Blockchain matters

Why does blockchain matter?

Balázs Héder, Ph.D.

December 2021

PART 2

Have you ever heard these phrases?

Blockchain matters

Blockchain is going to change the World!

Bitcoin bubble has been popped!

Bitcoin is a bubble!

Bitcoin is the money of criminals!

Bitcoin bubble is going to be popped!

Bitcoin is dead! Bitcoin Obituaries, url

Blockchain is immutable!

Bitcoin is the blockchain!

Blockchain is not Bitcoin!

Blockchain contains the truth!

Smart contracts are running on the blockchain.

Cryptocurrencies are useless, but blockchain is good!

Blockchain is secure!

Have you ever heard these phrases?

Blockchain matters

Blockchain is going to change the World!

Bitcoin bubble has been popped!

Bitcoin is a bubble!

Bitcoin is the money of criminals!

Bitcoin bubble is going to be popped!

Bitcoin is the blockchain!

Blockchain is immutable!

Blockchain contains the truth!

Smart contracts are running on the blockchain.

Cryptocurrencies are useless, but blockchain is good!

Blockchain is secure!

Confusing, isn't it? To get better understanding and to be able to decide which statement is true, follow this presentation series!

Outline of the whole series

Blockchain matters

- Little steps to the beginning
- The born of the technology
- Bitcoin, why is it so important?
- OK, so what is blockchain? And what is DLT?
- Consensus mechanisms
- Oracles
- Ethereum, the world computer
- Smart contracts
- Tokens and the digitization of physical objects, NFTs, SFTs
- The tsunami of cryptocurrencies
- ICO, IEO, STO, CeFi/DeFi, DID and other buzzwords
- The enterprise answer: consortium/private blockchain solutions
- When can/should I use blockchain? - The blockchain solution feasibility chart
- Possible use cases

Notation of references

Blockchain matters

References related to a slide are listed at the bottom of the slide, or right next to the text.

Visual Capitalist, G. Bhutada, “Purchasing Power of the U.S. Dollar Over Time”, 2021, url.

EOS, url

Solana, url

CertiK, “The Blockchain Trilemma: Decentralized, Scalable, and Secure?”, 2019, url

Blockchain matters

Part 2 - Bitcoin

What is Bitcoin?

Blockchain matters

- Open source software developed by Satoshi Nakamoto (unkown person or group of people) in 2008.
- P2P electronic cash system
  - Bitcoin (with capital): the software, the network
  - bitcoin: the currency, abbreviation is BTC or XBT, can be divided into 100 million parts, smallest unit is 1 satoshi (sat).
- Without middleman
- Decentralized, no central control, censorship, authorities, governments, etc. The software is open source, so the code is available to everyone to check, copy, or modify.
- Not a new invention, all of the technology pillars (P2P, PoW, blockchain, DLT, decentralization) were existed before.
- Public, anyone can join to the network
- Secure, never compromised, cost of 51% attack (for 1 hour) is more than 2M USD!
- Pseudonym
- Limited supply, programmed deflation policy.

S. Nakamoto, „Bitcoin: A peer-to-peer electronic cash system”, 2008, url

PoW 51% Attack Cost, url

The middleman problem

Blockchain matters

- In traditional (centralized) money system middlemen are necessary to avoid double spending.
- How to solve the problem in decentralized public systems with X million actors?
  - In a decentralized environment the source of the double spending is mainly the byzantine attack.
  - What to do against dishonest participants?
  - Who should write into the ledger, i.e. who creates the next block?
  - The one who writes the ledger should write the truth.
- Bitcoin's solution:
  - 10 minutes drawing with proof of work (mining)
  - Incentive rewards → The most profitable way is to be honest!
  - One true chain (the longest one)
    - Cost of 51% attack is huge.
    - It can be easily decided which version of the blockchain is valid.

N. Evans, Y. Pritzker, "Inventing Bitcoin", url

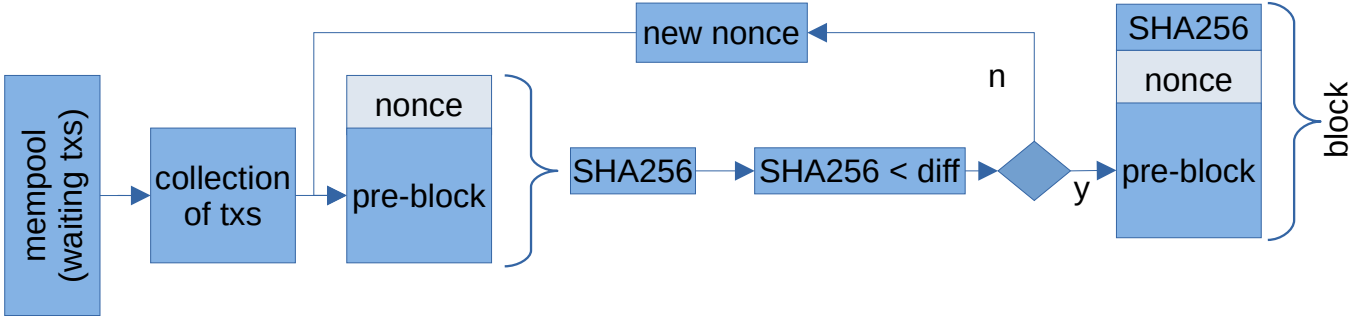
The proof of work and the mining

Blockchain matters

- The lottery
  - Every participant must be able to create his own lottery ticket for real money!
  - The fact that a ticket has won must be easily verified by the other participants.
- Bitcoin's solution
  - Cryptographic hash functions
  - Computation costs electric power
  - SHA256 (secure hash algorithm): output has length of 256 bit
- Mining (the nodes which are doing the mining process are called miners):
  - The pending transactions are waiting in the mempool. The mempool is synchronized by every miners.
  - The miner selects transactions from the mempool for the next block. The transactions with the highest transaction fee will be selected for the next block.
  - The miner chooses a random number (called nonce), write it into the block header and created the block. If its hash is smaller than the network difficulty, the miner wins and the block is broadcasted to the network.
  - Determining the correct nonce is time/energy consuming, but validating the nonce is easy and fast.

Hash function properties
1. deterministic
2. fixed output size
3. very fast computable
4. one-way function
5. unique output
6. avalanche effect

N. Evans, Y. Pritzker, "Inventing Bitcoin", url



Incentives

Blockchain matters

- The successfully generated new block is broadcasted to the network.
- If participants accepts the new block they add it to the ledger. The miner gets his incentive, because the first tx in the block is the so called coinbase transaction, which sends the incentive to the miner.
- The mining process starts again.
- The incentive
  - Block reward. Halving: the block reward is halved after each 210000th block (~4 years), in the beginning it was 50 BTC, currently (since 11th of May 2021) it is 6.25 BTC. The block reward will be zero around 2140 when all bitcoins will have been mined. (The hardcap is 21 Million BTC) -> Deflation policy
  - All the transaction fees of the transactions which are included in the block. (The transactions with highest fees are mined first.)

N. Evans, Y. Pritzker, “Inventing Bitcoin”, url

Hash rate

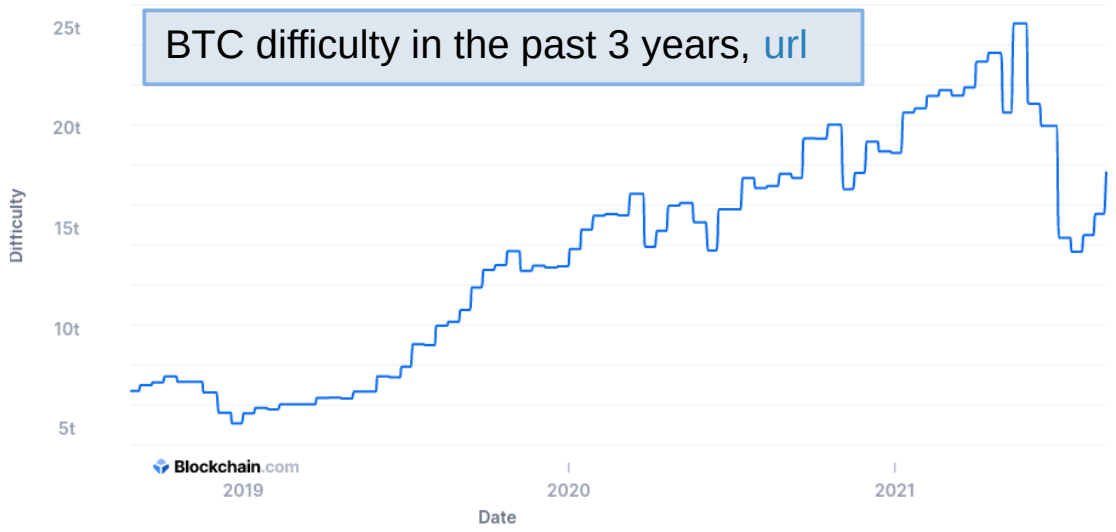
Blockchain matters

- Hash rate means how many hashes (with different nonces) a miner can calculate per second.
- The network hash rate is the total hash rate of the miners. As more and more miners join the network the network hash rate increases. To ensure the 10 minutes block time, the network difficulty also increases so finally faster and faster mining hardware is required to be able to generate new blocks.
- A whole industry was born where the goal is to build minder hardware with more and more hash rate and less and less kWh/hash.
- Mining eras and some typical hash rate values
  - CPU (2009 - 2010)
    - Intel P3 Coppermine: 0.39 Mhash/s
    - Athlon 64 3500+ : 1.18 Mhash/s
    - Intel Core 2 Duo E6850: 6.75 Mhash/s
  - GPU (2010 - 2011)
    - Geforce GTX590: 193.1 Mhash/s
  - FPGA (2011 - 2013)
    - Bitforce SHA256 Single: 832 Mhash/s
  - ASIC – Application Specific Intergrated Circuit (2013 -)
    - Antminer S1: 180,000 Mhash/s (0.18 Thash/s)
    - Antminer S9: 14 Thash/s

The network difficulty

Blockchain matters

- Difficulty changes after every 2016 blocks (~2 weeks) in order that the block time is approximately 10 minutes.
- In the beginning solo CPUs were efficient enough, but currently special ASIC (Application Specific Integrated Circuits) must be used!
- The ROI (return of investment) is approx. 1-1.5 year in case of the most modern ASIC devices.
- Mining farms
- In August 2021 the average price of mining a block is 15k-20k USD (electricity + hardware)

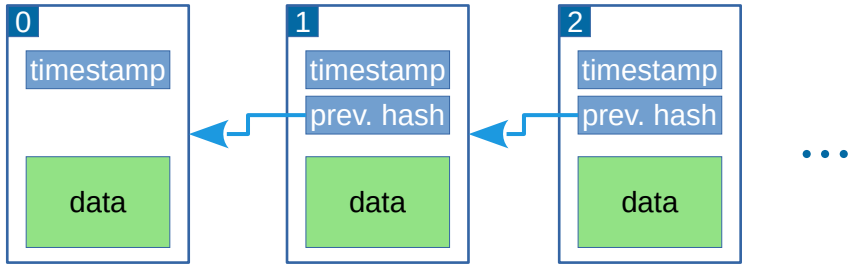


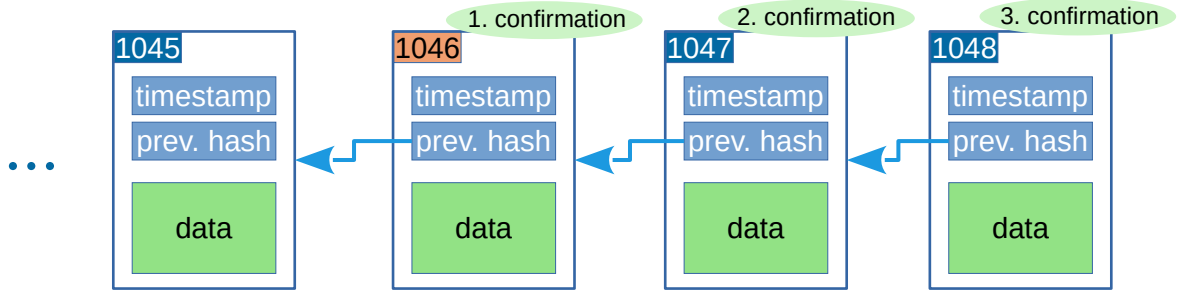


The chain of blocks, confirmations

Blockchain matters

- Blocks are arranged in a chain (the blockchain) using the sha256 hash function.
- Each block (except the genesis block) includes the hash of the previous block.
- When a block is confirmed by a node and appended to the blockchain, it has the first confirmation.
- Every additional appended block increases the number of confirmation of a given block.





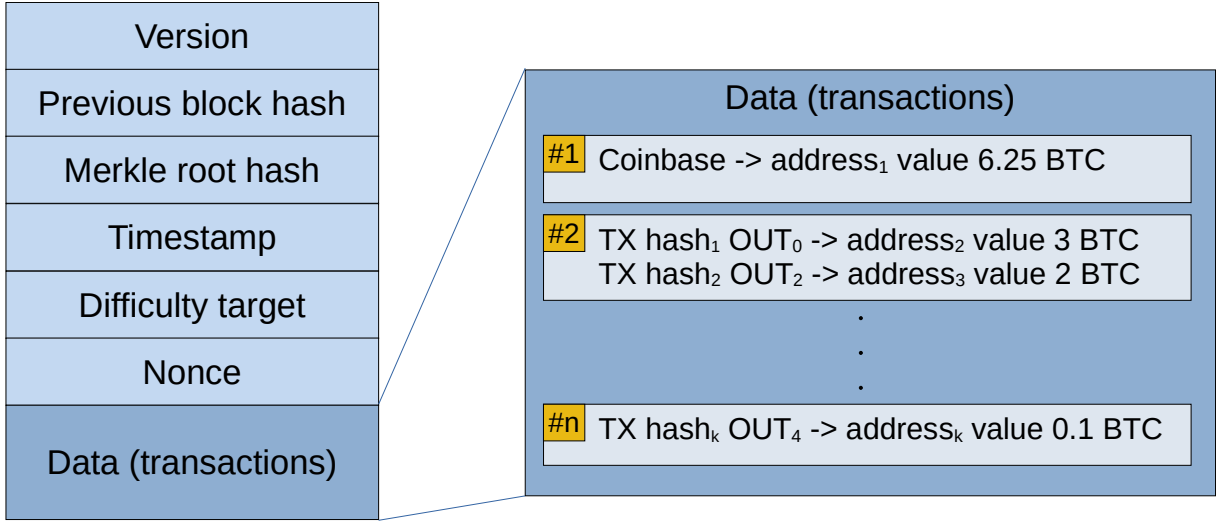
A. M. Antonopoulos „Mastering Bitcoin”, 2017, url

Content of a block

Blockchain matters

- Block size is 1 MB, Block header is 80 bytes
- Block hash = SHA256(SHA256(block header))
- Average block contains ~4000 txs each of which is 250 bytes in average (this means 7 transactions / second throughput)

Double hashing is against birthday attack (hash collisions).

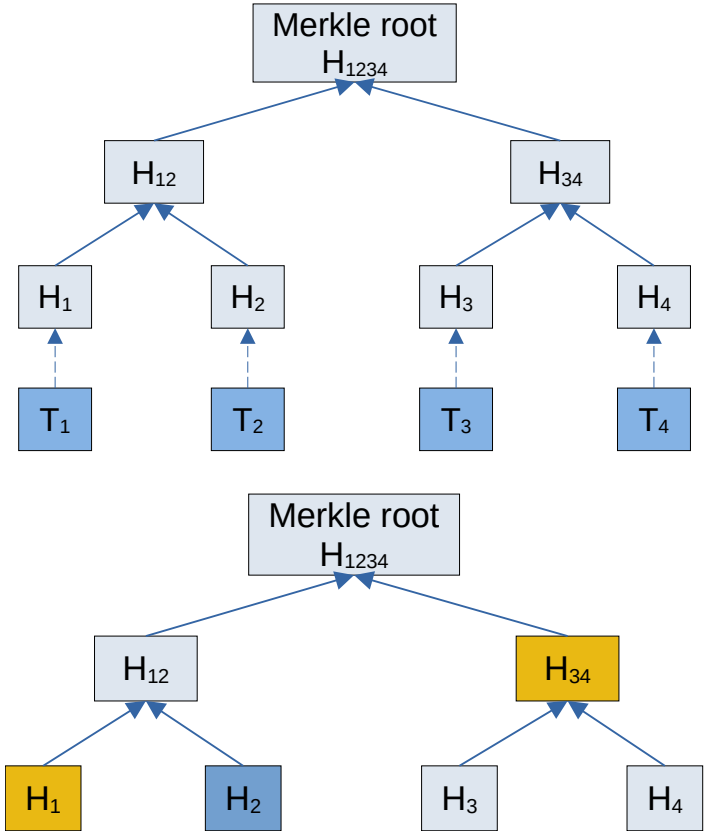


A. M. Antonopoulos „Mastering Bitcoin”, 2017, url

Merkle root

Blockchain matters

- Each block contains the summary of all the transactions in the block using a Merkle tree (binary hash tree).
- H_1 = SHA256(SHA256(T_1))
- H_{12} = SHA256(SHA256(H_1+H_2)), “+” means concatenation
- Merkle path: anyone can decide if a specific transaction is included in the block by checking the Merkle root in the block header (SPV wallet)
  - path length is $\log_2(N)$, where N is the number of txs.
- Example: prove that T_2 is in the block
  - the provided Merkle path: H_1,H_{34}
  - Anyone can compute H_{12} and then H_{1234} (Merkle root) and compare the value in the block header.

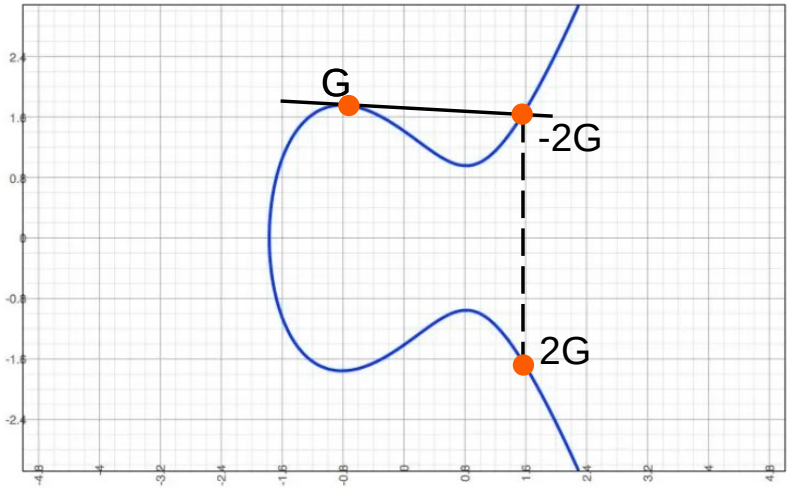


A. M. Antonopoulos „Mastering Bitcoin”, 2017, url

Bitcoin addresses

Blockchain matters

- Private key: random number between 1 and ($1.158 \cdot 10^{77}$-1) (slightly less than 2^{256})
  - You can send your BTC using your private key: the transactions must be signed with your private key.
  - Who owns your private key, owns your bitcoins! Keep your private key in a super safe place!!
- Public key = secp256k1(private key)
  - ECDSA: Elliptic Curve Digital Signature Algorithm (secp256k1)
  - K = k*G, where G is generator point (fix), k is the private key, K is the public key
- Address = Base58Check(SHA256(RIPEMD160(public key)))
  - Base58Check: easily recognizable, human readable characters
  - Example: 3FZbgi29cpjq2GjdwV8eyHuJJnkLtktZc5





secp256k1

SHA256, RIPEMD160
Base58Check

A. M. Antonopoulos „Mastering Bitcoin”, 2017, url

How to store bitcoin?

Blockchain matters

- (Self-hosted) wallet
  - You own the private key, but if you loose it, you loose all of your money
  - High degree of personal responsibility
- Third party service (Custodial platform: Inlock, BlockFi, PayPal, or exchanges: Binance, FTX, Coinbase)
  - You don’t have to take care of your private keys. A company owns them, but be careful: “Not your keys, not your coin!”
  - The assets should be adequately insured on the platform

Inlock: Unlock Your Crypto’s Potential, url

BlockFi, url

Bitcoin wallets

Blockchain matters

- Wallet is a software which automatically does
  - Address and key management (There are as many addresses (private key – public key pair) as necessary in the same wallet)
  - Communicate with the blockchain, create and sign transactions
- Hierarchical Deterministic (HD) wallet
  - Every key pair can be generated from a seed phrase (e.g. 24 words)
  - Your seed phrase must be stored in a safe place!
- Wallet types based on the storage of the keys
  - Web wallet
  - Software wallet
    - Desktop (e.g. Bitcoin Core, Electrum, Exodus, Coin)
    - Mobile (e.g. Coinomi, Electrum)
  - Hardware wallet (e.g. Ledger, Trezor). Always get your item from official source!
  - Paper wallet / wallet engraved on a piece of metal, etc.
- Wallet types based on Internet availability
  - Hot wallet (24/7 online) – least secure
  - Cold wallet (offline)
- Wallet types based on transaction verification
  - Full (node) wallet (e.g. bitcoind)
  - SPV (Simplified Payment Verification) wallet (e.g. Electrum)

Most secure Bitcoin storage solutions:

1. Memorize seed phrase
2. Engrave seed phrase in a peace of metal (fireproof)

In both cases you can use a hardware wallet (to send BTC).



Ledger Nano X, url

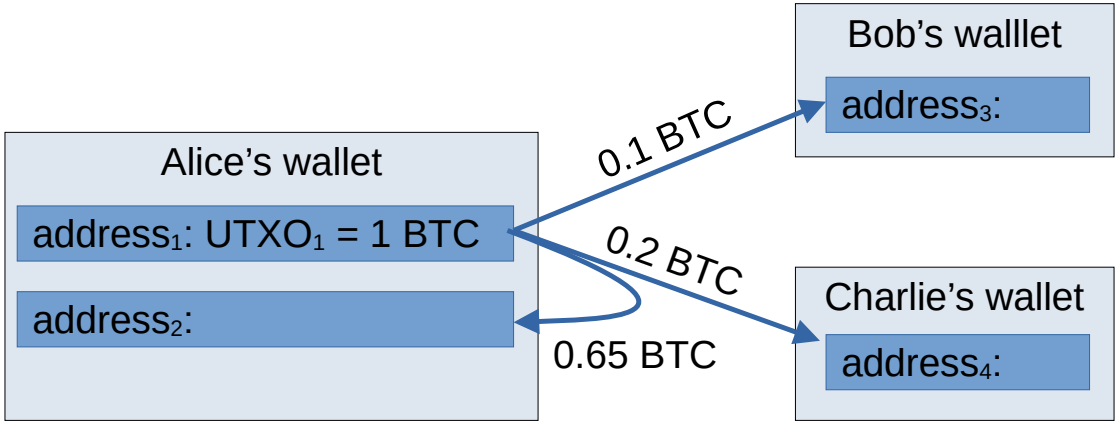


Cryptosteel, url

Bitcoin transactions

Blockchain matters

- Transaction consists of
  - Inputs (single or multiple)
  - Outputs (single or multiple)
- Outputs are the Unspent Transaction Outputs (UTXO).
- Inputs are the UTXOs of previous transactions.
- Balance of an address is the sum of UTXOs
- UTXO database
- TX fee is the sum of inputs minus the sum of outputs (chargeback outputs are usual).
- Transaction is signed by the private key: everyone can check based on the public key and the signature that the sender was entitled to spend the money. (The signature is also called witness.)
- When transaction is sent by the wallet it is included in the mempool which is being synchronized by all the peers.
- Transaction hash: SHA256(SHA256(transaction))



TX fee = sum(inputs)-sum(outputs) = 0.05 BTC

A. M. Antonopoulos „Mastering Bitcoin", 2017, url

Bitcoin explorers

Blockchain matters

- “A blockchain explorer is a piece of software that uses API and blockchain node to draw various data from a blockchain and then uses a database to arrange the searched data and to present the data to the user in a searchable format.”
- Practically, they are public web pages where blocks, transactions and addresses can be checked.
- blockchain.com, blockchair.com, etc.

Blockchain Explorer Tutorial – What Is A Blockchain Explorer, 2021, url

Blocks

Height	Hash	Mined	Miner	Size
698541	0..528a6bf89c920958b090b1def4cf4c481e4b0e57568a6	5 minutes	ViaBTC	1,318,288 bytes
698540	0..909d5e0ab7520e3670562940be0048e8e9a1d95b0bc24	8 minutes	Poolin	1,098,410 bytes
698539	0..e190615d64df794e907e5533c190a3dac013096892bc8	42 minutes	Unknown	1,489,015 bytes
698538	0..da26c44b002467aebc1206553d886508fa123921c266	58 minutes	Unknown	1,539,668 bytes

Transactions

Hash	0987dda228544ab534caca9ea748a66f0ce65a3ceb881d132a1fdfc...			2021-08-24 13:04
	1BcsJid3oVmBSVF4tdQJEEHfkcnFLj6fjv	0.00340200 BTC	1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX	0.00000684 BTC
			bc1qn8rsv3gw82ldyx2y7w5crf7mxkv6kt7eg3r...	0.00339000 BTC
Fee	0.00000516 BTC (2.314 sat/B - 0.578 sat/WU - 223 bytes)			+0.00000684 BTC
Hash	58c3367d784ef5e552cf917ea2cdf32ce0fee7522b601fdc93fd5266...			2021-08-11 21:37
	bc1qmyhkstfk5trd0eycpvu548wtsw70sj4rdnlx...	0.14064664 BTC	1PAiCX635zxNZNSkeKeqH6W85AZHBLWGAY	0.00008927 BTC
			35C9Ly4pBDBL6SVkyFtKbSwWbKYX16yHih	0.00003000 BTC
			1A8D3FGVHqdGYnUnRchZtah6HuepcYespQ	0.00001800 BTC
			bc1q5chpw8560qvkn6z4wnlgvqw5u85lcutvdsu...	0.00001217 BTC
			33cn2pd6DTf56XBiacChiCk5nyC5HU9w65	0.00001254 BTC

Blockchain.com, url

Participants in the Bitcoin network

Blockchain matters

- Node functionalities
  - Wallet
  - Miner
  - Full blockchain (block verification, tx verification)
  - Network routing
- Different types of participants
  - Full blockchain node with wallet and with miner (Bitcoin Core Reference Clients, solo miners)
  - Full blockchain node with wallet and without miner
  - Full blockchain node without wallet and without miner (only block and tx verification, network routing)
  - SPV (lightweight) nodes (wallets)
  - Mining pools (e.g. antpool.com), pool miners
  - Exchanges (e.g. Binance), custody services (e.g. Inlock)

A. M. Antonopoulos „Mastering Bitcoin”, 2017, url

Inlock: Unlock Your Crypto’s Potential, url

How can I participate?

Blockchain matters

- What is your goal?
- If you want to secure the network use bitcoind.
- If you want to mine you can use bitcoind and/or special mining software (e.g. cgminer)
- If you want to store BTC you should use Ledger Nano/Trezor + Cryptosteel
- If you want to trade use an exchange (FTX or Binance)
- If you want to have some interest use CeFI/DeFI platform (Inlock)

	Solo	Pool
CPU	bitcoind	cgminer
GPU	cgminer + bitcoind	cgminer
ASIC	cgminer + bitcoind	cgminer

Not profitable Can be profitable

The 51% attack

Blockchain matters

- To modify a block in the blockchain every following blocks must be re-generated.
- This must be done faster than the other miners generated new blocks. (Only the longest chain matters)
- The only thing to to this is owning 51% of hashing power.
- The cost of changing a transaction is increasing (the probability of changing a transaction is decreasing) with the number of confirmations. Currently the cost of 51% attack (for 1 hour) is more than 1.5M USD!
- Network participants (exchanges for example) are waiting 6 confirmations before accepting a Bitcoin transaction.
- Anyway, after a successful 51% attack the trust in Bitcoin network would be undermined, so BTC price would fall very quickly...
- But why to modify a block? For double spending. But wait… your new bitcoins would have a little value…
- In May 2019 somebody hacked Binance and stole 40 million USD in BTC (7000 BTC). A possible solution to makes this hack unhappened would have been that Binance would have co-operated with huge mining companies to get the required hash power and re-created the affected blocks. But finally Binance did nothing. This saved Bitcoin's credibility and of course BTC value.

PoW 51% Attack Cost, url

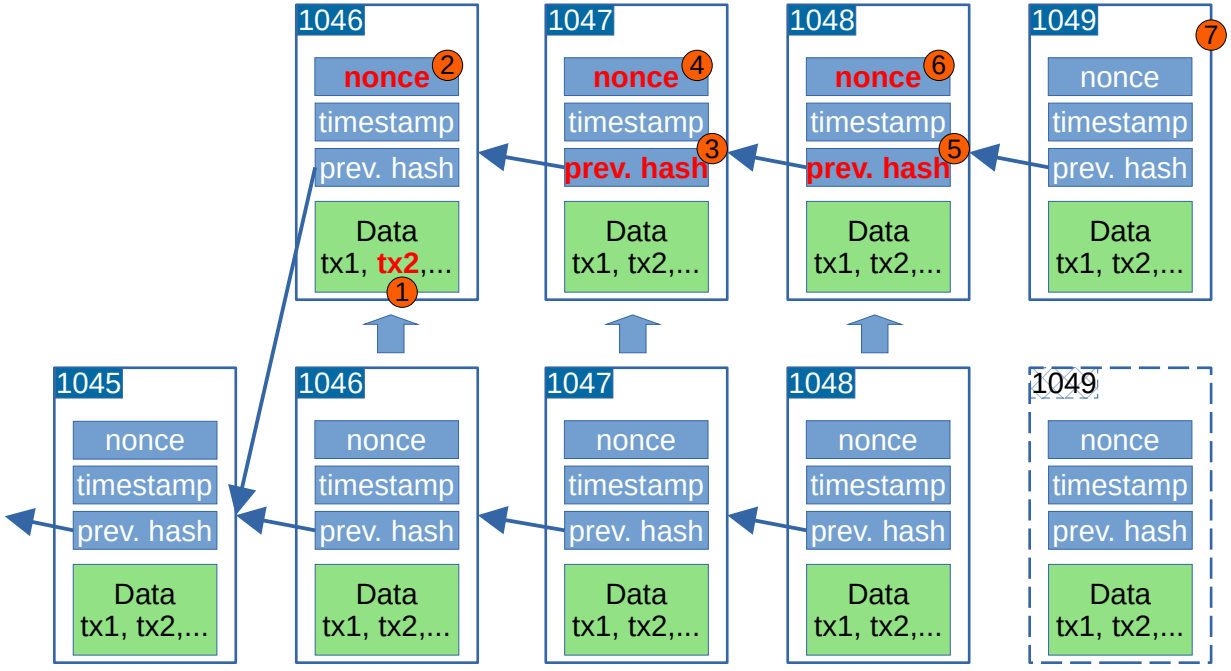
Z. Whittaker, C. Shue, "Binance says more than $40 million in bitcoin stolen in 'large scale", May 2019, url

The 51% attack

Blockchain matters

Example

- The attacker wants to modify tx2 in the block 1046, which already has 2 confirmations.
- The other miners are currently working on block 1049.
- The attacker must re-create blocks 1046, 1047 and 1048 and after that must create the new block 1049.
- The must do it earlier that the other miners finish block 1049.
- It the attacker succeeds his chain will be the longest, the only valid Bitcoin chain, the other miners must continue to work on block 1050 which is linked to the attackers block 1049.



The speed of a Bitcoin transaction

Blockchain matters

- A new block is created every 10 minutes (the block time is 10 minutes).
- The time until your transaction is included in a block highly depends on the transaction fee you are willing to pay.
  - If you paid high enough transaction fee, your transaction is included in the next block (in 0-10 minutes)
  - If you paid less, your transaction will be waiting in the mempool until one of the miners include it in a block.
- Anyway, your transaction in visible on the blockchain right after it is included in the mempool. Some of the merchants may already accept your payment at this stage especially in case of low value payments (coffee).
- Most of network participants (exchanges for example) are waiting 6 confirmations before accepting a Bitcoin transaction.
- This all means that a Bitcoin transaction can take at least 50-60 minutes (if the transaction fee is high enough so that the transaction is included in the next block).

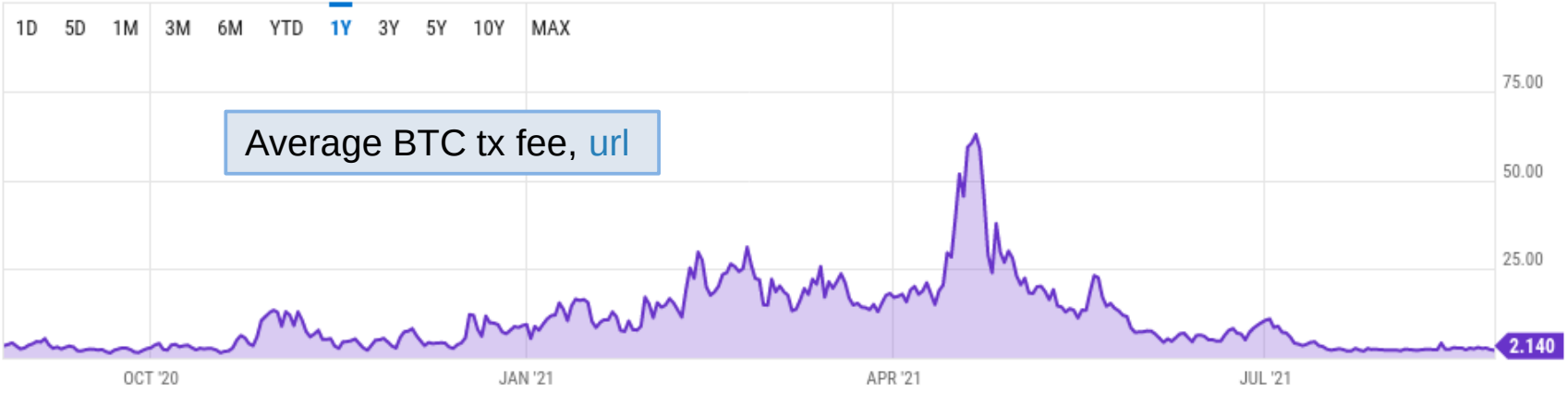
The cost of a Bitcoin transaction

Blockchain matters

- The time until the transaction is included in a block highly depends on the transaction fee and the current mempool size.
- If mempool is almost empty, a smaller transaction fee is enough so that the tx is included in the next block.
- Transaction fee is given in sat/byte.
- Currently (2021.11.15) 6.2 sat/byte fee is necessary to be included in the next block. This means approximately 0.7 USD!

Predicting Bitcoin fees for transactions, url

TX street, url



The forks

Blockchain matters

- Natural forks: different branches of the Bitcoin blockchain exist for a short time. Two or more miner successfully create new block, so there the network is in different states at different groups of peers. It is being resolved automatically.
- Hard forks: a part of the network starts operating under a different set of consensus rules than the rest of the network (for example larger block size). Blockchain splits into different branches.
  - Aug 2017: Bitcoin Cash (Roger Ver, Craig Steven Wright, 8 MB block size)
  - Nov 2017: Segwit2X (2 MB block size), cancelled
  - Other examples: Bitcoin Unlimited, Bitcoin Cash, Bitcoin SV (C.S.Wright, 128 MB block size), Bitcoin Gold, Bitcoin Green, etc.
- Soft forks: the cause is a software update. Compatible with older software versions. Both the updated and the unmodified clients can attend the consensus. No chain split.
  - Aug 2017: Segregated Witness (Segwit, separate unlocking script)
  - Script OP code updates

N. Evans, Y. Pritzker, “Inventing Bitcoin”, url

Bitcoin’s value proposition

Blockchain matters

- Scarce. The only truly finite resource in the Universe (except the other later developed crpyptos with hardcap), there will never be more than 21 million BTC. (Imagine what would happen to the exchange rate of gold if scientists suddenly were able to economically extract gold from extra terrestrial sources?
- But unlike gold, Bitcoin’s rate of increase will decrease forever, eventually reaching 0 once Bitcoin’s hard cap of 21 million bitcoin is reached.
- Primarily today Bitcoin is a store of value.
- Bitcoin may take over the role of gold (store of value, safe heaven)
- In some countries (e.g. Venezuela) international USD transfers are restricted. Bitcoin cannot be restricted.
- International money transfers, especially high amounts. (Try to transfer 1M USD to Kuala Lumpur. Will it be successful? If yes, with what amount of fees?
- One true chain… (with enough securing power)
- Never compromised.

Bitcoin S2F model

Blockchain matters

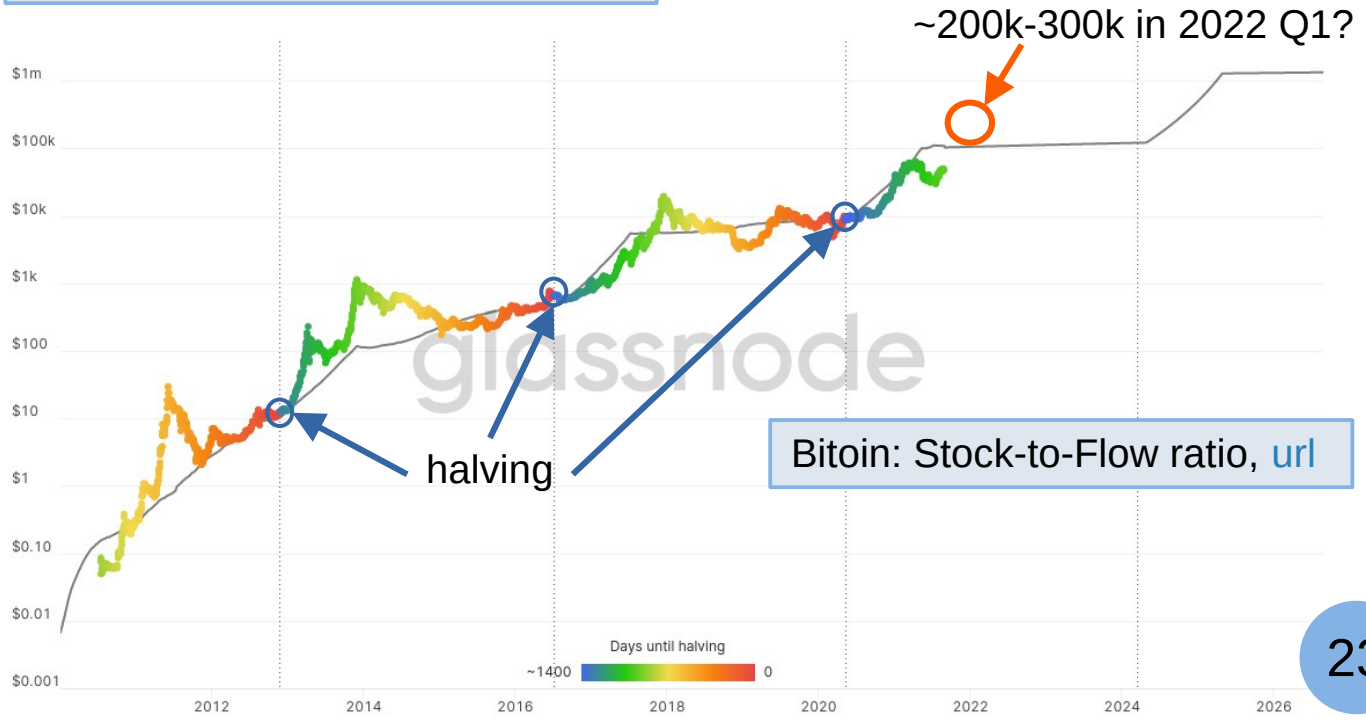
- S2F models are a measure of new supply relative to existing supply (stock growth rate) (In 2021: BTC: ~1.7%, gold: ~1.6%)
- Bitcoin S2F model was published in March 2019 by PlanB (a pseudo-anonymous bitcoin analyst Twitter group, with > 700k followers)
- The model almost broke several times (last time in July 2021), but finally didn't!
- The more times it confirmed the more people believe it and keep the model valid.



Bitcoin and the Stock-to-Flow (S2F) Model, url

PlanB@100trillionUSD, "Modeling Bitcoin Value with Scarcity, Mar 2019, url

PlanB@100trillionUSD, Twitter url



Bitcoin’s market capitalization

Blockchain matters

- Coinmarketcap
- Bitcoin’s current market capitalization is 903 billion USD (Sept. 2021)
- Tesla: 750 billion USD (Sept. 2021)
- Facebook: 1.044 trillion USD (Sept. 2021)
- Google: 1.913 trillion USD (Sept. 2021)
- Gold: 11.15 trillion USD (Sept. 2021)

Coinmarketcap, url

Bitcoin’s market capitalization

Blockchain matters

- Coinmarketcap
- Bitcoin’s current market capitalization is 903 billion USD (Sept. 2021)
- Tesla: 750 billion USD (Sept. 2021)
- Facebook: 1.044 trillion USD (Sept. 2
- Google: 1.913 trillion USD (Sept. 202
- Gold: 11.15 trillion USD (Sept. 2021)

What would be the price of BTC if Bitcoin would take over the role of the gold and exceeds its market capitalization?

>550.000 USD

Coinmarketcap, url

Bitcoin misbelieves and criticism

Blockchain matters

- Bitcoin will replace fiat currencies. No it won't. It conflicts governments' interest.
- Bitcoin will bring a financially equal World. No it won't. There always will be riches and poors…
- Bitcoin's energy consumption is much higher than that of current banking system. No it isn't. Bitcoin's ~120 TWh per year vs. banking system's ~250 TWh per year in 2021 Q1. Nevertheless Bitcoin's energy consumption is huge, but that is the price of decentralization and security.
- Obsolete mining hardware become rubbish. Maybe, but old Bitcoin mining hardware can use for mining other cryptocurrencies.
- Bitcoin is the money of criminals. This is not true. Bitcoin transactions are traceable and pseudonym. Cash is better for crime use cases, criminals prefer USD!
- Bitcoin has scalability problem due to 1 MB block size and 10 minutes block time. It is true, but is it really a problem? (Reliefs: Segwit, Lightning Network)
- Bitcoin is not decentralized, because more than 50% of mining power is concentrated in China in the hand of some huge mining companies. Don't forget that transactions/blocks are being verified by all (~12000) full nodes nodes located worldwide. Moreover this is not true since 2021 Q4.
- Bitcoin transaction is slow and expensive. Compared to what? Have you ever tried to transfer 10M USD to e.g. Uganda? Is it possible at all?
- Bitcoin throughput is slow comparing to VISA (~7 tx/sec vs. ~1700/sec). It is true, but is it really a problem?
- One of the novel cryptocurrencies ("Bitcoin killers") will ever replace Bitcoin. It isn't very possible, because of the first mover's advantage. Bitcoin is the first and the only cryptocurrency without a known creator, which is a big advantage in a decentralized world. And moreover Bitcoin is "too big to fail…" :)

Namcios,"Research: Bitcoin Consumes Less Than Half The Energy Of The Banking Or Gold Industries", url

Bitcoin’s life so far

Blockchain matters

	Years	Investors	Use cases	New products
The geek period	2008 - 2013	geeks	experimental toy, first P2P payments	software wallets, exchanges
The retail period	2013 - 2020	average people	first merchants accepting BTC, P2P payments	hardware wallets, FIAT gateways
The institutional period	2020 -	institutions (Microstrategies, Greyscale, Tesla, Paypal)	CeFI/DeFI, lending, custody services, interest-bearing deposits	Lightning Network wallets (Official currency of El Salvador since 09.2021)
The future		governments	banking, BTC pegged national currencies?	

Bitcoin’s life so far

Blockchain matters

	Years	Investors	Use cases	New products
The geek period	2008 - 2013			
The retail period	2013 - 2020			AT
The institutional period	2020 -			vallets El 021)
The future				

2010 – No one uses it.
2012 – Only computer nerds use it.
2013 – Only drug dealers use it.
2014 – Only money launderers use it.
2017 – Only gamblers use it.
2019 – Only a small percentage of population uses it.
2020 – Only small companies use it.
2021 – Only small countries use it.

What’s up in 2022?

What's up in 2022?, url

The Bitcoin Standard

Blockchain matters

- Gold standard was the almost perfect monetary system, but it had some significant deficiencies
  - Portability of physical gold is cumbersome.
  - States began to print more money which exceeded the gold reserve...
- Bitcoin knows all what gold knows, but better, because Bitcoin is really finite and its portability is not an issue.
- Bitcoin standard monetary system in the future?

S. Ammous, “The Bitcoin Standard: The Decentralized Alternative to Central Banking”, 2018, url

Further topics

Blockchain matters

- Advanced transactions, scripting
- Segregated Witness (Segwit)
- Lightning Network

Bitcoin Script, url | Segregated Witness, url | Lightning Network, url

So, what is Bitcoin?

Blockchain matters

- The first and the most decentralized cryptocurrency without any central control and censorship.
- The first truly finite “material” in the Universe.
- Programmed deflation policy.
- Data (transactions) stored in the Bitcoin’s blockchain is probably the only thing in the Universe which is certainly true. You can’t trust anyone or anything with 100% certainty but the Bitcoin’s blockchain.
- These 3 properties above are not true for cryptocurrencies or blockchain in general. Only Bitcoin has these properties!
- So, is the huge energy consumption a high price for Bitcoin?

And what is Bitcoin from legal perspective?

Blockchain matters

- It depends on the local legal regulations.
- Thing (a physical object which you can own)? - No, because bitcoin has no physical embodiment. Nevertheless, bitcoin falls mostly into this category.
- **Money**?
  - Right in rem: no, because BTC is not a thing :)
  - **Contract law**: yes :) Nobody forbids to pay with BTC.
- Security? - No, because there is no issuing authority.
- Intellectual property? - Only the Bitcoin software, not the coins.

Blockchain

matters

Coming up next: Blockchain

Blockchain matters

Thank you!

If you liked this material you can tip me

Blockchain matters

- Bitcoin: *3FvgmYScorEje3WTrdDn5synEU6j917SZz*
- Litecoin: *ltc1qs457h3899qj4yry8k6u5xva79wa8f6xspant4e*
- Ethereum: *0xdF7eAab54BC9070a140D0251247406cEe40029B7*
- QTUM: *MGo31aQ74yHJ9Lan4tgYeFy5XhtHZuoimQ*
- Tezos: *tz1VpDWz45fvqv69Laa6YVa3h6MtkCoq1BDc*

Blockchain

matters

Thank you again!