WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Smart Tender/Contract Management System Using Blockchain

Thilak K[1], Prof. Priya N[2]

[1,2] Department of MCA, Jain deemed to be university, Bangalore, india

ABSTRACT

Generally, the Tenders or contracts are used by governments and companies to procure goods or services. In the case of defective processes, improper tender management results in significant losses.Contractors are favoured, records aren't kept properly, there's a lack of openness, there's hacking, data is changed, and so on. To overcome this problem, we have used a simple and secure block chain technology and to secure by encryption coupled with indisputable block-based architecture for transaction management. In this case we make use of block chain technology to secure transaction-based documents along with transactions such as to provide a completely transparent tendering process, tender documents, applications, bid proposals, company profiles, past records, approving officer details, and rejection details are all required.

KEYWORDS - Block chain, Tenders, Bidders, Contractors

INTRODUCTION

Current e-tendering processes aren't 'fair and open,' which means that information isn't shared with all parties involved. When a corporation is chosen as the winner of a contract, for example, the information is disseminated 'as they wish. Organisations that bid on a same tender aren't told why their proposal was rejected or why one company was chosen as the winner. A corporation can request this information, but obtaining it is a time-consuming process. Despite the fact that checking these papers is possible, reviewing them takes time. A side from not being transparent, the security of these portals is a major worry, as it can lead to fraud and data manipulation in a central database. If a hacker acquires access to this central database, bids can be shared with competitors, resulting in severe financial and strategic losses for a corporation. Blockchain technology may be used to address these security problems since it focuses largely on information decentralisation and is safeguarded by encryption combined with an irrefutable block-based architecture for transaction management. As a consequence, Blockchain and Smart Contracts may be used to construct a transparent, decentralised, and secure tendering framework that allows bidders to keep track of portal functionality and all tender portal activity.

OVERVIEW OF BLOCKCHAIN

Blockchain is based on the notion of decentralisation. As a result, it's possible to consider it a distributed database. In this case, the distributed database employs full replication, which implies that each node has a complete copy of the blockchain. When the blockchain has to be updated as a consequence of a transaction, a process known as mining takes place. A block contains a large number of transactions. A consensus mechanism is used to send the mined block to the other nodes. There will be a cryptographic hash in the header of these blocks that references to the preceding block in the chain. If a transaction is tampered with, the hash associated with it changes, necessitating the re-mining of all following blocks, which is impractical. The immutability property of blockchain is utilised in this fashion. The implementation of blockchain and the consensus mechanism it employs are at the heart of the technology.

RELATED WORKS.

During the study, we discovered a variety of methods to this application.

Wang, Wenbo, et al. [1] "In blockchain networks, a survey on consensus methods and mining strategy management has been conducted." IEEE Access 7 (2019): 22328-22370.

The fast advancement of blockchain technologies over the last decade has piqued the curiosity of both academics and businesses alike. The blockchain network started as a decentralised, immutable ledger system for transactional data ordering in the Internet banking sector.It is now thought to be a powerful backbone/framework for decentralised data processing and data-driven self-organization in flat, open-access networks. The unique

decentralised consensus processes introduced by public blockchain are mostly to blame for the conceivable qualities of decentralisation, immutability, and self-organization. The lack of a comprehensive literature study on the development of decentralised consensus mechanisms in blockchain networks inspired this survey. We present a systematic view of blockchain network organisation in this study. Our in-depth examination of the state-of-the-art consensus protocols focuses on both the perspective of distributed consensus system design and the perspective of incentive mechanism design, emphasising the unique characteristics of decentralised consensus in blockchain networks. We also give a game-theoretic solutionthorough an examination of the approach used by individual nodes in blockchain backbone networks to self-organize. As a result, we present a thorough examination of the growing uses of blockchain networks in a wide range of telecommunications. We are particularly interested in the impact of consensus procedures on these applications. Finally, we go over some of the open difficulties in blockchain consensus protocol design, as well as some of the possible research avenues.

Summary: Wang, Wenbo and team describes in this paper, we provide a systematic vision of the organization of blockchain networks.

Ambegaonker, Ajeenkkya, Utkarsh Gautam, and Radha Krishna Rambola. [2] "Successful Tender process Approach using Block chain technology to Maintain Safety and Integrity." 2018 4th International Conference on Computing Communication and Automation (ICCCA). IEEE, 2018.

The problem with current tendering is that it only reaches a limited number of people; however, the internet is expanding, and tendering is not far behind. We have some online tendering systems, but they are not as secure as they should be because tendering contains confidential data that should not be leaked, and Blockchain solves that problem effectively. The goal of this study is to uncover better ways to tender, because tendering is such an important element of business and development that improving this system would lead to greater development. Time efficiency, employment, and a fair system are some of the elements that the suggested system of this research can enhance.

Summary: Ambegaonker, Ajeenkkya and team working on online system for tendering but it is not secure as Tendering contains sensitive information that should not be shared, and Blockchain effectively addresses this issue.

Zheng, Zibin et al. [3]"An introduction to blockchain technology, including its architecture, consensus, and future developments."2017 IEEE international congress on big data (Big Data congress). IEEE, 2017.

The blockchain, which is at the heart of Bitcoin, has recently gotten a lot of attention. Blockchain acts as an immutable record that allows decentralised transactions to take place. Blockchain-based applications are gaining traction in a variety of industries, including financial services, reputation management, and the Internet of Things (IoT), among others. However, there are still a number of issues with blockchain technology to address, such as scalability and security concerns. This paper provides an in-depth look of blockchain technology. First, we give an introduction of blockchain architecture before comparing some common consensus methods utilised in various blockchains. There are also brief mentions on technical issues and current improvements. We also discuss likely blockchain developments in the future.

Summary: Zibin and team provide an overview of blockchain architechture firstly and compare some typical consensus algorithms used in different blockchains.

Cachin, Christian, and Marko Vukolić. [4] "Blockchain consensus protocols in the wild". arXiv:1707.01873 arXiv preprint (2017).

A blockchain is a decentralised ledger for recording transactions that is maintained by numerous nodes without the need of a central authority and is based on a distributed cryptographic system. A consensus mechanism guarantees that all nodes agree on a unique sequence in which entries are attached to the blockchain, and all nodes check the information to be appended to it. Because they also deal with blockchain systems, consensus techniques for tolerating Byzantine flaws have gotten a lot of interest. The process of evaluating and establishing confidence in the robustness of consensus protocols exposed to failures and hostile nodes is discussed in this paper. We propose using standard cryptography and computer security practises such as public reviews, detailed models, and formal proofs; yet, many real-world system designers appear to be unaware of this. We also look at the failure models and attack resilience of the consensus algorithms employed by a variety of well-known permissioned blockchain systems.

Summary: Christian, and team discusses the process of assessing and gaining confidence in the resilience of a consensus protocols exposed to faults and adversarial nodes.

Pilkington, Marc. [5]"Principles and uses of blockchain technology." Research handbook on digital transformations. Edward Elgar Publishing, 2016.

This article explains the fundamentals of blockchain technology as well as some of its most cutting-edge uses. To begin, we'll go over the fundamental principles behind the blockchain, as well as the possible dangers and downsides of public distributed ledgers, as well as the trend toward hybrid solutions. Second, we highlight the key characteristics of decentralised public ledger platforms. We illustrate why blockchain is a revolutionary and foundational technology in the third section, and we sketch out a list of key applications in the fourth section, taking into account recent developments.

Summary: Pilkington and team expose the main features of decentralized public ledger platforms.

L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, [6] "Making smart contracts smarter" in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016, pp. 254–269.

Cryptocurrencies use a decentralised data structure called a blockchain to record transactions. Bitcoin and Ethereum, two of the most prominent cryptocurrencies, both allow the ability to encode rules or scripts for transaction processing. This functionality has grown to help put smart contracts, or full-fledged programmes that operate on blockchains, into practise. Ethereum's smart contract architecture has recently experienced a surge in popularity, with tens of thousands of contracts containing millions of dollars in virtual currency.
On this research, we look at the security of executing Ethereum-based smart contracts in an open distributed network similar to that of Bitcoin. We present various novel security issues in which an attacker might profit from smart contract execution by manipulating it.. These flaws point to a lack of grasp of the underlying platform's distributed semantics. We offer techniques to improve Ethereum's operational semantics to make contracts less susceptible as a refinement. We built Oyente, a symbolic execution tool for developers developing contracts on the existing Ethereum system, to discover potential security issues.

Oyente has identified 8, 833 Ethereum contracts as susceptible out of a total of 19, 366. This includes the DAO problem, which resulted in a $60 million loss in June 2016. We also describe the severity of additional assaults for numerous case studies using source code and confirm the attacks (which exclusively target our accounts) in the Ethereum main network.

Summary: L. Luu, D.-H and team introduce several new security problems in which an adversary can manipulate smart contract execution to gain profit.

METHODOLOGY

The Proposed Tender Management System uses block chain technology to ensure the complete tender management process is secure and efficient. A block chain is secured by encryption coupled with indisputable block-based architecture for transaction management. This enables the system to maintain a basic, transparent transaction with only the information that the system needs to know.

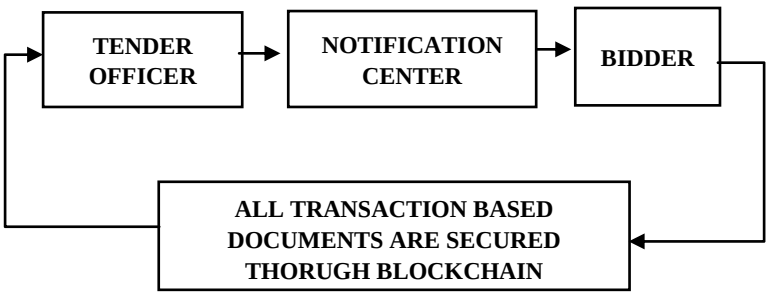

Figure1: working of blockchain

FUTURE SCOPE

There are two further research directions, which are as follows - The Smart Contract can be made more secure by using more complex cryptographic algorithms for eg. SHA-256 to encrypt its confidential contents. The use of blockchain is explored further in other government services.

CONCLUSION

When it comes to applications such as tender portals, where transparency and security are of foremost importance, traditional technologies and design patterns cannot be used as they put a threat to these requirements. As discussed earlier, there are many security requirements for a tendering framework that cannot be solved just by using a centralized tender portal for creating and bidding on the contracts.

The security requirements and openness required from this type of application can only be solved by using fair, open, decentralized technology such as

Blockchain and Smart Contracts.

In this paper, how such a system can be designed by mentioning various processes involved and their basic implementation.

REFERENCE

1. K. C. Davis, “The information act: A preliminary analysis,” TheUniversity of Chicago Law Review, vol. 34, no. 4, pp. 761– 816, 1967.

2. Ambegaonker, Ajeenkkya, Utkarsh Gautam, and Radha Krishna Rambola. "Efficient approach for Tendering by introducing Blockchain to maintain Security and Reliability." 2018 4th International Conference on Computing Communication and Automation (ICCCA). IEEE, 2018.

3. Pal, Om, and Surendra Singh. "Blockchain Technology and Its Applications in E-Governance Services."

4. Betts, Martin, et al. "Towards a safe and lawful e-tenderingenvironment."Journal of Information Technology in Construction 11 (2006): 89- 102

5. Zheng, Zibin,et al"An overview of blockchain technology: Architecture, Consensus, and Future Trends," says the author.2017 IEEE international congress on big data (Big Data congress). IEEE, 2017.

6. Pilkington, Marc. "Blockchain technology: principles and applications." Research handbook on digital transformations. Edward Elgar Publishing, 2016.

7. Wang, Wenbo, et al. "In blockchain networks, there is a survey on consensus methods and mining strategy management." IEEE Access 7 (2019): 22328-22370.

8. Cachin, Christian, and Marko Vukolić. "Blockchain consensus protocols in the wild." arXiv preprint arXiv:1707.01873 (2017).

9. Cuccuru, Pierluigi. "Beyond bitcoin: an early overview on smart contracts." International Journal

10. 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. ACM, 2016, pp. 254–269.

11. K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi,G. Gonthier, N. Kobeissi, N. Kulatova, A. Rastogi, T. Sibut-Pinote,N. Swamy et al., “Formal verification of smart contracts: