Summary Scaling Blockchains

Tim Sigl

The motivation in Altcoins for side chains is to stabilize the price volatility by pegging the coins value to the value of Bitcoin in its bootstrapping phase. To transfer coins between a main chain and a side chain the main chain must be able to verify transactions on the side-chain. The Bitcoin script is not powerful enough to validate other networks. Simplified Payment Verification (SPV) could be used to check a transaction on a side chain. This approach is not ideal since Bitcoin nodes would need to check all of the side chains block headers. In the best case the side chain transaction would contain all information needed to verify its legitimacy. To verify a transaction the user must 1. proof the inclusion of the sidechain tx in a sidechain block, 2. proof sidechain block header showing that this block has enough confirmations. The Bitcoin nodes will not verify those claims instead they will wait for users to present contradicting evidence. Sidechains are somewhat risky because they employ their own security mechanisms and coins can easily be stolen on an insecure sidechain.

Scaling mechanisms on Ethereum are divided into On-Chain and Off-Chain scaling mechanisms. One On-Chain scaling mechanism is sharding where the database of transactions is splitted horizontally to spread the load. Off-chain mechanism can be rollups where the transactions are executed outside layer 1 and the data later posted the the layer 1. Rollups can be done in the form of optimistic rollups where the transaction is assumed to be valid by default or zk-rollups where only the proof of validity is submitted. One other Off-chain solution are state channels where multisig contracts are utilized to enable participants to transact off-chain and commit their settlement to the mainnet. Sidechains are idenpended blockchains which run in parallel to the mainnet and are compatible with Ethereum via two-way bridges. The sidechain runs under their own chosen rules of consensus and block parameters.

The idea behind the Bitcoin Lightning Network is that not all nodes need to know a transaction if it is only between two users. Two users can establish a channel where they trade with real Bitcoin but don’t commit their transactions to the mainchain. Only after the two parties are finished with interacting with each other a final transaction is made to the mainchain. A payment channel is in practice just a 2 person multisig address. Each time a person in a channel is paid a new transaction is created but not broadcasted to the Bitcoin network. There is no risk involved since at any point the latest state could be broadcasted to the Bitcoin network. This also enhances privacy since the Bitcoin network only sees the opening and closing transactions of a channel. The initial balance of a channel is set up through a funding transaction. The balance is updated through commitment transactions. In the case Bob leaves the channel after Alice made the funding transaction her funds would be stuck in the multisig address since she is missing Bob's signature. To avoid such cases Bob must issue a signed transaction to Alice beforehand to send all funds back. Alice will use this transaction in the case Bob leaves. To prevent users from publishing old transactions, where they will get more funds than in the current transaction, users will get punished for such a behavior by losing all their funds to the other person in the channel. The punishment can be done by using a revocation secret that gets published for old transactions after a new transaction is created. Payment channels can also be made from A

to D over intermediary user B and C for example. They use special HTLC (Hash Time Locked Contracts) outputs where each forwarder gets a small fee.
Monoxide is a network idea to scale Blockchains via independent zones. Each zone has its own blockchain and consensus. This way the network is partitioned into independent zones which enable linear scalability with the number of zones. A swarm is a set of nodes replicating the same data. In the network exists a global swarm which is joined by all nodes replicating minimum common information. Additionally each zone gets its own zone-specific swarm where most of the communication happens. A block is divided into two parts, A chaining-block for chain information and a transaction-block carrying the actual confirmed transactions. A chaining-block is very small containing only around 100 bytes. In a cross-zone transaction, the transaction is first checked in its originating zone and then sent to the receiving zone via a relay transaction. To not cut mining power by the number of zones Chu-ko-nu mining is proposed where each miner is encouraged to create multiple blocks in different zones with only one PoW. Eventual Atomacity guarantees that a withdrawal operation carried by a relay transaction will eventually be picked up by rational miners.