Topic 5 Ethereum

Alexander Wandrup

Bitcoin has a few limitation when it comes to scripting.
Lack of turing-completeness, value-blindness, lack of state and blockchain-blindness

Etherium aims to create an alternative procols that does not have these limitation. The intent it to use this to buil decentralized application. Etherium is essentially a blockain with a built in turing-compelte programming language.

In etherium the state is made up of objects called “accounts”. It is made out of the nonce, ether balance, the accounts contranct code or the account’s storage. Ether is the crypto fuel of ethereum and is used to pay transaction fees. Transactions in Ethereum consists of a data packet that contains the recipient of the message, the senders signature, the amount of ether to be transferred, a startgas and a gasprice value. The STARTGAS, and GASPRICE fields are used for Ethereum’s anti-denial service model. STARTGAS represent the amount of computation steps allowed in the transaction, and GASPRICE is the fee for each step. This is used so the attacker have to spend proportionately for each resource they consume. The Ethereum blockchain is similar to the Bitcoin blockhain but it has a difference where ethereum blocks contain both the transaction list and the most recent state.