

to be [37].

Transaction fees and the gas limit help to prevent the execution of faulty code, like infinite loops and they help to save computational resources on the network. The gas limit also disincentivises potential denial-of-service attacks on the network [27][37].

### 3.2.3 Blockchain and mining

The Ethereum blockchain is very similar to Bitcoin. The most important difference is the fact, that a block not only contains a list of transactions but also the whole state of the network. The state is stored in a data structure called “Patricia Tree” [27].

The Patricia Tree is a modified Merkle Tree that is optimized for the insertion and deletion of nodes. It stores the state of all contract and externally owned accounts. Every block stores a reference to the root of the tree and updates only the parts that changed because of the effects of the transactions in that block. This allows new nodes to only download the Patricia Tree instead of all blocks to retrieve the state of all accounts and therefore saves a considerable amount of disk space. It is estimated that if this concept would be applied to Bitcoin, it would require a node to store between 5 and 20 times less data [27]. Ethereum also uses a different Proof-of-work algorithm, called Ethash, that produces a block every 12 seconds in average compared to 10 minutes in Bitcoin. This has the advantage, that transactions can be processed faster and a recipient of a transaction does not have to wait long until she can consider a transaction to be safe. It also increases the interactivity of applications that interact with contracts on the blockchain. Further, Ethash is memory hard and therefore ASIC resistant [37].

A negative effect of the fast block time is that the stale rate, the rate at which blocks that are not part of the main chain are produced, is increased. This is a security risk that can lead to centralization to mining pools since many miners will not be rewarded for their effort in mining new blocks. While in Bitcoin, such blocks are considered “orphan” and are no longer used, the GHOST protocol of Ethereum also allows for the inclusion of such “uncle” blocks and rewards the miners of them [27].

In contrast to Bitcoin, the mining reward for a block is static and exactly 5.0 ether. Successful miners also collect all gas that is used in the transactions of a block. Miners of “uncle” blocks receive 7/8 of the static block reward [37].

The total amount of ether issued in a year is statically bounded to 1/3 of the pre-sale, which is approximately 18 million ether. It is estimated that approximately 1% of the total monetary base is lost every year due to the death of key owners, lost of private keys or transactions to empty addresses. Therefore the supply of ether grows at a disinflationary rate until the rate of annual loss and destruction of ether will balance the rate of issuance and the currency no longer grows [27].

### 3.2.4 Light clients

A protocol for fully or partially light clients in the Ethereum network is still under development As of April 2017. However, fully and partially light clients will play an important role in the future.