International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-4, April 2019

Analysis of on-Chain and off-Chain Scalability Solutions in Blockchain Technology

G. Abinaya, S Mary Shalin Benigna, Hakshatha Devi, Venugopal Balaji, Ashwin Chakravarthy.K

Abstract*: Blockchain Technology is becoming extremely popular among various industries due to its many applications such as payment services, smart contracts, digital identity, supply chain management and others. To cope up with the increasing demand, Blockchains must be able to scale and process transactions at a much faster rate than its current capabilities. Since most of the Blockchains mainly focus on security and decentralization, scalability is often sacrificed. As a result, Blockchains have incredibly slow processing speed. Over the years, many scalability solutions have been proposed. In this paper, we discuss about the scalability issues which are currently present in Blockchain and further analyse various on-chain and off-chain scalability solutions of Blockchain Technology.

***Index Terms*: delegated proof of stake, hard fork, payment channel, sharding.**

I. INTRODUCTION

Blockchain is a decentralized and distributed ledger which records transactions securely without the involvement of any third party. It consists of a growing list of records called blocks and every new block added to the chain will contain a cryptographic hash of the previous block, a timestamp and transaction data. These transactions are publicly recorded and are immutable. The use of Blockchain also removes the possibility of Double-spending. A lot of industries are acquiring Blockchain Technology due to its decentralized nature. [1]

II. RELATED WORK

A. Advantages of using Blockchain

i) Transparency

In the traditional transaction system, a central authority keeps track of all the transaction data. The data shared with these central authorities can be easily violated and misused. To prevent this, Blockchain Technology is used. Since Blockchain is a distributed ledger, the data on a Blockchain is stored in encrypted blocks that are timestamped and managed by Consensus Mechanisms which all network participants agreed on.

ii) No Intermediary

With the help of Blockchain Technology, all the transactions take place peer-to-peer without any third party being involved. This builds trust in the system and eliminates the need for processing fees.

iii) Integrity

Everything is archived and authorized in a decentralized way and the system ensures that the data is processed in a reliable and transparent manner.

iv) High Availability

Since in a peer-to-peer network a copy of data is present in several nodes, it is easier to retrieve the data and it is all transparent.

v) Reduced Costs

Since most of the task will be automated and the transactions will take place online without any middleman to validate the transaction, it will be less expensive. [2]

B. Use Cases of Blockchain Technology

i) Cryptocurrency

This is one of the most popular applications of Blockchain Technology. Cryptocurrency is a type of digital currency in which cryptography is used to generate a unit of currency and to verify the transaction. For example, Bitcoin and Ethereum are the most popular cryptocurrency based on Blockchain.

ii) Smart Contracts

Smart contracts are basically a set of rules, a computer protocol which members of the Blockchain agree on in order to perform a credible transaction without third parties. These transactions are trackable and irreversible. [3]

iii) Auditing

Blockchain Technology can also be used in the auditing environment. In this, public Blockchain ledgers are used to record transactions which are proven to be more pertinent, authentic, precise and valid.

Manuscript published on 30 April 2019.
***** Correspondence Author (s)
G. Abinaya, Assistant Professor, Computer Science and Engineering Dept., SRM Institute of Science and Technology, Chennai, India.
S. Mary Shalin Benigna, B.Tech Computer Science and Engineering Dept., SRM Institute of Science and Technology, Chennai, India.
Hakshatha Devi, B.Tech Computer Science and Engineering Dept., SRM Institute of Science and Technology, Chennai, India.
Venugopal Balaji, B.Tech Computer Science and Engineering Dept., SRM Institute of Science and Technology, Chennai, India.
Ashwin Chakravarthy.K, B.Tech Computer Science and Engineering Dept., SRM Institute of Science and Technology, Chennai, India.

C. Scalability Issues in Blockchain Technology

When a Blockchain is developed, two main attributes are considered which is Security and Decentralization. Scalability is often sacrificed by some major Blockchains like Bitcoin and Ethereum. This results in the slow processing speed of the transactions being processed using the blockchain. Currently, Bitcoin can process a maximum of 7 transactions per second and Ethereum can process a maximum of 25 transactions per second whereas Visa and MasterCard can process more than forty thousand transactions per second. For cryptocurrencies to become a viable alternative to centralized systems, Blockchains must be able to scale and process transactions at a speed which is a lot more than its current capabilities. Some of the existing scalability issues are:

i) Block Size

In a Blockchain, every block is capable of holding a limited number of verified transactions. As the number of transactions made using Blockchains increase, the traffic in the network increases and more time will be required to process the transactions. This is a major concern which can be solved with an appropriate scalability solution.

ii) Cost

For verifying every payment, a mining fee, an incentive is paid to the miners. A higher priority is given to the transactions which give higher incentives. Due to the increase in the number of payments that are required to be verified, miners need higher computational power which is expensive.

iii) Response Time

Every payment needs to be validated before it's added to the block. It is a very slow process when there are plenty of transactions waiting in the queue. For example. Bitcoin Cash can handle 60 transactions per second whereas Visa can handle up to 47000 transactions per second. In order to compete with the fiat currency, cryptocurrency has to process a much higher number of transactions per second.

iv) Limitations

Since the number of transactions is growing rapidly in Blockchains, every new block has to increase its data limit for containing the history of all previous blocks. With the transaction data reaching its limit, there is a danger of collapsing the overall system. [4]

Table 1. Rate of Transactions made using selected Cryptocurrencies

Cryptocurrency	Protocol	Transactions per second
Bitcoin	PoW	7
Ethereum	PoW	25
Bitcoin Cash	PoW	60
Litecoin	PoW	55
Cardano	PoS	7
Stellar	SCP	1000
Ripple	RPCA	1500

III. METHODOLOGY

A. On-chain Scaling Solutions

These Scaling solutions are implemented directly on the blockchain to reduce the time taken for verification process and to lower the number of transactions on the queue. This is achieved using Scalability solutions such as Sharding and Hard forking. While both Sharding and Hard forking breakdown the queue to achieve that, the difference between them being, Sharding breaks down the Blockchain into smaller sub-blocks whereas Hard-forking creates a whole new subset of the previously existing consensus which leads to a diverging blockchain.

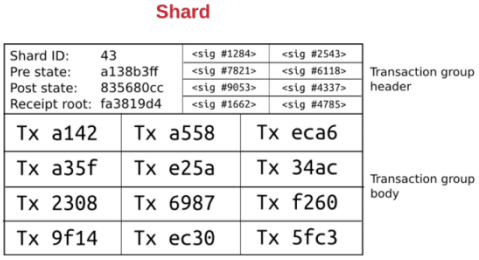
i) Sharding

The main purpose of sharding is to decrease the time taken to verify transactions in the Blockchain. This is done by fragmenting the Blockchain into sub-blocks called shards. After this, each shard is responsible for processing its own transactions. Since each shard will be processing in parallel by carrying out hundreds of transactions per second with a total of more than a thousand transactions per second, validating each transaction will become extremely faster. This reduces the overall time taken to validate transactions.

Normally, a block in Blockchain has only one layer which consists of a block header and the body that contains all the transactions. Merkle root of all transaction will be in the header. But with the help of Sharding, Ethereum suggested changing this into two levels of interaction. [5]

First Level

This level is called the transaction group in which each shard has its own group of transactions. The transaction group is divided into two parts:



Transaction group header:

The left part of the header consists of shard id, pre-state root, post-state root and receipt root.

Shard id: Each shard is given an id for a specific transaction group.

Fig. 1 First Level Sharding

Pre-state root: This is the state of root before the transaction is applied.

Post-state root: This is the state of root after the transaction is applied.

Receipt root: This is the receipt root after all transactions in the shard is applied.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

The validators are present in the right part of the header and are responsible for verifying the transactions in that shard. These validators are randomly chosen.

Transaction group body:

It contains all the transaction ID's which is present in the shard.

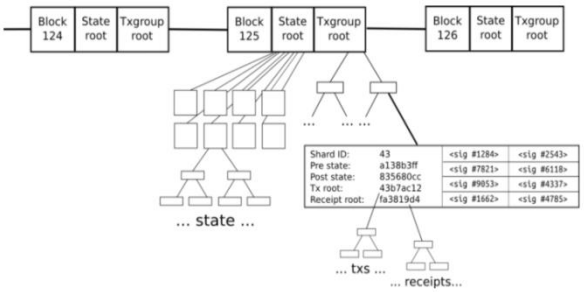


Fig. 2 Second Level Sharding

Second Level

In this level, two primary roots are added to the Blockchain:

State root: This represents the entire state where each contains its own sub states.

Transaction group root: This consists of all the transaction group present in the block. [6]

ii) Hard Fork

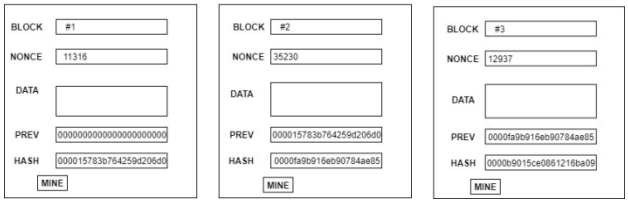


Fig. 3 A Typical Blockchain

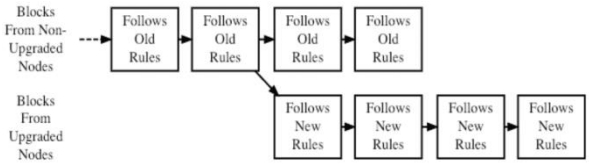
A hard fork is carried out when there is a need for upgrading the protocols by introducing a new consensus. This splits the Blockchain into two different ones which run simultaneously. Nodes which are running the previous versions of the software follows the old rules whereas the nodes which are running the new version follows the new set of rules. Hard forks are categorized into two ways:

Planned Hard Fork:

In this all the project developers and stakeholders will agree to a protocol upgrade prior to the hard fork. As the name suggests these hard forks are planned.

Contentious Hard Fork:

This occurs when there is a conflict of interest between the project developers and other network users on the changes being made to the Blockchain network. In this case, two separate chains are formed for both the new version and the old version of the software.



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

Fig. 4 Hard Forked Blockchain [7]

Hard fork can also be used to increase the block size so that a greater number of verified transactions can be stored in each block.

B. Off-chain Scaling Solutions

Off-chain Scaling Solutions are applied off the chain, that is they are applied outside the chain. This includes solutions such as Consensus algorithms, payment channel and so on. These solutions effect the time taken for transaction verification process by changing the fundamental way of how a transaction is verified by implementing efficient, faster and trustworthy consensus algorithm. Other off chain solutions like payment channel create smart contracts amongst two or more people in the blockchain, they create a shared wallet and when funds have to be sent the ownership of the amount is changed. This shared wallet can be dissolved when all the parties agree.

Payment Channel

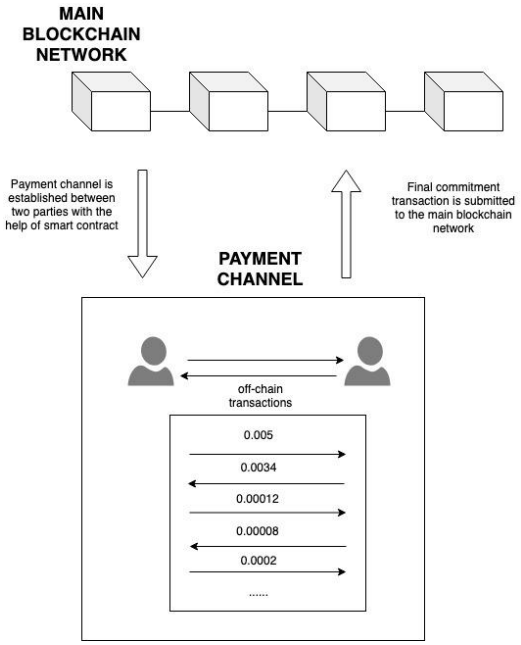


Fig. 5 Off-chain transaction using Blockchain

This mechanism is used by Bitcoin in which a transaction between two parties happen outside the Bitcoin Blockchain.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

In this, the transactions are moved to a private payment channel which has the same level of security as normal Blockchain. These channels can be closed by the users once the final transaction is published to the Blockchain. There are three phases of payment channel:

Anchor Transaction:

Firstly, a transaction should be made between the two parties in the blockchain to establish a payment channel. This transaction is called the anchor transaction.

Commitment Transaction:

Then a payment channel is established between the two parties with the help of a smart contract. A shared wallet is then set up, so transactions can be carried out between the parties by changing the ownership of the currency in the wallet. This channel is closed when the wallet is emptied. After every transaction, the previous state is made invalid so that the latest transaction state can be published on the blockchain after the wallet is emptied.

Settlement Transaction:

The payment channel can be closed by submitting the final commitment transaction to the Blockchain. [8] The shared wallet or the payment channel can also be closed if all the parties agree on it.

Since most of the transactions are happening in the off-chain payment channels between two parties, verification of every transaction by the whole network is not required. This reduces the overall cost and processing time.

Scalable Consensus Mechanism

Delegated Proof of Stake

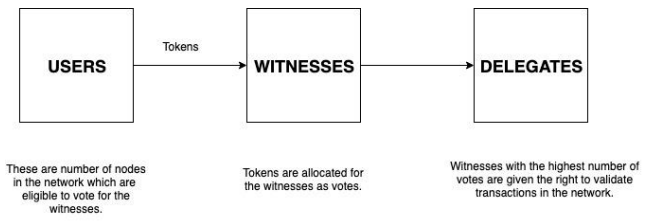


Fig. 6 Process of Delegates Selection

In this consensus mechanism, digital voting is carried out in which each user of the blockchain community has to vote for Witnesses (formally called Delegates) to validate transactions. The witnesses with the maximum number of votes will have the right to validate the transaction. These witnesses need not have the largest stake in the blockchain but the votes of users with large stakes will have a greater influence. [9]

As voting is always going on, the users can also vote to replace a witness with someone who is more trustworthy. Therefore, it is difficult to remain a witness in the top tier unless the person is legitimate, trustworthy and has invested a good sum in the Block chain.

The delegates should ensure that their node is always running for verifying transactions so that the queue containing unverified transactions do not pile up. A great amount of computational power goes into verifying transactions made on the Blockchain platform. The transactions are later recorded into a block. If there is an issue regarding the consensus, Delegated Proof of Stake allows this situation to be resolved in a fair and democratic demeanour.

IV. RESULT ANALYSIS

The following graphical representation indicates the transaction rate for payments made using VISA. The maximum number of transactions done being 60000 per second and 37000 per second being the lowest. The average trend is around 52000 transactions per second.

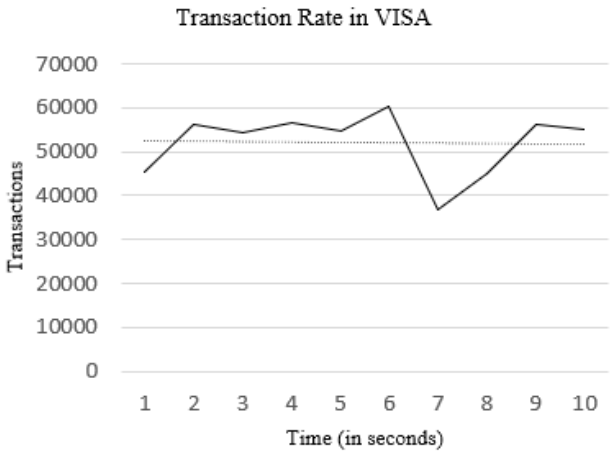


Fig. 7 Delineation of Time versus Transactions made using VISA

The following graphical representation indicates the rate of transactions for payments made on an ever increasing Blockchain having a reasonable amount of records. The maximum number of transactions being 60 per second and around 22 transactions per second being the lowest number of transactions made per second.

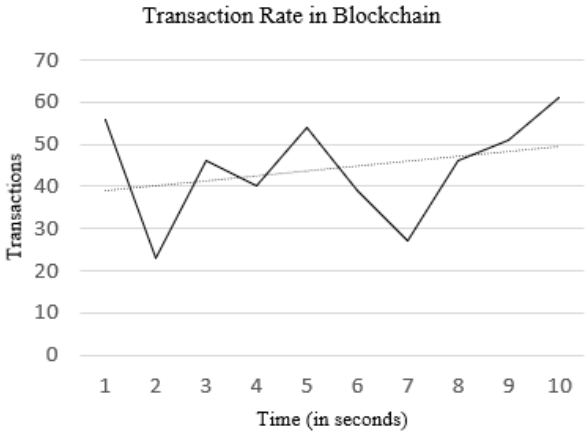


Fig. 8 Delineation of Time versus Transactions made using Blockchain

The following graphical representation depicts transaction rate after applying Scalability solutions discussed so far. The amount of payments verified on Blockchain has more than doubled after scaling the blockchain. The maximum number of transactions verified being around 220 per second, the average number of transactions being around 175 per second and the minimum number of transactions being around 150 per second.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

These Scalability solutions also make sure that as the number of blocks and the traffic for transaction verification increase the time taken to verify the transactions won't increase at an alarming rate.

Fig. 9 Delineation of Time versus Transactions made using Scaled Blockchains

All the above discussed Scalability Solutions improve the efficiency of the verification process and the rate at which the Blockchain platform verifies the transactions.

V. CONCLUSION AND FUTURE SCOPE

As the Blockchain technology continues to grow rapidly in various industries, scaling the blockchains has been a major concern which needs to be solved. This paper discusses the possible long-time scalability solutions which can make this technology a viable option in future. At first, the advantages and applications of Blockchain Technology are discussed. In addition to this, probable on-chain and off-chain scalability solutions are analysed.To conclude, it is evident that Blockchain technology is years away from overtaking the centralized networks.

Future research can be focused on finding scalability solutions for Blockchain Technology which will not affect the decentralization nature of the network.

ACKNOWLEDGMENT

This paper was supported by SRM Institute of Science and Technology, Ramapuram, Chennai. We thank our teacher and mentor G. Abinaya (Assistant Professor), for their expert assistance throughout all aspects of our study and sharing their words of wisdom that greatly improved the manuscript. We are grateful to all of those with whom we have had the pleasure to work during this project, without whom this project would not have been possible.

REFERENCES

1. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", 2008, https://bitcoin.org/bitcoin.pdf
2. https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/
3. "What are smart contracts in Ethereum", Smart Contracts Ethereum, [online] Available: https://blockgeeks.com/guides/smart-contracts/.
4. https://applicature.com/blog/blockchain-technology/blockchain-scalability
5. A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, "Blockchain and Scalability," 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2018.
6. https://blockgeeks.com/guides/blockchain-scalability/
7. https://www.investopedia.com/terms/h/hard-fork.asp
8. https://medium.com/coinmonks/payment-channels-in-bitcoin-470b28e47bb0
9. https://lisk.io/academy/blockchain-basics/how-does-blockchain-work

AUTHORS PROFILE

G.Abinaya, M.E., Assistant Professor, Dept. of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai.

S.Mary Shalin Benigna, B.Tech, Dept. of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai.

Hakshatha Devi, B.Tech, Dept. of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai.

Venugopal Balaji, B.Tech Dept. of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai.

Ashwin Chakravarthy.K, B.Tech Dept. of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai.