# **Improving Scalability in Blockchain: Sharding**

Sajan Maharjan (20182095)

**Motivation:**

The year 2017 saw the rise of blockchain and cryptocurrency. Prior to that Bitcoin and cryptocurrencies were limited to software developers, geeks and cyberpunks. About 3 billion dollars were invested into different blockchain systems in the year 2017. Although blockchain based cryptocurrencies and payment systems promise a future of distributed, decentralized, trustless payments without the need of a 3rd party, scalability issues in blockchains have presented a hindrance before they can replace traditional payment solutions such as VISA, MasterCard and PayPal. Currently two of the most popular blockchains in use- Bitcoin and Ethereum can only process transactions at the speed of 3 to 7 TPS and 15 to 20 TPS respectively. On the other hand, existing traditional centralized payment systems such as VISA and MasterCard process transactions at the speed of 1200 to 24000 TPS. This paper explores various possible available exploits to enhance the transaction processing capability in blockchain based payment systems. Particularly, one of the widely proposed scaling solutions- sharding has been described in detail.

**Problem:**

As mentioned in the previous section, the problem of blockchain lies in its transaction processing capability. Transactions are collected in blocks. There is a limit on the size of blocks in Bitcoin which defines an upper bound on the number of transactions that added in a single block. While there is no inherent block size limit in Ethereum, there is gas limit of 6.7 million per block. Also, block generation in Bitcoin, takes an average of 10 minutes and requires at least 6 confirmations while an Ethereum block is generated every 15-20 seconds and requires at least 12 confirmations to be permanently written on the blockchain. This scenario presents a difficulty when considering the use of cryptocurrency in day-to-day life.

**Proposed Solutions:**

A variety of solutions have been proposed to tackle the blockchain scalability problem. These scalability solutions can be broadly categorized as- Layer 1 solutions and Layer 2 solutions. Layer 1 solutions involve forking- which is a change or update to the core blockchain protocols or divergence from the previous version of blockchain. Examples of Layer 1 solutions include- increase in block size, change of consensus algorithms, sharding, etc. Layer 2 solutions do not require forking, but make changes to the layer built on top of the base blockchain layer. Off-chain and side-chain are examples of Layer 2 solutions.

Bitcoin Classic and Bitcoin Cash, are forks of the original Bitcoin protocol, which aims to improve scalability by increasing the block size of Bitcoin block. The developers of Bitcoin did not expect its widespread use as is now and had opted for a block size of 1MB to prevent spam transactions. In the case of Bitcoin classic, the block size was increased to 4MB which could hold 4000-8000 transactions per block and thereby increasing transaction processing speed of the block. Segregated Witness is another soft fork to the Bitcoin blockchain which reduces the size and repetition of signature in transactions, thereby allowing more transactions to be included in the block. Since, block size increase is a vertical scaling solution i.e. nodes require more processing to produce a single block, only powerful nodes will continue operating and cause centralization around powerful nodes in the network.

Another solution that can be used to address scalability, involves the change of consensus protocols. Currently, Bitcoin and Ethereum employ Proof-of-Work consensus algorithms. In this algorithm, consensus becomes more and more difficult to achieve as the size of network grows. Participation of every participating node in the transaction validation makes transaction processing slower. Another set of consensus algorithms called Proof-of-Stake and Delegated Proof-of-Stake establish consensus via a small group of stakeholders/delegates. Approval of blocks from a certain fraction of the delegates confirms block generation. As a result, it blocks are generated quicker and require less confirmation time. An example of a blockchain employing DPoS consensus algorithm is the EOS blockchain that has 21 delegates and processes 3000 transactions per second.

The literal meaning of a shard means a piece or fragment. Sharding involves splitting a blockchain into different sections/parts called shards, each of which can independently process transactions. Sharding is one of the horizontal scaling solutions i.e. it does not require additional processing by nodes rather scaling capabilities increase with the increase in the number of nodes. The sharding process has been discussed in detail in the later contents of this paper.

Off-chain, a layer 2 solution, cuts down data processing on the blockchain by running computations off-chain. Transfer agreement, escrow mechanisms, coupon based payment channels can be used in which both parties locally maintain their copies of transactions/records off-chain and only record transactions into the blockchain while opening and closing of deal between two parties. This solution is applicable if two parties regular transact/deal with one another. Say A buys a cup of coffee from B on a daily basis. Instead of writing daily records of each transaction between A and B, an off-chain solution can be used in which A and B record transaction into the blockchain only at the beginning and record daily transactions in locally maintained ledgers. In the event that A and B want to close accounts between them, then they both verify one another’s local ledger and close the deal by writing the final transaction to the blockchain. Off-chain transactions are instantaneous. Another layer 2 solution is called a sidechain, in which a separate blockchain is attached to the main chain that facilitates trading of assets both ways. Sidechains improve transactions scalability adhering to the fact that they are independent of the main chain, can run in parallel with the main-net, and does not boggle the main-net. For a given state of Ethereum blockchain, assets and tokens can be moved to the sidechain in order to de-congest Ethereum network. This allows block validation to be done on the sidechain and not on the main net. In this way, sidechains can take all the work and at some point in time give its state to Ethereum, so the previous state can be updated with the current state.

**Sharding Model:**