ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

A Solution for Banking Sectors to Make Secure Transaction Using Blockchain Technology

Mr.C.Manikandan[1], M.Sharmi[2], R.Sumi[3], S.Thangam[4]

Teaching Fellow, Department of Computer Science and Engineering, University College of Engineering, Nagercoil, Tamilnadu, India[1]

Student, Department of Computer Science and Engineering, University College of Engineering, Nagercoil, Tamilnadu, India. [2,3,4]

ABSTRACT: The banking industry is very much regulated for all jurisdictions, while banking sector representatives are distinguished by their conservative attitudes. The traditional banking system depends on the centralized servers which bring significant trust issues. The new technique employes the blockchain technology which is a shared and trusted public ledger of economic transactions that are grouped into blocks. The blockchain is an unhackable data storage system. But the wide dissemination of blockchain in the recent years, the overwhelming popularly of cryptocurrencies have contributed to the fact that management of many banks and financial organizations no longer deny the potential of blockchain technology. Large banks are increasingly conducting tests of decentralized asset technology and implementing blockchain in business processes. Banks continue to invest in a variety of projects and start-ups that are developing blockchain-based solutions. The unique hashes and proof of works thereby reduce the conflicts in the transactions that makes the system as another advantage.

KEYWORDS: publicledger, cryptocurrency, uniquehashes, proof of work

I.INTRODUCTION

Banking and financial services sector plays vital role in the development of a nation's economy. The past two decades witnessed dramatic transformations in the ways of doing business as more and more technological solutions were aggressively used in these financial institutions. The introduction of technological solutions have brought in convenience to the customers and cost effectiveness from the banking perspective, thus banks are highly obliged to maintain integrity of financial transactions and protecting the privacy of customers while being accountable to the stakeholders. However, the adoption of these technologies has brought in a large number of information security threats that may cause financial liabilities to the banks. Such information breach incidents may also result in tarnishing the goodwill of a bank and may lead to losing large number of existing customers. Therefore, understanding the information security threats and preventing such incidents are highly required in a professional banking environment. Thus, the present study focuses on studying the various information security threats faced by the banks and further propose practical suggestions for managing the information security threats.A Blockchain is a decentralized no single entity holds control over the system and all the members of the blockchain are equally responsible for enforcing and approving all the transaction, distributed database that is used to maintain a continuously growing list of records, called blocks. Each block contains a timestamp and a link to a previous block.Every transaction in a blockchain is verified by all the member of the network which restricts manipulations and improve security.By design and by purpose blockchains are inherently resistant to modification of the data.All transcations are secured, private and confidential.Fabric can only be updated by consensus of the participants.Functionally, a blockchain can serve as an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

way. Blockchain technology could be applied to many data processing functions, payments and fraud reduction are two areas with immediate traction. It's a technology that uses distributed databases and cryptography to record transactions. Blockchain was created to serve as the public transaction ledger for cryptocurrencies and its comingimpact on banks is a topic of wide debate within the financial sectors.

II.RELATED WORKS

Blockchain is like a Database, a way of storing records and transactions, Almost anything is recorded in Blockchain. Most transactions are between people need an intermediary to provide Trust and Security to facilitate the transactions.

L. Atzori,[1] proposed by "The internet of things:A survey,"to described Information should be the focus of communication and networking solutions. A secure scheme for IoT data storage and protection based on blockchain and blockchain overcomes the drawback of certificatess cryptographyby offering a platform for broadcasting the publickey of a user.K. G. Paterson,[2] proposed by"Certificateless public key cryptography," To avoid escrow of ID based cryptography.All the cryptographic operations by the user are performed by using a complee private key which involves both the KGC's partial key and the user's random secret value.The use of public key cryptography which avoids the inherent escrow of identity-based cryptography.I. Eyal, [3] proposed by "Bitcoin-ng: A scalable blockchain protocol."Bitcoin-NG shows that it is possible to improve the scalability of blockchain protocols to the point where the consensus latency is limited solely by the network diameter and the throughput bottleneck lies only in node processing power. Such scaling is key in allowing for blockchain technology to fulfill its promise of implementing trustless consensus for a variety of demanding applications including payments, digital asset transactions, and smart contracts—at global scale.S. Dziembowski, [4]proposed by "Proofs of space,"Construct a practical protocol for implementing these proofs (Posts).Increased by extending the time period over which data is stored without increasing computation costs.A decentralized digital currency scheme called Spacecoin is constructed that uses PoS to prevent double spending.F. Zhang[5], proposed by"Rem: Resource-efficient mining for blockchains." To show promise as potential infrastructure for financial transaction systems.REM is practically deployable and promising path to fair and environmentally friendly blockchains in partially-decentralized blockchains.A. Sahai[6]proposed by"Fuzzy identity-based encryption," Fuzzy Identity Based Encryption, which allows for error-tolerance between the identity of a private key and the public key used to encrypt a ciphertext. We described two practical applications of Fuzzy-IBE of encryption using biometrics and attribute-based encryption. Identity Based Encryption(IBM) schemes are both error-tolerant and secure against collusion attacks.S. Goldfeder[7],proposed by"Securing bitcoin wallets via a new dsa/ecdsa threshold signature scheme," To provide security ,implemented it and evaluated a two factor secure bitcoin .It eliminating single point of failure at every stage.K. Croman[8],proposed by"On scaling decentralized blockchains," To increasing popularity of blockchain-based cryptocurrencies has made scalability a primary and urgent concern.The results suggest that reparameterization of block size and intervals should be viewed only as a first increment toward achieving next-generation, high-load blockchain protocols, and major advances will additionally require a basic rethinking of technical approaches.L. Luu[9], proposed by "A secure sharding protocol for open blockchains," Most existing work related to Blockchain is ELASTICO, the first candidate for a secure sharding protocol for permissionless blockchains. At its core, ELASTICO scales up the agreement throughput near linearly with the computational power of the network and tolerates byzantine adversaries which controls up to one-forth computation capacity, in the partially synchronous network. It offers promising scalability in experiments and suggest strong usability in next-generation cryptocurrencies. E. Buchman,[3] "Tendermint: Byzantine fault tolerance in the age of blockchains",Byzantine not depends on centralized trust parties which solves a problem in public setings without a central authority.Terdetermint is high performance acheiveing 1000 of transaction per seconds.It contains two nodes can communicate safely across the network.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

III.ARCHITECTURE DIAGRAM

A.USER TRANSACTION

A user signs off on a transaction from their account, attempting to send a money from them to some one else

B.MINING

New transactions are broadcast to all nodes. Each node collects new transactions into a block. Each node works on finding a difficult proof-of-work for its block. When a node finds a proof-of-work, it broadcasts the block to all nodes. Nodes accept the block only if all transactions in it are valid and not already spent. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

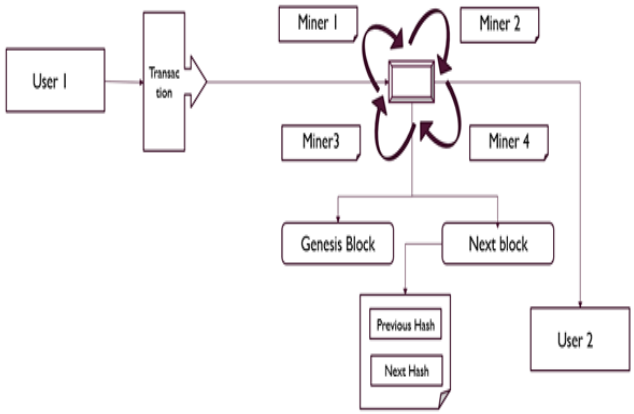

Figure1.1:Transaction Using Blockchain

C.BLOCK GENERATION

Every block in a blockchain consists of the same components. A block number,The hash of the previous block (via this means the 'chain' is being formed), Nonce, a Data: the transactions Timestamp :with the time the block is created / found , The hash of the current block

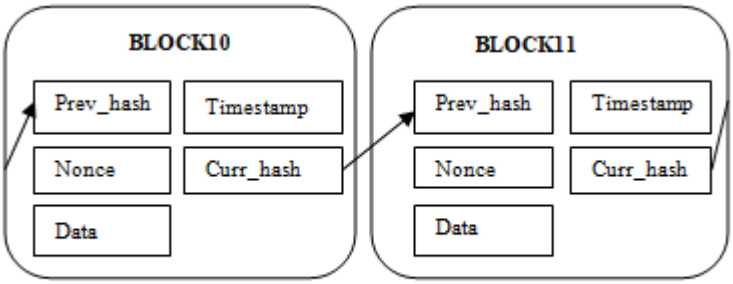

Figure 1.2: Two subsequent blocks in blockchain with their attributes

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Every block has a block number which, combined with the previous hash and the current hash, determine the order in which the transactions took place. The accompanying timestamp determine the time at which the transactions are recorded to have taken place. The Data contains the transactions, which could consist of nearly everything, not solely valuta. Last, but not least, there is the Nonce.

IV.ALGORITHM

To generate the hash value using SHA-256 algorithm and proof of work using Dagger hashimoto algorithm.

A.SECURE HASH ALGORITHM(SHA-256)

Secure hash algorithm is a cryptographic hash function with digest length of 256 bits.It is a keyless hash function.

STEP BY STEP HASHING WITH SHA-256

1.Padding: If *M* the message to be hashed, and *l* its length in bits where $l < 2^{64}$, then as a first step we create the padded message *M'*, which is message *M* plus a right padding, such that *M'* is of length *l'*, a multiple of 512.
2. Blocks: *M'* is parsed into *N blocks* of size 512 bits, M^1 to M^N, and each block is expressed as 16 *input blocks* of size 32 bits, M_0 to M_{15}.
3. Hash initialization**:** The initial hash value H^0 of length 256 bits (8 input blocks of 32 bits) is set by taking the first 32 bits of the fractional parts of the square roots of the first eight prime numbers
4.Message schedule.**:**We create a message schedule W^i, consisting of four 512-bit message blocks (each made of 16 input blocks). The first block of W^i is message block M^i, and the next three blocks are variations of M^i
5.The big shuffle**:** The input blocks of message schedule *W* are fed, one after the other, inputs a hash $\omega^i(t)$ and a message schedule input block $W^i(t)$, and outputs a hash $\omega^i(t+1)$. The initial hash $\omega^i(0)$ fed to the graph is the intermediate hash H^{i-1}: in the case of W^1, it's H^0 defined in the preprocessing step. $\omega^i(0)$ and $W^i(0)$ produce $\omega^i(1)$; inturn $\omega^i(1)$ and $W^i(1)$ produce $\omega^i(2)$, etc., until $\omega^i(63)$is produced.
6. New hash: After all input blocks from W^i have been used and we $\omega(63)$ has been created, we can create the new hash H^i such that each input block of H^i is the sum of the corresponding input block of H^{i-1} plus the corresponding input block of $\omega^i(63)$:
$H^i(j) = H^{i-1}(j) + \omega^i(63)(j)$ where, + is the addition modulo 2^n

B.DAGGER HASHIMOTO

The initial hashing algorithm used was supposed to be "dagger" algorithm that uses part of memory and fills it with random data generated from the nonce and header of the block.The way proof of work in bitcoin was generated is using sha256 over the nonce, *previous_block_hash* and *merkle_root.*

Step1:
ASIC machines execute sha256 very effectively. When a hash is generated using the *previous_block_header*, *merkle_root* and *nonce* it is used to generate another hash and that hash is what is compared to the hash target i.e if it is a successful hash you will have a proof of work.
hash_1 = sha256(previous_block_header, merkle_root, nonce)

Step2:
The second operation in Hashimoto is doing some shifting followed by modulo operations. So the hash_1 would be shifted right by one bit and increments every transaction. this will result in a new outcome which we will call "shifted_hash"

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

```
N = 64 #number of transactions
tx_ids=[]
for i in range(N):
    shifted_hash= hash_1 >> i #shift i bits to the right
```

Step3:
Next, the modulo of the shifted number will be calculated to choose a block number to get transactions from.
block = shifted_hash mod number_of_blocks #get a block from shifted_hash

Step4:
The transaction is chosen the same way we choose a block; except this time we will use the block's total number of transactions, let us call it all_block_transactions.
transaction = shifted_hash mod block.all_block_transactions

Step5
now for that transaction we obtain its id and shift left one bit. We keep that in the list tx_id[]
tx_ids.append(get_txid(transaction) << i)

Step6:
now the tx_ids[] has all N transactions. the next operation would be to XOR them together
tx_ids_all_XORd = functools.reduce(lambda i, j: int(i) ^ int(j), tx_ids))

Step7:
now tx_ids_all_XORd would be used as input to generate the final hash. the nonce would be shifted left to the most significant bit.
x_ids_all_XORd and with shifted_nonce would be XORed to generate the final hash.
final_output = tx_ids_all_XORd ^ shifted_nonce

V. SCOPE OF THE PROJECT

Blockchain could also lead to greater trust between trade partners due to their access to shared, trustworthy records and the technology's strong security features. This, along with real-time transactions, will increase the velocity of money and in turn cash flow and capital investments. Blockchain technology provides a high level of safety in storing and transmitting data, open and transparent network infrastructure, decentralization and low cost of operations. These impressive characteristics make blockchain a really
promising and in-demand solution, even in the extremely conservative and restricted bank industry.

VI.PROPOSED WORK

The traditional bank system uses centralized cloud for storing customer information that means we are placing a very large amount of trust in these third parties, particularly sensitive information like account details transaction etc.Blockchain reduces the number of middlemen while increasing security, which could reduce industry-wide transaction and processing costs by billions..A Blockchain functions as an open, decentralized ledger that effectively keeps track of transactions between two parties in a permanent and verifiable way.

VII.PERFORMANCE ANALYSIS

We analyse the performance for our scheme from two aspects security and threats.In traditional banking to provide high security but the level of threats also high.The Blockchain technology reduces the level of threats at the same time that provides the more security.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

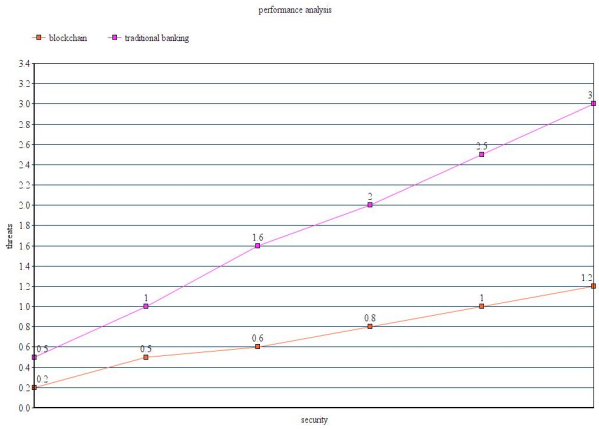

Figure 1.3 Security Vs Threats

VIII.FUTUREWORK

Blockchain and distributed ledgers have a bright future. As real-time, open-source and trusted platforms that securely transmit data and value, they can help banks not only reduce the cost of processing payments, but also create new products and services that can generate important new revenue streams.The biggest key to turning blockchain's potential into reality is a collaborative effort among banks to create the network necessary to support global payments. Banks need to look at the bigger picture and work together—and with non-banks—to help define the backbone that can underpin a universally accepted, ubiquitous global payment system that can transform how banks execute transactions.

IX.CONCLUSION

Blockchain technology could have a tremendous impact on the procedures for concluding and confirming transactions, managing cash, and optimizing assets, as well as many other business processes which altogether account for billions of dollars in annual expenses for banks today.The solutions developed are much faster and more reliable than most blockchain-based solutions on the market. We do our best to ensure that our technology is developed and implemented not only by companies in the IT sphere, but also in real sectors of the economy. Banking is one of the most promising spheres to benefit from the advantages of blockchain.Blockchain makes it possible to reduce timeframes that have become accepted and established, such as the time from a loan application being approved to the funds actually being received, the time required for interbank or international transfers to be carried out, the time required for processing and confirming personal information, and so on.Blockchain has passed the point of being a dreamy idea for the banking sector—it is already being implemented successfully.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010
[2] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in Asiacrypt, vol. 2894. Springer, 2003, pp. 452–473.
[3] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol." in NSDI, 2016, pp. 45–59
[4] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in Annual Cryptology Conference. Springer, 2015, pp. 585–605
[5] F. Zhang, I. Eyal, R. Escriva, A. Juels, and R. van Renesse, "Rem: Resource-efficient mining for blockchains." IACR Cryptology ePrint Archive, vol. 2017, p. 179, 2017
[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology–EUROCRYPT 2005. Springer, 2005, pp. 457–473
[7] S. Goldfeder, R. Gennaro, H. Kalodner, J. Bonneau, J. A. Kroll, E. W. Felten, and A. Narayanan, "Securing bitcoin wallets via a new dsa/ecdsa threshold signature scheme," 2015

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

[8] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer et al., "On scaling decentralized blockchains," in International Conference on Financial Cryptography and Data Security. Springer, 2016, pp. 106–125
[9] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016, pp. 17–30
[10] E. Buchman, "Tendermint: Byzantine fault tolerance in the age of blockchains," Ph.D. dissertation, University of Guelph, 2016.