This week's focus is on the scalability of Blockchains, primarily how to handle the Blockchain trilemma of achieving high scalability, without sacrificing decentralization and security. There are several proposed solutions for this. All of them consider which chain it wants to scale. For Bitcoin, the one method for scaling that seems to carry with it most potential is layer 2 scaling creating application-specific channels for transactions. For Ethereum, the scaling issue is somewhat more complex as it wants general-purpose composability with the EVM, not only application-specific. The scalability means higher throughput and faster finality.

We consider two ways of scaling. Off-chain, and on-chain. On-chain scaling requires changes to the core protocol of the mainnet. For Ethereum, sharding has been proposed as the most viable solution. The concept is to split the mainchain into shards. Sharding is the process of splitting a database horizontally to spred the load. This will reduce network congestion and increase transactions per second, by essentially creating more chains, known as chards. It will also lighten the load for each validator, as they only need to process the transaction for one shard.

Off-chain scaling is implemented separately from layer 1, they, therefore, require no changes to the core protocol. Solutions like layer twos are examples of this. They use the layer 1 consensus mechanisms for security on their own layer and derive solutions like optimistic rollups, ZK-rollups, or state channels. There also exist solutions that involve a separate chain such as side nets or plasma. These chains communicate with mainnet, but derive security from their own chain.

    - Optimistic rollup: is optimistic. It assumes that a transaction is valid, and only runs computation via fraud-proof in the event of a challenge
    - ZK-rollups: runs computation off-chain and submits a validity proof.
    - state channels utilize multisig contracts to enable transactions quick and free off-chain. The finality is settled on the mainnet. Currently, there are two channels: state channels, and payment channels.
    - A sidechain is an independent EVM-compatible blockchain running in parallel with the mainnet. They are compatible with Ethereum via two-way bridges and run under their own chosen rules for consensus, and block parameters
    - plasma is a separate chain anchored to the mainnet. It uses fraud proofs like optimistic to arbitrate disputes.
    - validium is a chain that uses validity proofs, like ZK-rollups, but data is not stored on the mainnet
- Different solutions might work together and minimize the attack vector while leveraging different mechanics for different use-cases. Hopefully, it might lead to increased scalability without sacrificing security.