A STUDY ON BLOCKCHAIN-BASED SMART CONTRACTS

Uminder Kaur[1], Tejinder Thind[2]
Assistant Professor[1], Assistant Professor[2]
School of Computer Science & Engineering[1,2]
Lovely Professional University, Phagwara, Punjab.

ABSTRACT

The smart contracts are an attractive aspect of blockchain technology. A smart executes on topmost of the blockchain to negotiate, run and implement a settlement between not trusted parties. This paper, performs a orderly analysis to gather from a technical perspective all work important for smart contracts. The goal is to recognize recent investigation issues and vulnerable problems in smart contract research to future studies. We're collecting papers from various scientific sources. Analysis shows that most of the papers concentrate on finding and solving smart contract problems. This identifies four key problems, namely codification, protection, privacy, and efficiency. The remainder of the articles concentrate on smart contract implementations or other matters related to smart contracts. Research gaps are found which must be talked in upcoming revisions.

Keywords

Blockchain Technology, Organized aligning study, Analysis.

Overview:

Smart contracts are a software component held in a blockchain network. The smart contract must be mounted on every computer in the network. So, all computers execute the script. This strategy ensures the outcome is correct and preserves the dignity of the contract. Smart contracts require the carrying out of trustworthy transactions. Such transactions are traceable and permanent. The objective of smart contracts is to provide superior safety to outdated contract rule and to diminish other transaction expenses related to contracts. A smart contract is a two-person, processor code agreement. We run on the blockchain, meaning that they can't be modified and kept in a public database. The transactions that take place inside a blockchain controlled smart contract, meaning they can be automatically submitted without a third party.

Literature Review:

1. Amritraj Singh et al presented in their paper a orderly analysis of state of the art progress in the validation of smart contracts. This paper also examines the most commonly addressed issues and weaknesses in methods of formalization associated with smart blockchain contracts.

2. In the area of smart contracts Daniel Macrinici et al conducted a detailed mapping study of current research within blockchain technology. Throughout their report, they addressed issues related to smart contracts based on blockchain, and offered solutions to those issues.

3. M. Khan et al synthesized detailed information engineering mapping studies to provide insight into emerging fields of software engineering, and to evaluate SMS patterns and reliability. To check and map SMS in SE to SE Body of Information (SWEBOK), they used the Systematic Literature Review method.

4. Amritraj et al provided to newcomers and researchers a comprehensive analysis oomain-specific programming activities from critical points of usability and security. Existing languages are not capable of unleashing the full potential of the blockchain, as insecure software with a steep learning curve for

developers has often resulted. It indicates that current contract development work is not adequate and is still in its infancy stage. To advance the state of the research in this area, a comprehensive and experimental review of current state-of - the-art practices is needed.

5. In this paper, Dspace et al endorsed the Blockchain Software Engineering discipline's necessity to address smart contract programming and other blockchain applications. They examined a bug exposed in a Smart Contract collection and maybe "unsafe" software design caused an assault on Equivalence, a file client, to freeze about 500 K Ethers (in November 2017, around USD 150M).
In this report, they reviewed the Parity and library source code and explored how best practices recognized could minimize such detrimental technology misconduct if implemented and adapted.They also focused on the complexity of the design of applications of Smart Contract, marks recent solutions inadequate, and called a clear Blockchain Software Work concept.

6. Biryukov et al have proposed Findel, a special language of the financial domain of the blockchain network. The researchers have created an Ethereum smart Findel contract, which calculates the operating costs of a marketplace. It also addressed the aspects of modeling and setting up financial contracts on distributed networks.

7. Hegedus et al proposed the implementation of certain famous OO metrics for smart contracts Solidity. In addition, they evaluated further than 10,000 smart contracts using their development instrument. The findings suggested that smart contract systems were small, not too complicated and either made very good comments or made no comments at all.

8. A systematic review of the literature (SLR) was performed by Yli-Huumo et al. to govern whatever latest work was printed in relative to the overall definition regarding blockchain. They removed legal, cultural, and controlling work from their study and concentrated on the technological blockchain documents; they placed 80 percent concentration on Bitcoin ventures and a mutual protection and confidentiality in particular. Blockchain technologies have diversified since 2016 and as such work aims to establish what research actually occurs with respect to cybersecurity solicitations.

9. In 2016 Conoscenti et al. completed an SLR explicitly addressing blockchain usage and adaptableness to IoT. Remarkably, they underlined that the blockchain could be utilised without the need of a central monitoring system to detect data misuse. Seebacher et al. presented an SLR in 2017, which has stressed that blockchain is becoming progressively effective on the provision structures. Our findings from the SLR indicate that blockchain is an important part of operating a business network.

Methodology

Systematic representing analysis as mentioned in [2] is the procedure for exploring the readings associated with smart contracts. The consequences of this review will enable to recognize and plan investigation spaces relating to smart contracts. The method for the systematic mapping analysis is to define research questions, review the scope, searching and screening to find relevant papers, keywording, classification scheme, data extraction and Systematic Mapping.

Classification of research questions:

This step is to classify the research questions to which the analysis aims to react. We had identified the following research questions for our study:
What are the latest topics in smart contract research?
What are the current expectations for smart contracts?
Which study gaps do future studies need to address?

Categorization of results

The first is the trouble writing smart contracts correctly. In this context, the correctness of smart contracts means contracts which work as their developers intend. The reason why proper smart contracts are important as those agreements have treasured currency units.

In an effort to tackle this problem, the literature proposed three solutions. The first approach is to semi-automate the expansion of smart contracts to simplify the writing procedure. Semi-automation means that human understandable contract depictions are converted into smart contract law. Another approach is to offer designers instructions to help them inscribe contracts appropriately.

The second issue is the inability of smart contracts to be changed or terminated. Regardless of blockchain's immutability functionality, after deploying it into the network, smart contracts cannot be changed or terminated. This is separate from the law that allows to change or revoke the laws. In a bid to address the matter, Marino et al. introduced usual guidelines allowing to alter or cancel smart contracts. These requirements are derived from lawful contracts. These principles were then used on smart contracts built on Ethereum in order to prove their success. The third is the lack of assistance in finding understated smart contracts. An underoptimized smart agreement is a agreement involving excessive or costly procedures.

Conclusion

Blockchain technology is a centralized catalogue that tracks all the communications in the network that had forever taken place. Blockchain's key innovation is that this enables not trusted groups to interact among themselves without necessity for a another trustworthy party. You can deploy dissimilar scattered requests besides cryptocurrencies on topmost of blockchain. Smart contracts are structures that are actually executable programs and are used to enforce untrusted parties to an agreement. There are many systems available but Ethereum is one of te most commonly adopted blockchain platform for smart contract development. This has helped us to recognize study gaps that must be addressed in future studies. From a technological point of view this study centered on smart contracts. We find that most papers identify problems with smart contracts and fix them. These issues have been grouped into four groups, codification, security, privacy and effectiveness.

References

[1] D. Macrinici, C. Cartofeanu and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study", *Telematics and Informatics*, vol. 35, no. 8, pp. 2337-2354, 2018. Available: 10.1016/j.tele.2018.10.004.

[2] A. Biryukov, D. Khovratovich, and S. Tikhomirov, ―Findel: Secure Derivative Contracts for Ethereum,‖ in Financial Cryptography and Data Security, 2017, pp. 453–467.

[3] B. Marino and A. Juels, "Setting standards for altering and undoing smart contracts," in International Symposium on Rules and Rule Markup Languages for the Semantic Web, pp. 151-166, Springer, 2016.

[4] T. Chen, X. Li, X. Luo, and X. Zhang, "Under-optimized smart contracts devour your money," in 2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER), pp. 442-446, IEEE, 2017.

[5] F. Idelberger, G. Governatori, R. Riveret, and G. Sartor, "Evaluation of logic-based smart contracts for blockchain systems," in International Symposium on Rules and Rule Markup Languages for the Semantic Web,167-183, Springer, 2016.

[6] C. Natoli and V. Gramoli, “The blockchain anomaly," in 15th International Symposium on Network Computing and Applications (NCA), 310-317, IEEE, 2016.

[7] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making smart contracts smarter," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, pp. 254-269, ACM, 2016.

[8] A. Juels, A. Kosba, and E. Shi, “The ring of gyges: Investigating the future of criminal smart contracts," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, pp. 283-295, ACM, 2016.

[9] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, “Town crier: An authenticated data feed for smart contracts," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, pp. 270-282, ACM, 2016.