IN5420 Ethereum

Michael Eikeland

February 2018

Ethereum

One can argue that Ethereum primarily is a blockchain-based cryptocurrency. By that definition it is in the same domain as Bitcoin. One way that it differs from Bitcoin - often pointed out as its most notable feature - is in its scripting language. Ethereum has a Turing-complete virtual machine that runs *smart contracts*. It addresses the concern of infinite loops (more general the halting problem) through implementing a *gas* system, where whoever invokes a contract has to pay per instruction of code executed. That mitigates attack, as a miner will terminate as either the attacker's gas money runs out or the gas limit is hit. Even though the contract isn't fulfilled, the miner still gets paid.

It also has other improvements over Bitcoin, such as a custom implementation of the *Greedy Heaviest Observed Subtree* (*GHOST*) protocol. It has the benefit of reducing the amount of "work" wasted when a block goes stale as stale blocks are included in the calculation of finding the "longest" chain. Ethereum requires all *full nodes* to keep track of the state in addition to all transactions as this is needed for the *smart contracts*. This property is often regarded as a problem for Ethereum's ability to scale. They do however claim that their data structure, a custom *Merkle-Patricia tree*, saves *5-20x* space as Bitcoin's data structure.