IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-18, May 2019 E-ISSN: 2347-2693

Impact of Blockchain to Secure E-Banking Transaction

Mausumi Das Nath[1]*, Tapalina Bhattasali[2]

[1,2]St. Xavier's College (Autonomous), Kolkata, India

*Corresponding Author: m.dasnath@sxccal.edu, Tel.: +91-9830659302

Available online at: www.ijcseonline.org

***Abstract*—** Although E-banking provides its customers a wide range of services at anytime and from anywhere, most of the research studies have indicated that security is the major concern to adopt it without any doubt. As digital world is full of known and unknown cyber threats, there is a real need to protect sensitive records from misuse. Blockchain is a new technology that just steps in to solve the issues. It is basically a linked list of blocks (public ledgers) that records data in hash functions with timestamps to store it anonymously with other participants within the chain. It eliminates third party dependency required for the traditional banking, which in turn reduces the probability of central point vulnerability. Data manipulation is impractical due to use of one-way hash function. There is no requirement of designing distributed trust model as all transactional data are verified with every relevant stakeholder. It has been studied here how Blockchain technology can be used for E-banking scenarios using hash algorithm along with nonce and what is its impact on the society to transfer financial data. However, there are still a few issues associated with Blockchain that need to be addressed before implementing it in real-life.

***Keywords*—**Blockchain, Hashing, Nonce, Distributed Ledger, E-Banking

I. INTRODUCTION

Due to the exponential growth of digital technology, different sectors have utilized the electronic platforms in a massive scale. The customers can get the benefit of various online services offered by the banks. The different transactional activities are fund transfer, bill payment, processing of loan application and disbursement through the online mode, etc. The other non-transactional activities are requesting a cheque book, generating monthly or quarterly statements, updating the contact information. A large number of customers have opted for the above facilities, because it is very easy to operate without any hassle. Even there is a notable amount of advancement and benefits, privacy, security, authenticity and integrity of digital transmission are at stake. The banks put up a trustworthy role in ensuring all the financial transactions performed digitally are sufficiently secured from any future threats. This enables the customers to carry out their banking operations efficiently as they can thoroughly monitor their account activity. On the other hand, cost, entity and transaction authentication are the other challenges along with the endorsement of a secured channel [1] faced by several banks. The banking sector is yet to find a strong, single technical solution to combat all the security challenges.

Thus, to keep the sensitive information from getting misused in the distributed network, the financial and even non-financial sectors [2] have opted for a different technology, termed as Blockchain, which is basically a chain of blocks to store digital data. The data inside the block can never be modified as this block is chained to the other blocks. It will be available to public in the same form as it was added to Blockchain. It is very easy for us to keep track of records without bothering about the risk that these are tampered by someone. If a customer's valid bank transaction record is added to Blockchain right now, he can prove it at anytime in future that he is the owner of that transaction. As no one can change the piece of information already added to blockchain, it can be said that the revolutionary concept can save data in immutable way.

Use of Blockchain on e-banking can reduce the duration of any transaction at anytime. This duration is basically the time-span taken to add a block in the blockchain. Banks can exchange funds more quickly and securely. We can define blockchain [3] as a set of transactions spread out in a network that have been executed and have been shared among all the contributing parties or entities. Each digitized event in the record is proved unanimously by the participants in the distributed system. The blockchain contains a particular and provable record of every single transaction ever performed. Usually, the blockchain technology is applicable to any digital event taking place between the two parties involved online. The tasks involved in blockchain are first to recognize and validate entries. Secondly it has to protect the entries as a valid one and finally it must save the

record. Hence, Blockchain eradicates the involvement of a trusted third party in the entire digital event. The trusted third party is vested with the power of validation, safeguarding and preserving any financial and non-financial event taking place via the communicating channel. Although minimal pilferage of financial data is unavoidable in traditional procedures, blockchain removes the dependency of a third party during an online transaction. As the security features are well maintained from several attacks and Man-In-the Middle Attacks [4], several banks have opted for this new technology, blockchain.

The rest of the paper is organized as follows. Section II presents a brief overview of the relevant works on e-banking security to identify the major limitations. Section III briefly explains how blockchain technology can work to improve the performance of e-banking scenarios. A theoretical analysis on impact of blockchain - based e-banking on society is discussed in Section IV. Section V concludes the paper.

II. RELATED WORK

E-banking scenarios are affected by various types of risk [5]. No single central authority can effectively safeguard a system connected to a public network. Many challenges regarding the security of transactions are the consequences of unprotected data being sent between clients and servers over the distributed network. The security features [6] of any e-banking application generally include authentication, identification and firewall protection. The Uniform Resource Locator (URL), also termed as internet address identifies a particular bank, whereas the customer is identified by his credentials, i.e, login ID and password to prove that he/she is only the authorized user, who can access their bank accounts. On the other hand, messages between customers and online banks use encryption techniques so that another person in the network, cannot view the contents of messages. Most browsers use a common encryption standard known as Secure Socket Layer (SSL). The advantage of the growth in economy and our dependence in the digitized platform has largely enabled the risks of cyber-attacks, pilferage of data by the intruders and hacking of the most confidential data over the communication channel. Thus, we depend highly on a trusted third party who claims to maintain security and privacy of our financial as well as our non-financial data. However, these parties are manipulated, hacked and even compromised. Several banks have moved to biometric authentication (in case of ATM) to authenticate a valid user [7], a successful transaction, etc. Various encryption techniques have been in use to encrypt a transaction to strengthen its security. Thereafter, need also arises to guarantee that no one tampers or alters the data at either end. There are different solutions to these online banking issues, whether it is software related or hardware related. Software issues are easily solved due to its minimal price and ease of availability. Guessing weak passwords , weak keys are still some of the challenges[8] of the E-banking security. It has many risks associated, as most of the encryption algorithm could be easily decoded by brute-force attacks. We need a solution to avoid the involvement of a third party. Generally, efficient encryption logic may increase the complexity of the overall procedure. To reduce overhead, we must have an alternative solution; so that no unauthorized entity can retrieve the confidential data. Blockchain technology could be used to solve all the above security issues in the e-banking scenario. There is no third party involved in the blockchain technology. The entries are first validated, then protected and finally the transactions are preserved and recorded. Major objective of using Blockchain in e-banking scenario is to transfer money along with relevant data without involving any third-party intermediary like bank. It is very difficult to change the data, once it is recorded inside the blockchain.

III. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

This section presents a brief overview on what is Blockchain technology and how it works [9].

Inside the blocks, data are stored. As all the blocks are linked together in order of time of the transactions as a chain, it is termed as blockchain. If very hard computations are done by the computing nodes participating within the blockchain to find the next block in exchange of some benefits, then these nodes will be termed as miner. The figures which are randomly generated based on the hash algorithm to find a block are known as nonce [10]. As huge amounts of processing power are required to find a block, it is almost impossible to alter the block. This keeps the data within blockchain safe.

A blockchain is a sequential list of blocks that records data. The basic idea is how digital information can be stored in a public database. As all the digital documents are time-stamped, it is not possible to tamper the information. These blocks are anonymously stored with other stakeholders within a network. This eliminates the focal points of vulnerability which cybercriminals can exploit. Moreover, previous blocks cannot be overwritten in a blockchain and all transactional data are verified with every relevant stakeholder, making data manipulation an extremely impracticable task.

The major features of blockchain include:

• Decentralization [11]: Instead of a central controlling system, blockchain delegates control among all its participants in the network, thus creating a mutual understanding among the peer entities.

• Usage of Digital signature: A transactional value is transmitted in the process which uses unique digital signatures. This method uses public key infrastructure, where primary key is used to verify the identity of valid sender. It creates a proof of ownership.

• Mining: Miners are entrusted upon the role of verifying and confirming the transactions by the distributed consensus system. It then stores the online events in blocks by applying reward miners for confirmation and verification of transactions and stores them in blocks using stringent cryptographic rules.

• Data integrity: The usage of intricate algorithms and the unanimous decision among users guarantee that transaction data, once approved cannot be tampered with. Data stored on blockchain thus acts as a single account of truth for all entities involved, reducing the risk of fraudulent activities by the intruders.

The blockchain contains a certain and provable record of every single transaction ever executed. The current e-services are based on truth and a reliant authority. The parties at both ends feel that their confidential data must be secured across an insecure channel. Banking events have been shared with the transacting parties or it can be any financial institution or bank telling us that our money has been delivered successfully and reliably to the valid destination. All the security parameters and privacy solely depend on the third party. However, these third party sources can be hacked, manipulated or compromised. This is where the blockchain technology comes useful. It has the technological potential to change electronic domain by enabling a distributed agreement where each and every online event involving digital, historic and current, can be verified at any time in the future. It does this without compromising the privacy of the digital assets and parties involved. Thus, this distributed consensus and secrecy are two important features used in blockchain technology. The advantages of Blockchain technology overrules the governing norms and technical challenges faced by other models adopted in the e-banking scenario. Blockchain technology is finding applications in wide range of areas. Earlier most financial institutions and banks considered blockchain technology as a hazard to traditional business models. But, with the growing menace and several cyber crimes, many banks are carrying out research and finding suitable measures to apply blockchain to bring the best in their services.

Blockchain, the technology that is used in the popular cryptocurrency 'Bitcoin', is revolutionary in many ways. It addresses multiple challenges associated with digital transactions, such as double spending and currency reproduction. Blockchain also reduces the cost of online transactions while concurrently increasing the security features such as authenticity and security. These benefits are amongst the prime reasons why the technology is being extensively deployed within the banking sector.

Involvement of third-party intermediaries in a transaction may solve double spending problem, but it includes hidden fees charged by large financial institutions to cover the relevant services. The banks need money for their operations, they start cutting commissions on each currency transaction they do for their clients. Sometimes this type of transaction becomes very expensive, especially in overseas transfer of money. Consumers commonly experience this with wire transfers to family and friends. However, the decentralized formatting of blockchain enables true ownership of one's funds. This eliminates the need for an intermediary, which in turn saves time and money of the consumers. Blockchain also provides a peer-to-peer (P2P) network that enables anyone to send and receive money easily. As a result, blockchain is widely adopted in day-to-day business.

Many banks tend to be unreliable and susceptible due to the demanding obligations of being a financial institution, making them more susceptible to bankruptcy and insolvency. Yet, blockchain will prevent bankruptcy entirely since the system is decentralized. Thus, money transfer will automatically and immutably be sent to and received by the valid participants within the Blockchain network.

Blockchain-supported transactions will be transparent on a public ledger, allowing any individual to see the amount transferred or received, receiver and sender information, and the timestamp. In addition, the design of blockchain enables it so that no one can tamper the data anyway. As we are considering here e-banking scenario, we assume here that a blockchain can store only transaction data like bitcoin Blockchain.

Sequential transactions are recorded along with timestamp in consecutives blocks and blocked are connected through links. Each and every block has been assigned a unique digital signature. If content of the block is changed, even by a single digit, a new signature will be generated for the block due to use efficient hashing algorithm, which includes complex mathematical formula to accept any string of input and produce a unique fixed length string of output.

Only digital signature is not sufficient to accept a block within the network. The hashes that meet certain constraints are accepted. As for example, a block will only be accepted if its digital signature starts with a consecutive number of zeroes. Nonce is a random number, which is added to every block for being changed repeatedly in order to find a

valid signature. A block contains transaction data, digital signature of the previous block, and a nonce. Mining is the process of using the nonce repeatedly to generate different random numbers and hashing the block's data to find a valid signature. Miners use computational power to continue this trial and error method. The winner must have more computational power to solve the puzzle quickly.

Any modification in a single block requires a new signature for all other blocks within the chain that need to be inserted at the end of each node. It is quite impossible. Suppose in a distributed scenario, there are several participating parties. Party A(Alice) wants to send money to party B(Bob). Then, this transaction is represented digitally as a block. The block thereafter is announced to each and every party present in the network. Everybody present in the network approve that the transaction is a valid and useable one. The block can then be added as a permanent and transparent record of transactions. The money then moves to the party B, i.e. Bob.

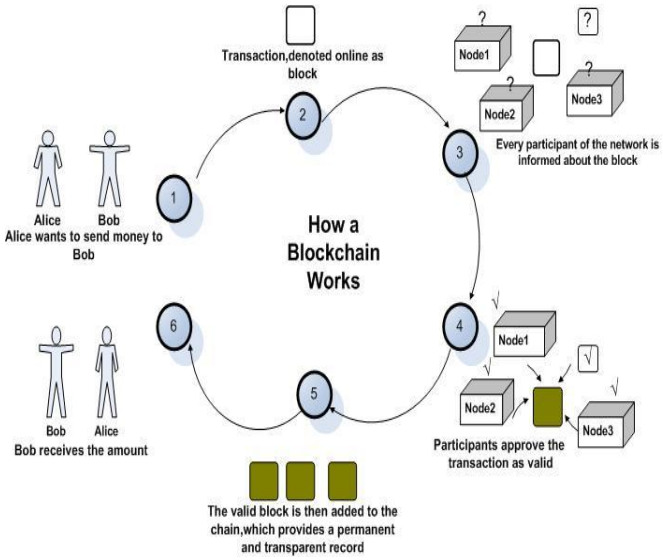

Figure 1: Working Methodology of Blockchain

IV. DISCUSSION

Blockchain is emerging as a technology capable of transforming e-banking sector [12] by making transactions faster, cheaper, more secure and transparent. It is a growing list of records which are linked using cryptography. Each block contains a timestamp, hash of the previous block, and transaction data. Many leading banks have decided to apply blockchain technology on their conventional transactions. The potential of this technology is huge to change the way transactions are made.

From the various research works, it has been noted that blockchain methodology provides all the security parameters to each of the participants involved in the network. Transactions in blockchain network become highly secure by the use of one-way Secure Hash Algorithm (SHA) [13], which generates a 160-bit message digest. Sender can use it to get a 160-bit hash for signing. It enhances with an added level of security during any online transaction. As a consequence, this has gained tremendous popularity and thus, several banks have adopted this technology. This has built trust and satisfaction in the customer's mind as their financial credentials are safe in the open network.

Consider a scenario, where Alice generates a transaction request for Bob. Instead of sending it to Bob alone, she broadcasts the request message on the entire Blockchain network to which she is connected. The message is forwarded to all the connected nodes. Some of the nodes which run a piece of software for mining the message are marked as miners. In the distributed network, every miner is expected to receive multiple messages at any given period of time. The miner combines all the messages in a single block.

The miner creates a hash on the block after formation of a block of messages. If any third party alters the content of this block, its hash value becomes invalid. As each message is time-stamped, no one can modify its chronological order. It ensures that the messages in the block are perfectly secured from tampering.

The blocks created by various miners are linked together to form a distributed public ledger. To insert a new block, a miner selects the hash value of the last block in the existing chain, merge it with its own set of messages to create a hash for the newly created block. It now becomes the new end for the chain. Thus, the chain keeps on growing with the nodes added by the miners.

As all transactions are time stamped, a distributed timestamp server needs to be implemented in a peer-to-peer network. To make the content of the block more secured, a random number is included within the block such that the block's hash meets a certain criterion, which is known as Nonce, a number. It is just like a puzzle. As for example, this criterion may be that the generated hash value must contain five leading zeros. The miners start with a Nonce value of 0 and continues until the generated hash value meets the specified criterion.

It may take several iterations until the desired hash value is generated. Once the miner successfully mines the block, it becomes the last block in the chain. There is a competition among multiple miners. The network rewards the first successful miner. The miner node having high computational capacity normally wins the competition.

Here, Alice generates a transaction request to transfer money to Bob's bank account. Alice signs it with her private key.

Then, she sends the transaction, her signature and copy of her public key to the Blockchain network. Later, any node in the Blockchain network can authenticate Alice's transaction using the details sent by Alice.

Consider an event, where a request is generated to transfer money from one bank account to another bank account. In this case, two banks need to update their own customer's account. In the current scenario, a huge amount of time and effort need to be spent by both banks to coordinate, synchronize, and check that each transaction happens in reality exactly as it is recorded. It needs to be ensured that there is no such discrepancy like double spending problem.

Blockchain can simplify the coordination and validation efforts because there is always a single version of records, not two disparate databases.

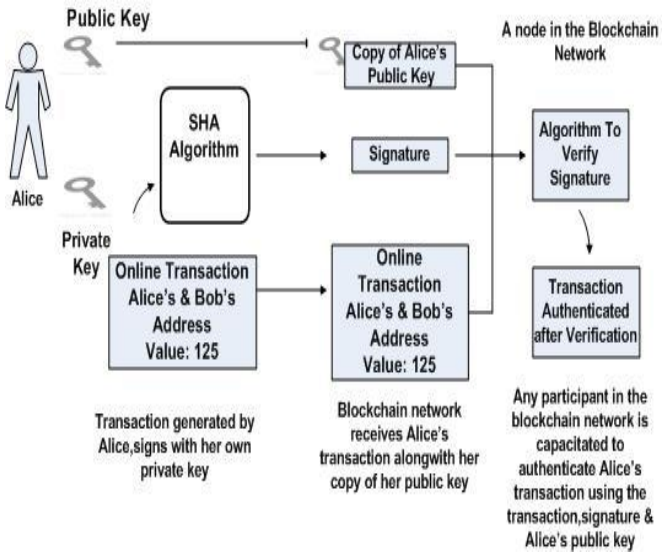

Figure 2: Transaction Authentication in Blockchain Network

Here, we can summarize how the blockchain can work.

- Anyone who wants to get banking services needs to create a transaction request message to the desired recipient.
- There may be many senders and receivers ready for this type of transaction.
- All the valid transactions need to be forwarded to all the nodes in the network.
- The network needs to ensure that every valid transaction recorded within the network must be included in any block over a reasonable amount of time. The miner nodes get incentives for its efforts.
- The node works on finding the proof-of-work (solve the puzzle).
- It broadcasts the block in the network after finishing proof of work.
- The new block will only be accepted by others after verifying that all transactions are valid.
- It needs to be ensured that the transactions recorded within the block are not duplicated anywhere. The node tries to find out proof-of-work on its newly created block. During this time, hash of the accepted block is taken as the previous hash.
- In this way, the blockchain network continues to grow day by day.

V. CONCLUSION

In the conclusion section, we can summarize the reasons why blockchain is gaining so much popularity.

- As it is decentralized, it is not owned by a single entity.
- One –way hash function like SHA is used to store the data. No one can tamper the data inside the blockchain as it is immutable.
- Records can be easily tracked as the mechanism is transparent to all.

The primary objective behind Blockchain technology is to provide confidentiality, security, protection, and sincerity to each of the participants in the distributed network. Although there are certain hurdles to combine all these parameters, blockchain has gained tremendous popularity in the e-banking scenario. More and more banks have shifted their paradigm to this technology because the security aspect has taken over their financial gains.

REFERENCES

[1] J. Cleens, V. Dem, J. Vandewalle, "On the security of today's online electronic banking systems", Journal of Computers & Security 21 (3), 257–269, 2002.

[2] J. Boersma, Blockchain technology use cases in financial services. Retrieved October 5, 2018, from https://www2.deloitte.com: https://www2.deloitte.com/nl/nl/pages/financial-services/articles/5-blockchain-use-cases-in-financial-services.html

[3] Y. J. Yang, "The Security of Electronic Banking, Technical Report", MD20783, University of Maryland, USA, 1998.

[4] B.Schneier, Applied Cryptography Second Edition: Protocols, Algorithms and Source Code in C, Wiley Computer Publishing, John Wiley & Sons, Inc.,pp. 266-271,470-475,2007.

[5] M.D. Nath, S.Karforma, "Object-Oriented Modelling Of Kerberos Based Authentication Process In E-Banking Transaction", International Journal of Computer Sciences and Engineering,Vol.-6, Issue-9, 2018.

[6] B. Schneier, "Two-Factor Authentication: Too Little, Too Late," Comm. ACM, vol. 48, no. 4, 2005.

[7] S. M. Darwish, A.M. Hassan , "A model to authenticate requests for online banking transactions", Alexandria Engineering Journal 51, 185–191, 2012.

[8] N. Jin, F. Cheng,"Network Security Risks in Online Banking", International Conference of Wireless Communication & Mobile Computing, Canada, pp. 1183–1188, 2005.

[9] Y. Yuan, F. Wang, "Blockchain:the state of the art and future trends,"Acta Automatica Sinica,Vol.42,no.4,pp.481-494,2016.
[10] H. Vranken, "Sustainability Of Bitcoin and Blockchains", Curr.Opin.Environ, 28, 1-9, 2017.
[11] G.Zyskind,O. Nathan, A.S.Pentland," Decentralizing privacy: using blockchain to protect personal data",in Proceedings of the IEEE Security and Privacy Workshops,SPW 2015,pp. 180-184,IEEE, 2015.
[12] T. Bhattasali, "Blockchain: Remoulding the Future of Banking Sector", YOUTHINK, vol. XIII, pp. 129-132, 2018.
[13] Cryptography Hash Function Explained:A Beginner's Guide, Available online at: https://komodoplatform.com/cryptographic-hash-function.
[14] BankChain community:Blockchain for banks, Available online at: www.bankchaintech.com

Authors Profile

Mausumi Das Nath is working as an Assistant Professor at St. Xavier's College (Autonomous), Kolkata. She completed MCA, PGDIT (Symbiosis, Pune) and M. Tech (IT).She has 18 years of teaching experience and 6 years of research experience.She is a reviewer of several international journals. Her research interest includes Network Security, Image processing and Data Mining.

Tapalina Bhattasali has finished her doctoral research from University of Calcutta along with international collaboration. She has been awarded honorary doctorate from IEU, Maldives for her work on secured healthcare framework for rural India. She is currently working as Assistant Professor in St. Xavier's College (Autonomous), Kolkata. She is a member of various professional societies like IEEE, ACM. She has published a number of research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE. Her main research work focuses on IoT-Cloud, Security, Data Analytics, Blockchain. She has several years of teaching and research experience.

