regard, the suitability of blockchain technology and its attributes of immutability and decentralization of stored information has been well documented. Supply chain is one of the few areas of construction where blockchain application has gained gradual success [1] and this supply chain accounts for a vital part of every construction. With a blockchain-enabled construction supply chain (CSC), much of the design and construction practices can be streamlined and accelerated [2]. The information architecture of intermediation has been reconfigured to address issues of ineffective information exchanges prevalent in traditional CSC [3]. Considering these, the paper proposes a scalable blockchain-based provenance system from project inception to facility operations which will connect planning, design, operational and transactional information in a distributed and auditable ledger. Information in the construction process is fragmented and leads to inefficiency and poor performance [4]. Therefore, a provenance ledger is proposed which will be accessible to relevant stakeholders.

2. Background

A supply chain encompasses all of the activities that go into the delivery of goods or services, beginning at the earliest stage of creation and ending at the final stage of destruction or extinction [5]. It also referred to the network between companies and their suppliers built for production and distribution of a specific product [6].

Fig. 1 below shows a bibliometric survey of blockchain and construction supply chain management using citespace to visualize co-citation from 2009 when the concept of blockchain was first known to the public, to 2022. Between 2009 and 2022, the most influential studies based on keyword search is *Supply Chain Management*, followed by *Lifecycle Sustainability Assessment*, and *communication channels*. *Threat Model Analysis* was the fourth most impactful area of study, *Traditional Information Systems* was fifth while *Real Time Information* was sixth.

Fig. 1 also shows relationships between the above keywords clusters. There is a strong relationship between the *Supply Chain Management* cluster, *Lifecycle Sustainability Assessment* and *Traditional Information Systems* as the clusters appear to overlap one another.

A major component of audit and provenance is the concept of traceability. Traceability is the ability to follow materials from the beginning of the supply chain to the customer who purchases a product [7]. Traceability is delivered through a sequential interrogation of customer-supplier links up or down a supply chain [8]. Fabrizio Dabenne et al studied traceability issues in food supply chain management and referred to traceability as the ability to guarantee that products “moving” along the food supply chain (FSC) are both tracked and traced [9].

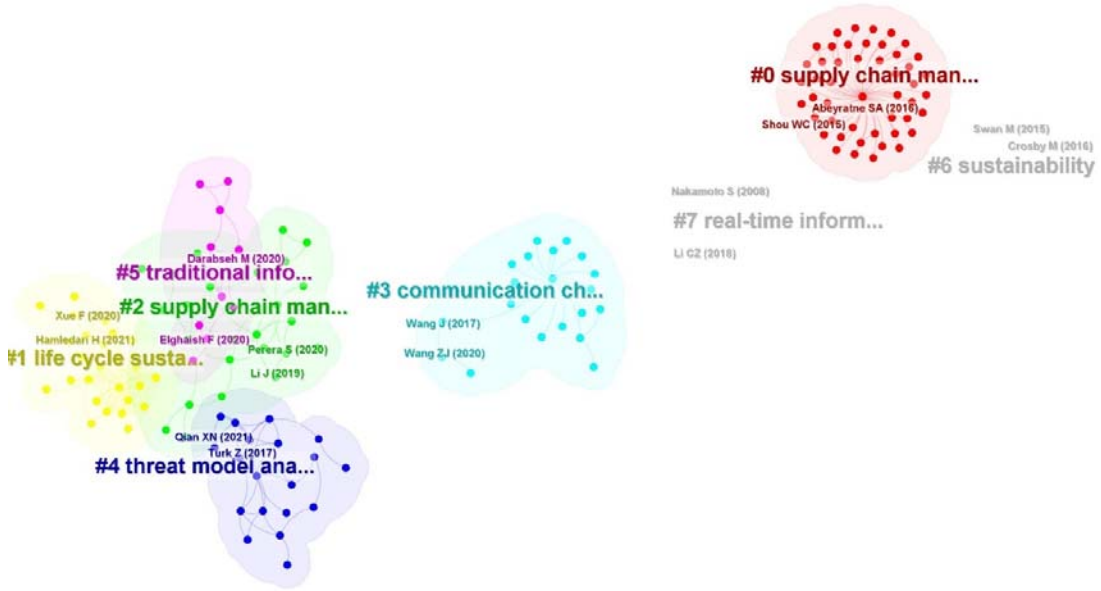


Fig. 1. Bibliometric mapping of research in blockchain and CSC.

Li et al proposed a quality traceability system framework based on Internet of Things and blockchain, positing that it can promote the solution of internal trust and supervision problem [10]. The aim of this study is to develop a model which provides traceability for every single component that makes up the construction of real estate assets.

2.1. Applicability of Blockchain Technology

Blockchain as a concept gained its current popularity after the creation of Bitcoin in January 2009. It was first referred in a white paper published under a pseuodnym - Satoshi Nakamoto [11], however, research into its application as a research area is quite recent. Bibliometric studies by Darabseh & Martins (2020) show the most recent scholarly work in blockchain research in construction dating back to 2017 [12].

Blockchain is an electronic cryptographic ledger which adopts a decentralized network model rather than storing all information in one database, the information is distributed and synchronized across all nodes in the network [13]. The decentralized nature of this database within the network and the interconnection of one block to another makes it immutable. A block contains a category of a record of transactions. New data is entered into a blockchain through a consensus mechanism. Zheng et al (2019) classified blockchains based on three different applications of decentralized degree namely; private, consortium and public blockchains. From private blockchains, to consortium blockchains to public blockchains, the degree of centralization increases [14]. The decentralization in blockchain is in the data storage and recording of data. It is not a homogenous technology, but a network of technology thereby creating a new form of distributed record keeping within a network.

Traceability and record keeping is fundamental to any supply chain management. Therefore blockchain, as distributed ledger technology, can reduce those complex bilateral communications and informational linkages and leakages by providing a single, shared, tamper-evident ledger that records the transactions as they occur [15].

Another profound attribute of blockchain, making it a suitable technology for a revolutionary supply chain management system is in the disintermediation of information. In this new privacy model, the transactions are public while the identities of the transacting parties are protected [16].

3. Proposed Model

Fig. 2 below depicts the proposed approach. The critical component of this new model is the use of smart contracts, executed at various levels of procurement. Smart contracts will automate transactions and provide validation of records in a provenance audit of a construction process, thereby enhancing the traceability and auditability of every component of the construction.

Although blockchain applications have transcended their initial domain as a digital currency, future endeavors from this study will integrate cryptocurrency transactions as a holistic blockchain solution. However, such an application is not within the scope of this study. The provenance model to support the framework in Fig. 2 can be developed in three ways based on their mode of data storage and retrieval namely:

- Two-dimensional provenance model
- BIM-enabled provenance model
- Hybrid provenance model

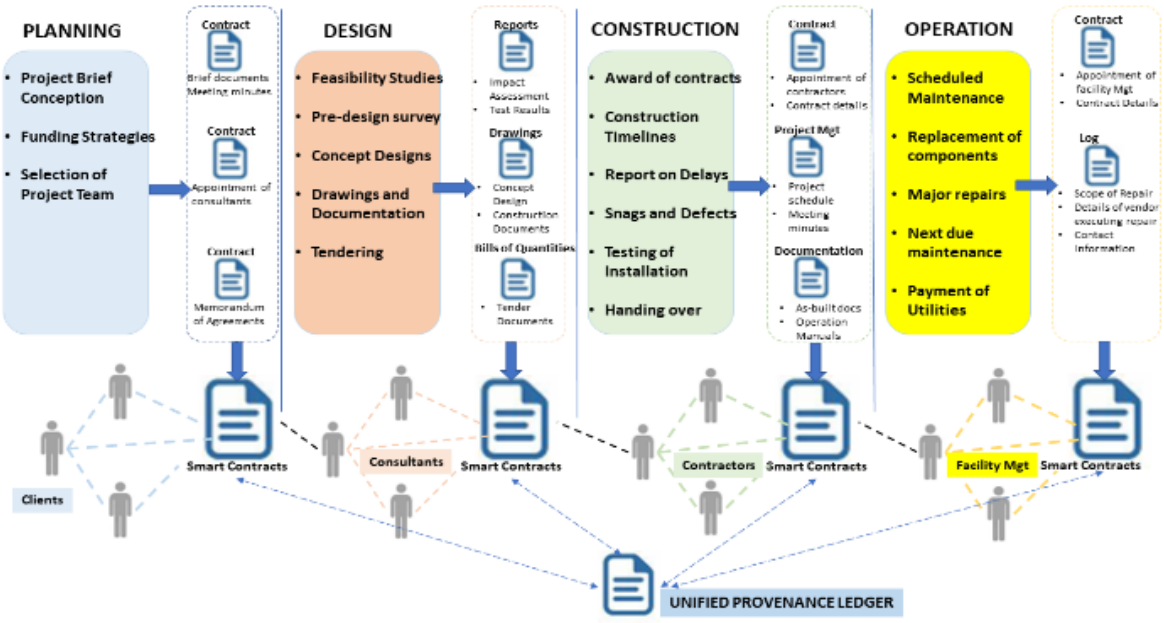


Fig. 2. Proposed Provenance Framework.

Regardless of which provenance model is applicable, the information flow and exchange throughout the project lifecycle is stored on a unified provenance ledger. Smart Contracts – a unique feature of blockchain which can monitor, control commercial transactions and business processes - can be seamlessly embedded into a supply chain [17]. Previous studies have proposed frameworks for Ethereum smart contracts as suitable automation and information storage mechanisms. [17, 18]. This framework also deploys the use of Ethereum smart contracts to manage the automation and business processes involved in the entire real estate value chain.

3.1. Two-dimensional Provenance Model

Paper-based or two dimensional provenance model refers to a model which relies totally on the storage of paper-based documents in a Common Data Environment (CDE). This approach is synonymous with traditional book-keeping. The CDE is similar to any cloud-based application which stores information written into it. As discussed earlier, the use of smart contracts as a platform to automate the supply chain process whilst also recording transactions on an immutable blockchain is what distinguishes this approach from traditional supply chain inventory.

The supply chain framework illustrated in this paper consists of the vertical and horizontal tiers. The vertical tiers represent a category of activities carried out by all stakeholders within a given phase of the project while the horizontal tiers represent a chronological chain of events executed by specific stakeholders across various phases of the project.

Fig. 3 below is an illustration of the information flow, storage, retrieval and traceability pattern of a two-dimensional provenance model, wherein every action is tied to a stakeholder, and the deliverables are recorded and timestamped before being saved in the CDE.

3.2. BIM-enabled Provenance Model

This approach is still largely theoretical as conceptual connections can be found sporadically in literature but its application in practice is not yet widespread [19]. The use of BIM for generation of information has become widespread in the Architectural, Engineering and Construction (AEC) industry in the past decade. Several authors have also proposed the concept of a Common Data Environment (CDE) as a platform for decentralizing information [20, 21], the lack of trust and the need for a trust-building platform to enhance information sharing was cited as the most critical factor in developing an information sharing platform [22].

BIM-based supply chain analysis tool is an example of object-oriented modelling which was proposed for regulating information flows through product modelling [23]. Fig. 4 illustrates the difference between a BIM-enabled provenance model and a two-dimensional provenance model. In this case, the BIM model is an integral part of the CDE. As the BIM model is passed on from one stakeholder to the next, the semantic information gets richer until the building reaches its end of life.

3.3. Hybrid Provenance Model

This is perhaps the most recommended approach as there are still a myriad of factors that limit the optimal deployment of BIM in AEC. [24], [25]. This research leverages existing advancement in blockchain-based supply chain management to develop a highly scalable provenance model.

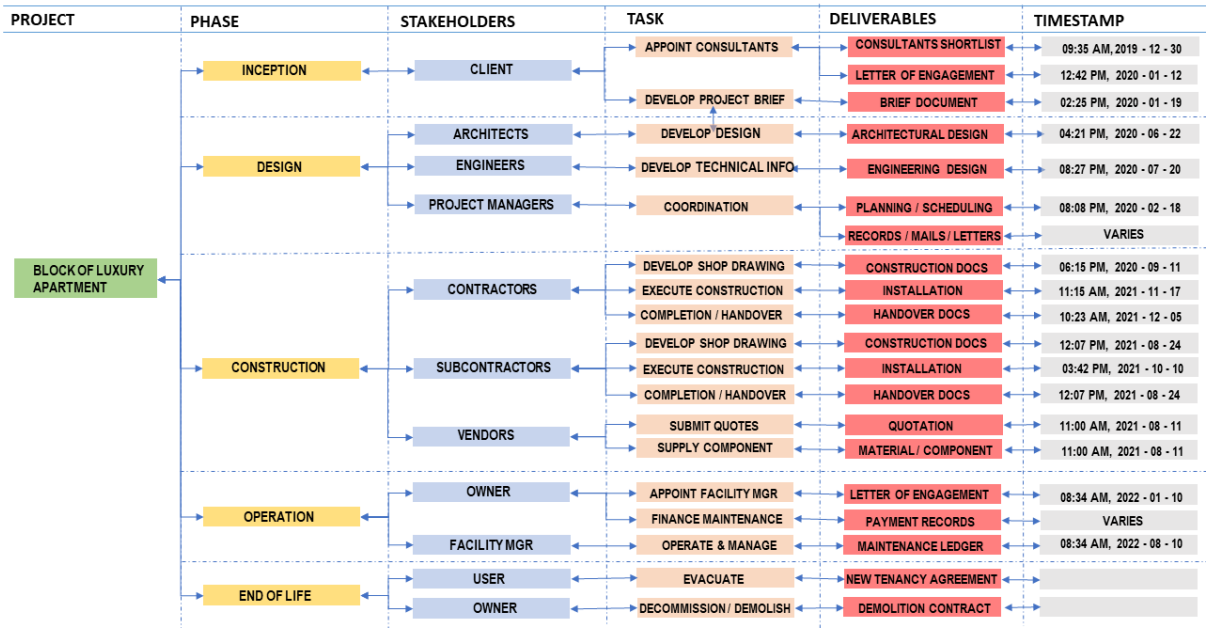


Fig. 3. Two-dimensional Provenance Model.

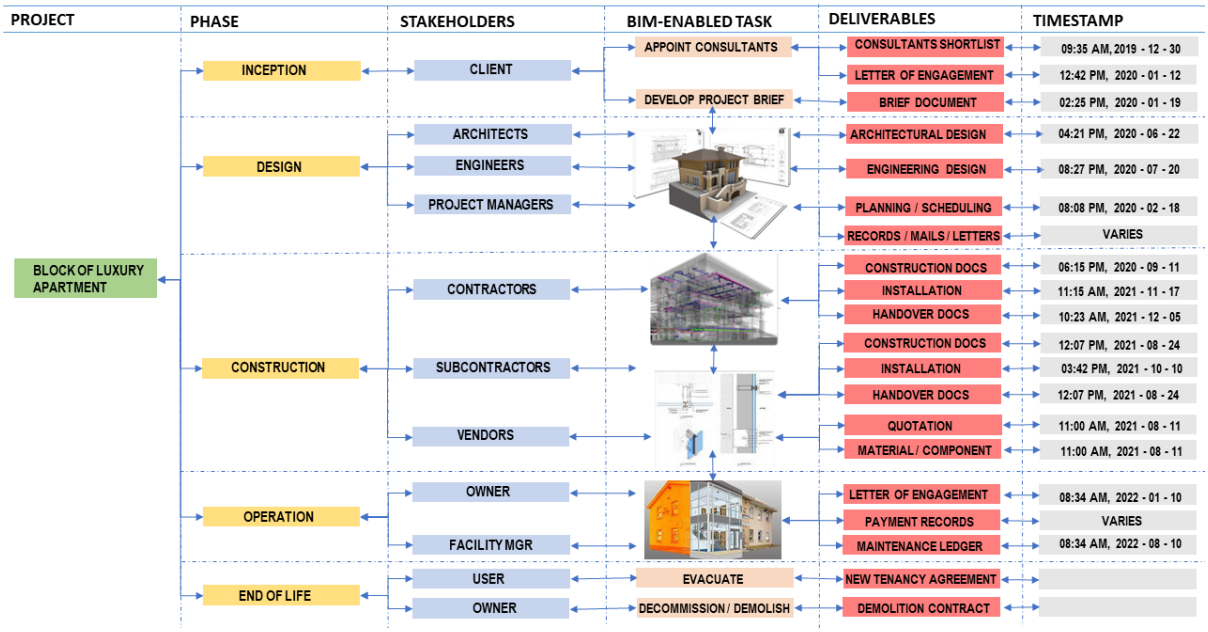


Fig. 4. BIM-enabled Provenance Model.

The proposed model computes various indices from the supply chain which is connected to every level of procurement in the construction. This computation will result in the concept of a 'provenance rating' for every construction, which is simply a measure of compliance of the procurement process to best practices. It also measures the traceability of all physical and non-physical components of the project to their sources. The workings of the provenance rating and traceability will require further research to attain the maturity level needed prior to its implementation.

Fig. 5 shows the framework for a hybrid provenance model. Its scalability is evident in the potential continuous increase in the number of vertical and horizontal tiers and can be suited for different contexts. In a hybrid provenance model, the BIM model and paper-based records are contained in the CDE. Two-dimensional information such as drawings, schedules and quantities can be extracted from the BIM model as deliverables or as a prompt for deliverables from other stakeholders.

4. Conclusion

In social exchange theory, trust has been identified as a critical influence for reducing adversarial behaviors in transactions [26]. Verification of

transactions without needing a centralized authority also addresses issues relating to inter-party trust [2]. Thus, this research explores the potentials of a provenance model that redefines trust and third-party roles in property transactions and any other transaction pertaining to construction. The proposed model combines two distinct theoretical applications of blockchain namely, supply chain management (SCM) and peer-to-peer transactions as seen with cryptocurrency. This new model is of particular importance in informal real estate markets especially in developing regions of the world where documentation is suboptimal, transparency is lacking, and third-party verification is difficult for high value items such as real estate.

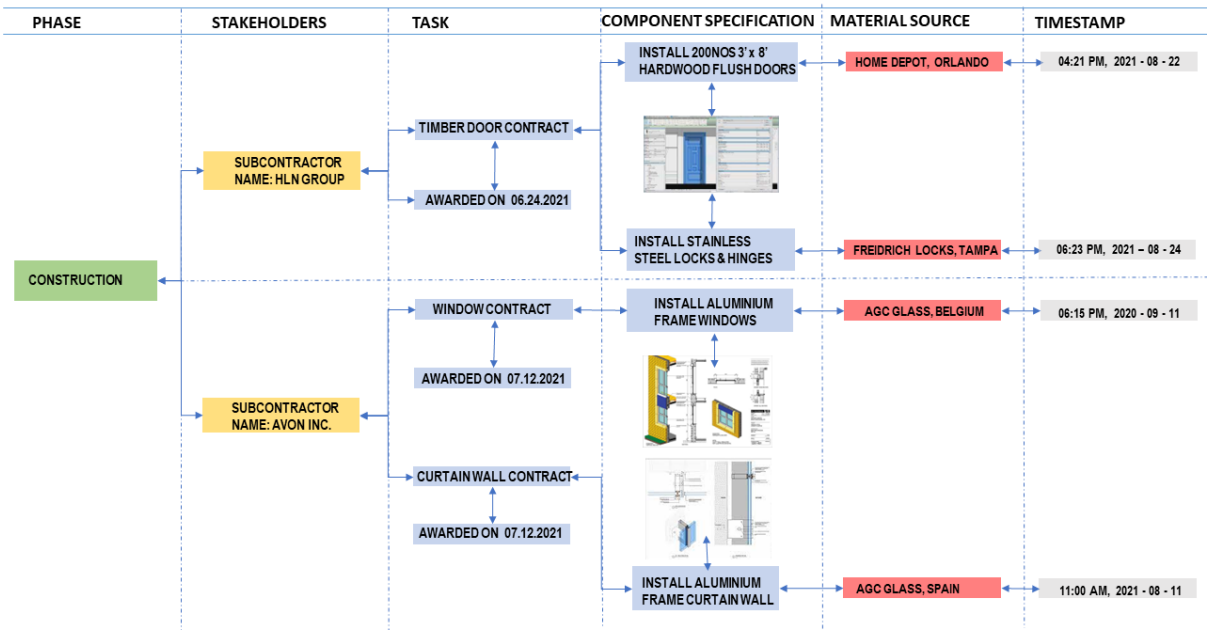


Fig. 5. Hybrid Provenance Model.

Trust is a major concern in 21st century business environment [27]. Therefore, trusted third parties are often hired to bridge the trust gap in numerous real estate transactions where there is need for product verification. Studies have already shown that blockchain can be deployed The blockchain disruptive force is rooted in eliminating intermediaries, allowing peers to transact directly in privacy and removing vulnerability to a controlling party. The result could be the elimination of mediators, enabling a shorter, less costly supply chain [16].

In this study, the unified provenance ledger - which is a by-product of this framework - can provide valuable insights especially with respect to true and transparent property value for real estate stakeholders. This provenance ledger is derived when all active participants in the delivery of real estate products are admitted unto a saleable blockchain network which is coordinated by the owner of the real estate product, for instance, the developer.

Moreover, this study redefines the concept of 'trust' as a major step change in transactional relationships amongst stakeholders [28].

5. Benefits and Future Potential

Although blockchain technology is still in its infancy and the promising prospect of scalability still remains a problem, future studies will benefit from ready-to-use blockchain-enabled applications which can be easily deployed within a number of digital frameworks such as supply chain management. One of the most important services of blockchain to supply chain is the removal of a third party [29].

An effective provenance model for real estate properties can also affect valuation of property and offer a more empirical benchmark for property valuation. It promises a greater degree of processing efficiency, transparency and accountability and reduction of property fraud. [30].

References

[1]. Qian, X., Papadonikolaki, E., Shifting trust in construction supply chains through Blockchain technology, *Engineering, Construction and Architectural Management*, 28, 02, 2021, pp. 584-602.

[2]. Nawari, N. O., Ravindran, S., Blockchain and the built environment: Potentials and limitations, *Journal of Building Engineering*, 25, 2019, 100832.

[3]. Xiong , F., Xiao, R., Ren, W., Zheng, R., Jiang, J., A key protection scheme based on secret sharing for blockchain-based construction supply chain system. *IEEE Access*, 7, 2019, pp. 126773-126786.

[4]. Hijazi, A. A., Perera, S., Calheiros, R. N., Alashwal, A., Rationale for the integration of BIM and blockchain for the construction supply chain data

delivery: A systematic literature review and validation through focus group, *Journal of Construction Engineering and Management,* 147, 10, 2021, 03121005.

[5]. Fitriawijaya, A., Hsin-Hsuan, T., A blockchain approach to supply chain management in a BIM-enabled environment, in *Intelligent Informed, Proceedings of the 24th International Conference of the Association for Computer-Aided Architectural Design Research in Asia (CAADRIA 2019),* 2019, 2, pp. 411-420.

[6]. Buyukozkan, G., Gocer, F., Digital Supply Chain: Literature review and a proposed framework for future research, *Computers in Industry,* 97, 2018, pp. 157-177.

[7]. Traceability: The Next Supply Chain Revolution, *Bain Company,* 2021.

[8]. Sarpong, S., Traceability and supply chain complexity: confronting the issues and concerns, *European Business Review,* 26, 3, 2014, pp. 271-284.

[9]. Dabenne, F., Gay, P., Tortia, C., Traceability issues in food supply chain management: A review, *Biosystems Engineering, 120*, 2014, 65-80.

[10]. Li, T., Xiaoli, Y., Wu, Y., Construction of an Engineering Construction Quality Traceability System Based on the Internet of Things and Block-chain, in *Proceedings of the International Symposium on Advancement of Construction Management and Real Estate*, Singapore, 2020, pp. 761-776.

[11]. Mattila, J., The blockchain phenomenon. The disruptive potential of distributed consensus architectures, *Berkeley Roundtable of the International Economy*, 16, 2016.

[12]. Darabseh, M., Martins, J., Risks and opportunities for reforming construction with blockchain: A biblio, *Civil Engineering Journal,* 2020.

[13]. Sylim, P., Liu, F., Marcelo, A., Fontelo, P., Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention, *JMIR Research Protocols,* 7, 9, 2018, e10163.

[14]. Zheng, R., Jiang, J., Hao, X., Ren, W., Xiong, F., Ren, Y., bcBIM: A Blockchain-Based Big Data Model for BIM Modification Audit and Provenance in Mobile Cloud, *Mathematical Problems in Engineering,* 2019.

[15]. Hewett, N., Lehmacher, W., Wang, Y., *Inclusive Deployment of Blockchain for Supply Chains.* World Economic Forum, 2019.

[16]. Bischoff, O., Seuring, S., August 17, Opportunities and limitations of public blockchain-based supply chain traceability, *Modern Supply Chain Research and Applications,* 2021.

[17]. Yakubu, B. M., Latif, R., Yakubu, A., Khan, M. I., Magashi, A. I., RiceChain: secure and traceable rice supply chain framework using blockchain technology, *PeerJ Computer Science*, 8, 2022, e801.

[18]. Omar, I. A., Debe, M., Jayaraman, R., Salah, K., Omar, M., Arshad, J., Blockchain-based Supply Chain Traceability for COVID-19 personal protective equipment, *Computers Industrial Engineering, 167*, 2022, 107995.

[19]. Papadonikolaki, E., Vrijhoef, R., Wamelink, H., July 13, Supply chain integration with BIM: a graph-based model, *Structural Survey,* 2015.

[20]. Sreckovic, M., Sibenik, G., Sigalov, K., Ye, X., Konig, M., Reitmayer, K., Srećković, M., Šibenik, G., Sigalov, K., Ye, X., König, M., Reitmayer, K., 2021, October, Upkeeping digital assets during construction using blockchain technology, in *Proc. of the Conference CIB W78*, 2021, pp. 11-15.

[21]. Wang, J., Wu, P., Wang, X., Shou, W., The outlook of blockchain technology for construction engineering management, *Frontiers of Engineering Management*, 2017, pp. 67-75.

[22]. Pishdad-Bozorgi, P., Yoon, J., Dass, N., Blockchain-based information sharing: A new opportunity for construction supply chains. *EPiC Series in Built Environment,* 1, 2020, pp. 274-282.

[23]. Papadonikolaki, E., Wamelink, H., Vrijhoef, R., *inteGration in desiGn and ConstruCtion: tHe Case oF bim-enabled sCm, in Proceedings of the 8th International Workshop When Social Science Meets Lean and BIM,* 2016, 37.

[24]. Wu, Z., Jiang, M., Li, H., Luo, X., Li, X., Investigating the critical factors of professionals' BIM adoption behavior based on the theory of planned behavior, *International Journal of Environmental Research and Public Health,* 18, 6, 2021, 3022.

[25]. Park, D., Choi, J., Ryu, S., Kim, M., A User-Centered Approach to the Application of BIM in Smart Working Environments, *Sensors,* 22, 8, 2022, 2871.

[26]. Young-Ybarra, C., Wiersema, M., Strategic Flexibility in Information Technology Alliances: The Influence of Transaction Cost Economics and Social Exchange Theory, *Organizational Science,* 10, 4, 1999, pp. 439-459.

[27]. Ertemel, A. V., Implications of blockchain technology on marketing, *Journal of International Trade, Logistics and Law,* 4, 2, 2018, pp. 35-44.

[28]. Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda, *International Journal of Information Management,* 49, 2019, pp. 114 - 129.

[29]. Ghaemi Asl, M., Adekoya, O. B., Rashidi, M. M., 2022, Quantiles dependence and dynamic connectedness between distributed ledger technology and sectoral stocks: enhancing the supply chain and investment decisions with digital platforms, *Annals of Operations Research*, 8, 2017, pp. 1-30.

[30]. Mendi, A., Cabuk, A., Blockchain applications in geographical information systems. *Photogrammetric Engineering Remote Sensing,* 1, 86, 2020, pp. 5-10.

(023)

Blockchain Impacts on Auditing

C. Moreira and F. Rodrigues
Lisbon Accounting and Business School, Av. Miguel Bombarda, 20, 1069-035 Lisboa, Portugal
Tel.: + 351924045803
E-mail: claudiamoreirastl@gmail.com, fjrodrigues@iscal.ipl.pt

Abstract: Globalization and technological advancements are causing changes in the business sector, which are motivating organizations to embrace revolutionary tactics in culture, structure, and processes to improve their ability to adapt to changes and difficulties. Since it assists management in making decisions, auditing is a crucial component of businesses. In this regard, it is crucial that it stay up with technology advancements in order to be able to quickly address organizational management needs and guarantee the consistency of operations. Technology is used as a support tool for the execution of the required procedures, and the audit activity is also continually evolving. Blockchain is the disruptive technology that will likely be used in the near future, despite its complexity. Due to the immutability and decentralization that the technology enables, the promise of improving processes' security, dependability, and transparency constitutes a huge advancement.

Keywords: Audit, Information systems audit, Blockchain, Information systems, Technological evolution.

1. Introduction

The transformations in the business world, arising from globalization and technological development are driving factors for companies to adopt revolutionary strategies in culture, structure, and processes, with respect to innovation, to increase their responsiveness to change and associated challenges.

Organizations are continuously focused on the emergence of possible opportunities that may lead to increased operational efficiency and effectiveness, to increase business productivity and profitability. In this sense, given the technological evolution, the interest in implementing technologies that allow the automation of processes and, consequently, that can provide more interesting operational results, is transversal in the business world.

As an integral part of the organizations, auditing assumes a preponderant role since it supports the management's decision-making process. In this sense, to remain timely, it is essential that it keeps up with technological evolution to be able to respond in a timely manner to the needs of organizational management, ensuring the reliability of processes.

Within the exponential technologies, blockchain is pointed out as being the revolution of the digital market, given its potential for disruption and application possibilities that cover a wide range of markets. The implementation of blockchain not only has implications for companies themselves, but also represents a profound impact for the audit profession, as the way in which financial statements are prepared and audited may also change.

Originally created in 1991, blockchain has gained greater relevance since 2009, in the context of cryptocurrencies, since it has served as the basis for bitcoin, an avant-garde alternative to financial transactions.

Also classified as the "future of the internet", blockchain, in a broad sense, is a decentralized paradigm that creates consensus and trust between parties, without the intermediation of third parties.

This technology has allowed, for the first time, the validation of events and transactions by several unknown parties, regardless of their geographical location, through consensus mechanisms, without the need for intervention by a central external authority, thus enabling the emergence of initiatives guided by immutability, transparency, security, and decentralization.

2. Objective

In global terms, the purpose of the present article is to demonstrate the possible impacts that blockchain technology may have on audit activity. In parallel, we seek to understand the perceptions of auditors regarding the effects of implementing this technology, both in the different phases of the work and in the future of the auditing profession.

It is also intended to identify, from the perspective of the surveyed professionals, the challenges inherent in the adoption of blockchain, as well as the benefits and disadvantages associated with it.

The results obtained from the survey of auditors in Portugal reveal that blockchain does have the ability to impact audit processes, however, it is imperative to deepen the knowledge of the technology and disseminate it, mainly among auditors.

Despite the benefits underlying the implementation of this technology, the paradigm shift in auditing is not without its obstacles and challenges and represents a complex picture. Because it is an innovative technology, blockchain is still in a phase of expansion and development and will naturally undergo major changes in the future.

3. Novelty

Blockchain technology is seen as one of the most instigating technologies of profound transformations in the digital world and for that reason the interest and investment in blockchain, given its enormous potential, is increasing. Blockchain could play a leading role in the transition to a new era that will transform the landscape of companies and society, in general, and the auditing sector, in particular.

Scientific and technological development is extremely important for any country and for that reason, this article also aims to generate knowledge that is useful for science and technology.

Given the topicality and innovation of the topic, this investigation also seeks to identify the main challenges and restrictions to the development of the study, as well as to launch interest in future research lines.

4. State-of-the-art

4.1. Limitations Underlying an Audit

The development of the business market depends, to a large extent, on the quality of the financial information disclosed, which must be reliable, relevant, accurate, comparable and capable of reflecting the true and appropriate image of the Organization.

In this context, the audit, as it results in an independent opinion, based on a careful and sustained analysis of all materially relevant aspects contained in the Financial Statements (FS), represents an important component in establishing trust between the related and interested parties of a business .The auditor is responsible for assessing the risks of material misstatement and must consider the origin of incorrect information and data, when they exist, as they may originate from an unintentional operational error or fraud resulting from collusion. These inconsistencies, despite being detectable, represent a risk to the auditor's work [3].Carrying out an audit, due to its scope and incidence, does not allow for the analysis and verification of all the documentation and transactions that took place. In this sense, the traditional term Audit Expectation Gap refers to the need for compliance and effective risk management. [1] states that the audit activity has the following limitations:· Reasonable cost – resources are limited, so the audit is carried out by sampling; Period of time – the opinion is issued, as a rule, up to 3 months after the end of the financial year, which may affect the analysis of events subsequent to the balance sheet date;·Accounting estimates – as these are estimates, their outcome is not predictable;· Accounting criteria – accounting standards allow the adoption of different accounting criteria and understandings;· Determining materiality – requires a high degree of professional judgment;·Audit report – standardization of opinion models may not reflect the real complexity of the work performed; Audit risk – auditor's susceptibility to issue an inappropriate opinion. Professional judgment, as it involves the application of competence and knowledge by the auditor on a given matter, is more susceptible to inaccuracies and, for this reason, may jeopardize the expressed opinion and, consequently, the reliability of the financial statements. Although international auditing standards do not make any direct reference to professional judgment, ISA 320 states that the auditor must take into account materiality and its relationship with audit risk, when carrying out their work.

4.2. Technological Evolution in the Context of Auditing Activity

The Information Age – also known as the Digital Age or Technological Age – emerged at the end of the 20th century, following the digital and technological transformations that occurred at a global level. Characterized by the popularization of computers and the internet, this period was significant for the automation process and for the awakening of the importance of the digital presence. In the current information revolution, which is increasingly crucial for the correct functioning of Organizations, the way in which information is collected, treated and made available has significant impacts on the effectiveness and efficiency of management and on the success of the Organization. “A company's management body will be the more efficient the greater the quantity and quality of useful information that it can have in a timely manner” [8]. With the development of Organizations and, consequently, the processes adopted, the amount of information that is generated and processed gradually increases, making the information handling process more complex [16]. With the development of Information Technologies (IT) and management techniques, companies now have the possibility of accessing computational tools that speed up the process of structuring and integrating data relating to their operations, increasing the availability and quality of information. The increase in the ambiguity and competitiveness of the markets has stimulated the creativity and proactivity of companies in the search for more effective and efficient uses of IT, given the important role they play in this conjuncture of corporate restructuring. There are several benefits associated with its use, namely, “in terms of saving time, improving quality in the workplace, the ability to store information or the possibility of working in a network” [6]. The need verified by companies to reduce costs also influences investment in IT, with the aim of optimizing operational processes. Information is indispensable for the success of Organizations and the technologies that process this information are essential in contributing to the improvement of all procedures, leading to the objectives and desired levels of competitiveness.

4.3. Relationship between Information Technologies and Auditing

The evolution of IT and the consequent continuous implementation of new Information Systems (IS) has significantly affected the business environment in virtually all areas of activity, from which auditing is no exception. The complexity and predominance of the IS translated into new requirements for the audit sector, since they oblige them to be increasingly monitored and audited. In response to the changes verified in the sphere of auditing, the traditional model used has undergone changes with regard to the way in which the FS are prepared and used, so it had to be adjusted to achieve the reality of continuous auditing. Although IT has significantly influenced the auditing profession in recent decades, the purpose of audits remains unchanged. However, it is crucial to adapt the procedures and methods that the audit should use to adjust to this new context. It is a reality that IT is accessible to any company, regardless of the sector of activity in which it belongs, since there are several computer programs that can be adapted to the size of each Organization. Thus, the audit must also be adjusted so that it is possible to develop the necessary work given the complexity of the companies. Given current circumstances, auditors are required to express a true and appropriate opinion based on large volumes of information and with a complex analysis framework. It is using IT that the auditor will be able to analyze this volume of data effectively and efficiently. The use of IT in an audit process makes processes that include administrative and routine tasks more efficient and increases the ability to work with high volumes of data. The importance that IT has in audit methodologies is evident, and it is crucial to monitor their evolution with regard to the acquisition of skills for the performance of an effective and efficient audit, which is essential due to the high amount of information that is computer generated.

4.4. The Main Features of Blockchain Technology

Nowadays, we can observe the exponential evolution of technology, from the creation of robots with artificial intelligence systems to the emergence of applications that have highlighted the concept of disruption. However, these innovations can be completely surpassed, in terms of disruption, by blockchain, also known as Distributed Ledger Technology, which has received immeasurable interest globally. The first suggestion of blockchain came in 1982 by the cryptographer David Chaum, but the use of technology became evident in the midst of the financial crisis, in 2008, as a support for bitcoin, whose disclosure was made by the pseudonym Satoshi Nakamoto in the article “Bitcoin: the peer-to-peer electronic cash system” [13]. This article focuses on a proposal for a version of electronic money that allows online transactions to be carried out directly between the parties without the intervention of third parties, namely financial institutions, with the aim of decentralizing payment over the network, which is clearly contrary to the traditional system. Nakamoto sought to demonstrate the viability of a payment system based on cryptographic technology that would guarantee the authenticity of electronic transactions, solving the problem of duplication of transactions – double-spending. In a simplified way, the double-spending problem refers to the possibility of digitally using the same payment unit in different transactions, resulting in a kind of “counterfeiting” of money through its multiplication. Blockchain technology emerged as an alternative to the traditional model of data storage and digital operations. According to [10], this technology does not depend on a central or hierarchical entity responsible for intermediation, that is, it is the “users who, together, control the information that enters this [blockchain network]”. Corroborated by [9], blockchain has allowed unknown people, from different parts of the world, to reach a consensus on the occurrence of a particular transaction or event without the need for intervention by a regulatory entity. Through the various existing suggestions to conceptualize the blockchain, it can be defined as a distributed ledger whose main purpose is the registration and respective verification of the information validated by it, without the intervention of any central authority, which is It is admissible to add items, but there is no possibility of changing the data entered or modifying their order [2]; [12]. According to [17] it is an efficient, reliable and secure system for recording financial transactions. The main difference compared to existing tools relates to the fact that the blockchain promotes the disintermediation and decentralization of all transactions, regardless of their category, not allowing their modification or manipulation, resulting in an immutable system, therefore, more reliable. Blockchain, therefore, deserves all the attention and although it is not yet possible to conclude how the technology will impact the business world, it presents promising opportunities for the future and has the potential to profoundly transform the panorama of Organizations and the society. In terms of organization, the blockchain is structured chronologically in the form of chained blocks, that is, in a continuous chain of blocks, which are linked and protected through cryptography, whose only possible operation is to add a new block at the end of the structure, which, once registered, does not allow any changes to be made. The first block in the chain is called the “genesis block”. Upon block validation, it is added to the end of the blockchain, as shown in Fig. 1, with the information ordered sequentially and chronologically.

Once introduced and validated, the data of any block cannot be changed or cancelled, as they become immutable. All records created and entered the blockchain are made publicly available to the entire network. According to [12], each block belonging to the blockchain is composed of two areas: header and transactions. The information contained in the header, and which allows validating the conformity of the blocks is the hash, a unique and exclusive fingerprint

assigned to each block when it is created, which works as a link between the previous and subsequent blocks and the timestamp, which records the date, time and data of the transaction. This interactive process allows confirming the integrity of the entire network, through the match with the previous block and so on until the initial block. Each of the blocks includes an identification number, called a hash, as well as, it has the information of the previous block, ensuring the network sequentially and the immutability of the blocks, as exemplified in Fig. 2.

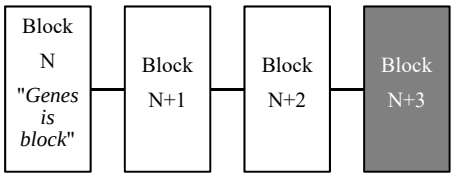


Fig. 1. Insertion of a new block to the blockchain. Source Adapted [12].

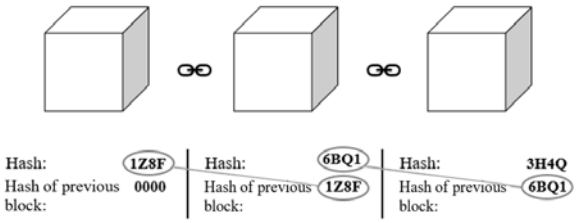


Fig. 2. Block chaining. Fonte [14].

The immutability property of the blockchain comes from the chained structure and the information made available about the blocks, since the fact that each block contains the hash of the header of the immediately preceding block makes any intention of changing each of the blocks difficult, as it would be necessary to equally change all subsequent blocks, which would require a very robust processing capacity.

4.5. Implications for the Audit

The digital transformation, added to the evolution of the global economy, causes considerable changes in the corporate world. The emergence of new negotiation possibilities with more complex transactions is increasingly common and, therefore, the risks associated with the dissemination of mistaken and undue information are higher. In this context, the audit assumes a fundamental role, by allowing the auditors to issue an independent opinion on the FS, in order to demonstrate the credibility of the Organization before the interested parties. Currently, auditing procedures are quite demanding and time-consuming, making it impossible to carry out audits in real-time, which ends up making decision-making difficult in the face of possible bias resulting from obsolete information. Thus, in order to follow the evolution of the business, it is important that new methodologies are adopted in audit work, which allow for more timely and proactive analyses, given the constant need to carry out audits of the DF. Blockchain technology, according to [18] has the possibility of causing changes in "all registration processes, including the way transactions are initiated, processed, authorized, recorded and reported. This generates changes in business models, with potential for greater standardization and transparency in communication and accounting". In this context, according to [19], blockchain technology may induce broad transformations in the audit sector, given its potential for creating more global, transparent and decentralized networks. Although this technology may cause changes to the approach currently used by auditors, blockchain will not replace professional judgment and it will be imperative to assess the reliability of the consensus protocol for each specific blockchain. For [5], auditors should seek to ensure that they have the necessary technical skills and that they take advantage of new technologies to leverage new available blockchain resources to make the audit process more efficient. There are several benefits pointed to the use of blockchain in the audit activity, according to [18], namely:

Access to information and transparency: possibility of storage in different locations and verification of transaction history, increasing security and speed in accessing information. Trust and data security: the fact that data is virtually immutable and verification mechanisms increase trust and control over it. Predictive Data Capacity: In addition to higher data quality, transaction history increases the predictive capacity of the data. Efficiency: cost reduction due to the need for less inputs and reduction of human errors. Data quality: Immediate availability, ease of transaction and data reliability provide an improvement in data quality.

In the research published by [7], it is mentioned that the implementation of the blockchain could contribute to gains in efficiency and effectiveness of audit work, by reducing time, cost and complexity, insofar as it would facilitate access to customer data and would also allow the performing audits in real-time. Corroborated by [11], the adoption of blockchain will translate into cost savings, as it allows for a better allocation of resources, given that the process of collecting and verifying evidence will require fewer resources compared to the current procedure. On the other hand, blockchain offers the opportunity to streamline audit processes, through the standardization and transparency of information and allows increasing the quality of reports, since it allows access to unalterable audit evidence [15]. [18] also sought to demonstrate the audit procedures that could be impacted:

Access to information and transparency: the blockchain would facilitate the availability of information, allowing the auditor to observe all the actions recorded by the technology, which would allow

for a faster understanding of the entity and its surrounding environment. Trust and control: blockchain would increase trust and control of accounting data, providing access to reliable information and enabling more timely analyzes of the internal controls established by the company. Data's predictive capacity: the transaction history increases the data's predictive capacity, allowing the auditor to obtain the necessary understanding of operations, business and control risks, identify abnormal operations/balances and analyze the evolution of certain accounts. Efficiency: Could eliminate many manual data extraction and audit preparation activities, which require a lot of work and time. Accelerating audit preparation activities would increase reporting efficiency and effectiveness. Data quality: the insertion of records in the blockchain increases the quality, trust and control of the data, which gives the auditor access to the entire history of information, enabling a safer and higher quality analysis, given the access to unalterable evidence.

In this scenario, the analysis of the assertions underlying the FS presented by the management could be carried out in an automated way. In addition, the fact that the blockchain allows testing of the entire population would promote the transfer of analyzes and tests by sample, which, in itself, would essentially improve the relationship between the risks and limitations implicit in audit work. Additionally, the blockchain's capacity to work in real time will allow continuous and more regular assessments to be carried out over time, as opposed to the usual retrospective assessments carried out at the end of each period. The automation of verification processes and the wide range of analyzes will lead to gains in effectiveness and efficiency in audit procedures, either through costs or through the reduction in the time required for execution. According to [4], the fact that data storage is carried out transparently and without ambivalence, the process of carrying out audits would be easier. While traditional auditing procedures remain essential, the use of blockchain will have a significant impact on business processes. Thus, it is crucial that auditors seek to obtain a greater understanding of the technology, since the evolution of procedures is guaranteed and it will certainly be necessary to re-qualify the skills they need to have. In this sense, it is necessary for a paradigm shift to occur, in which audit professionals are encouraged to abandon the traditional model of compliance verification in favour of new challenges that add value to the Organization, in order to respond to current risks and emerging. In the future, according to these assumptions, audit work is expected to be less exhaustive, however, more assertive.

5. Method

The first phase of the construction of this research consisted of a thorough and careful literature review to identify theories, opinions, and scientific evidence on the issue under study. Next, we conducted a questionnaire survey to auditors in Portugal, in order to support the results of the empirical study.

The questionnaire was sent out to a sample of 1483 respondents, to which 242 responses were obtained, corresponding to a response rate of about 16.

6. Conclusions

The use of blockchain technology may have strong contributions to the improvement of auditing processes. In a hypothetical operational context, through blockchain, the auditor will be able to access data practically in real time, thus obtaining the necessary information for analysis and audit evidence, in a timely and recurrent manner. In this way, audits that are currently performed retrospectively could begin to be analyzed in a more continuous way over time.

In this sense, the possibility of speeding up audit tasks may also allow the reduction of costs associated with audits, by mitigating the time gap existing in an audit process, particularly from the preliminary stage to the issuance of the opinion.

Although blockchain presents some complexities, this is the disruptive technology that is expected to be implemented soon. The possibility of making processes more secure, reliable, and transparent, due to the immutability and decentralization that the technology offers, represents a significant evolution.

References

[1]. Almeida, B. J. M., Manual de auditoria financeira: Uma análise integrada baseada no risco (3ª ed.), *Escolar Editora*, 2019.

[2]. Antunes, L., Tecnologia blockchain e criptomoedas. *Plátano Editora,* 2019.

[3]. Attie, W., Auditoria – Conceitos e aplicações (7.ª ed.), *Editora Atlas*, 2018.

[4]. Bartling, S., Fecher, B., Blockchain for science and knowledge creation, 2016. https://zenodo.org/record/1196756/files/Blockchain%20for%20Open%20Science%20and%20Knowledge%20Creation.pdf

[5]. Bonyuet, D., Overview and impact of blockchain on auditing, *The International Journal of Digital Accounting Research*, 20, 2020, pp. 31-43.

[6]. Borralho, C., Sistemas de planeamento e controlo de gestão, *Edições Sílabo*, 2018.

[7]. Brender, N., Gauthier, M., Morin, J-H., Salihi, A., The potential impact of blockchain technology on audit practice, Journal of Strategic Innovation and Sustainability, 14, 2019, pp. 35-59.

[8]. Costa, C. B., Auditoria financeira – Teoria e prática (12ª ed.), *Editora Rei dos Livros,* 2018.

[9]. Filippi, P., D., Wright, A., Blockchain and the law: the rule of code, *Harvard University Press*, 2018.

[10]. Freire, J. P., Blockchain e smart contracts – Implicações jurídicas, *Almedina*, 2021.

[11]. Liu, B., Yu, X. L., Chen, S., Xu, X., Zhu, L., Blockchain based data integrity service framework for IoT data, in *Proceedings of the 24th IEEE*

International Conference on Web Services (ICWS), 2017, pp. 468–475.
[12]. Martins, P., Introdução à blockchain, *FCA*, 2018.
[13]. Nakamoto, S., Bitcoin: A peer-to-peer electronic cash system, 2008, Available at: https://bitcoin.org/ bitcoin.pdf, Accessed 4 November 2019.
[14]. Pacheco, A., V., Bitcoin (6.ª ed.), *Editora Self*, 2021.
[15]. Raphael, J., & Steele, A., The impact of blockchain technology on audit: Audit opportunities in cognitive, blockchain and talent, 2020, https://www2.deloitte. com/us/en/pages/audit/articles/impact-of-blockchain-inaccounting.html.
[16]. Santos, V., Criatividade em sistemas de informação, *FCA*, 2018.
[17]. Silva. C. F., & Moro. S., Blockchain technology as an enabler of consumer trust: A text mining literature analysis, *Telematicsand Informatic*, 60, 2021.
[18]. Simões, M. P. A., Cavalcanti, J. A., Melo, J. F. M., Reis, C. Q., Benefícios do uso da tecnologia blockchain como instrumento para a auditoria contábil, *Revista Ambiente Contábil,* 13, 1, 2021, pp. 39-53.
[19]. Tapscott, D., & Tapscott, A., Blockchain revolution: How the technology behind bitcoin and other cryptocurrencies is changing the world, *Penguin Books,* 2018.