HOCHSCHULE MITTWEIDA
University of Applied Sciences

Wissenschaftliche Berichte | Scientific reports

Konferenzband zum Scientific Track der Blockchain Autumn School 2023

Nr. 2, 2023

Konferenzband zum Scientific Track der Blockchain Autumn School 2023
Impressum

Herausgeber:
Hochschule Mittweida
University of Applied Sciences
Der Rektor
Prof. Dr. rer. oec. Volker Tolkmitt
Der Prorektor Forschung
Prof. Dr.-Ing. Uwe Mahn

Redaktion dieser Ausgabe:
Hochschule Mittweida |Referat Forschung
University of Applied Sciences

Leitung:
Prof. Dr.-Ing. Andreas Ittner
Dr. Dipl.-[Wi.] Ing. Volker Wannack

Kontakt:
Hochschule Mittweida
University of Applied Sciences
Referat Forschung
Postfach 1457
D-09644 Mittweida

Tel.: +49 (0) 3727 / 58-1264
Fax: +49 (0) 3727 / 58-21264
forschung@hs-mittweida.de
www.forschung.hs-mittweida.de

ISSN 1437-7624

Erscheinungsweise:
Unregelmäßig

Auflage:
Belegexemplare

Förderung:
Die Hochschule wird mitfinanziert durch Steuermittel auf der Grundlage des vom Sächsischen Landtag beschlossenen Haushaltes.

Bundesministerium für Bildung und Forschung

Projektträger Jülich
Forschungszentrum Jülich

Foto Titelseite: Hochschule Mittweida

Bildnachweise werden direkt am Foto bzw. im jeweiligen Artikel aufgeführt.
Im Scientific Report gelten grammatikalisch maskuline Personenbezeichnungen gleichermaßen für Personen jeglichen Geschlechts.

Die Scientific Reports/Wissenschaftliche Berichte als Wissenschaftliche Zeitschrift der Hochschule Mittweida - University of Applied Sciences lösen die bisherigen Scientific Reports mit allen Volume I-III ab und erscheinen mit Nr.1, 1998 ab November 1998 in neuem Layout und in neuer Zählung.

Für den Inhalt der Beiträge sind die Autoren verantwortlich.

Im laufenden Kalenderjahr sind bereits erschienen:
Nr. 1, 2023
Entwicklung hybrider Arbeitssysteme

SCIENTIFIC REPORTS | WISSENSCHAFTLICHE BERICHTE
The main aspect of the Scientific Reports is to promote the discussion of modern developments in research and production and to stimulate the interdisciplinary cooperation by information about conferences, workshops, promotion of partnerships and statistical information on annual work of the Hochschule Mittweida (FH) University of Applied Sciences. This issue will be published sporadically. Contributors are requested to present results of current research, transfer activities in the field of technology and applied modern techniques to support the discussion among engineers, mathematicians, experts in material science and technology, business and economy and social work.

Die Scientific Reports der Hochschule Mittweida sind online verfügbar unter:
www.forschung.hs-mittweida.de/veroeffentlichungen/scientific-reports

Eine Veröffentlichung einzelner Beiträge erfolgt entsprechend der Open Access Strategie der Hochschule Mittweida auf dem Hochschulschriftenserver: https://monami.hs-mittweida.de

INHALTSVERZEICHNIS

A Systematic Literature Review on Blockchain Oracles: State of Research, Challenges, and Trends

Viola Süß[1], Bogdan Franczyk[1,2]

[1)] Leipzig University, Business Information System Institute, Leipzig, Germany

[2)] Wroclaw University of Economics and Business, Center for Intelligent Management Systems, Wroclaw, Poland

Abstract

To enable data exchange between the Blockchain protocol (on-chain) and the real world (off-chain), e.g., non-Blockchain-based applications and systems, a software called Oracle is used [3]. Blockchain oracle is an important component in the use of off-chain data for on-chain smart contracts. However, there is limited scientific literature available on this important blockchain topic. Therefore, in this paper, a novel systematic literature review based on intelligent methods, e.g., information linking, topic clustering and focus identification through frequency calculations, is proposed. Thus, the current state of scientific research interest, content and challenges, and future research directions for blockchain oracles are identified. This paper shows that there is little unbiased literature that does not call oracles a problem. From the results of this new literature review framework, relevant areas of data handling and verification with blockchain oracles are identified for future research.

Keywords: Blockchain Oracle; Smart Contract; Bibliometric analysis; Intelligent methods.

1. Introduction

Distributed ledger technology, particularly blockchain technology, is ready to complete the status of technology testing and gradually be applied in real-world, economic business cases [48]. To exchange data between off-chain and on-chain, a type of translator between the different data protocols is needed. This connecting infrastructure is called “blockchain oracle” and regulates the exchange of data between off-chain applications and on-chain transactions for smart contracts [3]. Smart contracts are simple program code that can process transactions on blockchains automatically [72]. From a technical perspective, oracles are at an intermediate stage where they often lack the basic characteristics of a blockchain such as decentralization, tamper resistance, and transparency [1]. And so, a regular oracle passes incoming data from the non-blockchain environment to the chain without any prior verification of correctness, where smart contracts access the data directly without verifying. Thus, many oracles pose a security and trust problem. This issue is also known as the "oracle problem" [16].

The objective of this paper is to identify the current state of research, content and challenges, as well as future research directions for blockchain oracles using a systematic literature review. The structured literature search uses an iterative [83] and linking procedure for the search [89], and the results are completed with intelligent methods. As a result of the literature analysis, overlapping topics are identified and clustered accordingly [88], and the focus of each publication is determined for content classification [66]. The software Litmaps is used for the graphical representation and maps a network of all authors of the literature retrieved. The goal is to identify areas of blockchain oracle research that are poorly covered or unaddressed.

The paper is structured as followed: After the introduction in section 1, a literature review is conducted in section 2 to identify the main areas. Based on this, the results of the literature review are subjected to a bibliometric analysis in section 4. This is done using intelligent methods, namely information linking, topic clustering, and focus identification. Finally, section 5 provides a comprehensive discussion of the results and identifies potential research gaps.

2. Literature review approach

The systematic literature search (Fig. 1) is conducted according to vom Brocke et al. [83]. The relevant search strings are "*blockchain oracle*" and "*decentralized oracle*". Not mentioning blockchain would distort the search results. The search strings are searched in the title and abstract. Search delimitation is made by using the Boolean operators ‘AND’ and ‘OR’. For this purpose, five scientific databases, IEEEXplore, arXiv, MDPI, Science Direct and Springer Link, have been queried with the given search string. The syntax of the search term query varies depending on the requirements of each database (Tab. 1).

Database	Search String
IEEEXplore	("Document Title":blockchain oracle OR decentralized oracle AND "Abstract":blockchain oracle OR decentralized oracle)
arXiv	title="blockchain oracle"; OR title="decentralized oracle"; AND abstract="blockchain oracle"; OR abstract="decentralized oracle"
MDPI	advanced=(@(title)"decentralized oracle")|(@(title)"blockchain oracle"@(abstract)"decentralized oracle")|(@(abstract)"blockchain oracle")
Science Direct	title, abstract, keywords="blockchain oracle" OR "decentralized oracle"
Springer Link	title="blockchain+oracle"+or+"decentralized+oracle"

Tab. 1: Used databases and search strings.

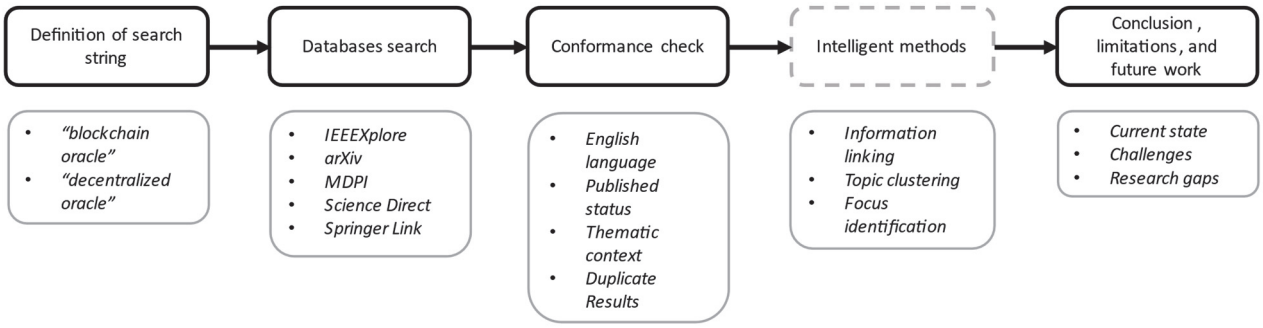

Fig. 1: Strategy of the systematic literature review.

The retrieved literature is checked for conformance, using only published English-language articles. Additionally, unfitting thematic results and duplicates are excluded. All remaining articles are analyzed via the following intelligent methods:

- **Information linking** is done by searching backward and forward through the relevant articles [89] to identify other relevant publications and establish a connection between the authors.
- **Topic clustering** examines content and topics for similarities and combines them through data abstraction. The results are presented in thematically hard clustered terms to identify and analyze important points in research [66]. The cluster terms result from thematic overlaps in the literature.
- **Focus identification** shows the frequency of content of the topics covered in the literature. This indicates statements about the importance of certain focal points as well as missing research.

After the literature analysis and consolidation, the results of the intelligent methods are evaluated. The results are processed in the conclusion, limitations, and future work sections. This is done by creating a research agenda that highlights the current state as well as future research. In an iterative process, the literature review cycle can then be repeated with more specific terms [83].

3. Literature review results

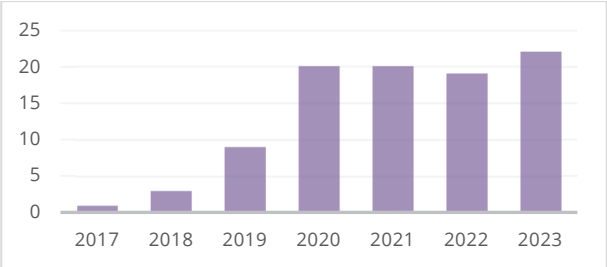

Fig. 2: Distribution of the published publications by year.

Following the strategy shown in Figure 1, a total of 85 scientific publications were found through the database search and after the conformance check. Nine more publications are added by the backward and forward search. A total of 94 published papers were found in the period from 2017 to 2023. Figure 2 shows the frequency distribution of the literature ordered by year of publication. While only one oracle-specific paper was published in 2017 [75], the number rises to a plateau of 20 publications in 2020 to 2023.

4. Intelligent methods analysis

The results of the systematic literature review are presented in this section with a bibliometric analysis using the intelligent methods: graphical information linking, overarching topic clustering and focus identification.

4.1. Information linking

The backward and forward search of information linkage has already been used for literature search. Some overlaps in subject areas and authors are found. Information linkage of the 94 publications found shows that four papers are cited particularly frequently (Table 2). Four papers have been identified as central through a considerably higher number of citations [1, 3, 10, 71]. It can be noted that 11 publications were cited on average between 8-14 times. 47 pieces of the found literature were not cross-cited [4-6, 8, 21, 23-25, 27, 30, 33-40, 42, 44, 46, 47, 51, 55-57, 59, 63, 64, 68, 70, 72, 73, 76, 79, 81, 82, 84, 87, 90, 92-96, 98, 99].

Title	Author/s	Number of Citations
Astraea: A Decentralized Blockchain Oracle	Adler et al. [1]	42
Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges	Al-Breiki et al. [3]	31
A Study of Blockchain Oracles	Abdeljalil Beniiche [10]	22
Augur: a decentralized oracle and prediction market platform	Peterson et al. [71]	22

Tab. 2: Highlighting the most frequently cited sources.

In order to show which authors are linked in terms of content, a graph is created that visualizes a bibliographic linkage of the literature retrieved. For a clearer representation of the connections between authors, only publications with at least eight cross-citations are shown graphically. Figure 3 shows the connections between 16 most cross-cited publications [1, 3. 10, 13, 16, 20, 41, 49, 53, 60, 61, 62, 71, 75, 77, 91]. The directed edges point in the direction of the made quote.

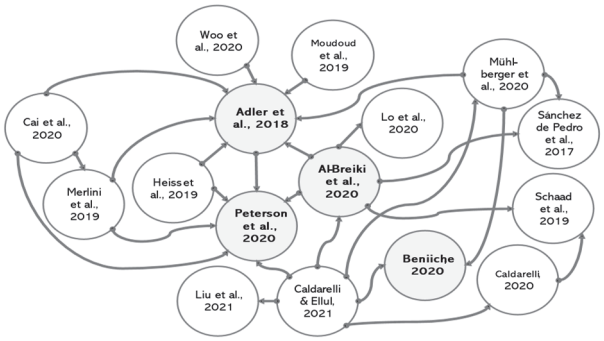

Fig. 3: Visualization of the 16 most cross-cited authors.

To draw a comprehensive picture of all links in the literature, Litmaps is used to populate the bibliography and create a map showing the referenced literature by author (Fig. 4). The dots represent the literature found and the lines show the "cited by" links. More frequently cited sources are presented in larger dots than publications with few or no citations. For better readability, not all points can be marked with the first author in each case. Three sources of the literature found [40, 57, 64] could not be mapped because they are not maintained by the software Litmaps.

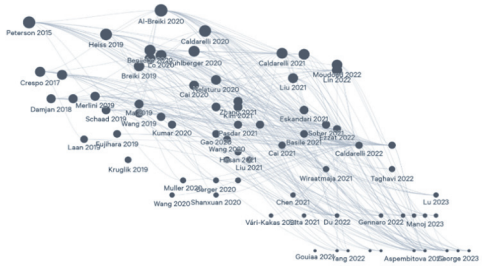

Fig. 4: Linking the authors with Litmaps.

Subsequently, a link between the papers is established based on the authors. The authors listed in Table 3 are assigned between two and a maximum of six published articles. The author Caldarelli has achieved the highest number of publications on blockchain oracle with six published articles [15-20].

Author	Count	Identified publications
Al-Breiki, H.	2	Al-Breiki et al., 2019 [2], Al-Breiki et al., 2020 [3]
Bartholic, M.	2	Bartholic et al., 2022 [7], Bartholic et al., 2023 [8]
Caldarelli, G.	6	Caldarelli et al., 2020 [15], Caldarelli 2020 [16], Caldarelli 2020 [17], Caldarelli & Ellul, 2021 [20], Caldarelli 2022 [18], Caldarelli 2023 [19]
Cai, Y.	2	Cai et al., 2020 [13], Cai et al., 2022 [14]
Liu, B.	2	Liu et al., 2021 [49], Liu et al., 2022 [50]
Pasdar, A.	2	Pasdar et al., 2021 [69], Pasdar et al., 2023 [70]
Wang, S.	2	Wang et al. 2019 [85], Wang & Yu 2020 [96]

Tab. 3: Overarching assignment of authors and publications.

4.2. Topic clustering

In this section, the literature is grouped according to the content of the title and abstract by topic. The scientific papers are analyzed, sorted thematically and grouped into suitable clusters for categorization. The thematic sorting identifies two clusters: *"design optimization"* and *"study"*. While literature classified as *"study"* analyzes the current state of research based on literature reviews, the literature classified as *"design optimization"* investigates approaches that deal with engineering procedures for the technical optimization of oracles. The design optimization is divided into further subcategories, namely data management, distributed systems, and verification (Fig. 5). We use a hard assignment to the clusters, so that the publications found can only be assigned to exactly one cluster. The four overarching clusters are:

- **Data management** is the management and transfer of data from off-chain to on-chain infrastructures via oracles.
- **Distributed systems** deal with the proper design of the decentralized multisystem infrastructure of oracles from an interoperability perspective.
- **Verification** is about checking the correctness of the off-chain data before transferring it to the blockchain protocol via oracle(s).
- **State of the art analysis** includes a literature review as a baseline effort and sometimes building on that to develop a method, framework, or prototype for using oracles in specific use cases.

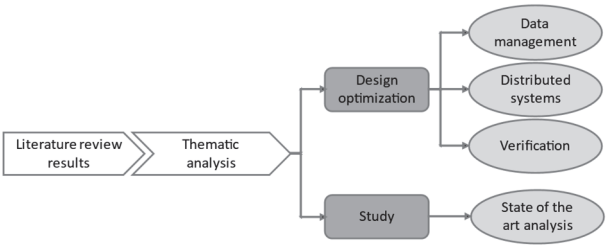

Fig. 5: Thematic categorization in the cluster approach.

The literature retrieved can be thematically categorized as the following (Tab. 4): Data management (17), Distributed systems (28), Verification (17), and in the literature review field, State of the art analysis (32).

Cluster	Publications
Data management	[24, 32, 33, 39, 46, 51, 59, 70, 72, 73, 78, 79, 86, 90, 93, 96, 97]
Distributed systems	[2, 11, 21, 22, 23, 27, 30, 31, 36, 37, 38, 42, 45, 55, 57, 58, 60, 61, 63, 64, 65, 71, 75, 80, 81, 91, 92, 95]
Verification	[1, 4, 13, 14, 26, 34, 50, 52, 56, 67, 68, 69, 76, 84, 85, 87, 98]
State of the art analysis	[3, 5, 6, 7, 8, 9, 10, 12, 15, 16, 17, 18, 19, 20, 25, 28, 29, 35, 40, 41, 43, 44, 47, 49, 53, 54, 62, 74, 77, 82, 94, 99]

Tab. 4: Cluster allocation of the found publications.

4.3. Focus identification

In this section, the topics of the publications are identified based on the focus areas and rated according to their frequency. The focus analysis was based on the title and abstract of the publications. A review of the software engineering literature without reference to an oracle use case is not the center of this section.

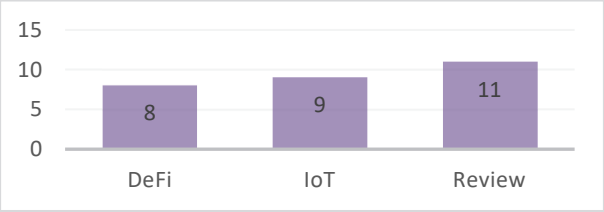

Fig. 6: Frequency distribution of the focus cluster.

The relevant use cases in the domains of Decentralized Finance (DeFi), Internet of Things (IoT), and Literature review are highlighted as focal points (Fig. 6). The term DeFi in connection with blockchain technology stands for the trustless and transparent provision of financial instruments without intermediaries [6]. The keyword IoT describes a network of interconnected electronic devices with limited capabilities [2]. The review relates to the conduct of a literature search. There are eight publications attributed to DeFi [6, 20, 24, 49, 50, 57, 87, 99] and seven to IoT [2, 23, 27, 59, 61,74, 82, 90, 91]. The literature review was recorded with 11 publications [3, 6, 16, 17, 18, 20, 23, 29, 35, 44, 74]. Some of the literature reviews also address the topics of DeFi [6, 20] or IoT [23, 74].

4.4. Evaluation of the results

This section summarizes the results of the intelligent methods. The number of found literature of 94 pieces in relation to the five queried scientific databases shows that there is relatively little literature about blockchain oracle. Since the beginning of this study, the number of publications has increased from one in 2017 to 23 per year in 2023 (Fig. 2). The results of the “Information linking” chapter show that the existing literature is often cross-cited, indicating that not much citable literature exists (Fig. 4). Half of the found publications were not cross-referenced and referred to more general blockchain sources. 43 of these papers were published in the last 2-3 years. This is indicative of the age of publication factor. Another observation is that articles in book publications are not cited from the Springer Link database. The number of most cited papers is very high in relation to the total number of publications (Tab. 2). The four most cited papers show strong interdependencies due to mutual cross-references. The lack of diversity in publications can also be confirmed by analyzing the authors. Seven authors (Tab. 3) were found to be exclusively responsible for 18 papers. One author, Caldarelli, stands out clearly with six publications. Caldarelli's works [15-20] are all classified under the category of literature review. Overall, the literature reviews settle on certain focus areas for oracles, which usually address only one problem, i.e., either the problem of centrality, security, or reliability. The topic clustering (Tab. 4) shows that research is conducted in about equal parts in the areas of Data management and verification. Distributed systems and the analysis of the state of the art receive more attention than the two previous topics. This is an indication that distributed oracle infrastructures have been already better researched than data management and verification structures in oracles. The identification of focus areas (Fig. 6) shows that some papers focused on specific use cases. This suggests that the most promising use cases for oracles are in a DeFi or IoT implementation or general literature reviews. The topic clustering from section 4.2 "state of the art analysis" contains the literature review results of the focus identification, but not vice versa. The cluster results contain many studies and comparisons on the technological implementation of blockchain oracles, but no literature review. However, this is only a small part of the total number of publications with a specific focus. Most publications cannot be assigned to any identifiable use case and deal with the technical implementation of oracles. It turns out that blockchain oracles are a topic in the areas mentioned, but the general technical benefits are explored more deeply than the application in concrete use cases.

5. Conclusion, limitations and future work

The goal of this paper is to provide an overview of the multi-layered research field of blockchain oracles. To this purpose, the systematic literature review is complemented by the application of intelligent methods. The analysis is carried out in three successive steps. First, the information of the authors of the literature is linked, then the topics are sorted according to content clusters and finally specific focus areas are identified. Overall, a multi-page analysis of the researched literature is performed, ranging from author categorization to topic categorization to focus analysis in real use cases. The literature results are thus placed in an overall context to each other. The small number of publications found, the many cross-references, the low diversification of the literature, and the few known authors indicate that there is still a need for research on blockchain oracles. Explicitly, the topics of data management and verification are less covered than literature reviews and distributed systems. This confirms initial research gaps in the general topic of blockchain oracles, especially in the area of verification and security in handling data.

Further studies can complement the literature search by querying higher-level AI-powered databases, such as Semantic Scholar, to identify content connections through the search and thus find further literature.

The literature search revealed that many publications on oracles are often concerned with the lack of typical blockchain properties. This disregards the fact that oracles are in a kind of in-between world. Blockchains can provide trust and transparency in data and transactions. These properties of a blockchain are not compromised

by technical non-blockchain-based oracles. On the other hand, oracles should of course consistently meet these requirements in terms of data security and integrity. In the long run, research will evaluate and develop its own technical conception of oracles. In addition, this literature review has highlighted the need for standardized oracle development, as there are approaches to solutions from decentralized, consensus-based oracles. Another indication of future research direction is the development of best practices for oracles that can be used for universal use cases. Isolated use cases, such as DeFi or IoT, could be identified. This shows that much of the published literature is concerned with technical development and not with specific applications in particular business areas. This gap has to be addressed in future research.

Another oracle topic deals with the issue of verifying data before it is transferred to a blockchain. The reason for this is that, according to the credo of blockchains, the written transactions are trustworthy, secure and tamper-proof, while the data originating from third-party systems is not verified by oracles. This raises the important question of the particular unique selling proposition of blockchain and should be explored in further research.

Acknowledgements

This work is funded by the Federal Ministry of Food and Agriculture (BMEL) on the basis of a resolution of the German Bundestag. The project is being carried out by the Federal Agency for Agriculture and Food (BLE) as part of the funding for digitalization in agriculture with the funding code 28DE102A18.

Contact

Viola Süß, suess@wifa.uni-leipzig.de

https://orcid.org/0009-0003-8518-2180

Bogdan Franczyk, franczyk@wifa.uni-leipzig.de

https://orcid.org/0000-0002-5740-2946

Literature references

[1] Adler, J., Berryhill, R., Veneris, A., Poulos, Z., Veira, N., Kastania, A. (2018): Augur: a Decentralized Oracle and Prediction Market Platform, in: Proceedings of the 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), page 1145–1152, doi:10.13140/2.1.1431.4563.

[2] Al Breiki, H., Al Qassem, L., Salah, K., Rehman, M. H. U., Sevtinovic, D. (2019): Decentralized Access Control for IoT Data Using Blockchain and Trusted Oracles, in: *2019 IEEE International Conference on Industrial Internet (ICII)*, Orlando, FL, USA, pp. 248-257, doi:10.1109/ICII.2019.00051.

[3] Al-Breiki, H., Rehman, M. H. U., Salah, K., Svetinovic, D. (2020): Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges, in: *IEEE Access*, vol. 8, pp. 85675-85685, doi:10.1109/ACCESS.2020.2992698.

[4] Almi'Ani, K., Lee, Y. C., Alrawashdeh T., Pasdar, A. (2023): Graph-Based Profiling of Blockchain Oracles, in: *IEEE Access*, vol. 11, pp. 24995-25007, doi:10.1109/ACCESS.2023.3254535.

[5] Antonio Pierro, G., and Mahugnon, H. (2023): An analysis of the Oracles used in Ethereum's blockchain, in: *2023 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)*, Taipa, Macao, pp. 878-885, doi:10.1109/SANER56733.2023.00106.

[6] Aspembitova, A.T.; Bentley, M.A. (2023): Oracles in Decentralized Finance: Attack Costs, Profits and Mitigation Measures, in: *Entropy 2023*, 25(1), 60, doi:10.3390/e25010060

[7] Bartholic, M., Laszka, A., Yamamoto, G., Burger, E. W. (2022): A Taxonomy of Blockchain Oracles: The Truth Depends on the Question, in: *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Shanghai, China, pp. 1-15, doi:10.1109/ICBC54727.2022.9805555.

[8] Bartholic, M., Burger, E. W., Matsuo, S., Jung, T. (2023): Reputation as Contextual Knowledge: Incentives and External Value in Truthful Blockchain Oracles, in: *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Dubai, United Arab Emirates, pp. 1-9, doi:10.1109/ICBC56567.2023.10174903.

[9] Basile, D., Goretti, V., Di Ciccio, C., Kirrane, S. (2021): Enhancing Blockchain-Based Processes with Decentralized Oracles, in: González Enríquez, J., Debois, S., Fettke, P., Plebani, P., van de Weerd, I., Weber, I. (eds) Business Process Management: Blockchain and Robotic Process Automation Forum, BPM 2021, Lecture Notes in Business Information Processing, vol 428. Springer, Cham. doi:10.1007/978-3-030-85867-4_8.

[10] Beniiche, A. (2020): A Study of Blockchain Oracles, in: arXiv: 2004.07140.

[11] Berger, B., Huber, S., Pfeifhofer, S. (2020): OraclesLink: An architecture for secure oracle usage, in: *2020 Second International Conference on Blockchain Computing and Applications (BCCA)*, Antalya, Turkey, pp. 66-72, doi:10.1109/BCCA50787.2020.9274455.

[12] Boi, M., Pinna, A., Lunesu, M. I. (2023): Blockchain oracles for document certification: A case study., in: *2023 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)*, Taipa, Macao, pp. 855-864, doi:10.1109/SANER56733.2023.00103.

[13] Cai, Y., Fragkos, G., Tsiropoulou, E. E., Veneris, A. (2020): A Truth-Inducing Sybil Resistant Decentralized Blockchain Oracle, in: *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, Paris, France, pp. 128-135, doi:10.1109/BRAINS49436.2020.9223272.

[14] Cai, Y., Irtija, N., Tsiropoulou, E. E., Veneris, A. (2022): Truthful Decentralized Blockchain Oracles, in: *International Journal of Network Management*; 32(2):e2179, doi:10.1002/nem.2179.

[15] Caldarelli, G., Rossignoli, C., Zardini, A. (2020): Overcoming the Blockchain Oracle Problem in the Traceability of Non-Fungible

Products, in: *Sustainability*, 12(6):2391, doi:10.3390/su12062391.
[16] Caldarelli, G. (2020): Understanding the Blockchain Oracle Problem: A Call for Action., in: *Information,* 11(11):509, doi:10.3390/info11110509.
[17] Caldarelli, G. (2020): Real-world blockchain applications under the lens of the oracle problem. A systematic literature review, in: *2020 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD)*, Marrakech, Morocco, pp. 1-6, doi:10.1109/ICTMOD49425.2020.9380598.
[18] Caldarelli, G. (2022): Overview of Blockchain Oracle Research, in: *Future Internet*; 14(6):175, doi:10.3390/fi14060175.
[19] Caldarelli, G. (2023): Before Ethereum. The Origin and Evolution of Blockchain Oracles, in: *IEEE Access*, vol. 11, pp. 50899-50917, doi:10.1109/ACCESS.2023.3279106.
[20] Caldarelli, G., Ellul, J. (2021): The Blockchain Oracle Problem in Decentralized Finance—A Multivocal Approach, in: *Applied Sciences,* 11(16):7572, doi:10.3390/app11167572.
[21] Chen, S., Zhu, J., Lin, Z., Huang, J., Tang, Y. (2021): How to Make Smart Contract Smarter, in: Sun, Y., Liu, D., Liao, H., Fan, H., Gao, L. (eds) Computer Supported Cooperative Work and Social Computing, ChineseCSCW 2020, Communications in Computer and Information Science, vol 1330, Springer, Singapore, doi:10.1007/978-981-16-2540-4_54.
[22] Chen, L., Yuan, R., Xia, Y. (2021): Tora: A Trusted Blockchain Oracle Based on a Decentralized TEE Network, in: *2021 IEEE International Conference on Joint Cloud Computing (JCC)*, Oxford, United Kingdom, pp. 28-33, doi:10.1109/JCC53141.2021.00016.
[23] Chung, K. H. Y., Li, D., Adriaens, P. (2023): Technology-enabled financing of sustainable infrastructure: A case for blockchains and decentralized oracle networks, in: *Technological Forecasting and Social Change*, Volume 187, 122258, ISSN 0040-1625, doi:10.1016/j.techfore.2022.122258.
[24] Cioara, T., Pop, C., Zanc, R., Anghel, I., Antal, M., Salomie, I. (2020): Smart Grid Management Using Blockchain: Future Scenarios and Challenges, in: *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Bucharest, Romania, pp. 1-5, doi:10.1109/RoEduNet51892.2020.9324874.
[25] Damjan, M. (2018): The interface between blockchain and the real world, in: Ragion Pratica, pp. 379-406, doi:10.1415/91545.
[26] Di Gennaro, M., Italiano, L., Meroni, G., Quattrocchi, G. (2022): *DeepThought*: A Reputation and Voting-Based Blockchain Oracle, in: Troya, J., Medjahed, B., Piattini, M., Yao, L., Fernández, P., Ruiz-Cortés, A. (eds) Service-Oriented Computing, ICSOC 2022, Lecture Notes in Computer Science, vol 13740, Springer, Cham, doi:10.1007/978-3-031-20984-0_26.
[27] Du, Y., Li, J., Shi, L., Wang, Z., Wang, T., Han, Z. (2022): A Novel Oracle-aided Industrial IoT Blockchain: Architecture, Challenges, and Potential Solutions, in: *IEEE Network*, doi:10.1109/MNET.103.2100395.
[28] Eskandari, S., Salehi, M., Gu, W. G., Clark, J. (2021): SoK: oracles from the ground truth to market manipulation, in: *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies (AFT '21), Association for Computing Machinery,* New York, NY, USA, pp. 127–141, doi:10.1145/3479722.3480994.
[29] Ezzat, S. K., Saleh, Y. N. M., Abdel-Hamid, A. A. (2022): Blockchain Oracles: State-of-the-Art and Research Directions, in: *IEEE Access*, vol. 10, pp. 67551-67572, doi:10.1109/ACCESS.2022.3184726.
[30] Fuertes Blanco, A., Shi, Z., Roy, D., Zhao, Z. (2023): Improving the Resiliency of Decentralized Crowdsourced Blockchain Oracles, in: Mikyška, J., de Mulatier, C., Paszynski, M., Krzhizhanovskaya, V. V., Dongarra, J. J., Sloot, P.M. (eds) Computational Science – ICCS 2023. ICCS 2023, Lecture Notes in Computer Science, vol 14073, Springer, Cham, doi:10.1007/978-3-031-35995-8_1.
[31] Fujihara, A. (2020): Proposing a Blockchain-Based Open Data Platform and Its Decentralized Oracle, in: Barolli, L., Nishino, H., Miwa, H. (eds) Advances in Intelligent Networking and Collaborative Systems, INCoS 2019, Advances in Intelligent Systems and Computing, vol 1035, Springer, Cham, doi:10.1007/978-3-030-29035-1_19.
[32] Gao, Z., Li, H., Xiao, K., Wang, Q. (2020): Cross-chain Oracle Based Data Migration Mechanism in Heterogeneous Blockchains, in: *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, Singapore, Singapore, pp. 1263-1268, doi:10.1109/ICDCS47774.2020.00162.
[33] Gao, Z., Zhuang, Z., Lin, Y., Rui, L., Yang, Y., Zhao, C., Mo, Z. (2021): Select-Storage: A New Oracle Design Pattern on Blockchain, in: *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Shenyang, China, pp. 1177-1184, doi:10.1109/TrustCom53373.2021.00159.
[34] George, W. (2023): Strategic behaviour and manipulation resistance in Peer-to-Peer, crowdsourced information gathering, in: *Mathematical Social Sciences*, Volume 124, pp. 1-23, ISSN 0165-4896, doi:10.1016/j.mathsocsci.2023.04.002.
[35] Gonçalves, M. J. A., Pereira, R. H., Coelho, M. A. G. M. (2022): User Reputation on E-Commerce: Blockchain-Based Approaches, in: *Journal of Cybersecurity and Privacy,* 2(4):907-923, doi:10.3390/jcp2040046.
[36] Goswami, S., Danish, S. M., Zhang, K. (2022): Towards a middleware design for efficient blockchain oracles selection, in: *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)*, San Antonio, TX, USA, pp. 55-62, doi:10.1109/BCCA55292.2022.9922433.
[37] Gouiaa, R., Hdhili, F., Jansen, M. (2022): A Dag Based Decentralized Oracle Model: Implementation and Evaluation, in: Prieto, J., Partida, A., Leitão, P., Pinto, A. (eds) Blockchain and Applications, BLOCKCHAIN 2021, Lecture Notes in Networks and Systems, vol 320, Springer, Cham, doi:10.1007/978-3-030-86162-9_31.
[38] Gupta, A., Gupta, R., Jadav, D., Tanwar, S., Kumar, N., Shabaz, M. (2023): Proxy smart contracts for zero trust architecture implementation in Decentralised Oracle Networks based applications, in: *Computer Communications*, Volume 206, pp. 10-21, ISSN 0140-3664, doi:10.1016/j.comcom.2023.04.022.
[39] Hasan, M., Ogan, K., Starly, B. (2021): Hybrid Blockchain Architecture for Cloud Manufacturing-as-a-service (CMaaS) Platforms with Improved Data Storage and Transaction Efficiency, in: *Procedia Manufacturing*, Volume 53, pp. 594-605, ISSN 2351-9789, doi:10.1016/j.promfg.2021.06.060.
[40] Hassan, A., Makhdoom, I., Iqbal, W., Ahmad, A., Raza, A. (2023): From trust to truth: Advancements in mitigating the Blockchain Oracle problem, in: Journal of Network and Computer Applications, Volume 217, 103672, ISSN 1084-8045, doi:10.1016/j.jnca.2023.103672.

[41] Heiss, J., Eberhardt, J., Tai, S. (2019): From Oracles to Trustworthy Data On-Chaining Systems, in: *2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, USA, pp. 496-503, doi:10.1109/Blockchain.2019.00075.

[42] Huang, M., Cao, S., Li, X., Huang, K., Zhang, X. (2022): Defending Data Poisoning Attack via Trusted Platform Module and Blockchain Oracle, in: *ICC 2022 - IEEE International Conference on Communications*, Seoul, Korea, Republic of, pp. 1245-1250, doi:10.1109/ICC45855.2022.9838252.

[43] Kaleem, M., Shi, W. (2021): Demystifying Pythia: A Survey of ChainLink Oracles Usage on Ethereum, in: Bernhard, M., *et al.* Financial Cryptography and Data Security, FC 2021 International Workshops, FC 2021, Lecture Notes in Computer Science(), vol 12676, Springer, Berlin, Heidelberg, doi:10.1007/978-3-662-63958-0_10.

[44] Kruglik, S., Nazirkhanova, K., Yanovich, Y. (2019): Challenges beyond blockchain: scaling, oracles and privacy preserving, in: *2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)*, Moscow, Russia, pp. 155-158, doi:10.1109/REDUNDANCY48165.2019.9003331.

[45] Kumar, M., Nikhil, N., Singh, R. (2020): Decentralising Finance using Decentralised Blockchain Oracles, in: *2020 International Conference for Emerging Technology (INCET)*, Belgaum, India, pp. 1-4, doi:10.1109/INCET49848.2020.9154123.

[46] Lin, I.-C., Kuo, C.-W. (2023): Trustworthy Blockchain Oracles for Smart Contracts, in: Tsihrintzis, G.A., Wang, SJ., Lin, IC. (eds) 2021 International Conference on Security and Information Technologies with AI, Internet Computing and Big-data Applications, Smart Innovation, Systems and Technologies, vol 314, Springer, Cham, doi:10.1007/978-3-031-05491-4_38.

[47] Lin, S.-Y., Zhang, L., Li, J., Sun, Y. (2022): A survey of application research based on blockchain smart contract, in: *Wireless Netw 28*, pp. 635–690, doi:10.1007/s11276-021-02874-x.

[48] Litan, A. (2022): Gartner Hype Cycle for Blockchain and Web3, 2022, https://blogs.gartner.com/avivah-litan/2022/07/22/gartner-hype-cycle-for-blockchain-and-web3-2022/, 29/07/2023.

[49] Liu, B., Szalachowski, P., Zhou, J. (2021): A First Look into DeFi Oracles," *2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, United Kingdom, pp. 39-48, doi:10.1109/DAPPS52256.2021.00010.

[50] Liu, B., Zhou, J., Lim, Y. Z. (2022): Being Accountable Never Cheats: An Incentive Protocol for DeFi Oracles, in: *2022 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, Newark, CA, USA, pp. 1-10, doi:10.1109/DAPPS55202.2022.00009.

[51] Liu, X., Chen, R., Chen, Y.-W., Yuan, S.-M. (2018): Off-chain Data Fetching Architecture for Ethereum Smart Contract, in: *2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB)*, Fuzhou, China, pp. 1-4, doi:10.1109/ICCBB.2018.8756348.

[52] Liu, X., Feng, J. (2021): Trusted Blockchain Oracle Scheme Based on Aggregate Signature, in: *Journal of Computer and Communications*, 09. 95-109, doi:10.4236/jcc.2021.93007.

[53] Lo, S. K., Xu, X., Staples, M., Yao, L. (2020): Reliability analysis for blockchain oracles, in: *Computers & Electrical Engineering*, Volume 83, 106582, ISSN 0045-7906, doi:10.1016/j.compeleceng.2020.106582.

[54] Lu, W., Li, X., Xue, F., Zhao, R., Wu, L., Yeh, A. G. O. (2021): Exploring smart construction objects as blockchain oracles in construction supply chain management, in: *Automation in Construction*, Volume 129, 103816, ISSN 0926-5805, doi:10.1016/j.autcon.2021.103816.

[55] Lu, S., Pei, J., Zhao, R., Yu, X., Zhang, X., Li, J., Yang, G. (2023): CCIO: A Cross-Chain Interoperability Approach for Consortium Blockchains Based on Oracle, in: *Sensors,* 23(4):1864, doi:10.3390/s23041864.

[56] Lv, P., Zhang, X., Liu, J., Wei, T., Xu, J. (2021): Blockchain Oracle-Based Privacy Preservation and Reliable Identification for Vehicles, in: Liu, Z., Wu, F., Das, S.K. (eds) Wireless Algorithms, Systems, and Applications, WASA 2021, Lecture Notes in Computer Science(), vol 12939, Springer, Cham, doi:10.1007/978-3-030-86137-7_54.

[57] Lys, L., Potop-Butucaru, M. (2022): Distributed Blockchain Price Oracle, in: Koulali, MA., Mezini, M. (eds) Networked Systems, NETYS 2022, Lecture Notes in Computer Science, vol 13464, Springer, Cham, doi:10.1007/978-3-031-17436-0_4.

[58] Ma, L., Kaneko, K., Sharma, S., Sakurai, K. (2019): Reliable Decentralized Oracle with Mechanisms for Verification and Disputation, in: *2019 Seventh International Symposium on Computing and Networking Workshops (CANDARW)*, Nagasaki, Japan, pp. 346-352, doi:10.1109/CANDARW.2019.00067.

[59] Manoj T., Makkithaya, K., Narendra, V. G. (2023): A trusted IoT data sharing and secure oracle based access for agricultural production risk management, in: *Computers and Electronics in Agriculture*, Volume 204, 107544, ISSN 0168-1699, doi:10.1016/j.compag.2022.107544.

[60] Merlini, M., Veira, N., Berryhill, R., Veneris, A. (2019): On Public Decentralized Ledger Oracles via a Paired-Question Protocol, in: *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Seoul, Korea (South), pp. 337-344, doi:10.1109/BLOC.2019.8751484.

[61] Moudoud, H., Cherkaoui, S., Khoukhi, L. (2019): An IoT Blockchain Architecture Using Oracles and Smart Contracts: the Use-Case of a Food Supply Chain, in: *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Istanbul, Turkey, pp. 1-6, doi:10.1109/PIMRC.2019.8904404.

[62] Mühlberger, R., Bachhofner, S., Castelló Ferrer, E., Di Ciccio, C., Weber, I., Wöhrer, M., Zdun, U. (2020): Foundational Oracle Patterns: Connecting Blockchain to the Off-Chain World, in: *Lecture Notes in Business Information Processing*, Springer International Publishing, pp. 35-51, doi:10.1007/978-3-030-58779-6_3.

[63] Müller, M., Rodriguez Garzon, S., Küpper, A. (2020): COST: A Consensus-Based Oracle Protocol for the Secure Trade of Digital Goods, in: *2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, Oxford, UK, pp. 72-81, doi:10.1109/DAPPS49028.2020.00008.

[64] Naderi, H., Shojaei, A., Ly, R. (2023): Autonomous construction safety incentive mechanism using blockchain-enabled tokens and vision-based techniques, in: *Automation in Construction*, Volume 153, 104959, ISSN 0926-5805, doi:10.1016/j.autcon.2023.104959.

[65] Nelaturu, K., Adler, J., Merlini, M., Berryhill, R., Veira, N., Poulos, Z., Veneris, A. (2020): On Public Crowdsource-Based Mechanisms for a Decentralized Blockchain Oracle, in: *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1444-1458, doi:10.1109/TEM.2020.2993673.

[66] Nitsche, A.-M., Schumann, C.-A., Franczyk, B., Reuther, K. (2021): Mapping supply chain collaboration research: a machine learning-based literature review, in: *International Journal of Logistics Research and Applications*, doi:10.1080/13675567.2021.2001446.
[67] Park, J., Kim, H., Kim, G., Ryou, J. (2021): Smart Contract Data Feed Framework for Privacy-Preserving Oracle System on Blockchain, in: *Computers*, 10(1):7, doi:10.3390/computers10010007.
[68] Park, S., Bastani, O., Kim, T. (2023): ACon²: Adaptive Conformal Consensus for Provable Blockchain Oracles, doi:10.48550/arXiv.2211.09330.
[69] Pasdar, A., Dong, Z., Choon Lee, Y. (2021): Blockchain Oracle Design Patterns, doi:10.48550/arXiv.2106.09349.
[70] Pasdar, A., Lee, Y. C., Ryan, P., Dong, Z. (2023): A Blockchain Oracle-Based API Service for Verifying Livestock DNA Fingerprinting, in: Troya, J., *et al.* Service-Oriented Computing – ICSOC 2022 Workshops, ICSOC 2022, Lecture Notes in Computer Science, vol 13821, Springer, Cham, doi:10.1007/978-3-031-26507-5_7.
[71] Peterson, J., Krug, J., Zoltu, M., Williams, A. K., Alexander, S. (2020): Augur: a Decentralized Oracle and Prediction Market Platform, doi: 10.13140/2.1.1431.4563.
[72] Popchev, I., Radeva, I., Doukovska, L. (2023): Oracles Integration in Blockchain-Based Platform for Smart Crop Production Data Exchange, in: *Electronics*; 12(10):2244, doi:10.3390/electronics12102244.
[73] Pupyshev, A., Dzhafarov, E., Sapranidi, I., Kardanov, I., Khalilov, S., Laureyssens, S. (2020): SuSy: a blockchain-agnostic cross-chain asset transfer gateway protocol based on Gravity, doi:10.48550/arXiv.2008.13515.
[74] Sadawi, A. A., Hassan, M. S., Ndiaye, M. (2022): On the Integration of Blockchain With IoT and the Role of Oracle in the Combined System: The Full Picture, in: *IEEE Access*, vol. 10, pp. 92532-92558, doi:10.1109/ACCESS.2022.3199007.
[75] Sánchez De Pedro, A., Levi, D., Cuende, L. I. (2017): Witnet: A Decentralized Oracle Network Protocol, doi: 10.13140/RG.2.2.28152.34560.
[76] Sata, B., Berlanga, A., Chanel, C. P. C., Lacan, J. (2021): Connecting AI-based Oracles to Blockchains via an Auditable Auction Protocol, in: *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, Paris, France, pp. 23-24, doi:10.1109/BRAINS52497.2021.9569808.
[77] Schaad, A., Reski, T., Winzenried, O. (2019): Integration of a Secure Physical Element as a Trusted Oracle in a Hyperledger Blockchain, in: *International Conference on E-Business and Telecommunication Networks*, doi:10.5220/0007957104980503.
[78] Sober, M., Scaffino, G., Spanring, C., Schulte, S. (2021): A Voting-Based Blockchain Interoperability Oracle, in: *IEEE International Conference on Blockchain (Blockchain)*, Melbourne, Australia, pp. 160-169, doi:10.1109/Blockchain53845.2021.00030.
[79] Stefanescu, D., Galán-García, P., Montalvillo, L., Unzilla, J., Urbieta, A. (2023): Industrial Data Homogenization and Monitoring Scheme with Blockchain Oracles, in: *Smart Cities*; 6(1):263-290, doi:10.3390/smartcities6010013.
[80] Taghavi, M., Bentahar, J., Otrok, H., Bakhtiyari, K. (2023): A reinforcement learning model for the reliability of blockchain oracles, in: *Expert Systems with Applications*, Volume 214, 119160, ISSN 0957-4174, doi:10.1016/j.eswa.2022.119160.
[81] van der Laan, B., Ersoy, O., Erkin, Z. (2019): MUSCLE: authenticated external data retrieval from multiple sources for smart contracts, in: *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing (SAC '19)*, Association for Computing Machinery, New York, NY, USA, pp. 382–391, doi:10.1145/3297280.3297320.
[82] Vári-Kakas, S., Poszet, O., Mirela Pater, A., Valentina Moisi, E., Vári-Kakas, A. (2021): Issues Related to the Use of Blockchains in IoT Applications, in: *2021 16th International Conference on Engineering of Modern Electric Systems (EMES)*, Oradea, Romania, pp. 1-4, doi:10.1109/EMES52337.2021.9484103.
[83] vom Brocke, J., Simons, A., Niehaves, B., Reimer, K., Plattfaut, R., Cleven, A. (2009): Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process, in: *European Conference on Information Systems.*
[84] Wang, S., Yu, X. (2020): Research on Trusted Identification of Blockchain Uploaded Data, in: *2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)*, Dalian, China, pp. 1036-1044, doi:10.1109/ICAICA50127.2020.9181948.
[85] Wang, S., Lu, H., Sun, X., Yuan, Y., Wang, F.-Y. (2019): A Novel Blockchain Oracle Implementation Scheme Based on Application Specific Knowledge Engines, in: *2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, Zhengzhou, China, pp. 258-262, doi:10.1109/SOLI48380.2019.8955107.
[86] Wang, Y., Liu, H., Wang, J., Wang, S. (2020): Efficient Data Interaction of Blockchain Smart Contract with Oracle Mechanism, in: *2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, Chongqing, China, pp. 1000-1003, doi:10.1109/ITAIC49862.2020.9338784.
[87] Wang, Y., Li, J., Su, Z., Wang, Y. (2022): Arbitrage Attack: Miners of the World, Unite!, in: Eyal, I., Garay, J. (eds) Financial Cryptography and Data Security, FC 2022, Lecture Notes in Computer Science, vol 13411, Springer, Cham, doi:10.1007/978-3-031-18283-9_23.
[88] Watson, R. T., Webster, J. (2020): Analyzing the past to prepare for the future: Writing a literature review a roadmap for release 2.0, in: *Journal of Decision Systems*, 29:3, pp. 129-147, doi:10.1080/12460125.2020.1798591.
[89] Webster, J., Watson, R. T. (2002): Analyzing the Past to Prepare for the Future: Writing a Literature Review, in: *MIS Quarterly 26*, no. 2: xiii–xxiii, doi:10.2307/4132319.
[90] Wiraatmaja, C., Zhang, Y., Sasabe, M., Kasahara, S. (2021): Cost-Efficient Blockchain-Based Access Control for the Internet of Things, in: *2021 IEEE Global Communications Conference (GLOBECOM)*, Madrid, Spain, pp. 1-6, doi:10.1109/GLOBECOM46510.2021.9685205.
[91] Woo, S., Song, J., Park, S. (2020): A Distributed Oracle Using Intel SGX for Blockchain-Based IoT Applications, in: *Sensors*; 20(9):2725, doi:10.3390/s20092725.
[92] Wu, X., Wang, H., Ge, C., Zhou, L., Huang, Q., Kong, L., Cui, L., Liu, Z. (2022): *CCOM*: Cost-Efficient and Collusion-Resistant Oracle Mechanism for Smart Contracts, in: Nguyen, K., Yang, G., Guo, F., Susilo, W. (eds) Information Security and Privacy, ACISP 2022, Lecture Notes in Computer Science, vol 13494, Springer, Cham, doi:10.1007/978-3-031-22301-3_22.
[93] Yadav, S., Rastogi, S., Soni, S., Kshitij, P., Malsa, N., Gupta, V., Ghosh, A., Shaw, R. N. (2023): Distributed Hotel Chain Using Blockchain and Chainlink, in: Shaw, R.N., Paprzycki, M., Ghosh, A. (eds) Advanced Communication and Intelligent Systems,

ICACIS 2022, Communications in Computer and Information Science, vol 1749, Springer, Cham, doi:10.1007/978-3-031-25088-0_43.

[94] Yang, F., Lei, L., Chen, L. (2022): Method of Interaction between Blockchain and the World outside the Chain based on Oracle Machine, in: *2022 IEEE 8th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, Jinan, China, pp. 101-106, doi:10.1109/BigDataSecurityHPSCIDS54978.2022.00028.

[95] Yang, T., Sun, Q., Chen, F. (2022): TransOra: A Transaction-preserving and Transparent Distributed Oracle on Permissioned Blockchain For Hybrid Smart Contracts, in: *2022 3rd International Conference on Computing, Networks and Internet of Things (CNIOT)*, Qingdao, China, pp. 1-11, doi:10.1109/CNIOT55862.2022.00010.

[96] Yu, H., Wang, H. (2023): Lattice-Based Threshold Signcryption for Blockchain Oracle Data Transmission, in: *IEEE Transactions on Intelligent Transportation Systems*, doi:10.1109/TITS.2023.3276920.

[97] Zhang, C., Zhu, L., Xu, C., Sharif, K. (2021): PRVB: Achieving Privacy-Preserving and Reliable Vehicular Crowdsensing via Blockchain Oracle, in: *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 831-843, doi:10.1109/TVT.2020.3046027.

[98] Zhang, S., Zhang, Y., Jing, X., Diao, X., Huang, G. (2022): DataAttest: A Framework to Attest Off-Chain Data Authenticity, in: Svetinovic, D., Zhang, Y., Luo, X., Huang, X., Chen, X. (eds) Blockchain and Trustworthy Systems, BlockSys 2022, Communications in Computer and Information Science, vol 1679, Springer, Singapore, doi:10.1007/978-981-19-8043-5_5.

[99] Zhao, Y., Kang, X., Li, T., Chu, C.-K., Wang, H. (2022): Towards Trustworthy DeFi Oracles: Past, Present and Future, IEEE Access, doi:10. 1-1. 10.1109/ACCESS.2022.3179374.

An Empirical Approach on Exploring NFT Launch Strategies

Robin Karle, Josepha Witt
University of Hohenheim, Stuttgart, Germany

Abstract: *In the field of Blockchain Technology applications and research, non-fungible tokens (NFTs) have gained significant attention in recent years. Whilst current research is focused on NFT use cases or the purchase of NFTs from an investor's perspective, the NFT launch (i.e. primary market) from a creator's perspective remains uncovered. However, the launch strategy is considered to be an important factor for the success of a product. Therefore, our research paper aims to explore launch strategies of NFTs. Thereby, we discuss the marketing mix instruments price (i.e. pricing strategy), place (i.e. mint mechanism), and promotion. Through an empirical approach of conducting eight expert interviews, we examine parameters that are used to define an NFT launch strategy and assess their preference of different stakeholders.*

Keywords: *Blockchain Technology, non-fungible token, NFT, launch strategies, pricing strategy, mint mechanism*

1. Introduction

In the field of Blockchain Technology (BCT) applications and research, non-fungible tokens (NFTs) have gained significant attention in recent years. NFTs are tokens which "are neither exchangeable nor divisible, meaning they have individual information and properties that make each token unique" (p. 2 in [1]); NFTs represent unique digital assets. Due to their characteristics (such as scarcity, proof of ownership, and proven authenticity), organisations in various fields have recognised the potential of NFTs as a novel marketing tool [2]. Current research outlines approaches how to use NFTs in marketing (e.g. [2]; [3]) or is mainly focused on NFT sales and purchases from an investor's perspective (e.g. [4]). What remains uncovered is the NFT launch, i.e. the first sale of the creator to one or more buyers (cf. primary market). However, the launch strategy of a product is considered as an important factor for the success of a product (e.g. [5]; [6]). Therefore, our research paper aims to explore launch strategies of NFTs. Thereby, we focus on tactic launch decisions [7] referring to the marketing mix instruments, i.e. product, price, place, promotion (referred to as 4P's). The product to be considered is pre-defined to be NFTs. Hence, we discuss the instruments price (i.e. pricing strategy), place (i.e. mint mechanism), and promotion. Through an empirical approach we examine parameters that are used to define an NFT launch strategy and assess their preference of different stakeholders.

2. Background

When Satoshi Nakamoto published the Bitcoin whitepaper [8], the cryptocurrency Bitcoin was introduced, i.e. the first fungible, Blockchain-based/cryptographic tokens. Crypto-graphic tokens are defined in smart contracts (i.e. software code automatically executed in a Blockchain network) [1]. Fungible tokens, such as cryptocurrencies, are inter-changeable with tokens of the same category [9]. However, several use cases require to represent the ownership of unique assets, which can be digital (e.g. files, gaming assets) or physical (e.g. cars, luxury goods) [10]; [11]. Such assets can be represented by cryptographic non-fungible tokens (NFTs). In contrast to e.g. cryptocurrencies, NFTs are unique and cannot be divided. Thereby, they enable digital scarcity [11]. As other cryptographic tokens, NFTs are defined in smart contracts and mainly refer to the standard Ethereum Request for Comments 721 (ERC-721) [1]. ERC-721 [12] introduces a standard interface which provides NFTs with a unique tokenID (stored immutable on a Blockchain). Furthermore, it enables to verify the owner of a specific NFT, to get the current token balance of a wallet address, and to transfer NFTs to other accounts. Hence, the standard ensures the main properties of NFTs, i.e. to be unique and immutable, change the ownership (cf. transferability), and verify it [12].

[1] provides a taxonomy which classifies NFTs across their whole lifecycle, i.e. referring to their origination (e.g. asset substance), distribution (e.g. price formation), transfer (e.g. wallet), trading (e.g. fees), and redeem (e.g. purpose). As our research is focused on the NFT primary market, we will briefly describe the high-level process of an NFT launch, i.e. the first phases of an NTF's lifecycle. First, an NFT creator / NFT project team determines which assets (e.g. digital collectibles) shall be represented, which type of NFT to create, which Blockchain network to use, etc. [1]. Afterwards, this information is digitised, i.e. the file, title, and description of the NFT are in a proper format [13]. When the NFT shall be sold for the first time and thereby created (i.e. registered on the Blockchain), it is launched. During a launch, a transaction containing the pre-defined data is sent to the respective smart contract, which executes the predefined functions (cf. ERC-721). Once the thereby initiated transactions are confirmed, the new NFT is "minted", i.e. the virtual representation is registered on the Blockchain [10]; [13].

Referring to a launch, it is differentiated between an NFT auction (i.e. a specific NFT is sold, e.g. "Everydays" from Beeple [14]) and an NFT drop [15]. During an NFT drop, a collection of NFTs is offered, which are still unique but have certain similarities. Thereby, the buyer purchases a certain number of NFTs from the collection but does not know which exact NFT is being obtained. Hence, the exact value of the NFT is not clear when purchasing it as NFT of a collection usually have different rarities [15].

3. Methodological Approach

As NFT launch strategies are widely unexplored in the scientific literature, we gather insights empirically from experts through interviews. A total of eight interviews were conducted with different stakeholders to capture their perspectives, i.e. being an expert who represents a certain group [16]. We interviewed experts (defined according to [17]) who have launched NFT projects (I6, I7, I8), who are investors of NFT projects at an early stage (I1), and collectors who mint NFTs and own a substantial NFT portfolio (I2, I3, I4, I5), illustrated in Table 1.

Type of organisation	Position	ID	Duration in mins
Venture capital for crypto investments	Head of NFT investments	I1	20
/	NFT collector & influencer	I2	43
Start-up for NFT data analysis	Founder & NFT collector	I3	37
Self-employed	Consultant for digital marketing and NFTs	I4	57
/	NFT collector	I5	82
NFT Start-Up	Founder & CEO	I6	18
AR Gaming & NFTs	Technical community lead	I7	41
AR Gaming & NFTs	Founder & CEO	I8	39

Table 1: Overview of interview partners

Afterwards, the interview records (337 minutes in total) have been transcribed according to [18] and evaluated by performing a structuring qualitative content analysis according to Mayring [19]. This systematic procedure aims to filter out certain aspects of the material and structure it according to previously defined criteria. As described in the chapter Introduction, we focus on tactic launch decisions [7] (cf. 4P marketing mix instruments) when exploring launch strategies of NFTs. Therefore, we structure the empirical findings according to the criteria pricing strategy, mint mechanism, and promotion (cf. deductive categories). By interpreting the empirical material, a category system is created [19], comprising of the deductive categories and inductive sub-categories based on the interpretation of the empirical material.

4. Results

As follows, the result of our analysis is described along the structure of the final coding frame (cf. Figure 1). It is comprised of the three deductive categories which have been introduced and various inductive subcategories which will be described as follows.

Figure 1: Coding frame resulting from the interview analyses

4.1 Price Setting

According to the empirical findings, the price setting for an NFT launch is determined by the categories market situation, benchmarking, financial plan, supply and demand, and maximum mint price (cf. Figure 1).

The market situation as a parameter for NFT mint price setting was mentioned by four experts. For example, I6 stated: "You would take the macro [economy, and] micro [economy] into consideration. So, what the underlying crypto market is doing". The interviews revealed that several aspects are considered regarding the market situation, such as the current Ether (ETH) price or whether the current situation can be described as a bear market (i.e. strong market decline, pessimistic investors) or a bull market (i.e. strong market increase; confident investors).

Benchmarking means that companies that want to launch NFT projects determine their prices based on the comparison to the price of similar NFTs. The founder of an NFT project (I6) stated: "other things have been priced on around that time in the market". Thereby, it can be evaluated how high the price of comparable NFT collections was, whether they sold all NFTs or how the launch performed in general. I7 and I8, who have created several NFT collections, agree on this approach. I2, an NFT influencer and collector, goes even further: "I would say that's probably how the typical NFT project is priced up".

Another parameter for NFT price setting is the financial plan; projects calculate their minimum price based on costs including the expected profit. Especially I5 puts strong emphasis on cost-based pricing, including the effort which was spent on the development. I7 and I8 also mention that effort should be included in the pricing, but do not explicitly point out cost-based pricing. Apart from costs, many interviewees emphasise that profit is crucial. I8 described that referring to the profit

achieved by the mint, he was able to convince his investors that NFTs are lucrative to earn money. I6 states that the generated revenue across all NFTs is important, rather than looking at an individual NFT; half of their mints are free mints. In contrast, I2 mentions that projects are taking advantage of the hype and trying to make as much profit as possible.

The parameters supply and demand are intertwined as a scarcity in the supply leads to a demand which cannot be satisfied. Notably, these parameters were only mentioned by the experts who had already launched an NFT project themselves. On the one hand, they explained that, as sellers, they do not want to set the price too high, even though there would be enough demand. It should still be room for growth on the secondary market: "You don't want to overdo it. You don't want to overcharge people to maximize your return because they will suffer in the secondary" (I8). This even resulted in a project launch of I7 and I8 where the community voted on the price beforehand; hence, the community determined the price. However, I8 is also slightly critical regarding the demand as a measure and stated: "there was a built-in system where, if it didn't sell out, the remaining [NFTs] would be locked anyway" to ensure scarcity and a high price.

On the other hand, the hype around a project and the resulting demand are influenced by the experience of NFT creators / NFT project teams, i.e. whether they have launched successful projects before. For example, I8 mentions his own collection where he could charge 0.2 ETH, as "you look at the floor price of the previous collections as well" and the community starts to trust in the projects. Furthermore, I8 referred to another project which had a mint price of 2.5 ETH. Nevertheless, the demand was high as people had confidence in the project since the floor price of the previous collection was at 100 ETH. The floor price refers to the lowest price for an NFT of a certain collection on the secondary market.

The maximum mint price refers to the buyer's perspective, i.e. whether they set themselves a maximum price for which they would buy an NFT. Many experts agree that this is completely dependent on the project and cannot be generalised. For example, I4 would start to conduct more intensive research from a mint price of 0.2 ETH upwards; I5 referred to 0.5 ETH. Aspects of interest are inter alia the organisation behind the projects and their previous projects. For I2 "it simply comes down to the atmosphere around it". This approach is also connected to the supply and demand as the maximum mint price depends on how strong the community and their demand is. In fact, an increased hype and resulting demand also increased the willingness to pay.

4.2 Mint Mechanism

According to the experts, the mint mechanism can be based on first come, first served, an allowlist, a Dutch auction, a raffle and other mechanisms (cf. Figure 1).

First come, first served (FCFS) is based on fixed prices and enables anyone to mint an NFT until the full NFT collection is sold. FCFS is referred to as a simple mechanism by the experts; I2: "here's our price, here's our supply, we hope we sell out". Also, many projects want to make the mint process as simple as possible. I6 even said "[t]hat's probably our preferred approach, because it's the fairest way to price it". Furthermore, a fixed price reflects the fact that the project has been given some thoughts about the appropriate price. Besides its' benefit of simplicity, the experts point out that the mechanism of FCFS has a major downside – gas wars. When the demand for NFTs is much higher than the supply, only the fastest buyers receive an NFT. Therefore, they spent large sums of transaction fees (gas cost) to accelerate the process of adding their transaction to the next block in order to securely mint an NFT.

An allowlist is a mechanism which is linked to the fixed price aiming to prevent gas wars. Thereby, a list of wallet addresses is created (i.e. allowlist/whitelist), which are guaranteed to be able to mint a predefined amount of NFTs [20]. Whilst most experts state that they initially liked the idea of a fairer approach, many of them are no longer convinced of this approach; "we've moved away from that recently" (I6). Mainly criticised is the way and the effort to get on such an allowlist. For example, I5 criticised that people working or going to school are not able to put in the effort which is required. I4 even hired a graphic designer to create fan art to become whitelisted.

The raffle as a mint mechanism addresses the critique of gas wars (cf. FCFS) and high effort for allowlist spots. In a raffle, mint slots are randomly assigned to registered wallet addresses (cf. lottery). Therefore, I2 and I5 emphasise that raffles are one of the fairest mint mechanisms. Furthermore, they are a good indication for NFT projects on the number of interested buyers. I8 highlights that raffles especially make sense in the bear market; otherwise they had no problems being sold out. Often, NFT raffles are performed on the website Premint. I4 likes that it enables to link raffle tickets to certain access requirements, such as following on Twitter. However, I4 also criticises that some projects on Premint can overallocate the mint permissions in the bear market and, thus, end up in a gas war again. Another downside is the abuse by so-called bots (i.e. software) and users creating multiple wallets. This results in "people that got several entries accepted" (I2), i.e. the mechanism being unfair again.

Dutch auctions (also reverse auctions), i.e. auctions starting at a very high price and lowering gradually until

the first buyer bids [21], are known by all experts. I2 and I4 like Dutch auctions as "that kind of sales are more fun [...] to watch" (I4) and they associate them with the sale of traditional art. However, most experts are not enthusiastic about Dutch auctions. For example, I6 criticises that: "it drives it optimises for the creators of the project to get the most money and it doesn't optimise for the value of the project, for the community". I1, I3, and I8 agree that one of the reasons for a Dutch auction is to generate as much revenue as possible. Also, it leads to an unfair distribution, "because if you have some extra Ethereum, you know you're going to get it" (I8). This aspect if faced by an adapted form of Dutch auctions.

Apart from established mint mechanisms, several experts suggest adapted versions for NFT launches. I2 and I4 mention a special form called fair Dutch auction. According to the description of I4, this approach works as follows: the lowest price of the auction is the final price. For example, the auction starts at 1 ETH and the last NFT is sold at 0.3 ETH; now, every buyer gets a refund of the difference to this price, i.e. a refund of 0.7 ETH for the first buyer. As everyone just pays the 0.3 ETH in the end, the experts consider this approach to be fair. Furthermore, I2 points out that this satisfies different kinds of buyers as "you have big money people out there that say, hey, I know I want 50 of these, but I don't have 3 hours to wait around [...]. So, I'll just buy in early knowing that I will get a refund and I'll get the appropriate price at the end."

Besides auctions, two experts suggest adapted selection procedures to mint a fixed price NFT. For example, I3 proposes virtual queues, i.e. "a queue that says our mint goes on sale at 02:00 p.m., and at 02:00 p.m. you click the queue button and you join a queue that's first come, first serve". Beyond that, I6 mentions that their project no longer uses an allowlist, but a kind of raffle with adapted mint conditions. Their algorithm "scores the wallet that you hold"; the chance to win a raffle ticket is weighted with the wallet score. "So, it rewards existing community members with the ability to get a higher chance of receiving the raffle ticket if you've got more of the community assets" (I6).

4.3 Promotion

For promoting NFT launches, the experts refer to the categories advertisements, partnerships, and scarcity marketing (cf. Figure 1).

Advertisements are used to call the attention of potential buyers to NFT launches. I7 and I8 mention how intensively they have been advertised in a bear market. Then, buyers are very cautious as there are a lot of NFT projects on the market; a solid marketing is very important to stand out from the other projects. Hence, the experts aimed to get as much attention as possible. I1 highlights the importance of having a presence on Twitter or Discord, because this is the "town of crypto" and where everyone is.

An important part of promotion activities for NFT launches are advertisements with partners or influencers; "we partnered with Brian, Lewis Hamilton and Snoop Dogg" (I8). Partners promote the project or special sub-collections of NFTs are created with them. The aim is that partnerships with well-known people increase the awareness and build trust in the project. Especially interesting is their payment model, as I8 states: "We actually didn't pay them any money. It was purely they all got some NFTs and [..] success at the [..] sale".

An existing marketing approach that has been adopted to promote NFTs is scarcity marketing. In the case of NFTs, a shortage in the supply is created, i.e. NFT collections are severely limited in their number of single NFTs. This approach aims to evoke a demand in potential buyers and make the minting experience more exciting. I4 mentions that mint mechanisms in general cause the aspiration to outbid others and get the opportunity to mint an NFT at all costs. I5 makes a comparison to his own life: "When I was in San Diego, I liked surfing bigger waves because it felt risky. [...] That was NFTs. There was a big excitement for people. I mean definitely the money is nice but the excitement was just great." This scarcity increases the demand when NFTs are minted, but also results in higher prices afterwards.

5. Discussion

As follows, the results obtained from the expert interviews are interpreted and discussed with regard to the literature.

5.1 Price Setting

In the business management pricing theory, three different pricing strategies are differentiated, i.e. cost-based pricing, competitor-based pricing, and value-based pricing [22].

Cost-based pricing is about creating prices based on costs, i.e. companies calculate their costs and add a profit margin to calculate the price. A variation of this approach is to calculate the price only based on the costs [22]. This cost-based approach without margin is reflected in the interviews, as some experts mention that mint prices were determined on the basis of costs, or that the effort was chosen as the reference point for determining the mint price. The suggestion to determine the price of NFTs according to their costs or the required funding to create them is also supported by [23] who makes recommendations for NFT projects. However, I8 points out the importance of the achieved profit to attract investors.

Following a competitor-based approach, the price is determined based on an analysis of similar or almost identical products of competitors [22]. This approach is often named by collectors who assume that creators

determined the price of their NFTs this way (cf. benchmarking). [23] also emphasises this approach and states that projects should analyse at what prices other NFT projects sell their NFTs. Although the competitor-based approach is mentioned in theory, according to the experts it is equally important to analyse the market (cf. bull market vs. bear market, ETH price), especially in the area of NFTs (cf. market situation).

The approach of value-based pricing refers to the demand of customers and their willingness to pay [22]. These aspects also have been discussed in the context of NFT pricing, summarised in the parameters supply and demand, and maximum mint price. Remarkably is that most NFT creators refer to the demand when determining the price. However, they do not set the price based on the willingness to pay, but rather stay below this price as they do not want to overcharge the customers given that there should still be room to grow on the secondary market. Some projects even let the community actively decide on a fixed price through voting, instead of a price which is determined on the overall demand.

Another aspect referring to the hype and resulting demand of a project is the experience of NFT creators, i.e. successful projects launched before. This ensures a certain confidence for another successful project and enables a higher price during the launch. The experts argue that this is enabled by an increased trust of the community. In theory, this approach is associated with the penetration strategy. Thereby, companies initially price products low to achieve a high market share, and later increase the price successively [6]. This strategy is suitable when manufacturers (i.e. creators) can sufficiently reduce the production and take a leadership position or when a low price is needed to overcome acceptance barriers [24]; [25]. Both arguments are valid for NFTs as creators can determine the number of NFTs in a collection (i.e. the supply), and the large number of NFTs and the volatility of cryptocurrencies can be an acceptance barrier for new customers.

In summary, all of the approaches of price setting in theory could have been identified in the expert interviews. However, many of the experts emphasise that not only the analysis of competitors but rather the current market situation in general is important, especially as it is more volatile. Accordingly, they e.g. look current cryptocurrency prices and publish prices only a few days before the launch such that it can be still adjusted. Surprisingly, none of the experts explicitly mentioned payments to artists who e.g. design digital collectibles. However, this might be included when referring to costs.

5.2 Mint Mechanism

As follows, we discuss the identified launch mechanisms along different mechanisms with fixed prices (cf. FCFS, allowlist, raffle) as well as variable prices, i.e. auctions. Thereby, we summarise their advantages and challenges and refer to their evaluation by the experts as well as the literature.

According to the literature, a fixed price on a first come, first served basis is the most widespread method of carrying out an NFT launch [15]. This is also reflected in the analysis of the interviews. All three experts who work on NFT projects agree that this mint mechanism is the most common for their NFT collections. Also, three of the NFT collectors, perceive FCFS based fixed prices as positive. Furthermore, according to the NFT literature, the price is usually set below the actual market price to increase participation in the launch [15]. This is also underlined by the experts who mention that the price should be determined such that it can still rise on the secondary market.

Whilst in the literature fixed prices on a FCFS basis are mainly associated with gas wars (e.g. [26]), the experts' opinions differ. On the one hand, experts from NFT projects report that they have never had problems with high gas fees in their own projects. On the other hand, an important issue mentioned during the interviews is the changed NFT value in case of gas wars. This means that an NFT that is actually priced at e.g. $100 suddenly costs $800 due to the high gas fees. This is especially counter-productive for the resale on the secondary market, which is an important aspect according to the experts. However, further mint mechanisms based on fixed prices which address the problem of gas wars are continuously developed (cf. usage of an Azuki contract ERC 721A [27]).

The mint mechanisms allowlist and raffle were inter alia built to reduce the amount of gas buyers have to pay when minting. Of all experts interviewed, only I3 stated that a fixed price in connection with an allowlist is his favourite mechanism. I5 mentioned that in the beginning an allowlist was a fair thing. In fact, allowlists have several benefits such as guaranteed access to mint, avoiding high gas fees, and not having to worry about bots buying up all of the NFTs [20]. However, I3 stated that this mechanism always depends on how to get an allowlist spot. I5 points out that, meanwhile, there are people who do nothing else all day but try to get on the allowlist. He thinks that is unfair to those who do not have time for that and suggests that the projects should have a varied system. I4 mentions that he hired a graphic designer to create fanart for him to get on the whitelist. Apart from the interviews, an NFT influencer described this approach in a tweet as follows: "It's a full-time job getting on whitelists for NFTs..." [28].

The experts as well as the literature considers raffles to be fair as the choice who can mint an NFT is randomised. Usually, selected wallet addresses have a certain period of time to mint, which allows them to mint when the gas fees are low. This, as well, reduces the transaction costs when minting an NFT [15]. The literature suggests different raffle-based NFT launch mechanisms, such as

[29]. Furthermore, the experts appreciate about a raffle via Premint the various requirements offered. For example, I8 thinks that raffles are very successful especially in the bear market. He justifies this by the fact that it was only possible for people to register for a raffle who own partner NFTs, as these are the people who are really interested and want to be part of the community. However, even this launch mechanism has its weaknesses, as people/bots e.g. register with multiple wallets and, thus, strongly increase their chances of winning a ticket. I3 compares this practice to the release of limited-edition sneakers, where bots were also used at some point (confirmed by [30]). I3 argues that because the mints gained more hype and became more competitive, people started trying other ways to ensure to get an NFT. Thereby, bots can be used in various ways, as described in detail by [31].

Apart from fixed price mechanisms which can be differentiated based on the selection procedure of wallet addresses which can mint, auctions determine this by variable prices. In a Dutch auction, the price is continuously reduced [21] until all NFTs are sold. According to the literature, the choice of this mechanism is justified by the fact that it does not create gas wars [32]. Interestingly, this argument has not been confirmed by our empirical data. None of the experts associate Dutch auctions with the avoidance of gas wars. In contrast, four of the experts relate them with profit maximisation of projects. For example, this is why I8 also emphasises that he explicitly did not choose a Dutch auction because he did not want to demand the maximum price but a price that he considered to be fair. This is faced by fair Dutch auctions, mentioned by two experts. Interestingly, this adapted approach of Dutch auctions is not known in the scientific literature, but seems to be designed for the launch of NFTs [33].

Moreover, the experts suggested different adaptions of existing auction mechanisms (cf. fair Dutch auction) or selection procedures (cf. adapted raffle mechanism based on wallet scores by I6), which are even unknown in the NFT-specific literature. Other adaptions are based on the launch of scarce products of different fields, such as the idea of virtual snakes (cf. I3), which are used in limited-edition sneaker releases [34]. Even though such adapted approaches aim to improve mint mechanisms, I3 adds the fairness cannot be ensured. For example, virtual queues require people to register at a certain point in time to join the group of the 10,000 first people who get the NFT. However, the human reaction is somewhere around 0.14 seconds and everything below that is pure coincidence or caused by bots. Therefore, they need to be excluded to ensure a fair mechanism.

Overall, most experts state that there is not one perfect mint mechanism; it rather depends on many factors. However, several mechanisms are susceptible to bots, which needs to be addressed to ensure a fair launch.

5.3 Promotion

The experts as well as the literature agrees that promotion is an important factor for NFT launches. According to [35] and [36], a project has to stand out from the crowd of NFT projects to attract attention. They name different strategies to do so, such as social media marketing, and advertisements with influencers. Partnerships with well-known people is what I7 and I8 also apply in their start-up to increase their reach. According to them, this also includes the formation of a community as a marketing tool. Further, I7 reports that they have engaged in other Discord channels (cf. social media) to advertise their project. According to I1, it is important to promote an NFT launch on Twitter or Discord. Overall, the empirical findings as well as the literature agree that it is important to generate attention and, therefore, to build a community.

Another promotion parameter for NFT launches is the fact that NFTs are usually scarce. I2 compares an NFT mint to the drop of exclusive sneakers, both are hyped products which are only available in limited quantities. I4 is convinced that NFT mints trigger a fear of missing out on something that others have. In the literature, scarcity marketing is well understood and the statements in the interviews can be confirmed. For example, [37] mention that once a product is available in limited quantities, people are more willing to fight for it. Furthermore, [38] confirms that scarce goods are mainly luxury goods and therefore scarcity and exclusivity are related. In the context of NFTs, projects use supplier-induced scarcity strategy, i.e. a conscious strategy of marketers to limit the production or availability of a product [39]. In the context of luxury goods, this strategy is also referred to as a limited-edition scarcity [40].

6. Conclusion

Our research contributes to the understanding of NFT launch strategies by referring to the pricing strategy, mint mechanism, and promotion. Thereby, we provide valuable insights for industry practitioners, artists, and collectors. As the discussion revealed, NFT projects mainly use established concepts from theory when planning and conducting their launches. However, some aspects are important along all marketing mix instruments when launching NFTs.

On the one hand, our empirical findings point out the importance of the market situation as it is highly volatile in this field. The market situation (i.e. bull/bear market, cryptocurrency prices, demand/supply) is important when determining the price (cf. competitor-based pricing; value-based pricing referring to the demand), the mint mechanism (e.g. raffles making sense in the bear market), as well as the marketing strategy (cf. attracting buyers in bear markets).

On the other hand, the community is an essential aspect of an NFT launch. During the price setting, the community is important as many experts as aim for fair

prices which enable further gains on the secondary market. Also, an established community resulting from a successful previous launch enables to set higher prices. In mint mechanisms, fairness is a major factor as well and, thus, several experts developed enhanced mint mechanisms. Furthermore, the community can be essential when taking part in raffles as several access requirements are community-related (cf. Premint), such as the participation in social media communities. When promoting NFTs, the experts put emphasis on the importance of partnerships and Twitter/Discord as a promotion channel, i.e. social media marketing in the crypto community.

Overall, our research introduces several parameters for NFT launch strategies. They provide opportunities for future research by facilitating the development of best practices when launching NFTs. These will aid practitioners in launching successful NFT projects, but also accelerate the adoption of Blockchain Technology in general.

Contact details

Department of Intelligent Information Systems, University of Hohenheim, Stuttgart, Germany

Josepha Witt

jwitt@uni-hohenheim.de / ORCiD 0000-0001-7668-4902

Literature references

[1] Kölbel, Tobias; Joussen, Katrin; Weinhardt, Christof (2023): Between Hype, Hope, and Reality: A Lifecycle-Driven Perspective on Non-Fungible Token, in: Proceedings of the 31st European Conference on Information Systems (ECIS), Kristiansand, Norway.

[2] Chohan, Raeesah; Paschen, Jeannette (2023): NFT marketing: How marketers can use nonfungible tokens in their campaigns, in: *Business Horizons,* 66 (1), pp. 43–50.

[3] Hofstetter, Reto; Bellis, Emanuel de; Brandes, Leif; Clegg, Melanie; Lamberton, Cait; Reibstein, David et al. (2022): Crypto-marketing: how non-fungible tokens (NFTs) challenge traditional marketing, in: *Marketing Letters,* 33, pp. 705–711.

[4] Ko, Hyungjin; Son, Bumho; Lee, Yunyoung; Jang, Huisu; Lee, Jaewook (2022): The economic value of NFT: Evidence from a portfolio analysis using mean–variance framework, in: *Finance Research Letters,* 47 (A).

[5] Cooper, Robert (1979): The Dimensions of Industrial New Product Success and Failure, in: *Journal of Marketing,* 43 (3), pp. 93–103.

[6] Hultink, Erik Jan; Schoormans, Jan P.L. (1995): How to launch a high-tech product successfully: An analysis of marketing managers' strategy choices, in: *Journal of High Technology Management Research,* 6 (2), pp. 229–242.

[7] Hultink, Erik Jan; Hart, Susan J.; Robben, Henry S.J.; Griffin, Abbie J. (1999): New consumer product launch: Strategies and performance, in: *Journal of Strategic Marketing,* 7 (3), pp. 153–174.

[8] Satoshi Nakamoto (2008): Bitcoin: A Peer-to-Peer Electronic Cash System, [online] https://bitcoin.org/bitcoin.pdf [28.07.2023].

[9] Oliveira, Luis; Zavolokina, Liudmila; Bauer, Ingrid; Schwabe, Gerhard (2018): To Token or not to Token: Tools for Understanding Blockchain Tokens, in: Proceedings of the 39th International Conference on Information Systems (ICIS), San Francisco, USA, December 13-16.

[10] Regner, Ferdinand; Urbach, Nils; Schweizer, André (2019): NFTs in Practice – Non-Fungible Tokens as Core Component of a Blockchain-based Event Ticketing Application, in: Proceedings of the 40th International Conference on Information Systems (ICIS), Munich, Germany, December 15.-18., pp. 1–17.

[11] Pawelzik, Leon; Thies, Ferdinand; Fachhochschule, Berner (2023): Selling Digital Art for Millions-a Qualitative Analysis of NFT Art Marketplaces, in: Proceedings of the 31st European Conference on Information Systems (ECIS), Kristiansand, Norway, June 11.-16., pp. 1–15.

[12] ethereum.org (2023): ERC-721 Non-Fungible Token Standard, [online] https://ethereum.org/en/developers/docs/standards/tokens/erc-721/ [28.07.2023].

[13] Wang, Qin; Li, Rujia; Wang, Qi; Chen, Shiping (2021): Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges, in: *arXiv preprint,* arXiv:2105.07447.

[14] beeple (2023): EVERYDAYS | the work of Mike Winkelmann, [online] https://www.beeple-crap.com/everydays [28.07.2023].

[15] Arditi, Andy; Hirsch, Dean; Garimidi, Pranav; Milionis, Iason (2021): An Initial Framework for NFT Auction Mechanism Design : Impossibility Results and Solutions, in: *Foundations of Blockchains, COMS 6998-006, Columbia University*, pp. 1–24.

[16] Flick, Uwe (2018): An introduction to qualitative research, 6th ed., Los Angeles: Sage.

[17] Bogner, Alexander; Littig, Beate; Menz, Wolfgang (2014): Interviews mit Experten: Eine praxisorientierte Einführung, Wiesbaden: Springer VS.

[18] Kuckartz, Udo (2018): Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung, 4th ed., Weinheim: Beltz.

[19] Mayring, Philipp (2010): Qualitative Inhaltsanalye - Grundlagen und Techniken, 11th ed., Weinheim: Beltz.

[20] White-Gomez, Alex (2022): Everything You Need to Know About NFT "Allowlists" and "Pre Mints", in: *ONE37pm*, 7/19/2022, [online] https://www.one37pm.com/nft/allow-lists-pre-mints [28.07.2023].

[21] Haucap, Justus (2020): Auktionen in Theorie und Praxis, in: *WiSt - Wirtschaftswissenschaftliches Studium,* 49 (12), pp. 36–42.

[22] Diller, Hermann; Beinert, Markus; Ivens, Björn; Müller, Steffen (2021): Pricing: Prinzipien und Prozesse der betrieblichen Preispolitik, 5th ed., Stuttgart: Kohlhammer.

[23] Dee, Jim (2022): What Should the Mint Price Be When Launching a Set of 10,000 Generative NFTs on the ETH Blockchain?, [online] https://medium.com/web-design-web-developer-magazine/what-should-the-mint-price-be-when-launching-a-set-of-10-000-generative-nfts-on-the-eth-blockchain-4744f9fc4ef [28.07.2023].
[24] Guiltinan, Joseph P. (1999): Launch strategy, launch tactics, and demand outcome, in: *Journal of Product Innovation Management,* 16 (6), pp. 509–529.
[25] Kotler, Philip (2003): Marketing Mangement, 11th ed., Upper Saddle River: Prentice-Hall.
[26] Ko, Kyungchan; Jeong, Taeyeol; Woo, Jongsoo; Hong, James Won-Ki (2022): An Analysis of Crypto Gas Wars in Ethereum, in: Proceedings of the 23rd Asia-Pacific Network Operations and Management Symposium (APNOMS), Takamatsu, Japan, September 28-30, pp. 1–6.
[27] Azuki: Introducing ERC721A: An Improved ERC721 Implementation, [online] https://www.azuki.com/erc721a [25.07.2023].
[28] Fanzo (2022): It's a full-time job getting on whitelists for NFTs..., [online] https://twitter.com/iSocialFanz/status/1482779919440564225?s=20 [28.07.2023].
[29] Ko, Kyungchan; Jeong, Taeyeol; Woo, Jongsoo; Hong, James Won-Ki (2023): Alleviating Crypto Gas War in NFT Launching, in: Proceedings of the 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Dubai, United Arab Emirates, May 1-5, pp. 1–5.
[30] Mcconnell, Alex (2021): How Bots are Being Used to Skew NFT Prices for Big Profit, [online] https://netacea.com/blog/how-bots-skew-nft-prices-for-big-profit/ [28.07.2023].
[31] Kasada (2022): How NFT Bots Exploit Marketplaces Why NFTs are the Latest Target for Scalper Bots, [online] https://www.kasada.io/nft-bots/ [28.07.2023].
[32] Centieiro, Henrique (2021): What is a Dutch Auction and Why it Matters in the NFT Space?, [online] https://medium.com/geekculture/what-is-a-dutch-auction-and-why-it-matters-in-the-nft-space-59d5d26369f9 [27.07.2023].
[33] Rei (2022): PXN Fair Dutch Auction Public Sale, [online] https://medium.com/@rei_49876/pxn-fair-dutch-auction-public-sale-bc79a22a8168 [27.07.2023].
[34] Loeffen, Tygo (2022): Rise Rise of the Purchasing Programs. Reluctant Adoption of 'Bots' within Sneaker Consumer Culture, Radboud University: Master Thesis.
[35] Dhruv, Singhwani (2022): Best design practices & strategy to launch your own NFT project, in: *Trends in Computer Science and Information Technology,* 7 (1), pp. 7–9.
[36] Macy, Scott (2022): NFT Marketing Guide 2022, [online] https://medium.com/geekculture/nft-marketing-guide-2022-22fa8ed7cb3a [27.07.2023].
[37] Grossman, Herschel; Mendoza, Juan (2003): Scarcity and appropriative competition, in: *European Journal of Political Economy,* 19 (4), pp. 747–758.
[38] Oruc, Ruziye (2015): The effects of product scarcity on consumer behavior: A meta-analysis, Europa Universität Viadrina Frankfurt (Oder): Doctoral Thesis.
[39] Balachander, Subramanian; Liu, Yan; Stock, Axel (2009): An Empirical Analysis of Scarcity Strategies in the Automobile Industry, in: *Management Science,* 55 (10), pp. 1623–1637.
[40] Janssen, Catherine; Vanhamme, Joëlle; Lindgreen, Adam; Lefebvre, Cécile (2014): The Catch-22 of Responsible Luxury: Effects of Luxury Product Characteristics on Consumers' Perception of Fit with Corporate Social Responsibility, in: *Journal of Business Ethics,* 119 (1), pp. 45–57.

Application of Blockchain Technology for Supply Chain Management - The Example of Paper-Based Coffee Cups

Naiema Shirafkan, Marcus Wiens
TU Bergakademie Freiberg, Freiberg, Germany

Abstract:
Safety, quality, and sustainability concerns have arisen from global supply chains. Stakeholders incur risk regarding these factors, given their significance and complexity. Thus, each business's supply chain risk management must prioritize product characteristics. Accordingly, an effective traceability solution that can monitor and regulate product and supply chain aspects is crucial, especially in a given scenario. This re-search paper elucidates the potential of smart contracts in blockchain to enhancing the efficacy of business transactions and ensuring comprehensive traceability within the supply chain of paper-based coffee cups The improved levels of transaction transparency and security in traditional supply chains have been achieved through the digitization of supply chain ecosystem interactions and transactions. This approach makes verifying sources, manufacturing procedures, and quality standards easier in complex supply chains. Accordingly, the integration helps stakeholders monitor and track the whole ecosystem, promoting transparency, predictability, and dependability.

1. Introduction

This article shows an application of blockchain technology to the supply chain of paper-based coffee cups as means to enhance efficiency, safety and security in supply chain management. It emphasizes the growing concerns about product safety and the importance of traceability throughout the supply chain procedure. The process of establishing traceability involves collecting and managing critical data to determine the product's origin and enable the exchange of information [19]. However, the dynamic nature of data in the supply chain poses challenges in monitoring and tracing the products as they go through various stages [12]. In case of product distribution, close coordination among multiple stakeholders is required to identify relevant product characteristics and to intervene in the process, e.g. removal affected products swiftly [17]. However, exchanging information between stages in the supply chain proves to be a challenging and time-consuming coordination process [13].

Consequently, we introduce blockchain technology as a promising solution for ensuring traceability in the supply chain of the case paper-based coffee cups. It explains that blockchain's transparency, immutability, and security can be effectively utilized in supply chain management [25]. The complexity of the supply chain, involving multiple stakeholders, necessitates a secure framework for tracking information about the products, and safety without relying on a centralized authority [6]. Additionally, blockchain technology addresses these challenges and can enhance trust among stakeholders by providing a shared distributed ledger and tamper-proof records [3]. Accordingly, the article also mentions Ethereum, a programmable blockchain platform, which allows for the execution of smart contracts without third-party intervention [20]. It discusses how blockchain and Ethereum smart contracts can efficiently trace and track paper-based coffee cups, integrating business transactions and workflows in the supply chain as shown in Figure 1. Then, we present the system design, architecture, and sequence diagrams, along with the theoretic implementation of smart contract algorithms governing interactions among key stakeholders.

The paper explores the use of blockchain in this specific product supply chain. It discusses some related literature in Section 2, presents the design and system overview in Section 3, describes implementation details including smart contract algorithms in Section 4. The article concludes in Section 5 by outlining research challenges and future work.

2. Literature review by exploring the related works

In this section, we review the existing body of literature concerning the utilization of blockchain technology in the industry of paper-based coffee cups and its associated supply chains. While there has been a steady increase in the amount of literature addressing blockchain applications in areas such as banking, finance, and insurance, existing research on the issue of food and packaging production remains limited but is fast gaining traction.

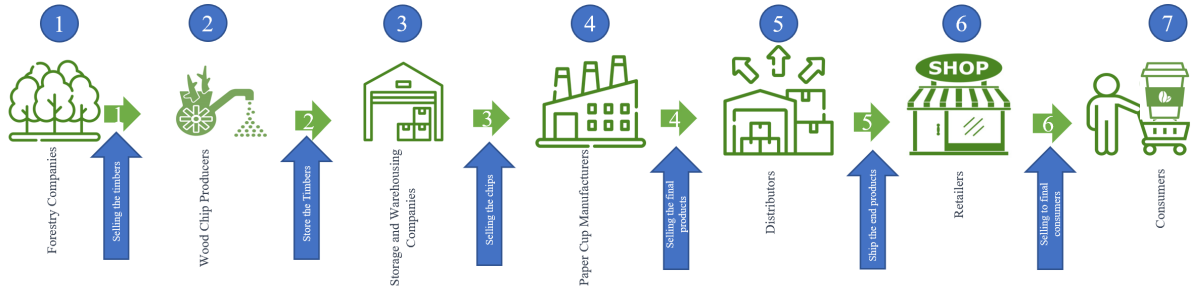

Figure 1-Traditional Participants in Supply Chain of paper-based coffee cup

Bager et al. 2022, highlights the potential of blockchain technology in creating secure and decentralized supply chain management systems. The authors propose an event-based methodology called REALISTIC, along with an event-driven system architecture, for tracking products in supply chain networks. The study focuses on the coffee industry, showcasing a case study and an open-source prototype to validate the proposed approach [1]. The other study examines the potential of blockchain in promoting sustainability in supply chains by Bager et al. 2022. While the pilot implementation highlights certain benefits, it suggests that blockchain is not a one-size-fits-all solution. Digitizing the supply chain using centralized digital solutions can achieve similar outcomes without the high costs associated with blockchain due to the higher cost of implementation. Blockchain may be more suitable for high-end or segregated supply chains, but implementation challenges exist, and the value lies in understanding incentives, trust, technology availability, and data transfer [2]. Additionally, Tian 2017 puts forth a blockchain-based traceability system for the food supply chain, incorporating Hazard Analysis and Critical Control Points (HACCP) and the Internet of Things (IoT) [23]. Tian 2016, also discusses the advantages and disadvantages of RFID and blockchain for traceability in the agricultural food supply chain [22].

Furthermore, IBM has played a leading role in utilizing blockchain technology to enhance supply chain transparency in the food industry. Their solutions have helped food companies improve efficiency, reduce fraud, and ensure the safety and authenticity of food products. Consumer surveys indicate a growing demand for transparency, with a majority valuing knowledge of food origins and willingness to pay more for responsibly sourced products, while brand loyalty is positively influenced by complete transparency [11]. Tse et al. 2017 explore the application of blockchain technology in the food supply chain at a high level and draw comparisons with traditional solutions, emphasizing aspects related to security, integrity, and trust [5].

Düdder and Omri's paper 2017 highlights the significance of using Blockchain technology to address sustainability challenges in supply chains, urging for more research and collaboration in this area. While efforts have primarily focused on finance, the authors advocate for expanding Blockchain applications to promote sustainability and benefit society as a whole [7]. Moreovre, Groschopf et al. 2021, highlight the potential of smart contracts in supply chains, emphasizing their ability to streamline processes, reduce errors, and lower costs. It explores the relationship between smart contracts, sustainability, and supply chain management, noting that research in this area is still limited. The article defines smart contracts, conducts a literature review, proposes a conceptual framework, and suggests research propositions and trade-offs regarding technology development, business processes along the supply chain, and sustainability. Despite its limitations, the paper aims to inspire further research and practical applications in the context of Industry 4.0 ecosystems, promoting the integration of physical and digital worlds in supply chain optimization [10]. Wamg et al. 2019, presents a blockchain-based product traceability system using smart contracts, ensuring immutable records of product transfers. The system allows consumers to participate as nodes, maintaining information flows and reducing data tampering risks. An event response mechanism verifies transaction parties' identities and stores events permanently in the blockchain. A decentralized application (DApp) is developed, and future research focuses on optimizing the system through IoT for error reduction and QR code technology to enhance consumer experience and simplify operations. The system demonstrates data accessibility, tamper-proofing, and resistance to man-in-the-middle attacks according to security analysis results [24]. Mao et al. 2018 introduce a blockchain-based credit evaluation system that employs smart contracts for efficient management in the food supply chain [14].

The aforementioned instances serve as evidence of the increasing inclination towards the utilization of blockchain technology to augment the levels of information security, transparency, and authentication within the supply chains of food production and related sectors. While numerous studies explore the conceptual application of blockchain in product supply chains, our paper aims to bridge the gap by presenting a specific implementation framework and approach. We demonstrate how blockchain and Ethereum smart contracts can provide an efficient, trusted, secure, and decentralized traceability solution for the industry of paper-based coffee cups and its supply chains. Our work highlights the

key features of the proposed system, including architecture, metadata, sequence diagrams, and algorithms, which can be applied to various use cases involving multiple stakeholders in the agricultural supply chain.

3. A Blockchain-Based Approach for in Implementing the Traceability in the Mentioned Case

This section will outline the proposed solution for the tracing, tracking, and execution of transactions within paper-based coffee cup supply chains. The solution utilizes the Ethereum blockchain and smart contracts. Our solution eliminates the need for a trusted centralized authority and offers a high level of integrity, reliability, and security for managing and ensuring the safety of products supply chains. Moreover, the solution leverages Ethereum smart contracts to establish an integrated smart system that ensures the safety and quality of products delivered to end consumers as it is shown in Figure 2. The execution of contract functions and code is autonomously performed by globally distributed mining nodes through the utilization of smart contracts on the public Ethereum blockchain platform [16]. These nodes validate and execute transactions, store data, and maintain a replicated ledger synchronized across the network [15]. The smart contracts receive transactions and trigger events, allowing participating entities to monitor, track, and receive alerts for any violations within the product value chain [18]. Specifically, the solution focuses on the paper-based coffee cups supply chain. The system architecture includes key participants such as the Forestry Companies/Tree Farmers, Wood Chip Producers, Storage and Warehousing Companies, Paper Cup Manufacturers, Distributors, Retailers, end End-user Consumers, regarding the Ethereum blockchain with the Ethereum Virtual Machine (EVM) executing the smart contract. Every individual involved in the blockchain possesses an Ethereum account that is distinguished by a distinct Ethereum Address (EA). This EA is responsible for cryptographically signing and verifying the integrity of transactions, thereby establishing a connection between each transaction and a particular account [4]. Accordingly, each participating entity has a role, association, and interactions with the smart contract. The seven participating presented entities in Figure 1 and their role are summarized as follows:

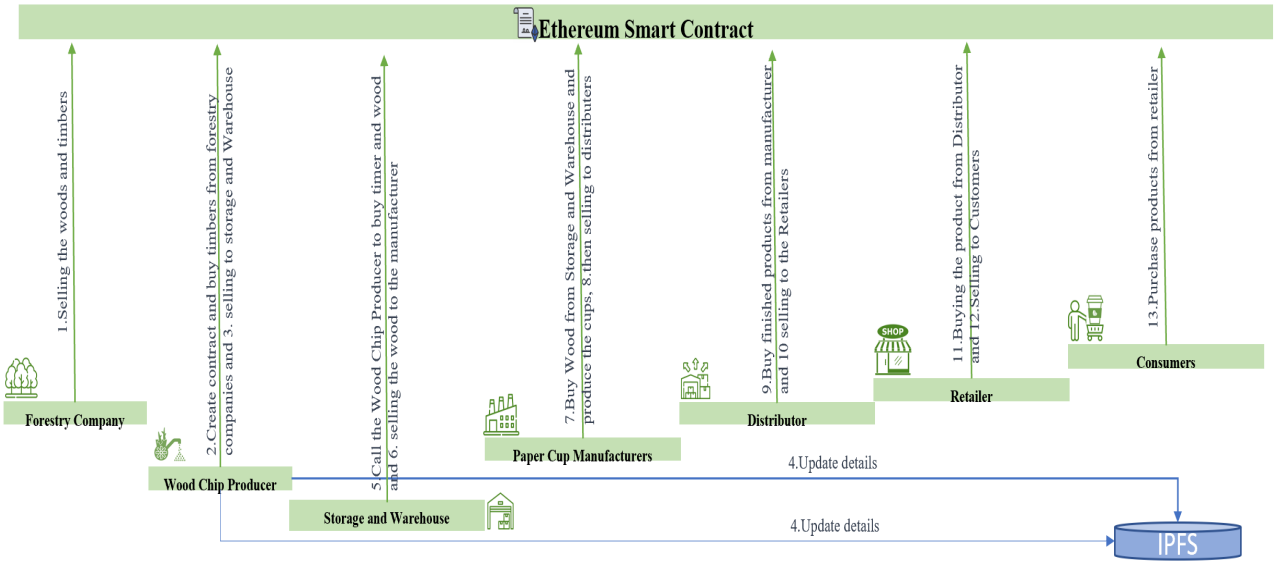

Figure 2-System overview for automating paper-based coffee cup traceability using Ethereum smart contracts

1.Forestry Companies/Tree Farmers: These stakeholders are responsible for managing and harvesting trees mainly in the forests. They ensure a sustainable supply of timber by planting, growing, and harvesting trees specifically for the paper industry. Loggers are also involved in cutting down trees in accordance with forestry regulations. They transport the logs to the next stage of the supply chain.

2.Wood Chip Producers: Once the trees are cut down, the logs are sent to wood chip producers. Their role is to debark the trees (removing the outer layer) and chip them into smaller pieces. These wood chips will serve as the raw material for paper cup production.

3.Storage and Warehousing Companies: These stakeholders provide storage facilities for the chipped wood until it is ready for further processing. They ensure proper inventory management and facilitate efficient supply chain operations.

4.Paper Cup Manufacturers: Paper cup manufacturers receive the chipped wood as their raw material. They have specialized machinery and equipment to process the wood chips into pulp. The pulp is then formed into paper sheets, which are further treated to make them suitable for cup production. The manufacturers convert the treated paper into cups, including shaping, cutting, and forming them with the necessary coating and designs. Then, they provide additional components necessary for paper cup production, such as lids, sleeves, and any branding or labeling materials required by the manufacturers.

5.Distributors: Distributors play a crucial role in the supply chain by transporting the manufactured paper cups from the production facilities to various retailers and wholesalers. They coordinate logistics and ensure the cups reach the intended destinations in a timely manner.
6.Retailers: Retailers, such as coffee shops, cafes, and convenience stores, are the end points where consumers can purchase paper-based coffee cups. They stock and display the cups for consumers to buy.
7.Consumers: Consumers are the ultimate stakeholders in the supply chain process. They purchase and use the paper-based coffee cups to enjoy their hot or cold beverages.

The study provides a supply chain-wide Ethereum smart contract framework to monitor production securely [8]. The foster companies produce trees and records details such as germination, chemical composition, viability, quality, and dormancy. The Wood Chip Producer purchase the tress, documents timber accumulation growth using decentralized file systems and timestamps, and debarks the timbers in a Warehouses, considering factors like temperature and moisture. The manufacturer refines the woods, analyzes its quality, eliminates moisture, and prepares the finished product as coffee-cups. The distributor buys the final product and serves as a point of contact for prospective purchasers. The distributor then sells the items to the retailer, who ultimately sells them to customers directly.

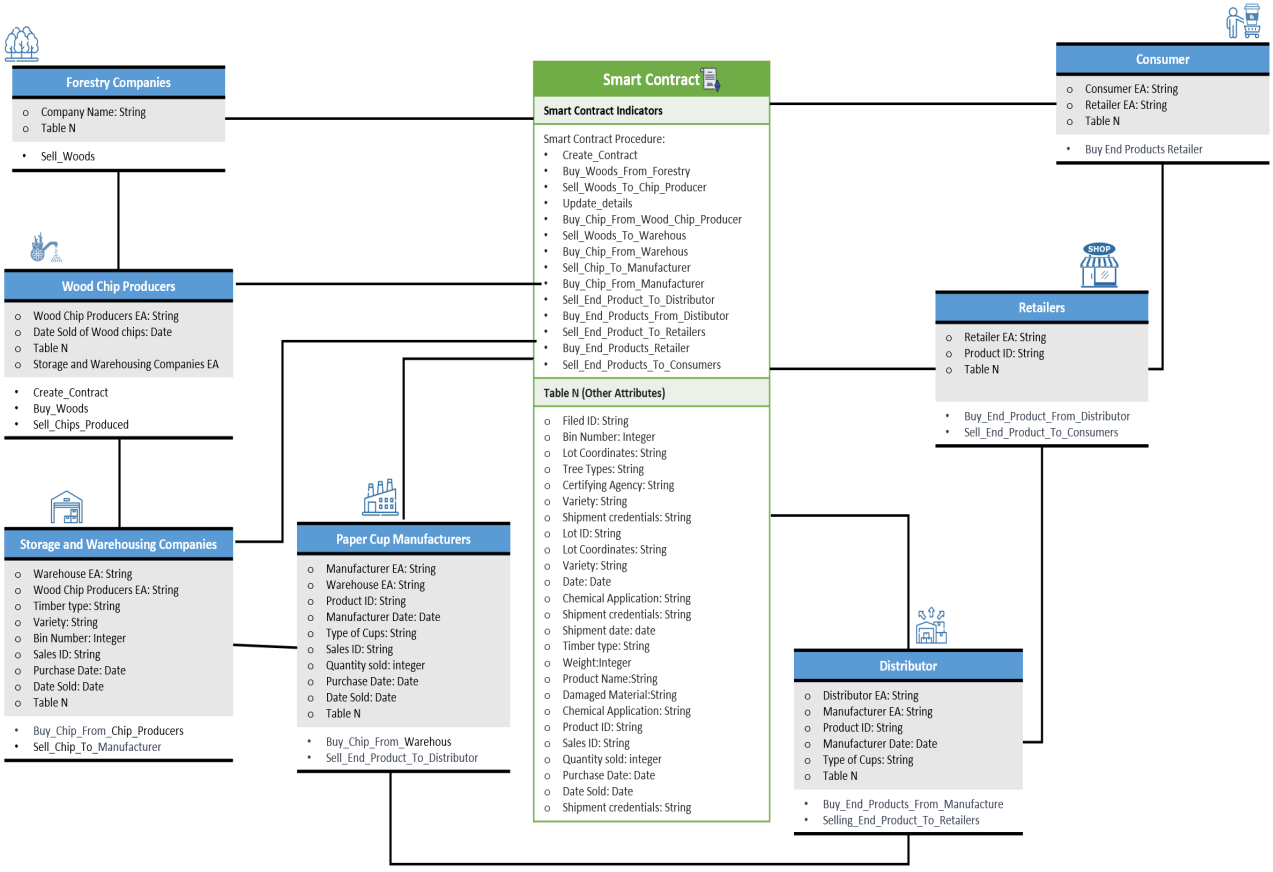

Figure 3-Interconnection between Stakeholders and smart contract diagram on Ethereum Platform

The entity-relationship diagram in Figure 3 illustrates the attributes, functions, and relationships between the participating entities and the smart contract, which rely on metadata and relations for successful smart contract implementation. In the context of blockchain and IPFS, all images, data, and records are digitally signed and attributed to a specific actor. For instance, when a Wood Chip Producer uploads MPEG files, they become the recognized owner of those files, assuming responsibility for any inaccuracies or fraudulent content. Smart contracts on the blockchain can be programmed to automatically enforce penalties if the farmer engages in dishonest behavior [9]. Alternatively, cameras with built-in capabilities and communication can be installed in the fields to capture and directly transmit images to the blockchain for recording and storage. These hardware cameras can be securely designed to prevent hacking or tampering, ensuring that the uploaded images can be audited, trusted, and open to dispute or verification by any participant or stakeholder on the blockchain [21]. Each participant in the system possesses an Ethereum address (EA) and interacts with the smart contract by invoking specific functions. Figure 4 illustrates the sequence of events in a scenario where a Wood Chips Producer creates a smart contract. After an offline agreement between the Forestry Company and the Wood Chips Producer, the Wood Chips Producer purchases seeds from the Forestry Company, triggering the invocation of the

WoodsRequestedByWood-ChipProducer event, which is accessible to all active participants (i.e., the Wood Chip Producer and the Forestry Company). The Forestry company executes the sellWoods() function, providing attributes such as the Forestry Company Ethereum Address (Wood Company EA), Ethereum Address of Wood Chip Producer (Wood Chip Producer EA), Quantity, LotAttributes, and more. The Forestry Company updates tree growth details at regular intervals on the file system using IPFS, saving the tree image in IPFS and storing the IPFS hash in the smart contract. This process continues until the harvesting stage, with crop growth images recorded periodically. As illustrated in Figure 4, the updateGrowthImage() function is responsible for capturing and documenting the growth of trees. Whenever an image is uploaded to the InterPlanetary File System (IPFS), its hash value is recorded in the smart contract, and subsequently, the TreeGrowthImageUpdated event is disseminated to all currently engaged entities. Upon the completion of the crop harvesting process, a contractual arrangement is established between the Forestry Company and the Warehouse for the purpose of storage. The Forestry Company obtains information regarding the levels of moisture, humidity, weight, and duration of storage within the Warehouse. Subsequently, upon reaching a mutual understanding, the company proceeds to sell the Chips for storage within said Warehouse. Figure 4 illustrates the implementation of the buyWood() function by the Warehouse and the sellToEleva-tor() function by the Forestry Company.

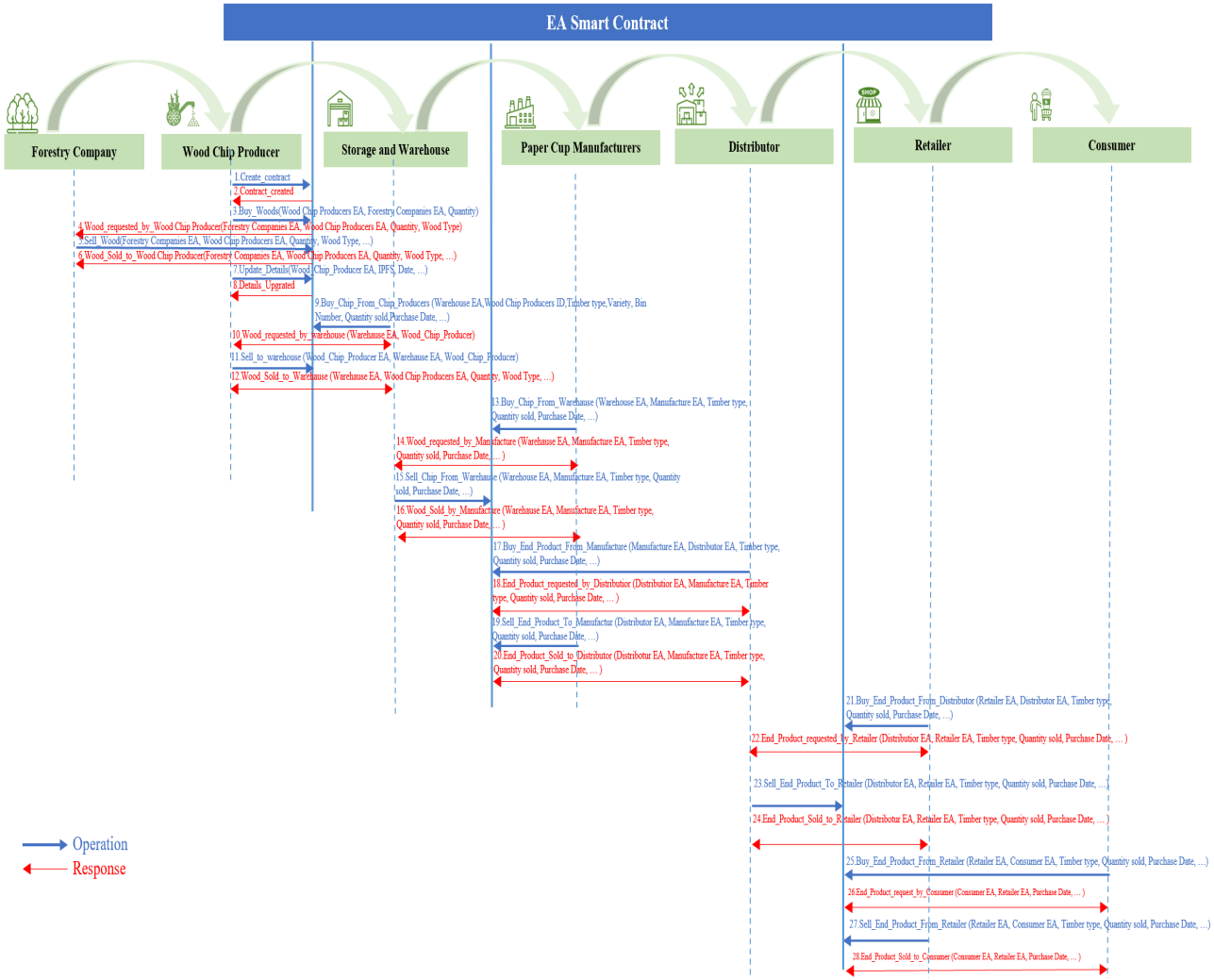

Figure 4-Progression architecture of interconnection between Stakeholders and smart contract diagram in the case

Accordingly, the message sequence diagram depicting the process of the grain processor purchasing grain from the Warehouse. The buyTimber() function is executed by the processor, passing parameters such as the Ethereum addresses of the requesting grain processor (Processor EA) and the Timber Warehouse (Warehouse EA), Quantity, and DateOfPurchase. This triggers the TimberRequestedByWarehouse event, prompting the Warehouse to execute the sellWoodToProcessor() function. The WoodSoldToWarehouse event is broadcasted across the network, sharing details such as the buyer and seller Ethereum addresses, Quantity, and DateOfSales. Subsequently, the distributor entity expresses its interest in purchasing finished products from the processor. Correspondingly, the buyProductFromManufacturer() function is executed by the distributor. Typically, the distributor serves as a warehouse that buys, stores, and ships products in large quantities to

wholesalers or retailers. The ProductRequestedByDistributor event is triggered, prompting the processor to sell the Cups to the distributor. The forestry company then executes the sellProductToDistributor() function, providing parameters such as the Ethereum addresses of the timbers, distributor, quantity sold, and date of sales. The ProductSoldToDistributor event is activated, notifying the actively involved entities (i.e., Manufacturer and Distributor) at that specific point in time.

Moreover, Figure 4 illustrates the message sequence diagram demonstrating the collaboration between the distributor, retailer, and the consumer through the smart contract. The distributor engages with interested retailers to sell goods, while the retailers request limited quantities of goods from the distributor. Accordingly, the retailer executes the buyProductFromDistributor() function, triggering the ProductRequestedByRetailer event. The distributor responds by executing the sellProductToRetailer() function, and the ProductSoldToRetailer event informs all participants about the cups' sale. The end consumers then purchases the product from the local retailer by executing the buyProductFromRetailer() function, triggering the EndProductRequestedByConsumers event through the smart contract. Finally, the retailer sells the product to the end consumers by executing the sellEndProduct() function, and the smart contract broadcasts the sale with the EndProductSold event.

The use of our proposed blockchain-based solution with smart contracts in the paper-based coffee cups supply chain offers traceability advantages, providing verifiable and unalterable information to all stakeholders without relying on a central authority. Starting from wood transactions between the forestry company and the Wood Chip producer, the entire volume of timbers produce sold between subsequent entities is logged and can be verified. Transactions, such as the sale of chips, cannot be modified or tampered with, ensuring transparency and preventing the mixing of woods with different quality criteria. The Wood chips producer's periodic uploading of images via IPFS creates a digital record that validates the agreed-upon conditions and facilitates continuous monitoring of storage growth. Traceable identifiers per lot and IoT-enabled containers equipped with sensors, cameras, GPS locators, and communication capabilities further ensure continuous monitoring of quality compliance and provide real-time notifications on product conditions. With blockchain, this information is tamper-proof and readily accessible to all stakeholders, eliminating the need for intermediaries. Standard identifiers such as global location identifiers or GPS geotagging can be used to add additional attributes, ensuring precise tracking of the product's physical location or stakeholder locations within shipping or storage containers. It is important to acknowledge that in the supply chain, there is a possibility of stakeholders engaging in fraudulent activities or recording false data. However, the blockchain system accurately records such fraudulent data with validated attribution to the originating stakeholder. If, at a later stage, the data is identified as incorrect, all participants and judges can confidently attribute the data to the specific actor or stakeholder involved. The blockchain can effectively detect and expose fraud in this manner. To address and mitigate such fraudulent activities, smart contracts can be programmed to include additional functions that invalidate shipments or the entire supply chain process. Penalties can be imposed on the fraudulent stakeholders, or alternative corrective actions can be taken. These corrective actions generate new data and actions that are linked to the fraudulent data, ensuring precise traceability and auditability that is both accurate and indisputable.

4. Current Algorithm for interaction between each stakeholder in the Smart Contract Network

The following part comprehensively explains the algorithms that develop the operational principles of the proposed blockchain-based procedure. The first stage entails the Wood chip producer launching the setup of a smart contract and reaching a consensus on the purchasing conditions with a registered forestry company. Algorithm (I) in Figure 5 outlines the process of wood sale, which includes verifying the Wood chips producer's registration, payment of the wood price, and updating the contract and participant states accordingly.

I) Forestry Companies sell Wood to Wood Chip Producer

Input:
- "W" as the list of registered Wood Chip Producer
- Ethereumaddress (EA) of Wood Chip Producer
- Ethereumaddress (EA) of Forestry Companies
- Quantity
- Wood_Type
- Wood_Brand
- Wood_Price

1. Contractstate is Created
2. State of the Wood Chip Producer is Wood_request
3. Forestry Companies state is ready
4. Restrict access to only W belongs to Wood Chip Producer
5. If Wood Chip Producer = registered and Wood_Price = Paid, then :
6. Contract state changes to Wood_Request_Submitted
7. Change state of Wood Chip Producer to wait_for_Wood
8. Forestry company state Agree_to_sell
9. Create a notification message stating sale of Woods
10. End
11. Else
12. Revert contract state and show an error.
13. End

II) Manufacture buy Wood to Warehouse

Input:
-"M" is the list of the registered Manufacturerer
-Ethereumaddress (EA) of Manufacture
-Ethereumaddress (EA) of Warehause
-Quantity
-Chip_Price
-Date _purchased

1. Contractstate is Buy_From_Warehause
2. State of the Wood Chip Producer is Wood_request
3. Timber_Wood state is Chips_bought_From_Chip_Producer
4. Restrict access to only M belongs to Manufacturerer
5. If Wood Chip Producer = agreed and Wood_Price = Paid, then :
6. Contract state changes to Wood_Request_Submitted
7. Change state of Wood Chip Producer to wait_for_Wood
8. Chip_Producer_company state Agree_to_sell
9. Create a notification message stating sale of chip to requesting Manufacture
10. End
11. Else
12. Contract state changes to Wood_Request_failed.
13. State of Manufacturer is request_failed.
14. Chip_Producer_company state is cancel_request_of_Processor
15. Create a notification message stating request failure
16. End
17. Else
18. Revert contract state and show an error.
19. End

Figure 5-Current Algorithm for interaction between each stakeholder in the Smart Contract Network from Forestry Company to Warehouse

Algorithm (II) in Figure 5 describes the process of selling woods from the Warehause to the grain Manufacturer. Important factors such as moisture content, bin number, date of purchase, and shipment date are considered. The contract state transitions to BuyFromWarehause, and conditions regarding the registration of the grain processor and payment are checked. If the conditions are met, the contract and participant states are updated, and all active entities are notified of the Chip sale.

Otherwise, the contract and participant states revert to their initial state, and the transaction is terminated.

The next stage involves the Cups processor selling the finished product to distributors. Algorithm (III) in Figure 6 explains the system state and participant roles involved in the purchase of products by retailers from distributors. Parameters such as date of product manufacture, quantity sold, and date of purchase are important considerations. The contract restricts access to registered retailers and verifies the acceptance of the sale agreement and completion of product payment. Successful transactions result in state updates and notifications, while failure scenarios trigger corresponding state changes and notifications to participants.

III) Distributor sell End_Product to Retailer

Input:
- "R" as the list of registered Retailers
- Ethereumaddress (EA) of Distributor,
- Ethereumaddress (EA) of Retailers,
- Quantity Sold
- Wood_Type
- Wood_Brand
- Wood_Price
- Date_Manufactured
- Date_Purchased

1. Contractstate is Coffee_Cups_Sold_to_Distributors
2. Distributors State is Coffee_Cups_received_from_Manufacturer
3. Retailer state is Ready_to_Purchase
4. Restrict access to only R belongs to Retailers
5. If Sale is agreed and Product_payment= successful, then :
6. Contract state changes to Sale_Request_Agreed_Success
7. Change state of Distributors to Producr_sold_to_Retailer.
8. Retailer state Cups_Delivered_Successful
9. Create a notification message stating Success_trade
10. End
11. Else
12. Contract state changes to Sale_Request_failed.
13. State of Distributors is request_failed.
14. Retailer state is cancel_request_of_Processor
15. Create a notification message stating request failure
16. End
17. Else
18. Revert contract state and show an error.
19. End

IV) Consumers buy End_Product from Retailer

Input:
- "C" as the list of registered Consumers
- Ethereumaddress (EA) of Retailers,
- Ethereumaddress (EA) of Consumers,
- Quantity Sold
- Product_ID
- Sales_ID
- Date_Purchased

1. Contractstate is Coffee_Cups_Sold_to_Distributors
2. Retailer State is Coffee_Cups_received_from_Manufacturer
3. Consumers state is Ready_to_Buy
4. Restrict access to only C belongs to Consumers
5. If Sale is agreed and Product_payment= successful, then :
6. Contract state changes to Sale_Request_Agreed_Success to concumers
7. Change state of Retailers to Producr_sold_to_consumers.
8. Consumer state Cups_purchased_Successful
9. Create a notification message stating Success_purchase
10. End
11. Else
12. Contract state changes to Sale_Request_failed.
13. State of retailers is request_failed.
14. Consumer state is cancel_purchase_of_Processor
15. Create a notification message stating request failure
16. End
17. Else
18. Revert contract state and show an error.
19. End

Figure 6-Current Algorithm for interaction between each stakeholder in the Smart Contract Network from Distributors to Consumers

Finally, Algorithm (IV) in Figure 6 describes the algorithm for consumers purchases from retailers. The consumers, as the final entity in the product processing and tracking model, initiates the purchase process. The contract verifies consumers access, checks important parameters for tracking the product, and updates the contract and participant states accordingly. Successful payments result in state changes and notifications, while incorrect payments lead to failure states and corresponding notifications to participants.

5. Conclusion

In this article, we have put forth a proposal for a solution and a versatile framework that utilizes the Ethereum blockchain and smart contracts to facilitate the traceability, tracking, and business transactions the supply chain of paper-based coffee cups with the help of applying blockchain technology.

Our aim is to eliminate intermediaries and the central point of processing. We have provided comprehensive information regarding the system's architecture, design, entity-relation diagram, interactions, sequence diagrams, and implementation algorithms. Our solution demonstrates its applicability to trace and track the paper-based cups supply chain, but it is important to note that the presented aspects and details can be adapted to offer trusted and de-centralized traceability for any Wood or food produce. It is worth mentioning that blockchain technology still encounters significant challenges in terms of scalability, governance, identity registration, privacy, standards, and regulations. As part of our future work, we intend to address some of these key challenges and develop corresponding solutions. Furthermore, our proposed solution will incorporate automated payment mechanisms and incorporate proof of delivery. This involves the utilization of cryptocurrency and smart contracts to automate and centralize the payment process for all parties involved, following the successful completion of the physical delivery of crops and products.

Acknowledgments

Special thanks to the German Research Foundation who supplied financial support for this conference.

References

[1] Bager, S. L., Düdder, B., Henglein, F., Hébert, J. M., and Wu, H. 2022. Event-based supply chain network modeling: Blockchain for good coffee. Frontiers in Blockchain 5, 846783.

[2] Bager, S. L., Singh, C., and Persson, U. M. 2022. Blockchain is not a silver bullet for agro-food supply chain sustainability: Insights from a coffee case study. Current Research in Environmental Sustainability 4, 100163.

[3] Biswas, D., Jalali, H., Ansaripoor, A. H., and Giovanni, P. de. 2023. Traceability vs. sustainability in supply chains: The implications of blockchain. European Journal of Operational Research 305, 1, 128–147.

[4] Buterin, V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.

[5] D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu. 2017. Blockchain application in food supply information security. In 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), 1357–1361. DOI=10.1109/IEEM.2017.8290114.
[6] Difrancesco, R. M., Meena, P., and Kumar, G. 2022. How blockchain technology improves sustainable supply chain processes: a practical guide. Operations Management Research.
[7] Düdder, B. and Ross, O. 2017. Timber tracking: reducing complexity of due diligence by using blockchain technology. Available at SSRN 3015219.
[8] Filippi, P. de, Wray, C., and Sileno, G. 2021. Smart contracts. Internet Policy Review 10, 2.
[9] Giovanni, P. de. 2020. Blockchain and smart contracts in supply chain management: A game theoretic model. International Journal of Production Economics 228, 107855.
[10] Groschopf, W., Dobrovnik, M., and Herneth, C. 2021. Smart contracts for sustainable supply chain management: Conceptual frameworks for supply chain maturity evaluation and smart contract sustainability assessment. Frontiers in Blockchain 4, 506436.
[11] 2023. IBM Supply Chain Intelligence Suite - Food Trust. https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust. Accessed 14 July 2023.
[12] Katsaliaki, K., Galetsi, P., and Kumar, S. 2022. Supply chain disruptions and resilience: a major review and future research agenda. Annals of Operations Research 319, 1, 965–1002.
[13] MacCarthy, B. L., Ahmed, W. A., and Demirel, G. 2022. Mapping the supply chain: Why, what and how? International Journal of Production Economics 250, 108688.
[14] Mao, D., Wang, F., Hao, Z., and Li, H. 2018. Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain. International journal of environmental research and public health 15, 8, 1627.
[15] N. Kannengießer, S. Lins, C. Sander, K. Winter, H. Frey, and A. Sunyaev. 2022. Challenges and Common Solutions in Smart Contract Development. IEEE Transactions on Software Engineering 48, 11, 4291–4318.
[16] Nizamuddin, N., Salah, K., Ajmal Azad, M., Arshad, J., and Rehman, M. H. 2019. Decentralized document version control using ethereum blockchain and IPFS. Computers & Electrical Engineering 76, 183–197.
[17] Q. Lu and X. Xu. 2017. Adaptable Blockchain-Based Systems: A Case Study for Product Traceability. IEEE Software 34, 6, 21–27.
[18] Schütte, J., Fridgen, G., Prinz, W., Rose, T., Urbach, N., Hoeren, T., Guggenberger, N., Welzel, C., Holly, S., and Schulte, A. 2018. Blockchain and smart contracts.
[19] Sharma, C., Sharma, S., and Sakshi. 2022. Latent DIRICHLET allocation (LDA) based information modelling on BLOCKCHAIN technology: a review of trends and research patterns used in integration. Multimedia Tools and Applications 81, 25, 36805–36831.
[20] Smart Contracts on Blockchain? 2023. IBM. https://www.ibm.com/topics/smart-contracts. Accessed 6 July 2023.
[21] Steichen, M., Fiz, B., Norvill, R., Shbair, W., and State, R. Blockchain-based, decentralized access control for IPFS. In 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). IEEE, 1499–1506.
[22] Tian, F., Ed. 2016. An agri-food supply chain traceability system for China based on RFID & blockchain technology. IEEE.
[23] Tian, F., Ed. 2017. A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. IEEE.
[24] Wang, S., Li, D., Zhang, Y., and Chen, J. 2019. Smart contract-based product traceability system in the supply chain scenario. IEEE Access 7, 115122–115133.
[25] Wang, Y., Wang, Z., Yang, G., Ai, S., Xiang, X., Chen, C., and Zhao, M. 2021. On-chain is not enough: Ensuring pre-data on the chain credibility for blockchain-based source-tracing systems. Digital Communications and Networks.

Blockchain Applications in the European Higher Education Arena

Anastasia, Platonava, Marc, Cashin
Technological University of the Shannon: Midlands Midwest, Athlone, Ireland

This desk research will initiate an exploration of present and potential blockchain applications in the higher education sector of Europe. The aim of this research is to create a theoretical base for a further postgraduate research and analysis, so to create an effective model/framework to augment the integration of blockchain technology into existing organizational processes, initially in higher educational institutions, but which may be adaptable and generalizable to other specific uses. Due to the novelty of the topic, academic resources related to the research area are limited. Most studies seem to focus on blockchain-based applications in industries such as finance, healthcare, and supply chain management, and there is little evidence of the impact of blockchain technology on education. This paper discusses present and suggests some potential blockchain-based applications in education in Europe and beyond. This research provides a groundwork for education and academia stakeholders, policymakers and researchers to exploit the potential of blockchain in different functions of an education system.

1. Introduction

The world has witnessed several stages of the technological development. Currently, we are living in Industry 4.0 or the Fourth Industrial revolution, which includes technologies like AR/VR (augmented and virtual reality), AI (artificial intelligence), machine learning and blockchain technology. The world is developing too fast and these technological advancements bring deep changes into the nature of knowledge and skills required in the labor market. This in turn puts enormous pressure on traditional educational institutions and teaching and learning practices, calling for improved lifelong learning, skills development and recognition systems.

Improving the quality of life globally means investing in education. It improves social stability and long-term economic growth. Ensuring inclusive and equitable quality education and promoting lifelong learning opportunities for all is one of the top priority goals of the United Nations Sustainable Development Goals [1].

Technology has improved access to education for an increasing number of students. The COVID-19 pandemic was one of the factors that exposed educational challenges. It forced educational institutions to temporarily close their doors, which affected nearly 1.6 billion learners in more than 190 countries and all continents [2]. With the Russia-Ukraine war in place, Ukraine needed to shift to an emergency remote teaching and learning mode that has already been adopted in the past because of the pandemic. These two incidents underpinned the need for digital technologies in the education sector and a higher level of digital capacity and innovations in the education sector and a higher level of digital capacity and innovations [3].

In the 21st century, computers have become an integral part of nearly every facet of education. Blockchain technology has recently received significant attention from EU institutions, policymakers and government. It is poised to bring about a similar transformative impact in the education sector. Blockchain technology holds tremendous potential for addressing various educational challenges and facilitating improved monitoring of learning outcomes for both educators and students. Blockchain has a significant impact on educational learning and teaching methods. This advancement brings both opportunities and challenges for universities, affecting internal processes and organizational structure. As the momentum for change builds, organizations and institutions that have laid the groundwork for adopting and utilizing blockchain technology will gain a competitive edge in their respective markets and regions.

This study will incorporate desk research and will focus on present anf potential applications of blockchain technology in higher education sector. This desk research will explore scientific journals, government data and media reports. Specific points of interest include use-cases of blockchain technology in education sector in Europe and beyond.

This research paper is only a preliminary mapping exercise and in no way represents a comprehensive assessment or the final word on the current state of blockchain technology in education sector of Europe. This paper provides a groundwork for education and academia stakeholders, policymakers and researchers to exploit the potential of blockchain in different areas of an education system.

2. Background

Blockchain technology

Blockchain technology has emerged as a groundbreaking phenomenon that hit the global world since the invention of the Internet *[4; 5].* Several authors mentioned that blockchain represents the second era of the Internet *[6; 7].* This technology cannot be touched or seen, therefore, its intangible nature presents a challenge in explaining it. Visually, it can be imagined as a chain of blocks, that are linked to each other *[8; 9].* These blocks

contain information in them, which can be stored in any format (text, pictures or audio files).

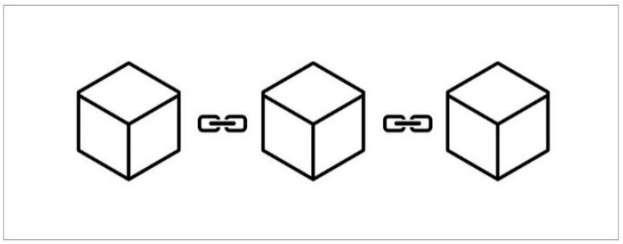

Fig. 1: Structure of Blockchain

Blockchain technology was initially described in the early 90s, as a tool to timestamp digital documents, so to eliminate the possibility of backdating or tampering with them. In this case, blockchain may be seen as a "digital notary", digital notebook that lots of people can use and write in, with some special features that make it really secure and trustworthy.

In 2008, blockchain was revealed in a paper called "Bitcoin: A Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto (the pen name), so to create the digital cryptocurrency called Bitcoin. The initial idea behind blockchain is that it is a virtual database, which is used by Bitcoin and other cryptocurrencies for secure and anonymous transactions *[10].* Since then, there was an emergence of other blockchain implementations, such as Ethereum and Hyperledger *[11; 12].* Nowadays, blockchain technology is much more than just a tool to enable digital currencies, it is a platform, which has a nearly limitless amount of applications across almost every sector. It is a new global infrastructure that could transform many existing processes in business, governance and society *[13].*

Blockchain Generations

Blockchain 1.0 is an initial version of blockchain, the concept of which was introduced by Satoshi Nakamoto in 2008. It is used for secure and transparent transactions flow on a Bitcoin blockchain. Nowadays, this version of blockchain is used not only for Bitcoin, but for other existing altcoins – all cryptocurrencies created after Bitcoin.

Second generation of blockchain is called Blockchain 2.0. It is started in 2013 with an introduction of Ethereum *[11].* Ethereum speeded up the development of decentralized finance (DeFi), decentralized autonomous organizations (DAOs), initial coin offerings (ICOs), and non-fungible tokens (NFTs). While Bitcoin has been created solely for operating as peer-to-peer digital cryptocurrency, Buterin developed Ethereum as a platform on which many cryptocurrencies, including its own – Ether – can operate. Blockchain 2.0 can be defined as the second generation of blockchain technology that is focused on smart contracts. Smart contracts refer to digital programmes stored on a blockchain that are automatically executed when predetermined terms and conditions are met *[14].* Smart contracts are exactly the same as contracts in the real-world, but they are digital.

Blockchain 3.0 generation refers to blockchain's impact on economy and market. It is defined as an enterprise and institutional blockchain. During this stage engineers tried to enhance blockchain's scalability and security features, allowing blockchains to interact with each other and to facilitate speedier cost-effective transactions. Blockchain 3.0 is an upgraded version of blockchain 2.0, which makes blockchain more capable for running DApps.

Blockchain 4.0 generation is all about industry applications. Blockchain 3.0 is fitted into Blockchain 4.0 and it is usable in real-life business scenarios by satisfying Industry 4.0 demands by making blockchain promises come to life. It is important to notice that there is still room for better enhancement and next generations of blockchain. For example, blockchain can be easily enjoyed by humans and business if it has a user-friendly interface.

Blockchain technology enables the creation of a decentralized environment, where transactions and data are not under the control of any third-party organizations *[15].* Rather than having a central administrator like a traditional database, blockchain has a network of replicated databases synchronized via the Internet and visible to those via the network. Blockchain is an open, distributed ledger that can efficiently record transactions between two parties in a verifiable and permanent way without the need for a trusted third party *[16].*

For the purpose of this research, authors define blockchain as a decentralized distributed ledger, which allows peer to peer transactions secured by cryptographic rules. It is a registry or journal (ledger), which does not have a central authority to control the database (decentralized), which involves many participants who store information (distributed) and operates safely due to securing information from unauthorized access (cryptographic rules). Blockchain is a registry that is distributed among many participants with no central entity to control.

Educational Challenges

Skills Development and Recognition. The European Union undergoes continual transformations, which result in evolution in the demand for relevant knowledge, skills and competencies. One of them is the recent spread of COVID-19 which has created an unprecedented global health pandemic, resulting in a global economic crisis. This crisis has impacted businesses and institutions of all sizes in different ways – from closure to struggling to stay afloat to changes in business models – resulting in job losses *[17].* At the moment, 40% of employers cannot find people with the right skills to fill their vacancies *[18].* To effectively navigate these changes, individuals must possess a set of fundamental competences, including literacy, numeracy and digital proficiency. Education and

training play a pivotal role in empowering young individuals, particularly by facilitating the development of these competences and providing them with an optimal foundation for their future endeavors. To identify and address the acquisition of necessary knowledge, skills and attitudes, while preventing the emergence of skills gaps and mismatches, it is essential to establish effective communication channels between the education and training sector and the needs of the EU economy.

Fraud Tampering. In education systems certificates state that the achievements of the students and different activities are mostly issued on paper or other physical forms. Universities and institutions are responsible for the issuing and validation of academic certificates, such as diplomas. That requires educational institutions to be constantly available to perform this validation when requested by external entities, such as employers. Moreover, paper certificates are prone to tampering and forging. We still live in a paper-based economy of student records, which has a lot of problems, such as widespread fraud *[6].* However, recent research showed that the counterfeit in diplomas involves not only lower-tier staff but also activists, governmental members, officials and university candidates *[19].*

Degree mills are one of the ways how to get a fake diploma. Degree mills are fraudulent providers of higher education and training, offering degrees and certificates that may be considered bogus and have no academic value *[20].* Very often, degree mills look like usual colleges or university, with the website, publications, contact details and attractive logo. However, if we take a closer look, we will see that the logo has been "borrowed" from a real university and a bit modified, contact details will lead you to the post box or even fake address, and real address of the institution does not even exist. Nevertheless, their degrees can be purchased for much cheaper price than the tuition fee paid. Degree mills stop the efforts to assure quality in education. Fake degrees also have a negative impact on the students: because degree mills are unaccredited institutions, their diplomas or ECTS are not recognized, so students cannot continue their educational path. Moreover, employees, who tend to verify candidate's diploma before making a job offer, very easily understand that it is a scam. It all has a negative impact on public educational institutions and legitimate service providers, as people start losing trust towards colleges and universities.

Decrease in University Enrollment. Educational sector all over the world experienced a decline in enrolment of students. There is a number of factors, which have influence on this indicator: rise in tuition fee, widely promoted massive open online courses, political situation in some regions (Ukraine, countries of the Middle East). There are many reasons why tuition fees are increasing globally. For example, increase in labour and supply costs in the USA was one of the factors that led to the increase in average tuition and fees up to 1.2 percent for public universities in fall 2020 and 1.6 percent in fall 2021 *[21].* High energy costs, alongside with the decline in real pay for university staff forced university vice-chancellors in England and Wales to call for an increase in tuition fees. It leads to the idea to cut the number of UK students universities take, but increase the number of international and postgraduate students, whose fees are not capped by the Government. Overall, tuition fees are a burden for many young students. As you can see from the Figure 2, tuition fee crisis has a negative impact on overall economy. People either enter the university and then leave it, because of an increase in tuition payments, or even do not apply for any study programme. It leads to the situation, when people avail of an opportunity of getting a fake degree (if they have money) or they end up with no degree at all. Of course, employers are not happy with that, as it has an impact on their businesses and overall economy.

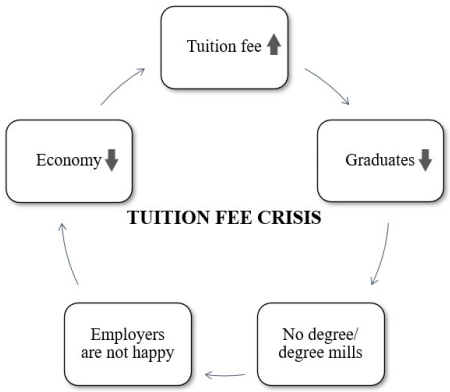

Fig. 2: Tuition Fee Crisis

There are many more challenges in education, which are discussed on the European level, such as digital transformation, which includes online learning and quality of higher education, integration and skills recognition of migrants and refugees, learning mobility of staff and students and lifelong learning.

Blockchain technology is becoming an increasingly popular tool to address these challenges in education sector.

3. Blockchain in Education

Let's have a look at the Figure 3, which summarizes 10 blockchain use-cases in education, both present and potential applications.

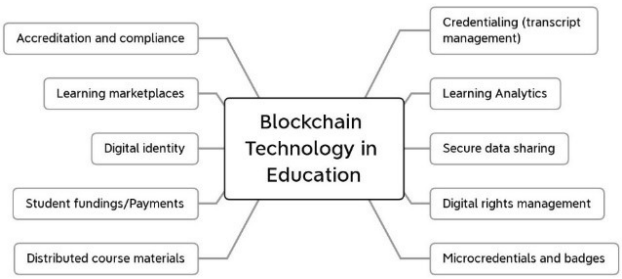

Fig. 3: Summary of Present and Potential Applications of Blockchain Technology in Education Sector

Present Applications of Blockchain in Education

Credentialing (Transcript Management)

One of the most famous and researched use-cases of blockchain technology in the field of education is called transcript management. Transcript management can be understood as a process of collecting, organizing and storing students' data, which includes, but is not limited to the documents confirming grades achieved, courses taken and degrees conferred. The idea behind introducing blockchain into the educational sector as a storage for academic credentials is in storing digital academic transcripts and issuing the degrees. This blockchain use-case has been widely researched by many authors *[16; 19; 22].* It is also referred to the transformation of the traditional centralized record storage of students and staff to the distributed network. That eliminates the need for the third party to verify the details as well as using less resources (time and money). Moreover, blockchain technology provides people with 24/7 access to the information required. Blockchain technology provides a secure and innovative means of realizing the concept of the self-sovereignty *[23].* Several authors considered that linking blockchain and higher education diplomas can positively impact students around the world *[24].* Overall, the process itself becomes very simple, but more secure and transparent.

There are several existing applications of blockchain technology in this area in Europe and beyond:

Blockcerts. The Massachusetts Institute of Technology and the University of Nicosia, Cyprus are the pioneers of Blockcerts adoption. This open-source blockchain-based application allows students to quickly and easily get a verifiable, tamper-proof version of their diploma that they can share with employers, schools, family, and friends. To ensure the security of the diploma, the Blockcerts Wallet uses the same blockchain platform that powers the digital currency Bitcoin, which was built "on-top" of a blockchain and can also work with Ethereum or Hyperledger *[19].* MIT use-case of blockchain technology is an example where learners have a full autonomy over their own records. Blockcerts is considered to be an internationally recognized standard for securing important digital records, however, it does not allow blockchain to be used in a global higher education credit and grading platform yet. Also, Blockcerts does not allow to upload bulk documents and has no well-developed revocation system *[25].* As has been pointed out by several authors, who argued that that the Blockchain protocol does not provide any strong mechanism for authenticating the issuing institution, since the issuer authentication is basically performed on the basis of an unauthenticated issuer profile available online and referenced from inside the certificate *[26].* Simply speaking, it means that fake academic certificate issued by a fake educational institution can be put on the blockchain platform, but Blockcerts will not be able to recognize it.

There are several universities around the world that have adopted Blockcerts for their academic credentialing systems and they are presented in the Table 1.

Block.co. Block.co platform has been developed by the University of Nicosia in 2014 and it is a pioneer in blockchain credentialing applications. Similar to Blockcerts, it also serves as a system to upload certificates on a blockchain. The advantage of using Block.co lies mainly in its cost reduction since it allows to upload multiple documents on the blockchain that will be hashed together *[19].* Block.co platform allows to secure PDF documents from fraud without any intermediaries. The documents generated are entirely self-contained and self-verifiable, which means they include both the blockchain proof and data inside the document itself without requiring the installation of extra software or apps *[27].* While both Block.co and Blockcerts use blockchain technology, they are not directly similar. Also, their specific implementations are different, with Block.co being more focused on enterprise blockchain solutions (hospitality, fashion and beauty, telecommunications industries), while Blockcerts is more focused on the education sector and digital credentialing.

Institution	Record Type	Year
Massachusetts Institute of Technology, USA	Degree/certificates	2017
University of Nicosia, Cyprus	Degree/certificates	2017
Pallavan School and Vasant Valley School, India	Leaving Certificates, Language Certificates, Character Certificates, Letters of Recommendation, and Five Areas of Development Mark Sheets	2019
Maryville University, USA	Degree/certificates	2019
Lehigh University, USA	Career Skills Certifications	2019
RCSI Bahrain, Bahrain	Degree/certificates	2021
The University of Rome "Tor Vergata", Italy	Degree/certificates	2018
University of Melbourne, Canada	Teaching certificate	2017
University of Milano-Bicocca, Italy	Degree/certificates	2019
University of Padova, Italy	Degree/certificates	2019
Central New Mexico Community College	Certificates	2017
Southern New Hampshire University	Degree/Certificates	2018
Singapore Management University	Degree/Certificates	2019

Table 1: Current users of Blockcerts for students' credentials

BTCerts. The BTCerts project was inspired by Blockcerts and developed by the University of Birmingham's IT Services department and the Centre for Doctoral Training in Cloud Computing for Big Data in collaboration with blockchain technology company Learning Machine. BTCerts uses blockchain technology to issue and verify academic credentials. It aims to create a secure and immutable platform for students to share their academic credentials, which can be verified by potential employers, universities and any other institutions. It also aims to solve several weaknesses found in Blockcerts, such as utilizing a multi-signature scheme to ameliorate the authentication of certificates; exerting a safe revocation mechanism to improve the reliability of certificates revocation; establishing a secure federated identification to confirm the identity of the issuing institution *[28].* BTCerts uses the Blockcerts open standard and allows students to access their digital certificates through a secure web portal. The platform also enables students to share their certificates with employers and other institutions via a secure link, allowing for easy and secure verification of their academic achievements. BTCerts is currently being piloted with the University of Birmingham's CDT students and will be rolled out to the wider university in the future.

Micro-credentials and badges

European Commission stated that the lack of digital solutions for the validation, recognition and storage of micro-credentials remains one of the obstacles to the further development and adoption of micro-credentials *[29].* Badging was the initial response to online credentialing. Blockchain technology, in return, may support the issuance of digital badges. It provides education sector with security through validating academic certificates and credentials registered on blockchain. At the same time, blockchain provides an opportunity to verify the documents in real-time all around the world. Similar to blockchain use-cases in transcript management, it provides features like decentralization, immutability, security and availability, which are leveraged for the issuance of micro-credentials and digital badges. On the other side, views are mixed regarding the feasibility and potential risks of blockchain technology adoption. Some concerns are related to the significant investments in terms of an organizational strategy that can help to transform the internal processes and training of employees *[30].*

In 2019, the World Wide Web Consortium (W3C) created the Verifiable Credential Model 1.0 standard. This not only standardizes certification exchange at the national level, but also ensures that digital diplomas and electronic documents are recognized worldwide. Blockchain technology enables this standard to be implemented with a higher degree of security, trust, interoperability and robustness than any other solution that uses traditional technologies. Issuing micro-credentials and badges on the blockchain platform has been researched and piloted by several institutions, organizations, researchers and developers. UK has developed Ethereum's Smart Contracts to document micro-credentials (badges) as an open source solution. Several authors proposed a system, where blockchain technology will be incorporated in the digital badge and in the examination app *[31; 32].* One author explored the possibilities of extension eAsel, a competency web-based platform, to support blockchain micro-credential certificates *[33]*.

The main purpose is to eradicate the problem of fake certificates/achievements. One researcher introduced a concept of Smart Badges for supporting lifelong learning *[34]*. In comparison to the traditional online or digital badges that just record a learning achievement, Smart Badges can also offer job or course recommendations based on a student's portfolio.

Credentify. Credentify is a decentralized blockchain-based cloud service which empowers students, educational staff and universities across Europe to issue and receive micro-credentials that can be summed up into ECTS. It allows accreditation of the traditional learning experience to be fast, safe, reliable and accountable. Main aim of this initiative is to ensure that micro-credentials are certified and mapped to the European qualifications frameworks and can be embedded into other forms of Higher Education *[35]*.

Credentify is the first European free and open issuer of blockchain-secured stackable ECTS credentials that are university and student owned, and verifiable anywhere, anytime, thus in turn improves transfer and transparency of credentials. It is at present being piloted by five European universities: Duale Hochschule Baden-Württemberg, Germany; Vytauto Didziojo Universitetas, Lithuania; Tampere University, Finland; Fondazione Politecnico di Milano, Italy; Institut Jozef Stefan, Slovenia.

The development of Credentify has occurred in a context of increasing requests from graduate students to recognise learning achieved online and elsewhere. Credentify provides students the opportunity to get credentials from multiple universities recognised as part of their studies, and it supports portability and storage of digital student data *[36]*. One of the advantages of Credentify is that it offers a standard format for documenting micro-credentials in terms of ECTS, using existing recognition tools.

BCdiploma. BCdiploma is the first blockchain credentialing platform which allows to automatically issue forgery-proof credentials and micro-credentials once a passing grade has been determined. More than 170 institutions over 21 countries use blockchain to secure digital credentials.

The French governmental project within the European Blockchain Partnership, fr.EBSI, launched in 2021, is a response to the new standard introduced by the W3C – the "verifiable credentials". The University of Lille is a leader

of this project, BCdiploma is the technical operator. The University of Lille is one of the first educational institutions to achieve a real digital transformation of its academic department. In its White Paper, published in 2023, it explained the way it is issuing its students a digital certificate of completion of their degree or certificate issued on a low-energy blockchain *[37]*. The University of Lille aims at issuing diplomas in the European Blockchain Service Infrastructure - blockchain ecosystem. This infrastructure, deployed by the European Commission and the European Blockchain Partnership, provides a blockchain and trusted digital environment to support cross-border applications such as "track and trace", "verifiable credentials", "trusted data exchange" and IP management *[38]*.

The University of Lille has issued over 32 000 blockchain credentials since 2021, and student satisfaction rate of using the digital certificate was at 76%, what confirms the project's success *[37]*. One of the advantages of this project is low-energy consumption. Lille University decided to issue academic certificates on the Avalance blockchain, which operates on a Proof-of-Stake protocol. Based on the latest Ethereum research, it can be estimated that the emission of a digital certificate by the Lille University is about 0.025 g of CO2, compared to an average of 4 g of CO2 for an email without an attachment *[39]*.

Academic certificates are designed not only for websites, but also for smartphones, thus making it easier to share it via social media networks. It is also possible to share documents by sending a link to the recipient or through scanning a QR Code directly.

XenEd. The XenEd is an innovative technology, which is used as a platform for the delivery of MOOCs. This platform provides functionalities to better monitor and track learner progress and provides a seamless and flexible online learning experience to learners. University of Mauritius in a partnership with a software engineering products and services company the Crystal Delta Pty Ltd launched iLearn – a MOOC platform based on the concept of open learning and micro-credentials based on Ethereum blockchain. This platform provides learners with the possibility to earn micro-credits that can be accumulated and transferred into recognized university credits. The XenEd platform provides functionalities for iLearn, so to better monitor and track learner progress and to provide a flexible online learning experience. The University of Mauritius is a pioneering institution in the development of education technology in an academic field and in innovation in teaching and learning through technology *[40]*.

University of Hawaii at Manoa. Institution performed qualitative research in their own blockchain-based micro-credential management system and found that qualitative evaluation reveals that such systems can decrease the overall cost and administrative workload *[41]*.

Hyland Credentials. Hyland Credentials started as Learning Machine, which developed Blockcerts open standard with the MIT Media Lab. Currently, company positions itself as a global leader in blockchain-based digital credentials and the only records provider in the world with a product in market for multi-chain issuing and self-sovereign identity *[42]*. Hyland Credentials provides its services to the government, healthcare and education sectors. Its education products and services relate to diplomas and certificates, transcripts, examinations, photo ID's and Open Badge. Company supports the importance of micro-credentials and recognition of specific skills and achievements.

Student Funding/Payment

The original concept behind the invention of blockchain technology is its possibility to be used as a platform for recording, sharing and storing financial transactions. In education environment blockchain technology helps universities to keep a clear digital record of payments for each student while using cryptocurrency as tuition payment. It can also be used to create a secure and transparent platform for managing student funding, such as scholarships or grants. This type of blockchain application saves money and time not only for educational institutions, but also for individual learners *[43]*. Blockchain can be used as an efficient manner to exchange information and eliminate the need of such third or intermediary parties based on its high security level *[44]*.
Nowadays, there are some pioneer schools who are already accepting tuition fees in cryptocurrency and tutors graduates on digital currencies. The widespread adoption of blockchain technology and digital assets has encouraged universities to plan for the future and accept cryptocurrency payments. On the one side, bitcoin adoption allows universities to stay ahead in the "blockchain race", while sensitizing students on the market trends. On the other side, cryptocurrency payments may be used to ease the burden on international students who spends extra fees on transaction, as well as make it more efficient for everyone.

University of Nicosia. University of Nicosia is the first accredited educational institution worldwide to accept cryptocurrency for tuition payments *[45]*. University of Nicosia expected that the initial adoption of blockchain will come from the students in Africa. In 2017 a new student from the South Africa made a payment of 1 BTC (at that time the equivalent of 670 EUR) toward tuition for an online Master of Business degree programme. From that moment Bitcoin was accepted throughout the entire University of Nicosia system, which includes online programmes and affiliated schools. Those students who wished to use Bitcoin for tuition fees could pay at the university's finance office or through an online merchant processing service – BitPay Payment Gateaway. University of Nicosia was willing to receive Bitcoin as a payment for the study programmes, but due to its volatility, the university promptly converted the cryptocurrency into

EUR. As per today (15 May 2023), for unknown reasons this payment option is currently unavailable.

IEBS. Innovation and Entrepreneur Business School in Spain (IEBS), an educational provider of the online courses, was the first digital business school to accept Bitcoin payment. Compared to the University of Nicosia, the Spanish college addressed the volatility of Bitcoin by providing international students with a stable exchange rate.

Since then, other international schools have followed the same example. In 2014, King's College in New York became the first accredited US institution to grant digital currency payments (in a partnership with a bitcoin trading company "Coin.co") and even donations *[46]*. The University of Cumbria, UK became the first public institution to accept Bitcoin as a form of tuition payment. However, it offered this opportunity exclusively to the students who were enrolled in Master degree programmes related to cryptocurrencies. Two years later, the European School of Management and Technology in Germany (ESMT) started accepting Bitcoin cryptocurrency for any degree or executive education *[47]*. ESMT was the German university that recognized the importance and need of cryptocurrency transactions, due to the fast clearance (in around 10 minutes), compared to weeks or months offered by the traditional payment systems. It started accepting Bitcoin as a tuition fee payment and then included to dash, ethereum and litecoin cryptocurrencies as possible options. Currently, universities have not set up a financial infrastructure that would process crypto payments, therefore educational institutions have to partner with the crypto merchant companies, start-ups and other institutions to handle transactions.

Potential Applications of Blockchain in Education

Digital rights management

The idea behind introducing blockchain technology into digital rights management lies into a possibility of managing and protecting digital content, such as textbooks and course materials, music and videos, ensuring that copyright owners are properly compensated and that content is not illegally shared. This blockchain use-case may be of a great value for students and learners from the creative industries (such as musicians, artists, videomakers), as it may enable students to create and share digital portfolios of their work. The application of blockchain technology as a digital rights management tool also enables copyright owners (students in this case) to track the usage of their digital assets. With the help of blockchain technology, digital rights management can be set up to automatically restrict access to a digital asset if needed. At the moment, companies across blockchains are starting to use NFTs, which are used to verify unique items and digital assets, which also may be of a potential application in education sector.

Learning Analytics

Blockchain technology can be used to track and analyse student data for a better student learning experience. Also, blockchain can help lecturers and education stakeholders to understand students' hard and soft skills, strengths and weaknesses and provide learners with a personalised learning features and experience. One researcher proposed a blockchain based approach for connecting learning data across different Learning Management Systems (LMS), Learning Record Stores (LRS), institutions and organizations *[48]*.

Secure data sharing

Blockchain technology can be used to securely share student data in any educational ecosystem between students, lecturers, institutions and many more, ensuring that the data remains private and secure.

Distributed course materials

Blockchain technology can be used to create decentralized platforms for sharing and distributing course materials, enabling lecturers to share resources with their peers and collaborate more effectively.

Digital Identity

Blockchain technology can be used to create secure and verifiable digital identities for students and educators, enabling them to securely access online resources and verify their identity for exams and other activities.

Learning Marketplaces

Blockchain technology can be used to create peer-to-peer learning marketplaces, where students can connect with tutors and other educators to access personalized learning opportunities.

Accreditation and compliance

Blockchain technology can be used to create secure and transparent systems for accrediting educational programs and ensuring compliance with regulatory requirements.

Conclusion

The research trend indicates that there is an increasing interest in applying blockchain in the education sector. However, present blockchain-based applications in education are limited to the areas of tuition fee payments, academic transcripts and micro-credentials. Considering the importance and potential of introducing blockchain technology in education sector of Europe, additional research should be conducted on potential use-cases of blockchain technology in education, which may allow to create an effective framework to augment the integration of blockchain technology into existing organizational processes in higher educational institutions of Europe.

Contact details

Contact person: Anastasia Platonava

E-Mail address:

A00226775@student.tus.ie

anastasia.platonava@research.ait.ie

ORCID: 0000000186560743

Literature references

[1] UNSDG. (2015). Goal 4. Quality Education. https://sdgs.un.org/goals/goal4
[2] United Nations. (2020). Education during COVID-19 and beyond. https://unsdg.un.org/resources/policy-brief-education-during-covid-19-and-beyond
[3] European Commission. (2020). Digital Education Action Plan 2021-2027.
[4] Drescher, D. (2017). Blockchain Basics. Apress. https://doi.org/10.1007/978-1-4842-2604-9
[5] Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. SSRN Electronic Journal. https://doi.org/10.2139/SSRN.2580664
[6] Jagers, C. (2017). THE STATE OF DIGITAL EDUCATION.
[7] Tapscott, D. (2018, April 5). Blockchain represents the second era of the internet. https://www.52-insights.com/don-tapscott-blockchain-represents-the-second-era-of-the-internet-interview/
[8] Antonopoulos, A. M. (2010). Mastering Bitcoin : unlocking digital crypto-currencies.
[9] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017, 557–564. https://doi.org/10.1109/BIGDATACONGRESS.2017.85
[10] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org
[11] Buterin, V. (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.
[12] Cachin, C., Schubert, S., & Vukolić, M. (2017). Non-determinism in Byzantine fault-tolerant replication. Leibniz International Proceedings in Informatics, LIPIcs, 70, 24.1-24.16. https://doi.org/10.4230/LIPIcs.OPODIS.2016.24
[13] WEF. (2018). Building Block(chain)s for a Better Planet. https://www3.weforum.org/docs/WEF_Building-Blockchains.pdf
[14] IBM. (2022). What are smart contracts on blockchain? Retrieved September 1, 2022, from https://www.ibm.com/topics/smart-contracts
[15] Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. IEEE Access, 6, 5112–5127. https://doi.org/10.1109/ACCESS.2018.2789929
[16] Arndt, T., & Guercio, A. (2020). Blockchain-based transcripts for mobile higher-education. International Journal of Information and Education Technology, 10(2), 84–89. https://doi.org/10.18178/ijiet.2020.10.2.1344
[17] International Organisation of Employers. (2021). Addressing Skills Development.
[18] European Commission. (2022). Skills and qualifications. https://ec.europa.eu/social/main.jsp?langId=en&catId=1146
[19] Caldarelli, G., & Ellul, J. (2021b). Trusted Academic Transcripts on the Blockchain: A Systematic Literature Review. Applied Sciences, 11(4), 1842. https://doi.org/10.3390/app11041842
[20] Eaton, J. S., & Uvalic-Trumbic, S. (2008). Degree Mills: The Impact on Students and Society.
[21] College Board Research, T., Ma, J., & Pender, M. (2021). Trends in College Pricing and Student Aid 2021. www.collegeboard.org
[22] Patel, K., & Das, M. L. (2020). Transcript Management Using Blockchain Enabled Smart Contracts. In D. , D. M. Hung (Ed.), Distributed Computing and Internet Technology. ICDCIT 2020. Lecture Notes in Computer Science (Vol. 11969, pp. 392–407). Springer. Cham. https://doi.org/10.1007/978-3-030-36987-3_26
[23] Tapscott, D., & Kaplan, A. (2019). Blockchain Revolution in Education and LifeLong Learning: Preparing for Disruption, Leading the Transformation. www.blockchainresearchinstitute.org/contact-us
[24] Castro, R. Q., & Au-Yong-Oliveira, M. (2021). Blockchain and Higher Education Diplomas. European Journal of Investigation in Health, Psychology and Education 2021, Vol. 11, Pages 154-167, 11(1), 154–167. https://doi.org/10.3390/EJIHPE11010013
[25] Vidal, F. R., Gouveia, F., & Soares, C. (2020). Revocation Mechanisms for Academic Certificates Stored on a Blockchain. Iberian Conference on Information Systems and Technologies, CISTI, 2020-June. https://doi.org/10.23919/CISTI49556.2020.9141088
[26] Grech, A., Sood, I., & Ariño, L. (n.d.). Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education. https://doi.org/10.3389/fbloc.2021.616779
[27] University of Nicosia | Block.co. (2023). Retrieved March 20, 2023, from https://block.co/industries/university-of-nicosia/
[28] University of Birmingham. (2018). https://blog.bham.ac.uk/itinnovation/2018/05/24/blockchain-based-academic-certificate-authentication-system-overview/
[29] Orr, D., Pupinis, M., & Kirdulyte, G. (2020). Towards a European approach to micro credentials: a study of practices and commonalities in offering micro-credentials in European higher education. NESET Report. https://doi.org/10.2766/7338
[30] Lecocq, K. (2020). A EUROPEAN APPROACH TO MICRO-CREDENTIALS. https://doi.org/10.2766/94725
[31] Kistaubayev, Y., Mutanov, G., Mansurova, M., Saxenbayeva, Z., & Shakan, Y. (2022). Ethereum-Based Information System for Digital Higher Education Registry and Verification of Student Achievement Documents. Future Internet, 15(1), 3. https://doi.org/10.3390/fi15010003
[32] Jirgensons, M., & Kapenieks, J. (2018). Blockchain and the Future of Digital Learning Credential Assessment and Management. Journal of Teacher Education for Sustainability, 20(1), 145–156. https://doi.org/10.2478/JTES-2018-0009

[33] Wu, J. (2022). UNIVERSAL MICRO-CREDENTIAL CERTIFICATIONS POWERED BY THE BLOCKCHAIN: AN EXTENSION FOR EASEL. The Pennsylvania State University
[34] Mikroyannidis, A. (2020). Blockchain Applications in Education: A Case Study in Lifelong Learning. 21–25.
[35] Knowledge 4 All Foundation Ltd. (2019). https://k4all.org/project/credentify/
[36] Credentify. (2020). https://credentify.eu/about/
[37] University of Lille. (2023). Implementation of Blockchain Digital Credentials at University of Lille - France.
[38] European Blockchain Service Infrastructure. (2023). Retrieved March 24, 2023, from https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home
[39] Ethereum Energy Consumption | ethereum.org. (2023). Retrieved March 24, 2023, from https://ethereum.org/en/energy-consumption/
[40] Ethereum Crystal Delta Ltd. (2023). https://crystaldelta.com/university-of-mauritius-launches-ilearn-a-mooc-platform-based-on-the-concept-of-open-learning-and-micro-credentials/
[41] Kishore, S., & Chan, J., & Muthupoltotage, U. P. & Young, N., & Sundaram, D. Blockchain-based Micro-credentials: Design, Implementation, Evaluation and Adoption (2021). Hawaii International Conference on System Sciences Proceedings (HICSS). http://hdl.handle.net/10125/71442, The University of Auckland Business School Research Paper Series, Available at SSRN: https://ssrn.com/abstract=3964194
[42] Hyland Credentials. (2022). https://www.hylandcredentials.com/about
[43] Steiu, M.-F. (2020). Blockchain in education: Opportunities, applications, and challenges. https://firstmonday.org/ojs/index.php/fm/article/download/10654/9726/71482
[44] Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-Based Applications in Education: A Systematic Review. Applied Sciences 2019, Vol. 9, Page 2400, 9(12), 2400. https://doi.org/10.3390/APP9122400
[45] University of Nicosia. (2013, November 21). University of Nicosia. https://www.unic.ac.cy/cyprus-university-world-first-to- accept-bitcoins-for-tuition-rt-business-news/
[46] Hyland Credentials. (2022). The King's College. (2014, June 13). The King's College. https://www.tkc.edu/stories/kings-is-first-u-s-college-to-accept-bitcoin/
[47] ESMT Berlin. (2017, December 20). ESMT Berlin. https://esmt.berlin/knowledge/esmt-berlin-bitcoin-pays
[48] Ocheja, P., Flanagan, B., & Ogata, H. (2018). Connecting decentralized learning records: A blockchain based learning analytics platform. ACM International Conference Proceeding Series, 265–269. https://doi.org/10.1145/3170358.3170365

Bridging assets between the Lightning Network and EVM-compatible blockchains

Tim Käbisch
Hochschule Mittweida, Mittweida, Deutschland

The cryptocurrency ecosystem has seen significant growth with Ethereum and Bitcoin as foundational pillars. Ethereum introduced smart contracts revolutionizing decentralized applications (dApps) across various domains. Scalability challenges led to alternative ecosystems like Binance Smart Chain and Polygon, maintaining compatibility through the Ethereum Virtual Machine (EVM). Bitcoin also faces scalability issues, leading to the Lightning Network's development—an off-chain solution with payment channels for scalable instant transactions. Interoperability is increasingly crucial as the cryptocurrency ecosystem continues to grow, enabling seamless interactions between assets and data across multiple blockchain platforms. EVM-compatible blockchains and the Lightning Network offer unique advantages in their respective use cases. This paper utilizes atomic swaps to create a secure, fast, and user-friendly trustless bridge between the Lightning Network and EVM-compatible blockchains, fostering the growth of both ecosystems and unlocking novel opportunities.

1. Introduction

In the fast-evolving cryptocurrency ecosystem, numerous innovative ideas and blockchain platforms have emerged. Nevertheless, two ecosystems remain the prominent pillars of the cryptocurrency landscape: Ethereum and Bitcoin.

The introduction of smart contracts by the Ethereum network revolutionized the blockchain industry, empowering the development of diverse decentralized applications (dApps) spanning various domains like insurance, decentralized finance (DeFi), social platforms, and games. [1] Yet, scalability challenges persist within the Ethereum network, leading to the emergence of alternative blockchain ecosystems such as Binance Smart Chain, Polygon, and Avalanche. [2] Despite their distinctions, these ecosystems share a common feature - utilizing the Ethereum Virtual Machine (EVM) to modify their networks, fostering compatibility with the broader Ethereum ecosystem. [3]

Bitcoin [4], as the second pillar, stands as a widely-used global system, maintaining a transparent record of transactions on a publicly accessible ledger. However, its scalability encounters challenges due to each participating computer bearing the responsibility of validating, observing, and storing every transaction. Addressing this scalability concern, Joseph Poon and Thaddeus Dryja proposed a solution in their paper *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. [5] The Lightning Network, functioning as a second layer on top of Bitcoin, introduces off-chain payment channels, enabling users to conduct even the smallest transactions, such as micropayments, without the need to publish them on the Bitcoin blockchain. Since its initial proposal in 2015, followed by protocol implementation in 2018, the Lightning Network has garnered considerable attention from developers and investors, with numerous applications currently in development. [6, p. 9-12]

As the cryptocurrency ecosystem undergoes continuous growth and development, the importance of interoperability has become increasingly vital. Interoperability in the context of blockchain technology refers to the seamless interaction of assets and data across multiple blockchains. While exchanging data and value between parties using the same blockchain platform, like Bitcoin, is straightforward, it becomes more complex when different blockchain platforms are involved. EVM-compatible blockchains and the Bitcoin Lightning Network offer distinct advantages in their respective use cases. Establishing interoperability between these two systems by building a bridge holds the potential to unlock new possibilities and use cases, making it a significant focus area for research and development. [7]

Past attempts to construct a bridge between the Lightning Network and EVM-compatible blockchains are evident through various prototypes on GitHub. [8, 9] However, the need to run a separate Lightning node limits its accessibility to the masses. This paper presents the implementation of a secure, fast, and user-friendly trustless bridge between the two systems using atomic swaps to enable a seamless transfer of assets.

2. EVM-compatible blockchains

In the domain of software development, programmers commonly employ high-level programming languages, including Java, Python, or C++. Despite being human-readable, these languages cannot be directly executed by a computer's central processing unit (CPU). Consequently, a crucial process known as compilation is employed to translate the code into machine-executable bytecode. A compiler, a specialized software program, performs this task by converting the high-level code into a lower-level, machine-readable format. Once compiled, the CPU can execute the bytecode, enabling the computer to operate the program as intended.

Blockchain networks, such as Ethereum, operate as decentralized systems across globally distributed nodes. This unique distributed architecture sets them apart from traditional computing systems, as they do not rely on a single central processing unit (CPU) for program execution. Instead, the Ethereum network employs the Ethereum Virtual Machine (EVM) as a software-based CPU to execute bytecode on each network node. This enables developers to write smart contracts in high-level programming languages like Solidity, which are subsequently compiled into bytecode for execution by the EVM. This approach fosters the Ethereum network's operation without the need for a central control point, ensuring a truly decentralized and versatile *world computer*. [3]

When a smart contract is deployed on a blockchain network, it is replicated across all nodes in the network. Users can interact with the contract by submitting transactions, which are executed by each node's Ethereum Virtual Machine (EVM). The EVM ensures that the transactions are processed consistently across all nodes, resulting in a synchronized global state. In essence, the EVM acts as the central component of the distributed state machine, coordinating the execution of transactions to maintain a consistent state among all network participants. [10, p. 297]

3. Lightning Network

The Lightning Network is a revolutionary protocol that facilitates fast and cost-effective online value exchange. Serving as a second-layer technology for Bitcoin, it enables scalable transactions between users, including micropayments for the smallest amounts. Introduced in 2015 and implemented in 2018, the Lightning Network has gained considerable interest from developers and investors, with numerous applications currently in development. [6, p. 1]

3.1 Scaling Bitcoin

Bitcoin, a widely-used global system, faces scalability challenges as each participating computer validates, observes, and stores transactions. The increasing popularity and transaction demand have led to the frequent reaching of the block size limit. When blocks are full, additional transactions queue up, leading to increased fee competition. Consequently, lower-value transactions may become unprofitable during high-demand periods. One solution is to raise the block size limit, allowing more transactions. However, this would shift costs to node operators, requiring greater resources for blockchain validation and storage. Larger block sizes also impose higher bandwidth and processing requirements, leading to increased centralization as fewer individuals can afford to operate a node. [6, p. 9]

Bitcoin's scalability is often compared to Visa, which can process around 40,000 transactions per second at peak usage. [6, p. 9] To match Visa's capacity, Bitcoin would require a block size limit of approximately eight gigabytes, resulting in over one terabyte of transaction data daily with a block mined every 10 minutes on average. This increased size would make running a node at home impractical, limited only to large companies with ample resources. However, even achieving Visa's transaction capacity would only equal traditional financial payment networks and might not be sufficient for future demands with the rise of microtransactions and machine-to-machine payments. [6, p. 9-10]

The paper *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments* by Joseph Poon and Thaddeus Dryja presents a solution to Bitcoin's scalability challenge through the Lightning Network. This second-layer network introduces off-chain payment channels, allowing users to transact without recording each transaction on the Bitcoin blockchain. Payment channels are established as 2-of-2 multi-signature addresses, enabling efficient and unlimited payments within the channel's lifespan. Transactions occur off-chain through signed transactions, and the channel can be closed by broadcasting the latest transaction to the blockchain. [6, p. 10-12, 40]

The Lightning Network's ability to enable instant payments with minimal fees has captured the attention of developers interested in building Lightning Applications (LApps). One promising use case for LApps is pay-per-use, offering users the option to pay solely for the specific services they utilize, rather than subscribing to a fixed plan. This model can be advantageous for various scenarios, such as newspaper subscriptions, where users only pay for the articles they read, or music streaming services, where they only pay for the songs they listen to. Additionally, lightning payments can extend to everyday goods, like purchasing coffee at a restaurant or snacks from a vending machine. Compared to traditional payment methods like cash or credit cards, lightning payments offer faster and cheaper transactions, benefiting both consumers and providers. [11, 12]

3.2 Invoices

Bitcoin transactions involve sending funds to the receiver's Bitcoin address, accessible only with the corresponding private key. This address can be used multiple times without limitations. Conversely, the Lightning Network relies on unique invoices to initiate payments. The recipient generates a unique secret (preimage) for each invoice and must reveal it in the end to complete the payment. To prevent fund theft, a different secret should be used for each payment. Payments on the Lightning Network are atomic, ensuring they are either fully successful or not, with no partial states. Recipients can share invoices through various channels, including email, chat, or QR codes. [6, p. 55, 336]

A lightning invoice contains vital details, such as the payment hash, payment amount, payment description, and expiry time. The payment hash plays a critical role as the

payment identifier and key to finalizing the payment. To generate the payment hash, a unique secret (preimage) is selected and then hashed using the SHA-256 algorithm. The preimage remains exclusively known to the invoice creator, as reversing the SHA256-algorithm is practically impossible. [6, p. 56]

In the Lightning Network, payments are facilitated through hashed timelock contracts (HTLCs), allowing funds to be securely transferred through a route of payment channels from the payer to the recipient. HTLCs ensure that intermediaries cannot steal the funds during the routing process. To finalize the payment, the recipient must reveal the preimage to settle the HTLC along the route. Thus, if the payer possesses the preimage, the payment is completed, and the preimage serves as proof of payment. This concept of utilizing the preimage as proof of payment is crucial to this work and will be further explored in chapter 4. [6, p. 56]

3.3 WebLN

WebLN serves as a set of established guidelines for Lightning applications and client providers, aiming to facilitate secure interactions between web applications and users' wallets. It provides a programmatic interface that empowers applications to make payments, generate invoices for receiving payments, and perform other associated functionalities seamlessly. Initializing and executing WebLN merely necessitates a few lines of JavaScript code, a popular language extensively used for developing web applications. [13]

Alby, a versatile and open-source browser extension, serves as a prominent provider of WebLN. It is purpose-built to provide profound integration between the Bitcoin Lightning Network and web applications. The primary intent of this extension is to ease the web payment process by using the WebLN standard as a bridge between websites and Lightning Network nodes. This interface has significantly simplified the user experience for payments, authentication procedures, and other related functions. [14]

The extension's capabilities make it a perfect fit for the paper’s objective: creating a trustless bridge between the Lightning Network and EVM-compatible blockchains. Utilizing Alby in this context can significantly improve the user experience, enhancing its efficiency and reliability. The implementation of the WebLN standard in Alby enables the sending of payments with just a few lines of code, as shown in figure 1. [14]

```
1   await webln.enable();
2   const invoice = "lnbc10u1pjqw9nnp...";
3   const result = await webln.sendPayment(invoice);
```

Figure 1: Lightning Payment with WebLN

4. Concept

The concept of atomic swaps empowers users to transfer funds between distinct blockchain ecosystems without the need for centralized exchanges as intermediaries. This is accomplished through the use of hashed timelock contracts (HTLCs). However, a prerequisite for this is the compatibility of both ecosystems with the same hashing algorithm. Since both the Lightning Network and EVM-compatible blockchains utilize the SHA-256 hashing algorithm, atomic swaps can be effectively used to bridge assets between these two distinct ecosystems.

Hashed timelock contracts (HTLCs) are a type of smart contract that establish conditional payments between two parties. These contracts combine two fundamental concepts: hashlock and timelock, to ensure the transaction's execution adheres to the agreed-upon terms. A hashlock acts as a constraint that prohibits spending an output until specific data, matching a predetermined hash, becomes available. On the other hand, a timelock restricts a transaction from being executed until a predetermined time or deadline is reached. In essence, HTLCs involve a sender locking cryptocurrency up in a contract and sharing a secret with the recipient following a specific action. The recipient can access the funds if they provide the correct secret within a set time frame (the timelock). If they fail to do so, the funds revert to the sender. [15]

The primary concept of this paper is to construct an HTLC that can be unlocked following payment on the Lightning Network. This approach enables an individual to lock up funds in an HTLC on an EVM-compatible blockchain and generate a lightning invoice for the equivalent value of those funds. Subsequently, the HTLC and invoice are provided to a second individual, who, upon payment of the invoice, gains the ability to unlock the funds from the HTLC. This process effectively enables the exchange of funds on the EVM-compatible blockchain for Bitcoin on the Lightning Network.

The core idea behind this concept is to utilize the payment hash of the lightning invoice as the hashlock for the HTLC. This payment hash is generated by selecting and hashing a unique secret (preimage) for the payment, as described in section 3.2. Additionally, the payer possesses the preimage after completing the payment, effectively making the preimage serve as proof of payment.

Hence, an individual could generate a lightning invoice and employ the payment hash as the hashlock for an HTLC on an EVM-compatible blockchain. The value of the lightning invoice corresponds to the value of the funds locked up within the HTLC. Subsequently, the HTLC and invoice are provided to a second individual. Unlocking the HTLC necessitates presenting the corresponding preimage to the hashlock, which essentially means providing a value that, when hashed using the SHA256 algorithm, matches the hashlock. Since the hashlock used in the HTLC is the payment hash of the lightning invoice, the preimage of the lightning invoice also functions as the preimage of the HTLC. As a result, once the second individual successfully pays the lightning invoice and becomes aware of the preimage, they can unlock the HTLC by presenting this obtained preimage. This concept is illustrated in figure 2.

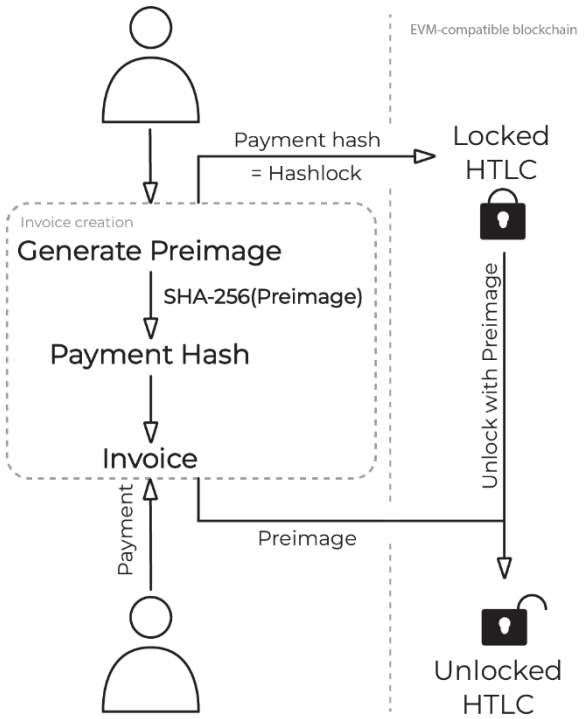

Figure 2: Concept

5. Implementation

In the proposed solution, swaps are always performed between a customer and the operator. However, the design ensures that neither the customer nor the operator needs to place trust in each other. At its core, the implementation consists of three components:

- User Interface (Customer)
- Backend (Operator)
- Smart Contract (HTLC)

For seamless interaction with both an EVM-compatible blockchain and the Lightning Network, a set of tools is required. Users utilize two browser extensions linked to the user interface, as depicted in figure 3. Specifically, Alby is employed for Lightning Network interaction, and Metamask is utilized for the interaction with an EVM-compatible blockchain. On the other hand, the operator utilizes LNbits, a Lightning Network payment management platform, to generate and settle invoices, while leveraging the web3.js library for interactions with EVM-compatible blockchains. [16]

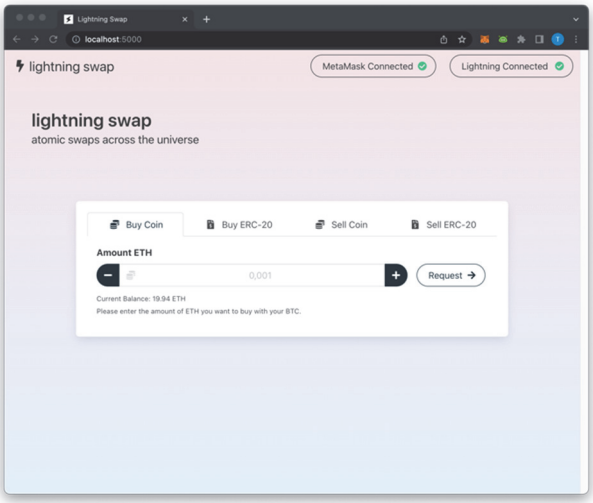

Figure 3: User Interface

The smart contract can be deployed on any EVM-compatible blockchain, enabling a bridge between the Lightning Network and the corresponding blockchain (e.g., Ethereum or Polygon). The term *native coin* is used in this paper to avoid specifying a particular cryptocurrency like ether, as the proposed solution is not limited to the Lightning Network and Ethereum but can be established with any EVM-compatible blockchain. Additionally, it is essential to differentiate between the native coin of a blockchain and tokens. The native coin represents the currency of the blockchain system, such as ether on Ethereum or MATIC on Polygon. In contrast, tokens do not have their blockchain but operate on top of other blockchains. These tokens are usually created in compliance with a specific standard, such as the ERC-20 standard.

This implementation includes four directions: buying native coins and ERC-20 tokens with Bitcoin on the Lightning Network (LN) and selling native coins and ERC-20 tokens for Bitcoin on the LN. While the process of buying native coins with Bitcoin on the Lightning Network is described in detail, the other directions are only briefly discussed in this paper.

5.1 HTLC in Solidity

Implementing a hashed timelock contract (HTLC) within a smart contract is a vital aspect of the proposed concept, which can be accomplished using the Solidity programming language. The HTLC implementation in this paper is based on a library accessible on GitHub. [17] The data for a hashed timelock contract (HTLC) is stored in a *struct*. Among other things, this struct contains elements such as the sender and recipient addresses, the hashlock, and the timelock. Each HTLC's data is stored in

a map, using a 32-byte identifier (ID). To manage HTLCs, the smart contract includes several functions:

a) **haveContract**: This function verifies the existence of an HTLC associated with a given 32-byte ID. It returns a boolean value of true if the HTLC exists and false otherwise.

b) **newContract**: To create a new HTLC, the newContract function is used. It requires three parameters: the intended receiver (who will withdraw funds by providing the preimage), the hashlock, and the timelock. The number of native coins locked in the new HTLC is specified by the msg.value, representing the number of native coins included in the transaction executing the newContract function.

c) **getContract**: Access to HTLC information is possible using the getContract function, which requires providing the HTLC identifier (ID). If an HTLC exists for the given ID, all stored information associated with the HTLC will be returned.

d) **withdraw**: The primary objective of an HTLC is to enable the receiver to unlock and claim their funds by providing the preimage that unlocks the hashlock. The withdraw function facilitates this functionality, taking the HTLC identifier (ID) and the preimage as parameters to claim the funds associated with the HTLC.

e) **refund**: In cases where the intended receiver fails to unlock the HTLC, the creator of the HTLC can reclaim the funds. The refund function allows the creator to call it after the timelock has expired to reclaim their funds.

Although the HTLC mechanism is similar for native coins and ERC-20 tokens, there are slight variations in the implementation for ERC-20 tokens.

5.2 Lightning – Native Coin

This section examines the scenario where a customer acquires native coins using Bitcoin on the Lightning Network (LN). The associated protocol for this situation is visually represented in figure 4. All customers engage in swaps with the operator; however, the design ensures that neither the customer nor the operator is required to place trust in each other.

Before starting a swap, the customer needs to connect their Metamask and Alby wallet to the user interface. They select the network and the number of coins they want to buy with Bitcoin on the Lightning Network, then send an HTTP POST request to the operator. This request, sent to the *offerCoinBuy* endpoint, includes the desired number of coins, the customer's address, and the chosen network.

The operator sends the customer an offer, which contains the details for the swap. Furthermore, it includes a lightning invoice to be paid for accepting the offer (the *offer invoice)*. This protects the operator from spam and unnecessary costs, as the operator bears the gas costs

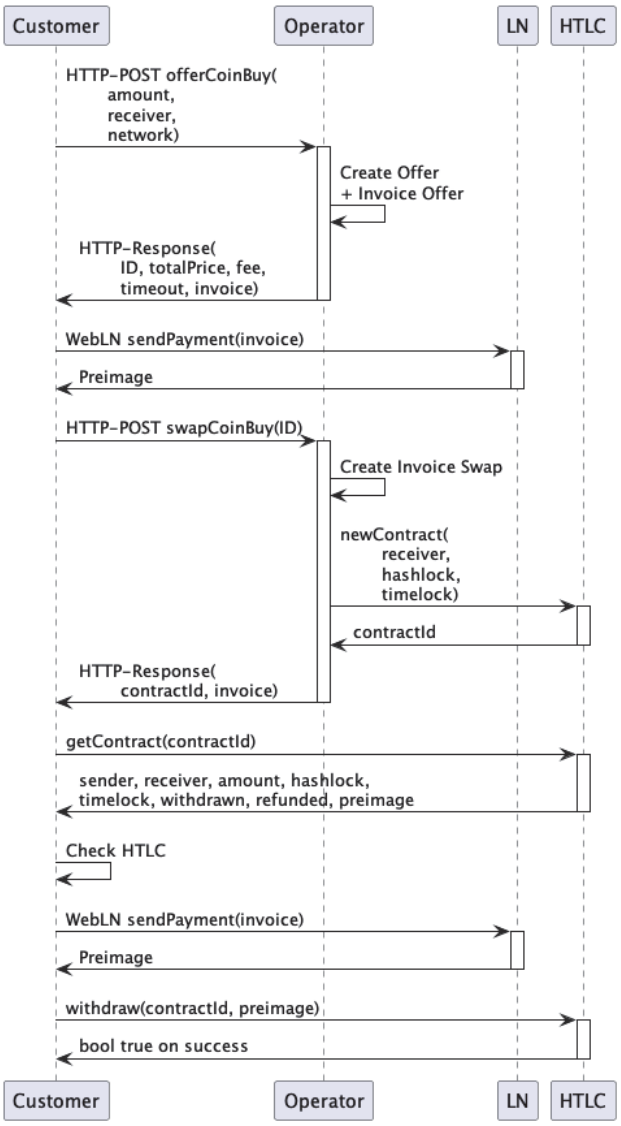

Figure 4: Protocol: Lightning – Native Coin

for creating the HTLC and potential extra costs if the customer fails to conduct the swap. This step prevents customers from requesting a swap without the intention to conduct it. The offer also includes a timeout, which allows the customer time to consider the offer and prevents the operator from committing to a specific exchange rate for an extended period.

The offer is presented to the customer via the user interface. Within the specified timeout, the customer can accept the offer by paying the lightning Invoice using their connected Alby wallet. Upon payment, the user interface sends an HTTP POST request to the operator's *swapCoinBuy* endpoint, including the offer's identifier (ID) to initiate the creation of the HTLC. The operator validates the presence of an offer corresponding to the given ID, verifies that the customer responded within the specified timeout, and ensures the payment of the invoice. If all conditions are met, the operator proceeds to create a lightning invoice for the equivalent value of the requested native coins (the *swap invoice)*.

The payment hash of the lightning invoice serves as the hashlock for creating the HTLC, as explained in detail in

chapter 4. The operator creates a new HTLC by executing the *newContract* function of the smart contract, effectively locking up the native coins. The function returns a 32-byte identifier, the *contractId*, which, along with the lightning invoice, is sent back to the user interface in response to the HTTP request.

Before prompting the customer to pay the lightning invoice, the user interface carries out multiple verification checks. These checks involve verifying whether the invoice's payment hash aligns with the HTLC's hashlock, if the HTLC's timelock is set to at least five minutes in the future, whether the amount locked up in the HTLC matches the requested amount, and if the HTLC's recipient corresponds to the customer's address. The verification check guarantees that the customer does not need to trust the operator blindly. The customer can independently verify all crucial information before paying the lightning invoice of the operator. Upon successful verification, the customer can be confident that after paying the lightning invoice, they can unlock the HTLC and retrieve their funds.

After verifying the HTLC's integrity, the customer pays the lightning invoice using their Alby wallet. Upon successful payment processing on the Lightning Network, the customer knows the payment's preimage (as outlined in section 3.2) and uses it to withdraw their requested native coins from the HTLC. The user interface provides a claim button that initiates a transaction and prompts the customer for confirmation in their Metamask wallet. The transaction calls the smart contract's *withdraw* function, submitting the HTLC's identifier and preimage. The smart contract checks if the preimage aligns with the HTLC's hashlock.

Finally, the smart contract concludes the swap by transferring the coins locked in the HTLC to the customer. Consequently, the customer obtained their desired native coins, and in exchange, the operator received their Bitcoin on the Lightning Network.

Nonetheless, it's important to note that not all swaps may be successfully conducted. If the customer fails to accept the offer, the operator will discard the offer once the timeout period lapses. Should the customer accept the offer but fail to pay the lightning invoice to conduct the swap, the operator must wait for the HTLC to expire due to the timelock. Once it expires, the operator can trigger a refund by invoking the *refund* function of the smart contract. Conversely, if the operator attempts to deceive the customer, the customer will detect this through the verification checks and could simply abort the swap by refraining from paying any invoice.

5.3 Other directions

In addition to purchasing native coins, customers can also buy ERC-20 tokens supported by the operator on the relevant network. While each blockchain has only one native coin, it may support multiple ERC-20 tokens, each identified by a unique address. In contrast to native coins, ERC-20 tokens cannot be directly sent using a regular transaction. Instead, transferring ERC-20 tokens requires utilizing specific functions provided by the ERC-20 token contract.

Hence, the protocol for purchasing ERC-20 tokens, compared to the one for buying native coins, necessitates the following adjustments: the customer is required to specify the address of their preferred ERC-20 token and the management of ERC-20 tokens must be configured accordingly. Besides these modifications, the protocol remains quite similar to buying native coins.

The protocol presented in section 5.2 can also be applied in reverse, enabling customers to sell their native coins and ERC-20 tokens for Bitcoin on the Lightning Network. Similar to the buying process, the customer engages in a swap with the operator, and both parties do not need to trust each other. Upon submitting an HTTP request, the customer receives an offer from the operator, specifying the amount the operator is willing to pay for the native coins or ERC-20 tokens the customer intends to sell.

From this point onward, the customer and operator essentially switch roles compared to the protocol illustrated in figure 4. The customer takes charge of creating the lightning invoice and the hashed timelock contract (HTLC). These tasks are performed programmatically by the user interface, and the customer's role is to confirm the actions in their Alby and Metamask wallets, respectively.

Following this, the customer forwards the lightning invoice and HTLC to the operator. Before paying the lightning invoice, the operator conducts the verification checks outlined in section 5.2. This ensures that the operator does not need to trust the customer. Once the HTLC's integrity is confirmed, the operator pays the lightning invoice, revealing the payment's preimage. Finally, the operator retrieves their native coins or ERC-20 tokens from the smart contract by providing the preimage. On the other hand, the customer received their Bitcoin on the Lightning Network. This protocol enables customers to sell their native coins or ERC-20 tokens for Bitcoin on the Lightning Network in a trustless manner.

6. Conclusion

This paper has shown the development of a trustless bridge that facilitates asset transfer between the Bitcoin Lightning Network and EVM-compatible blockchains. Due to the solution's versatility, it is capable of creating a bridge between the Bitcoin Lightning Network and any blockchain that is compatible with the Ethereum Virtual Machine (EVM). To establish a bridge, the HTLC smart contract simply needs to be deployed on the corresponding EVM-compatible blockchain. The primary focus of this work has been on the technical aspects of the solution. Nevertheless, for the operational deployment of the developed platform, certain non-technical factors, such as economic and security considerations, require further consideration.

Adequate liquidity on the Bitcoin Lightning Network and EVM-compatible blockchain is crucial for the platform's operation. A rebalancing mechanism is needed to prevent trade disruption due to asset shortages. Furthermore, developing a sustainable monetization model, such as charging a competitive swap fee, is essential. Additionally, a comprehensive analysis of costs for customers and the operator, considering the Lightning Network payment route and the demand on the corresponding EVM-compatible blockchain, is required.

Finally, one downside of atomic swaps is the *free option problem*. It refers to a situation where one party can exploit the time delay between the initiation and execution of the swap to gain an advantage. During this time, market conditions may change, allowing the exploiting party to decide whether to proceed with the swap or back out, potentially resulting in an unfair advantage. By implementing a timeout, the free option problem can be mitigated, as is done in the proposed solution. However, determining the optimal duration of the timeout still requires further clarification. [18]

This paper paves the way for the development of a production-ready service that enables a trustless bridge between the Bitcoin Lightning Network and EVM-compatible blockchains using atomic swaps. This research aims to foster the growth of both ecosystems, unlocking new opportunities for them to leverage each other's advantages.

References

[1] Ethereum.org. “What is Ethereum?” (2023), [Online]. Available: https://ethereum.org/en/what-is-ethereum. (last visited on 09/05/2023).

[2] Kearney, Leal. “What are EVM Compatible Blockchains? A Guide to the Ethereum Virtual Machine”. (2023), [Online]. Available: https://blog.thirdweb.com/evm-compatible-blockchains-and-ethere um-virtual-machine/. (last visited on 09/05/2023).

[3] GoCrypto. “What are EVM-compatible blockchains?” (2022), [Online]. Available: https://medium.com/eligma-blog/what-are-evm-compatible-blockchains-64f91c97038e. (last visited on 23/02/2023)

[4] Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”. (2008), [Online]. Available: https://bitcoin.org/bitcoin.pdf. (last visited on 09/05/2023).

[5] Joseph Poon, Thaddeus Dryja. “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments”. (2016), [Online]. Available: https://lightning.network/lightning-network-paper.pdf. (last visited on 09/05/2023).

[6] Andreas Antonopoulos, Olaoluwa Osuntokun, René Pickhardt, Mastering the Lightning Network. O’Reilly Media, Inc., 2021, ISBN: 978-1-492-05486-3.

[7] Cointelegraph. “What is blockchain interoperability: A beginner’s guide to cross-chain technology”. (2023), [Online]. Available: https://cointelegraph.com/learn/whatis- blockchain - interoperability - a - beginners - guide - to - cross - chain -technology. (last visited on 19/04/2023).

[8] Leon Do. “submarine-swaps”. (2020), [Online]. Available: https://github.com/leondo/submarine-swaps. (last visited on 26/04/2023).

[9] Aleksey Bykhun. “ln-eth-swap”. (2018), [Online]. Available: https://github.com/caffeinum/ln-eth-swap. (last visited on 26/04/2023).

[10] Andreas Antonopoulos, Dr. Gavin Wood, Mastering Ethereum. O’Reilly Media, Inc., 2018, ISBN: 978-1-491-97194-9.

[11] Blocktrainer. “Bitcoin zum Anfassen: Der Lightning Snackautomat”. (2023), [Online]. Available: https://www.blocktrainer.de/bitcoin-zum-anfassen-der-lig htning-snackautomat. (last visited on 09/03/2023).

[12] Coincharge. “Payment per newspaper article with Bitcoin Lightning”. (2023), [Online]. Available: https://coincharge.io/en/payment-per-newspaper-article-withbitcoin-lightning. (last visited on 09/03/2023).

[13] Alby. “WebLN Guide”. (2023), [Online]. Available: https://github.com/getAlby/webln-guide. (last visited on 06/03/2023).

[14] Alby. “lightning-browser-extension”. (2023), [Online]. Available: https://github.com/getAlby/ lightning-browser-extension#lightning-web-extension. (last visited on 06/03/2023).

[15] Minima. “Understanding Hashed Time-locked Contracts (HTLCs)”. (2022), [Online]. Available: https://www.minima.global/post/understanding-hashed-time-lockedcontracts-htlcs. (last visited on 17/03/2023).

[16] LNbits. “Free Open-Source Bitcoin Lightning Accounts System with Extensions”. (2023), [Online]. Available: https://lnbits.com. (last visited on 09/03/2023).

[17] C. Hatch. “hashed-timelock-contract-ethereum”. (2021), [Online]. Available: https://github.com/ chatch/hashed-timelock-contract-ethereum. (last visited on 26/04/2023).

[18] M. Hammond. “Blockchain Interoperability Series: Atomic Swaps”. (2019), [Online]. Available: https://medium.com/@mchammond/atomic-swaps-eebd0fa8110d. (last visited on 28/07/2023).

Business Reputation Systems Based on Blockchain Technology — A Risky Advance

Simon Hemmrich
Universität Paderborn, Paderborn, Deutschland

Reputation is indispensable for online business since it supports customers in their buying decisions and allows sellers to justify premium prices. While IS research has investigated reputation systems mainly as review systems on online platforms for business-to-consumer (B2C) transactions, no proper solutions have been developed for business-to-business (B2B) transactions yet. We use blockchain technology to propose a new class of reputation systems that apply ratings as voluntary bonus payments: Before a transaction is performed, customers commit to pay a bonus that is granted if a service provider has performed a service properly. As opposed to rival reputation systems that build on cumulated ratings or reviews, our system enables monetized reputation mechanisms that are inextricably linked with online transactions. We expect this system class to provide more trustworthy ratings, which might reduce agency costs and serve quality providers to establish a reputation towards new customers.

Keywords: Trust, Risk, Reputation System, Blockchain Technology, Business Reputation System.

1. Introduction

Online business requires buyers to trust that sellers will deliver a product or service as promised. However, buyers have incomplete information about the seller's capabilities and are exposed to the risk of not being satisfied as expected. A way to reduce this uncertainty is to establish trust (Luhmann, 2017) or reputation (Jøsang et al., 2007), increasing the buyer's confidence in a buying decision (Sullivan & Kim, 2018). Trust is a social construct and refers to "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer et al., 1995, 712). Reputation is an observable public opinion about an entity standing out from a group (Jøsang et al., 2007). It can be established with reputation systems that are information systems (IS).

Reputation systems reliably collect, store, and distribute information about an entity's past behavior (Cai & Zhu, 2016; Resnick et al., 2000). An entity might refer to a person, a group, or an organization. Reputation systems purvey reputation to provide objectified measures to assess trustworthiness subjectively (Jøsang et al., 2007; Jøsang, 2016), particularly to select trustworthy entities for buying decisions based on ratings from unknown agents (Resnick & Zeckhauser, 2002). Thus, reputation systems include ratings or reviews to inform third parties. Review systems feature plain text reviews and other metrics, while in rating systems, a product or service is rated typically, e.g., with a star rating. Both types are often used in a B2C context to indicate a seller's reputation (Gutt et al., 2019; Moreno & Terwiesch, 2014). Well-known examples that integrate both types are amazon.com and yelp.com.

Reputation has been proven to play an important role in business deals, supporting buying decisions and allowing sellers to achieve higher prices (Ba & Pavlou, 2002; Moreno & Terwiesch, 2014). Many value propositions in a B2C context are rated every day, including products, accommodations, shares, rideshares, mini-jobs, and more. However, although these systems are designed to reflect reputation and establish trust, they are also infused with "spam, tampered ratings, and reviews, and paid reviews" (Subramanian, 2018, p. 81), since ratings are disconnected from the actual transaction.

Surprisingly, no global reputation system is available for companies to rate each other's products or services on a daily basis. Since millions of transactions are performed among companies every day using digital technologies, a profound basis for rating other companies' performance would be available. However, very few efforts have been made to design such systems (Dikow et al., 2015; Gutt et al., 2019), even though "creating a reliable, trustworthy distributed record system, or ledger, may be fundamental to how we organize interpersonal and inter-organizational relationships" (Beck et al., 2017, p. 381). Reputation systems help to solve the famous lemon market problem (Thierer et al., 2016), where asymmetric information between providers and customers leads to an adverse selection of bad products while driving good products out of the market (Akerlof, 1970).

Blockchain technology is discussed to deliver a missing link to design better and robust reputation systems (Cai & Zhu, 2016; Catalini & Gans, 2016; Möhlmann et al., 2019). Blockchain technology is known to establish trust between economic actors without the need to install a trustworthy intermediary. A blockchain is built on a distributed peer-to-peer network to provide a reliable,

public, and tamperproof infrastructure to conduct trustworthy and secure transactions (Nakamoto, 2008). This technology defines new ways to trust each other, prompting IS research to revisit trust as a construct (Beck et al., 2016; Ostern, 2018). Related research views this technology as a trust-free transaction system (Beck et al., 2016) or a trusted code (Simser, 2015). Research on blockchain-based reputation systems currently focuses on designing algorithmically secure and anonymous systems (e.g., Bag et al., 2018; Bazin et al., 2017). However, purely technological approaches struggle to induce reliable data on-chain from the outside world (Greenspan, 2016), disregarding off-chain reputation mechanisms.

We posit that reputation is a subjective phenomenon that builds on social relations, so off-chain trust mechanisms must be considered alongside technological mechanisms. However, until now, the trust perspective on blockchain technology is rarely addressed in top IS journals (Ostern, 2018), although IS research can explain how to establish trust with this technology (Risius & Spohrer, 2017; Seidel, 2018). While there have been calls for finding design mechanisms to build reliable blockchain-based reputation systems (Voshmgir & Zargham, 2020), an unresolved challenge is to enable individualized reputation and design proper incentive mechanisms (Pereira et al., 2019). Thus, we derive the research question: How can we use the trust concept for designing business reputation systems?

Therefore, we set out to revisit the trust construct and explain how the closely related concept of risk can be combined with blockchain-secured transactions to establish trust in B2B transactions. Our approach aims to represent trust relations backed with safeguards to help others to trust. Based on our initial findings, we provide two core contributions to this research-in-progress paper. First, we review and clarify the role of trust concerning blockchain technology. Second, we introduce the idea of leveraging a risky advance as a trust signal by a service provider offering a price discount while getting paid with voluntary bonuses, thereby demonstrating its capability and building a reputation. This idea is innovative since it breaks with established approaches to review or rate a seller retrospectively after transactions have been concluded. Monetary payments as ratings have three advantages. They allow us as researchers to conceptualize a system with a tangible risky advance representing one-sided trust relations. The amount of payments allows us to differentiate the significance of ratings as a parameter. The economic value of ratings is likely to increase the expressiveness of positive ratings since they cost money and might mitigate reciprocity issues.

In Section 2, we review the core concepts of trust, risk, and reputation, along with their role in existing reputation systems, before reviewing key properties of blockchain technology. We summarize and justify our research method in Section 3. In Section 4, we sketch out the idea for designing a blockchainbased B2B reputation system using the reputation mechanism of a risky advance that helps to ease trust between unknown business agents. Section 5 discusses the research contribution and concludes the paper, sketching the path ahead for a new class of reputation systems.

2. Related Research

2.1. Trust and Risk, System Trust, and Reputation

Trust is a multidimensional social construct studied extensively in the social context. It refers to various aspects of cognition, emotion, and behavior. Trust is highly subjective and varies depending on the purpose and context. It is indispensable for social interactions and reduces decision uncertainty. As a social lubricant, trust also enables fluid business exchange (Arrow, 1974; Sun, 2010).

In general, trust is an expectation about the actions to be performed by others—unlike calculus, and it starts before it is possible to monitor the actions of another actor (Williamson, 1993). As a priori concept, trust always comes with the risk that trust is unwarranted (Luhmann, 2017). It goes hand in hand with a voluntary willingness to take a risk, to lose something that appears valuable, even if a trustor does not expect to be disappointed (Deutsch, 1958; Mayer et al., 1995; Schoorman et al., 2007). Thus, there must be something at stake for trust to be built (Kee & Knox, 1970; Schoorman et al., 2007), indicating a constitutive relation between risk and trust (Chetty et al., 2021; Siegrist, 2021). When one makes a voluntary risky advance in a certain matter, it eases giving trust of the other party particularly (Gambetta, 1988; Luhmann, 2017).

System trust is decisive in reputation systems (Pennington et al., 2003). It is independent of a person's risk tendency or motives (Shapiro, 1987). As a form of distributed trust, it emerges in social systems and is based on explicit and organized control mechanisms, according to concrete requirements. These concrete requirements include safeguards built into the system to preserve the fragility of trust by sanctioning adverse behavior (Luhmann, 2017). In this way, a reputation system works as a collaborative sanction system that discourages untrustworthy behavior (Jøsang et al., 2007).

Trust is closely related to reputation. It is a positive, cognitive assessment by an individual towards another individual or entity, while reputation relates to a group's positive, distributed opinion (Bromley, 2001; Jøsang et al., 2007). Like trust, reputation is contextual, valuable, takes time to build, and is destroyed quickly (Dasgupta, 1988). Reputation occurs only compared to other potential trustees and can help foster trusting a specific trustee. When there is not enough information on whom to trust, peers that have already built trust are consulted—even if they are strangers—as long as they are in a similar position as the trust seeker. Demonstrating to have

trusting customers representing a reputation cancause new, yet uncertain customers to trust (Moreno & Terwiesch, 2014).

Trusting in fellow customers who, themselves, trust a provider creates a transitive relation of trust. Trust transitivity states that trusting a third person depends mainly on what extent a referral is trusted (Jøsang et al., 2007; Jøsang, 2016) (Figure 1). First-order trust refers to trusting a recipient directly, while reputation is a form of second-order trust derived from observing peers' first-order trust. 3.

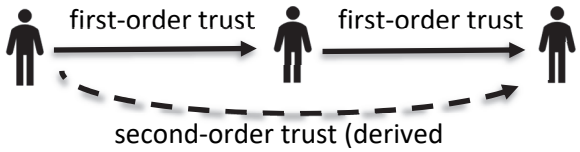

Figure 1: Trust transitivity principle (modified from Jøsang et al. 2007).

2.2. Trust and Risk Inscribed in Information Systems

Early research in IS investigates reputation in game-theoretical settings, splitting up into research on reputation systems to model trustworthiness between (computational) network nodes and research to assess the trustworthiness of sellers/service providers in e-commerce, e.g., through review systems.

Trust and reputation have been ascribed to network nodes (e.g., computer nodes, companies) as well as to things (e.g., vehicles), departing from their original conceptualization as emotional or cognitive concepts. Since trust is inherently based on cognitive processes, modeling trust has no solid validation point in the computational context. Still, modeling trust in these systems has its raison d'être for designing reliable and secure IS (Jøsang, 2016). Computational trust—a quantity or score— refers to an online node's technical capabilities and network contribution from calculated propagated ratings (Jøsang et al., 2007). See Bellini et al. (2020) for a comprehensive view of current reputation systems.

For e-commerce, Jøsang et al. (2007) recognize risk as an inherent characteristic of reputation systems, distinguishing classes of trust according to the risk context. Risk includes, for instance, the risk of not making a good buying decision (decision trust), not being satisfied with a service or product (provision trust), not being part of an honest system (system trust), having no sufficient control mechanisms (reliable trust), and the risk to select false identities (identity trust). However, the concept of risk is often considered a sideline phenomenon in reputation systems (F. Li et al., 2012), even provided that conceptualizing risk shifts the underlying trust mechanism in reputation systems drastically (Litos & Zindros, 2017). For computational reputation networks, risk conceptions are often considered implicitly as a computational network score. However, this also has the disadvantage that reputation is not specifically but globally condensed, which contradicts the social view of trust as an individual construct. Integrating risk in rating processes is hardly discussed in online marketplaces (e.g., Amazon.com or eBay.com) or other business reputation systems. This faint consideration of risk in reputation mechanism might be a reason for false reviews, fraud, and customers' reluctance to trust ratings provided on online marketplaces since a seller and buyers have nothing to be risked in the rating process. Therefore, we conceptualize a reputation system with a risky advance to strengthen buyers' ratings, and make it at the same time easier for trustworthy sellers to win over new customers.

2.3. Blockchain Technology as an Enabler of Reliable Trust

A blockchain is a distributed ledger recording digital transactions between nodes in a network securely. Transactions are hashed, stored in blocks, and appended to a previous block, establishing an ever-growing chain of blocks, in which transactions can hardly be changed (Buterin, 2014). Every node holds a copy of the current state of the blockchain, representing an immutable ledger that is stored in the distributed network (Nakamoto, 2008). Transactions are transparent in the network, and parties can verify them easily. Based on this, smart contracts can be committed on a blockchain, providing a reliable basis for automated business exchange (Buterin, 2014). Blockchains shift trust away from the contractor to the entire blockchain network if the network and the smart contracts are deemed reliable (Kim, 2020; X. Li et al., 2008; Seidel, 2018). A blockchain can help foster trust, as it has the following features:

- Immutability refers to reliable transactions secured as (relative) tamper-proof records in a blockchain. Parties can verify executed transactions themselves, eliminating the need for a central authority to validate transactions. In a blockchain-based reputation system, ratings can be stored reliably, and no single actor can change, nor disavow a rating (Cai & Zhu, 2016).

- Distributed trust in a blockchain network (Seidel, 2018) is a form of system trust. System trust is established with a series of control mechanisms, comprising validation mechanisms in the network to approve transactions, so that reputation ratings (as transactions) can be verified.

- Decentralization lowers an intermediary's ability to restrict and control activities in a system (Filippi, 2016). A decentralized blockchain network with many independent validators makes most attack scenarios virtually impossible. Manipulating blockchain-secured ratings of transactions is highly unlikely.

- Transparency relates to the visibility of transactions, including transaction content, limited to protecting users' privacy. Privacy also allows pseudo-anonymity so that users can decide with whom to share private data. For reputation systems, parties can apply different

pseudonyms that cannot be linked, signing a transaction with different personal keys (Filippi, 2016).

These features imply that contractual agreements cannot be changed without the approval of the counterparty, reducing the need to monitor or check the contractors' actions. In this way, a blockchain can reduce agency costs by providing a basis of reliable trust for business exchange (Murray et al., 2019) and prevent strategic lying about ratings. Similarly, rating agreements can be secured on a blockchain.

3. Method

In this research-in-progress paper, we conceptualize a reputation system for the B2B context. Our idea is based on theoretical literature on trust. Implementing a risky advance mechanism in blockchain-secured transactions, which serve as an immutable, trusted, decentralized, and transparent ledger can help to build second-order trust represented as reputation.

Conceptual research is a non-empirical research method (Mora et al., 2008) for developing a theory based on reflecting on existing theoretical concepts. This paper's theoretical concepts comprise different types of trust and risk. Based on these concepts and core properties of blockchain technology, we conceptualize how a risky advance can be implemented in an IS to ease decision trust in B2B settings. Additionally, we implement control to safeguard the risky advance of a service provider.

The conceptual findings build the first steps of a more comprehensive design science research project (Peffers et al., 2008), in which we plan to build and evaluate a blockchain-based reputation system that instantiates the findings presented in this paper. For this endeavor, the theoretical concepts discussed here will be used as kernel theories to develop, implement, and evaluate an innovative IS artifact (Kuechler & Vaishnavi, 2008). We use our theoretical perspective on trust and known problems in related reputation systems to build design principles for implementing a software prototype. Other researchers can build on these design principles and integrate risk (and thus trust) in the rating process of sellers.

4. Conceptualizing Blockchain-Based B2B Reputation Systems

4.1 Requirements and Design Principles

Related literature summarizes six main problems related to current reputation systems (Bellini et al., 2020; Jøsang et al., 2007): (1) low incentive for evaluation, (2) positive and reciprocal evaluations, (3) too many ratings (ballot-stuffing), (4) change of identity (whitewashing), (5) unfair valuations, and (6) discrimination (bad-mouthing). Revising how trust as a construct works (observation, selection, and risk assignment in a systemic context) (Luhmann, 1995, 2017), we build on these problems to identify requirements and design principles (Gregor et al., 2020) to design a blockchain-based business reputation system (Table 1).

	Requirements	Design Principles
a)	Business relationships	A reputation system should represent the true socioeconomic relationship of the transacting parties.
b)	Economic commitment	A reputation system should give evidence of the economic commitment between the transacting parties.
c)	Information contextualization	A reputation system should provide non-cumulated information and allow contextual information to be filtered and selected.
d)	Performance differentiation	A reputation system should allow for portraying performance differentiation among service providers.
e)	Linkable services	A reputation system should allow linking different service objects.
f)	Selection of ratings	A reputation system should allow a buyer to select which ratings are forwarded.
g)	Open system	A reputation system should be open to new participants.
h)	Raters' fairness	A reputation system should allow responding to a rater's bad rating.
i)	Systemic fairness	A reputation system should support a system equilibrium of fair ratings.
j)	Peer-to-peer system	A reputation system should be based on a distributed system, avoiding a single powerful gatekeeper that can influence the ratings.

Table 1: Requirements and Design Principles for Business Reputation Systems.

4.2 Concept

We investigate reputation systems to establish trust based on transactions between business parties, while we do not consider reputation systems on the blockchain validation layer itself. We will now briefly explain how the idea works, in general, before building on the identified design principles. We propose establishing bonus payments between the transacting parties, enabling a service customer SC(x) to pay a part of the liabilities only if they are satisfied with the service delivered by a service provider SP. With this risky advance, we integrate risk in the transaction, since a SP risks a loss of profit by not receiving the bonus share; but also risks reputation, since the transaction can be visible to others. In this way, we consider what we learned about trust in theory, which is that trust and, thus reputation, can be created more effectively by exposing oneself to being vulnerable (Mayer et al., 1995). In doing so, SP also raises the trust expectation of a SC(x) to fulfill a service as promised, encouraging prospective customers' SC(p) decisions to do business with this SP. If not satisfied, a SC(x) can decide to pay only a basic payment (trans(y)) to the SP, but no bonus payment (trans(x)). If satisfied, the SC(x) might pay trans(x) to acknowledge proper service provision (Figure 2).

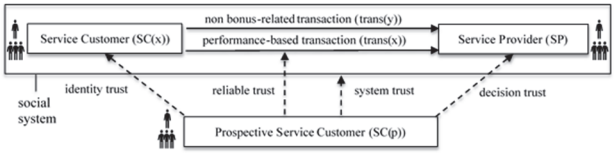

Figure 2: Trust in a performance-based reputation system.

The payment transactions are visible for other SC(p)s, who use the payment history of a SP as a basis to decide if they want to transact with this SP. The SC(p) will interpret the received trans(x) (in relation to trans(y)) as a rating of the SP's past performance. The SC(p) can compare a requested service with (similar) services rated. We can expect that the willingness of SC(p) to conduct business with SP would increase when the SP receives trans(x) from different SC(x) on a regular basis since this points to several satisfied SC(x). Vice versa, a SP can demonstrate receiving trans(x), gaining a trust advantage over

competing SPs that received fewer transactions or lower bonuses. The SP will unlikely make a risky advance and enter into a business with a SC(x) that pays bonuses infrequently or whom he does not trust. Therefore we will introduce a safeguard to indicate exploitive SC(x) (see h); i)). Observing the transaction history, a SP can assess the risk of not receiving a trans(x) from a SC(x), which prevents him from engaging with exploitive SC(x)s.

Based on the information provided by SC(x), a SC(p) can decide to engage with a SP. Therefore, a SC(p) needs to trust in the SC(x)'s identity (identity trust), in the immutability of the transaction (reliable trust), and that the SC(x) and SP do not conspire (system trust), before trusting a SP (decision trust). Identity trust can be achieved by verifying identities that are deemed trustworthy; reliable trust is obtained with an immutable ledger. System trust relies on establishing systemic mechanisms rooted in business parties' economic self-interest. We posit that our system needs to be built on the following design principles:

a) Business relationship: Each transaction is recorded on a blockchain, providing a full picture of reputation. The lack of an incentive to elicit ratings (Neumann & Gutt, 2019) is fixed by deriving reputation from every on-chain transaction. Only metadata is public, while transaction details are hidden.

b) Economic Commitment: The parties establish a smart contract that specifies the bonus payments and is made visible to others. This clear economic commitment is quantified with the payment value and the money at risk for a SP. The smart contract also enables the integration of a counter-rating mechanism for ratings perceived as unjustified, controlling who can give a counter-rating (see h)).

c) Information contextualization: Blockchain data can be filtered to identify services fitting a SC(p)'s purchase intent. The SC(p) selects relevant metadata according to a service description supplied in a smart contract and may apply additional evaluation metrics. Importantly, the selection choice of SC(p) includes that the raters' identity (SC(x)) is known or deemed trustworthy, based on verifiable ratings.

d) Performance differentiation: Services are described in a smart contract to indicate different value propositions. In particular, the trans(x) payment amount can be contracted on different levels, depending on how much risk a SP is willing to take for building a reputation.

e) Linkable services: A SP can create one or more seller identities, representing various service categories (Blömer et al., 2018; Zhai et al., 2016). Positive ratings of a service linked to an address/identity can promote customers' trust in the corresponding service provider's service.

f) Selection of ratings: A SC(x) is able to decide with whom to share ratings and not to disclose sensitive information to a competitor. This can be achieved with privacy-preserving techniques to hide the exact transaction amounts (Hemmrich et al., 2023). Equally, the SC(p) decides which rating to pick up to prevent being tricked by a fraudulent SC(x) or SP. Viewing a transparent transaction history, a SC(p) can learn over time which identities are trustworthy. After a sufficient information basis exists, SC(p) might place trust in specialized intermediaries to filter for honest addresses that fit his own assessment.

g) Open system: In a public blockchain network, parties can always join and leave the reputation system. Private spaces might be set up to exchange information about services conducted between SC(x) and SP to inform a SC(p). A SC(p) might pay the SC(x) for additional information to achieve an information advantage (e.g., for knowing SC(x)s true identity, and service details) to reduce the risk of engaging with a bad SP. A SC(x) can prove to have this information without revealing it.

h) Raters fairness: To overcome the problem that a SC(x) exploits the risky advance offered by SP, we propose a counter-rating mechanism. When a SC(x) does not pay a trans(x), the SP receives a one-time certificate to counter-rate the SC(x). This certificate allows a SP to rate to what extent the SP considered the omission of a trans(x) rating justified. For this counter-rating, a star-based rating might be used, revealing more information about the exchange relationship for another observing SP to decide whether to offer a risky advance for a particular SC(p).

i) Systemic fairness: Even if the quality of a service is good, an opportunistic SC(x) always has no interest in paying a trans(x). To establish fairness for counter-ratings, we propose a systems balance mechanism, making unpaid trans(x) visible depending on a threshold. Bad ratings get revealed if a SC(x) regularly decides not to pay trans(x). We suggest defining a threshold (e.g., 90%), at which counter-ratings become visible, as determined by the blockchain protocol rules shared in the network. This display incentives SC(x)s to pay trans(x) to at least 90% to SPs that offered a risky advance because else the exploitive behavior of a SC(x) becomes visible in the reputation system. Consequently, a SC(x) would try to stay below this threshold in order to continue doing business with SPs and being trusted. However, once revealed, every SP can view counter-ratings as revealing a SC(x) excessive exploiting behavior. Intuitively, SPs will pick SC(x)s, who can prove to pay trans(x) regularly to other SPs. This serves as a safeguard for SPs' risky advance, building trust (Luhmann, 2017). Avoidance of a SC(x) to pay too much (unobservable down to the threshold) and selective SP probably lead to a fair system equilibrium, filtering bad actors. Lastly, the threshold should correspond to the quality distribution in a market, at which counter-ratings would be visible to separate high-quality SPs from bad-quality SPs.

j) Peer-to-peer system: Blockchain technology builds on a distributed network that replaces the need for an

intermediary, alleviating problems like data breaches, censorship, fraud, or high commission fees.

5. Discussion and Conclusion

We proposed an incentive scheme for reputation systems based on a risky advance of a service provider to his customer, thereby, using safeguards built on a blockchain to establish decision trust. We expect that this system can provide high-quality SPs with a competitive advantage over weaker-performing competitors, promoting good service quality. Compared with existing rival systems, our approach exhibits five main differences. First, ratings become an inherent part of business transactions, whereas current systems disconnect transactions from ratings. Second, ratings are carried out with payments, making the ratings quantifiable. Third, implementing the system with blockchain facilitates reliable trust, since ratings are immutable, transparent, trustworthy secure. Fourth, we propose a performance differentiation threshold to set incentives and sanction mechanisms aiming to establish a systemic equilibrium. Fifth, services can be rated quicker than writing a review, and service ratings can be differentiated regarding different services.

Blockchain technology can help to make these new reputation mechanisms feasible, paving the way for a new system class of reputation systems. Blockchain-based reputation systems provide control mechanisms to select and verify information service customers and service providers provide. Modifying ratings and strategic lying about ratings, e.g., when selling rating information, is impossible, presupposing a reliable blockchain network. Selecting trustworthy ratings is essential, but might be challenging initially, reflecting a cold-start problem. However, we assume that a marketplace for trading information about the trustworthiness of ratings will form since rating information has an economic value.

We acknowledge that this system might also be applied without blockchain technology. However, we posit that blockchain technology makes particular sense here because rating information is sensitive data, and centralized instances are always exposed to the risk of being compromised, among other disadvantages (Locher et al., 2018; Subramanian, 2018). However, please note that with this technology comes a limitation regarding conflict resolution. Some conflicts are hard to solve since data is stored immutably on the blockchain. However, we assume that a seller who allows himself to be rated accepts this and has a positive relationship with a rating service customer, expecting positive ratings.

Limiting attacks would also be important, and possible attack scenarios should be comprehensively researched to find eventual weak spots in the incentive scheme. Sending trust signals in the form of a risky advance, which is safeguarded through making bad behavior visible, can probably make a positive outcome for both, the service provider and the service customer, more likely. This is because customers want to get or stay in the position of getting trust signals (through the risky advance), while a service provider can expect positive ratings. However, a customer is able to give bad ratings, but, viewed from an overall system perspective, would do it as a rational actor (to stay in the system) only to a limited degree. If he decides otherwise, probably no seller would want to interact with him anymore. Parameters for disclosing bad rating customers need to be adjusted accordingly to the quality distribution in the market.

We assume that agency costs (e.g., monitoring a service provider's actions, searching for trustworthy service providers, and committing to trustworthy service customers) can be reduced with this system. We build this concept primarily for one-time business deals, making it more attractive to switch business partners. However, this concept might be adjusted to repeated business transactions extending its usefulness.

The multilateral design of incentives provided with this reputation system might result in a system equilibrium. Indeed, we see it as a potential solution to the famous lemon market problem (Akerlof, 1970). Developing such systems might be helpful to counteract adverse selection in business markets. A blockchain can help secure reputation systems, preventing business parties from compromising them. Thus, our blockchain-based system might level information asymmetries by establishing trust and reputation on a systems level promoting good service quality. Whether a system equilibrium is realized with our system needs to be explored in more profound settings, like game theory or lab experiments. This would contribute to complementing the design and evaluation of the proposed system.

6 References

[1] Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. The Quarterly Journal of Economics, 84(3), 488–500. https://doi.org/10.2307/1879431

[2] Arrow, K. J. (1974). The Limits of Organization. The Fels Lectures on Public Policy Analysis. Norton.

[3] Ba, S., & Pavlou, P. A. (2002). Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior. MIS Quarterly, 26(3), 243–268. https://doi.org/10.2307/4132332

[4] Bag, S., Azad, M. A., & Hao, F. (2018). A Privacy-Aware Decentralized and Personalized Reputation System. Computers & Security, 77, 514–530. https://doi.org/10.1016/j.cose.2018.05.005

[5] Bazin, R., Schaub, A., Hasan, O., & Brunie, L. (2017). Self-Reported Verifiable Reputation with Rater Privacy. In Proceedings of the 11th IFIP International Conference on Trust Management (IFIPTM), Gothenburg.

[6] Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain Technology in Business and Information Systems Research. Business & Information Systems Engineering, 59(6), 381–384. https://doi.org/10.1007/s12599-017-0505-1

[7] Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). Blockchain - The Gateway to Trust-Free Cryptographic Transactions. In Proceedings of the 24th European Conference on Information Systems (ECIS), Istanbul.
[8] Bellini, E., Iraqi, Y., & Damiani, E. (2020). Blockchain-Based Distributed Trust and Reputation Management Systems: A Survey. IEEE Access, 8, 21127–21151. https://doi.org/10.1109/ACCESS.2020.2969820
[9] Blömer, J., Eidens, F., & Juhnke, J. (2018). Practical, Anonymous, and Publicly Linkable Universally-Composable Reputation Systems. In Cryptographers' Track at the RSA Conference 2018, San Francisco.
[10] Bromley, D. B. (2001). Relationships Between Personal and Corporate Reputation. European Journal of Marketing, 36(3/4), 316–334.
[11] Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/en/whitepaper/
[12] Cai, Y., & Zhu, D. (2016). Fraud Detections for Online Businesses: A Perspective from Blockchain Technology. Financial Innovation, 2(1), 1–10. https://doi.org/10.1186/s40854-016-0039-4
[13] Catalini, C., & Gans, J. S. (2016). Some Simple Economics of the Blockchain (Working Paper 22952). National Bureau of Economic Research. http://www.nber.org/papers/w22952 https://doi.org/10.3386/w22952
[14] Chetty, R., Hofmeyr, A., Kincaid, H., & Monroe, B. (2021). The Trust Game Does Not (Only) Measure Trust: The Risk-Trust Confound Revisited. Journal of Behavioral and Experimental Economics, 90, 101520. https://doi.org/10.1016/j.socec.2020.101520
[15] Dasgupta, P. (1988). Trust as a Commodity. In D. Gambetta (Ed.), Trust: Making and Breaking Cooperative Relations (pp. 49–72). Blackwell.
[16] Deutsch, M. (1958). Trust and Suspicion. Journal of Conflict Resolution, 2(4), 265–279.
[17] Dikow, H., Hasan, O., Kosch, H., Brunie, L., & Sornin, R. (2015). Improving the Accuracy of Business-to-Business (B2B) Reputation Systems through Rater Expertise Prediction. Computing, 97(1), 29–49. https://doi.org/10.1007/s00607-013-0345-x
[18] Filippi, P. de (2016). The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies. Journal of Peer Production(7).
[19] Gambetta, D. (1988). Can We Trust Trust? In D. Gambetta (Ed.), Trust: Making and Breaking Cooperative Relations (pp. 213–237). Blackwell.
[20] Greenspan, G. (2016). Why Many Smart Contract Use Cases Are Simply Impossible. https://www.coindesk.com/three-smart-contract-misconceptions
[21] Gregor, S., Kruse, L. C., & Seidel, S. (2020). Research Perspectives: The Anatomy of a Design Principle. Journal of the Association for Information Systems, 21(6), 1622–1652. https://doi.org/10.17705/1jais.00649
[22] Gutt, D., Neumann, J., Zimmermann, S., Kundisch, D., & Chen, J. (2019). Design of Review Systems – A Strategic Instrument to Shape Online Reviewing Behavior and Economic Outcomes. The Journal of Strategic Information Systems, 28(2), 104–117. https://doi.org/10.1016/j.jsis.2019.01.004
[23] Hemmrich, S., Bobolz, J., Beverungen, D., & Blömer, J. (2023). Designing Business Reputation Ecosystems—A Method for Issuing and Trading Monetary Ratings on a Blockchain. In Proceedings of the 31st European Conference on Information Systems (ECIS), Kristiansand.
[24] Jøsang, A. (2016). Subjective Logic: A Formalism for Reasoning Under Uncertainty. Springer. https://doi.org/10.1007/978-3-319-42337-1
[25] Jøsang, A., Ismail, R., & Boyd, C. (2007). A Survey of Trust and Reputation Systems for Online Service Provision. Decision Support Systems, 43(2), 618–644. https://doi.org/10.1016/j.dss.2005.05.019n
[26] Kee, H. W., & Knox, R. E. (1970). Conceptual and Methodological Considerations in the Study of Trust and Suspicion. Journal of Conflict Resolution, 14(3), 357–366. https://doi.org/10.1177/002200277001400307
[27] Kim, J. W. (2020). Blockchain Technology and Its Applications: Case Studies. Journal of System and Management Sciences, 10(1), 83–93. https://doi.org/10.33168/JSMS.2020.0106
[28] Kuechler, B., & Vaishnavi, V. (2008). On Theory Development in Design Science Research: Anatomy of a Research Project. European Journal of Information Systems, 17(5), 489–504. https://doi.org/10.1057/ejis.2008.40
[29] Li, F., Pieńkowski, D., van Moorsel, A., & Smith, C. (2012). A Holistic Framework for Trust in Online Transactions. International Journal of Management Reviews, 14(1), 85–103. https://doi.org/10.1111/j.1468-2370.2011.00311.x
[30] Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do We Trust New Technology? A Study of Initial Trust Formation with Organizational Information Systems. The Journal of Strategic Information Systems, 17(1), 39–71. https://doi.org/10.1016/j.jsis.2008.01.001
[31] Litos, O. S. T., & Zindros, D. (2017). Trust is Risk: A Decentralized Financial Trust Platform. In 21st International Conference on Financial Cryptography and Data Security (FC 2017), Sliema.
[32] Locher, T., Obermeier, S., & Pignolet, Y. A. (2018). When can a Distributed Ledger Replace a Trusted Third Party? 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) (pp. 1069–1077). IEEE.
[33] Luhmann, N. (1995). Social Systems. Stanford Universitiy.
[34] Luhmann, N. (2017). Trust and Power (C. Morgner & M. King, Trans.). Polity.
[35] Mayer, R., Davis, J., & Schoorman, D. (1995). An Integrative Model of Organizational Trust. The Academy of Management Review, 20(3), 709–734. https://doi.org/10.2307/258792
[36] Möhlmann, M., Teubner, T., & Graul, A. (2019). Leveraging Trust on Sharing Economy Platforms: Reputation Systems, Blockchain Technology and Cryptocurrencies. In R. Belk, G. M. Eckhardt, & F. Bardhi (Eds.), Handbook of the Sharing Economy (pp. 290–302). Elgar.
[37] Mora, M., Gelman, O., Paradice, D., & Cervantes, F. (2008). The Case for Conceptual Research in Information Systems. In Proceedings of the International Conference on Information Resources Management (CON-FIRM).

[38] Moreno, A., & Terwiesch, C. (2014). Doing Business with Strangers: Reputation in Online Service Marketplaces. Information Systems Research, 25(4), 865–886. https://doi.org/10.1287/isre.2014.0549
[39] Murray, A., Kuban, S., Josefy, M., & Anderson, J. (2019). Contracting in the Smart Era: The Implications of Blockchain and Decentralized Autonomous Organizations for Contracting and Corporate Governance. Academy of Management Perspectives. Advance online publication. https://doi.org/10.5465/amp.2018.0066
[40] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
[41] Neumann, J., & Gutt, D. (2019). Money Makes the Reviewer Go Round–Ambivalent Effects of Online Review Elicitation in B2B Markets. In 25th Americas Conference on Information Systems (AMCIS), Cancun.
[42] Ostern, N. (2018). Do You Trust a Trust-Free Transaction? Toward a Trust Framework Model for Blockchain Technology. In Proceedings of the International Conference on Information Systems (ICIS), San Francisco.
[43] Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2008). A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems, 24(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302
[44] Pennington, R., Wilcox, H. D., & Grover, V. (2003). The Role of System Trust in Business-To-Consumer Transactions. Journal of Management Information Systems, 20(3), 197–226.
[45] Pereira, J., Tavalaei, M. M., & Ozalp, H. (2019). Blockchain-Based Platforms: Decentralized Infrastructures and its Boundary Conditions. Technological Forecasting & Social Change, 146, 94–102. https://doi.org/10.1016/j.techfore.2019.04.030
[46] Resnick, P., Kuwabara, K., Zeckhauser, R., & Friedman, E. (2000). Reputation Systems. Communications of the ACM, 43(12), 45–48.
[47] Resnick, P., & Zeckhauser, R. (2002). Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System. In M. R. Baye (Ed.), The Economics of the Internet and E-Commerce (11th ed., pp. 127–157). JAI.
[48] Risius, M., & Spohrer, K. (2017). A Blockchain Research Framework: What We (don't) Know, Where We Go from Here, and How We Will Get There. Business & Information Systems Engineering, 59(6), 385–409. https://doi.org/10.1007/s12599-017-0506-0
[49] Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An Integrative Model of Organizational Trust: Past, Present, and Future. The Academy of Management Review, 32(2), 344–354.
[50] Seidel, M. D. L. (2018). Questioning Centralized Organizations in a Time of Distributed Trust. Journal of Management Inquiry, 27(1), 40–44. https://doi.org/10.1177/1056492617734942
[51] Shapiro, S. P. (1987). The Social Control of Impersonal Trust. American Journal of Sociology, 93(3), 623–658. https://doi.org/10.1016/j.ijinfomgt.2017.12.008
[52] Siegrist, M. (2021). Trust and Risk Perception: A Critical Review of the Literature. Risk Analysis, 41(3), 480–490. https://doi.org/10.1111/risa.13325
[53] Simser, J. (2015). Bitcoin and Modern Alchemy: In Code We Trust. Journal of Financial Crime, 22(2), 156–169. https://doi.org/10.1108/JFC-11-2013-0067
[54] Subramanian, H. (2018). Decentralized Blockchain-Based Electronic Marketplaces. Communications of the ACM, 61(1), 78–84. https://doi.org/10.1145/3158333
[55] Sullivan, Y. W., & Kim, D. J. (2018). Assessing the Effects of Consumers' Product Evaluations and Trust on Repurchase Intention in E-Commerce Environments. International Journal of Information Management, 39, 199–219. https://doi.org/10.1016/j.ijinfomgt.2017.12.008
[56] Sun, H. (2010). Sellers' Trust and Continued Use of Online Marketplaces. Journal of the Association for Information Systems, 11(4), 182–211.
[57] Thierer, A., Koopman, C., Hobson, A., & Kuiper, C. (2016). How the Internet, the Sharing Economy, and Reputational Feedback Mechanisms Solve the Lemons Problem. U. Miami L. Rev., 70(3), 830–878.
[58] Voshmgir, S., & Zargham, M. (2020). Foundations of Cryptoeconomic Systems (Working Paper Series) [, WU Vienna University, Vienna]. RIS.
[59] Williamson, O. E. (1993). Calculativeness, Trust, and Economic Organization. The Journal of Law and Economics, 36(1), 453–486. https://doi.org/10.1086/467284
[60] Zhai, E., Wolinsky, D. I., Chen, R., Syta, E., Teng, C., & Ford, B. (2016). Anonrep: Towards Tracking-Resistant Anonymous Reputation. In 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI) (pp. 583–596). USENIX.

Chainlock - Blockchain-gestützte, smarte Schließanlagen

Robert Manthey, Richard Vogel, Matthias Vodel
Hochschule Mittweida, Fakultät für Computer- & Biowissenschaften, Mittweida, Deutschland

Abstract
Controlling access authorizations for laboratories, buildings or sites is essential for many companies and facilities, but with increasing size it also involves considerable effort and greater costs. Checking and updating authorizations also requires extensive logistics and confidence in the correct operation of central management facilities.
The combination of electronic locking system with decentralized blockchain technology presented here makes it possible to both simplify and decentralize authorization management and avoid singular points of failure. At the same time, offline capability of the locks can also be realized without major effort.

Kurzfassung
Die Kontrolle von Zutrittsberechtigungen für Labore, Gebäude oder Standorte ist für viele Firmen und Einrichtungen von essenzieller Bedeutung, mit zunehmender Größe aber auch mit erheblichem Aufwand und größeren Kosten verbunden. Die Überprüfung und Aktualisierung der Berechtigungen erfordert außerdem eine umfangreiche Logistik und Vertrauen in die korrekte Arbeitsweise der zentralen Verwaltungseinrichtungen.
Durch die hier vorgestellte Kombination von elektronischem Schließsystem mit dezentraler Blockchaintechnologie ist sowohl eine Vereinfachung und Dezentralisierung der Berechtigungsverwaltung als auch die Vermeidung singuläre Fehlerstellen möglich. Gleichzeitig kann ohne größere Aufwende auch eine Offlinefähigkeit der Schlösser realisiert werden.

---

1. Einleitung

Universitäten oder Bürogebäude besitzen meist unterschiedlichste Zugangsberechtigungen für verschiedene Bereiche, wie den Zutritt eines Mitarbeiters zu mehreren Büros an Arbeitstagen, für Reinigungskräfte zu allen Büros von 18-21 Uhr oder Wartungstechnikern am 3. jedes Monats, ähnlich Abbildung 1. Deren Management erfolgt durch den Einsatz von Schlüsseln mit spezifischen mechanischen Konfigurationen je Berechtigungsgruppe, ähnlich Abbildung 2. Somit führen Berechtigungsänderungen und der damit verbundene physischen Austausch der Schlüssel zu beträchtlichem Aufwand und Kosten sowie im Fall von Schlüsselverlusten zum Ersatz der betroffenen Schlösser mit noch beträchtlich größeren Aufwendungen.

Abbildung 1: Komplexes Beispiel mit unterschiedlichsten Schließberechtigungen für Türen und Fenster der einzelnen Gebäude, sowie zeitlicher Einschränkungen.

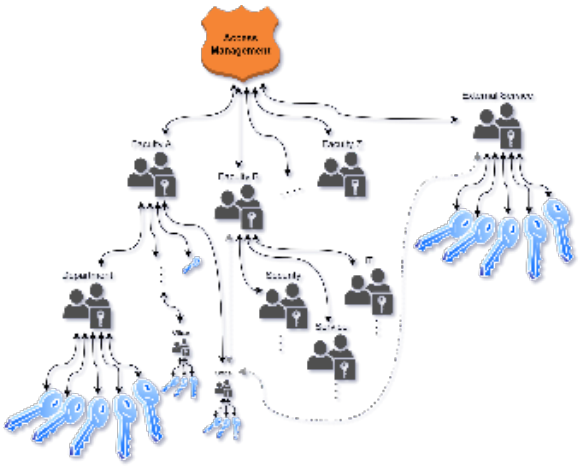

Abbildung 2: Komplexe Hierarchie der Verwaltung von Schlüsseln in größeren Einrichtungen mit Abteilungen und Fakultäten, einzelnen Generalschlüsseln sowie mit sich überschneidenden Berechtigungsbereichen.

Bei elektronische Schließsysteme reduzieren sich dieser zwar aufgrund der dynamischeren Berechtigungskonfiguration, sie erfordern aber meist eine bestehende Datenverbindung zwischen dem Schloss und dem Management. Dies bringt initial bauliche Anpassungen und größere Anschaffungskosten mit sich sowie ein dauerhaftes Vertrauen in eine zentrale Instanz.

Durch den Einsatz der Blockchaintechnologie und ihrer dezentralen Informationsverteilung können diese Nachteile erheblich reduziert und die Verwaltung der Zugangsberechtigungen deutlich vereinfacht werden.

Die vorgestellte Lösung nutzt verschiedene, miteinander interagierende Blockchains welche die Aktualität der Berechtigungsdaten gewährleisten sowie die Berechtigungen der einzelnen Schlösser repräsentieren. Während des Schließvorgangs werden sowohl alle relevanten Blöcke als auch Informationen, durch welche deren Aktualität verifizierbar ist an das Schloss übermittelt. Der aktuelle Berechtigungsstand ergibt sich anschließend aus der Übersetzung dieser Blockdaten und der Aktualisierung des internen Zustands des Schlosses. Nach der Verifikation der Nutzeridentität erfolgt gegebenenfalls die Durchführung der Schließaktion.

Die Repräsentation der Berechtigungen erfolgt in Form von Einträgen in einzelnen Transaktionen in der zugehörigen Mikroblockchain und die Reihenfolge innerhalb der Mikroblockchain. Das dezentrale Berechtigungsmanagement und der Konsens verhindert die Manipulation von Berechtigungen, den Ausfall des Systems sowie die Unabhängigkeit vom Schließanlagenhersteller.

2. Grundlagen

Für die Verwaltung von Zutrittsberechtigungen und Schließsystemen werden Lösungen von mehreren kommerziellen Anbietern bereitgestellt, wobei etablierte klassische Schließsysteme auf dem berechtigten Besitz eines physischen Schlüssels, wie z.B. die von Konntec[1] basieren. Diese bieten für einzelne Schließeinheiten zwar einerseits den Vorteil geringer Kosten von nur ca. 60 €, aber andererseits die Nachteile der erheblichen Einschränkungen in Bezug auf Flexibilität bei Veränderung der Zutrittsberechtigungen. Im Fall des Entzugs von Berechtigungen können zusätzlich noch weitere beträchtliche Kosten für den Austausches mehrere Einheiten entstehen[2].

Bei elektronische Schließsysteme wie CES OMEGA FLEX von CES[3], blueSmart von WINKHAUS[4] oder Clex prime von UHLMANN & ZACHER[5] sind die laufenden Kosten zwar geringer und die Berechtigungssteuerung flexibler, die einzelnen Einheiten aber deutlich kostenintensiver. Darüber hinaus setzt die Aktualisierung der Berechtigungen entweder eine permanente Datenverbindung oder Programmierungsaktionen durch autorisiertes Personal mit entsprechendem Zeitverzug voraus.

Systeme wie Lokkit[6] nutzen zwar bereits Blockchaintechnologie, beschränken sich aber auf Prototypimplementierungen. Darüber erfolgt die Verarbeitung auf dem Smartphone des Nutzers, dem wiederum vertraut werden muss.

Diese Schließsysteme weisen die Problematik der zentralen Speicherung und Verwaltung der Zutrittsberechtigungen und des damit einhergehenden Vertrauens in den Hersteller bzw. Verwalter auf. Eine unabhängige Prüfung der Schließtechnik, der Zutrittsberechtigungen und der Berechtigungshistorie ist durch Dritte nur mit beträchtlichem Aufwand durchführbar.

Die grundlegende Technologie der Blockchain wurde von [4] als Basis für digitale Währungen wie Bitcoin. Hierbei werden Angaben zum Betrag um Informationen zu Absender und Empfänger ergänzt und zu einer Transaktion kombiniert. Deren anschließende Verteilung an verschiedene, zufällig ausgewählte Knoten dieses Blockchainnetzwerks erschwert die Möglichkeiten zur unberechtigten Veränderung durch Dritte. Diese Knoten kombinieren verschiedene Transaktionen sowie Informationen zum Vorgänger zu einem neuen Block, welcher als Kandidat für den neuen Kopf der Blockchain dem Consensus-Verfahren präsentiert wird, wodurch eine fortlaufende Kette verbundener Blöcke entsteht, Abbildung 3, deren nachträgliche Veränderung nicht unbemerkt durchführbar ist. [2]

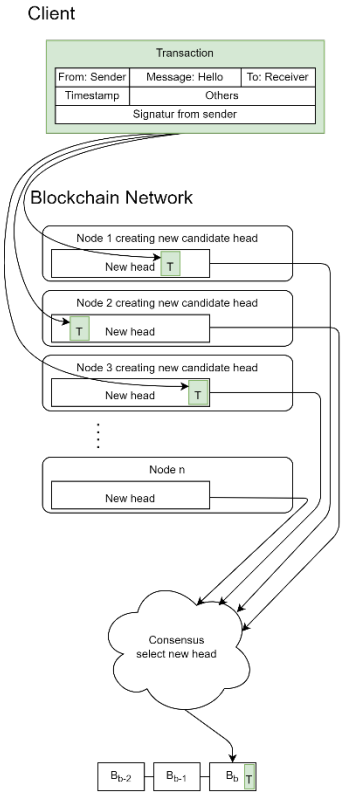

Abbildung 3: Prinzipieller Ablauf der Blockchain mit Transaktionserstellung, Blockbildung, Kandidatenauswahl und Anhängen eines neuen Kopfblocks. [7]

[1] https://www.konntec.de/geschaeftlich/produkte/mechanische-schliessanlage

[2] https://kiwi.ki/schliessanlage/kosten

[3] https://www.ces.eu/de_us/produkte/elektronische-schliesssysteme/ces-omega-flex/elektronikzylinder.html

[4] https://www.winkhaus.com/de-de/zutrittsorganisation/elektronische-zutrittsorganisation/elektronische-schliesssysteme/bluesmart

[5] https://uundz.com/systeme/clex-prime

[6] https://news.hslu.ch/siemens-zeichnet-projekt-von-informatik-absolventen-aus/

Einige Blockchainimplementierungen wie Hyperledger Fabric [1] realisieren weitere Funktionen wie Smart Contracts oder bedingte Transaktionsausführungen, wodurch die Verwaltung von Zugangsberechtigungen oder auch eine verteilte Identitätsverifikation ermöglicht werden. [3, 5, 6]

3. Design

Für die Verwaltung der Zugangsberechtigungen erfolgt eine Aufteilung der unterschiedlichen Teilbereiche, Abbildung 4. Die eigentlichen Regeln eines Schlosses lehnen sich an das Format von RFC 6321 (xCal) an und werden in Transaktionen einer dafür zuständigen internen Mikroblockchain gespeichert. Die Informationen bezüglich des aktuellen Kopfes jeder Microblockchain finden sich als Transaktionsdaten in einem Block einer öffentlich zugänglichen Blockchain. Hierdurch kann einerseits die Aktualität der aktuellen Zugangsberechtigungen sichergestellt und andererseits die teure Speicherung größerer Datenmengen in öffentlichen Blockchains vermieden werden.

Ein Nutzer lädt mit der auf seinem Smartphone vorhandenen App eine Kopie der Blockchains und lässt seine Identität durch eine qualifizierte Stelle digital bestätigen, sobald dieser Kontakt zum entsprechenden Netzwerk aufbauen kann.

Sobald ein Schließvorgang durchgeführt werden soll baut das Smartphone eine Verbindung zum Schloss mittels Bluetooth auf. Hierdurch erhält dieses die Informationen über den aktuellen Stand der Microblockchain des Schlosses und die Anforderung alle Blöcke der Mikroblockchain, welche seit dessen letzten Aktivität angehängt wurden, sowie die zur Identitätsprüfung notwendigen Informationen. Zu diesem Zeitpunkt ist nur eine Kommunikation zwischen Schloss und Smartphone notwendig, wodurch die Offlinefähigkeit des Schließsystems gewährleistet ist.

Das Schloss prüft die Korrektheit und Aktualität der Blöcke und erneuert damit den aktuelle Berechtigungsstand. Nach der anschließenden Verifikation der Nutzeridentität erfolgt die Durchführung der Schließaktion bei entsprechender Berechtigung des Nutzers.

4. Zusammenfassung und Ausblick

Der vorgestellte Ablauf der Verwaltung von Zugangsberechtigungen für Schließanlagen kombiniert die technischen Möglichkeiten elektronischer Schließanlagen mit den dezentralen Eigenschaften der Blockchaintechnologie und der Datenspeicher und -verteilfähigkeit moderner Smartphones um ein dezentrales, offlinefähiges Schließsystem zu erstellen. Die dabei vorgenommene Zwischenspeicherung von Daten kann ohne weitere Sicherung erfolgen, da Veränderungen durch die inhärenten Eigenschaften der Blockchain sofort bemerkt werden. Gleichzeitig ist eine Prüfung der Korrektheit bzw. Aktualität der Regeln der Zugangsberechtigung jederzeit von Dritten durchführbar und nachvollziehbar.

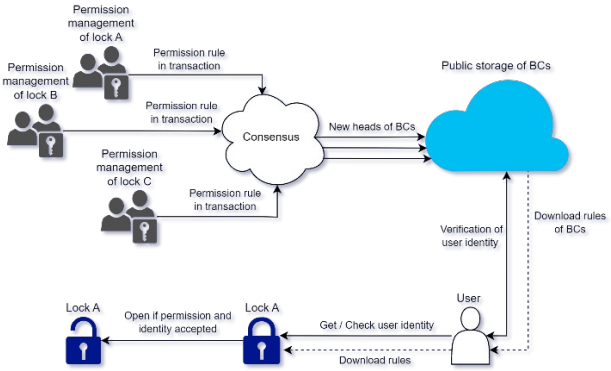

Abbildung 4: Vorgesehener Ablauf, der die verteilte Verwaltung von Berechtigungen, den verteilten öffentlichen Speicher von Blockchains (BCs) mit periodischem Download von Regeln durch einen Benutzer und periodische Überprüfung der Benutzeridentität darstellt. Das Herunterladen der Regeln auf das Schloss, wie die Überprüfung der Identität des Nutzers erfolgt, sobald dieser in Reichweite ist und eine Aktion des Schlosses anfordert. Dieses wertet die Berechtigungen aus, prüft die Identität des Nutzers und führt die gewünschte Aktion gegebenenfalls aus.

Danksagung

Diese Arbeit wurde teilweise im Rahmen des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekts *Chainlock - Blockchain-gestützte, smarte Schließanlagen* (Projektnr. 8233216) durchgeführt.

Kontaktdaten

Robert.Manthey@hs-mittweida.de
Richard.Vogel@hs-mittweida.da
Matthias.Vodel@hs-mittweida.de

Literaturverzeichnis

[1] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed Cocco, and Jason Yellick. 2018. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the Thirteenth EuroSys Conference (Porto, Portugal, 2018-01-30) (EuroSys '18). Association for Computing Machinery, New York, NY, USA, Article 30, 15 pages. https://doi.org/10.1145/3190508.3190538

[2] Christian Cachin and Marko Vukolić. 2017. Blockchain Consensus Protocols in the Wild. arXiv:1707.01873 [cs.DC] https://arxiv.org/abs/1707.01873
[3] Md Sadek Ferdous, Farida Chowdhury, and Madini O. Alassafi. 2019. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. IEEE Access 7 (2019), 103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173
[4] Satoshi Nakamoto. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. (03 2009), 9 pages. https://bitcoin.org/bitcoin.pdf
[5] Drummond Reed, Manu Sporny, Dave Longley, Christopher Allen, Ryan Grant, and Markus Sabadello. 2021. Decentralized Identifiers (DIDs) v1.0. W3C. https://www.w3.org/TR/2021/CRD-did-core-20210529/
[6] N. Szabo. 1994. Smart Contracts. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOT-winterschool2006/szabo.best.vwh.net/smart.contracts.html
[7] R.Manthey, R.Vogel, M.Baumgart, C.Roschke, M.Ritter, M.Vodel. 2023. Decentralized Resilient Smart Lock System with Ofline Capabilities – ChainLock. In Proceedings of the 16th International Conference on Pervasive Technologies Related to Assistive Environments (PETRA) 5-7 July 2023, Corfu Island, Greece

Decentralizing Scholarly Publishing: An Innovative Blockchain Approach in Sea of Wisdom

Evgenii Alekseevich, Saurov[1], Daniil Andreevich, Gorokhov[2]
[1)] University of Applied Sciences, Mittweida, Germany
[2)]Hanze University of Applied Sciences, Netherlands
* Both authors contributed equally to this work.

Abstract:
In the swiftly changing world of academic publishing, the Sea of Wisdom platform seizes the opportunity to innovate. By combining the technologies of blockchain, decentralized finance (DeFi), and Non-Fungible Tokens (NFTs) with traditional scholarly communication, we present a groundbreaking, decentralized solution. Our design, although adaptable, primarily uses Ethereum's Virtual Machine, tapping into its robust scientific community.

In der sich schnell verändernden Welt des akademischen Publizierens ergreift die Sea of Wisdom-Plattform die Chance zur Innovation. Durch die Kombination der Technologien von Blockchain, dezentraler Finanzierung (DeFi) und Non-Fungible Tokens (NFTs) mit traditioneller wissenschaftlicher Kommunikation präsentieren wir eine bahnbrechende, dezentrale Lösung. Unser Design ist zwar anpassungsfähig, nutzt aber in erster Linie die Virtual Machine von Ethereum, um die robuste wissenschaftliche Community zu nutzen.

1. Introduction

The rapid digitization of many sectors has exerted a profound pressure on organizations to keep pace with the evolving technological landscape and consumer digital demands. The scholarly publishing industry, which is integral to the diffusion of knowledge and scientific advancement, is no exception. The long-standing traditional model of publishing scholarly works has come under scrutiny, given the issues of opacity, delays in the review and publication process, and an often unfair remuneration model for authors and reviewers [1].

Simultaneously, as the scholarly publishing landscape is being critically assessed, we are witnessing the rise of promising technologies that offer transformative potential. One such technology is blockchain, which has been identified as a potent catalyst for sweeping societal and economic change [2]. From its inception in 2008, the disruptive capabilities of blockchain have been postulated to profoundly alter various business models and value chains across myriad sectors, from Fintech [3] to healthcare [4], music industry [5] and, as we propose in this paper, scholarly publishing [6].

In this study, we explore the challenges and opportunities that blockchain technology presents within the realm of scholarly publishing. The current discourse on the application of blockchain in this field is dichotomized between ardent optimists and cautious pessimists. Consequently, our goal is to offer a balanced and well-informed perspective on the value creation potentials of blockchain within this industry. Thus, the guiding research question we seek to address is:

RQ: How can the scholarly publishing industry create value with blockchain technology?

In answering the research question, we adopt a dual-strategy approach: creating an economic incentive structure for each participant and demonstrating an MVP of a decentralized publishing platform. The economic model caters to all stakeholders, ensuring fairness and promoting engagement. The MVP, embodied in the Sea of Wisdom platform, operationalizes the process, underlining blockchain's potential to reform scholarly publishing with enhanced transparency, immutability, and efficiency.

2. Previous Work

The scholarly work of Niya et al. (2019) illuminates the transformative potential of blockchain technology in academic publishing, however, the direct translation of these insights into a real-world application remains unexplored [6]. Similarly, Stojmenova Duh et al. (2019) provide a compelling discourse around cryptoeconomic incentives fostering cooperation among researchers, yet the practical implementation of this concept demands further elucidation [7]. Kosmarski (2020), while successfully outlining a number of challenges to blockchain adoption in academia, doesn't sufficiently focus on practical solutions to surmount these obstacles [8].

Our research and proposed platform organically grow from this solid groundwork laid by the aforementioned studies. We aim to address the identified shortcomings by not only advocating the theoretical application of blockchain technology in academic publishing but also operationalizing this theory via the creation of a Minimum Viable Product (MVP). We build upon the cooperative incentive structures proposed by Stojmenova Duh et al. (2019) and endeavor to demonstrate their functionality in a tangible context. Additionally, we respond to the challenges delineated by Kosmarski (2020) with practical solutions, illustrated through our platform. In this way, our

work contributes to existing literature by bridging the gap between theoretical potential and tangible execution in the application of blockchain technology to academic publishing.

The aspirational undertakings of numerous blockchain startups in academia, such as scienceroot.com [9], eurekatoken.io [10], DEIP [11], and orvium.io [12], further underline the aforementioned gap between theoretical postulations and practical implementation. Driven by the promise of creating a platform that transcends conventional repositories, these startups ambitiously sought to foster reputational and incentives systems, and introduce novel mechanisms for research management and collaboration.

Regrettably, the majority of these initiatives succumbed to the realities of execution, failing to progress beyond their aspirational conceptual stage to a functional Minimum Viable Product (MVP). This frequent failure to translate vision into viable execution – with Orvium standing as a notable exception – illustrates the need for a pragmatic, step-by-step approach to harnessing blockchain technology in the service of academic publishing [9, 10]. The contrast between the promise of transformative potential and the harsh reality of failed implementation underscores the necessity of our research and the platform we propose, which is designed to bridge this very gap.

3. Formulation of the Issue and Suggested Resolution

The pivotal element within our platform is a scholarly work - a manuscript or scientific paper proffered by the academic author. Traditional academic journals typically offer no financial incentive for authors to publish their research, with some even imposing charges for publication [13]. However, within the infrastructure of our platform, we shift this paradigm by recognizing each scholarly paper as an invaluable asset that provides an avenue for authors to accrue potential rewards.

Indeed, this conceptualization of an academic work as a distinct, ownership-verified asset corresponds seamlessly with the functionalities offered by Non-Fungible Tokens (NFTs). NFTs, unique cryptographic entities existing on a blockchain, can effectively provide indisputable proof of ownership. By wrapping each scholarly paper as an NFT, we foster a secure environment where authorship is cryptographically verified and protected. This system engenders not only an unprecedented level of transparency but also potential avenues for academic authors to realize the inherent value of their intellectual contributions.

We can postulate the work-as-an-asset idea in mathematical notations:

$$W = Work; \quad (1)$$

$$R = Review; \quad (2)$$

$$P = Platform; \quad (3)$$

We propose that the value V of the final product (scholarly paper) purchased by a reader is an additive function of W, R and P.

Mathematically, this relationship can be expressed as:

$$V = f(W) + g(R) + q(P) \quad (4)$$

where:
$f(W)$ - value contributed by the work itself (e.g., originality, depth of research, importance of findings)

$g(R)$ - value added by the thorough review process (ensuring quality, correctness, and relevancy)

$q(P)$ - value provided by the platform (allowing for efficient distribution, communication between parties, and secure transactions)

This formulation indicates that a scholarly paper gains value not just from the inherent quality of the work itself, but also from the rigorous review process and the supportive platform that enables dissemination and dialogue around the work. As such, this model captures the comprehensive value proposition of purchasing and engaging with a scholarly paper on the SeaOfWisdom platform.

A. Monetary Incentivization and its Execution within the SeaOfWisdom Platform

- Author

Monetary incentives play an essential role within the SeaOfWisdom platform, serving to encourage authors, reviewers, and readers' active participation. Our platform revolutionizes the traditional academic publishing ecosystem by leveraging blockchain technologies to provide tangible rewards for all users involved in the publishing process.

Implementing this economically motivated construct within SeaOfWisdom is facilitated via the employment of an ERC-20 compliant token. This token serves as the primary medium of exchange within our platform, enabling a streamlined process for financial transactions and incentivization schemes. Authors are rewarded with these tokens for their contributions, reviewers receive tokens for their expert evaluations, and readers utilize these tokens to gain access to academic papers.

Our unique design cultivates an environment that fosters mutual benefit and continuous engagement within the scholarly publishing sphere, effectively driving the democratization of knowledge dissemination and acquisition.

- Reviewer

Central to the operational integrity of a decentralized publishing platform like SeaOfWisdom is the presence of high-quality content, which is largely dictated by the expertise and fairness of the individuals engaged in the reviewing process. We have instituted a mechanism within SeaOfWisdom whereby individuals possessing a PhD or a higher academic qualification can verify their expertise and partake in the reviewing process.

Upon the successful validation and publication of a paper, reviewers receive a one-time reward once a pre-defined number of purchases for the respective paper is achieved. This incentivization mechanism aims to ensure the participation of reviewers and upholds the quality of content on the platform.

This provision of a financial reward creates a compelling economic incentive for participation in SeaOfWisdom's reviewing process. Outside of traditional academia – teaching or engaging in a research program, opportunities for individuals possessing a PhD to monetize their academic qualifications are considerably limited. SeaOfWisdom disrupts this paradigm by pioneering a unique avenue for individuals to derive financial benefits directly from their scholarly credentials.

This transformative approach reevaluates the conventional understanding of a PhD qualification's value proposition, driving potential increased returns on the significant investment made in obtaining such a title. In effect, SeaOfWisdom imparts a tangible, monetizable value to the academic qualification itself, engendering a more robust and fluid academia-industry economic interplay.

In pursuit of transparency and immutability, every review, along with its associated metadata, is stored on IPFS. Each manuscript submitted for publication requires a minimum of two positive reviews before it can be officially published on the platform.

To deter fraudulent activities and uphold the integrity of the reviewing process, reviewers are necessitated to stake a deposit - a precautionary measure reminiscent of the Proof-of-Stake (PoS) mechanism in Ethereum 2.0, where validators are mandated to stake 32 Eth. The deposit staked by a reviewer in SeaOfWisdom, albeit significantly lower, serves a similar purpose. In instances where a reviewer exhibits unfair conduct, the staked deposit can be leveraged to impose penalties, thereby preserving the quality of content and the overall credibility of the platform.

- Reader

In the paradigm espoused by our platform, a scholarly paper, subjected to stringent scrutiny and approved by leading scholars with demonstrated track records (PhD or higher), is transmuted into a tangible asset bearing intrinsic value. This positions the work as a highly desirable acquisition, stimulating a potent demand for purchase.
The principal readership is anticipated to emerge from both governmental and private academic institutions, inclusive of universities, libraries, research centers, and other entities engaged in scholarly pursuits. Reflective of their inherent value and popularity, the prices of these scholarly works are dynamically adjusted and denominated in the native SOW tokens. Furthermore, to ensure pricing stability and broaden accessibility, we envisage incorporating stable coins as an additional medium of exchange in the future.

Furthermore, we have built in mechanisms to actively encourage readers to engage deeply with the purchased work. In the subsequent versions of the platform, we plan to implement a dispute resolution mechanism, allowing users to initiate a dispute with the author, should they question any of the findings or referenced materials. Such disputes are initiated with a commensurate deposit of funds, serving to validate the sincerity of the disputant's intent. The resolution of such disputes is handled by an independent panel of reviewers, who, after evaluating the dispute, award the resolution funds to the party they deem to be correct.

Moreover, the platform is designed to motivate users to query the author and seek clarifications on points of interest or doubt. As an additional incentive, users have the option to tip the author for comprehensive and insightful answers, thereby creating a dynamic academic exchange that enriches the learning process and increases the inherent value of the scholarly work.

B. Technical Implementation (fig. 1)

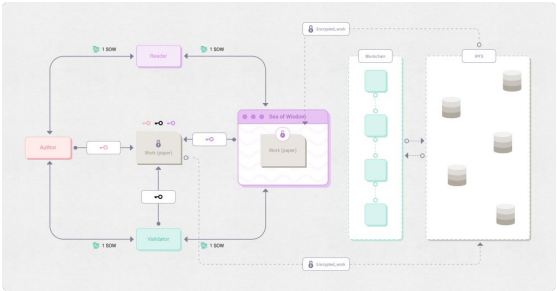

Figure 1: Diagrammatic Representation of the Decentralized Scholarly Publishing Platform, Grounded in Blockchain Technology.

Blockchain: The Blockchain serves as the unalterable digital ledger of this platform, housing all smart contract codes and transaction data. It provides a chronological record of transactions, including payments for paper access and rewards distributed to authors and reviewers.

Frontend (not shown in Fig. 1): The user interface is developed using HTML, CSS, and TypeScript, heavily relying on JavaScript libraries web3.js and ethers.js. The web3.js module is instrumental in enabling seamless interaction between the EVM-compatible blockchain and frontend elements. Authors, reviewers, and readers can interact

with the underlying blockchain and IPFS infrastructure through this intuitive browser interface.

Interplanetary File System (IPFS): Upon an author's submission of a paper, the frontend oversees the transfer of the paper's content, along with its metadata, to IPFS. This action triggers the generation of a unique hash for the uploaded file, which is then recorded on the blockchain. This approach leverages IPFS to offset the exorbitant costs linked with storing files directly on the blockchain, while the unique hash functions as a permanent and unalterable link to the paper, ensuring reliable, decentralized access regardless of network conditions.

Native token (SOW): The platform employs a native token, constructed on the Ethereum blockchain conforming to the ERC-20 standard. OpenZeppelin, a library for secure smart contract development, is used to ensure the security and reliability of the token. Readers use this token to gain access to scholarly papers, while authors and reviewers receive tokens as incentives for their respective contributions.

Scientific Paper Token (SPT): In our quest to create an equitable, transparent, and decentralized academic publishing landscape, we introduce the Scientific Paper Token (SPT), a novel token standard inspired by Ethereum's ERC-721 protocol, a de facto standard for Non-Fungible Tokens (NFTs). Conceptualized and implemented as a smart contract on the Ethereum blockchain, the SPT operates at the intersection of technology, economics, and scholarly communication, presenting an innovative solution to long-standing problems in the publishing industry. At a high level, each instance of the SPT embodies a unique scholarly paper within our platform, ensuring the indivisibility and distinctiveness of the intellectual property it represents. It serves as a multi-faceted digital asset encapsulating vital attributes and operations pertinent to the lifecycle of an academic paper, including authorship, review, ownership, access, and remuneration. In addition to the common features of an ERC-721 token, the SPT incorporates several key enhancements catering specifically to the needs of the academic publishing ecosystem: *Ownership and Authorship*: The SPT is intrinsically tied to the original authors of the academic work it represents. The token is minted by the authors and, as such, establishes undeniable proof of authorship. It can also be transferred or sold, enabling the potential for a dynamic market in academic publishing rights; *Review and Approval Status*: Each token stores a mutable status field, indicating the approval status of the corresponding paper. This feature facilitates a transparent peer-review process; *Access and Expiry*: The SPT introduces a mechanism to control access rights to the associated scholarly work. It employs a mapping structure to store the access rights of individual users, alongside an expiry timestamp dictating the duration of this access; *Economic Incentives*: The SPT holds an immutable initial price, setting a precedent for a fair, demand-based compensation model for authors and reviewers. In a broader perspective, the SPT serves as a foundational building block in our endeavor to restructure academic publishing. It fosters the much-needed transparency, and fairness, and by leveraging the power of the blockchain, enables a decentralized and democratized scientific community.

Backend (not shown in Fig. 1):: The infrastructure of the platform is developed in Golang adopting a microservice architecture, which enables a robust, modular backend. Each microservice is specialized for a specific task, including optical character recognition for uploaded papers, anti-plagiarism detection, and paper formatting, among others. These specialized services communicate seamlessly via the gRPC protocol, providing efficient service-to-service interaction. The services are also accessible as RESTful APIs, predominantly for internal use. However, future development plans include public API access, expanding the platform's capabilities to third-party developers, thereby fostering a comprehensive scholarly ecosystem.

4. Operational Flow

This section provides an elaborate discourse on the operative schema of the proposed platform, encapsulating pivotal elements into business logic (Fig. 2):

- As an author, the user is enabled to upload their scholarly manuscript to the platform via the web interface, furnishing requisite metadata like the author's name, title of the paper, abstract, keywords, among others. Subsequent to this upload, the system mints a unique ERC721 token (Non-Fungible Token or NFT) on the Ethereum blockchain, symbolizing the author's proprietary rights over the uploaded manuscript.
- The manuscript, once uploaded to the InterPlanetary File System (IPFS), generates a distinctive hash that functions as a permanent locator to the manuscript. Leveraging the web3.js library, the web interface triggers a smart contract to inscribe the IPFS hash onto the EVM-compatible blockchain.
- Upon accruing two affirmative reviews, the manuscript is officially disseminated on the platform, thereby rendering it accessible for public acquisition.
- Readers inclined to access the manuscript remunerate the platform's native ERC-20 tokens, which are directly transferred from the reader's wallet to the author's wallet.

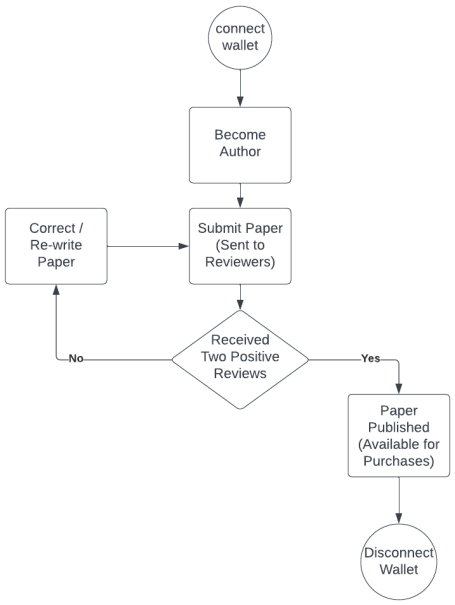

Figure 2: Illustration of the Scholarly Manuscript's Lifecycle, from Initial Submission to Final Publication on the Platform.

5. Conclusion

This research underscores the transformative potential of blockchain technology in academic publishing, aiming to bridge the chasm between theoretical propositions and pragmatic application. By developing a blockchain-centric platform, we have created a solution that tackles key issues in traditional scholarly publishing, including peer-review opacity, unfair remuneration, and restricted paper access.

However, we understand that technological progression comes with its unique set of challenges. Major constraints like mass adoption and plagiarism detection, albeit daunting, are surmountable through intuitive user interfaces, digital wallet tools like UniPass [14], and anti-plagiarism mechanisms [15].

In conclusion, our research is a decisive stride towards a more open, fair, and rewarding academic publishing ecosystem, despite recognizing that the path ahead demands continuous innovation, adaptation, and resilience.

References

[1] Nosek, B. A.; Alter, G.; Banks, G. C.; et al. (2015): Promoting an open research culture, in: Science, vol. 348, no. 6242, pp. 1422-1425.

[2] Leible, Stephan; Schlager, Steffen; Schubotz, Moritz; Gipp, Bela (2019): A Review on Blockchain Technology and Blockchain Projects Fostering Open Science, in: Front. Blockchain, vol. 2. [online] https://doi.org/10.3389/fbloc.2019.00016 [19.11.2019].

[3] Nelaturu, Keerthi; Du, Han; Le, Duc-Phong (2022): A Review of Blockchain in Fintech: Taxonomy, Challenges, and Future Directions, in: Cryptography, vol. 6, no. 2, pages not specified.

[4] Arbabi, Mohammad Salar; Lal, Chhagan; Veeraragavan, Narasimha Raghavan; Marijan, Dusica; Nygård, Jan F.; Vitenberg, Roman (2023): A Survey on Blockchain for Healthcare: Challenges, Benefits, and Future Directions, in: IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 386-424.

[5] De Leon, Ignacio; Gupta, Ravi (2017): The Impact of Digital Innovation and Blockchain on the Music Industry. [online] https://theblockchaintest.com/uploads/resources/Ignacio%20De%20Leon-Ravi%20Gupta%20-%20The%20Impact%20of%20Digital%20Innovation%20and%20Blockchain%20on%20the%20Music%20Industry%20-%202017%20Nov.pdf [Accessed: 21.07.2023, 00:00].

[6] Niya, Sina Rafati; Pelloni, Lucas; Wullschleger, Severin; Schaufelbühl, Andreas; Bocek, Thomas; Rajendran, Lawrence (2019): A Blockchain-based Scientific Publishing Platform, in: Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pages not specified.

[7] Stojmenova Duh, Emilija; Duh, Andrej; Droftina, Uroš; Kos, Tim; Duh, Urban; Simonič Korošak, Tanja; Korošak, Dean (2019): Publish-and-Flourish: Using Blockchain Platform to Enable Cooperative Scholarly Communication, in: Publications, vol. 7. [online] https://doi.org/10.3390/publications7020033 [Accessed: 21.07.2023, 00:00].

[8] Kosmarski, Artyom (2020): Blockchain Adoption in Academia: Promises and Challenges, in: J. Open Innov. Technol. Mark. Complex., vol. 6. [online] https://doi.org/10.3390/joitmc6040117 [16.10.2020].

[9] ScienceRoot. Available: https://scienceroot.com. [Accessed: 21.07.2023, 00:00].

[10] "Eureka Scientific Publishing Platform," Eureka Smart Contract Source Code, Available: https://github.com/eureka-blockchain-solutions/eureka-token-contract/blob/master/src/test/resources/Eureka.sol. [Accessed: 21.07.2023, 00:00].

[11] DEIP, "Decentralized Research Platform," Available: https://deip.world. [Accessed: 21.07. 2023, 00:00].

[12] Orvium (2019): Accelerating Scientific Publishing, [online] https://docs.orvium.io/Orvium-WP.pdf [Accessed: 21.07. 2023, 00:00].

[13] Budzinski, Oliver; Grebel, Thomas; Wolling, Jens; Zhang, Xijie (2020): Drivers of article processing charges in open access, in: Scientometrics, vol. 124, pages 2185-2206.

[14] "Introduction," Unipass Documentation, [Online]. Available: https://docs.wallet.unipass.id/introduction/intro. [Accessed: 21.07. 2023, 00:00].

[15] N. Pachina, V. Orobinskaya, A. Pachin, and D. Konovalov, "Tools for Detecting Plagiarism on the Websites of Scientific Publications and Ways to Protect them," in 2022 4th International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA), Lipetsk, Russian Federation, 2022, pp. 597-599, doi: 10.1109/SUMMA57301.2022.9973983.

Dezentrale Authentifizierung als Antwort auf das Oracle Problem im Kontext der Zertifizierung von grünem Wasserstoff

Jakob Amann, Jan Bittner, Volker Wannack
Blockchain Competence Center der HS Mittweida, Mittweida, Deutschland

Das Ziel des vorliegenden Papers ist die Darstellung eines Konzepts zur Lösung des Oracle Problems im Kontext der Wasserstoffproduktion mit erneuerbaren Energieproduktionsformen. Der vorgeschlagene Ansatz setzt auf die Authentifizierung des Stroms, der für die Produktion des Wasserstoffs verwendet wird, durch eine Vielzahl an umliegenden Akteuren mit gleichen Stromgewinnungsanlagen, welche die Authentizität der Stromproduktion bezeugen. Das Konzept setzt auf einen Authenticity-Score, welchen jedes Zertifikat erhält, sowie einen Trust-Score, der jedem Zeugen zugeschrieben wird. Jedes Zertifikat muss von verschiedenen Akteuren mit ausreichenden Trust-Score bezeugt werden, um einen Authenticity-Score zu erhalten, der über einer festgelegten Schwelle liegt und somit nachweist, dass der produzierte Wasserstoff tatsächlich „grün" ist.

1. Einleitung

Die globalisierte Welt steht vor der Bewältigung einer der größten Herausforderungen der letzten Jahrzehnte – der Energiewende. Luftverschmutzung, Klimawandel & Co. zwingen uns dazu die Art und Weise, wie wir Energie gewinnen und transportieren zu überdenken und die Primärenergiebereitstellung auf erneuerbare Energieproduktionsformen (Photovoltaik und Wind) umzustellen. Damit diese neue Art der Energieversorgung auch in Zeiten von Dunkelflauten und Windstille gesichert ist und auch weiterhin alle (vor allem industrielle) Energieprozessbedarfe gedeckt werden können, bedarf es der Produktion bzw. des Imports von grünem Wasserstoff (H2).

H2 wird meist mittels Elektrolyse hergestellt. Bei diesem energieintensiven Prozess ist es wichtig, dass nachweislich erneuerbare Energieproduktionsformen verwendet werden, damit der produzierte Wasserstoff auch als grün gilt. Die regulatorischen Vorgaben in Europa sehen vor, dass der verwendete Strom entweder direkt mit erneuerbaren Energien generiert werden muss oder der im Stromnetz vorhandene Strom zum Großteil aus erneuerbaren Energieproduktionsformen gewonnen worden sein muss, um grünen Wasserstoff zu produzieren [1] – wie der Nachweis dafür jedoch erstellt wird, ist noch nicht abschließend festgelegt. Eine Möglichkeit diesen Zertifizierungsprozess abzubilden, bietet die Blockchain-Technologie. Diese Technologie verspricht Fälschungssicherheit, rückwirkende Unveränderlichkeit und daraus resultierend, ein hohes Vertrauen in die dort gespeicherten Zertifikate. Diese Eigenschaften sind natürlich stark von der konkret gewählten Architektur des Netzwerkes abhängig, jedoch sind diese Aspekte grundsätzlich genau die, die man bei „ehrlichen" Zertifikaten erwartet und benötigt.

Im Bereich der Erneuerbaren Energien gibt es mit dem Herkunftsnachweisregister (HKNR) des Umweltbundesamts eine zentrale Instanz, die Zertifikate ausstellt, überträgt und vernichtet. Dieses System funktioniert grundsätzlich gut und findet sich in ähnlicher Form in den meisten europäischen Ländern. Jedoch treten drei grundsätzliche Probleme auf:

- Begrenzte Skalierbarkeit aufgrund mangelnder Automatisierungsmöglichkeiten
- Schwierigkeiten bei grenzübergreifenden Transaktionen
- Zertifikate können den tatsächlichen Ursprung des gelieferten Stroms verschleiern, sodass nicht-erneuerbare Energie als grün verkauft werden kann[1]

Die Blockchain-Technologie bietet die Möglichkeit die Abwicklung des Zertifizierungsprozesses zu automatisieren und somit massiv Zeit und Geld einzusparen. Durch eine einheitliche, vertrauenswürdige und technologisch ausgereifte Lösung können grenzübergreifende Transaktionen extrem vereinfacht werden. Das ist im Kontext von Wasserstoff insbesondere wichtig, da es als Energieträger fungiert und es somit aussichtsreich erscheint in den sonnenreichen Gegenden der Welt H2 zu produzieren und diesen dann von dort an die Orte zu transportieren, wo die Energie gebraucht wird. Zudem ist es denkbar "jedes Gramm Wasserstoff" zu zertifizieren, wodurch die Herstellungsprozesse eine Transparenz erreichen, die schon heute im Bereich der Erneuerbaren Energien wünschenswert wären.

2. Hauptteil

2.1. Forschungsprojekt: Blockchain-basierter Wasserstoffmarkt (BBH_2)

[1] Es liegt in der physikalischen Eigenschaft von Strom, immer den kürzesten Weg zu nehmen. Der zum Herkunftsnachweis gehörende Strom aus erneuerbaren Energien fließt in den allgemeinen „Stromsee". Dieser wird dann lediglich bilanziell zugewiesen.

Um dieses enorme Potenzial für dieses Zukunftsthema zu evaluieren, forschen Mitarbeitende des Blockchain Competence Center Mittweida (BCCM) in Kooperation mit Vertretern aus der Energiewirtschaft (Exxeta AG) sowie Bio-Gas- & Wasserstoffproduzenten (Ökotec GmbH) zusammen, um eine blockchainbasierte Lösung für den Wasserstoffmarkt zu entwickeln und ausgiebig zu testen. Das Ziel ist die Entwicklung eines ausgereiften Produkts, dass den europäischen Wasserstoffmarkt inklusive Zertifizierungsprozess abbilden kann. Das Projekt Blockchain-basierter Wasserstoffmarkt (BBH_2) läuft bereits seit dem Jahre 2022 und hat eine prognostizierte Laufzeit bis 2025. Es wird im Rahmen der "Technologieoffensive Wasserstoff" des Bundesministeriums für Wirtschaft und Klimaschutz im 7. Energieforschungsprogramm der Bundesregierung gefördert [2]. Es ist Teil der Blockchain-Strategie der Bundesregierung [3], sowie der Nationalen Wasserstoffstrategie [4].

Bisher wurde bereits der erste Prototyp für die Zertifizierung des Wasserstoffproduktionsprozesses entwickelt. Hierbei lag der Fokus insbesondere darauf erste Erfahrungen in der Blockchainentwicklung im Wasserstoffkontext zu erlangen. Für den ersten Prototypen wurde eine Lösung entwickelt, die auf Ethereum basiert und ein Account-Balance Model verwendet, um die Zertifikate eindeutig zuzuordnen und transferieren zu können. Der Prototyp kann mit MetaMask unter folgenden Link (https://staging.bbh2.exxeta.info/) getestet werden.

Da das Ziel des Projekts darin besteht eine robuste, effiziente und vertrauenswürdige Lösung zu entwickeln, die die Anforderungen des Wasserstoffmarkts erfüllt, werden verschiedene Prototypen entwickelt, ausgiebig getestet und ihre Stärken und Schwächen mit Hilfe der Konsortialpartner analysiert, um am Ende eine belastbare Lösung vorweisen zu können. Aktuelle Entwicklungen zu dem Projekt können Sie auf der Webseite des Projekts (https://www.hydrogenchain.de/) einsehen.

2.2 Problemstellung: Authentische Daten auf der Blockchain

Die Blockchain-Technologie ist dafür bekannt, dass sie eine manipulationssichere, rückwirkend unveränderliche, dezentrale Datenbank darstellt [5]. Um diese Eigenschaften zu gewährleisten sind bereits einige Aspekte hinsichtlich der Blockchainarchitektur zu beachten, die zu ausreichender Dezentralität und Sicherheit führen. Darauf wird ihm Rahmen dieses Papers jedoch nicht näher eingegangen werden. Stattdessen geht es um ein Szenario, in dem eine technische Lösung, die diese Eigenschaften erfüllt, zur Verfügung steht, wobei hiermit die Authentizität der Zertifikate noch nicht sichergestellt ist. Die genannten Kerneigenschaften der Blockchain-Technologie sind wertlos, wenn die eingespeisten Daten fehlerhaft sind - *Garbage In, Garbage Out.* Deshalb liegt der Fokus in dieser Arbeit auf der Frage, wie man vertrauenswürdige, authentische Daten auf die Blockhain bekommt.

Das Oracle Problem beschreibt ebendiese Schwierigkeit authentische Daten in die dezentrale Datenbank zu bekommen, ohne auf eine zentrale Kontrollinstanz oder die Gutmütigkeit der Beteiligten angewiesen zu sein. Eine zentrale Instanz, die die Authentizität der Daten überprüfen und gewährleisten würde, würde eine dezentrale Blockchainlösung, die diese Daten speichert obsolet machen, da man erneut eine sogenannte „trusted third party" hätte – also eine außenstehende Instanz, der man Vertrauen muss und die somit als „single point of failure" angesehen werden kann [5].

Eine Lösung für dieses Problem soll in diesem Paper vorgestellt werden: die dezentrale Authentifizierung. Die Grundidee ist, dass man statt einer zentralen Instanz, die die Authentizität der Daten sicherstellt, auf die Überprüfung der eingespeisten Daten durch viele Beteiligte setzt. Diese Beteiligten tragen zu einem **Authenticity-Score** bei, den jedes Zertifikat bekommt. Hierbei wird sichergestellt, dass ausreichend viele unabhängige Akteure die Authentizität des Zertifikats bezeugen, um einen Betrug äußerst unwahrscheinlich zu machen. Um zusätzlich einen Anreiz für die Authentifizierenden zu schaffen sich regelkonform zu verhalten, erhalten diese einen **Trust-Score**, der ihre Glaubwürdigkeit darstellt und beeinflusst, wie viel sie zu dem Authenticity-Score des Zertifikats beitragen können.

Im Folgenden wird das Konzept der dezentralen Authentifizierung vorgestellt und eine mögliche Implementierung via safe-UR-chain [6] (sUc) dargestellt. Das Konzept von sUc basiert grundlegend auf der Kombination von unternehmensinternen Blockchains, die untereinander Blockhashes austauschen und in ihre Blöcke einbauen, um so eine Unveränderlichkeit der Daten auf eine sehr datensparende Art und Weise sicherzustellen. Zusätzlich werden im Rahmen dieses Konzept die Transaktionen auf einer öffentlichen Blockchain aggregiert, um die unabhängige Überprüfbarkeit zu gewährleisten und eine doppelte Verwendung der Zertifikate (Double Spending) zu verhindern. Eine detaillierte Beschreibung des Safe-Ur-Chain-Ansatzes würde den Rahmen dieser Arbeit übersteigen. Dafür findet sich ein schemenhaftes Schaubild des Konzepts in Abbildung 1.

2.3 Dezentrale Authentifizierung als Antwort auf das Oracle Problem

Das BBH_2 Projekt zielt wie oben erwähnt unter anderem auf die Herstellungsprozesse des grünen Wasserstoffs ab. Damit der hergestellte Wasserstoff als grün gilt, muss dieser mit Hilfe erneuerbarer Energien hergestellt werden [1]. Damit kann der Zertifizierungsprozess nicht erst bei der Produktion des H_2 beginnen, sondern muss bereits vorher ansetzen – bei der Stromproduktion. Genau hier setzt auch der Ansatz der dezentralen Authentifizierung an.

Um das Konzept greifbar zu machen, wird es anhand eines beispielhaften Ablaufs dargestellt. Safe-Ur-Chain setzt wie bereits erwähnt auf die Verwendung

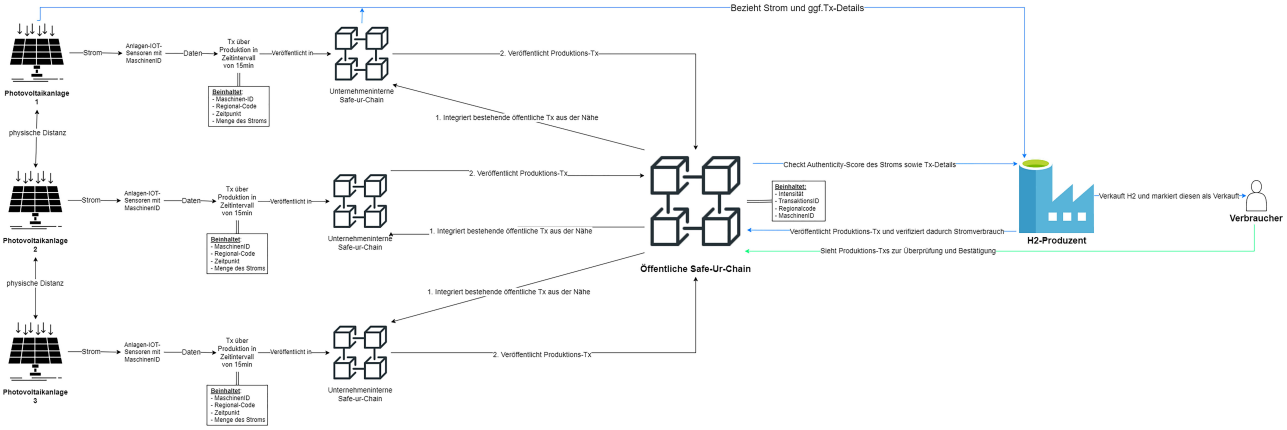

Abbildung 1: Schemenhafte Darstellung des Konzepts der dezentralen Authentifizierung

unternehmensinterner, privater Blockchains, die miteinander kommunizieren und Blockhashes austauschen [6]. Wenn nun bspw. eine Photovoltaikanlage Strom produziert, dann wird diese Stromproduktion auf der privaten Blockchain des PV-Anlagenbetreibenden per Transaktion festgehalten. Diese Transaktion beinhaltet den Regional-Code (also den Standort) der Anlage, den Zeitpunkt der Produktion und die Menge des produzierten Stroms in einem gewissen Zeitintervall. Das Zeitintervall ist hier bevorzugt klein zu wählen, um eine möglichst genaue Erfassung zu garantieren. Gleichzeitig muss er groß genug sein, um technisch mit einem angemessenen Aufwand umsetzbar zu sein. Somit bietet sich für dieses Konzept ein Zeitintervall von beispielsweise 15 Minuten pro Transaktion an.[2]

Um die Einspeisung in dieser Frequenz sicherstellen zu können, ist die Verwendung von IoT-Geräten, die mit der Blockchain kommunizieren, unabdingbar. Diese Geräte bieten nicht nur die Möglichkeit, Daten in standardisierter Form unternehmensübergreifend einzuspeisen, sondern erhöhen durch den Einsatz von Technologien wie TPM (Trusted Platform Modules) auch die Sicherheit. Ein solches TPM garantiert, dass die Geräte nach ihrer Produktion nicht mehr modifiziert werden können [7]. Dies minimiert das Risiko von Manipulationen und stellt sicher, dass die Geräte nur den vorgesehenen, authentischen Code ausführen.[3]

Darüber hinaus bieten selbstverwaltete Maschinenidentitäten (sog. Self-Sovereing-Identities) das Potenzial die Sicherheit weiter zu erhöhen und geben zudem den Beteiligten die Möglichkeit selbst zu entscheiden, welche Daten sie preisgeben wollen [8]. Somit kann je nach Bedarf ein sehr datensparendes und privatsphäre-orientiertes System erschaffen werden.

Nachdem die Transaktion für die Stromproduktion per PV-Anlage automatisch erstellt wurde und in die organisationsinterne Blockchain geschrieben wurde, muss diese noch authentifiziert werden. Hier kommen die umliegenden Akteure ins Spiel. Anhand des Regionalcodes, der bei der Initialisierung jeder Anlage dieser zugewiesen wird, und sich in jeder Transaktion wiederfindet, können umliegende PV-anlagenbetreibende identifiziert werden. Auf einer zusätzlichen öffentlichen Blockchain werden die Produktionstransaktionen gesammelt, wobei hier ein äußerst datensparendes Modell verwendet wird, bei dem lediglich die Intensität (welche berechenbar aus der produzierten Strommenge sowie der Größe und Effizienz der Anlage ist) der Sonnenstrahlung, die TransaktionsID, der Regionalcode und die ID des Anlagenbetreibenden festgehalten wird. Damit können automatisiert umliegende Betreiber gleicher Stromproduktionsanlagen identifiziert werden und ihre Transaktionen zum Nachweis ihrer eigenen Stromproduktion als Beleg dafür genutzt werden, dass der produzierte Strom tatsächlich mit Hilfe der entsprechenden Technologie hergestellt wurde.

Hierfür nehmen die Anlagebetreiber die TransaktionsID eines umliegenden Anlagenbetreibers und verknüpfen diese mit ihrer ursprünglichen Transaktion. Damit steigt der Authenticity-Score des produzierten Stroms in Abhängigkeit von zwei Aspekten. Erstens der Distanz zwischen beiden Anlagenbetreibern (ermittelbar über den Regionalcode) und zweitens über den Trust-Score des Betreibers, den man als Zeuge involviert. Damit die Authentifizierung aber nicht einfach nur an einen benachbarten Anlagenbetreiber abgegeben wird, kann jeder Zeuge nur einen gewissen Beitrag zum Authenticity-Score der Transaktion beitragen.

Ein Ansatz ist, dass jeder Zeuge maximal 20 Punkte zum Authenticity-Score beitragen kann und ein Zertifikat erst dann als gültig gilt, wenn es über 100 Punkte[4] hat. Um zurück zum Beispiel von oben zu kommen, gehen wir

[2] Nach der aktuellen Einschätzung der Forschenden sollte dieser Zeitintervall bei maximal wenigen Minuten liegen, jedoch muss der Feldtest zeigen, welcher konkrete Wert sich als robust und praktikabel erweist.

[3] Dieser Ansatz verlagert das Vertrauensproblem ein Stück weit auf die Hersteller dieser Geräte. Auf diesen Punkt wird in der Diskussion am Ende nochmal gesondert eingegangen.

[4] Dieser Wert ist zunächst frei gewählt. Er kann und sollte basierend auf praktischen Erfahrungen angepasst werden.

davon aus, dass der Anlagenbetreiber, der den (PV-)Photovoltaikstrom produziert, noch nie etwas fehlerhaftes bezeugt hat und somit den maximalen Trust-Score von 100 erreicht. Da der Regionalcode eins zu eins mit dem der Anlage übereinstimmt (es handelt sich um die Anlage selbst), gibt es keinerlei Abzüge für die Entfernung zu der Anlage. Somit trägt der Produzent selbst 20 Punkte zum Authenticity-Score seines Zertifikats bei. Damit fehlen aber noch mindestens 80 Punkte, die er benötigt, um ein gültiges Zertifikat zu erhalten. Somit wäre er auf mindestens vier weitere Anlagenbetreiber mit perfekter Glaubwürdigkeit (Trust-Score) in unmittelbarer Nähe angewiesen, um dazu zu kommen. Da dies unwahrscheinlich ist, können auch Betreiber weiter entfernter Anlagen[5] als Zeugen herangezogen werden. Jedoch wird hier aufgrund der größeren Distanz angenommen, dass diese weniger zur Authentizität beitragen können, was sich in folgender beispielhafter Gleichung widerspiegelt:

$$Authenticity = \sum_{i=1}^{n} 20 * \frac{Trust_i}{100} + (Distanz_i * (-2))$$

Es ist anzumerken, dass die konstanten Zahlenwerte hier schlichtweg gewählt sind und an die unmittelbare Implementation angepasst werden müssen. So ist bspw. die Distanz zwischen zwei Stationen davon abhängig, ob man deren Standort mit Hilfe GPS-Koordinaten bestimmt, was eine unmittelbare Umrechnung der Distanz in (Kilo-)Meter erlaubt. Hier wird davon ausgegangen, dass der ideale Authentifizierer einen Trust-Score von 100 hat und unmittelbar neben der Anlage des Stromproduzenten lokalisiert ist (Distanz = 0). Somit könnte diese Instanz 20 Punkte zum Authenticity-Score des Zertifikats beitragen. Gleichzeitig erlaubt diese Herangehensweise, dass Zeugen, die mehr als 10 km entfernt sind (Distanz = 10) nichts mehr zu dem Zertifikat beitragen können – im Gegenteil. Wer diese Daten nutzt, um sein Zertifikat zu validieren, reduziert dessen Authenticity-Score.[6]

Mit diesem Ansatz ist die Produktion des Stroms nachweislich, rückverfolgbar und authentisch zertifiziert. Wird nun der Strom an einen Elektrolyseur gegeben, um damit H_2 zu produzieren, so erhält dieser neben dem Strom auch die TransaktionsID der Stromproduktion. Der H_2 Produzent erzeugt ebenso eine Transaktion für die Herstellung des H_2, in der erfasst wird, wie viel Wasserstoff zu welchem Zeitpunkt unter welchem Stromeinsatz produziert wurde. Dafür baut dieser die StromproduktionstransaktionsID in seine Wasserstoffproduktionstransaktion ein, um eine nachverfolgbare Kette zu erzeugen, die die unternehmensinternen Blockchains miteinander verknüpft. Nun kann mittels dieser Wasserstoffproduktionstransaktion lückenlos und authentisch bewiesen werden, wie diese Menge Wasserstoff produziert wurde.

Zu bedenken ist natürlich, dass der produzierte Strom unmittelbar verbraucht wird und nicht gelagert wird, bis die Stromproduktionstransaktion authentifiziert ist. Das ist aber in diesem Ansatz kein Problem, da durch die Verknüpfung des produzierten Wasserstoffs mit der Stromproduktionstransaktion auch noch nachträglich der Wasserstoff authentisch zertifiziert werden kann, solange auf der öffentlichen Blockchain zum Produktionszeitpunkt ausreichend Transaktionen vorhanden sind, die als Zeugen herangezogen werden können.

Nachdem nun der Wasserstoff produziert und authentisch zertifiziert worden ist, ist es entscheidend, dass man verhindert, dass der gleiche nachweislich mit erneuerbaren Energien produzierte Strom für die Zertifizierung einer anderen H_2 Produktion herangezogen wird (Double-Spending Problem). Dafür ist es notwendig, dass die H_2 Produzenten ihre Produktionstransaktion an die öffentliche Blockchain geben, damit die zugehörige Stromproduktionstransaktion für alle als bereits verwendet ersichtlich ist (Spending-Transaction). Wenn nun der Wasserstoffproduzent den Wasserstoff verkauft, gibt er die letztlich erwähnte Spending Transaction an den Käufer, welcher dann in der öffentlich einsehbaren Blockchain den authentischen und fälschungssicheren Nachweis für die Produktion seiner Menge Wasserstoff hat, der den Produktionsprozess von Anfang an abbildet, ohne sensible Daten preiszugeben.

3. Fazit: Stärken & Schwächen der dezentralen Authentifizierung

Das vorgestellte Konzept bietet eine aussichtsreiche Möglichkeit den Zertifizierungsprozess von Wasserstoff grammgenau und verlässlich abzubilden. Jedoch ist das Konzept aufgrund seiner theoretischen Natur noch nicht als unmittelbare Lösung des Oracle-Problems zu verstehen, sondern vielmehr als eine Antwortmöglichkeit anzusehen. Um sowohl die Schwierigkeiten dieser Thematik sowie des Ansatzes als auch die Vorzüge des Konzepts zu verdeutlichen, werden im Folgenden die Grenzen und Erweiterungsmöglichkeiten kurz diskutiert.

Die in diesem Paper vorgeschlagene dezentrale Authentifizierung setzt auf IoT-Sensoren, die in einer hohen Frequenz Daten generieren und an die interne Blockchain geben. Dadurch verschiebt sich die Notwendigkeit einer zentralen Instanz vertrauen zu müssen zur Notwendigkeit den Herstellern der Geräte Vertrauen zu müssen. Maschinenidentitäten sowie Hardwaremodule bieten hierfür einen vielversprechenden Ansatz Risiken zu minimieren. Bestimmte Hardwaremodule können sicherstellen, dass das Gerät seit der Produktion nicht verändert wurden. Da die Hersteller kein Interesse daran haben fehlerhafte Geräte auszuliefern, um Strafen zu vermeiden sowie ihren Ruf nicht zu schädigen, wird dieses

[5] Auch hier müssen die Parameter gewählt werden. Für den Anfang schlagen wir einen Abzug von 2 Punkten pro 10 km Distanz zu der Produktionsstätte vor.

[6] Diese Formel ist als Hilfe zur Darstellung für die konzeptionelle Idee zu verstehen und nicht als Vorschlag für eine konkrete Implementierung.

Problem als äußerst relevant, aber nicht unlösbar angesehen.

Neben potenziell manipulierten Geräten könnten auch findige Betrüger versuchen einem authentischen Gerät andere Gegebenheiten (wie bspw. Wind an windstillem Tag) vorzugaukeln. Um diese Angriffsvektoren identifizieren zu können, muss der technische Prozess des spezifischen Geräts inspiziert werden, was im Kontext eines Konzepts nicht möglich ist. Zudem sollten derartige Manipulationen durch abweichende Produktionsbedingungen der umliegenden Authentifizierenden bzw. Deren Sensoren auffallen. Genau das ist die zentrale Stärke des Ansatzes. Bei Betrugsverdachtsfällen könnten unangekündigte Besuche der Regulierungsbehörden diesem nachgehen, was aufgrund der klaren lokalen Zuordnung problemlos möglich wäre.

Der eingeführte Trust-Score ermöglicht zudem eine netzwerkinterne Sanktionierung von fehlerhaften Mitteilungen bzw. Schadhaften Akteuren sowie die Möglichkeit ein wirtschaftliches Anreizmodell zu entwickeln, welches die Authentifizierer an den Zertifikats- bzw. Handelserträgen teilhaben lässt. Somit könnte ein Anreiz geschaffen werden, dass auch Nicht-Produzenten dem Netzwerk beitreten und bspw. Durch die Bezeugung von Sonneneinstrahlung und die damit verbundene Bezeugung der Authentizität der Zertifikate entgeltlich entlohnt werden. Die konkrete Ausarbeitung dieses Anreizmodells steht jedoch noch aus und sollte sich stark an den Erkenntnissen der spieltheoretischen Forschung sowie deren Umsetzung in Bitcoin und anderen dezentralen Projekten orientieren.

Ein grundsätzlicher Nachteil des Ansatzes ist die Notwendigkeit IoT-Geräte anzuschaffen und von Grund auf eine (unternehmensinterne) Blockchain aufzusetzen. Hierbei sind die Kosten für die IoT-Geräte aktuell nicht abschätzbar. Für die Blockchain-Infrastruktur sollte ein leistungsschwacher Computer (wie bspw. Ein RaspberryPi) ausreichen,[7] womit sich die Kosten lediglich auf wenige hundert Euro belaufen. Zudem ist mit diesem Ansatz die Entwicklung einer günstigen und einfachen Plug-'n-Play Lösung denkbar, die weniger technikaffinen Menschen die Möglichkeit gibt an dem Netzwerk teilzunehmen.

Ein großer Vorteil dieses Konzepts ist, dass es die Notwendigkeit einer aufwändigen Registrierung bei einer zentralen Instanz wie dem HKNR bzw. dem Umweltbundesamt hinfällig macht. Jeder kann an dem Netzwerk teilnehmen, solange Anforderungen[8] erfüllt werden. Das erlaubt eine grenzübergreifende Skalierung des Netzwerkes und reduziert die (bürokratischen) Einstiegshürden massiv, da jegliche Abnahmeprozesse der Anlagen wegfallen. Gleichzeitig wäre es denkbar, dass man Akteure wie das Umweltbundesamt mit einer Sonderrolle innerhalb des Netzwerkes versieht, um die händische Abnahme von Anlagen zu ermöglichen, um auch den Anlagenbetreibern eine Möglichkeit zu bieten an dem Netzwerk teilzunehmen, die aus bestimmten Gründen die Anforderungen sonst nicht erfüllen können bzw. wollen[9]. Hierbei sei jedoch betont, dass dies der grundsätzlichen Idee eines dezentralen Netzwerks mit freien und gleichen Mitgliedern widerspricht und Anpassungen an der Blockchainarchitektur vorgenommen werden müssten.

Der Ansatz bietet zudem das Potenzial durch den Einbezug von Wetter- und Satellitendaten, die Vertrauenswürdigkeit der Zertifikate noch weiter zu erhöhen und die Betrugsmöglichkeiten noch weiter einzuschränken. Diese sind zudem immer günstiger und in besserer Qualität weltweit verfügbar, was die Skalierbarkeit des Ansatzes stark vereinfacht.

Bei diesem Ansatz wurden insbesondere Photovoltaik- und Windanlagen bedacht. Geothermie, Wasserkraft und weitere nachhaltige Energieproduktionsformen wurden nicht in Betracht gezogen und deren Einbezug müsste in einer weiteren Ausarbeitung des Konzepts eruiert werden.

Schließlich sei erwähnt, dass eine zentrale Annahme des Ansatzes ist, dass dieser davon ausgeht, dass die Stromproduktion unmittelbar mit der Wasserstoffproduktion verbunden ist und keine Übertragung des Stroms durch das Stromnetz erfolgt. Diese Annahme ist in der realen Welt mit Blick auf den Anspruch des Projekts den gesamten europäischen Wasserstoffmarkt abzubilden, nicht haltbar. In Kooperation mit Netzbetreibern ist aber auch hier eine Erweiterung des Ansatzes denkbar, wobei letztlich eine Verknüpfung des eingespeisten Stroms mit der Entnahme ebendieses Stroms zur Wasserstoffproduktion hergestellt werden muss. Das scheint technisch umsetzbar zu sein, wobei hier vermutlich das Problem bestehen bleibt, dass man nicht den "gleichen" Strom verfolgen kann, sondern lediglich eine bilanzielle Erfassung für das Stromnetz verwenden kann.

Abschließend kann festgehalten werden, dass die hier vorgestellte dezentrale Authentifizierung einen aussichtsreichen Ansatz für die Lösung des Oracle-Problems im Kontext des Wasserstoffmarkts darstellt. Um eine abschließende Evaluation durchzuführen ist eine tatsächliche Implementierung des Ansatzes unausweichlich.

[7] Hierbei sei erwähnt, dass ggf. Zwei Geräte angeschafft werden: eins für die unternehmensinterne Blockchain und eins als Node für die öffentliche Blockchain.

[8] Diese können neben der Anforderung die eigenen Daten auf einer internenen Blockchain zu speichern auch darin bestehen bestimmte IoT Geräte verwenden zu müssen.

[9] In diesem Fall würde alleinig das UBA die Authentizität der Daten anstatt einer Vielzahl von (unbekannten) Authentifzierern bezeugen.

Literaturverzeichnis

[1] Directorate-General for Energy, “Delegated regulation on Union methodology for RFNBOs”, European Commission, C(2023) 1087.

[2] V. Wannack, „Blockchain Based Hydrogen Market (BBH2) - A Paradigm-Shifting, Innovative Solution for a Climate-Friendly and Sustainable Structural Change”, 22. Nachwuchswissenschaftler*innenkonferenz (NWK), Vol. 2 (2022).

[3] Bundesministerium für Wirtschaft und Energie, Bundesministerium der Finanzen, „Blockchain-Strategie der Bundesregierung“ (2019).

[4] Bundesministerium für Wirtschaft und Energie, „Die Nationale Wasserstoffstrategie“ (2020).

[5] G. Caldarelli, „Understanding the Blockchain Oracle Problem: A Call for Action”, Information (2020), 11, 509.

[6] E. Neumann, “Existenznachweise für Daten in unternehmensübergreifenden Blockchain-Netzwerken“, 22. Nachwuchswissenschaftler*innenkonferenz (NWK), Open Conf Proc 2 (2022).

[7] Trusted Computing Group, “TPM 2.0 - A Brief Introduction” (2019).

[8] X. Zhu, Y. Badr, “Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions”, Sensors 18 (12), 4215 (2018).

Opportunities and Limitations of Decentralization in Decentralized Science

Bence, Lukács[1], Benjamin Heurich[1], Lukas Weidener[2]
[1)] Institute for Applied Blockchain (IABC), Berlin, Germany
[2)] UMIT Tirol, Hall in Tirol, Austria

Decentralization is one of the key attributes associated with blockchain technology. Among the different developments in recent years, decentralized autonomous organizations (DAOs) have been of growing interest. DAOs are currently a key part of another emerging use case, namely decentralized science (DeSci). Given the novelty of the field, an integrative definition of DeSci has not been established, but some inherent concepts and ideas can be traced back to the Open Science movement. Although the DeSci movement has the potential to benefit the public, for example through funding underrepresented research areas or more inclusive and transparent research in general, some negative aspects of decentralization should not be neglected. Due to the novelty of blockchain and emerging use cases, research can and should precede mass adoption, to which this paper aims to contribute.

1. Introduction: The decentralization of scientific processes

Over the last few decades the scientific community and its processes have undergone various phases of change. While the scientific method remained open and accessible for anyone to make use of, institutions started to close their doors and retreat further within their walled gardens. It can be argued that through incremental closing of scientific institutions and its processes, innovation and development was hindered, as there weren't any feedback-mechanisms available for the public and society at large. Additionally, through this insulation, parts of the scientific system became more profit-driven in order to (simply) survive and upkeep the status quo of the previously gained reputation. Most recently, this centralization and in-transparency resulted in major issues, such as the *Reproducibility Crisis* [1], corruption of the peer-review [2] and publication processes [3].

Some countermeasures were taken, starting with the Open Access movement, which generally focused on the accessibility and availability of scientific publications for a broader public through open licensing. Then the Open Science movement further expanded openness principles within the scientific community and started to encourage the building of open structures, fostering collaboration and enabling society and its citizens to take a bigger part of knowledge creation. The most current iteration within scientific processes is based on the principles of decentralization. As we will further expand on in the following pages, technological decentralization offers scientists and the scientific community, as well as society at large, a new way of operating. Because of these new developments and the urgency to solve the aforementioned issues, it becomes especially important for the scientific community to take a scientific approach to these new technological developments, and objectively reflect on what the current state, as well as what the risks and benefits for the field are, i.e. research should precede mass adoption, which this paper aims for.

2. Decentralization Paradigm (DLT and Blockchain technology)

Decentralization, Distributed Ledger Technology (DLT), and Blockchain are interconnected concepts that have gained significant attention from a sociological perspective. Sociologists have recognized the potential of decentralization, DLT, and blockchain to transform social structures and power dynamics. These technologies can promote greater inclusivity, reduce reliance on centralized authorities, and enable direct participation and cooperation among individuals and groups. However, it is essential to critically examine their implementation to address potential challenges and ensure that they align with sociological principles of equity, fairness, and social justice. As these technologies continue to evolve, a social-scientific analysis will continue to play a vital role in studying their societal impact, ethical implications, and potential to reshape social relations.

In sociology, decentralization refers to the distribution of power, authority, and decision-making across multiple nodes or actors within a social system. It is the opposite of centralization, where power and control are concentrated in a single authority or entity. Decentralization aims to empower individuals or smaller groups, promoting autonomy and participation in decision-making processes. Descriptively speaking, decentralization can foster cooperation, collaboration, and democratic practices within various social structures, such as organizations, communities, or governments.

2.1 DLT and Blockchain

Distributed Ledger Technology (DLT) as a technological framework that enables the decentralized storage and management of data across multiple nodes or comput-

ers has the potential to sustainably carry this development, if implemented and governed accordingly. Instead of relying on a central authority or database, DLT distributes the data across a network of participants, creating a tamper-resistant and transparent system. So, from a sociological perspective, DLT can be seen as a manifestation of decentralized organizational principles in technology. By removing the need for intermediaries and allowing direct peer-to-peer interactions, DLT promotes trust and cooperation among network participants, facilitating consensus-building and democratic decision-making.

Blockchain is a specific type of DLT that operates on a chain of blocks. All blocks are linked together in a chronological and immutable sequence, making it virtually impossible to alter previous records without consensus from the network making it a potent tool for achieving transparency and accountability in various domains, including finance, supply chain management, and governance. By ensuring data integrity and decentralization, blockchain can create a more equitable and trustful environment where participants have increased control over their data and interactions.

2.2 Characteristics of decentralized technologies

Thanks to these characteristics, DLT and blockchain have the potential to revolutionize various industries, including science and academia. The decentralized nature of these technologies ensures data integrity, traceability, and immutability, thereby enhancing trust and reducing the need for intermediaries. Applying the decentralization paradigm to scientific research and data management can foster open collaboration, data sharing, and reproducibility, ultimately promoting the advancement of knowledge. Researchers can use blockchain to timestamp and store research data, ensuring its authenticity and preventing data tampering. This creates a transparent and trustworthy record of research findings, enhancing the integrity and credibility of scientific publications. Moreover, decentralized funding platforms powered by blockchain can facilitate direct peer-to-peer funding for research projects, bypassing traditional funding agencies and streamlining the process.

3. Open Science, DeSci and the emergence of DAOs

Open Science (OS), as defined by UNESCO in their 2021 publication aims to alleviate many of the issues mentioned at the beginning of the paper. The OS principles are based on three pillars, which (1) increases collaboration among scientists through sharing research openly, (2) involves the global (scientific) community, as well as citizens, by focusing on accessibility (e.g., multilingual) and (3) extends the scientific process outside of traditional scientific institutions [4]. Among the key words included within the *openness* context for science are open accessibility and availability of research output, open data, open-source software, and open infrastructure.

By promoting transparency on different levels and supporting all approaches toward openness in the research process, OS aims to democratize access to scientific knowledge creation. Through following the aforementioned principles, other researchers can replicate and validate scientific findings, thereby enhancing their reliability and credibility, and give society at large easier access in order to validate the need for research and benefit from it. The OS movement has led to some important changes in the scientific publishing landscape, with an increasing amount of scientific literature being accessible to the public without cost. Furthermore, the OS movement has led to the establishment of preprint servers, enabling researchers to share their findings with the community before undergoing peer review for formal publication.

The principles of OS align closely with those of Decentralized Science (DeSci) since both movements advocate for the democratization of scientific knowledge and the use of (open) technology to facilitate the sharing and collaboration of scientific research. However, while OS primarily focuses on the openness of the research process and increased collaboration, especially the replicability of results, DeSci extends this idea to include the decentralization of the research infrastructure, leveraging blockchain technology, and other Web3 technologies to create a more equitable, participatory, and inclusive scientific ecosystem.

3.1 DeSci as an extension of Open Science principles

DeSci represents a novel movement in the scientific domain, with no universally accepted definition to date. A widely referenced definition, provided by the Ethereum Foundation, describes DeSci as “a movement that aims to build public infrastructure for funding, creating, reviewing, crediting, storing, and disseminating scientific knowledge fairly and equitably using the Web3 stack” [5]. Although blockchain technology is not explicitly mentioned in this definition, it is an integral component of the Web3 stack and plays a pivotal role in the operationalization of DeSci. Blockchain technology and especially the associated features and applications such as smart contracts, governance tokens or NFTs, are fundamental to the current DeSci ecosystem. To summarize, DeSci bears significant parallels with the OS movement, as Web3 technologies serve to extend the principles by incorporating novel technological advancements (i.e. data storage, collaboration mechanisms and funding procedures).

3.2 DAOs as new structures for scientific processes

Essential to the current DeSci movement are Decentralized Autonomous Organizations (DAOs). This type of organization represents a novel form of organizational structure enabled by blockchain technology. While there is no universally accepted definition for DAOs, for the purpose of this publication, we will adopt the definition

provided by the World Economic Forum (WEF): "Decentralized autonomous organizations (DAOs) are structures that use blockchains, digital assets, and related technologies to direct resources, coordinate activities, and make decisions" [6]. The term DAO was first prominently introduced in relation to 'The DAO' in 2016, an ambitious project built on the Ethereum blockchain that aimed to operate as a leaderless venture capital fund [7]. Despite its eventual downfall due to a security breach, The DAO served as a significant milestone in the exploration of decentralized governance models.

In the definition by the WEF, 'digital assets' likely refer to governance tokens, which are utilized in the decision-making process over shared resources (e.g., shared monetary funds as part of a treasury) and activities within the DAO (e.g., funding scientific research). These tokens often represent voting rights, allowing token holders to influence the direction of the organization.

The 'related technologies' within the context of the definition of the WEF likely primarily refer to smart contracts, which are fundamental to the autonomous operation of DAOs. By utilizing smart contracts, DAOs can automate (trans-)actions such as funding research or paying for services, once a decision-making process, typically in the form of on-chain voting, has been completed.

DAOs play a significant role in the current DeSci movement and represent a paradigm shift in organizational structures and governance models, challenging traditional centralized authority with a decentralized, transparent, and democratic approach. However, the practical implementation of DAOs presents a host of challenges and complexities, ranging from technical and security issues to legal and regulatory considerations. In particular, within the context of DeSci, the challenges associated with DAOs will be the context of this publication.

3.3 DeSci DAOs: More than theory – VitaDAO

DeSci-DAOs aim to provide a new method of participation, inclusivity, and accessibility to science. By leveraging the capabilities of the Web3 stack, including blockchain technology, smart contracts, and Non-Fungible Tokens (NFTs), DeSci-DAOs have the potential to revolutionize the scientific landscape. As of the current writing period, a significant proportion of DAOs have predominantly concentrated their efforts on fields such as medicine, natural sciences, and biotechnology. This focus, while offering substantial potential for invigorating research areas that traditionally suffer from underfunding (such as rare diseases), also introduces a new set of challenges and risks (e.g., safety and control of decentralized biological research).

Table 1. Selection of DeSci-DAOs

DeSci DAO	Objectives
VitaDAO	Funding and advancing longevity research
HairDAO	Research support and funding to cure hair loss
ValleyDAO	Financing and democratizing the governance of synthetic biology technologies
BeakerDAO	Decentralized funding of the DeSci ecosystem
CerebrumDAO	Funding solutions to advance brain health and prevent neurodegeneration

At the time of writing, the VitaDAO community comprised approximately 10,000 members, with over 2,000 individuals holding the available governance token ($VITA). These governance tokens play a pivotal role in decision-making processes within the DAO, particularly in matters such as the allocation of funds for longevity research [8]. To date, VitaDAO has successfully raised in excess of $10 million, a portion of which originates from Pfizer Ventures, a traditional pharmaceutical sector entity [9]. This investment from a conventional sector player underscores the growing interest and potential of this novel approach to scientific research and funding. VitaDAO has already funded more than 15 projects, with research areas spanning various aspects of longevity science [10].

4. Risks and benefits of decentralized scientific processes through DAOs

4.1 Benefits for science

This section explores the potential benefits of DeSci ranging from funding underrepresented research areas to enhancing transparency, participation, and interdisciplinarity in the scientific process.

4.1.1 Funding

One potential benefit of DeSci is the funding of underfunded research areas. A prime example of this is HairDAO, a DAO "that is advancing research and development for hair loss treatments in an open-source and democratic way" [11]. Hair loss, specifically androgenic alopecia, is a condition that has been overlooked by traditional pharmaceutical research, despite causing a high level of suffering among those affected. Androgenic alopecia is a common form of hair loss in both men and women, and genetic and hormonal factors play significant roles. Research in this area is crucial, as it not only seeks to provide solutions for those suffering from hair loss, but also contributes to our understanding of human biology and aging.

4.1.2 Transparency and Trust

Increased transparency in the scientific process, which includes research, reviewing, publishing, and access to research, is a cornerstone of the OS movement and a key aspect of DeSci. Transparency is instrumental in fostering trust through better replicability. The replication crisis in various scientific fields has raised concerns regarding the reliability of scientific findings and the validity of policy and action items that were based on certain research. OS and DeSci, with their emphasis on technological, as well as methodological transparency and openness, provide a solution to this crisis. Moreover, transparency in the scientific process can lead to increased participation and access to the overall research process and provides more feedback opportunities for citizens. This is not limited to researchers, but extends to non-researchers as well, such as patients or patient advocacy groups. People interested in a specific topic or research can contribute based on their experiences and skills, even anonymously, without the need for specific degrees. The democratization of participation in the scientific process is a significant benefit of DeSci.

4.1.3 Interdisciplinarity

The concept of interdisciplinarity in the context of OS and DeSci is gaining traction in the academic community. It is increasingly recognized that the complex problems of today's world often require insights from multiple disciplines. However, in traditional scientific research, there are often barriers to such interdisciplinary collaboration, including institutional structures and norms that tend to compartmentalize knowledge within specific disciplines. DeSci, with its emphasis on open collaboration and decentralized governance, has the potential to break down these barriers. By leveraging the capabilities of the Web3 stack, DeSci can facilitate collaboration among researchers with diverse backgrounds and expertise regardless of their institutional affiliations. This can stimulate the exchange and fusion of ideas and knowledge from diverse fields, catalyzing innovative solutions to complex problems.

4.1.4 Protection and Management of Intellectual Property (IP)

Another significant advancement that DeSci can offer in comparison with traditional scientific practices is a novel approach to the protection and management of intellectual property (IP) rights. In conventional systems, the creation and management of IP rights are complex processes that often involve a multitude of stakeholders, including researchers, academic institutions, and corporate entities [12]. This complexity, coupled with the high value associated with IP rights, often results in limited accessibility and transparency for researchers and the public. Furthermore, the existing process can lead to a concentration of IP ownership among certain well-funded entities such as pharmaceutical companies. In contrast to this traditional, time-consuming, and cost-intensive IP management process, DeSci introduces the concept of Intellectual Property Non-Fungible Tokens (IP-NFTs) [13]. These are unique tokens that represent intellectual property assets on the blockchain. Their non-fungibility and ability to tokenize intellectual property rights have significant implications for the funding and conduct of scientific research. By converting intellectual property into a tokenized form, researchers can protect their findings and attract funding in a more cost-effective, time-efficient, and transparent manner. In the context of DeSci, IP-NFTs serve as a bridge between intellectual property and the web3-mediated scientific landscape, allowing scientists to tap into a new source of funding for their research and transact on their discoveries in a novel manner.

4.1.5 Translational research

DeSci holds the potential to expedite translational research, often encapsulated by the phrase "from bench to bedside" [14]. This process involves the application of basic scientific discoveries made under laboratory conditions (the 'bench') to patient care (the 'bedside'). However, the journey from bench to bedside can be slow due to the multi-stage nature of research, which includes clinical trials and the presence of regulatory, administrative, and funding-related barriers [15]. By leveraging the web3 stack, including blockchain technology and DAOs, DeSci can facilitate translational research through increased data and result sharing, interdisciplinary collaboration, and transparency.

4.1.6 Censorship resistance

Another potentially significant benefit of DeSci is its reduced level of censorship in the scientific research process. In the traditional scientific system, universities and grant providers such as the government or pharmaceutical companies significantly impact the current research landscape by providing funding only to research they evaluate as valuable [16]. These entities may choose to fund research that aligns with their own interests or perceived societal value, which can result in underfunding in certain research areas such as rare diseases. This selective funding can also lead to a form of censorship where high-impact research that does not align with the interests of these entities may be overlooked or suppressed. DeSci, with its decentralized and democratic approach, offers a potential solution to these challenges. By decentralizing the funding and decision-making processes, DeSci can ensure a more equitable distribution of resources and reduce the potential for censorship, thereby fostering a more diverse and inclusive scientific research landscape.

4.2 Unique challenges for science

The decentralization of science through DeSci and the web3 stack, while offering numerous benefits, also presents a set of unique challenges and risks.

4.2.1 Accountability

One primary concern is accountability. By their very nature of being potentially fully decentralized and autonomous, DAOs can face difficulties in attributing responsibility in cases of fraudulent or unethical scientific activities. As mentioned in the previous section, the openness of DAOs and the possibility of participating in the scientific process either pseudonymously or anonymously can lower the barriers to entry and increase interdisciplinary collaboration. However, this could also provide an avenue for individuals to pursue personal agendas that could mislead other participants or skew the overall research process. Although the decision-making process in most DAOs is not fully decentralized (yet) and is overseen by elected core members who represent the interests of the organization, there is a risk that these core members could collude to influence the community based on their personal interests.

4.2.2 Decision-making

The token-based voting and decision-making processes inherent to DAOs, while democratizing and inclusive, also present potential risks. The decentralization of decision-making power to token holders can lead to a situation in which the majority's interests may not always align with the broader public or the organization's mission. This is particularly relevant in the context of DeSci, where the research agenda and allocation of resources could potentially be influenced by a minority of token holders with significant voting power. This risk is further amplified in the early stages of a project, when a majority of tokens are often distributed to the public, creating an opportunity for pseudonymous individuals or institutions to accumulate voting rights. This could potentially lead to a concentration of decision-making power, contrary to the democratic ethos of the DAOs. Therefore, it is crucial for DeSci-DAOs to implement robust governance structures and mechanisms to prevent such manipulation and ensure that the decision-making process remains fair, transparent, and aligned with the organization's mission.

4.2.3 (Decentralized) Intellectual Property (IP) Risks

In the context of intellectual property (IP) rights, DeSci-DAOs could potentially own IP rights after funding research, such as through the use of IP-NFTs. Although this approach provides a novel way to fund research and incentivize scientific discovery, it also presents potential risks. For instance, the DAO could potentially limit the use of research findings either by restricting access to the research or by imposing licensing fees. Although this is unlikely, given that the commercialization of IP-NFTs is fundamental to the success of the DAO and the ethos of open science, a significant risk remains if a limited number of individuals (including the founding or “core team”) accumulate tokens. This could potentially lead to a situation in which IP rights associated with a particular research project are controlled by a small group of individuals. Furthermore, the tokenization of IP rights could potentially lead to fragmentation of IP ownership, complicating the licensing and commercialization processes. Another potential risk in the DeSci landscape pertains to the underutilization (or complete lack of utilization) of IP rights owned by a DAO. This could stem from a lack of active participation or voting apathy among the token holders. In a DAO, decision-making processes are typically predicated on a certain threshold of token-holders participating in a vote for it to pass. If this threshold is not met, decisions cannot be made, which could lead to stagnation in the decision-making process and, by extension, under-utilization of IP rights. This could potentially slow down the pace of R&D and discourage members from participating, especially if they view the governance tokens more as a long-term investment rather than an active tool for participation in the DAO's activities. This risk is particularly relevant in the context of DeSci, where the decision-making process can directly affect the direction and pace of scientific research. For instance, decisions related to the allocation of resources for research, the commercialization of research findings, and the licensing of IP rights could be delayed due to voting apathy. This could potentially hinder the progress of scientific research and the realization of its benefits, endangering the overall mission of the DeSci-DAO.

4.2.4 Ethics

Finally, the reduced level of censorship, while being a potential advantage of DeSci, can also pose a significant risk. The absence of traditional governmental or regulatory oversight in the funding and approval process could potentially pave the way for research that is ethically questionable or harmful. For instance, research involving the manipulation of harmful viruses or cloning of humans, which are generally considered ethically and morally contentious, could be pursued without traditional checks in place. In the traditional scientific landscape, research proposals undergo rigorous ethical reviews by institutional review boards or ethics committees that assess the potential risks and benefits of the proposed research. This process was designed to protect the welfare and rights of research participants and ensure that the research was conducted in an ethical manner. However, in DeSci-DAO, where funding and approval decisions are made through a decentralized voting process, it is possible that such ethical considerations may not be adequately addressed.

5. Conclusion: A potential future for/of science

Decentralized Science and its implementation through DAOs present intriguing possibilities for the scientific community. By enabling democratized access to funding and decision-making, DeSci has the potential to revolutionize the scientific landscape. It could foster greater inclusivity, allowing researchers from diverse backgrounds and regions to participate in the scientific process and address a broader range of societal challenges. DAOs, as

self-governing entities, can facilitate collective decision-making in research allocation and project funding. This participatory approach aligns with sociological principles of decentralization and could reduce the dominance of traditional research institutions or powerful funding bodies. Involving a diverse group of stakeholders in the decision-making process may lead to more equitable resource distribution and research prioritization, considering a wider range of perspectives and needs.

However, this transformative potential comes with certain risks that require careful consideration. Governance structures within DAOs may be subject to power imbalances, where certain actors wield more influence than others. Sociologists must examine how decision-making processes within DAOs could be influenced by individual biases, social hierarchies, or external forces. Additionally, the implementation of DeSci must address ethical concerns related to data privacy, data ownership, and accountability. Sociologists should assess how decentralized data sharing and collaboration might impact research ethics, intellectual property rights, and potential misuses of scientific knowledge. Sociological research on DeSci and DAOs is essential to navigate the potential benefits and risks they pose to the scientific community. By addressing issues of power dynamics, accountability, and ethics, sociologists can help maximize the positive impact of DeSci while minimizing potential negative consequences, paving the way for a more inclusive and responsible scientific future.

Acknowledgements / Information on sponsors

Lukas Weidener is a member and investor in multiple DeSci-DAOs and project.

Contact details

Oranienstraße 185, Berlin, 10999 Berlin

Contact persons:

bence.lukacs@iabc.dbuas.de / 0000-0002-3723-6549

Literature references

[1] Baker, Monya (2016): 1,500 scientists lift the lid on reproducibility, Nature 533, 452–454 (2016). https://doi.org/10.1038/533452a.

[2] Petrescu, Maria; Krishen, Anjala S. (2022): The evolving crisis of the peer-review process, J Market Anal 10, 185–186 (2022). https://doi.org/10.1057/s41270-022-00176-5.

[3] Committee on Publication Ethics and STM (2022): Paper mill research, DOI: https://doi.org/10.24318/jtbG8IHL.

[4] UNESCO (2021): UNESCO Recommendation on Open Science, https://unesdoc.unesco.org/ark:/48223/pf0000379949.locale=en, Accessed: 31.07.2023

[5] Ethereum Foundation: Decentralized Science (DeSci). https://ethereum.org/en/desci, Accessed: 31.07.2023

[6] World Economic Forum (2023): DAOs for Impact. https://www3.weforum.org/docs/WEF_DAOs_for_Impact_2023.pdf, Accessed: 31.07.2023

[7] Jentzsch, Christoph. (2017): DECENTRALIZED AUTONOMOUS ORGANIZATION TO AUTOMATE GOVERNANCE, https://lawofthelevel.lexblogplatformthree.com/wp-content/uploads/sites/187/2017/07/WhitePaper-1.pdf

[8] VitaDAO (2021): How VitaDAO Works, https://vitadao.medium.com/how-vitadao-works-61bbf861fe96, Accessed: 31.07.2023

[9] Cumbers, John (2023): Longevity Startup VitaDAO Raises $4.1m, Backed By Pfizer, Balaji Srinivasan, https://www.forbes.com/sites/johncumbers/2023/01/30/longevity-startup-vitadao-raises-41m-backed-by-pfizer-balaji-srinivasan, Accessed: 31.07.2023

[10] DeFrancesco, L., Klevecz, A. (2022): Decentralized investor communities gain traction in biotech.Nat Biotechnol 40, 1310–1315 (2022), https://doi.org/10.1038/s41587-022-01459-z

[11] HairDAO: Landing Page, https://hairdao.xyz, Accessed: 31.07.2023

[12] Fehder, D.C., Murray F., Stern, S. (2014): Intellectual property rights and the evolution of scientific journals as knowledge platforms. International Journal of Industrial Organization (Volume 36) https://doi.org/10.1016/j.ijindorg.2014.08.002.

[13] Molecule: Intro to IP-NFT, https://docs.molecule.to/documentation/ip-nfts/intro-to-ip-nft, Accessed: 31.07.2023.

[14] Feldman AM (2015): Bench-to-Bedside; Clinical and Translational Research; Personalized Medicine; Precision Medicine-What's in a Name? Clin Transl Sci. 8(3):171-3. doi: 10.1111/cts.12302.

[15] Abu-Odah, H., Said, N. B., Nair, S. C., Allsop, M. J., Currow, D. C., Salah, M. S., Hamad, B. A., Elessi, K., Alkhatib, A., ElMokhallalati, Y., Bayuo, J., & AlKhaldi, M. (2022): Identifying barriers and facilitators of translating research evidence into clinical practice: A systematic review of reviews, Health & Social Care in the Community, 30, e3265– e3276. https://doi.org/10.1111/hsc.13898.

[16] Watson, Clare (2021): Health researchers report funder pressure to suppress results. https://www.nature.com/articles/d41586-021-02242-x, Accessed: 31.07.2023.

Tokenization of Ownership Management for Web-of-Things with Role-based Modeling

Orçun, Oruç, Uwe, Aßmann, Maliha Raja
TU Dresden, Dresden, Germany

Currently, the Internet of Things (IoT) is connected to the virtual world through the Web of Things (WoT), allowing efficient utilization of real-world objects with Internet technologies. The WoT facilitates abstract interaction between applications and connected IoT devices, allowing owners to switch between devices while using multiple ones. To achieve this, virtual assets in WoT devices can be tokenized through smart contracts and transferred using hashed proof as transactions within blockchain networks that support virtual currencies. The goal of Web of Things is to establish connectivity, interoperability, and integration among IoT devices using web standards and protocols, reducing reliance on device manufacturers. This enables easy integration of Web 3.0 cryptocurrency for device management. This study proposes a solution for WoT applications involving different cryptocurrency definitions. Finally, simulation results are presented to demonstrate the tokenization-based ownership transfer in the Web of Things.

1. Introduction

Large-scale networks in the Internet of Things (IoT) face challenges, such as fragmented monitoring and isolated data, which impede comprehensive observation. When adopting diverse IoT technologies for different purposes, fragmentation occurs due to varying architecture of each solution. Inventory monitoring involves managing and controlling stocks using various sensors distributed throughout a network. Scalability is essential for end-users to effectively utilize IoT solutions in their business operations. To address these issues, the Web of Things (WoT) has been introduced. It represents virtual objects as proxies for abstract entities linked to physical objects. Each „thing" is defined with metadata, events, and properties, enabling communication and management of WoT devices through a messaging framework or design pattern.

Application development is challenging and complex when it comes to Internet of Things (IoT) devices due to the diverse standardization of programming interfaces and communication protocols among different IoT platforms. For example, Arduino, Raspberry Pi, and BeagleBone are three common development boards used in IoT programming, and developers must write applications specific to each board's specifications. Consequently, this poses difficulties when transitioning an application from one protocol (e.g., OPC-UA) to another protocol (e.g., COAP). One of the primary objectives of the Web of Things (WoT) architecture is to provide a unified framework that spans from micro controller-level devices to cloud-based applications [1].

Ensuring data and application ownership is vital in complex applications, such as supply chain simulations involving retailers, wholesalers, and manufacturers. In such simulations, product tags must be shared and authenticated among members. Radio Frequency Identification (RFID) technology is commonly used to tag products in warehouses or items on assembly lines, consisting of components like RFID tags, RFID readers, and RFID-tag database. Each asset is represented by an RFID tag registered in the database, which may contain ownership-related data. Applications utilizing RF tags facilitate the transfer of ownership between parties. Data ownership in the Web of Things is also another important factor to protect accessing, processing, or getting benefits from economic exploitation. For instance, parties of Web of Things should be in an agreement to initiate access, processing, or economic exploitation of data. Ownership can be thought of as control and data ownership including access, create, modify, package, sell or remove data, and access privileges to others [2].

Traceability and auditability are essential functions for ownership transfer within a single network. The list of involved parties should be registered in the network to ensure data ownership in the Web of Things (WoT) applications. Cryptocurrency items, operating directly on the blockchain layer through autonomous programming entities (smart contracts), can provide traceability and reliable ownership transfer for WoT. Tokens, representing the token economy using Web3.0 technology, serve as a conceptual representation of ownership. The distinctiveness of tokens economy, proof of ownership plays a significant role in determining the priority of the communi-

[1] https://www.w3.org/2015/05/wot-framework.pdf

[2] https://ori.hhs.gov/education/products/n_illinois_u/datamanagement/dotopic.html

cation environment between WoT nodes. Another notable aspect is asset tokenization, which converts tangible and intangible assets into traceable digital tokens. Each token type, whether representing a fraction or the entirety of ownership, enables manageable and trackable ownership of assets[3].

Main contribution and research questions: The main focus of this research is to introduce a transparent and tamper-proof dataset that provides traceable records for ownership transfer in Web of Things devices. In this specific application, the need for multiple data tags between parties is eliminated by utilizing non-fungible fractional tokens (Fractional NFTs) and fungible tokens. Additionally, the concept of Fractional NFTs can be integrated to role-based self-sovereign identity, abstracted by smart contracts, to fulfill particular roles such as Issuer, Verifier, and Holders.

This study demonstrates the integration of these elements to achieve a seamless and secure ownership transfer mechanism for Web of Things devices.

1.1 Research Questions

In this research study, we would like answer the following research question to struct the main objective of this thesis.

1) How can different cryptocurrency interfaces be integrated with Web of Things ownership entities?

2) How can self-sovereign identity features such as Issuer, Verifier, and Holder be implemented through smart contract programming in Web of Things solutions?

2. Background

2.1. Identity and Data Management

The establishment of secure and reliable interactions among WoT devices of utmost importance, necessitating the utilization of unique identities for devices and entities. Identity management solutions such as digital certificates, public-key infrastructure (PKI), or decentralized identity frameworks such as Self-Sovereign Identity (SSI) can be employed to fulfill this requirement. The present study primarily focuses on SSI, aiming to differentiate it from crpytocurrency-based interactions. It is imperative that Identity and Data Management adhere to principles of data ownership and governance, as authorized access could have detrimental effects on the entire WoT ecosystem. Therefore, the safeguarding of data privacy and content assumes paramount significance, necessitating the application of modern encryption techniques such as HTTPS or MQTT-TLS. While blockchain technology does offer a certain level of security, this aspect should not be disregarded.

2.2 Cross Domain Collaboration

In the realm of technological advancements, the Web of Things (WoT) emerges as a potent force, facilitating effortless interaction and collaboration among diverse entities across multiple domains. It empowers devices, platforms, and services from disparate domains to collaborate their efforts and work harmoniously towards the achievement of shared objectives. In order to foster cross-domain collaboration, it becomes crucial to establish a robust foundation and interoperability among data models, standard protocols and interfaces. In Figure 1 illustrates a fundamental interaction between ownership transfer and web of things ecosystem, exhibiting the interconnectedness and significance of these elements in the WoT landscape.

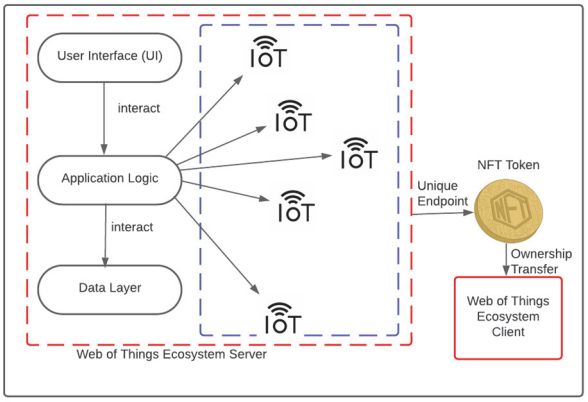

Fig. 1: Web of Things Ecosystem Demonstration Through Client and Server

2.3 Role-based Modeling

Role-based modeling elucidates how objects can take on diverse roles in multiple collaborations, effectively representing multiple identities. Due to the inherent nature of objects, each object must embody a single identity upon its creation. However, to represent distinct roles or multiple identities within a single object, we need to construct a player relationship through mixins, traits, design patterns (e.g. decorator, mediator, adapter, role object patterns) or subtyping. In the context of this study, roles are generated using modified mediator pattern with "lockNFT()" function, which facilitates the division of a Non-Fungible Token (NFT) into multiple holders through the involvement of an issuer and verifier. This approach enables the representation of various roles and identities within the context of the NFT ecosystem.

2.4 Democratizing Ownership

It refers to the concept of decentralizing ownership and empowering entities to have control other devices. These entities may have influence over the devices, data, and services within the WoT ecosystem. Individual nodes

[3] https://due.com/blockchain-asset-ownership/

should be empowered with greater control and autonomy over devices and services in the WoT.

2.5 Self-sovereign Identity

Self-sovereign identity minimizes the reliance on third parties and instead promotes a decentralized approach to private authentication storage, enabling individuals to manage their identities and access to them [1]. With this definition, it becomes apparent the smart contract technology can empower individuals with ownership and control over personal data related to ownership. Upon deploying a smart contract, true decentralization is achieved as individuals gain full control over the data layer of the smart contract. The use of smart contracts eliminates the centralization of control, as every node in the network must synchronize with the latest version of the smart contracts.

2.6 Types of Cryptocurrencies

Within the domain of digital currency, a range of token standards are available, including ERC-20, ERC-721, ERC-1155 and ERC-3475. These tokens can be utilized in single or multiple smart contracts, depending on their specific requirements and definitions. Through the facilitation of token transfers. Web of Things (WoT) devices can effectively monitor transactions between devices and allocate computing resources based on token expenditure. The tokenization of smart contracts also enables the development of decentralized applications (dApps). In the context of dApps designed for groups of IoT devices, the implementation of multiple replicated transaction ledgers becomes feasible without the need for a central authority.

The ERC-20 interface is widely employed across a range of scenarios within the blockchain industry. It provides a comprehensive set of functions that enable the efficient distribution of tokens within a blockchain network. These functions encompass obtaining the total token supply, verifying the balance of an account, managing allowances, executing token transfers, granting approval for token usage, and facilitating transfers between accounts. Consequently, it can be inferred that ERC-20 tokens should possess the capacity to retrieve the total token supply, evaluate the balance of designated accounts, facilitate seamless token transfers, and authorize token usage.

In response to the shortcomings of the ERC-20 token standard, the Ethereum community has proposed the ERC23 and ERC223 token standards. These proposed standards aim to address the following issues: lost tokens, lack of event handling, optimization of ERC20 address-to-contract communication, and disparities between Ethereum and Token Transfer mechanisms [4] [5].

Introducing an interface for managing various token types, including fungible, non-fungible, and semi-fungible tokens, ERC-1155 enables the deployment of a single contract that consolidates these token types. This consolidation eliminates the need for separate contracts associated with different token standards, such as ERC-20 for fungible assets and ERC-721 for non-fungible assets. The approach of consolidating token types within a single contract mitigates the issue of opcode bloat in the blockchain virtual machine. An illustrative example of leveraging this capability can be seen in the case of Gnosis [6], a company that utilizes conditional tokens to address multiple use cases while reducing gas costs for users by considering potential future outcomes in trading. Similarly, within the context of ownership transfer, this type of token holds potential for various scenarios involving the transfer of ownership within Web of Things (WoT) devices.

ERC-3475 is a standardized interface for contracts that handle multiple callable bonds. This standard entails a more intricate data structure than ERC-20, but it offers distinct functions to facilitate the reading and transfer of bond collections, as well as the issuance and redemption of bonds. By utilizing ERC-3475, it is possible to create numerous types of bonds within a single contract. Each bond is associated with a "classID", which allows for the definition of new configurable token types.

ERC-725 and ERC-735 have been created to address blockchain-based identity solutions and involve the implementation of proxy smart contracts that can be managed by other smart contracts. These standards are specifically designed to cater to Self-Sovereign Identity use cases within blockchain applications. The key distinction between ERC-725 and ERC-735 is that the former represents the identity itself, while the latter represents the claims associated with the identity.

ERC-223 was introduced to address a significant bug in the ERC-20 standard for token exchanges. This bug was specifically related to the "*transfer()*" function within the blockchain network. In the case of transferring tokens to an externally owned account (EOA), the transfer could appear successful even if the EOA did not receive the tokens properly, potentially resulting in the token being permanently lost or burned. As a solution, ERC-223 proposed new standards for the "*transfer()*" function within the ERC-20 standard, aiming to rectify this issue.

---

[4] https://github.com/Dexaran/ERC223-token-stan-dard

[5] https://github.com/iam-dev/ERC23

[6] https://www.gnosis.io/

ERC-667 seeks to combine the functionalities of both ERC-20 and ERC-223 standards, specifically focusing on enabling seamless token transfers and "*call()*" functions. Its primary objective is to facilitate token transfers through triggered contracts within a single transaction.

The ERC-721 standard is used to establish ownership of Non-Fungible Tokens (NFTs). Unlike ERC-20 tokens, NFTs cannot be treated interchangeably due to their unique properties. Essentially, ERC-721 serves as a token standard specifically designed for non-fungible assets. Common use cases for ERC-721 can include digital artwork, game collectibles, gaming characters, and art images.

ERC-173 establishes a standardized interface for contract ownership. Important aspects of ERC-173 include:

- The standard aims to minimize the number of functions in the interface to prevent contract bloat.
- ERC-173 provides backward compatibility.
- ERC-173 efficiently organizes the gas cost associated with smart contracts and this standard introduces a new approach for interacting with token contracts, ensuring compatibility with the ERC-20 Fungible Token Standard[7].

ERC-875 facilitates the use of non-fungible tokens by enabling the bundling of tokens into groups. This allows for peer-to-peer atomic transfer to occur within a single transaction. Essentially, atomic transactions guarantee that all internal transactions will either succeed or fail together.

ERC-918, known as the Mineable Token Standard, is a specification outlined in Ethereum Improvement Proposals. It relies exclusively on mining activities conducted through the Proof-of-Work concept. This standardization is commonly referred to as „Proof of Work Minting."

ERC-2615 is an extension to ERC-721 non-fungible token standard (NFT) to support rental and mortgage functions. This interface has been produced for real-world entities in the world such as mortgage agreements, real property with written agreements.

ERC-4626 is a standard for tokenized vaults that utilize ERC-20 tokens. It encompasses common functions like *transfer*, *transferFrom*, *balanceOf*, and *totalSupply*. This token type enables users to gain profits from their stakes. However, this token type does not address the security aspects between endpoints in a decentralized network. On the other hand, the Sealed NFT Metadata (ERC-3569) introduces a smart contract-based mechanism for immutable NFT metadata [8]. Both ERC-4626 and ERC-3569 are open standards, which means that they can be used in a mixed way through correct interfaces. This allows developers to create more complex and sophisticated applications that utilize the benefits of both standards.

All of these token types can be used in a mixed way through the appropriate interfaces. The specific implementation can vary based on requirements, but in this case, we have utilized the ERC-721 and ERC-20 standards to create the Fractional NFT.

3. Motivation and Challenges

In the context of supply-chain applications, ownership plays a crucial role in the transfer of goods between various participants such as retailers, manufacturers, and wholesalers. As an example, a tagged object can be moved from a manufacturer to a retailer. It is important to have visibility into the origin of the data source, the creation timestamp, and the expiration date at this stage. However, ensuring secure transfer of ownership between different data owners remains an ongoing research challenge. In this study, we aim to explore the feasibility of using different token types to address this challenge. By implementing a fully trustworthy ownership model using a block explorer, we can transparently track ownership through the Merkle tree data structure. Transactions between parties will be identifiable through the use of different token types. Last but not least, we would like to show the main case study to demonstrate technical challenges and theoretical limitations with regards to this research study.

4. Related Work

4.1 Web of Things and Ownership Transfer

Authors [2] describe for ownership transfer mechanism in the area of medical IoT devices [2]. According to authors, ownership principle can be transferred through immutable chained blocks by means of smart contracts addresses. Medical Internet of Things device owners can set some rules and conditions for access and modify the records pertaining to the Medical IoT device ownership [2]. Another study shows us how using blockchain technology can provide unique identifiers for IoT devices through records immutability [3]. In this study, while deploying an IoT system, the owner of the device dictates the transfer of ownership [3]. Transferring the device ownership will require a transfer process in a secure manner or device ownership can split between different owners. For instance, an IoT device can be held by tenants and a lender companies. According to the authors [3], large IoT infrastructures must be managed and controlled from a security perspective. One of the core problem in such big IoT systems is the lack of forward and backward secrecy with respect to the old and new owners. To solve this problem, the authors [3] offers a solution called BYODID (Bring-Your-Own-Device-Identity) to

[7] https://eips.ethereum.org/EIPS/eip-777

[8] https://eips.ethereum.org/EIPS/eip-3569

ensure a single user can have a transferable identity from one enterprise to another.

Each IoT device has a form of credentials that must be shared with a remote entity. According to the authors, ownership transfer is the process of updating the credentials on a protocol layer [6]. The ownership transfer process should be divided into three phases: deployment, ownership transfer preparation, and ownership transfer [6]. Even though this protocol design was designed for large IoT infrastructures, there is no real case study to evaluate the performance of ownership transfer protocol.

In order to protect privacy leaks, authors [8] proposed an automated ownership that would be triggered in the event of any ownership change. They proposed an automatic handling of ownership, which is the first system without user interaction during ownership change [8].

4.2. Security Challenges of Web of Things

Web of Things (WoT) is expected to make accessibility of smart things easy and promote by combining novel values according to the identity management such as ownership, identification, and social security [4]. Authors of the paper [4] concluded that authentication schemes like OAuth, JWT are not adequate to provide ownership transfer mechanism in WoTs.

Ownership transfer should be provided in a supply chain and changing ownership occurs when a wholesaler delivers tagged products to a retailer [5]. The authors of the paper [5] basically conducted a survey how to allow the secure and seamless transfer of ownership of RFID-tagged objects from one owner to another owner. As the authors stated, ownership transfer in IoT is generally supplied with Ownership Transfer Protocols (OTP), so one should take consideration of a particular protocol while deploying IoT applications regarding ownership transfer [5].

Burmester et al. [7] defines three steps of ownership transfer control, which are:

a) Preparation of a tag to be owned by another user.

b) Employing a trusted third party for a trustable link between current and new user.

c) Taking control of delivered tag when the protocol is completed.

In the conclusion of this paper, authors stated that preventing unauthorized tracking and secure ownership transfer are two major problems that need to be solved [7].

4.3. Token Types

Angelo et al. mention that security tokens are helpful to simulate the behavior of issuer, verifier, and holder [9]. Ownership transfer in cryptocurrency can be achieved through token contracts and *safe transfer* is a particular mechanism where token withdraw from an address or transferred to an address. While implementing this process, role-based authentication with lock control can be defined in the token contract [9]. Moreover, ownership transfer mechanism activities can be logged through cryptocurrency specific events [9].

Tokens can be categorized, according to di Angelo et al., into payment tokens, security tokens and utility tokens [9]. According to die Angelo et al., security token standards are proposed and discussed but not yet finalized [9]. Even in the Ethereum Mainnet, function signatures of security tokens are sparse, so one can assume that it is still an emerging technology yet [9].

5. Implementation

5.1. Design of the Use Case

The use case in Figure 2 has been successfully accomplished using Hardhat and the Solidity language package. These tools have been employed to showcase the fundamental functions of the use case, as well as the logic behind the issuer, verifier, and holder roles. In this implementation, the holder assumes the role of managing a specific data type within the Solidity language. As the holder, their responsibility is to safeguard the identification medium required by the verifier. On the other hand, the verifier is granted the authority to verify the identification medium on behalf of the issuer.

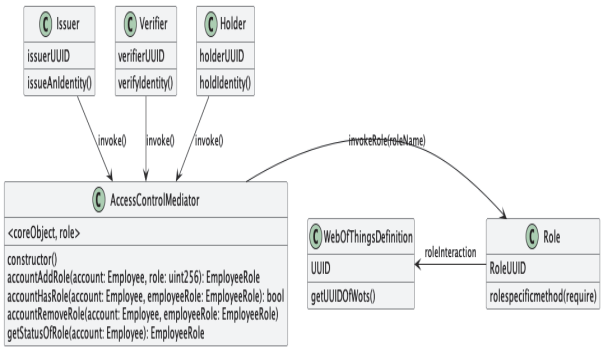

Fig. 2: Class Diagram for Access Control Mediator, Issuer, Verifier, Holder, Role, and WebOfThings Definition

In the use case scenario, inventory tracking in a warehouse has been implemented. According to the use case, the following activities are involved: receiving, inspection, putaway, storage, packaging and shipping. Basically, updating an inventory record and updating a storage record are accomplished by roles generated through the mediator pattern. Additionally, to achieve inventory tracking, fractional NFTs will be shared among WoT Devices.

6. Result

In order to assess the outcomes of proposed application in a qualitative manner, we aim to evaluate the incurred expenses related to both execution and deployment of the smart contract. By examining the costs associated with these aspects, we can obtain valuable insights into

the financial implications of the application's implementation.

6.1. Quantitative Evaluation

Operation performance in terms of time calculation is crucial to understanding the efficiency of multiple contracts involved: the verifier, issuer, holder, and web of things identity processes. In Figure 3, deployment cost of self-sovereign identity is relatively big because smart contract role creation has a lot of interactions among each other. However, as can be seen in Figure 4, execution costs of smart contract are relatively high in the context design pattern role creation contract (Administrator contract).

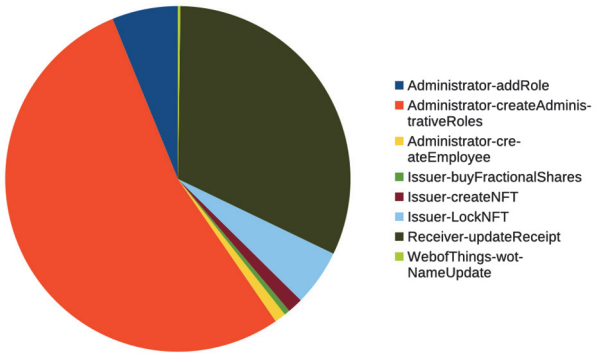

Fig. 3: Smart Contract Deployment Cost

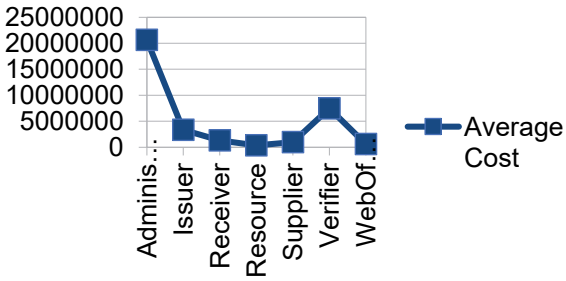

Fig. 4: Smart Contract Execution Cost

7. CONCLUSION

The metadata of the Web of Things (WoT) can be effectively represented through self-sovereign identity members, which can be verified by the verifier. This verification process ensures the smooth ownership transfer within the WoT ecosystem.

Additionally, the concept of fractional non-fungible tokens (NFTs) can be applied to Web of Things Tagged Resources, thereby establishing a robust self-sovereign identity system. Alternatively, a security token approach can also be explored; however, the current standard in this field is still in its nascent stages and not yet mature enough to be deployed for imitating self-sovereign identity use cases.

Roles within the system can be defined using various approaches, such as adapter, decorator, or role object patterns. However, it is important to note that the implementation of these patterns should be reliant on smart contract programming languages, as in the Solidity-Ethereum ecosystem have more constrained virtual machines and lack certain object-oriented properties. Moreover, most of the smart contract languages do not support object-orientation.

The code can be found under the GitHub link[9].

7.1. Future Work

Issuer and Verifier can be represented using various ERC interfaces or combination of them. The current implementation utilizes ERC-20 and ERC-721 interfaces to define the distribution token among the issuer, verifier, and holders. Moreover, the security token standard[10] can be integrated with one of the specific ERC interfaces. To minimize the cryptocurrency costs associated with the self-sovereign identity system, it is necessary to implement different design patterns and compare the final deployment results and function execution. This approach ensures optimal cryptocurrency efficiency throughout the system.

Acknowledgements / Information on sponsors

This work is funded by the German Research (DFG) within the Research Training Group Role-Based Software Infrastructures for continuous-context-sensitive Systems (GRK 1907)

Contact details

Orçun, Oruç: orcun.oruc@tu-dresden.de
Uwe, Aßmann: uwe.assmann@tu-dresden.de
Maliha, Raja: maliha.raja@tu-dresden.de

[9] https://github.com/zointblackbriar/Paper-Code/tree/main/Tokenization-Of-Ownership-Ma-nagement-for-Web-of-Things-new

[10] https://github.com/SecurityTokenStandard/EIP-Spec

Literature references

[1] Alblooshi, M.; Salah, K. and Alhammadi, Y. (2018). Blockchain-based ownership management for medical IoT (MIoT) devices,: 151-156.

[2] Gunnarsson, M.; Gehrmann, C.; Furnell, S.; Mori, P.; Weippl, E. and Camp, O. (2020). Secure Ownership Transfer for the Internet of Things., : 33-44.

[3] Sardar, R. and Anees, T. (2021). Web of things: security challenges and mechanisms, IEEE Access 9 : 31695-31711.

[4] Samaila, M.; Neto, M.; Fernandes, D.; Freire, M. and Inácio, P. (2018). Challenges of Securing Internet of Things Devices: A survey, Security and Privacy 1.

[5] Omar, A. S. and Basir, O. (2018). Identity management in IoT networks using blockchain and smart contracts, : 994-1000.

[6] Burmester, M.; Munilla, J.; Ortiz, A. and Caballero-Gil, P. (2017). An RFID-Based Smart Structure for the Supply Chain: Resilient Scanning Proofs and Ownership Transfer with Positive Secrecy Capacity Channels, Sensors 17.

[7] Khan, M. S. N.; Marchal, S.; Buchegger, S. and Asokan, N. (2019). chownIoT: enhancing IoT privacy by automated handling of ownership change, Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers 13 : 205-221.

[8] Di Angelo, M. and Salzer, G. (2020). Tokens, types, and standards: identification and utilization in Ethereum, : 1-10.

[9] Di Angelo, M. and Salzer, G. (2021). Towards the identification of security tokens on Ethereum, : 1-5.

Current State of MEV in the Ethereum Ecosystem

Sebastian Wunderlich
Hochschule Mittweida, Mittweida, Germany

Over recent years, Maximal Extractable Value (MEV) has gained significant importance within the decentralized finance (DeFi) ecosystem. Remarkably, within just two years of its emergence, MEV has seen an extraction of approximately 600 million USD - a phenomenon that has sparked concerns regarding potential threats to blockchain stability.
With growing interest in the Ethereum network and the growing DeFi sector, research surrounding MEV has substantially increased. This work aims to offer a comprehensive understanding of MEV. Additionally, this research quantifies the largest types of MEV (Arbitrage, Sandwich and Liquidations) from March 2022 to March 2023. The data are then compared to other sources, revealing a general upward trend, with a particularly noticeable increase in Sandwich Attacks.

1. Introduction

Maximal extractable value (MEV) refers to the potential financial gain that can be obtained from exploiting the vulnerabilities or inefficiencies in a given system. It was first identified as a problem as early as in 2014 by a Reddit user [1]. The concept of Maximal Extractable Value (MEV) encompasses the additional value that can be obtained from block production, going beyond the standard block reward and gas fees. MEV extraction involves manipulating transactions within a block by including, excluding, or changing their order. Participants in this process, namely searchers, builders, and validators, have varying levels of control and dependency. Searchers rely on builders to include their MEV bundles, avoiding theft or omission, while builders depend on validators to incorporate these MEV bundles into blocks [2].

In the Ethereum ecosystem, MEV has garnered significant attention due to its potential impact on the overall security and stability of the network [3]. In addition, MEV offers miners an extra source of financial incentives that can be utilized for bribery [4] and undercutting attacks [5]. These attacks involve adversarial miners intentionally providing monetary rewards, such as extractable MEV and transaction fees, on a forked blockchain to attract mining power. The concentration of revenue objectives by MEV relayers further amplifies the potential value that miners can extract, thereby increasing the risks associated with consensus layer forks [6].

This paper will utilize a MEV detection Script developed by Weintraub et al. [7] and compare the results with scraped Data from Zeromev [8], presenting Data from March 2022 until March 2023. During this time a critical change happened, Ethereum's transition from Proof of Work to Proof of Stake, known as The Merge.

Afterward, this paper examines the findings and takes a close look at the limitations tied to the data collected. The paper also discusses potential avenues for future exploration, shedding light on upcoming opportunities in this field.

2. Background

Maximal Extractable Value has been under heavy investigation. First brought to attention by Daian et al. [3] who descibed the phenomenon and its negative effects. The profound impact of MEV was underscored by Flashbots [9] development of "mev-inspect," a tool that unveiled pre-merge MEV data and offered insights into its extraction.
Arbitrage has been studied by Torres [7], Hansson [10] and McLaughlin, Kruegel and Vigna [11]. Zuest [12] and Wang [13] investigated Sandwich Attacks and Qin et al. [6] presented a comprehensive study.

Weintraub et al. [7] developed a MEV detection Script and made it publicly availabe. Zeromev [8] provides a detailed database. Heimbach et al. [2] explore MEV after Ethereum's transition.

3. Methodology

This paper utilizes a modified version of the mev-inspect tool as introduced by Weintraub et al. [7], which will be referred to as MEV detection Script or just Script. The focus is on the Ethereum blocks from 14,444,725 (dated March 23, 2022) to 16,666,666 (dated March 23, 2023).

The selected cut-off point builds on the research of Weintraub et al. [7], which covers data from block 10,000,000 (dated May 4, 2020) to block 14,444,725 (dated March 23, 2022). By employing the Script this work aims to contribute further to the Ethereum ecosystem's existing knowledge base.

Additional data was scraped from Zeromev, a platform renowned for being a leading source of MEV data. This dataset was used to compare the performance and accuracy of the modified MEV detection tool in identifying MEV instances.

The work from Weintraub et al. [7] builds upon Qin, Zhou, and Gervais [6] and thus uses the same heuristics to detect MEV. In the case of Arbitrage, given the expansive nature of the Ethereum blockchain, which consists of more than 11 million blocks and surpasses a billion

transactions, a balance between efficiency and comprehensiveness was essential. An instance of this compromise is the implementation of a scanning window of 100 blocks for detecting arbitrage attacks. This methodology is potentially incapable of identifying arbitrage attacks in cases where transactions are separated by more than 100 blocks. Moreover, limitations emerge from the specific focus of the detection heuristics on bot-performed arbitrage attacks. Attackers can execute transactions directly with a susceptible contract, circumventing the use of bot contracts. However, differentiating these transactions from those of benign users presents a significant challenge. In an effort to minimize potential false positives, the focus was confined exclusively to bot contract operations. Therefore, while this might lead to some false negatives, the results should be viewed as providing a conservative estimate [14].

Additionally, the Sandwich detection mechanism operates under the assumption that both transactions of a single sandwich take place within the same block. This assumption facilitates the efficient processing of the vast blockchain history, but it is not entirely accurate. Situations may arise where the transactions of a profitable sandwich span across multiple blocks, which our current methodology would fail to detect. Therefore, these outlined limitations highlight the necessity for further refinement and enhancement of the current heuristics and methodologies [6].

A further constraint of our methodology is its exclusive focus on the most recognized and prevalent forms of Maximal Extractable Value (MEV): sandwiching, arbitrage, and liquidation. This specialized focus prevents the inclusion of other potential types of MEV. Were additional variants to exist, they would require the development and application of distinct detection techniques and subsequent analyses. This narrow scope, while enabling detailed examination of specific MEV forms, limits the breadth of MEV activity that can be accurately captured and assessed.

3.1. Technical Approach

Relevant data for research on Maximal Extractable Value (MEV) was gathered utilizing a modified version of the mev-inspect software developed by Weintraub et al. [7]. This software is specifically designed to analyze and quantify MEV (Arbitrage, Sandwich, Liquidation) on the Ethereum Mainchain. The following setup and hardware were used:

A Docker image was adapted for different chip architecture (ARM64 to ARM64) and executed on Google Cloud using an N2 highcpu instance (Intel Cascade Lake) with 80 vCPUs and 80GB memory.

There are generally two methods to access the required data. The first method involves setting up and synchronizinga Geth archive node, which allows downloading and storing the complete history of the Ethereum blockchain, including all transactions and smart contract data. The second method involves using an RPC provider, which provides a remote interface to interact with the Ethereum blockchain. However, the substantial storage requirements and lengthy synchronization time of an archive node (currently estimated at approximately 14 TB of data [15]) made a more efficient approach desirable.

Instead of using a Geth archive node, a connection was made to Remote Procedure Call (RPC) endpoints provided by reputable service providers such as Alchemy. This allowed accessing the required data without the extensive resource burden associated with maintaining an archive node.

Despite the initial plan to utilize RPC endpoints provided by service providers such as Alchemy for data access, the strategy needed adjustment due to the high volume of requests that exceeded Alchemy's capacity. As a solution, a fully synchronized Geth node, generously made available by the community, was employed for effective access to the necessary blockchain data.

Adopting this methodology made it possible to access and analyze the pertinent blockchain data while mitigating the resource demands of maintaining a local archive node.

Sandwiches were evaluated by extracting token transfer events through a comprehensive crawl of archive node data. To detect sandwiching, the heuristics developed by Torres, Camino, and State. [14] were applied. These heuristics are based on the assumption that attackers engage in buying and selling the same type of tokens as the victim, executing two separate transactions. It is noteworthy that the quantities of tokens bought and sold by the attacker are nearly identical, and the gas price of the attacker’s initial transaction exceeds that of the victim’s transaction.

The quantification of arbitrage MEV was conducted by extracting token swap events through an exhaustive crawl of archive node data. To identify arbitrage opportunities, the heuristics proposed by Qin, Zhou, and Gervais [6] were utilized. The assumption underpinning these heuristics is that an arbitrage scenario involves multiple swap events, and all these swap events are contained within a single transaction, forming a closed loop.

Quantifying liquidation MEV required a systematic crawl of archive node data, specifically targeting liquidation events across various lending platforms. By extracting relevant information from these events, such as liquidated debt and received collateral, it was possible to analyze and measure the impact of liquidations. The script implemented for this purpose was designed to detect liquidations on prominent lending platforms. The script specifically scans for events like Aave’s LiquidationCall event and Compound’s LiquidateBorrow event, which directly correspond to instances of liquidation [7].

3.2. Data Sources

Historical blockchain data was accessed through a Full Archive Node. This approach enabled access to detailed transaction traces, transaction receipts, and block metadata.

Cryptocurrency price data was included by integrating the Coingecko API [16] into the research workflow. The script was adjusted to adhere to the rate limits imposed by the API.

The Script was deployed on Google Cloud, running for a total of 24 hours to investigate the three primary MEV types. Arbitrage made up the largest part of the investigation, requiring the longest duration for execution, producing a significant 5.2 GB of data. Sandwiches generated approximately 3.2 GB of data. Finally, liquidations produced a modest 175 MB. The retrieved data was then saved in a MongoDB database for further analysis.

4. Results

The chapter includes a discussion of the MEV results obtained from the MEV script used.

A key observation from the analysis was the apparent uptrend in the occurrence of MEV activities over time. This growing trend illustrates an evolving dynamic within the Ethereum ecosystem, revealing the increasing prominence of MEV as a factor in on-chain operations.

4.1. Data MEV Script

Particularly noteworthy was the surge in sandwich events, which came to light as a substantial contributor to the overall MEV activity. With 556,334 recorded instances, sandwiches emerged as a significant on-chain event in the analyzed period.

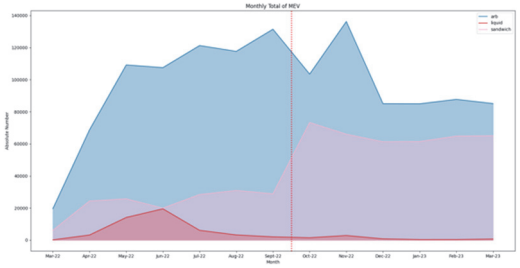

Fig. 1: Total monthly MEV Script

Arbitrages, characterized by the capitalization on price discrepancies across different exchanges, were the most prevalent type of MEV, totaling 1,258,479 instances. This indicates the vast extent of opportunity present on the Ethereum network for traders to exploit such disparities for profit.

Liquidations, albeit less frequent in occurrence compared to arbitrages and sandwiches, still presented a noteworthy count of 54,803 instances. Liquidations, defined by the compulsory closure of positions when collateral falls beneath the required level, exhibit an essential component of risk management in DeFi platforms.

The comprehensive results thus highlight a vibrant MEV landscape within the Ethereum ecosystem, characterized by a rising trend and considerable instances of sandwiches, arbitrages, and liquidations.

The presence of negative profit in certain MEV transactions may appear paradoxical initially. However, a closer inspection of block-level dynamics provides a plausible explanation. Ethereum validators exercise control over all transactions within a block. A single transaction, despite yielding a negative profit, may enable a larger, positive net profit when combined with other transactions within the same block. Hence, while examining MEV profitability, it's essential to focus on the cumulative profit across all transactions within a block, underlining the complex interplay of Ethereum transactions.

A significant trend in the MEV landscape is the marked increase in the prevalence of sandwich attacks. These types of attacks have become especially appealing after PBS due to their risk-free nature. If a transaction within the bundle fails, the entire bundle remains unexecuted, thereby eliminating potential losses for the attacker.

Heimbach et al. support this, indicating a significant increase in these types of attacks. Their findings document a total of 1,208,707 sandwich attacks during their data collection period, with a stark contrast between the frequency of attacks in PBS and non-PBS blocks. In fact, their data suggests that nearly all sandwich attacks were taking place within PBS blocks [2]. This underscores the influence of PBS on the facilitation of sandwich attacks. Similarly, Wahrstaetter et al. provide additional perspective on the rise of sandwich attacks. Their research highlights an increase in the confirmation latency for Ethereum transactions following the platform's transition to Proof-of-Stake and Proposer-Builder Separation (PBS). Such delays in transaction confirmation are likely to exacerbate the risk of sandwich attacks [17]. Wahrstaetter et al. further note that the design of MEV-Boost, aimed at enhancing decentralization, inadvertently creates an environment favorable for risk-free sandwich attacks. This potential side effect, they argue, might warrant regulatory attention [18].

4.2. Data Zeromev

The data utilized in this section has been primarily obtained through API access provided by Zeromev. This open-source resource has dedicatedly compiled data on various MEV Types making it a valuable point of reference.

A custom script was developed to extract detailed block data. The primary goal of this script was to calculate the monthly frequency of different types of MEV: arbitrage, liquidation, and sandwich attacks. This allowed for an examination of trends over time, providing insights into the evolution and prevalence of different types of MEV.

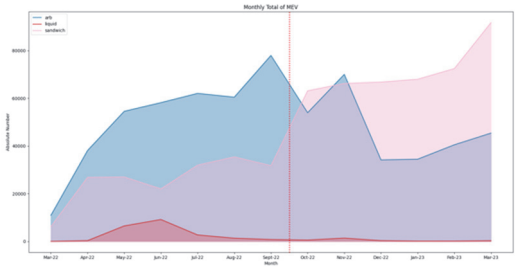

Fig. 2: Total monthly MEV Zeromev

The process of identifying and counting sandwich attacks required particular attention. Sandwich attacks consist of a front-run transaction, one or more victim transactions, and a back-run transaction. Initially, each victim transaction was counted as a separate sandwich attack. However, this approach overlooked the fact that multiple victim transactions can be part of the same sandwich attack within a single block. As such, the methodology was revised to count the front-run and back-run transactions within each block. This change in approach ensured that each sandwich attack, regardless of the number of victims, was counted only once, providing a more accurate picture of the frequency of sandwich attacks.

An examination of the extracted data reveals a discernible upward trend in the prevalence of MEV, particularly an increase in sandwich attacks. These attacks have become notably more frequent over time, illustrating a shift in the choice of MEV strategies adopted.

While liquidations are certainly present within the dataset, their relative frequency compared to the other MEV types is significantly lower. Despite their presence, liquidations do not appear to play a dominant role in the MEV landscape. This could suggest a trend towards strategies that offer a more predictable return, or possibly reflect the characteristics of the protocols and market conditions under analysis.

4.3 Script vs. Zeromev

This Section provides a systematic comparison between two primary data sources. The comparison revolves around the three primary financial metrics: Arbitrage, Sandwich, and Liquidation.

Arbitrage data shows less absolute magnitude in Zeromev compared to the script-based method, yet follows a similar trend across both sources. Sandwich data, on the other hand, is higher in Zeromev than the script data, while sticking to an analogous trend. In the case of Liquidation data, the script reveals a greater magnitude than Zeromev, albeit exhibiting a consistent trend between both sources. Notably, during the final month of observation, both data points converge closely.

In every corresponding graph is the inclusion of a dotted line. This line represents a significant event, 'The Merge', that occurred in September, thus serving as a crucial point within the analyzed period.

A substantial discrepancy has been observed between the Script and Zeromev with regard to detected arbitrage instances. The Script consistently identifies a larger number of such instances than Zeromev. In this section, potential explanations for this observed discrepancy, focusing on differences in detection techniques, definitions, and the handling of various arbitrage scenarios are presented.

4.3.1 Abitrage

A significant difference between the two lies in the handling of split arbitrages. A split arbitrage refers to a series of transactions where tokens are exchanged across more than two liquidity pools. This can be represented as a sequence: Token1 -> PoolA -> Token2 -> PoolB(50%) -> Token1 -> PoolC(50%). While the Script appears capable of handling multi-step transactions and, therefore, detecting split arbitrages, it is unclear to what extent it can detect more complex split arbitrages. Conversely, Zeromev explicitly states that it does not support split arbitrages, contributing to a lower number of detected arbitrage instances [67].

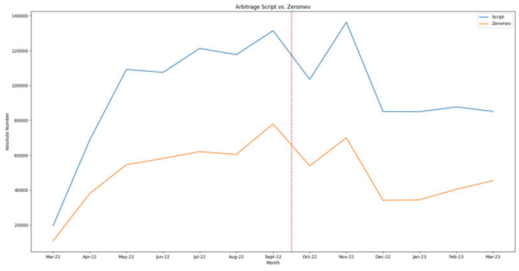

Fig. 3: Arbitrage Script vs. Zeromev

A second area of difference between the two tools lies in the handling of overlapping MEV. Zeromev admits to difficulties in detecting overlapping MEV situations. These include cases where arbitrage opportunities coexist with other types of MEV, such as sandwich attacks. If the Script handles overlapping MEV more adeptly, this could account for its higher arbitrage detection rate.

Further contributing to these discrepancies is the respective definition of arbitrage employed by each tool. The Script classifies a transaction as arbitrage when there is a price disparity for a single currency between two exchanges, thus rendering the exchange profitable even after accounting for mining fees. Zeromev's precise definition of arbitrage is, however, unclear from the information available. Any deviation in these definitions might lead to different detection outcomes.

Additionally, the inclusion of frontrun arbitrage in the Script could contribute to the observed discrepancy. Frontrun arbitrage involves a participant identifying an arbitrage opportunity in the public mempool and executing the same transaction with a higher gas fee to preempt the original transaction. It is plausible that

these instances are included as arbitrage by the Script, while Zeromev could categorize them as sandwich attacks or another MEV type, leading to fewer detected arbitrage instances.

4.3.2 Sandwich Attacks

Upon a comparison of our detection Script and the Zeromev sandwich attack data, a number of differences surface that could potentially explain the higher detection rates of sandwich attacks reported by Zeromev. It is crucial to note that these are potential explanations based on the information available regarding Zeromev's methodology. To fully understand why Zeromev detects more sandwich attacks than the MEV Script by Weintraub et al., a closer comparison of both pieces of code is needed. However, since Zeromev's code and the specific rules it uses aren't openly available, this detailed comparison cannot be done.

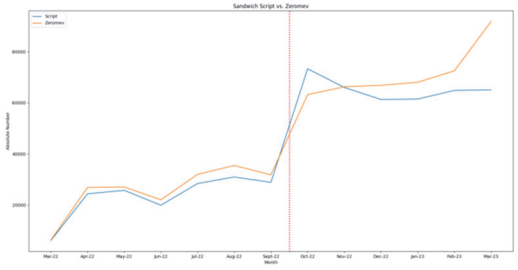

Fig. 4: Sandwich Attacks Script vs. Zeromev

Zeromev has integrated a comprehensive mechanism for the identification of what is termed "position taking". This occurs in instances where the output of the attacker's frontrun does not equate to their input in the backrun, resulting in an imbalance. Such instances could falsely inflate the estimated profitability of the attack. The thorough adjustment for position taking in Zeromev's algorithm might thus contribute to the system's increased identification of sandwich attacks.

Additionally, Zeromev employs a distinct method to extend the parameters of Automated Market Maker (AMM) pools from the sandwich transactions. This approach allows Zeromev to recreate and analyze the attack with more accuracy. Zeromev also demonstrates its robustness by minimizing potential errors attributable to differences in protocol mechanics and fee structures across the varied DeFi protocols in the Ethereum ecosystem. By factoring in these differences, Zeromev likely achieves a more precise detection of sandwich attacks.

Furthermore, Zeromev displays resilience in handling outliers, including but not limited to, Pool Imbalance Attacks, Low Liquidity/Malicious Tokens, Split Transactions, and Undetected Reverts. The specific handling of these outlier conditions could contribute to a more extensive detection of sandwich attacks [19].

Finally, Zeromev's broader analysis, which includes considerations for user losses, might add to the larger set of detected sandwich attacks.

4.3.3 Liquidation

In the domain of liquidations, a distinct variance has been noted between the Script and Zeromev, particularly before the Merge. The Script, in these instances, consistently detected more liquidations than Zeromev. This could potentially be attributed to differences in the underlying heuristics, specific definitions of liquidations, or processing methods employed by each tool.

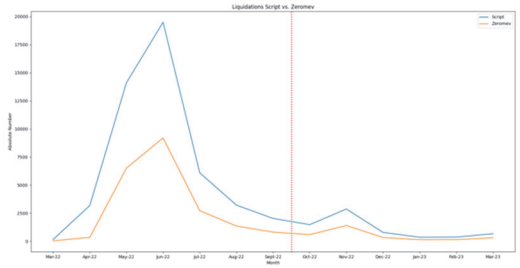

Fig. 5: Liquidation Script vs. Zeromev

However, this divergence appears to lessen significantly following the implementation of the Merge. Post-Merge, the Script and Zeromev demonstrate an increasing convergence in detected liquidations. This increased alignment suggests that the heuristics or data processing techniques used by both tools are becoming more consistent with each other, or that the Merge has impacted the on-chain conditions and mechanisms associated with liquidations, leading to a closer correlation between the two tools.

5. Discussion

The work presented is not without its limitations, owing to the constraints imposed by the methodology employed and the inherent complexity of the domain being explored. The following discussion describes some key areas where these limitations manifest, focusing on limitations related to the Script.

One limitation concerns the difficulty in dealing with overlapping MEV instances, such as mixed arbitrage and sandwiches, or overlapping sandwiches. At the present moment, there exists no MEV detection software that can fully resolve these scenarios. Lastly, certain types of MEV, despite being identifiable, are not quantified within this thesis. The research also unveiled the complexities of quantifying MEV. These complications arose from several factors, the most significant of which was the scope of the investigation.

This research was primarily centered around decentralized exchange DEX to DEX based MEV, whereas CEX to DEX interactions, which are harder to quantify but undeniably present, were not investigated. Furthermore, the ever-evolving landscape of protocols and their adoption presented additional challenges in the accurate measurement of MEV.

Another limitation of this research lies in the types of MEV explored. This work focused on known and major

types of MEV, leaving room for unidentified types and those possibly known only to specific entities.

The issue of MEV detection heuristics also complicates the process, as different heuristics yield different results, and not all researchers provide open access to their methodologies and code. Thus, comparing different results is difficult. This is in line with Judmayer et al. [20], who already came to the conclusion that a quantification of MEV is inherently difficult due to the continuously evolving network environment and the variety of value-extraction mechanisms. The adoption of the transparent approach championed by Weintraub et al. [7], who publicly disclosed their results and code, and Hansson [10], with his detailed appendix outlining the employed heuristics, would be a beneficial practice for all researchers in this field.

Although this work offers an in-depth exploration of MEV on the Ethereum mainnet, it does contain some limitations. Layer-2 protocols were not thoroughly investigated. A comprehensive analysis involving the setup of dedicated nodes was not pursued. This is attributed to the distinct characteristics of each L2 protocol, the vast volume of blocks they produce which requires substantial computational capacity, and the significant resource investment for node setup. Therefore, while L2 protocols were briefly considered, a full-scale examination was beyond the scope of this work.

6. Conclusion

This research has undertaken a comprehensive exploration of Maximum Extractable Value (MEV) in the Ethereum ecosystem, offering a deep dive into the MEV landscape and selected types of MEV and their effects on network stability, user experiences, and overall transactional fairness

The quantitative investigation focused on the major types of MEV, namely Arbitrage, Sandwich Attacks, and Liquidations, using the MEV detection script developed by Weintraub et al. [7]and comparing its results with data from Zeromev [8]. By inspecting approximately 2.5 million blocks, this research not only contributes to the understanding of MEV but also enriches the research community by providing an additional dataset. This work revealed a general rise in MEV and a significant surge in Sandwich Attacks, a toxic type of MEV. The Relayer ecosystem is witnessing diversification, evident from a decrease in Flashbots related block activities [21]. The research findings provide insights into the effectiveness of MEV quantification scripts in identifying and categorizing MEV, as well as revealing its impact on the Ethereum ecosystem.

Categorizing MEV requires a deeper understanding of the economic and political dynamics within the entire system. The classification of MEV types involves complex considerations that extend beyond technical implementation, as it is an economic and political discussion that necessitates a holistic understanding. While MEV quantification scripts play a valuable role in providing initial insights, a broader and interdisciplinary perspective is crucial for a comprehensive understanding of MEV's impact and the development of robust solutions.

This work reveals that MEV poses a significant impact on the Ethereum network, manifesting both beneficial and detrimental effects. On one hand, MEV provides opportunities for profit through mechanisms like Arbitrage, contributing to the financial dynamism of the network. On the other hand, the rise of harmful MEV types, such as Sandwich Attacks, threatens the integrity of the network and creates a potential barrier to Ethereum's promise of a decentralized and fair financial system

This work has highlighted the urgency to address harmful MEV types, hinting towards an ongoing challenge that the Ethereum community needs to address. This challenge presents a vast area for future research, specifically focusing on strategies to mitigate harmful MEV impacts and enhancing transactional fairness in the Ethereum network. This line of research holds significant promise, with potential to yield rewar-ding outcomes and innovative solutions to substantial challenges faced within the field, potentially not only fixing problems in the decentralized ledger world but also in traditional finance [22].

7. Future Work

The concept of Maximal Extractable Value (MEV), with its multifaceted nature and extensive scope, sets the stage for plentiful future research prospects. The significance of MEV is broad and far-reaching, influencing an array of disciplines. Several potential areas of study are discussed in the following.

Cross-chain MEV amplifies the complexity of MEV in the context of numerous blockchain networks. As highlighted by Judmayer et al. there may be scenarios where miners, motivated by potential gains, resort to reordering or excluding transactions based on the occurrence of cross-chain payments on other chains [23]. Consequently, comprehensive exploration of this cross-chain MEV landscape presents a unique and fruitful opportunity for future research. Such a study could delve into understanding the impact of MEV on the security and stability of various blockchains, and may even pave the way for the identification of potential methods to diminish its negative consequences.

Moreover, the investigation of cross-domain MEV stands as another path for further inquiry. This research's prime goal would be to understand the relationship between MEV and multiple application classes, along with identifying the possible areas of overlap or influence [24]. The findings could offer valuable insights that may inform strategies for optimizing MEV across domains.

The transition to PoS presents a novel dimension for MEV, referred to as multi-block MEV. The deterministic nature of block proposal in PoS systems, where the

upcoming block proposers within an epoch can be known in advance, enables the possibility of exploiting MEV over multiple blocks. Heimbach et al. underscore the security implications of multi-block MEV in PoS and advocate for a greater degree of decentralization to address these risks [2]. While there have been preliminary attempts [25] to understand the full impact, the field may benefit from more in-depth and extensive research.

Additionally, an exciting avenue for future research is a more thorough exploration of Layer-2 protocols. Given the growing volume of transactions happening on L2s, a comprehensive analysis, including setting up dedicated nodes for extensive data validation, could significantly enhance understanding. A first attempt for Arbitrum, Optimism and Polygon has been done [26].

In conclusion, these prospective research directions aim to explore further into the diverse nature of MEV. This exploration could provide a more comprehensive understanding of MEV's role and implications in the ever-evolving landscape of blockchain technology. It could also contribute towards the development of more robust systems and applications with a greater awareness of MEV. Additionally, these research efforts might also pave the way for improved quantification methods and foster a clearer understanding of the overall picture of MEV in the blockchain environment.

References

[1] Pmcgoohan, "Miners Frontrunning," r/ethereum, Aug. 11, 2014. www.reddit.com/r/ethereum/comments/2d84yv/miners_frontrunning/ (accessed Jan. 23, 2023).

[2] L. Heimbach, L. Kiffer, C. F. Torres, and R. Wattenhofer, "Ethereum's Proposer-Builder Separation: Promises and Realities," arXiv, May 2023, pp. 5–8. Accessed: Jun. 02, 2023. [Online]. Available: http://arxiv.org/abs/2305.19037

[3] P. Daian et al., "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges," p. 14, Apr. 2019, doi: 10.48550/arXiv.1904.05234.

[4] J. Bonneau, "Why Buy When You Can Rent?," in Financial Cryptography and Data Security, J. Clark, S. Meiklejohn, P. Y. A. Ryan, D. Wallach, M. Brenner, and K. Rohloff, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2016, pp. 19–26. doi: 10.1007/978-3-662-53357-4_2.

[5] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, "On the Instability of Bitcoin Without the Block Reward," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, in CCS '16. New York, NY, USA: Association for Computing Machinery, Oktober 2016, pp. 154–167. doi: 10.1145/2976749.2978408.

[6] K. Qin, L. Zhou, and A. Gervais, "Quantifying Blockchain Extractable Value: How dark is the forest?," presented at the 2022 IEEE Symposium on Security and Privacy (SP), Dec. 2021, pp. 198–214. doi: 10.1109/SP46214.2022.9833734.

[7] B. Weintraub, C. F. Torres, C. Nita-Rotaru, and R. State, "A Flash(bot) in the Pan: Measuring Maximal Extractable Value in Private Pools," in Proceedings of the 22nd ACM Internet Measurement Conference, Oct. 2022, pp. 3–5. doi: 10.1145/3517745.3561448.

[8] Pmcgoohan, "zeromev," 2023. https://zeromev.org/ (accessed Feb. 03, 2023).

[9] Flashbots, "MEV Explore," 2023. https://explore.flashbots.net/ (accessed Jan. 25, 2023).

[10] M. Hansson, "Arbitrage in Crypto Markets: An Analysis of Primary Ethereum Blockchain Data," Rochester, NY, Nov. 2022, pp. 9–14. doi: 10.2139/ssrn.4278272.

[11] R. McLaughlin, C. Kruegel, and G. Vigna, "A Large Scale Study of the Ethereum Arbitrage Ecosystem," p. p.14, 2023.

[12] P. Züst, "Analyzing and Preventing Sandwich Attacks in Ethereum," Bachelor Thesis, pp. 7–12, 2021.

[13] Y. Wang, P. Zuest, Y. Yao, Z. Lu, and R. Wattenhofer, "Impact and User Perception of Sandwich Attacks in the DeFi Ecosystem," in CHI Conference on Human Factors in Computing Systems, New Orleans LA USA: ACM, Apr. 2022, pp. 1–15. doi: 10.1145/3491102.3517585.

[14] C. F. Torres, R. Camino, and R. State, "Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain," p. 18, 2021.

[15] Etherscan, "Ethereum Full Node Sync (Archive) Chart | Etherscan," Ethereum (ETH) Blockchain Explorer, 2023. http://etherscan.io/chartsync/chainarchive (accessed Jun. 18, 2023).

[16] Coingecko, "Crypto API Documentation," CoinGecko, 2023. https://www.coingecko.com/en/api/documentation (accessed Jun. 21, 2023).

[17] A. Wahrstätter et al., "Blockchain Censorship," arXiv, Jun. 2023, p. 10. Accessed: Jun. 13, 2023. [Online]. Available: http://arxiv.org/abs/2305.18545

[18] A. Wahrstätter, L. Zhou, K. Qin, D. Svetinovic, and A. Gervais, "Time to Bribe: Measuring Block Construction Market," arXiv, May 2023, pp. 1–3, 12–14. Accessed: Jun. 01, 2023. [Online]. Available: http://arxiv.org/abs/2305.16468

[19] pmcgoohan, "data sources & limitations," zeromev, 2023. http://info.zeromev.org/sources.html (accessed Jun. 27, 2023).

[20] A. Judmayer, N. Stifter, P. Schindler, and E. Weippl, "Estimating (Miner) Extractable Value is Hard, Let's Go Shopping!," pp. 2–7, 2021.

[21] T. Wahrstätter, "MEV-Boost," mevboost.pics, 2023. https://mevboost.pics/mevboost.pics (accessed Jun. 13, 2023).

[22] L. Heimbach and R. Wattenhofer, "SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance," Sep. 2022, pp. 2–4. doi: 10.1145/3558535.3559784.

[23] A. Judmayer et al., "Pay To Win: Cheap, Crowdfundable, Cross-chain Algorithmic Incentive Manipulation Attacks on PoW Cryptocurrencies." 2019. Accessed: Jun. 23, 2023. [Online]. Available: https://eprint.iacr.org/2019/775

[24] A. Obadia, A. Salles, L. Sankar, T. Chitra, V. Chellani, and P. Daian, "Unity is Strength: A Formalization of Cross-Domain Maximal Extractable Value," Dec. 2021, pp. 1–8. doi: 10.48550/arXiv.2112.01472.

[25] J. R. Jensen, V. von Wachter, and O. Ross, "Multi-block MEV." arXiv, Jun. 12, 2023. doi: 10.48550/arXiv.2303.04430.

[26] A. Bagourd and L. G. Francois, "Quantifying MEV on L2s: A Study of Polygon, Arbitrum, and Optimism".

ISSN 1437-7624