Ethereum

Lars Erik Wik

February 22, 2022

Summary

Bitcoin has a limited amount of built-in application specific functions, based on the nature of its scripting language. Ethereum on the other hand can support any application through smart contracts, which are Turing-complete programs that live on the blockchain. These programs are written in byte code, and are executed on an Ethereum-specific Virtual Machine. A smart contract has its own funds, and can be interacted with by users through API's provided by the contract. [3]

The Turing-complete programming language of Ethereum makes it much more than just a cryptocurrency. Instead any arbitrary application can be built on and run on top of the Ethereum network. E.g. decentralized storage, computing, or domain name services just to mention a few. [2]

While Bitcoin keeps a ledger of unspent transactions, Ethereum uses an account based model by utilizing a Modified Merkle Patricia Trie containing four trie data structures; the transaction trie with the purpose of recording transactions; the receipt tree with the purpose of recording the outcome of each transaction; the state trie with the purpose of keeping a key-value pair for each Ethereum account; and the storage trie with the purpose of storing all contract data. [1]

With Ethereum's upcoming Casper update, anyone who holds ether can participate in block validation by sending a special transaction that locks their funds in a deposit as a proof-of-stake. In proof-of-stake you do not have to divide your computing power in order to work on multiple chains; thus in contrast to proof-of-work miners would have an incentive to work on multiple chains simultaneously. In Ethereum this problem can be solved by giving penalties to disobedient validators by proof-of-misbehavior. [4]

References

[1] Dustin Brickwood. "Understanding Trie Databases in Ethereum". In: *Shyft Network* (Aug. 2018). URL: https://medium.com/shyft-network-media/understanding-trie-databases-in-ethereum-9f03d2c3325d (visited on 02/20/2022).

[2] Vitalik Buterin. "Ethereum Whitepaper". In: *Etherium* (2013). URL: https://ethereum.org/en/whitepaper/ (visited on 02/20/2022).

[3] Arvind Narayanan et al. *Bitcoin and Cryptocurrency Technologies*. Draft. Princeton University Press, 2016. Chap. 5, 8.

[4] "Proof of Stake FAQs". In: *Etherium Wiki* (Nov. 2020). URL: https://eth.wiki/en/concepts/proof-of-stake-faqs (visited on 02/20/2022).