When Distributed Ledger Technology meets Traditional Payment Systems-Benefits and Challenges

Abstract: Blockchain technology is a distributed ledger system that focuses on certain features such as scalability, decentralization, high throughput and user friendly environment. In the upcoming era it can be seen that with the help of these characteristics, this technology can act as the most crucial need of the organizations or industries. Most of the industries involve financial database functionalities and have to ensure security in the online payments or transactions between the companies. This work is aimed at defining a proposed solution based on understanding the payment channel being trustworthy and secure on the basis of transactions with the help of Blockchain Technology. The comparison is made to traditional payment systems. Understanding the consensus algorithms with respect to the solutions provided by blockchain for convectional payment system. Hence this paper on blockchain technology payment medium comparison would improve the methods of safe and secure payments and will create an understanding for secure payments using consensus algorithms.

Keywords: Blockchain, Distributed Leger, proof of work, hashing, SHA256, payment System,Consensus Protocols

1. Introduction

At present, everyone is dependent on online methods for every possible work. One of the examples can be taken as online shopping. The reason is the absence of time in the busy lifestyle of people. By shopping online, people can get everything they need at their place by staying at their position. However, like everything, online shopping has many benefits as well as disadvantages or we can say legitimate risks. When the user login to any web application for purchase, he/she gives their input and these credentials go to the server. The server authenticates them. This is where the threat to payment system attack comes in role.
Payments syetems are built convectionally and are vulnerable to several kinds of threats. The credentials are provided by the user and reaches the server indirectly following the malicious path. These are captured by an attacker in the middle itself and the user's credentials are passed to the attacker. The attacker secures the credentials and allows the user to access the web application. In this way, many times the user does not know that the attack has occurred. After much research, to eliminate the possibility of a attack, the authors have found an optimized solution using Blockchain technology [1-3].

This paper is organized as follows: Introduction section is described as the payment system and needs for a better payment system that the convectional being followed. Section 2 reviews about the blockchain technology and types of blockchains present in the system Section 3 focuses on working of consensus algorithms and its variations in traditional systems. Section 4 reviews the real-world problems and how the proposed model reduces the vulnerability of various attacks and providing security better than traditional systems. Section 5 discusses the challenges faced by traditional payment systems and solutions provided by blockchain technology for them. In the next section, this paper presents blochain technology based payment system application advantages. The last section of this paper defines conclusion and future work.

2. Blockchain Technology

As the name “Blockchain" suggests it is a combination of two words “Block” that can be also said as units in general explanation and “Chain” meant as linking, “Blockchain" is a kind of shared or distributed ledger which contains transactional records without any singular authorization of an entity. In a generic explanation,

this work can also say that it is a kind of database that supports reading and appending based on transactions. It ensures security with the help of cryptographic hashing, translucency, and Decentralization [4-6]. It records and stores all the transactions occurring in a network by eradicating the need of "trusted" external parties such as payment processors. Referring blockchain as a trust machine is like trusting innovation in a cynical world. It acts as an evolution with no third party validation in any exchange [7-8].

Due to decentralization, a peer-2-peer network is operated without the need of trusted intermediaries or authorities. The nodes of the external users in the network 2 are then verifying the transactions by the computed rules of the system to make sure everything within the system is valid before it gets executed. The affirmation is essential because all transactions and records in a blockchain are unchangeable or immutable. The elegance of the Blockchain is that it obviates the need for a central authority to verify trust and the transfer of value [9]. It transfers power and control from large entities to the many, enabling safe, fast, cheaper transactions even though we may not know the entities we are dealing with.

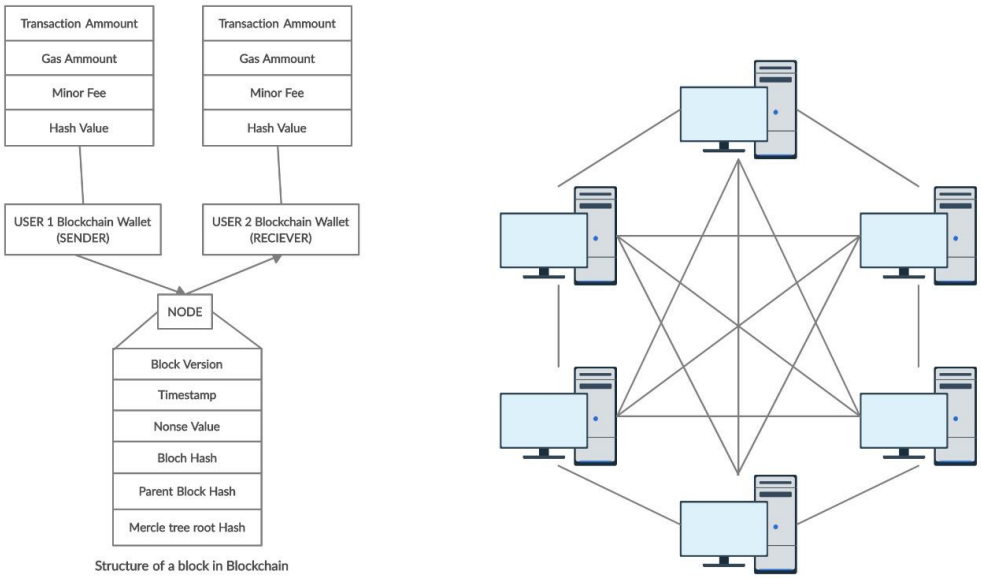

Figure 1 Working of Blockchain network

2.1 Types of Blockchain

Essentially, there are two types of Blockchain: Public Blockchain and Private Blockchain. Alternatively too as Consortium and Hybrid Blockchain. Blockchain are differentiated due to their different uses in different industries. So understanding all the types in order: Public Blockchain is the type that will be accessible to everyone without any restriction of the participant (Authorized/Unauthorized). No control is kept over the network hence ensures security and immutability as no individual could make changes in the Blockchain. Private Blockchain is a kind of Blockchain that requires permissions for access and to participate in the network for validation. These permissions are authorized by the blockchain developers while creating the blockchain. They are used to store sensitive information and only available to the group of people present within an organization. Consortium Blockchain can be also referred to as a sub-divided part of Private Blockchain. The difference lies in the authorization of the blockchain as it is handled or governed by a group of people rather than a single entity. They are quite efficient collectively in collaborating with the business of a kind. Hybrid Blockchain is a combination of the benefits received by the public blockchain-based on transparency and private Blockchain based on privacy or

security maintained. It is also referred to as the multi-chain network of blockchains. This provides flexibility in the business to segregate the data by transparency and privacy [10].

3. Consensus Algorithms

Consensus blockchain is mainly about a familiar agreement state within the distributed ledger to establish trust amongst all the peers in the shared computing environment. The Blockchain consensus protocol has some specific criteria such as understanding an agreement, co-operation, collaboration, inclusive, equal process to every node and each node is mandatory to participate in the consensus process. This paper would like to elaborate on the strengths and weakness between the traditional and blockchain payment systems. In respect to traditional systems, blockchain will help in expanding the provision of financial services in less or under-developed areas [11-14]. If a condition is designed for international transactions, traditional money wire methods would increase the complexity for the transactions.

Consensus algorithms are algorithms that ensure the security and integrity of data on distributed systems and processes. The consensus algorithm provides a community to decide whether the transaction is authenticated and not authenticated. The same idea about the transactions made around the agreement. Consensus algorithms prevent double spending problems and make transactions in blockchain more reliable The goal of consensus algorithms is to encourage mutual agreement, promote economic incentive, ensure equity and fault-tolerant blockchain mechanism.

Steps involved in Consensus Algorithm:

- Start of the program
- User mines a block in the blockchain
- Predefined Interfaces will be implemented by consensus algorithms such as PoW, PoS etc.
- These algorithms help in calculating the timestamp of a particular block
- Along with the time stamp, hash value is also calculated by the algorithms
- Check whether the block chain is valid or not of the mined blocks
- End of the program

4. Blockchain Technology and Payment Systems Interplay

Traditional payment systems are centralized hence are dependent on a central entity. If the attack is made on the central entity, the whole network gets affected. Whereas in blockchain this problem is solved due to its decentralization property. Also blockchain technology has the potential to lower the costs of security, auditability and governance significantly. Blockchain systems may offer services at a fine price levels than the traditonal payment systems. They are suitable solutions for corporate organizations and could potentially generate a significant shareholder value in respect to traditional systems. Understanding a situation based on international transactions the complexity would be much higher. Blockchain technology requires high computational resources and might be slower when compared but are secure more along with outperforming incumbents.

Blockchain is recognized as an innovation to secure administration and remote trade, presented as money related wrong-doings as a rule. It is one of the prime reasons why money related firms should select their own blockchain applications for the administration of advancement organizations. In our proposed work, when any transaction is added. They are checked that either they are validated or rejected after addition into the system in the pool of all unconfirmed transactions. Within the pool of transactions a set of them is chosen for the block. The next

step of blockchain based model is to apply any of the consensus algorithms such as Proof of Work. At this moment, miners would come into the role. They are paid fees for security, validation, execution of smart contract as well. The solved block by miners is broadcasted and verified. Now, new block is added into the chain (blockchain) after confirmation and transaction confirmed between sender and receiver. If a participant node tampers with a block, its results will be deflected in changing of hash, mismatch of hash values, the local chain of node rendered in an invalid state. Safe payments are made by blockchain technology. Hashing and asymmetric key encryption is used for securing the chain and for efficient validation and verification. Mostly we use digital signatures by Elliptic curve cryptography in blockchain network. A transaction for transferring assets will be authorized, non-repudiable and unmodifiable. They are first examined by the digital signing process and then applies it to that transaction. Digital signatures confirm that data is hashed and encrypted. In a Blockchain's block, first computing the state root hash, transaction root hash and then receipt root hash are shown at the bottom of the block header. These roots and all the other entities in the header are combined in a hash together with the variable nodes to solve the proof of work puzzle.

Most of the people have many types of cards like credit card, debit card etc. They can use it to pay for things. But some also have cryptocurrencies such as bitcoin, ethereum at their disposal. There are many advantages of using blockchain ledger in transaction in place of credit/debit card or other online fund transfer options. Key benefits of using blockchain is Decentralization (Blockchain is a decentralized ledger) Trust (In blockchain, trust level among stakeholders are high) and Security (Every transaction in blockchain is verified by all the members of the net- work which restricts manipulation and improves security). Blockchain also helps in smart contracts because it gives the facility of the computer code, storage of any type of digital information. Blockchain accelerates the process of the funds clearing and settlement. Blockchain helps in the process of syndicating the loans. Usually Syndicating loans takes an average of 19 days for banks to complete the process but blockchain reduce the time by reducing the intermediate steps or processes. Block-chain provides a secure payment system. Chances of operational and financial fraud risks are very less using blockchain technology.

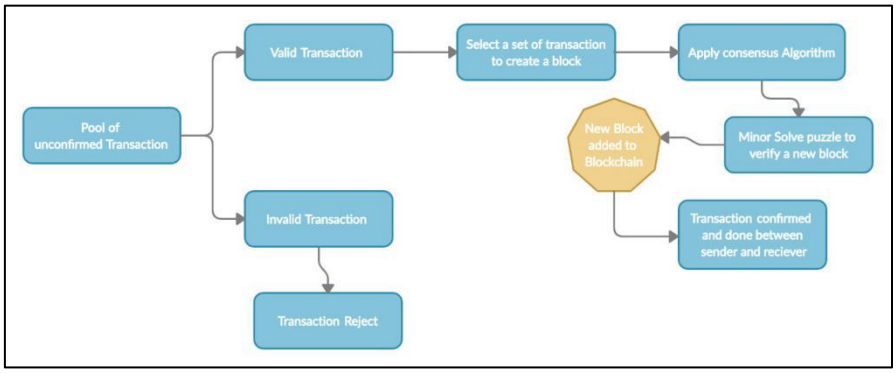

Figure 2: Blockchain Transactions Authentication and Validation

5. Challenges in Traditional Payment System and Its Countermeasures

Many attacks are possible in online web applications. In the present time, dealing with them is a very big challenge. The main attacks/challenges are XSS, Broken Authentication, Security misconfiguration, Sensitive data exposure, or man-in-middle attack. Now discuss XSS (Cross-Site Scripting) attack, This attack is usually done on websites that receive data from the user. With XSS attack attacker can steal cookies, session token, and other sensitive information from the user's browser. Our paper provides an optimal solution of man-in-middle attack. These are OWASP real-time trending attacks [15-17].

Table 1: Challenges and Solutions

Challenges faced by Traditional Approach in Payment Systems	**Solutions provided by Blockchain Technology in Payment Systems**
Integrity of original transaction records is not publicly visible within the central financial institution.	In a proposed public blockchain, all transaction records are open and transparent therefore all the nodes involved in the storage for transaction block data can review the present transaction data. Hence integrity of each transaction record is maintained over the system. [18].
If the central entity of the traditional payment sytem fails or gets hampered, all the other set of entities connected to the system will stop their working the instant.	Failure of any entity does not affect the normal operation of blockchain network due to its decentralization property. For blockchain network people do not need to operate, manage and maintain manually at any time [19].
Storage for traditional payment systems is limited hence increases the chances for cyber-attacks.	Reducing the risk of cyber-attacks, because the storage of blockchain is distributed [20].
Data with respect to central based financial system is at stake to be modified and deleted within the system.	Blockchain network transaction data cannot be modified and deleted because of the concepts of hashing [21].
Cross border payments are difficult in traditional systems for payments.	Blockchain can improve cross-border payments by offering added security, higher transfer speed, and lower conversion fees [21].
Verification in respect to KYC as well speed for transactions is dependent on entities.	Blockchain can speed up the accounts payable and receivable process with its immediate ledger update and accuracy of information, especially for insurance companies and vendors along with verification.
For larger companies, it is difficult to keep track of numerous business deals and accounts financially.	Blockchain is a distributed peer to peer network approach. All transactions are in a centralized system maintained by a single server, but in blockchain each peer can view the transactions within the network. Thus, large organizations make it easy to track transactions[22].
Traditional payment systems do not comprise of consensus algorithms.	Consensus mechanism is a key feature of blockchain to improve the overall robustness and integrity of shared ledgers. Consensus mechanism among network participants is a prerequisite to validating new blocks of data

	and mitigates the possibility that a hacker or one or more compromised network participants can corrupt or manipulate a particular ledger [23].
Privacy of the sender and reciever is not maintained.	Blockchain based payment system do not have their account numbers or names only hash values are available that cannot be ideally recovered hence privacy is maintained [24].
Traditional financial transactions are impossible without intermediaries like banks. Banks are central link that make sure that the money being transffered will get to the predetermined recipient. After the transaction the only wish for a sender is to wait for the recipient.	With blockchain, it is possible to avoid cental interference in many cases. One can send their digital payments from their virtual wallet to a recipient's virtual wallet with the help of a set of digital keys. For performing such transactions , the address of the recipient has to be known. Such transactions are quick, secure and irreversible, which makes them more advanced than the traditional systems [24].
Auditing of transactions and records is not possible in convectional systems.	Blockchain structure is beneficial for real time audits and making it secure from the modifications of any kind.
Traditional system cannot get rid of payment delays and the time-consuming procedures of the outdated payment system.	With blockchain, instant, secure transactions can be an affordable, implementable and unique alternative for many businesses ventures/companies[25].

6. Blockchain Technology based payment applications

Blockchain being a peer to peer as well as decentralized network can have a wide range of usability in certain organizations of industries. Applications of blockchain are present in various methods thus describing it in payment based applications. Many people and organizations can complete successful transactions without acknowleding the identity of each other due to blockchain. In figure 3, It can be observed that the employees of the banks, staff and other workers from the hospitals, IOT device users, super market or mall mantinence people can do transactions using a single blockchain according to their requirements of their system. For every pool of valid transaction a blockchain block will be created. In Blockchain based decentralized payment system any person can check the transaction detail at any time when they want which is not possible centralized payment system. Maintaining privacy as well as integrity along with security via hashing is improving standards of blockchain technology in the mordern upcoming era and along with other technologies such as IOT, security and more.

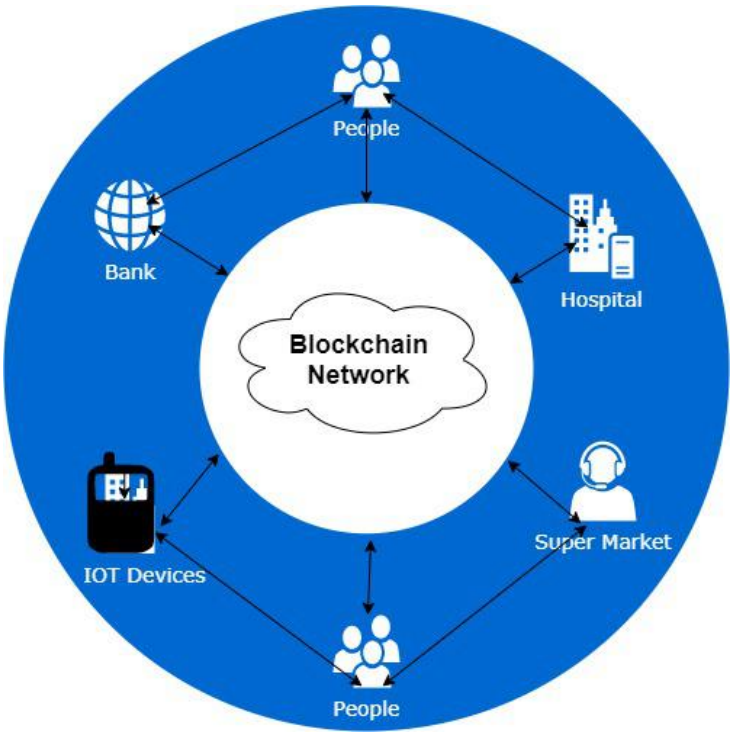

Figure 3 Applications of payment based systems via blockchain

7. Conclusion and Future Work

This paper concludes by the challenges, comparison and applicational advantages that blockchain technology will be helpful in getting rid of the traditional payment systems for securing online payments. This can be implemented in all areas or fields in respect to secure online payments or transactions over a vast network. In the current time, 77% of finance related companies plan to use blockchain by 2020, indicating that many are happy with what they can do. At present, this innovation requires some work to integrate effectively. Co-operation, scalability and energy use are just a few couple of examples of specialized foundations that should be defeated to get compelling outcomes with the help of blockchain from the square. Blockchain has progressed significantly in a brief timeframe. All the organizations that implement payment options in online mode can move to blockchain technology for a scalable and secure platform orientation.

REFERENCES

[1] McAndrews, J. (1997). Network issues and payment systems. *Federal Reserve Bank of Philadelphia Business Review, December*.

[2] Agarwal, S., Khapra, M., Menezes, B., & Uchat, N. (2007, December). Security issues in mobile payment systems. In *Proceedings of ICEG 2007: The 5th International Conference on E-Governance* (pp. 142-152).

[3] Lorenz, G. W. (1996). Electronic stored value payment systems, market position, and regulatory issues. *Am. UL Rev.*, *46*, 11

[4] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.

[5] Gupta, S. S. (2017). *Blockchain*. John Wiley & Sons, Inc.

[6] Risius, M., & Spohrer, K. (2017). A blockchain research framework. *Business & Information Systems Engineering*, *59*(6), 385-4093

[7] Zhang, Y., Deng, R. H., Liu, X., & Zheng, D. (2018). Blockchain-based efficient and robust fair payment for outsourcing services in cloud computing. *Information Sciences*, *462*, 262-277.

[8] Khalil, R., & Gervais, A. (2017, October). Revive: Rebalancing off-blockchain payment networks. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 439-453).

[9] Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in Government: Benefits and implications of distributed ledger technology for information sharing.

[10] Chan, P. M. W., Lee, J. J. S., & Haldenby, P. A. J. (2019). *U.S. Patent No. 10,282,711*. Washington, DC: U.S. Patent and Trademark Office.

[11] Nguyen, G. T., & Kim, K. (2018). A Survey about Consensus Algorithms Used in Blockchain. *Journal of Information processing systems*, *14*(1).

[12] Chaudhry, N., & Yousaf, M. M. (2018, December). Consensus algorithms in blockchain: comparative analysis, challenges, and opportunities. In *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)* (pp. 54-63). IEEE.

[13] Zoican, S., Vochin, M., Zoican, R., & Galatchi, D. (2018, November). Blockchain and consensus algorithms in the Internet of Things. In *2018 International Symposium on Electronics and Telecommunications (ISETC)* (pp. 1-4). IEEE.

[14] Gramoli, V. (2020). From blockchain consensus back to byzantine consensus. *Future Generation Computer Systems*, *107*, 760-769.

[15] Kirda, E., Kruegel, C., Vigna, G., & Jovanovic, N. (2006, April). Noxes: a client-side solution for mitigating cross-site scripting attacks. In *Proceedings of the 2006 ACM symposium on Applied computing* (pp. 330-337).

[16] Bisht, P., & Venkatakrishnan, V. N. (2008, July). XSS-GUARD: precise dynamic prevention of cross-site scripting attacks. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 23-43). Springer, Berlin, Heidelberg.

[17] Jain, S., Tomar, D. S., & Sahu, D. R. (2012). Detection of Javascript Vulnerability At Client Agen. *International Journal of Scientific & Technology Re- search*, *1*(7), 36-41.

[18] Po-Wei Chen , Bo-Sian Jiang , Chia-Hui Wang . Blockchain-based payment collection supervision system using pervasive Bitcoin digital wallet. *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).*

[19] Christophe van Cauwenberghe.Blockchain and payments:Lessons learned and future prospects. *Societe Generale*.

[20] Celine Chen and Shawn Hayashikawa. Easier and Faster Payments with Blockchain. *Societe Generale*.

[21] Chowdhury, M. J. M., Ferdous, M. S., Biswas, K., Chowdhury, N., & Muthukkumarasamy, V. (2020). A survey on blockchain-based platforms for IoT use- cases. *Knowledge Eng. Review*, *35*, e19._15

[22] Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017, August). Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference* (pp. 357-388). Springer, Cham._19

[23] Duong, T., Fan, L., & Zhou, H. S. (2016). 2-hop blockchain: Combining proof-of-work and proof-of-stake securely. *Cryptology ePrint Archive, Report 2016/716*._20

[24] Kumar, A., & Jain, S. (2019, July). Proof of Game (PoG): A Game Theory Based Consensus Model. In *International Conference on Sustainable Communication Networks and Application* (pp. 755-764). Springer, Cham._21

[25] Erin English. Can Blockchain Help Reduce the Financial Industry's Cyber Risk?.*MMC Publication 2018*