SCALING BLOCKCHAIN

There are different problems when we try to solve the problem of scale in blockchain. One of them is when we create a new block we need to update the state of the "cashing process", a transaction in Bitcoin, in which you spend 1 or more "checks" (actually known as UTXOs) and create 1 or more UTXOs to new destinations from those spent funds. To update the state of the UTXO set requires bandwidth equal to all the transaction volume to keep up with the changes, so a question related to this problem is about to find the best block size (although probably increasing the block size is not the solution since this action would increase the work of validation that can lead to a centralization risk). One possible solution for scaling blockchain is *moving from a blockchain to a tree*. Two blocks that can be mined at the same time, can be placed into a tree as parallel nodes without conflicting. The idea is that individual miners only had to deal with subsets of this tree (and still be able to verify transactions), reducing the bandwidth used. Using this structure, (i) a node can reference multiple parents, (ii) two nodes can contain the same transaction, and (iii) it increases the block rate relative to the Bitcoin block rate. Miners incentives must be aligned with correct operations, and the consensus is created by on the profit-maximizing miners, in which the reward needs to be proportional to a miner's target difficulty. Since two nodes can have the same parent (sibling nodes), that implies that it cannot be decide the miner coin allocation till all beads are seen by all nodes since it needs to be evaluated which block has the most work.

Finally, there is an interesting solution, called *pegged sidechains*, to avoid the Bitcoin centralization risk problem (as well as for other cryptocurrencies) and to scale blockchains. This solution is based on enabling bitcoins (and other ledger assets) to be transferred between multiple blockchains. To do that, we need that: (i) assets that are moved between sidechains should be able to move back to the original sidechain, (ii) assets should be moved without counterparty risk, (iii) transfers should be monotonic, (iv) sidechains should be firewalled and (v) users should not be required to track sidechains that they are not using.