Summary Smart contracts Alexander Wandrup

Blockchain and cryptocurrencies popularity since bitcoin released have had massive increase in popularity and interest. Although bitcoin is the biggest cryptocurrency it suffers from a limited and insufficient programming language. That’s what other bitcoin based blockchains like Ehterium tries to improve upon. These currencies utilise a concept called smart contracts to make the currencies more functional while still maintaining decentralization.

The smart contract is a program that runs on the blockchain and is executed by all consensus nodes. These consist of program code, a storage file and it also contain currency. Users create the contracts by posting a transaction to the blockchain, this contract can not be changed after it is created. A contract executes when it receives a transaction and can both receive and send currency. A contract have several points where you can send your transaction. These points are essentially functions for the contract and the transaction works as function calls.

In etherium contracts also use gas in order to prevent a contract to use to much resources or to prevent contracts to be used as denial of service attacks. If a contract runs out of gas during a transaction it will revert all changed done to its original state but the gas is not refunded. The user who sends the transaction must spend currency to purchase gas.