American Journal of Electronics & Communication

Anay Ghosh et. al., American Journal of Electronics & Communication, Vol. II (2), 5-11

Applications of Blockchain Technology in Financial & Personal Data Security

Anay Ghosh, Faizan Anwar, Arya Sarkar, Surya Sarkar, Sarthak Bose, Sayantan Aditya, Debanjan Saha

Department of Computer Science and Engineering,

University of Engineering and Management, New Town, Kolkata, West Bengal, India.

Abstract

Blockchain technology is defined as a decentralised-systems where the ledger that records the provenance of a digital asset is distributed amongst the users of the blockchain network. Blockchain stores and shares data in a distributed, trusted and immutable manner, removing intermediaries, and not requiring a centralized dependency for checking transactions. Transparency in blockchain provides a less complicated method for accessing ledger-based transactions over networks and makes the system more reliable in terms of data security. The technology is not actively used in today's world due to lack of research and infrastructure and hence the purpose is to modify the algorithms that can be implemented in the existing technology towards the fintech industry and help developers tackle their problems regarding financial data of the users. We surveyed plenty of resources and came across the concepts of distributed hyperledgers, integrated system architecture and secured hashing algorithms [SHA]. Using these concepts as a base we developed algorithms that are interestingly well grounded based on the statistical results gained by us while testing the algorithms. Our research indicates that the proposed algorithms can be implemented into today's technical infrastructure resolving some of the key issues faced by the users using fintech

and digital transactions for their day-to-day financial operation.

1. Introduction

Cryptographer David Chaum first proposed a blockchain-like protocol in his 1982 dissertation "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups." Further work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta. They wanted to implement a system where document timestamps could not be tampered with. In 1992, Haber, Stornetta, and Dave Bayer incorporated Merkle trees to the design, which improved its efficiency by allowing several document certificates to be collected into one block.

The first blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008. Nakamoto improved the design in an important way using a Hash-cash like method to timestamp blocks without requiring them to be signed by a trusted party and introducing a difficulty parameter to stabilize rate with which blocks are added to the chain. The design was implemented the following year by Nakamoto as a core component of the cryptocurrency bitcoin, where it serves as the public ledger for all transactions on the network

Blockchain can increase financial efficiency by reducing manual manipulation. In intercompany transactions, blockchain will create one version of the ledger allowing intercompany transparency and settlement at the same instant.

This will allow Finance to focus more towards value creation activities. The use of smart contracts will enhance governance and compliance of intercompany transactions.

The advantage of one single database is that it holds all the transactions, allowing to trace transactions, supporting documentation and reconcile accounting entries. Reconciliations between departments and subsidiaries will become almost at the same instant while ensuring transparency across all the interested parties.

Due to the immutable digital ledger that blockchain technology provides, the Triple Entry Accounting concept can apply where all accounting entries involving outside parties are cryptographically sealed and linked through a smart contract to a third entry.

In recent years, research relating to blockchain and smart ledgers has gained in popularity due to the emergence of cryptocurrencies, such as Bitcoin and Ethereum. Blockchain stores and shares data in a distributed, trusted and immutable manner, re- moving intermediaries, and not requiring a centralized dependency for checking transactions. Transparency in blockchain pro- vides a less complicated method for accessing ledger-based trans- actions over networks; it connects with different computing powers from multiple nodes in the blockchain network, making it extremely powerful with respect to calculation speed. Blockchain comprises various techniques and services, including Consensus Protocol, Hash Cryptography, Immutable Ledger, Distributed P2P Networking, and mining, which are now introduced in more detail:

Consensus protocol: In a blockchain network, certain users have individual access rights to grant transactions that are updated in the system, known as consensus protocol.

Hash cryptography: A blockchain uses SHA256 hash for adding transactions. This is developed by the NSA and is 64 characters long. Hash algorithms include features, such as one-way cryptography, deterministic, faster computation, the avalanche effect, and must withstand collisions.

Immutable ledger: All transactions in a blockchain network are recorded, while the shared ledger cannot be modified or tampered with.

Distributed P2P network: All transactions are broadcast over the network to different users to distribute and update the data.

Mining: Miners use blocks of nonce values to achieve hash values in the network. This requires high computation speed to achieve and obtain the reward.

1.1 Advantages of Blockchain

Blockchain technology uses a distributed network, containing data in tamper-resistant forms. Blockchain transactions are only updated or added through the creation of new hash values and, therefore, existing transactions cannot be modified. To understand this, the potential use of blockchain technology needs to be de- scribed against all features which make the blockchain unique from others:

a. Distributed ledger: Transactions are appended in a distributed system on the network, which creates system recovery by eliminating a single point of failure or centralized entity;

b. Consensus mechanism: Transactions are only updated when all verified users in the network agree to the condition of the transaction;

c. Provenance: The complete data or asset's history is available on the blockchain network;

d. Immutability: Records on the network cannot be modified or tampered with; thus, all information is secure and trusted;

e. Finality: When a transaction is committed on a blockchain, it cannot be modified or reversed; and

f. Smart contract: The codes are created on a blockchain network, and the computer and nodes execute on a triggered event. Hence, the codes are auto-executed within the time frame.

g. To this end, Blockchain has the potential to reduce transparency and security issues, such as trust of third parties at any stage of a transaction; this means that all intermediaries or third parties are eliminated with the advent of blockchain technology.

1.2 Problem statement

The problems that are being faced in today's world by the people regarding the security of the financial and personal data is quite distressing and hence with increase in implementation of digital technology for financial transactions the infrastructure needs to be updated in order to counter increasing cybersecurity threats and loop holes that are being discovered by the developer community as users of that services are increasing with time. Due to advancement in techniques that are used to violate the applications and services, more efficient algorithms are to be used in order to prevent frauds and data breaches.

Our research focuses on developing new algorithms using blockchain technology that can prevent forthcoming situations regarding manhandling of data and using it to manipulate, disrupt, violate or misuse of user's privacy and finances.

2. Literature review.

The proper implementation of blockchain technology depends on how fast, robust and reliable the network is and the safety of transactions are also ensured for the people to make use of it. The current scenario of blockchain and crypto-currency are at a very unstable state as most of the people fail to understand and use the technology and the one who does are taking an unfair advantage of the system. The sustainability and mapping of a robust system was vastly described in a 2019 article by Simon Fernandez-Vazquez et al which address the limitations and gaps in the fintech industry due to which they are not able to accept blockchain as a mainstream technology for transaction. These issues have been discussed widely in [4]. In order to ensure the security of the transactions that take place within the network an article published in 2018 on the topic Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application by Meiliana Sumagita et al [2] and it paves a way toward the usability of an advanced hashing algorithms that would be more reliable option for the security of a system that handles financial transactions in an efficient manner. The workflow algorithm and architecture play a very crucial role in development of such systems and ensure the convenience of operation for the user. This study shows the implementation of branched blockchain algorithm which was first introduced as a countermeasure to the vulnerabilities of a blockchain system in the year 2018 by Huru Hasanova et al. The topics and architectures have been discussed in the following article and provides a fruitful insight on then shortcomings of the system in [3].a recent published paper by

Sudeep Tanwar et al discusses the use of a health record system based on blockchain that re cross organizational and are an easy to access resource for the users and administrators that is being constantly updated and thus provides a proper infrastructure to review history and the present situations as well [1]. We in this article have discussed how it can be used in a FinTech platform to keep an eye on fraudulent transactions and suspicious activities of the network and their avoidance. Hence the proposed methods have been discussed further in the article.

3. Proposed Method.

The purpose of this proposed research is to normalize the use of blockchain technology in our day-to-day life as a solution for safe transaction and to tackle the problems faced in today's world regarding data.

A blockchain integrates fintech system is a device, physical medium, program or a service which stores the public and/or private keys. In addition to this basic function of storing the keys, they more often also offer the functionality of encrypting and/or signing information. Signing can for example result in executing a smart contract, a cryptocurrency transaction. To be very specific a dual branched blockchain is to be used which will contain the proof of work (PoW) and proof of stake (PoS) are to be stored in a distributed Hyperledger as a record of transaction and available balance for a user an account. The account can only be accessed by the user and the data cannot be violated or duplicated by any third party as it is nearly impossible to penetrate a blockchain and or to trace back and tamper the user data.

3.1 Workflow

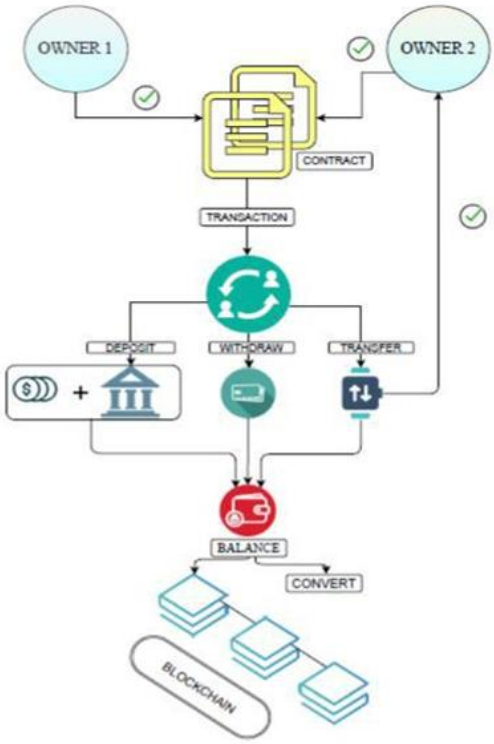


Fig1: Workflow of Process

3.2 Algorithms

The proposed algorithms that are stated below show the step-by-step functions used in the to resolve the problem encountered. The proposed fintech system has four main components / functions admin, only-owner, transaction and conversion.

3.2 Algorithms

The proposed algorithms that are stated below show the step-by-step functions used in the to resolve the problem encountered. The proposed fintech system has four main components / functions admin, only-owner, transaction and conversion.

3.2.1[ADMIN]

1. Procedure ADMIN
2. Input Aid, Access Key
3. While (true) do
4. If (Aid valid) then
5. {
6. Show Transactions
7. Start for
8. For (Transactions)
9. {
10. Show transaction history
11. List time stamp
12. Show amount transacted
13. Output WEI
14. }
15. End for Add balance
16. Enter amount in console
17. Enter access key
18. Verification (true)
19. Add balance successfully

Withdraw amount

20. Enter amount in console
21. Enter access key
22. Verification (true)
23. Withdraw amount successfully Send money
24. Enter input (Aid, receiver's address)
25. Enter amount (ether / wei)
26. Verification
27. Sent successfully
28. Else (Aid==Aid') then
29. Execute
30. Only owner function….
31. Else
32. {
33. invalid id
34. not exist
35. }
36. End else
37. End procedure

3.1.2. [ONLY OWNER]

1. Procedure ONLY OWNER
2. If (Aid + Access Key==True) then
3. {
4. execute Procedure 1
5. execute For
6. }
7. Else
8. {
9. show warning…
10.
11. }
12. End if
13. End procedure

3.1.3. [Transactions]

1. Procedure TRANSACTIONS
2. Enter input (Aid, Access Key)
3. While (true)then
4. {
5. Execute [add balance / withdraw amount]
6. Verify user
7. Create block
8. }
9. End while
10. Link block
11. Transaction successful
12. End procedure

3.1.4. [Conversion]

1. Procedure CONVERSION
2. Enter input
3. Enter amount (in console to desired currency)
4. For (amount entered)
5. {
6. Select denomination
7. Denomination wei
8. {
9. Convert denomination
10. Output currency…
11.
12. }
13.
14. Denomination ether
15. {
16. Convert denomination
17. Output currency…
18.
19. }
20. }
21. End for
22. End procedure

4. Results and Simulations

The data is fetched and simulated on open-source Ethereum platforms and the PCs used during the simulations were intel core i5 8th CPU Gen with 4gb RAM and 256gb SSD operating at a network speed of 100mbps. The

simulated data and graphs are shown further on the paper and provides an insight over the working of algorithms collectively.

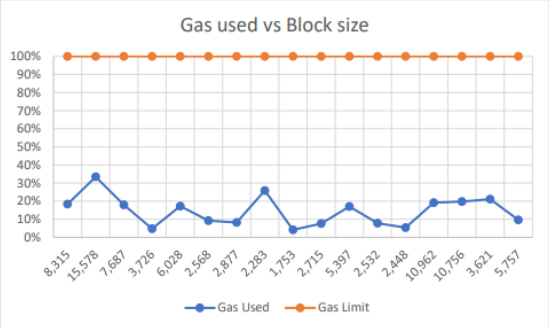
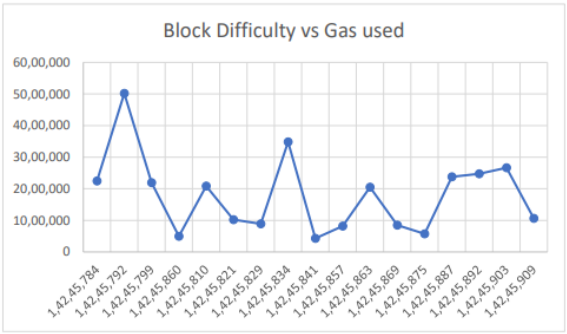


Fig 4.1: Graph of Gas used vs Block size.

The following graph (fig 4.1) shows the gas used by the block for adding it to the network (in percentage consumed) as we can see that the maximum limit for adding a block is depicted by the gas limit (line in orange) and hence the gas consumption for the adding a single block is 35% of the gas limit assigned for addition of a new block of transaction. The hypothesis may change after a certain number of block cycles.



s **Fig 4.2: Graph of Block Difficulty vs Gas used (in Gwei)**

The second graph (Fig 4.2) gives an idea about how the difficulty of mining a block affects the gas consumption or the amount of Ethereum derivative(Gwei) is being used for transaction and is increasing difficulty it is being decreased and hence the more number of contracts and block are added into the network the difficulty of mining a successive block increases , with increasing difficulty in mining the efficiency of the network increases Fig 4.2: Graph of Block Difficulty vs Gas used (in Gwei) simultaneously. Block Difficulty is a multiple of the minimum amount of PoW that any valid block can contain. It represents the number of estimated hash it takes to find a valid has that is to be entitled to a block.

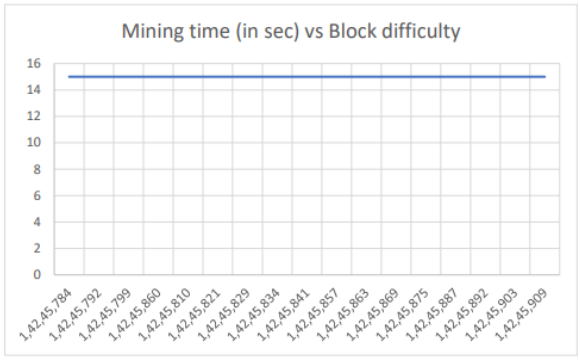


Fig 4.3: Graph of Mining time of a block vs Block difficulty

Third Graph (Fig 4.3) shows the mining time of block vs its difficulty as the time remains constant it can also increase as the difficulty of the network increases with time.

Systems are needed to assigned in order to decrease the time consumed by the function and use it in real time for transaction of digital currencies. Hence the time taken for each new blocked to be mined is 15 sec and it remains constant for the present cycle.

5. Conclusion

The use of blockchain in the domain of fintech and data security increases the reliability for the user as it is easier trust a decentralised system in terms of data privacy and security. The implementation of the system plays a critical role as it would dilute the concentration of data handled by a single organisation and would also reduce the monopoly created in the market over user data. The proposed method can further be improved in the following section based on the technological advancements that are still to be done in the near future.

a. Block security: Our proposed research makes the use of secured hashing algorithm (SHA-256) and a dual branched blockchain architecture to secure the data provided by the users, but further

improvements can be made by testing secured hashing algorithm (SHA-512) and a multibranched blockchain architecture to the existing algorithms in order to get better results regarding the encryption and decryption process for user data.

b. Hyperledger management: The existing block architecture uses a dual to one Hyperledger (Dual branched blockchain is connected to a single Hyperledger), this makes it easier to transfer Hyperledger from one machine to another increasing the portability but at the same time makes the blockchain vulnerable. This can be tackled by improving the ledger architecture, for example: using a segmented ledger, multiledger system (still in R & D).

c. Infrastructural Advancement: Applying the existing algorithms into a more advance machine significantly reflect the difference in results produced as the algorithms can be dynamically modified to support various different platforms and more advanced infrastructure (Supercomputers, Quantum Computers etc.).

References.

[1] Sudeep Tanwar, Karan Parekh, Richard Evans; Blockchain-based electronic healthcare record system for healthcare 4.0 applications; Journal of Information Security and Applications 50 (2020) 102407

[2] Meiliana Sumagita and Imam Riadi; Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application; International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(4): 373-381The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-001

[3] Huru Hasanova , Ui-jun Baek ,Mu-gon Shin , Kyunghee Cho, Myung-Sup Kim; A survey on blockchain cybersecurity vulnerabilities and possible countermeasures

[4] Simon Fernandez-Vazquez, Rafael Rosillo *, David De La Fuente and Paolo Priore; Blockchain in FinTech: A Mapping Study.