**Bitcoin basics**

**Bitcoin as a currency, protocol and language**

Bitcoin really is:

Currency:

* Currency, language protocol
* Worldwide digital currency’
* Permissionless, anyone can use it, only internet connections
* No central bank (defi), no company no coorporation, runs 24/7/365
* Code open source, anyone can look at it, anyone can be a part of the development team, your code will be accepted if it is good enough
* Decentralized ecosystem because of open source code, trustless system.
* Inflation capo f 21 million bitcoin, hard corded into the source code. Will reach this point in 100 years, at 17 million now. Bitcoin can therefore not be inflateed like fiat.

Protocol:

* Language that computers use to communicate. Network of computers that is the bitcoin network they all communicate with eachother by predefined rules. When a transaction comes they know how to cmmunicate with eachother. If something is wrong f.eks. two versions of the blockchain (Forks). Forks are resolved in the protocol
* Different rules on how to handle problems. All the rules combined is the bitcoin network

Language:

* Bitcoin is a language with the primary medium as the internet, but theoretically nothing is stopping me from using SMS, a hand written letter and even smoke signal, that a miner can set into the blockchain.
* Therefore bitcoin is uncensorable

**Bitcoin ecosystem: miners, wallets, nodes SPVs.**

**Miners:**

* Miners are the only ones that can add transaction into the blockchain, inherently a node, but the nodes can not add the transacitons only validate them, if it is valid the miners will add the transaction into a block and then into the blockchain.
* Mining makes the network secure, hashrate (computer power). No censorship, can not double spend never use the same UTXO twice, can not og back and remove a transaction from the blockchain.
* Incentives: miners want to make money and they do that by securing the network. If someone double spends then the miner will use money. As long as the miner follows the rules and plays by the rules, then they get paid.

Proof of work and incentives:

* Make the miners spend a lot of electricity.

Every miner makes their own block with different transactions and there is a competition between the miners to append their block into the blockchain and earn money from it.

* Every miner have to spend a lot of electricity to solve a cryptographic puzzle. First to solve the puzzle will have their block apprehended to the blockchain, and the other blocks will be cancelled. He gets block reward (inflation) and transaction fees.
* The new block will get propegetated through the nodes. If your block has malware ( you break the rules, double spend or smth). If thats the case your block will be dropped and you wont get the rewards even though you have spent a lot of electricity to solve the puzzle and get your block apprehended.
* Therefore you are incentivized to follow the rules.
* The first transaciton in the block is without input because we have ijnflation, the first transaction is always the block reward, and the block reward is decreasing with time (only 21 million bitcoin)
* How to we reward mijners in the future? Through transaction fees because the demand for bitcoin will be higher. Block reward will in the end be 0 and only transaciton fee rewards

Pow nad integreti:

* When someone wants to add a new block, theyh need to solve a cryptographic puzzle. This cryptographic puzzle is based on contents from previusu blocks. The link from the old block to the new block being added is the puzzle. These links are expensive, and not random, base don the information from the previus block. If you remove a transaction from one block then the link between the next block will be broken and the next block, and all links from that block and forward will be broken.
* **If youk change the context of one block, then all the links forward from that block wil be broekn, and the nodes will see that this blockchian is invalid (d0snt make sense), and to make the chain make sense again then you need to solve the new puzzle being created based on the new content in the block because a transaction was removed. Now all the links from the block that was originally removed a transaction from has a new puzzle that needs too be solved. Therefore you cant remove a transaciton because it will take so many years to fix it, and everyone else will be adding new block to the chain because the network always choses the longest chain. Therefore by removing a transaction you wont be able to make money from mining again.**
* The difficulty to this puzzle is proportionate to the hashrate of the network, impossible to solve with only one computer.
* The network will always chose the longest chain with the most proof of work. Means that the miners have proven their work trough all the electricity spent.
* It is never worth for someone to og back and remove a transaction from the blockchain because it will be impossible for you to fix it nad you can never catch up to everyone else.

Math being proof of wokr:

* Each block has a hash. The digital fingerprint of the block, this is base don all th transactions that happened in the block, but also base don the hash of the previus blocks.
* This means that the unique fingerprint of the block is based in the previus hash, and the transactions of your current block. If a transaction in one block is changed then you change the hash in that block, but also if you change anything in the previus block then the hash in that block and the next block will also beb changed. This links with all the blocks in the blockchain because the previus hash is based on the hash from the block before.
* Also based on a random number that the miner have to find, called a **nonce**, when we hash the nonce together with the transaction list and the previus hash so that our hash (the fingerprint of our block) is less than a so called target. The target is a humber thatg depends on the difficulity of the network, if many people are mining the target jumber will be lower, and harder to guess. Only way fro the miner to deduce the nonce is to just keep guessing and guessing and guessing and hashing. And see if the hash number is lesser than the target.
* So when miners compete with eachother to compøete the cryptographic puzzle, all they are doijng s trying to guess this nonce.
* Only reason you have this system isj to make the miners spend money, so that they want to get the rewards, and therefore play by the rules, because otherwise their block will be rejected.
* The target: When the difficulty is high the target is low. The more mijners, the more energy the miners have to spend to guess the right nonce.

The difficulity of mining:

* A block is added approximately every 10 minutes (block time), therefore the network needs to adjust the difficulty depending on how many miners there are.
* If new blocks are produced to quickly it might generate orphaned blocks (so called stale blocks) the block rejected from the example below.
* We have for example to miners that have produced a block at exactly the same time andn are propegating the block through the network, one is in Australia so the nodes closest to him will get hisn blocks and propegeate the block. Another is in the US and propegates his blocks. Half of the network has oneversion of the truth and the other half has another version of the truth. Both are valid, one node believes that one sie is true and another node believes that the other side is true. When the next miner tries to put his block ijnto the blockchain what version of the truth prevails will depend on where this next block is placed because the network always choses the longest chain. The other block that then is excluded from the chain and removed, and the transaction from the block will be returned to the memepool. In the end always only one version of the truth
* What do you calla confirmed transaction? Best practice is to wait for 6 confirmations. This means that when your transaction is in a block added to the chain, you wait for 6 more blocks to be added before it is confirmed. So that your block dosnt get rejected like the example above.
* Why we have to wait 10 miutes is to minimize the probability to get stale blocks.

**Wallet:**

* Send or receieve Bitcoin
* The transaction is signed with your wallets private key, gets sent out to the network of computers, and the transaction will be broadcasted to all the nodes, and the transaction is in an unconfirmed state (not put into the blockchain)
* Stores your private keys, when you want to send bitcoin it will create and sign transactions, then broadcast the transaction to the network
* When you recieve founds your wallet will read the blockchain and notify you that you have founds you can spend.
* No coins in bitcoin
* You can store you private key in different ways: through a node, mobile phone through an SPV, Paper wallet (write down your private key on paper, cant send transactions)
* Hardware wallet:

USB device that stores your private keys, it is also offline and cant be hacked, if you don t connect it to the internet. You have a USB device connected to your computer, on the computer you will have an application that is communicating witht the wallet. The application will ask the wallet to sigjn the transaction, and the USB will sign the transaction in the USB, and then send the transaction to the application and then the application can broadcast it.

Transactions and UTXOs:

* UTXO: unspent transaction output
* Transaction: they have inputs and outputs, can have any number of inputs, and can have any number of outpus. Bitcoin transaction can send bitcoin to several different recipents at the same time. Can send from yourself to person A, B, C and myself in the same transaction. Input is where you got the money from, happened previously. Just laying around until yoku use them in a transaction. Sum of the inputs must match the sum of the outputs (or input higher than the output).
* B can for example create a new transaction witht the 0,5 he recieved as a input and then send for example 0,2 to D and 0,3 to E.
* The money B recieved from for example his mum will then be a spent transaction output, and the money D recieves will be an UTXO until he spends it again and it is a spent transaction
* Bockchain tracks UTXO, it tracks which transactions are unspent.
* Wallet says: I have this private key, which transaction outputs can i spend. Blockchain will give back what yoku can spend, wallet adds up these UTXOs and shows you your balance. Really isnt a balance store don the blockchain only the wallet saves that.
* If you have 2 UTXOS 1 with 0,5 and one with 0,4 and you want to buy a bicycle for o0,7, then you will send 0,7 to the bicycle store and then 0,2 back to yourelf because you ahve to spen the entire UTXO. Inputs always = to output.

Transaction Fees:

* Inputs need to be spent, but **inputs=output+transaction** fee. When miners mine new blocks they will chose the blocks with the highest fees because the fee will gok tok the miner.

Node

* The nodes checks that the transaction makes sense (not spending something you dont have, then the nodes will refuse), if it makes sense the transaction the nodes will validate it, but only the miners can add transaction into the blockchain

SPVs

* Nodes that does not have the entire blockchain, small node that trusts a full node when it wants to read the blockchain. If you are using an SPV for example if you are using you phone, because your phone can not have your entire blockchain, therefore you might be trusting a full node somewhere else, because you still need the entire blockchain to send a transaction.

Homework:

Wallets:

1. A bitcoin wallet stores your private key. The private key allows you to send and recieve bitcoin: By signing your transaction with your private key, the nodes can verify that you have the founds to make that transaction happen. Then the miners add this transaction into the blockchain.

UTXOs:

1. UTXOs are a transaction where you have gotten an input, but not used that input for an output yet. When you for example recieve 0,5BTC from your mum that is an UTXO, and when you for example send 0,2BTC to person A and 0,3BTC to person B then your transaction is spent and no longer a UTXO. The 0,2BTC that now belongs to person A will be their UTXO. A wallet adds up all your UTXOs and that is how you get your balance.
2. Then your transaction simply wont go through (The nodes will not validate it) because input will not equal output, and in a transaction input always have to equal output.
3. The fee is Transaction input - transaction output=fees. The fee goes to the miners and will want fees as high as possible so the fee amount will be to get the transaction through the blockchain in a reasonable amount of time. The higher the fee the faster the transaction will og through
4. You can increase privacy by having multiple inputs and outputs, and even sending founds to different addresses that you control.

Memepool:

* The memepool is where all transacitons are stored after they have been verified by the nodes. The miners take the transactions with the highest fees from the memepool, most staoshis per byte (because each block has a specific size), because the miners are incentivized to make the most money.
* The transactions with the lowest fees will take very long to be added to the blockchain because the miners priorities the transactions with the highest fees. Memepool will grow.
* A growing memepool will produce higher transaction fees because when the transaction is created you get a fee that will get your transaction through the blockchain within a reasonable time. Because miners chose the transactions with highest satoshi/byte.

Mining:

1. It is important to make miner sspend money while mining because it incentivises them to follow the rules. If they dont follow the rules and for example manipulate transactions then the nodes will see that something in that block dosnt make sense, and not add it to the blockchain. The miner will not get the blockreward and transaction fee reward and have lost alot of money on electricity to solve the cryptographic puzzle.
2. It is very difficult to og back and change a previus block because the one block is always connected to another (blockchain) because the link between the blocks is based on the cryptographic puzzle from the two blocks (hashes). So if you change one block then you will have to mine every block from that block and forward again for the links to make sense again and the nodes to accept your copy of the blockchain. And while you have to change all these blocks other miners will have added alot of new blocks so you would also have to catch up again because the network always choses the longest blockchain. The insane amount of electricity and computing power you need for this will never be worth changing that one transaction.
3. By making the target number lower if there are more miners. Tiss makes it more difficult because the nonce you need to guess for the hash to be below the target nuber is between 0 and infinity and the lower the target number is, by probability it will be harder to find a nonce that makes the hash under the target number.

Mining continuatuion:

1. It is important that the blocks are cryptographicly linked togethter so that a miner cant change the content of one block without changing huge parts of the chain. This is never profitable for the miner because it is nearly impossible to get the chain to make sense again, and if they area ble to, it would never be profitable for the miner.
2. The blockstructure is built up so that the blocks are connected to eachother through the blocks hashes. For example you have 3 blocks a, b and c. Block b will be base don the hash of block a, and block c will be base don the hash of block b. If you change the hash of block a, then block b and c dosnt make sense anymore and nodes wont approve the chain.

Stale blocks:

1. When two miners solve a block at the same time, the nodes closest to where the block was solved will propegate that block, while the ndoes closest to the other block will propegate the other block. If bothh blocks are valid then the nodes will have different versions of the blockchain that bot hare valid.
2. A stale block is a block that was removed from the blockchain
3. A stale block occurs when nodes have to versions of the blockchain with two different blocks that are both valid, and then the next block added will be added to one of the two blockchains that have been created. The network will approve the chain where the next block is added because it always chosess the longest chain (depends on difficulty aswell). The chain then removes the other block where a new block was not added, and now it is only one version of the truth again on all the nodes.
4. Your transaction is a part of a block and to make sure that your block dosnt become a stale block it is important to wait until atleast one more block is added to confirm the transaction.

Summarizing tasks:

1. The difference beetwen a SPV and a full node is that a SPV only have smaller parts of the blockchain. This is because for example your mobile phone dont have the capacity to have a copy of the entire blockchain, and therefore you only have parts of it through an SPV, which is again connected to a full node and trusts that node.
2. When a transaction is broadcasted it is being added to the memepool.
3. The miner picks what transacition will be added to the next block based on the transactionfee and the size of the transaction. The miner wants to make the most money and therefore choses the transactions with most satoshis/byte because each block has a fixed size. The satoshis they get are based on the transaciton fee you payed.