2018 IEEE International Conference on Software Quality, Reliability and Security Companion

Blockchain and Scalability

Mrs. Anamika Chauhan
Department of Information Technology
Delhi Technological University
New Delhi, India
anamika@dce.ac.in

Om Prakash Malviya
Department of Information Technology
Delhi Technological University
New Delhi, India
omprakashmlv9@gmail.com

Madhav Verma
Department of Information Technology
Delhi Technological University
New Delhi, India
madhavverma48@gmail.com

Tejinder Singh Mor
Department of Information Technology
Delhi Technological University
New Delhi, India
tejindersinghmor@gmail.com

***Abstract* — Bitcoin has shown great utility around the world with the drastic increase in its value and global consensus method of proof-of-work (POW). Over the years after the revolution in the digital transaction space, we are looking at major scalability issue with old POW consensus method and bitcoin peak limit of processing only 7 transactions per second.With more companies trying to adopt blockchain to modify their existing systems, blockchain working on old consensus methods and with scalability issues can't deliver the optimal solution. Specifically, with new trends like smart contracts and DAPPs, much better performance is needed to support any actual business applications. Such requirements are pushing the new platforms away from old methods of consensus and adoption of off-chain solutions. In this paper, we discuss various scalability issues with the Bitcoin and Ethereum blockchain and recent proposals like the lighting protocol, sharding, super quadratic sharding, DPoS to solve these issues. We also draw the comparison between these proposals on their ability to overcome scalability limits and highlighting major problems in these approaches. In the end, we propose our solution to suffice the scalability issue and conclude with the fact that with better scalability, blockchain has the potential to outrageously support varied domains of the industry.**

Keywords – Blockchain, Bitcoin, Ethereum, Lightning Protocol, Sharding, DPoS, Inspector Node.

I. Introduction

Blockchain has shown its tremendous ability in disrupting how digital transactions are carried out in a more secure and transparent manner. But the question still stands - does it have the ability to serve other real-world applications? Such confusion is because of the hindrance caused by its scalability issues.

Scalability issues arise due to limited block size and current consensus method where every node in the network sequentially validate the transaction before it being published in the blockchain. This problem intensifies with an increase in the number of transactions requiring more nodes to support the network but simultaneously increasing the number of steps for the transaction to travel and reach full consensus with every node. We can also see a proportional relationship between fall in scalability of the blockchain and increase in the network size. This flaw is the major setback that is stopping the mass adoption of blockchain for real-world applications.

II. What is Blockchain ?

The concept of blockchain recently came into limelight when the hype around Bitcoin and other cryptocurrencies gained momentum. Blockchain is the underlying principle behind cryptocurrencies. At the centre of blockchain, is a distributed ledger that records all the transactions that take place in the network. A blockchain network is usually described as decentralized because it is replicated across many network participants, each of which collaborate in its maintenance. In addition to being decentralized and collaborative, the information recorded on the blockchain is also immutable which guarantees that once a transaction has been added to the ledger it cannot be modified. This property of immutability assures the participants that their information is safe and secure.

At the very beginning of a blockchain is the 'genesis block'. Each block has certain attributes associated with it like- timestamp, nonce, version etc. The primary attribute among all of them is the 'hash' of the block which is generated by the merkle root of the current block and the hash of the previous block in the chain. It is this 'hash' which imparts two major properties to blockchain:

1. Linking of a block to its next block in the chain.
2. Any change to the data present in the block, would be immediately reflected in the hash of the block and all the blocks succeeding it.

The major advantage of a blockchain is that it doesn't depend on a central entity like some traditional banking system. Cryptocurrency investors are heavily encouraged by this property of the blockchain because instead of a central authority, it is the users and the developers joined to the network, who take important decisions.A big example of this is the inability to reach the 80% consensus on an upgrade in Bitcoin which lead to a hard fork in Bitcoin few months ago.

III. What is Bitcoin

Bitcoin is the first digital currency based on the blockchain technology. The concept of bitcoin and blockchain came into existence through a whitepaper named Bitcoin: a

978-1-5386-7839-8/18/$31.00 ©2018 IEEE
DOI 10.1109/QRS-C.2018.00034

peer to peer electronic cash system in the year 2008 and was released as an open source software in the year 2009 [1].

The main characteristic of Bitcoin is that it works in a decentralised manner. No single individual or organisation controls the Bitcoin network. The whole network is maintained by a group of dedicated computer or servers spread across the world which we call 'nodes'. It is these nodes which help in the verification and validation of all the transactions taking place in the Bitcoin network. This property of decentralization has attracted many individuals to adopt this new technology , who are not in the favour of a central authority controlling all their funds.

Another property of the bitcoin network is that each node or individual joined to it is represented by his/her public key instead of his real identity. While the senders of the traditional electronic payments are generally identified by some process of verification, the users of Bitcoin operate in an anonymous manner.

Bitcoin uses Elliptical Curve Digital Signature Algorithm to sign transactions [2]. This signing of transactions ensures that only the rightful owners have access to their assets and no one else. This signature is essential for maintaining the authenticity and integrity of the bitcoin network.

Unlike fiat currencies, Bitcoin has a limited supply that is tightly controlled by an underlying algorithm. In total there will be 21 million Bitcoins that will ever be produced. The reward for currently mining a block in the Bitcoin network is 12.5 coins. This reward is reduced in a proportional way every 4 years. This hard cap on the total supply makes Bitcoin a more tempting asset. In theory, if demand grows and the supply remains the same, the value will automatically increase.

IV. WHAT IS ETHEREUM ?

Ethereum has scored itself the second spot in the hierarchy of cryptocurrencies. The Ethereum project was proposed by Vitalik Buterin in the year 2013 and launched completely in the year 2015, after raising 19 million dollars in its presale. Ethereum is expected to surpass Bitcoin in the long run due to a major technological differences and applications that it can offer.

Ethereum is a distributed public blockchain similar to Bitcoin but the most important distinction between the two is in terms of its desire and potential [3]. Where Bitcoin offers only a single application of the blockchain technology that is peer to peer electronic cash transfer, Ethereum on the other hand opens up a new dimension of running decentralised applications on the blockchain network using certain programming code called "smart contracts".

A smart contract is a piece of code written in a certain programming language (Solidity in case of Ethereum) that can facilitate the exchange of money or anything of value. When smart contracts are deployed, they become independent entities that can execute certain commands when a series of conditions are met [4].

In the Ethereum network when a node mines a block, it is rewarded in the form of a crypto-token called Ether. Ether is the currency used to deploy smart contracts and pay the transaction fees associated with each transactions. Apart from being used as a token, Ether can also be used for trading and buying other cryptocurrencies.

The vision of Ethereum was to provide developers a platform to build decentralised applications. It has an aim to become the second Internet which runs in a decentralized manner and where the major decisions are taken by the users and developers that are joined to the network instead of a central authority.

Due to this reason, the DAO project was launched in the year 2016. The DAO (Decentralized Autonomous Organization) was the first of its kind - a fully decentralized organization with no single leader. It was made using a collection of smart contracts written on the Ethereum blockchain. It was owned by everyone who purchased tokens, but in this case tokens acted as contributors that gave the token holders voting rights on major decisions instead of giving them equity shares and ownership in the organisation.

V. SCALABILITY ISSUES ASSOCIATED WITH BITCOIN AND ETHEREUM

With the increasing popularity and adoption of cryptocurrencies like Bitcoin and Ethereum, they are compelled to think about a very basic problem in the initial design i.e. the lack of scalability. As cryptocurrencies are becoming more mainstream day by day, the number of transactions are also increasing in an exponential manner. Let's have a look at the increase in the number of transactions in Bitcoin and Ethereum in the past few years.

The below figures indicate that cryptocurrencies are being adopted at a very fast rate but as they have gotten more popular, a series of issues have come up regarding them and the major issue among it is the problem of scalability. Actually, the main problem lies in the basic principle on which the Bitcoin principle is based that is the mining nodes have to verify each and every transaction that occurs in the network [5] .

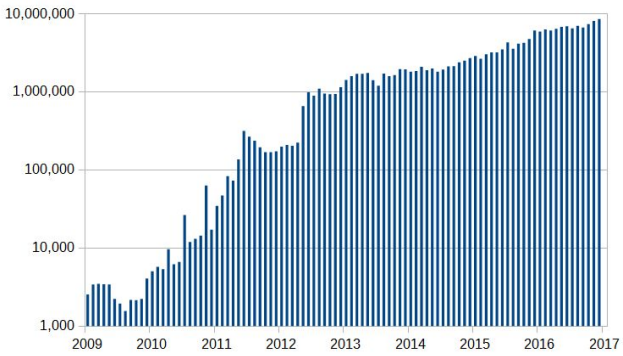

Figure 1 : A graph denoting the increase in bitcoin transactions over the last 10 years.
Source : blockgeeks.com

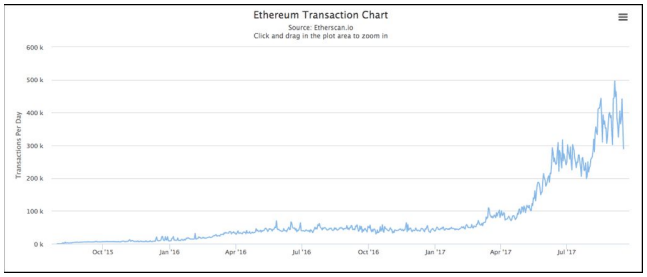

Figure 2 : A graph denoting the increase in ethereum transactions over the last 10 years.
Source : blockgeeks.com

Eventually, it is the miners who become the bottleneck in the transaction process. The process of verification was achievable when Bitcoin started in 2008 but as more and more people joined the network the number of transactions every second changed in a very drastic manner.

In the previous year itself there were at least 130,000 transactions occurring every day. Since this is a huge amount, it has become very difficult for the mining nodes to verify this lot. As a result of this, the waiting time for a transaction has increased upto 29 minutes. This means that more often than not, people would have to wait for a new block to be mined in order for their transaction to be verified.

Unfortunately, Ethereum isn't doing any better in this regard as well. Theoretically, Ethereum is expected to verify atleast 1000 transaction per second but due to the gas limit imposed on each block it is only able to process around 20. This number is very small in front of electronic payment giants like Paypal and Visa, that are able to verify around 193 and 1670 transactions per second respectively.
Supporters of cryptocurrencies have argued to switch to other Altcoins but have always feared this step due to two main reasons:

1. No coin is widely accepted and trusted as Bitcoin and Ethereum
2. If any other cryptocurrency becomes as popular as Bitcoin and Ethereum it will probably face same problem.

Due to these problems, the developers of Bitcoin are proposing a new Lightning Protocol to speed up the verification process and similarly the makers of Ethereum have proposed the method of sharding to overcome this situation.

VI. BITCOIN LIGHTNING PROTOCOL

A. Opening of Channel

Let's say there are two parties who want to create a bi-directional payment channel between them for multiple transactions during a fixed time period. The first thing they need to do is to fund the payment channel where the funding should be equal to the amount of trades they are going to do with each other. Both the parties need to send their funds for the payment channel to a specific multisignature address. Once the fund is sent, it is locked up in multisig address where signatures of both parties will be needed to unlock or spend any fund/BTC [6].

Both the parties can create transactions from their regular bitcoin address and it will need signatures from both sides to become a valid transaction. There is also a time period for each transaction which if not fulfilled, within a particular time period, both the parties will get their refund after that (eg. 30 days from when the address is created)

Now, if one party wants to back out in between the transaction, it needs to get the incomplete transaction signed by the counterparty. But the asymmetry here is that his counterparty will get the refund after 1000 blocks (a week). This prevents unnecessary cancellations and cheating.

B. Exchange

Once the funds are locked, parties can perform exchange of amount. This means that they can transact with each other, and the fresh transaction after the funding transaction, is achieved by exchange of fraud-protection proof, with signing of transaction by each party. So, if a party tries to cheat by broadcasting false transaction, counter-party can show the fraud to the miners by showing them previous transactions and it will cause the guilty party to lose all of its funds. Though, counterparty will have the time of one week to notify guilty party. Even if anybody else recognizes the fraud or the false transaction, he will get a small bounty from that money. This practice discourages cheating and fraud.

C. *Closing of Channel*

There can be two ways to close the channel. First, as discussed above, will be if any of the party chooses to opt out of the transaction, and is ready to face 1000 blocks delay for the refund. Second will be when all the transactions are done and channel reaches end of the duration.
Once the channel is closed, regardless of the number of transactions between both the parties, only two transaction will be recorded in the blockchain, opening and closing transaction.

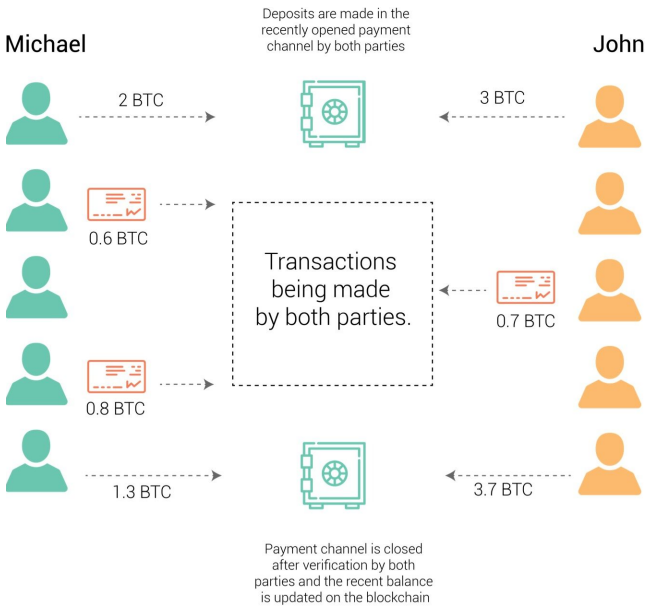

Figure 3 : A figure showing an off channel exchange between two parties.

D. *Multiple Channels Connections*

Now let's see how lightning network is going to help get the transactions done among multiple network channels. Let's say if there are 3 parties and there is already a channel established between party 1 and party 2, then there is a channel between party 2 and party 3. Now, if party 1 wants to transact with party 3 then he doesn't need to create another channel, because they can transact with each other by routing payment through already existing networks. Here, for routing payments, party 1 is given a secret key by party 3. As there is already a connection established between 2 & 3, Party 1 lets party 2 pay on its behalf to party 3 in exchange of a secret key. Now, Party 2 shows this secret key to party 1 and if both of their secret keys match, it would mean that party 2 has paid party 3 and is not lying.Such a system of multiple network channels can be extended to any number of participant channels.

VII. ETHEREUM SHARDING

Ethereum developers proposed another method to scale the blockchain by dividing them into shards where each shard has its own history of transactions and states. Certain nodes will verify only certain shards, thus the load on network will be reduced. This would allow to get transactions processed across a bunch of partitions 'Shards' rather than the mainchain handling all the transactions itself [7].

Elements of a Shard:

Collators : Nodes in a certain shard will be called Collators, which will be creating Collations. Collation is a specific structure containing important data like transaction and state history about certain shard. Each Collation will have a Collation header which will contain the following information:

1. Which shard the collation will respond to.
2. Current state of shard (before all the transactions are processed).
3. State of the shard after all the transactions are processed.
4. Digital signatures from at least ⅔'s shards confirming that the Shard is legit.

Supernodes : Supernodes will be the nodes taking all collations across all the shards and putting them in a single block which will be later added in Ethereum blockchain. This new kind of Block will be valid if :

1. All transactions are valid in all of the collations.
2. Collations have the same state as their current state before processing transactions.
3. Collations have the same state as specified in collation header, after processing transactions.
4. Collations must be digitally signed by ⅔'s of collators.

Now let's see what happens when a transaction happens across shards.

Receipts : The idea of receipts is what makes the cross shards transactions easy. Let's say there is party 1 in shard 1 and party 2 in shard 2, then to process a transaction between party 1 and party 2 (party 1 wants to pay 'x' ether to party 2) first the transaction is sent to shard 1 which reflects changes in party 1's balance, and system then generates a receipt for the transaction, which is gonna be stored in merkle root because they can be easily verified. Then a transaction is sent to shard 2 with receipt data as well which checks whether receipt has been spent or not.
It then reflects changes in party 2's balance and also marks the receipt as spent. Now, shard 2 can create new receipt for subsequent transaction.

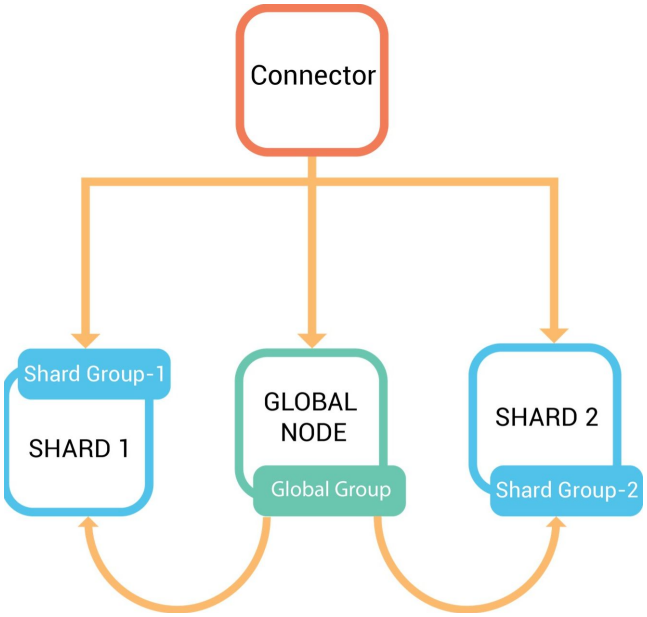

Figure 4 : Sharding Structure

Super Quadratic Sharding

In order to further scale the Ethereum network after sharding, there comes the concept of super quadratic sharding, which means dividing network into shards of shards. Such a complex system is too complex to imagine at this point of time, but if in future sharding becomes successful, then super quadratic sharding might become a useful technique to scale the network which will provide the network massive potential that can be scaled up till any level.

VIII. DPOS SOLUTION BY EOS

DPoS is a solution provided by EOS to scale blockchain for 100,000 transactions per second. Let's see how this solution is going to help the blockchain meeting the demand of ever rising crypto economy.

In DPoS systems, token holders select the block producers by continuous voting procedure. Anyone can become a block producer on the basis of the votes that he gets, and then he can produce the Block in proportion to his vote collection relative to other producers. In DPoS system, Blocks are produced in the rounds of 21. At the beginning of each round top 20 unique producers are selected automatically by total approval and the last producer is chosen on the basis of its proportional vote count relative to other producers [8].

In this system, a new block is produced exactly every 3 seconds by exactly one producer at a given time. Such a system has 100% block producer participation so transaction will be confirmed with 99.9% certainty in average 1.5 second after the time of broadcast.

Problem:

A new block in every 3 seconds is an exceptional performance measure for a blockchain which will get transaction confirmed much faster, but this system lacks something which is known as 'fraud proofs'.

Let's see how this affects the system and other problems as well:

1. DPoS removes merkle proofs that prevent regular users to audit execution of any part of the system. If regular users want to audit, they will have to run a full node which is not feasible at all.
2. Nodes producers are fired or hired on the basis of votes they collect. Voting power depends upon stake of user in EOS tokens. More tokens one holds more will be his voting power which shows a slight way towards centralization just like the concept of having more hashing power combined meaning more control over the chain.
3. In every 3 seconds, exactly one full node will produce a block which defines the way for a scalable blockchain. But, for a single full node to produce one block would mean much higher computational energy, which only large enterprises can afford. So, its scalability depends on much higher computational power like every other scalability solution.

IX. WHICH IS MOST OPTIMAL SOLUTION ?

Well, when we talk about scaling Blockchain there can be two ways to scale it:

1. Offchain scaling
2. Onchain scaling

Let's see which solution holds the basic functionalities of Blockchain.

Problems with Off chain scaling (Lightning network):

1. For a lightning network, every time a party wants to pay another, it will have to open a channel between both the parties. Where opening and closing are the transaction which will be recorded on the main chain that would mean both transactions are going to take traditional mainchain transaction time. So it won't be a real time transfer of value because of the time taken by one party to open a channel.
2. In a lightning network, duration for a channel to last is fixed so there will be a recurring problem of opening and closing transaction time period between

the two parties who want to transact even after closing their channel in future.
3. In order to open a channel on lightning network there must be sufficient funds put by both parties to transact with each other.
4. On Bitcoin network, current transaction fees is too high around 30$ per transaction. So, in such a system opening and closing transaction will cost too much if the transaction is of just 10$.
5. Fifth, and the most important, factor that worries is all of these transactions are being verified and validated off mainchain, which violates the very basic rule of blockchain where every transaction is verified by some predefined set of rules, basically where for each transaction participating full nodes compete with each other to verify and validate them.

Problems with current model of Sharding

1. The main problem that comes with sharding is 'single-shard takeover attack'. Where if an attacker takes over majority of collators in a single shard, he could manipulate them to create a malicious shard and submit malicious transaction as well.
2. Well, solution proposed for above mentioned problem is to assign each shard validator nodes or collators by random sampling. Each shard will be assigned a bunch of collators but the nodes that will be verifying transactions will be selected by random sampling from that set of collators.
3. Then there comes another problem that after each reshuffling of collators, each node will have to download and install a new shard, which is a problem that we can't' ignore because it will affect the speed of transaction as well.

X. OUR SOLUTION - INSPECTOR NODE

Well, we can't deny that lightning network is a powerful solution to scale blockchain, like a second layer of Blockchain which routes payment across various payment channel on the network. But, it doesn't carry core functionalities of Blockchain, as it is a offchain solution. So operations of a blockchain network are not applied at this layer.

Among all of other scaling solutions, Sharding seems the most effective solution. As it holds core functionalities of Blockchain with it. Each shard works like a seperate blockchain network, which operates completely as Satoshi Nakamoto visioned a blockchain to work.

Let's see how we can remove the problems that currently Sharding model is facing, and how can we make the solution more effective and secure.

Inspector Node:

We need to ensure that only a fixed no. of Collators should validate the transactions for a shard, without reshuffling or random sampling. That would mean each shard will be assigned a fixed no. of nodes for validation and verification of transactions over shard. Then there comes the problem,

If an attacker takes over majority of the shards, He can submit malicious transaction in shard, which is gonna spoil the main property of a blockchain which is 'Highly secured'.

Here we propose the concept of 'Inspector nodes', which will contribute only to investigate and eliminate malicious activity going on in a shard.

Functions of Inspector node:

1. This node will keep checking whether a majority is being developed among collators. If it sees that an attacker is trying to take over some shards (if it has already acquired a minimum percentage of hashing power from the nodes, which will be different for each shard), it will prevent the attacker from doing so and would reshuffle the nodes assigned to a shard instantly. In such a case, only when an attack is likely to happen, nodes will be reshuffled by random sampling.
2. There will be a fixed number of inspector nodes assigned to each shard, which will keep an eye on every broadcasted transaction in the network to see if there is anything suspicious about that transaction or not.
3. To prevent majority from being formed inside a network, we need to keep the competition tight among validating nodes. This is where we propose a unique incentive model for Inspector nodes.

Incentive Model for Inspector Nodes:

1. Every Inspector node, who finds the malicious activity first inside shard, will be rewarded with all the funds involved in the malicious transaction, and that fund will be cut from suspect node's account (which will be cut in a ratio if there is more than one node).
2. Apart from that, Inspector nodes will be paid inspection fees as well if there is not any malicious activity happening in the network and that inspection fees will be cut from block reward of every node in a specific ratio (How many Ethereum a node has mined, a percentage of that reward will be paid to inspector nodes) as network maintenance fee, which

will be minimal as no. of Inspector node will be much less than validating nodes.

3. If any other validating node finds malicious activity and submit it, then inspector nodes will reward that node with all the funds involved in that transaction, it will keep competition in place among nodes.
4. This incentive model will prevent the attackers from practicing malicious operations as it can cost them their funds.

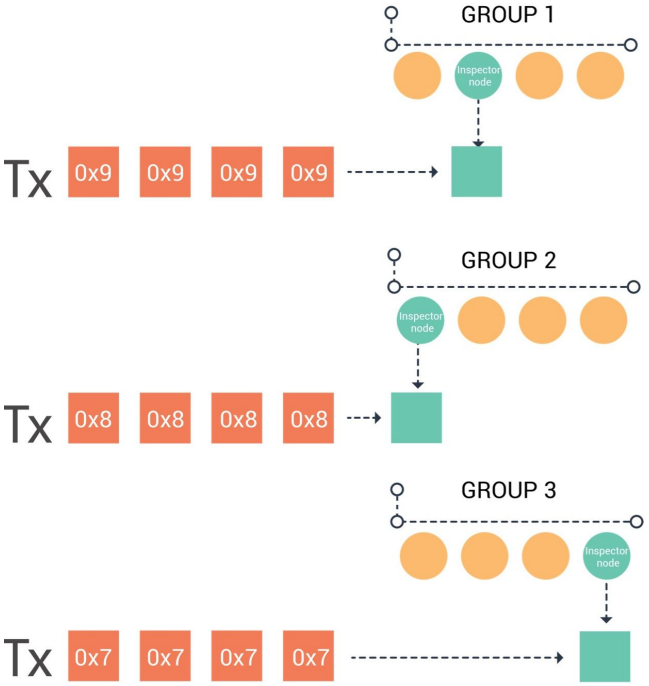

Figure 5 : Inspector nodes in action

XI. CONCLUSION

The only hurdle in Blockchain technology's way to scale upto masses is its scalability issue. There are various solutions floating in the technology space but each one comes with some problems associated with it. After analysing several possibilities of faults in all solutions, we have extracted that Sharding is the best possible method for scaling the blockchain as it includes core values and features of Blockchain. Having included our newly introduced Inspector node model in the current Sharding model, we can make this solution even better and faultless. The proposed solution contains three core functionalities of Blockchain : Decentralization, Security and Scalability. With having three main pillars of a solid and disruptive invention together, we can surely create the biggest disruption in industries, after Internet. Blockchain is still in its early stages, and we hope within next 5 years, it will transform a lot of things where transformation will be driven by scalability.

REFERENCES

[1] S. Nakamoto, "A Peer-to-Peer Electronic Cash System", (2008).
[2] "Elliptic Curve Digital Signature Algorithm," *Elliptic Curve Digital Signature Algorithm - Bitcoin Wiki*. [Online]. Available: https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm.
[3] "What is Ethereum? - CoinDesk Guides," *CoinDesk*, 31-Mar-2017. [Online] Available: https://www.coindesk.com/information/what-is-ethereum/.
[4] "What are smart contracts in Ethereum," *Smart Contracts Ethereum* [Online] Available: https://blockgeeks.com/guides/smart-contracts/.
[5] "The Raiden Network a Beginner's Guide.". [Online]. Available: https://blog.springrole.com/lightning-protocol-the-raiden-network-a-beginners-guide-c9d7bc702748
[6] "What is the bitcoin lightning protocol.". [Online]. Available: https://99bitcoins.com/what-is-the-bitcoin-lightning-network-a-beginners-explanation/
[7] "How to Scale blockchain using Ethereum Sharding.". [Online]. Available: https://medium.com/@rauljordan/how-to-scale-ethereum-sharding-explained-ba2e283b7fce
[8] "How EOS can solve the blockchain scaling problems". [Online]. Available : https://itsblockchain.com/eos-scaling/