Augmenting integrity and scalability in mobile payment applications using blockchain

Shibin David^{1}, Jasper W Kathrine¹, K Martin Sagayam² and Krit Salah-ddine³*

¹Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, India

²Department of Electronics and Communication Engineering, Karunya Institute of Technology and Sciences, Coimbatore, India

³EDP Department of Informatics - Physics, Ibn Zohr University, Agadir Morocco

Abstract. The transactional information from the mobile wallets is offloaded from the mobile device to the mobile transaction server. The transaction involves various communication standards, confidential transaction information to ensure flawless transaction of data. There exist several encryption techniques to preserve confidentiality, hashing schemes to prove the integrity, signature schemes to prove the identity in the mobile transaction using mobile wallet applications. Even though mobile wallet possesses secure algorithms, the transactions are facing security issues such as double spending, lack of dispute redressal issue, lack of forward secrecy, lack of anonymity in the transaction and security. Therefore, Blockchain based Mobile transaction Scheme is proposed to solve the security issues including integrity, double spending and improve scalability. This paper presents a strategy which implements blockchain framework by using irreversible keys for mobile wallet applications. The proposed scheme proves to be secure against the security attacks and enhances integrity and scalability compared to the existing schemes.

1 Introduction

Blockchain is a distributed ledger used to transfer the data from one node to another node and only authorized people can open the data [1]. A centralized operation that stores and administers the data and access control policies in centralized ways and leads to a single point of failure. This causes a bottleneck for the entire system since block chain is decentralized in nature; it does not have a single point failure. Blockchain is considered the more secure way to carry out the transaction via the network. Because of its decentralized nature and cryptographic algorithm, it becomes a hard issue to be attacked by a third party.

The process of verifying and registering transactions on the Blockchain is immediate and permanent [1,2]. The ledger is distributed across multiple nodes, meaning that each data has its replica and is instantly stored across the system at each node. When a transaction is processed in the block chain, all nodes record, and check and settles details of the transaction, such as price, asset, and ownership, within seconds. A change/modification reported on any one ledger is also recorded on all other copies of the ledger at the same time. Because each

transaction is recorded transparently and securely across all ledgers, there is no need for third party verification and is free for all to witness.

To create the block, the hash of the last block in the chain is chosen, combined with its own collection of messages and hash of the newly created block is created. Considering three blocks, each contains data about transactions and if we compare it with some stand-alone word documents, the transaction is clearly defined as the flow process. All these blocks are combined together. To get the final block, each block gets a unique digital signature that exactly matches the data string in that block. If something changes within a block, the block will get a new signature. This change occurs even if only a single digit changes [3,4]. Now apply the hash rule in each block and secure the data. User feeds the data to the hash function and generates the hash of data. The hash and private key are then fed to the algorithm of signatures, which generates a digital signature on a certain hash. The consumer then transmits the data to the intended receiver with the digital signature. The recipient verifies the hash value generated by the sender and feeds the receiver into the algorithm after receiving the data and the signature. The hash value is generated

*Corresponding author: zionshibin@gmail.com

as the output. In order to establish the hash value of the original data, the receiver often uses the same hash function. The recipient gets the assurance that a digital signal is accurate if the newly created hash value matches the user's hash value.

Blockchain is a distributed ledger system [3] that can transfer data between users efficiently. The transaction is stored in records called blocks and each block is connected to form a Blockchain. Each block in the Blockchain contains the transaction data, hash value, hash of prior block and timestamp. It is a decentralized ledger, which helps to manage the data and its decentralized nature, and the cryptographic algorithm makes it immune to attack.

The Blockchain is designed in such a way that it refuses modification. Blockchain is used for secure transaction of data over the network. The idea of the Blockchain technology came into existence in 2008 [5-7]. Blockchain uses decentralized distributed ledger which makes transactions to get stored in every block after that if we want to modify the data it has to be done in every block, which is difficult for the attackers to find each blocks and modify the data.

The major two categories of block chain include public and private Blockchain [8]. Public blockchain is a fully decentralized blockchain and anyone is open to join the network. Private blockchain is more centralized than public blockchain and in private blockchain; only authorized people can access the data. Ex. Hyper ledger and R3 corda.

The scope of the paper is

- To study the Blockchain mechanism and its proof.
- To enhance the integrity and scalability of the existing mobile transaction mechanisms.
- To avoid double spending and fraudulent transactions

2 Background and Research Motivation

Block chain comprises blocks of data which are interlinked with each other. Each data block is the hash value of the previous block present in the chain. The number of blocks created in a chain depends on the size of the input bits present in the data. Figure 1 represents the general flow of the block chain.

Fig. 1. General Flow of block chain

Each block comprises the record including the hash value of its own and the hash value of the previous block along with the time stamp used to create the message digest. The average size a block present in the block was reported as 1.33 MB. The data used in each block are also appended with the hash values generated using a secure hashing algorithm. The same process is continued for the multiple numbers of blocks present in the data transmission [9,11]. Figure 2 represents the records present in the block and the inter-link of the blocks in the block chain. When the number of transactions increases, the need for security increases and the integrity of the transaction needs much attention. The use of this block chain process can be implemented in crypto currency wallet which makes the digital asset unalterable.

Fig.2. Hashing mechanism

2.1 Block chain in E-commerce applications

Ecommerce and other industries have started to realize the importance of blockchain technology for their business growth and effective interactions with the customers [10-12]. Blockchain will serve as the backbone of digital trust, providing security at interactions on a massive scale. It will allow for decentralized marketplaces to emerge with no centralized team and will provide lower prices for consumers and better rules for retailers. Blockchain technology and e-commerce unlock a host of interesting business prospects in the pursuit of transparency, trustworthiness and cost reductions [13].Block chain can be implemented in one of the e-commerce applications called mobile wallets for improving the scalability and integrity of the transaction between the end users.

Fig.3. Block chain architecture in mobile transactions

Figure 3 depicts the transactional flow between the customer wallet and vendor wallet. When a customer initiates the transaction, the transaction details are appended and communicated through the network. The transactional information are validated in the network and sent for verification. Verification process includes the verification of the transaction information including the identity of the customer, time stamp, nonce value,

transaction amount, digest value. Block chain plays an important role in performing an irreversible transaction which is acknowledged before it reaches the vendor wallet. This proves the identity of the user involved in the transaction, validates the transaction and enhances the scalability of the transaction.

Initially when a customer login using a mobile wallet application, the password is encrypted using a symmetric encryption algorithm. When the password matches with the stored password available in the database of the application, then the transaction is allowed after proper verification. If it doesn't match with each other, then the transaction is not permitted and the session expires. Figure 4 depicts the password verification process in the mobile wallet applications.

Fig.4. Password authentication

2.2 Steps involved in the mobile transactions

Nowadays Global transactions are prone to money laundering and high cost. Remittance companies such as Abra, Align Commerce and Bitspark that offer end-to-end blockchain-powered remittance services already started using blockchain for global transactions which gives better solutions. Santander, the first bank to merge blockchain to payment app, is one such example, which allows 24 hours payment and clears the next day.

The VAT administration system[14] works as a centralized server which is easily open for hackers to hack into it. In this paper, the decentralized storage network (DSN) and the smart contract (SC), are combined to create a new model based on Blockchain technology to authenticate the transaction, calculate Value-Added Tax and approve VAT payment, which runs on a host PC for encrypting and decrypting data.

Between the parties involved in a transaction, instruments through which viable off-chain agreements could be made. This is known as latent transactions [15] which is used for late payments. It also gives the catalog where any blockchain member can subscribe and from where one can sell services in a real-time manner with adaptive pricing, based on the context (demand, activity at runtime etc.).

The steps involved in the transaction are as follows.

of securities. Any peer of the network can trigger transactions.

2. The transactions are always forwarded to the broker to validate orders.
3. The broker sends the order to an investment manager who will broadcast the ordered transactions to all peers for consensus, or agreement, on the proposed order.
4. If the order of transactions is agreed upon, the transactions are executed and appended to the ledger on each validating node. The ledger is then replicated to all network peers.
5. The central counterparties will handle the movement of cash for the transaction of order and do the confirmation.
6. The central securities depository takes a role along with custodians and maintains asset ledger. It handles fund and asset transfer and security services.

2.3. Consensus Algorithms - An overview

One of the essential components in the distributed blockchain is the application of a Consensus mechanism to the blockchain. Consensus mechanisms [16] allow secure updating of a distributed shared state and have been a topic of active research in the past three decades. This is a method through which distributed peers come to an agreement to validate the transaction. There are numerous consensus algorithms designed under various assumptions to solve different problems. However, there is no perfect consensus algorithm to suit any problems of concern.

The consensus algorithm is a mechanism that makes all blockchain peers come to an agreement with the same message, and to ensure that the latest block added to the chain is correct. It should guarantee that the message stored by the peer will not create any fork attack and the system remains protected from malicious attacks. If the consensus of peers agrees upon the transaction's validity, then the transaction is considered valid. However, arriving at an effective consensus with a large number of users is difficult and time-consuming.

There is always a trade-off among consistency, availability and partition fault tolerance (CAP) while applying consensus algorithms. Consensus protocols have three key properties including Safety, Liveness and Fault Tolerance. This section details and provides insights into the most widely used consensus algorithms of the distributed blockchain.

2.3.1. Proof-of-Work (PoW)

This consensus algorithm is the most commonly used method for many peers to accept a block. As a blockchain network with distributed peers does not have a central authority to validate or confirm the transactions, choosing a participant to validate a transaction becomes crucial to build the blockchain [17]. Adding a block to the chain requires confirmation from any special peer. A special peer or node that is capable to gather all the transactions into blocks and provide confirmation is called a miner and the process is called mining.

In this method a complex puzzle that is time-consuming and difficult to solve but easy to verify is given to the miners. The solution to the puzzle is carried out in random fashion with multiple trial and error methods before the proof of work is produced. The miner who solves the puzzle can create a new block and confirms the transactions. One of the methods is hashing the input values. The current block will contain the hash of the previous block and this makes the method computationally intensive if the number of users and network is high. As the probability of new block generation is low because to create a new block all the previous blocks have to be regenerated. So, tampering of data is not possible. Ethereum and Bitcoin make use of the PoW consensus model. Though this model ensures security, the computational cost of mining is high and requires complex hardware with huge computation power. This PoW consensus method is adopted by Ethereum and Bitcoin.

2.3.2. Proof-of-Authority (PoA)

This consensus algorithm finds most trustworthy node for validating the transactions. There is no guarantee that the person more stake can dominate the blocks in the chain. As in Point of Sale (PoS), the single miner can operate the blocks out of self-interest. But this can be avoided in this method. The decision taken on a miner or validator is confirmed and approved by the majority of the peers in the blockchain network[18]. So, the blocks and transactions are approved by the validator. This model works similar to a PoW with a centralized scheme, PoA allows only trusted peers as validators. As this PoA works based on trusted validators, this system is applicable for a private and test blockchain. However, it can also be applied in the public blockchain network. This is model requires no computational power and doesn't require communication between the peers to arrive at the consensus. This method removes the concerns on holding the stake to continue as a validator as in PoS. This model is applied in various scenarios and helps maintain the privacy of the validators.

3 Proposed Methodology

The proposed methodology is used to enhance the integrity and scalability of the transaction made using the mobile wallet applications. Block chain technology is applied over the huge transaction made using the mobile wallets which preserve the digital asses of the user. This scheme is applied over the application for verification and validation of the user request and provides the successful transaction between the users.

Table. 1. Notations used in the protocol

Notations used	Meaning of the notation
d	Transactional data
k_i	Secret key
N	Nonce value
t_s	Time stamp
$E(d)$	Encrypted transactional data
H	Quark hash function
A	User A
B	User B

In our protocol, user A is allowed to initiate the communication with user B. Initially, per-transaction key is generated to encrypt the data to be transmitted. The encryption of the data takes place using a symmetric encryption algorithm (AES) and the encrypted data is

communicated over the network. The transaction is proven to be valid once it reaches a consensus as per the order of occurrence of transaction. In this model, a block chain validator is present in the communication channel to perform validation by checking whether the transactions are legal. When a transaction is broadcasted into the network, miners undertake a transaction and validate it. After verifying its legitimacy, it is put into a block.

The transactional data including the timestamp, hashed encrypted data, nonce, and the original data are appended together before it reaches the verification stage. The miners present in the network will listen to multiple transactions due to latency.

Fig.5. Proposed model

Hence, each miner will be able to verify transaction and build their own block. The priority of choosing the transaction depends on the transaction fee made by the initiator. When the transactions are monitored and owned by individual miners, they arrive at a consensus on which the successive block is included. When user B, receives the information pertaining the transaction, it will be irreversible and legitimate.

4. Analysis of the proposed model

4.1. Scalability

Another important challenge in implementing the blockchain technology is handling the decentralized system with a huge number of peers. Scalability is the

feature of handling the increase in the load of transactions. As a result, transaction, processing rate and the latency of communication increase. Due to the consensus protocol, the latency between the transaction submission and confirmation is affected. In the proposed model, there are possibilities for 'n' number of transactions to be performed from the user's end. But, our protocol is designed to manage the volume of transactions involved in it. Scalability can be measured as the ratio of block size with that of the average transaction size in bytes. Figure 6 represents the various measure of scalability in Ethereum, bitcoin, visa and our proposed protocol. The inference of this property is that scalability needs much concentration to manage the consensus mechanism.

Fig.6. Number of transactions performed by various protocols per month (approximately)

4.2. Blockchain Audit

Auditing a blockchain brings several complexities. Firstly, real-time analysis is difficult because of the possibility of forks, which guarantees no reliability of data. The streamline of financial reports and audit processes are required to manage the network. The written records could still have tampered and the blockchain could be rebuilt if a majority of the participants reach a consensus. In this perspective, it becomes extremely difficult for a regulatory authority to audit blockchain and to check whether the data and transactions have tampered or not. Therefore, it is a challenge to secure the data and prevent vulnerabilities from fraudulent users. However, our protocol is designed in a perspective to improve the integrity and avoid double spending in transactions. This involves protection of transaction messages from tampering and other security issues such as fraudulent transactions can be avoided.

5. CONCLUSION

The proposed protocol applies the consensus algorithm upon the mobile transactions and creates a block chain. In the proposed protocol, validation and verification of the transaction using the mobile applications are done with the involvement of miners. The mined transactions based on the priority of transaction fee payment get entered into the block. With the help of quark hashing and the per-transaction key, the transaction is secured and achieves integrity and scalability. This can also be applied on the mobile wallet applications to avoid double spending, fraudulent transactions in it.

References

1. Xiao, S., Research on the information security of sharing economy customers based on block chain technology. *Information Systems and E-Business Management*, 18(4), 487–496 (2020). <https://doi.org/10.1007/s10257-018-0380-4>.
2. Chen, Y., Zhang, Y., & Zhou, B., Research on the risk of block chain technology in Internet finance supported by wireless network. *Eurasip Journal on Wireless Communications and Networking*, 2020(1) (2020).
3. Xu, Y., Wu, M., Lv, Y., & Zhai, S., Research on application of block chain in distributed energy transaction. In *Proceedings of 2017 IEEE 3rd Information Technology and Mechatronics Engineering Conference, ITOEC 2017* (Vol. 2017-January, pp. 957–960) (2017).
4. YAN, H., HUANG, B.-B., & HONG, B.-W., Distributed Energy Transaction Pattern and Block Chain Based Architecture Design. *DEStech Transactions on Environment, Energy and Earth Sciences*, (epee) (2018).
5. Lee, K., James, J., Ejeta, T., & Kim, H., Electronic Voting Service Using Block-Chain. *Journal of Digital Forensics, Security and Law* (2016).
6. Jovicic, S., & Tan, Q., Retracted: Machine learning for money laundering detection in the block chain financial transaction system. *Journal of Fundamental and Applied Sciences* (2018).
7. Lü, L., Li, G., Hu, J., Zhen, H., Xiang, Z., & Zhou, G., Research on support environment of user side peer-to-peer transaction in energy block chain. *Dianli Jianshe/Electric Power Construction*, 40(5), 38–47 (2019).
8. Block-Chain Based Authentication Technique., *International Journal of Engineering and Advanced Technology*, 9(3), 1127–1133 (2020).
9. Mubarakali, A., Bose, S. C., Srinivasan, K., Elsir, A., & Elsier, O., Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain. *Journal of Ambient Intelligence and Humanized Computing* (2019).
10. Kumar, M. V. R., Singh, S., Bhandarkar, M. A., Prashant, P., & Bhalaji, N., Block chain technologies for fund release as finality in financial transaction. *International Journal of Innovative Technology and Exploring Engineering*, 8(7), 46–49 (2019).
11. A Study on the Privacy Act for Block-chain Based REC Transaction System., *Korean Lawyers Association Journal*, 68(6), 121–157 (2019).
12. Fu, X. T., Chen, S., & Zhang, N., Proxy-cryptocurrency payment system. *Tongxin Xuebao/Journal on Communications*, 38(7), 199–206 (2017).
13. Gupta, A., Patel, J., Gupta, M., & Gupta, H., Issues and Effectiveness of Blockchain Technology on Digital Voting. *International Journal of Engineering and Manufacturing Science*, 7(1), 20–21 (2017).
14. V. C. Nguyen, H. L. Pham, T. H. Tran, H. T. Huynh, and Y. Nakashima, "Digitizing invoice and managing vat payment using blockchain smart contract," in *ICBC 2019 - IEEE International Conference on Blockchain and Cryptocurrency*, , pp. 74–77, 2019.
15. A. B. Popa, I. M. Stan, and R. Rughiniş, "Instant payment and latent transactions on the Ethereum Blockchain," in *Proceedings - 17th RoEduNet IEEE International Conference: Networking in Education and Research, RoEduNet 2018*, 2018.
16. A. Baliga, "Understanding Blockchain Consensus Models," no. April, 2017.
17. S. Zhang and J. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Express*, no. xxxx, pp. 1–5, 2019.

18. S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs Proof-of-Authority : Applying the CAP Theorem to Permissioned Blockchain," pp. 1–11.