Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

ISSN NO. 2320-5407

Article DOI:10.21474/IJAR01/10986
DOI URL: http://dx.doi.org/10.21474/IJAR01/10986

*RESEARCH ARTICLE*

# SURVEY PAPER ON CURRENT BLOCKCHAIN SOLUTIONS FOR SECURE BANKTRANSACTIONS

**Preetha S., Akhilesh N.S and Aniruddha M.N**
Department Of ISE, B.M.S. College Of Engineering,VTU, Bengaluru, India.

*Manuscript Info*

*Manuscript History*
Received: 14 March 2020
Final Accepted: 16 April 2020
Published: May 2020

*Keywords:-*
Block Chain, Current Implementations, Secure Bank Transaction

*Abstract*

Blockchain has been seeing a great deal of popularity in recent years. The technology is considered revolutionary for its ability to provide security and trust in even the most anonymized networks and environments. It does by providing a distributed immutable ledger where any kind of information and can stored and shared in a safe way. However, despite its promising feature set we are still yet to see Blockchain adopted on a wide scale for applications that strongly benefit from the mentioned feature set. One such example of this is Bank Transactions, which are still managed by Banks using the standard centralized servers.Sowhy is Blockchain not seeing widespread adoption in this area despite the clear benefits it provides. In this survey paper, we review various implementations of Blockchain as of the year 2020 and try and provide an explanation as to why each of these implementations is unable to fit all the criteria needed for it to be used in the area of secure bank transactions.

## Introduction:-

Blockchain is an interesting technology since it presents the first and only true alternative to traditional database systems. Traditional database systems involve storing all data on a central server. Computers can then request for this data from the server when they need to, using a standardized protocol, the computers that do this are often referred to as clients. This architecture is widely known as the client-server architecture and is now almost universal. While this type of database system has served us well and will continue to do so, it is not without its limits.

The Client-Server architecture's biggest flaw is that it creates a single source of truth which in turn results in a single point of failure, since all the data is stored in a single server or set of servers. Consider what would happen if for example, hackers were to find a way to break or penetrate a large bank's servers. The damage that would result from such an event would be catastrophic. It is this exact problem that Blockchain hopes to solve. But before explaining how Blockchain is able to solve this issue, emphasize and reference is done only to Blockchain as an alternative to traditional databases and not as an improvement or a replacement. This is because traditional databases have many advantages over Blockchain (such as them being more flexible and easier to setup and use that enable them to work better in many use cases and we are in no way, suggesting that they will be replaced by Blockchain.

Blockchain is often described as a decentralized or distributed immutable ledger. The word "Blockchain" itself derives from how data in a Blockchain is stored in the form of blocks which are linked together like chain thereby forming a chain of blocks or a "Blockchain". In computer science terminology, one may think of it as a type of linked list. There are two properties in particular that make Blockchain special:-

**Corresponding Author:-Preetha S**
Address:-Department Of ISE,B.M.S. College Of Engineering,VTU, Bengaluru, India.

1. The first is that the Blockchain is immutable, meaning data can be written into the Blockchain but once written, cannot be changed or removed.
2. Second is that the Blockchain is distributed or decentralized meaning that the actual chain of blocks is not stored in a single computer but rather spread across a large network of computers while being constantly synchronized between them.

These two properties put together allow for any data on the chain to be secure. Since, the order to break the chain, one would need to attack and replace the entire chain on every computer in the network which in large networks becomes unrealistic.

True Immutability in the world of software is virtually impossible, hence current Blockchain being used by Bitcoin can only attain a type of pseudo-immutability by using a combination of cryptography, specifically Hashing, and Networking. Hashing is a cryptographic function which creates a unique fixed-length ID when passed any kindof information, this ID is often referred to as a hash. A good hashing function will work such that even the slightest change in the information being passed to it will generate a completely new hash and the generated hash cannot be used to derive the information back. Most popular hashing function used today is the SHA-256 algorithm created by the NSA, but other such hashing algorithms include the SHA-1, SHA-512 etc.

In Blockchain, each block holds three main pieces of data, the first is any kind of information that needs to be stored in the Blockchain. Second is the hash of the previous block in the chain if there is no previous block, then a random hash or value is used and the third is the hash of the first two pieces of data. This leads to the formation of a type of cryptographic link that connects every block in the chain to the next one. If one were to try and change any of the blocks in the chain all the blocks that come after it would immediately disconnect since they were dependent on the hash of the previous block to generate their own hash, one could then simply check the hashes to realize that the chain has been altered. But this by itself is not enough to make the Blockchain immutable, since a powerful machine could simply alter a block in the middle of the chain and regenerate the hashes for the rest of the blocks represents the distributed nature of Blockchain.

Blockchain is not stored on a single server but on a number of machines across a network, specifically a peer-to-peer (P2P) network. A peer-to-peer network is a network where every peer in the network is either directly using a connection or indirectly through a peer/s connected to each other. In addition to being stored on every node in the p2p network, the Blockchain is also being constantly synchronized. This ensures that if one of the Blockchain in the network were compromised, the other nodes would immediately identify and rectify it based on a majority. In addition to this, whenever a new Block is added to the Blockchain the new Block is immediately spread across the network and validated.All of this makes extremely difficult for a hacker/s to hack the chain, since they would need to compromise at least 51% of the network before they are able to hack the chain. The actual process of ensuring that the Blockchain is synchronized across the network and new blocks are validated is done using something known as a consensus protocol.

Based on all the information presented, one must wonder why Blockchain are not in mainstream implementation right now though it seems to present a great deal of security. Such a technology would be exceptionally useful in places like Banks where security of information is vital. So why this technology not implemented in these places? In this case an attempt to address one such implementation use case of BlockchainisBank Transactions.

**Literature Survey:**

Satoshi Nakamoto [1] discussed how a distributed immutable ledger could be used to create a new form of currency, one where a party could perform a payment directly to another without any intermediary Bank or financial authority. This form of currency is known as a cryptocurrency and was first brought to light by the famous Bitcoin paper. A great technical details how the present Bitcoin Blockchain works (or how it could be implemented back then) and Bitcoin is the largest Blockchain network in the world was presented.

So why not use the same techniques implemented by Bitcoin to secure its transactions on Bank transactions. Especially since Bitcoin has shown itself to be effective even in a completely anonymous network. The problem however comes with the underlying protocol used by Bitcoin, the proof-of-work protocol [3]. The proof-of- work (PoW) protocol is the protocol used primarily by Bitcoin and Ethereum [12], two of the biggest blockchain networks in the world. So while it is clearly effective, it comes with a major flaw. The PoW protocol requires a special process called Mining,

Mining is the process of solving a complex cryptographic puzzle and one who finds a solution will be rewarded by the network with a fixed amount of the network's cryptocurrency. Mining is essential for the PoW protocol but it is also extremely inefficient. According to Digiconomist,mining consumes about 75 TWh of energy annually which is comparable to the annual power consumption of Venezuela. While many efforts have been made to make Mining more efficient, it's core design forces it to be time and power consuming. Banks are not willing to implement a protocol that would require so much electrical costs.

Another problem with the PoW protocol comes from its vulnerability to a certain kind of attack known as the 51% attack. The 51% attack occurs when in a blockchain network, more than half of the network is composed of malicious participants. PoW protocol builds on the practical byzantine fault tolerance protocol [4] or pBFT for short which is a protocol that dictates how a network can come to a consensus over a set of information being shared between the network. pBFT has shown to have a tolerance of upto33%. This means that within the network, if upto 33% of the participants are fraudulent, the network can still come to a consensus on the information being shared. The PoW builds on the pBFT protocol and has a higher 49% tolerance. However, while a scenario where 51% of a network is fraudulent is rare in a large network, it isn't unreasonable in a small or medium one and additionally in an anonymous network operated by banks, the banks themselves would have no way of verifying if any of the vast majority of other users are involved in any kind of foul-play, making the 51% attack even more likely.

Blockchain used by Bitcoin is referred to as a public Blockchain since the network that hosts the Blockchain is public i.e Open for all. Anyone can join this network without even needing to provide his/her identity to participate. But Blockchain don't need to be hosted on public networks. They can be hosted inside a private and trust based network as well. This form of Blockchain is especially useful for corporations. A corporation would want to have control and awareness over all participants of a network it owns. This is possible in a private Blockchain where the network will only allow participation if an interested party can provide some proof of identity so the corporation and network can trust that specific party (since it can hold them accountable in case of any fraudulent activity via the id proof).

Several tools exist that allow corporations to create their own private Blockchain. Most famous of these tools is Hyper ledger Fabric are discussed in [2] [8] [9]. Hyper ledger fabric which is now an open source project managed by Linux Foundation under the Hyper Ledger Bracket is a specialized tool that can be used to create secure Blockchain based networks for the internal use of an organization. Hyper ledger provides several benefits on top of the already existing benefits of a private network. It supports smart contracts [5] similar to Ethereum but unlike Ethereum, contracts in fabric can be programmed using general-purpose languages like Java, Python etc., channels and organization level privacy. An organization can store and manage the identities of all its employees without needing to expose those identities to other organizations and when any kind of official communication needs to occur between employees of two different organizations. A private channel can setup for the secure exchange of identities to facilitate the communication.All such features play very well in the use of Bank transactions.

Two Banks can maintain a shared network where each Bank can privately and securely manage the identities of all their clients and allow for transactions from one Bank to another using secure and private channel. So why don't Banks adopt a Hyper Ledger Fabric based Blockchain approach? The problem comesfrom hyper ledger Fabric being designed for use inside private and enclosed organizations whereas individuals often perform Bank transactions from around the world. Additionally, Banks would need to cooperate with each other in order to operate a shared private network which is effort that most Banks will not agree to invest in when they already have existing centralized solutions to manage. Therefore, an ideally accepted solution would have to be one made up of a public Blockchain where Banks need to concern about managing the identity of their clients, validating their identity upon any transaction and validating the transaction itself without needing to worry about maintaining the network itself.

So far, we have found that most popular public Blockchain solutions require Mining which is extremely power consuming and efficient while the most popular private Blockchain solutions require network maintenance. There have however been efforts made in creating public Blockchain solutions that don't require Mining. One of the most popular of these solutions is the Proof-of-Stake protocol[7] or PoS for short, which replaces the standard Mining with something known as Minting, which consumes barely any electricity at all. PoS could have fit the use cases in bank transactions were it not for the fact that there are few practical implementations of Proof-of-Stake and PoS being difficult to setup. PoSrequires a reasonably large network to even be feasible, so most of the existingPoS solutions are only switching to PoS after having started using PoW. PoS is still a promising solution, enough so that even the second largest Blockchain network in the world (Ethereum)is developing a new protocol for their network that revolves around PoS (This protocol is called Casper [10] and its successful implementation could potentially put an end to mining) but is still too far in its early stages to be considered a solution for this use case. The same however can also be said of the Proof-of-Burn protocol [6] or PoB for short, another protocol that tries to create a Blockchain solution that doesn't require Mining.

Proof-of-Burn is somewhat similar to PoS in that instead of mining for new coins, you would burn old ones to get more new ones in proof-of-stake, you would stake old ones to get new ones, like in an auction. But while like PoS, it is significantly less power consuming and more efficient than PoW. It also shares the same disadvantages as PoS, being that it is hard to setup and there aren't many large scale practical implementations of PoB. Moreover, both PoS and PoB are designed to be operated in networks where every peer generally operates as an individual and does not offer any benefits for organizations acting as peers.Meaning that if one of these protocols were used to implement Blockchain in Bank transactions, the actual process of making sure new transaction info reaches and is validated by both the banks involved in the transaction must be handled by the banks themselves.

Most public Blockchain solutions do not accompany well with the needs of private organizations in a Blockchain network, fortunately however, there do exist a few which do, the most promising of these is the Proof-of-Reputation protocol (PoR) [11]. In PoRinstead of Mining, there exists something known as validating. Validating is a simple process which does not involve any kind of CPU intensive puzzle to solve and therefore, does not consume much electricity. Where PoR is different from other protocols however is that it has multiple types of users. Generallymost public Blockchain solutions are designed for networks where every peer perform the same functions and no one peer is any different than the other (Even in the Bitcoin network, miners can also be regular bitcoin users and vice versa) but in PoR, there exists two distinct types of users. The first is a regular user who performs any transactions in the system and the other is the validator whose job is similar to what the miner does. But unlike in Bitcoin where regular users can also be miners, validators can only be large organizations.

Large organizations typically have a considerable amount of reputation to maintain. Therefore they are unlikely to involve themselves in fraudulent activity since they would be putting their reputation at risk in the event that they are caught. This is essentially the main source of security in PoR protocol. The reason why this works well in the context of bank transactions is because validators here would simply be the Banks and a Bank could potentially lose all of its money almost instantaneously if it is caught performing some kind of fraudulent activity. People put their money in Banks as an agreement, as such the security provided by a Bank is based very heavily in the trust that the Bank is able to establish with its clients. So in a PoR implementation, Banks would get all the benefits of a PoS andPoB protocol (No Mining).While also gaining specific benefits that are geared towards organizations such as Bank(since transactions need to be validated by a validator before they can put on the Blockchain, it enforces a stronger rule for the Bank's involvement in the transaction than PoS or PoB). Unlike the other solutions,a PoR solution is actually feasible for this use case, the only limitation being that the protocol needs to be refined a bit more to accommodate a few extra rules:

Unlike in PoR, where any user can his/her transaction validated by any validator, specific restrictions need to be set place to ensure that certain users can only be validated by certain validators (essentially validators orbanks in which these users have bank accounts).Additional rules or information needs to be provided on how validators (Banks) can privately manage and validate the identities of users (clients) within transactions. With these additional steps set in place, a PoR based Blockchain implementation could potentially be used in securing Bank Transactions and we explain how to do this in our paper about this topic [13]. Table1 summarizes the various kinds of solutions, approaches, approaches and applications.

**Table 1:-** Summary of various solutions.

| Solution Name | Used By | Approach | Limitation |
|---|---|---|---|
| Proof-of-Work(PoW) | Bitcoin, Ethereum and several others | Creates a competitive environmentusing Mining to enforce security | Mining is extremely inefficient and power consuming |
| Hyperledger | Amazon, IBM | Creates a private network with | not well suited for public networks |

| | | | |
|---|---|---|---|
| Fabric | and several others | user authentication, smart contracts and private channels | and requires network maintenance |
| Proof-of-take (PoS) | Few (Being adopted by Ethereum in Casper) | Replaces Mining with the more efficient minting | Notenough practical implementations to leverage and does not sup- port private organizations as peers |
| Proof- of-Burn (PoB) | Few | Replaces Mining with the more efficient coin burning | Not enough practical implementations to leverage and does not sup- port private organizations as peers |
| Proof-of-Reputation (PoR) | Few | Replaces Mining with the more efficient validating and supports private organizations as peers | few practical implementations but can be adjusted to provide a potential practical solution |

## Conclusion:-

Blockchain has proven to be an extremely ground breaking technology but its implementation main-stream has been hindered due to various limitations. In this paper, we seek to address some of the major limitations of Blockchain, the high resource utilization, cost and maintenance of the predominant protocol being used and to also point out the hindrances for Blockchain continued integration into everyday life. Also show why traditional banking systems are not using current Blockchain solutions to enhance their security and improve the transparency of their transactions.

## References:-

1. Nakamoto, Satoshi, and A. Bitcoin. "A peer-to-peer electronic cash system." Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf (2008).
2. Androulaki, Elli, et al. "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains(2018)." arXiv preprint arXiv:1801.10228(1801).
3. P. Hooda, "Proof -of -Work (PoW)Consensus," GeekForGeeks, [Online]. Available: Proof-of-Work.
4. P. Hooda, "practical Byzantine Fault Tolerance," GeekForGeeks, [Online]. Available: Practical Byzantine Fault Tolerance.
5. P. Javeri, "Smart Contracts and Blockchain," 2019. [Online].Available: Smart Contracts.
6. J. Frankenfield, "Proof of Burn," Investopedia, 2018. [Online]. Available: Proof-of-Burn.
7. P. Hooda, "Proof -of -Stake (PoS) in Blockchain," GeekForGeeks, [Online]. Available: Proof-of-Stake.
8. Gaur, Nitin, et al. Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer. Packt Publishing Ltd, 2018.
9. P. B, "Architecting a Hyperledger Solution - Things to keep in mind," 2018. [Online]. Available: Hyperledger Fabric Hacker- noon.
10. Moindrot, Olivier, and Charles Bournhonesque. "Proof of Stake Made Simple with Casper." ICME, Stanford University (2017).
11. Gai, Fangyu, et al. "Proof of reputation: A reputation-based consensus protocol for peer-to-peer network." International Conference on Database Systems for Advanced Applications. Springer, Cham, 2018.
12. Buterin, Vitalik. "Ethereum: A next-generation smart contract and decentralized application platform." URL https://github. com/ethereum/wiki/wiki/% 5BEnglish% 5D-White-Paper (2014).