Proceedings of the 2019 IEEE International Conference on Information Technologies (InfoTech-2019)
19-20 September 2019, St. St. Constantine and Elena, Bulgaria

Systematic Literature Review of Blockchain Applications: Smart Contracts

Elva Leka[1], Besnik Selimi[2] and Luis Lamani[3]
[1,2]South East European University, Tetovo, Macedonia
[3]Polytechnic University of Tirana, Tirana, Albania
el23618@seeu.edu.mk, b.selimi@seeu.edu.mk, luis.lamani@fgjm.edu.al

Abstract – **Blockchain technology has received extensive attention recently, but still a large of technical challenges such as scalability and security. This paper helps to find where recent studies have been focused on and offers a broad perspective relating blockchain applications and smart contracts, their main problems and corresponding solutions and will help to specify gaps and future research. The study extracted 292 articles from top Digital Libraries such as IEEE, ACM, Science Direct and Springer. After a detailed review process only 28 publications were considered based on defined inclusion and exclusion criteria.**

Keywords – **blockchain technology; smart contract security; systematic literature review.**

I. Introduction

Blockchain is a peer-to-peer distributed ledger technology which records transactions, agreements, contracts, and sales. A blockchain ledger is a list ('chain') of groups ('blocks') of transactions, where blocks are linked to one other in sequential order [1]. Blockchain ensures that transaction is secure, thanks to the use of cryptographic methods.

The key advantages of blockchain are decentralization, persistency, non-repudiation, anonymity and auditability. This technology makes decentralized consensus possible, i.e. agreement between untrusted players, without the need for central certification authority. Consensus is generated by cryptography-enabled algorithms running on a distributed network of peers and enabling (in the case of Bitcoin [2]) virtual currencies that do not depend on the existence of a central bank. More recently, blockchain technologies also support the decentralized execution of code, e.g. the Ethereum [3] blockchain, defining a new model of decentralized computation and enabling smart contracts. Smart contracts are essentially a piece of code executed on a decentralized virtual machine, EVM [4].

From our literature review process, we believe that blockchain technologies will be one of the next technologies revolutions. There are several reviews relating blockchain, mainly focused on: different consensus protocols [5]; currency aspect of blockchain [1,6,7]; different areas of applications such as in IoT [4], healthcare, education, voting system, government; security aspect [8,9]. Other reviews focus on blockchain-based smart contracts [10], attacks and vulnerabilities of smart contracts [11]. At this work we take a look at the current research on challenges and limitations of blockchain. The structure of the paper is organized as follows. In Section 2 is described the review process. Findings and results are presented in Section 3. Section 4 gives conclusions of the research and offers some recommendation for future research.

II. Systematic review process

To conduct the literature review, we use Systematic Literature Review (SLR). Using SLR, helps us to provide a visual summary, a map of results by categorizing the papers and aim to present an overview of research in order to identify gaps.

According Peterson principle [12], to perform a systematic mapping study, we should be focused on 5 steps. Starting from developing the research questions as the first step, then extract the information gathered. Concluding with answering the research questions and identifying research gaps in the last phase as it is shown in Figure 1.

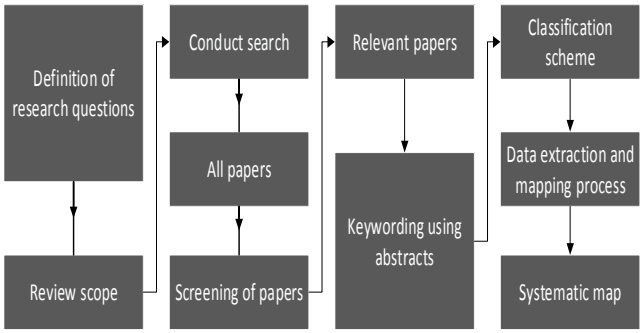

Figure 1. Five steps of the process which are used for selection of primary studies.

The main tasks of this paper are: (1) identify which are current research topics in blockchain; (2) identify different researches and contributions on detecting threats/vulnerabilities; (3) how publications have evolved over time; (4) identify which are the research gaps.

A. Screening of papers for Inclusions and Exclusions

The main sources of articles we read were from well-known digital libraries such as: IEEE, ACM, Science Direct, and Springer Link. We extracted 292 high quality published papers in the blockchain and smart contract domain. Then we considered 60 papers as primarily studies focused on this domain. We excluded papers which had not English as the main language, had not full text availability; or had some other meaning than blockchain used in

978-1-7281-3274-7/19/$31.00 ©2019 IEEE

computer sciences. 32 papers were removed as they were duplicates, resulting on 28.

III. Information Extraction and Results

We designed a data extraction form, in order to gather and classify the required information.

Task 1. Which are current research topics in blockchain?

We made some different classification schemes relating to papers we read. First, we classified them into those categories: cryptocurrencies oriented; blockchain-based applications; security vulnerabilities identified; proposed solutions to detect vulnerabilities. We analyzed that percentage distribution of each category, was respectively 17%, 31%, 34% and 18%.

From papers we read, we noticed that blockchain technology can be applied in many financial fields, different business services, making transactions and even predict the markets [1]. For example, it can be used to perform digital payments [11], cryptocurrency payment and exchange [13] or blockchain-based peer to peer implementations of prediction marketplace systems [14]. Blockchain technology can be used in many other domains, including pharmaceutical industry, integrity verification, governance, healthcare management, privacy and security, voting systems, internet of things and education [15,16,17,18]. Blockchain may offer different implementation solutions used in distributed networks in order to enhance security and reliability [19]. Furthermore, it can be used to store educational records related to reputational rewards in education domain [20].

Then, we found that some of the papers were relating with smart contract issues [21,22]. They were mainly focused at codifying, security, privacy and performance issues. In Figure 2 it is presented a classification scheme that addresses main challenges of blockchain applications.

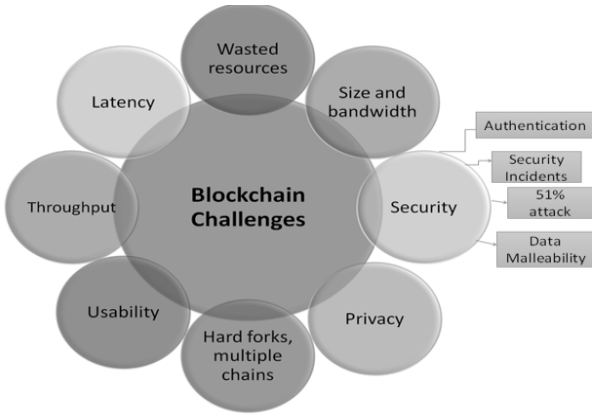

Figure 2. Selection process of primary studies.

Analyzing the papers, we found that Bitcoin and Ethereum were two of most well-known platforms that use the smart contract's concept. Figure 3 presents a classification scheme related to smart contracts: where the categories are: security issues, smart contract application, platform, usage of smart contracts, design patterns.

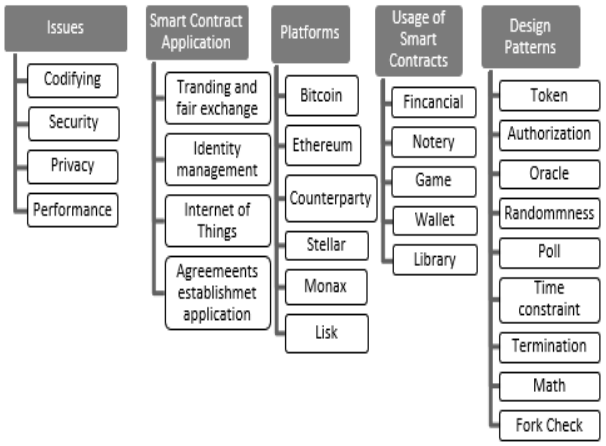

Figure 3. Classification scheme related to smart contracts

Task 2. Identify the security vulnerabilities of blockchain and smart contract?

Some of the most common vulnerabilities are: endpoint vulnerabilities, public and private key security, blockchain integration platforms, untested at full scale, lack of standards and regulation, untested code and vulnerabilities on smart contracts. We should be concerned about smart contract because there is increasing evidence that perhaps greater than 40%, of Ethereum smart contracts are vulnerable, such as DAO or the thief of $32.6 million on June 2017 caused by a multi signature wallet. According authors at [23], both malicious miners and users can exploit certain classes of vulnerabilities. To make smart contract development safer, some researchers were focused on analyzing most common errors in smart contracts and tried to solve them [24,25]. Some recent works propose tools to detect vulnerabilities through static analysis of the contract code [26]. Quantumstamp [27] ensures that all audited smart contracts conform to a security standard. It improves the blockchain infrastructure they implemented a decentralized security protocol.

Task 3. How publications have evolved over time?

At our study, primary papers were published after 2014. When looking more closely how publications have evolved over time: 2 papers (7%), were published in 2014, 1 paper (4%) was published in 2015, 6 papers (21%) were published in 2016, 8 papers (29%), in 2017, 11 papers in 2018 (39%).

Task 4. Identify which are the research gaps

After we did the systematic mapping study, we found the gaps mainly focused on scalability and performance issues. As a future research might be deploying and running secure smart contract on different implementation of blockchain.

Lately, blockchain is not only used in applications focused on the digital currencies, but it applied in many other important domains. From our literature review, an important domain to be focused on is implementation of blockchain in education. We can use blockchain and smart contract [28]: to secure and issue certificates; to implement a distributed application for transferring credits and having an automatic recognition; to make digital transactions to receive payments form students; to use student

identification within educational institutions; and to track intellectual property.

An interesting future work might be implementation of a blockchain powered smart contract application on education domain for verifying digital properties.

IV. CONCLUSION

Recent years the blockchain technology field increased interest both from academia and from industry. We identified current research topics and offered a broad perspective relating blockchain applications and smart contracts. Using systematic literature review, we identified their main problems relating to implementation and vulnerabilities as well as corresponding solutions.

We found that there was a gap on application of blockchain in education. The current implementations of using blockchain and smart contract in education are in pilot stages. Some existing projects are focused on student payments, how to manage records of students, or management of credentials and transcripts.

As a future work, we will use blockchain technology and smart contract to implement a platform for intellectual property management. As a case study, might be a platform where scientist can share their study in a secure and efficient manner. Using the blockchain to manage ownership-rights, to have democratic eco-system and offer equal rights for publishing your data.

REFERENCES

[1] F., Restuccia, S., D'Oro, S., S. Kanhere, T.,Melodia, S., K., Das, "Blockchain for the Internet of Things: Present and Future", in IEEE Internet of Things Journal, Vol.1, No.1, pp.1-5, 2018.

[2] Bitcoin, https://www.bitcoin.com.

[3] C., Dannen, "Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginner". Apress, 2017.

[4] K., Christidis, M., Devetsikiotis, "Blockchains and smart contracts for the internet of things", in IEEE Access 4, pp.2292-2303, 2016.

[5] L. S., Sankar, M. Sindhu, M. Sethumadhavan, "Survey of consensus protocols on blockchain applications", in Proceedings of the 4th International Conference on Advanced Computing and Communication Systems (ICACCS) IEEE, pp. 1-5, 2017.

[6] M.C.K., Khalilov, A., Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems", in IEEE Communication Surveys, 2018

[7] M., Garriga, M., Arias, A., D., Renzis, "Blockchain and Cryptocurrency: A comperative framework of the main Architectural Drivers", in Proceedings of Sample Conference, November, 2018.

[8] M. A. Khan, K. Salah, "IoT security: review, blockchain solutions, and open challenges". In: Future Generation Computer system, pp. 395-411, 2017.

[9] W. Meng, E. W. Tischhauser, Q. Wang, Y., Yang, J. Han, "When intrusion detection meets blockchain technology: a review". In IEEE Access 6, pp. 10179-10188, 2018

[10] Y., Yamada, T., Nakajima, M., Sakamoto, "Blockchain-L1: a study on implementing activity-based micro-pricing using cryptocurrency technologies". In: ACM International Conference Proceedings Series, pp. 203-207, 2017.

[11] N. Atzei, M. Bartoletti and T. Cimoli, "A survey of attacks on Ethereum smart contracts" in IACR Cryptology ePrint Archive, pp.99-110, 2016

[12] K. Petersen, R. Feldt, S. Mujtaba, M. Mattason, "Systematic mapping studies in software engineering," in Proceedings of the 12th International Conference on Evaluation and Assesment in Software Engineering, pp.71-80, 2008

[13] D. Cawray, "37Coins Plans Worldwide Bitcoin Access with SMS-Based Wallet, http://www.coindesk.com/37coins-plans-worldwide-bitcoin-access-based-wasllet/., 2014

[14] Viacoin Whitepaper, https://github.com/viacoin/documents/raw/master/whitepapers/Viacoin_whitepaper.pdf, 2014

[15] K. Megget, "Securing the supply chain", 2018.

[16] J., Kishigami, S., Fujimura, H., Watanable, A., Nakadaira, A., Akutsu, "The blockchain-based digital content distribution system". In: 2015 IEEE Fifth International Conference on Big Data and Cloud Computing, pp. 187-190, 2015.

[17] M., Zeilinger, "Digital art as 'monetised graphics':enforcing intellectual property on the blockchain. Phil. Tech. 31(1), pp.8-17, 2018.

[18] P.K., Sharma, M., Chen, J.H., Park, "Block-VN: A distributed blockchain based based vehicular network architecture in smart city. In: Information Processing System 13 (1), pp. 184-195, 2017.

[19] K., Fan, Y., Ren, Y., Wang, H., LI, Y., Yang, "Blockchain based efficient privacy preserving and data sharing scheme of content-centric network in 5G. IET Commun, 12(5), pp. 527-532, 2018

[20] M., Turkanovic, M., Holbl, K., Kosic, M., Hericko, A., Kamisalic, "EduCTX: A blockchain-based higher education credit platform. IEEE Access 6, pp. 5112-5127, 2018

[21] M. Alharby, A. Moosel, "Blockchain-based smart contracts:A systematic mapping study" in 3rd International Conference on Artificial Intelligence and Soft Computing, August 2017.

[22] Z. Zheng, Sh. Xie, H. N. Dai, X. Chen, H. Wang, "Blockchain Challenges and Opportunities: A Survey," in International Journal of Web and Grid Services. December 2017.

[23] L. Loi, C. Duc-Hiep, O. Hrishi, P., S., and A. Hobor, "Making Smart Contracts Smarter" in ACM SIGSAC Conferece on Computer and Communications Security (CCS '16), New York USA, pp. 254-269, 2016.

[24] K. Bhargavan, A. Delignat-Lavdaoud, C. Fournet, A. Gollamudi, G. Gonthier, N. Kobeissi, N. Kulatova, A. Rastogi, A. Sibut-Pinote, N. Swamy, and S. Zanella-Beguelin, "Formal verification of smart contracts: Short Paper" in ACM Workshop on Programming Languages and Analysis for Security (PLAS '16), (2016)

[25] J. Pettersson and R. Edstorm, "Safer smart contracts through type-driven development: using dependent and polymorphic types for safer development of smart contracts," Master thesis in Computer Science, Chalmers University of Technology of Gothenburg, 2016.

[26] N. Atzei, M. Bartoletti and T. Cimoli, "A survey of attacks on Ethereum smart contracts" in IACR Cryptology ePrint Archive, pp. 99–110, 2016

[27] Quandstamp. "A proposal for automated security audits in the blockchain", September 2017.

[28] A., Grech, A. F., Callmeri "Blockchain in Education", JRC Science for Policy Report, 2017