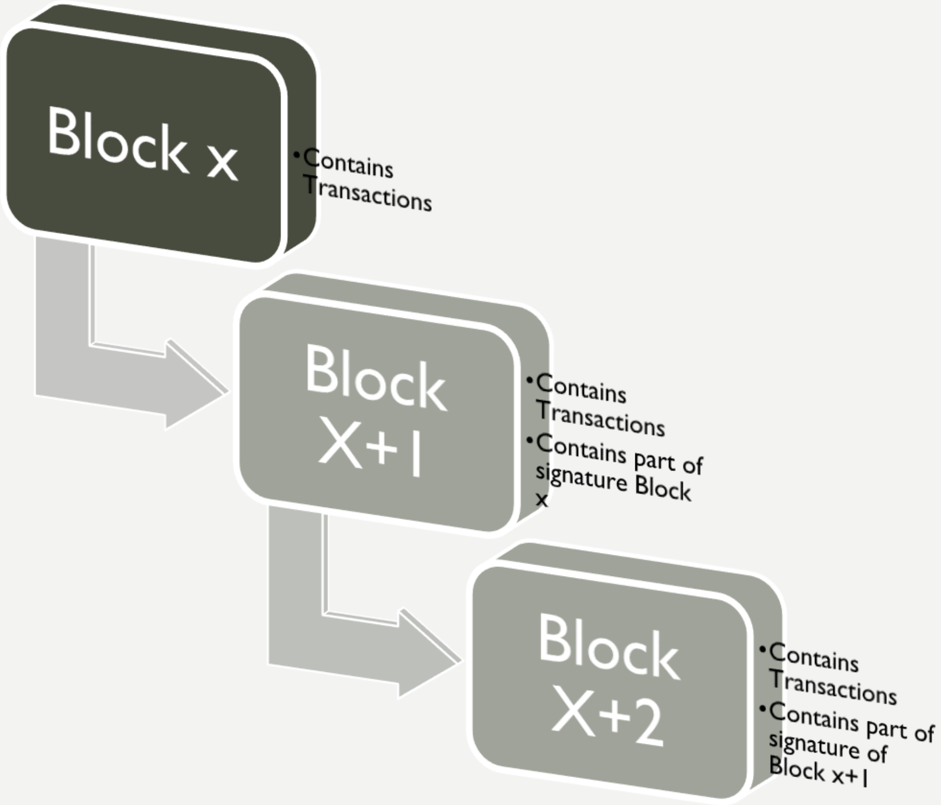
BLOCKCHAIN

THE BASIC CONCEPTS

WHY IT‘S CALLED „BLOCK CHAIN“ - SIMPLIFIED



Block x

- Contains Transactions

Block X+1

- Contains Transactions
- Contains part of signature Block x

Block X+2

- Contains Transactions
- Contains part of signature of Block x+1

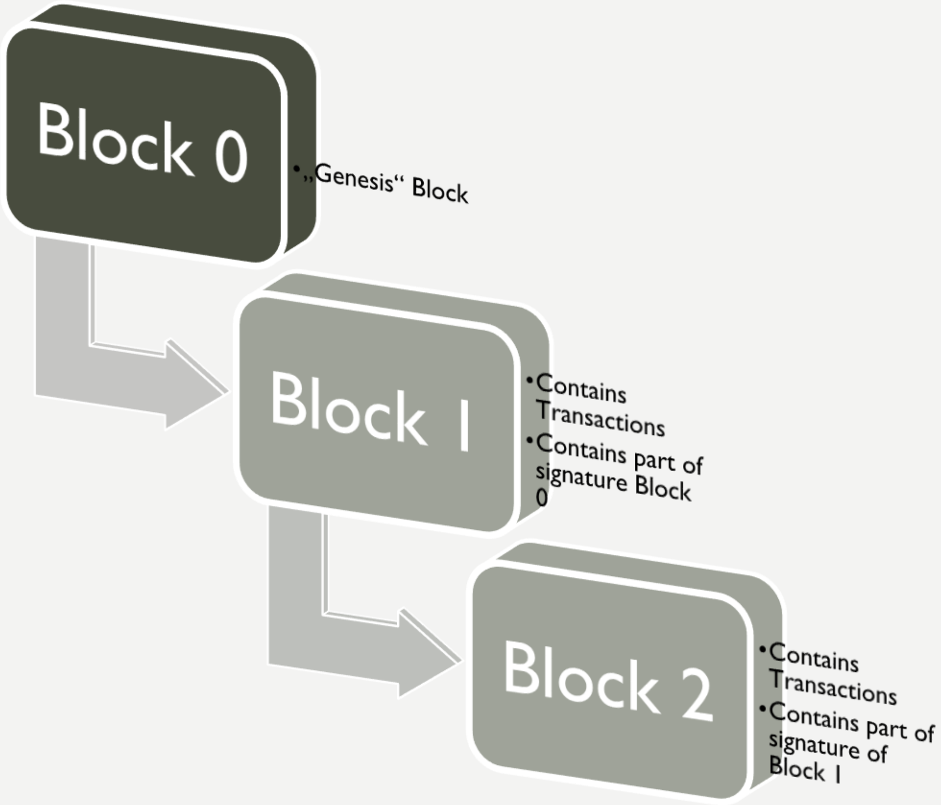
WHAT ABOUT THE FIRST BLOCK?

- It‘s called the „genesis“ block
- Can be configured (geth: genesis.json file, a config file)

- In the „main-net“ everybody connects to an existing blockchain, but someone started with a „genesis“ block

- A Private network is technically exactly the same as all other networks
  - Just you are in control
  - And probably you are the only node (but more can connect)

WHY IT‘S CALLED „BLOCK CHAIN“ - SIMPLIFIED



Block 0

- „Genesis“ Block

Block 1

- Contains Transactions
- Contains part of signature Block 0

Block 2

- Contains Transactions
- Contains part of signature of Block 1

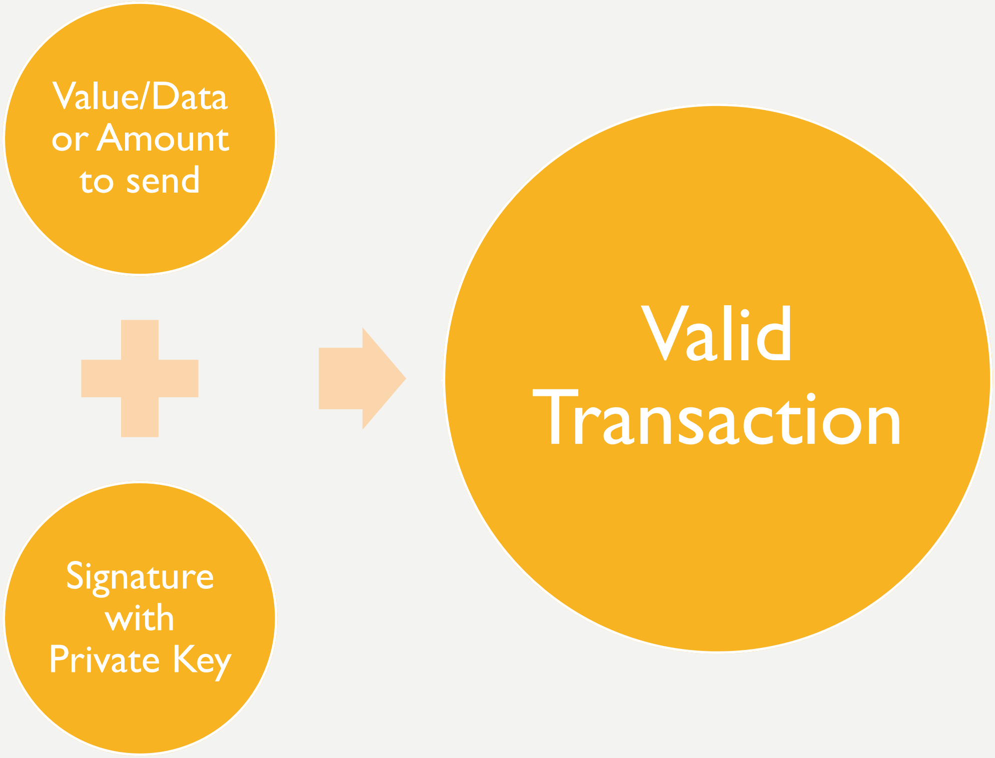
HOW IS A NEW BLOCK CREATED?

- By miners – it needs to be mined
- Solving a “mathematical riddle”
  - Hard to find the answer
  - But easy to verify

- Think of simplified „3*x=9; find x!“
  - Easy to verify, just plug it in and see if the result fits

- Bitcoin/Ethereum Main net: currently Proof of Work
  - Need calculating power (and electricity) to solve the riddle and „mine a new block“

HOW IS A TRANSACTION CREATED?



Value/Data or Amount to send

Signature with Private Key

Valid Transaction

PRIVATE KEY/PUBLIC KEY/ADDRESSES SIMPLIFIED

- Private Key
  - Used to sign transactions
- Public Key
  - Derived from the Private Key
  - Used to verify transactions
  - Can not bring back your Private Key
- Ethereum Address
  - Derived from the Public Key

WHERE IS THE „LOCATION“ OF THE BLOCKCHAIN

- On every computer
- Massive distributed database
- Trusted if you (and only you) hold the private keys
- Accessible through clients (GoEthereum, Parity, Ethereum++,…, MetaMask)

- Go Ethereum (geth) downloads the whole chain!

- Working with Distributed Apps (Dapps) – they assume you have access to the blockchain *on your computer*.
  - Unlike traiditonal database systems which are installed on the server-side

WHAT IS PROOF OF STAKE

- Proof of Work (PoW): You need to put in work to mine new blocks
- Proof of Stake (PoS): You need to put in Ether to mine new blocks

- Great, because better for the environment (doesn‘t burn energy)

- In the testing phase currently, possible switch is in 2018 (Casper)

- Will be probably a mix between PoW and PoS.

WHAT YOU LEARNED

- All chains, private, public, test, etc. are the same
- They start with a genesis block

- Don’t loose your *private keys*

- Access to the blockchain is client-side

- Current way of mining: Proof of Work (PoW)

QUESTIONS/SUGGESTIONS?

- Head over to the Q&A
  - We answer regularly

- Leave us a feedback
  - That‘d be great! ☺

- Disappointed, found a problem?
  - Send us a message
  - Head over to the course repository