# Questions.

## Chapter 1: Introduction

### What are the main Bitcoin terms?

There are many Bitcoin system terms. The list of the Bitcoin system terms is described below (it is not exhaustive):

* Address
* Public key
* Private key
* UTXO
* Transaction
* Block
* Difficulty Target
* Distributed Ledger
* Blockchain
* Proof Of Work
* Consensus
* Wallet
* Node
* P2P network

### What is a Bitcoin address?

Bitcoin address is a list of letters and digits usually represented in Base58Check format. In fact, this address is a hash of a public key of the recipient. There are several types of Bitcoin addresses: for example P2PKH – Pay To Public Key Hash or P2SH – Pay To Script Hash.

### What is a Bitcoin transaction?

A Bitcoin transaction is a data structure that represents an operation of locking some bitcoins to an address of a recipient. This data structure has several informational items: one or more inputs, one or more outputs, the amount of bitcoins to be transferred. There are different types of transactions available in the Bitcoin network: for example a normal transaction, a Coinbase transaction.

Each transaction on average is 200-300 bytes, but of course, the size of the transaction depends on the number of transaction inputs and outputs.

### What is a Bitcoin block?

A Bitcoin block is a data structure that consists of a block header and a block data. Block data consists of transactions in this block. The initial size of the Bitcoin block was 1Mb and the Bitcoin architecture was developed to generate one block every 10 minute.

Miners work on the blocks, competing to create a block hash that corresponds to the difficulty target currently calculated in the network.

### What is a Bitcoin blockchain?

A Bitcoin blockchain is a set of blocks, connected to each other by references, starting from the Genesis block, or block with height 0. Usually a blockchain is represented by a stack of blocks, starting from the Genesis block and going upwards to the current block. Therefore, there is a term of block height.

### What is a Bitcoin transaction ledger?

It is a ledger of all transactions in the Bitcoin system from the beginning of the Bitcoin operation. All transactions could be traced to their origins.

### What is a Bitcoin system? What is a bitcoin (cryptocurrency)? How are they different?

A Bitcoin system consists of many things: protocols for communicating between different Bitcoin participating nodes in a P2P network, Bitcoin nodes of different types (full node, lightweight node), bitcoin currency. Bitcoin currency is only a part of the system.

### What is a full Bitcoin stack?

A full Bitcoin stack is the Bitcoin node that has all the current blocks in the system and is able to track all the transactions until the very first initial transactions.

### What are two types of issues that digital money have to address?

The first issue is to ensure that the money is not counterfeit, and the second issue is the issue of double-spending.

### What is a “double-spend” problem?

It is a problem that is applicable to digital money: how to ensure that the owner of money does not spend this money twice.

### What is a distributed computing problem? What is the other name of this problem?

Another name of the problem is Byzantine Generals Problem.

### What are the other applications of the solution to this problem in addition to the cryptocurrency?

People quote many things, such as elections and many others.

### What is an election?

An election is the process by which all the nodes decide which network state is the best now (by choosing a blockchain with a greater length).

### What is a consensus?

Consensus is a network agreement about the current network state. The consensus in the Bitcoin ecosystem is emerging.

### What is the name of the main algorithm that brings the bitcoin network to the consensus?

It is Proof of Work (PoW).

### What are the different types of bitcoin clients? What is the difference between these clients? Which client offers the most flexibility? Which client offers the least flexibility? Which client is the most and least secure?

They are: full client, lightweight client and web client. A full client downloads and stores the complete blockchain, it can trace all the transactions from the first, it can verify all the transactions. A lightweight client does not download the full blockchain, it downloads only the block headers. To check transactions it uses a procedure called SPV – Simplified Payment Verification. Both full and lightweight clients store keys internally. A Web client is a client that uses external nodes to do transaction processing (initiation, verification, etc). The most secure client is the full client and the least secure client is a Web client.

### What is a bitcoin wallet?

A bitcoin wallet is a SW that stores the key pairs for the users: public and private keys. It also does many other functions, for example aggregating small amounts from many accounts into larger amount in one account, assembles the best mixture of UXTO together to pay for something. It creates new key pairs and new addresses to get the change.

### What is a confirmed transaction and what is an unconfirmed transaction?

An unconfirmed transaction is a transaction that has been created, and has probably been sent to the network and even has probably been verified by the network, but it has not been included into any blocks yet. A confirmed transaction is a transaction that has been included in at least one block. A transaction that has been confirmed in a block and there are 6 blocks in total including the one in which there is a confirmed transaction is considered to be immutable.

## Chapter 2: How Bitcoin works.

### What is the best way to understand transactions in the Bitcoin network?

The best way to understand transactions in the Bitcoin network is to see some use cases.

### What is a transaction? What does it contain? What is the similarity of a transaction to a double entry ledger? What does input correspond to? What does output correspond to?

Transactions are like entries in a double entry bookkeeping ledger. There are inputs and outputs in transaction. Input corresponds to a debit and output corresponds to a credit.

### What are the typical transactions in the bitcoin network? Could you please name three of such transactions and give examples of each type of the transaction?

There is one to many transaction: for example when one company pays many of its employees. There is change collection transaction: many to one, for example when a wallet consolidates all its small UTXOs into one larger UXTO, and there is several to several (or one to several), for example when your wallet finds the UTXOs that cover the payment amount requirement, and generates (or uses existing) address to get the change.

### What is a QR and how it is used in the Bitcoin network? Are there different types of QRs? If so, what are the different types? Which type is more informational? What kind of information does it provide?

QR stands for Quick Response. This is a code (square code) that mobile applications can easily read. There are different QRs available, some of the QRs simply define the Bitcoin address and some define payment request with parameters. Clearly, a payment request with parameters is more informational. It provides information about the address to which the payment should be made, amount of the payment, message for the payment, etc.

### What is SPV? What does this procedure check and what type of clients of the Bitcoin network usually use this procedure?

SPV is an abbreviation of Simplified Payment Verification. This is a procedure that is used to check if some transaction has been confirmed or not. Usually lightweight clients use this type of transaction.

## Chapter 3: The Bitcoin client.

### How to download and install the Core Bitcoin client?

You can download the binary or use GIT repository to download, compile and install the Core Bitcoin client on your operating system.

### What is the best way to test the API available for the Core Bitcoin client without actually programming? What is the interface called?

The best way is to use RPC calls available from the Core Bitcoin client. The interface is called JSON RPC.

### What are the major areas of operations in the Bitcoin client? What can we do with the client?

The major areas of operations of the Bitcoin Core client are addresses, transactions, and blocks.

### What are the available operations for the Bitcoin addresses?

They are create a new address (key pair), encrypt the wallet, backup the wallet, restore the wallet.

### What are the available read operations for the Bitcoin transactions? How is a transaction encoded in the Bitcoin network? What is a raw transaction and what is a decoded transaction?

Read transaction with a specific TXID from the network. A transaction TXID is encoded as a hex string. A raw transaction is the transaction encoded in hex, so instead of giving the readable output the command line will output a hex string. The decoded transaction is a transaction with all the fields decoded.

### If I want to get information about a transaction that is not related to any address in my own wallet, do I need to change anything in the Bitcoin client configuration? If yes, which option do I need to modify?

By default the Bitcoin Core client only stores and provides information only about the local addresses. If you want the Bitcoin client to be able to represent the information about any transaction in the network, you have to launch it with the option: txindex=1.

### What are the available read operation for the Bitcoin blocks?

You can read the block of a specific block hash or you can read a block of a specific height.

### What are the available operations for the creation of the transactions in the Bitcoin network?

They are create raw transaction, decode raw transaction, sign raw transaction and send raw transaction.

### How do you normally need to address the unspent output from the previous transaction in order to use it as an input for a new transaction?

You need to address both: the transaction hash and the output number of the previous transaction.

### What is the mandatory operation after creating a new transaction and before sending this new transaction to the network? What state does the wallet have to be in order to perform this operation?

This operation is the transaction signature, it is done with the private key of the user and the wallet must be in the unlocked state of the transaction.

### Is the transaction ID immutable (TXID)? If not why, if yes, why and when?

When the transaction is send to the network the TXID can be changed. But once the transaction is confirmed, TXID is not changeable. It is called transaction malleability.

### What does signing a transaction mean?

It means signing some parts of the transaction with the private key of the user. In other words it is unlocking the UTXO, locked by some previous transaction.

### What are the other options for Bitcoin clients? Are there any libraries that are written for some specific languages? What types of clients do these libraries implement?

There are many different Bitcoin clients, for example libbitcoin (C++), bitcoinj (Java), btcd (Go) and pycoin (Python).

## Chapter 4: Keys, Addresses and Wallets.

### What is a PKC? When it was developed? What are the main mathematical foundations or functions that PKC is using?

PKC is an abbreviation for Public Key Cryptography. PKC was developed in the 1970s. The main foundations for the PKC is the prime number mathematics and elliptic curve cryptography.

### What is ECC? Could you please provide the formula of the EC? What is the p and what is the Fp? What are the defined operations in ECC? What is a “point to infinity”?

ECC stands for Elliptic Curve Cryptography. The EC formula used in Bitcoin is y\*y (mod p) = (x\*x\*x + 7) (mod p). P is a very large prime number and it is equal to 2256 - 232-29-28- 27-26-24-1. Fp is a field of numbers. There are two operations defined in ECC: addition and multiplication. “A point to infinity” is a special point on the EC that has a property: P+P1=P1.

### What is a Bitcoin wallet? Does this wallet contain coins? If not, what does it contain then?

A Bitcoin wallet is a software or hardware that is used to store the key rings: corresponding pairs of public and private keys.

### What is a BIP? What it is used for?

BIP is an abbreviation for Bitcoin Improvement Proposal. There are many BIPs for the ecosystem. For example, a BIP recommends encrypting the wallet to make the private keys more secure.

### What is an encrypted private key? Why would we want to encrypt private keys?

Whoever owns the private key could spend the UTXO allocated to the corresponding public key hash. Therefore, it is recommended never to store the key in the plain form. It is good to keep the key or rather the whole wallet encrypted.

### What is a paper wallet? What kind of storage it is an example of?

A paper wallet is a storage in which you store your private keys, since you do not want to keep them in your computer to avoid people stealing them from your wallet in your computer. This is an example of a cold storage.

### What is a nondeterministic wallet? Is it a good wallet or a bad wallet? Could you justify?

A nondeterministic wallet (a Type-0 nondeterministic wallet) is a key storage where all the private keys are generated independently from each other. This is not a very good wallet, since every time a new key is generated, the owner has to backup the keys.

### What is a deterministic wallet?

Deterministic wallet is a wallet which has all the private keys generated using deterministic key generation procedure. Each private key is created from the previous private key using one-way hash function.

### What is an HD wallet?

HD wallet is a Hierarchical Deterministic wallet, it is a set of key pairs that are generated deterministically from the initial seed or so called master key.

### How many keys are needed for one in and out transaction? What is a key pair? Which keys are in the key pair?

Two keys are required for one in and out transaction. One public key and one private key. The public key is provided with the signature to unlock the UTXO (to unlock the referenced amount from some previous transaction). A key pair is a pair of two keys: one public and one private key. A public key is generated with one-way function from a private key.

### How many keys are stored in a wallet?

As many as it is required by the user of the application. Could be few or could be really many.

### How does a public key gets created in Bitcoin? What is a “generator point”?

Public key gets generated by the formula K = k\*G, where k is the private key and G is the generator point. This is a special point on the plain and it is standard and known by everyone. It is described in the standard secp256k1.

### Could you please show on a picture how ECC multiplication is done?

### How does a private key gets created in Bitcoin? What we should be aware of when creating a new private key? What is CSPRNG? What kind of input should this function be getting?

A private key gets created using Pseudo Random Number Generator. When creating a new private key we should make sure that there is random information input into the algorithm of random number generator. CSPRNG stands for Cryptographically Secure Pseudo Random Number Generator. Such functions should look for inputs from user, for example mouse moves.

### What is a WIF? What is WIF-Compressed?

WIF stands for Wallet Interchange Format. This format is used to transfer key chains and key pairs between different wallets. WIF – compressed means that only one-half of the public key is stored: since the public key is generated from the private key using ECC, the public key has x and y coordinates on the plane. Therefore, only x coordinate is stored as well as the sign of the y coordinate. This saves half of the storage for the public key.

### What is Base58 encoding and what is Base58Check encoding? How it is different from Base64 encoding? Which characters are used in Base58? Why Base58Check was invented? What kind of problems does it solve? How is Base58Check encoding is created from Base58 encoding?

Base64 encoding is encoding with digits and letters, “+” and “/”. It is radix 64 encoding, which means that with one symbol a digit from 1 to 64 is encoded.

### How can Bitcoin addresses be encoded? Which different encodings are used? Which key is used for the address creation? How is the address created? How this key is used and what is the used formula?

Most of the Bitcoin addresses are encoded in Base58Check format. Double hash or HASH160 encoding is applied to the public key. First, SHA256 and then RIPEMD160 hash functions. The result is 20 bytes which are encoded with Base58Check format. The prefix is the version number, for public key it is 0x00

### Can we visually distinguish between different keys in Base58Check format? If yes, how are they different from each other? What kind of prefixes are used? Could you please provide information about used prefixes for each type of the key?

Yes, we can. Bitcoin address is 0x00 (or 1 in Base58), P2SH is 0x05 (3), Bitcoin Testnet is 0x6F (m or n), Private Key WIF 0x80 (5, K or L), BIP038 Encrypted Private Key 0x0142 (6P), BIP032 Extended Public Key 0x0488B21E (xpub).

### What is an index in HD wallets? How many siblings can exist for a parent in an HD wallet?

An index indicates a child of a specific parent. There are 32 bits reserved for a node. A parent can have 2 billion children.

### What is the depth limitation for an HD wallet key hierarchy?

There is no depth limitation for an HD wallet key hierarchy. It could be extended as much as it is needed.

### What are the main two advantages of an HD wallet comparing to the nondeterministic wallets?

The tree structure of HD keys can represent some organizational meaning. In addition, the sequence of public keys could be created by users without having access to the private keys.

### What are the risks of non-hardened keys creation in an HD wallet? Could you please describe each of them?

Extended public key contains the chain code. If the private key is somehow revealed then all the children private keys could be generated by the perpetrator. A child private key with the parent chain code could be used to get the private key of the parent.

### What is a chain code in HD wallets? How many different chain code types there are?

A chain code is used to introduce some random data into the process. There are parent and child chain codes.

### What is the mnemonic code words? What are they used for?

Mnemonic code words represent the seed (or master) private key. Using these keywords a seed key could be recovered and thus all the other keys in the hierarchy.

### What is a seed in an HD wallet? Is there any other name for it?

A seed is a master private key. Using this private key all the other keys could be recovered. Another name is the master key.

### What is an extended key? How long is it and which parts does it consist of?

An extended key is the key and the chain code concatenated. 256 bits of each create 512 bits of the extended key.

### What is P2SH address? What function are P2SH addresses normally used for? Is that correct to call P2SH address a multi-sig address? Which BIP suggested using P2SH addresses?

P2SH address is a Pay To Script Hash address. It is an address that starts with 3. It basically means pay to the script that has a specific hash. So, to unlock the UTXO sent to the P2SH address the receiver should use both the signature as well as the script. No, it is not correct to call P2SH a multi-sig address. Multi signature script is only one of the scripts that could be used. BIP016 introduced this feature.

### What is a WIF-compressed private key? Is there such a thing as a compressed private key? Is there such a thing as a compressed public key?

WIF compressed private key is a misnomer. There is no such thing as WIF compressed private key. There is WIF compressed public key. WIF compressed private key is 1 byte longer than WIF uncompressed private key. WIF compressed private key indicates that wallets should generate WIF compressed public keys from this private key and use such public keys.

### What is a vanity address?

A vanity address is the address that starts with a specific symbols to look more familiar or attractive.

### What is a vanity pool?

A vanity pool is a pool of servers that calculate private-public key rings so that the public key follows some template that is easily recognizable. For example with a prefix containing some specific word, for example “bitcoin”. Usually they charge some fees for their services.

### What is a P2PKH address? What is the prefix for the P2PKH address?

P2PKH stands for Pay To Public Key Hash. This is a hash of a public key of the recipient. Usually this is the transaction that is used most often. The prefix is 1.

### How does the owner prove that he is the real owner of some address? What does he have to represent to the network to prove the ownership? Why a perpetrator cannot copy this information and reuse it in the next transactions?

The owner has to represent two things: the first is the public address and the second is the encrypted with the private key some parts of the transaction. All participants in the network check that the public key corresponds to the address (since address is the hash of the public key) and using the public key they decrypt the parts of the transaction and check them against the actual transaction parts. If they are equal, that proves that the applied private signature is correct. A perpetrator cannot simply copy the signature in the new transactions, since the network after decrypting the signature with the public key will understand that the signature belongs to another transaction and will discard such a transaction.

### What is the rule for using funds that are secured by a cold storage wallet? How many times you can send to the address that is protected by the private key stored in a cold storage? How many times can you send funds from the address that is protected by the private key stored in a cold storage?

The rule is to use the private key only once from the storage, so if you want to send the funds outside, you should only do it once. You can send as many times as you want to your cold storage public address and key.

## Chapter 5: Transactions.

### What is a transaction in Bitcoin? Why is it the most important operation in the Bitcoin ecosystem?

Transactions are data structures that are used to transfer the value between the participants in the bitcoin system. Because it is the central operation of the Bitcoin ecosystem.

### What is UTXO? What is one of the important rules of the UTXO?

UTXO is an abbreviation of Unspent Transaction Output. This is an amount that is encumbered against some specific public key and that has not been used in any transaction as an input. One of the most important rules of the UTXO is that it has to be spent at once. It is like indivisible amount.

### Which language is used to write scripts in Bitcoin ecosystem? What are the features of this language? Which language does it look like? What are the limitations of this language?

The language is called Script. The programs in this language are written in reverse Polish notation. It uses stack for its operations. It looks like Forth. The limitation of the Script is that it is not Turing complete language, so some functions, such as loops are not available. There are simple if operators available.

### What is the structure of a transaction? What does transaction consists of?

Transaction has transaction hash and output index (they show the index of the transaction from which the funds have been collected), unlocking script size and unlocking script and then the sequence number (not used).

### What are the standard transactions in Bitcoin? How many standard transactions there are (as of 2014)?

There are 5 of them: P2PKH, pay to public key, P2SH, Data output: OP\_RETURN, and multi-sig.

### What is a “locking script” and what is an “unlocking script”? What is inside these scripts for a usual operation of P2PKH? What is a signature? Could you please describe in details how locking and unlocking scripts work and draw the necessary diagrams?

A locking script is a script that locks some specific UTXO against some address. An unlocking script is a script that is provided by the recipient to get access to the funds. A signature is an encryption of some parts of the transaction to prove that you have the private key. Everyone in the network could use the public key to check if the signature is correct.

### What is a transaction fee? What does the transaction fee depend on?

A transaction fee is the difference between the inputs and the outputs of the transaction. The transaction fee depends on the size of the transaction, not on the value inside the transaction.

### If you are manually creating transactions, what should you be very careful about?

One of the most important rules is that you have to spend the whole referenced UTXO, which means that you have to be careful to lock the change against your other public address. Otherwise the remaining amount of UTXO (input – output) will be collected by the miner.

### Could you please provide a real life scenario when you might need a P2SH payment and operation?

For example when you want to have two people who need to sign some specific transaction to withdraw or transfer funds. This is multi-signature script and operation.

### What is the Script operation that is used to store in the blockchain some important data? Is it a good practice? Explain your answer.

The operation is OP\_RETURN. This is a special operation that was created to save some information in the blockchain.

## Chapter 6: The Bitcoin Network.

### What is the network used in Bitcoin? What is it called? What is the abbreviation? What is the difference between this network architecture and the other network architectures? Could you please describe another network architecture and compare the Bitcoin network and the other network architectures?

The network used in a Bitcoin ecosystem is a P2P network or peer-to-peer network. All the participants in the network are equal, there are no dedicated masters in the network. Another widely used network architecture is server-client. A server is a kind of master of the network and

### What is a Bitcoin network? What is an extended Bitcoin network? What is the difference between those two networks? What are the other protocols used in the extended Bitcoin network? Why are these new protocols used? Can you give an example of one such protocol? What is it called?

A Bitcoin network is a P2P (peer to peer) network with a flat topology. There are no dedicated servers. An extended Bitcoin network is a network that runs Bitcoin and some other proprietary protocols, for example for pool management (Stratum). Pool management protocols are used to be able to connect different miners together to have a higher chance of mining new blocks.

### What are the main functions of a bitcoin node? How many of them there are? Could you please name and describe each of them? Which functions are mandatory?

The main functions of a Bitcoin node are: wallet, full blockchain node, routing node and mining node. There are 4 of them. Routing node is the mandatory node: it connects the client to the network (P2P network), checks and forwards transactions and blocks. Wallet functions provide users with services of generating new addresses, sending bitcoins to other addresses, etc. Full blockchain functions allows a node to collect all the blocks generated from the start of the network and could analyze every transaction to the initial transaction. Mining node functions allow to verify transactions and create new blocks, confirming these transactions.

### What is a full node in the Bitcoin network? What does it do and how does it differ from the other nodes?

A full blockchain node collects all the blocks and is able to verify all the transactions fully. From the initial generation of the bitcoins to their spending.

### What is a lightweight node in the Bitcoin network? What is another name of the lightweight node? How lightweight node checks transactions?

A lightweight node is a node in a Bitcoin network that does not download or store full block information. Another name of a lightweight node is a mobile node. The lightweight node checks transactions using block headers, Merkle root and path as well as Bloom filters.

### What are the main problems in the SPV process? What does SPV stand for? How does SPV work and what does it rely on?

SPV stands for Simplified Payment Verification. The main problem of the SPV is that it cannot see the full network picture and it cannot follow the UTXOs fully. The process is simplified comparing to the full process.

### What is a Sybil attack?

A Sybil attack is a partitioning attack. This is an attack on a lightweight node. A lightweight node uses SPV procedure to verify transactions. This procedure only checks if transactions exist in the blockchain. A Sybil attack is a partitioning attack, so lightweight clients check some neighbours and if such a lightweight client is surrounded by attacking nodes, they can convince the lightweight node of a certain network status even if it does not exist.

### What is a transaction pool? Where are transaction pools stored in a Bitcoin network client?

### What are the two different transaction pools usually available in implementations?

A transaction pool is a memory storage in miners. They collect all the transactions from the network and check them. If the transactions are correct and have confirmed (or checked) parents, then the transaction is put into the transaction pool in a specific client. If the parents are not available, the transactions are put into orphan pool.

### What is the main Bitcoin client used in the network? What is the official name of the client and what is an unofficial name of this client?

The main bitcoin client used in the network is Bitcoin Core. The unofficial name of this client is Satoshi client.

### What is UTXO pool? Do all clients keep this pool? Where is it stored? How does it differ from the transaction pools?

UTXO pool is the pool of all UTXO currently available in the network. A full nodes collects all the blocks and follows each of the transactions. So, it stores the UTXOs in its own memory. Transaction pool stores information about checked but unconfirmed transactions, but the UTXO pools stores the information about the UTXOs.

### What is a Bloom filter? Why are Bloom filters used in the Bitcoin network? Were they originally used in the initial SW or were they introduced with a specific BIP?

A Bloom filter is a specific filter use to get information from peers only about some specific transactions. Initially some specific transactions were requested from the peers, but it is not secure since the peers knew which addresses and transactions interest the client (lightweight client). Bloom filters solve this problem. Bloom filters can generate false negatives but never false positives.

## Chapter 7: The Blockchain.

### What is a blockchain?

A blockchain is a set of blocks, where one block succeeds the other. The later block refers to the previous block by indicating the previous block hash.

### What is a block hash? Is it really a block hash or is it a hash of something else?

Block hash is actually a hash of the block header and not of the whole block.

### What is included in the block? What kind of information?

In the block there is information about the previous block (previous block hash), there is Merkle root for all the transactions, there is nonce and there are transactions and there is block hash. Also there is target difficulty.

### How many parents can one block have?

A block can have only one parent.

### How many children can one block have? Is it a temporary or permanent state of the blockchain? What is the name of this state of the blockchain?

A block can have several children, especially when for example some miner generate a new block approximately at the same time. These blocks are called siblings. This state is a temporary state of the network and it is resolved when a new block is created (the longer chain wins and takes over the shorter chain).

### What is a Merkle tree? Why does Bitcoin network use Merkle trees? What is the advantage of using Merkle trees? What is the other name of the Merkle tree? What kind of form must this tree have?

Merkle tree is a binary search tree. Bitcoin ecosystem uses Merkle tree to quickly check whether one specific transaction is included in the block. It saves time and computation, since the amount of information that needs to be checked is much less. The Merkle tree is a balanced binary search tree.

### How are blocks identified in the blockchain? What are the two commonly used identities? Are these identities stored in the blockchain?

Blocks are identified either by their hash or by their position in the blockchain (so called block height). These identities are not stored in the blockchain.

### What is the average size of one transaction? How many transactions are normally in one block? What is the size of a block header?

The average size of a transaction is about 300 bytes. Since one block is about 1Mb in size there will be about 3000 transactions in a block. The size of a block header is 80 bytes.

### What kind of information do SPV nodes download? How much space do they save by that comparing to what they would need if they had to download the whole blockchain?

SPV nodes download the block headers instead of the full blocks. Since the block header size is only 80 bytes and the full block takes 1Mb, the SPV nodes only use 1/12000 of the storage capacity comparing to the full blockchain download.

### What is a usual representation of a blockchain?

A usual representation of a blockchain is a tower of blocks, where one block is put on top of the other block. Therefore a term block height is used.

### What is a genesis block? Do clients download this block and if yes – where from? What is the number of the genesis block?

A genesis block is a block 0 – the initial block of the blockchain. The clients do not download this block. This block is generated by the SW of each client.

### What is a Merkle root? What is a Merkle path?

Merkle root is a hash of all the transactions in the block. If the number of transaction is odd then the last transaction is duplicated to create a balanced tree. Then two transactions are hashed and the hash is put as a parent of those two transactions. Merkle path is a path in the Merkle tree for a specific transaction to reach the Merkle root.

## Chapter 8: Mining and Consensus.

### What is the main purpose of mining? Is it to get the new coins for the miners? Alternatively, it is something else? Is mining the right or good term to describe the process?

The main purpose of the mining is to verify transactions and confirm transactions into blocks. The main purpose is to support the Bitcoin network and ecosystem. To encourage the miners the new bitcoins are given to the miners. Therefore, the bitcoins are the incentive, but not the main purpose of the mining process. Mining is not a good term for the process, since mining means extracting something precious for example from earth.

### What is PoW algorithm?

PoW is Proof of Work algorithm. This algorithm tries to find the hash for a block of transactions that correspond to a specific pattern (specifically it must be lower than some number). The miners work on the pool of transactions that they have calculating the hashes and once the hash is calculated the block is released to the network.

### What are the two main incentives for miners to participate in the Bitcoin network? What is the current main incentive and will it be changed in the future?

The two main incentives are to collect fees and to collect bonus bitcoins. The current main incentive is to collect bitcoins but since the supply is diminishing, after all the bitcoins have been generated the main incentive will be the fees.

### Is the money supply in the Bitcoin network diminishing? If so, what is the diminishing rate? What was the original Bitcoin supply rate and how is it changed over time? Is the diminishing rate time related or rather block related?

Yes, the money supply in Bitcoin network is diminishing. The diminishing rate is halving every 210000 blocks (or approximately every 4 years). Initially 50 bitcoins were given to the miner who generated the block.

### What is the maximum number of Bitcoins available in the network after all the Bitcoins have been mined? When will all the Bitcoins be mined?

The maximum number of bitcoins in the network will be 21 000 000. All the bitcoins will have been mined by the year 2140.

### What is a decentralized consensus? What is a usual setup to clear transactions? What does a clearinghouse do?

A decentralized consensus is a procedure when several participants in the network decide about what is true and what is not of the network state. It is not a usual setup to clear transactions. Usually a clearinghouse (a centralized authority) does the clearing.

### What is deflationary money? Are they good or bad usually? What is the bad example of deflationary spiral?

Deflationary money is money that appreciate with time. So it means good and services become cheaper. However, sometimes that is a problem, since people stop consuming and thus the economy becomes less stable because of the lower consumption. A bad example of a deflation spiral is Japan in the 90s.

### What is an emergent consensus? What is the feature of emergent consensus? How does it differ from a usual consensus? What are the main processes out of which this emergent decentralized consensus becomes true?

An emergent consensus is not a final consensus. It is rather a consensus that happens repeatedly in the network. This is a consensus about which transactions are considered to be correct and which are incorrect. A usual consensus is a onetime consensus. The main processes underlying the emergent decentralized consensus are transaction verification and block verification.

### Could you please describe the process of Independent Transaction Verification? What is the list of criteria that are checked against a newly received transaction? Where can these rules be checked? Can they be changed over time? If yes, why would they be changed?

Independent Transaction Verification is a process that happens on each node that receives some transaction. There are many criteria used to check the transaction. For example, whether locking and unlocking scripts match.

The rules that each transaction is being checked against could be seen in the source code of the Bitcoin Core client. These rules can be changed over time because the Bitcoin ecosystem evolves and new checks are introduced or some old checks are removed.

### Does mining node have to be a full node? If not, what are the other options for a node that is not full to be a mining node?

A mining node does not have to be a full node. A mining node could be part of a mining pool, connected to the node that has all the information.

### What is a candidate block? What types of nodes in the Bitcoin network create candidate blocks? What is a memory pool? Is there any other name of the memory pool? What are the transactions kept in this memory pool?

A candidate block is a block that is not part of the blockchain yet. A candidate block is created by a miner, by putting transactions into the block, creating a block header. Some parameters, such as nonce are iterated through to create the solution to the PoW algorithm. A memory pool are transactions that have been checked as correct, but which have not been mined yet. The other name of the memory pool is transaction pool. The transactions kept there are the transactions that have the proper parents in the blockchain or in the memory pool.

### How are transactions added to the candidate block? How does a candidate block become a valid block?

The first transaction is always a Coinbase transaction. This transaction creates coins and allocates them to the miner. The other transactions are prioritized list of transactions. A candidate block becomes a valid block when a solution to the PoW algorithm is found (a correct nonce that corresponds to the right difficulty target.

### What is the minimum value in the Bitcoin network? What is it called and what is the value? Are there any alternative names?

The minimum value in the Bitcoin network is 1/100000000 (one in one hundred million). It is called satoshi.

### What is the age of the UTXO?

The age of the UTXO is the number of blocks that have elapsed since the UTXO has been recordered in the blockchain.

### How is the priority of a transaction is calculated? What is the exact formula? What are the units of each contributing member? When is a transaction considered to be old? Can low priority transactions carry a zero fee? Will they be processed in this case?

The priority has the formula: SUM (Value of Input\*Input Age)/Transaction size. Value of input is in satoshis, age is in number of blocks and size is in bytes. The transaction is considered to be old when it is at least one day old. Yes, low priority transactions can carry a fee of zero. And they will be processed since the UTXO will age and it will increate the priority of the transaction.

### How much size in each block is reserved for high priority transactions? How are transactions prioritized for the remaining space?

50 kbytes of space is reserved for high priority transactions. High priority transactions are transactions for which the calculated priority is greater than 57600000. The other transactions are prioritized according to their fee per byte of transaction.

### Do transactions expire in Bitcoin? Can transactions disappear in the Bitcoin network? If yes, could you please describe such scenario?

Transactions do not expire in Bitcoin. They can disappear for example when all the miners that had this transaction in the memory pool are rebooted. Since memory pool is kept in memory after a reboot it is cleared.

### What is a generation transaction? Does it have another name? If it does, what is the other name of the transaction? What is the position of the generation transaction in the block? Does it have an input? Is the input usual UTXO? If not – what is the input called? How many outputs there are for the generation transaction?

A generation transaction is a transaction that creates bitcoins and allocates them to the miner. Another name of this transaction is a Coinbase transaction. The position of the transaction is the first in the block. It has an input (one input) but it is not a usual input (reference to the previous transaction) and it does not have unlocking script. The input is called “Coinbase input”. There is only one output.

### What is the Coinbase data? What is it currently used for?

Coinbase data is a field in the generation transaction that is of 2-100 bytes in size. Initially they were arbitrary and could be used for anything. Now, since the version-2 blocks they are used for block height, for pool membership information, for extra nonce and during the time of voting for P2SH format, this coinbase data contained the vote.

### What is little-endian and big-endian formats? Could you please give an example of both?

These are the two commonly used standards for encoding numbers. Little endian format is when the least significant digits are put in front. Big endian format is when the most significant digits are put in front.

### How is the block header constructed? Which fields are calculated and added to the block header? Could you please describe the steps for calculation of the block header fields?

First of all the transactions are chosen that will be part of the block. Then their hashes and Merkle tree root hash is calculated. Then the previous block hash is added, then the other parameters are added: nonce, difficulty target and timestamp. In addition, a version number is added. This version number describes the version of the block structure.

### What is a mantissa-exponent encoding? How is this encoding used in the Bitcoin network? What is the difficulty target? What is the actual process of mining? What kind of mathematical calculation is executed to conduct mining?

Mantissa-exponent encoding is an encoding used to code the difficulty target. It is a 4 bytes field, one byte is the exponent and three bytes are mantissa (or coefficient). A difficulty target is a number that indicates what range of hashes are acceptable as results of PoW algorithm. The actual process of mining is to go via different values of nonces to find a hash that will be lower than the difficulty target. The mathematical operation is calculation of hash value of a block header.

### Which hash function is used in the Bitcoin mining process?

It is SHA256.

### Could you describe the PoW algorithm? What features of the hash function does it depend on? What is the other name of the hash function? What is a nonce? How can we increase the difficulty of the PoW calculation? What do we need to change and how do we need to change this parameter?

PoW algorithm is an algorithm of finding the input that produces an output of a specific value, lower than the difficulty target. It depends on two features of the hash function: one is producing an output of a specific size and another is that it is almost impossible to find two different inputs that produce the same output. Another name is digest. Nonce is a variable that can be changed to produce different output. To increase the difficulty of the PoW calculation we can reduce the target, so that the requirement is to find a hash that is lower than the target. The lower the target, the more difficult it is to find the hash.

### What is difficulty bits notation? Could you please describe in details how it works? What is the formula for the difficulty notation?

Difficulty bits is a notation of coefficient and exponent. The formula is target = coefficient \* 2 ^ (8\*(exponent – 3)). Once the target is calculated the PoW algorithm needs to find the hash that is lower than the target.

### Why is difficulty adjustable? Who adjusts it and how exactly? Where is the adjustment made? On which node? How many blocks are taken into consideration to predict the next block issuance rate? What is the change limitation? Does the target difficulty depend on the number of transactions?

The difficulty is adjustable and it depends on the overall capacity of the network. How many hashes the network can calculate at any given moment of time. Each miner in the network adjusts it. 2016 blocks are taken into consideration to predict the next block issuance rate. The rate of change should not be more than 4. The target difficulty is independent on the number of transactions.

### How is a new block propagated in the network? What kind of verification does each node do? What is the list of criteria for the new block? What kind of process ensures that the miners do not cheat?

A block is sent to everyone in the network. Each node that receives the block verifies it. There are a number of criteria used for block verification, for example:

* The block structure must be valid.
* The block header hash must be less than the target difficulty.
* The block size is of correct limits.

Since each block does independent verification, this ensures that the miners do not cheat.

### How does a process of block assembly work? What are the sets of blocks each full node have? Could you please describe these sets of blocks?

A process of block assembly works at every node. Once a new block is received the hash of the previous block is analyzed (the hash is given in the header). If the hash is the hash of the top block in the primary blockchain, then this new block is added on top of the primary blockchain. If it is the hash of a parent, then there is an alternative blockchain created (secondary blockchain). If the hash does not belong to any block in the primary or secondary blockchain then the block is put into an orphan pool.

### What is a secondary chain? What does each node do to check this chain and perhaps to promote it to the primary chain? Could you please describe an example when a fork occurs and what happens?

A secondary chain is a chain of the same length as the primary chain, it forks at the parent. Each node checks cumulative difficulty of the blockchain and promotes the one with the most proof of work (the longest). A fork occurs when two blocks are generated at about the same time. Then the network waits for the next block and accepts the longest chain as the correct chain.

### How quickly forks are resolved most of the time? Within how many new block periods?

Usually block forks are resolved in less than 20 minutes. It is possible to have two blocks generated at about the same time, but the probability of such event happening for two consecutive times is very low. So, the problem gets resolved within one new block period (since the initial fork was created).

### Why the next block is generated within 10 minutes from the previous? What is this compromise about? What do designers of the Bitcoin network thought about when implementing this rule?

It is generated within 10 minutes to balance the confirmation time of a transaction and probability of creating a new fork. If the designers decided to use shorted timeframe then the confirmation time will be faster, but the probability of forks increase.

### What is a hashing race? How did Bitcoin hashing capacity has changed within years from inception? What kind of hardware devices were initially used and how did the HW utilization evolved? What kind of hardware is used now to do mining? How has the network difficulty improved?

A hashing race is a situation when the network hashing capacity and end user hashing capacity increase significantly within time. Initially the block confirmation could be run on end PCs and laptops, then GPU processors were used, then ASICs and now there are special mining rigs.

### What is the size of the field that stores nonce in the block header? What is the limitation and problem of the nonce? Why was an extra nonce created? Was there any intermediate solution? If yes, what was the solution? What are the limitations of the solution?

The size of the field that stores nonce is 4 bytes. This will allow for 4 billion different hashes. The limitation is that sometimes miners go through all the values of the nonce and still do not find the solution to the PoW algorithm. Besides the speeds of the current miners are much more than 4Ghash/sec, which means that all the space of nonce is exhausted in just 1 second. The previous solution was to change slightly the timestamp, but in order for the block to be valid the time could not be that much different from the current time. The solution was to get some space from the Coinbase Data field that could be from 2 to 100 bytes. Extra 8 bytes are extracted from the Coinbase Data and allocated to the nonce.

### What is the exact solution for the extra nonce? Where does the new space come from? How much space is currently used and what is the range of the extra nonce now?

The extra nonce comes out of Coinbase Data field. This field is used in the first transaction of each block. Since the first transaction does not use any unlocking script, it has 2-100 bytes of data available for the different applications. 8 bytes of this data is used for extra nonce. So, overall the size of the nonce is 12 bytes, or 96 bits.

### What is a mining pool? Why was it created? How are normally such pools operated? Do they pay regularly to the pool participants? Where are newly created Bitcoins distributed? To which address? How do mining pools make money? How do the mining pools calculate the participation? How are shares earned calculated?

A mining pool is a set of mining servers or rigs combined together to compete in the block PoW algorithm. It was created because single miners, however powerful, stand only very little chance of finding the hash that corresponds to the difficulty target. Such mining pools pay regularly to the participants, depending on the capacity they add to the pool. If the pool is successful in generating new bitcoins, these bitcoins are given to the pool address. Then the pool distributes this money to the pool participants. They have their own margin for the pool management. The pool gives the lower difficulty target to the participants and counts how many each participant submitted results. The shares are calculated based on the submissions.

### What is a managed pool? How is the owner of the pool called? Do pool members need to run full nodes? Explain why or why not?

Managed pool is a pool that is managed by an individual or a company. The owner of the pool is called “pool operator”. Usually the pool server is connected to some of the full nodes and has access to the full blockchain. The pool members do not need to run their own full nodes.

### What are the most famous protocols used to coordinate pool activities? What is a block template? How is it used?

Stratum is one of such protocols. Another is Get Block Template (GBT). Since many miners do not keep the full blockchain, the pool server does the blockchain collection and thus it prepares the list of transactions to be mined in the next block. It puts all the necessary data to the block header (transactions, Merkle root path, etc) and sends the templates to the pool participants. They use this block templates and iterate through the nonce range to come with the solution.

### What is the limitation of a centralized pool? Is there any alternative? If yes, what is it? How is it called? How does it work?

The limitation of the centralized pool is that the pool management can steal the bitcoins newly generated and use pool for some other purposes, such as consensus attacks. There is an alternative, called P2Pool, this is a P2P pool that is built on the alternative blockchain. The participating nodes calculate the hashes and put the hashes that solve the necessary difficulty target into the supporting blockchain.

### What is a consensus attack? What is the main assumption of the Bitcoin network? What can be the targets of the consensus attacks? What can these attacks do and what they cannot do? How much overall capacity of the network do you have to control to exercise a consensus attack?

A consensus attack is when several participants agree to attack the network and produce blocks which confirm transactions that are not fully correct. The main assumption is that most of the participants in the Bitcoin network are honest. These attacks cannot steal bitcoins of other people since they still do not have the access to the private keys of these people. However, they can double spend money for example or they can do DoS attacks against some specific addresses and transactions. Usually people call these attacks “51% attacks”, but they can be executed with much lower network control and capacity.

## Chapter 9: Alternative Chains, Currencies and Applications.

### What is the name of alternative coins? Are they built on top of the Bitcoin network? What are examples of them? Is there any alternative approach? Could you please describe some alternatives?

The name of the alternative coins are altcoins or colored coins. They use the Bitcoin infrastructure and are built on top of the Bitcoin network. An alternative approach is to use the code of the Bitcoin client and change it to create another ecosystem. This approach creates altchains. Examples are Litecoin, Dogecoin, Namecoin, etc.

### Are there any alternatives to the PoW algorithm? If yes – what are the alternatives? Could you please name two or three?

Yes, there are several other algorithms, for example PoS – Proof of Stake for example. It is quite popular. Some ecosystems that use hybrid approach exist. PoW is a PoS, but not the other way around. There are also other algorithms such as Proof of Publishing.

### What is the operation of the Script language that is used to store a metadata in Bitcoin blockchain?

OP\_RETURN.

### What is a coloured coin? Could you please explain how it is created and how it works? Do you need any special SW to manage coloured coins?

A coloured coin is a bitcoin with a specific attached data to the transaction. There is actually no colour attached to the coin. A coloured coin usually is worth more than the amount of bitcoins attached to the transaction. Yes, you need special SW to handle such coloured coins. This SW not only handles usual Bitcoin transactions, but also handles this special data and information.

### What is the difference between alt coins and alt chains? What is a Litecoin? What are the major differences between the Bitcoin and Litecoin? Why so many alt coins have been created? What are they usually based on?

Alt coins are built on top of the Bitcoin infrastructure. Therefore, they use the same blockchain as the Bitcoin. Altchains use their own blockchain and their own codebase. Litecoin uses a different PoW algorithm that is not so easily transferrable to ASIC. Litecoin has larger amount of coins, 84 million coins at maximum and a new block is generated every 2.5 minutes. As of 2014 there are 500 coins. Most of them are based on the Bitcoin code with not so many changes.

### What is Scrypt? Where is it used and how is it different from the original algorithm from which it has been created?

Scrypt is an algorithm that has been created from the PoW and from a password stretching algorithm that has been used to withstand brute force attacks. Scrypt is resistant to GPU and ASIC mining.

### What is a demurrage currency? Could you please give an example of one blockchain and crypto currency that is demurrage?

A demurrage currency is a currency that is designed to have negative store rates. It is done to encourage spending and not hoarding large amounts of it. An example of demurrage money is Freicoin.

### What is a good example of an alternative algorithm to PoW? What is it called and how is it different from the PoW? Why the alternatives to Bitcoin PoW have been created? What is the main reason for this? What is dual-purpose PoW algorithms? Why have they been created?

A good example of an alternative algorithm to PoW is PoS: Proof of Stake. The idea is that the owners of large stakes in a specific altchain are interested in keeping that chain honest so that they can enjoy their assets. If they start cheating, the public will abandon the altchain and the owners will lose the assets. The alternatives to the PoW have been created since PoW consumes too much electricity. Dual purpose PoW are the PoW which are doing some useful calculations, for example decoding some DNA, calculating prime numbers, or other.

### Is Bitcoin “anonymous” currency? Is it difficult to trace transactions and understand someone’s spending habits?

Bitcoin is pseudonymous currency. It is not difficult to trace transactions and get the spending habits of people.

### What is Ethereum? What kind of currency does it use? What is the difference from Bitcoin?

Ethereum is another blockchain and ecosystem. It has been created to help resolve the issues and problems present in the Bitcoin ecosystem. The currency in Ethereum is ether. Ethereum offers wide options for creating smart contracts in the blockchain. It is more focused on smart contract rather than on currency.

## Chapter 10: Bitcoin security.

### What is the main approach of Bitcoin security?

The main approach of the Bitcoin security is that the security of the ecosystem must be based in the ecosystem itself, rather than in the end nodes. In this case, the security will be the strongest.

### What are two common mistakes made by newcomers to the world of Bitcoin?

Two common mistakes are to store the keys from several users in one centralized wallet or storage. If such a server is compromised then all the bitcoins are lost (there are many examples of that for example, cryptocurrency exchanges). A second common mistake is to take some transactions offline from blockchain to save some charges.

### What is a root of trust in traditional security settings? What is a root of trust in Bitcoin network? How should you assess security of your system?

The root of trust in a traditional security setting is a central security core upon which all the rest of security in the system is built on. In Bitcoin, the root of trust is the genesis block and following blockchain.

### What is a cold storage and paper wallet?

A cold storage is a storage of the private keys outside of a PC. For example, on a piece of paper (or several papers saved in different places). A paper wallet is a wallet where the keys are saved in a text form. It could be the keys or it could be the mnemonic words that help recovering the seed private key.

### What is a hardware wallet? How is it better than storing private keys on your computer or your smart phone?

A hardware wallet is a special type of hardware that was created with the sole purpose of storing the private keys of Bitcoin or altcoin systems. They are much more secure and while hackers can access a PC and steal the keys, it is much more difficult for hardware wallets. Because of this reason and because of the specialization of the hardware wallets they are better than storing the keys on your PC or smart phone.