Summary

5. Ethereum

Ethereum expands the range of potential applications of blockchain to non exclusively financial uses of the technology (Buterin, 2013). The use cases described in its whitepaper include the tokenization of assets, the creation of stable coins and derivatives, decentralized identity and reputation systems, file storage, and DAOs.

The main innovations in Ethereum compared to the Bitcoin blockchain concern: the adoption of a Turing Complete programming language enabling the development of smart contracts and the adoption of the GHOST protocol to increase the block confirmation rate. Moreover, the fee and currency issuance model differ: while the issuance in Bitcoin is capped, Ethereum is based on a perpetual growth of the monetary supply at a rate which decreases over time.

As regards the state model, Ethereum adopts account objects, rather than the Unspent Transaction Outputs.

The underlying data structure on which the blockchain is based is a Modified Merkle Patricia Trie (Brickwood, 2018).

This is characterized by increased verification efficiency compared to classic Merkle Trees. In Ethereum, four Modified Merkle Patricia Tries are present: the Receipt Tree, State Tree, Storage Tree and Transaction Tree.

Both Bitcoin and Ethereum consensus protocols currently rely on Proof-of-Work, even though the Ethereum ecosystem is now evolving towards a two-layer structure consisting of a Beacon Chain maintaining consensus through Proof-of-Stake (consensus layer), and 64 shard-chains (execution layer) processing transactions and storing data (Ethereum.org). This aims to solve the scalability bottleneck inherent to the current PoW consensus protocol. From a security perspective, PoS reduces the chances to form centralized cartels and enhances protection from 51% attacks. Furthermore, PoS consensus is far more energy-efficient compared to PoW, as the capacity to propose blocks is not dependent on the miners' computational power used, but, rather, on the amount of ether being staked. As a consequence of reducing the energetic cost borne by validators, the need for new coin issuance will decrease(eth.wiki).