Ethereum

Tim Sigl

Questions

1. When is a transaction based ledger a better solution compared to an account based ledger? Pros and Cons.
2. Why is contract code execution done by all nodes? Seems highly inefficient.
3. Is the mining algorithm still dependent on random data and computation which makes ASICs infeasible?
4. Doesn't sharding make the network vulnerable to attacks because you split validators to all shards? Meaning it will be sufficient to own 51% of a shard?
5. Can you expand the Ethereum network by just adding more shards? Like double the shards from 64 to 128?
6. Isn’t sharding also limited by the central coordinator chain?
7. Are Level 1 scaling solutions like sharding, switching to PoS preferred over Level 2 scaling solutions like side chains? It feels like Level 1 solutions are harder to implement then Level 2 solutions because it is necessary to change the core protocol.
8. What is the difference between chain-based PoS and BFT-based PoS?
9. What is the advantage of asynchronous Byzantine Fault Tolerance? (it allows for messages to be indefinitely delayed or lost, but how is this an advantage?)

Summary

Ethereum does support a turning complete scripting language that enables smart contracts with loops and complex logic. A SC can be called by anyone by its address. You pay a specified gas price for every instruction of the contract. Ethereum is account based which means that any tokens someone owns is stored in an account. In contrast to Bitcoin is the whole state of the blockchain saved in every block. Accounts can either be controlled by a person (i.e. externally owned) or controlled by contracts. The scripting feature enables Ethereum to support sophisticated applications like decentralized finance (DeFi), decentralized autonomous organisations (DAO) and decentralized storage. Ethereum has a blocktime of only 10 seconds. Ethereum makes use of an extension to regular merkle trees called merkle patricia tree. This allows for more efficient inserts and updates. Also Ethereum makes use of four different tree, namely a receipt tree, a state tree, a storage tree and a transaction tree.
The main reasons for Ethereum to upgrade its network are improved scalability and security and being more eco friendly. Before the upgrades Ethereum only supported a max TPS of 15, including high feed because of the congested network. The suggested proof of stake system will use much less electricity because not all nodes have to solve a cryptographic puzzle. The already launched beacon chain uses proof of stake. Later on the mainnet will be sharded into 64 shards. One shard will contain the old Ethereum blockchain. In proof of stake systems validators take turns proposing and voting on the next block with each vote

being weighted by the size of the deposit of a node (stake). Also it discourages centralized cartes more than a proof of work style consensus. Proof of stake has the ability to use economic penalties to make various forms of 51% attacks more expensive (faulty nodes can be slashed).