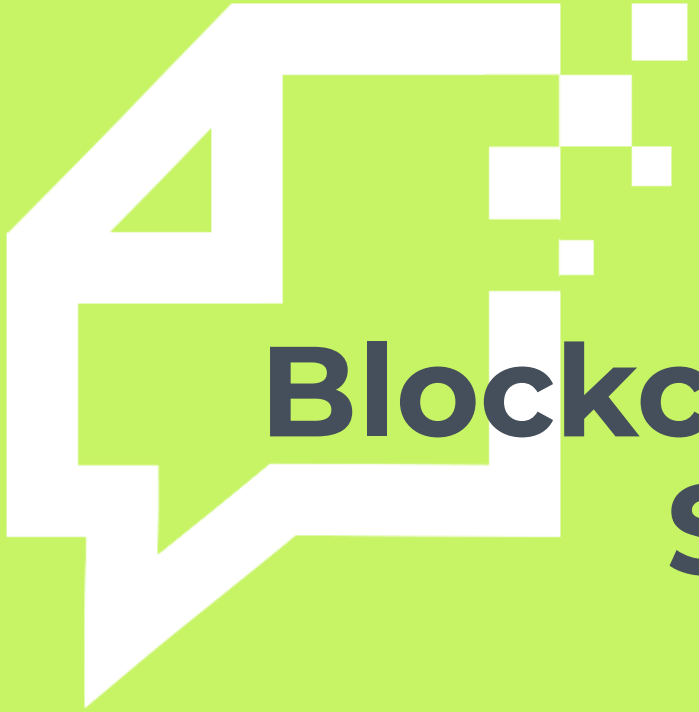
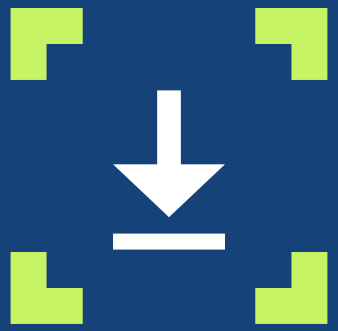


Blockchain & Crypto Skillz for Sales

Free Crypto Course

Learn the basics of Crypto and Bitcoin to start your journey in the crypto trading world.

Download the full Crypto Course HERE



Free Crypto Course

Download the full Crypto Course
HERE

?

Who are we

Encrypted Reviews

We write the most genuine and trusted reviews of all things crypto that exist online. Our reviews focus on what the platform offers but also presents a step by step guide to get you up and running if you are keen to get started.

Encrypted Reviews

- We got into Blockchain and Crypto in 2016.
- Encrypted Reviews is a team of highly qualified individuals with more than 15 years of experience.
- We specialise in everything crypto, reviewing digital trading platforms, crypto wallets and bitcoin online casinos.
- We might have missed the mining phase but we've bought bitcoin, we've lost our Ethereum private keys, bought alt coins that were ridiculous, lost money, read pipe dream white papers, gone to a few conferences, etc.
- We have worked in online trading but before the crypto phase.
- When it comes to crypto trading we are hobbyist and, during the better days of Bitcoin, have made decent profit trading crypto.

This Course

Course Objectives

- Blockchain & Crypto 101
- Understanding the Blockchain/Crypto Landscape.
- Connecting the dots between crypto services providers (B2B)

Course Structure

- Session 1: Learn Everything about Blockchain
- Session 2: Learn Everything about Bitcoin
- Session 3: Other Cryptocurrencies and Altcoins
- Season 4: DiFi, Application & Regulation

Temperature Check

How would you describe your knowledge of Blockchain and Crypto?

A. Every day I'm Hodl'ing - *I'm a pro*
B. I know the mainstream things but not technical details: *I'm curious*
C. I know a bit but am not confident: *I'm a novice*
D. I know very little about this digital magic: *I'm a noob*

****What is your goal for this course?****

Session 1

Agenda

- **Blockchain**
  - Key Points
    - Immutability
    - Decentralisation
    - Safety
  - Ledger
    - Public Ledger
    - Centralised vs. Distributed Ledger
    - Byzantine Generals Problem
  - Advantages and Disadvantages
- **Uses of Blockchain**
  - Overview
  - Ownership and Compensation
  - Academic Certificates
  - Real Estate Investment
  - Supply Chain Shipping
  - Solar Energy Management
- NFTs
- **Cryptography**
  - Key Points
  - Cryptographic hash functions
  - Bitcoin Hash Keys

?

What is Blockchain

Blockchain

Blockchain is a software technology that allows the sharing of information peer to peer.

Key Points

- Blockchains, like their name indicates, store data in “blocks” which are chained together.
- Every transaction is saved into a new block.
- A new block is then chained to the previous block of data.
- The data is chained in chronological order and sealed with a time stamp.
- The information stored in the blockchain can be shared without the need of third-party intermediaries, such as banks, government organisations, etc.
- The goal of blockchain is to allow digital information to be recorded and distributed only. Editing is not possible and nothing can be undone.
- The three main characteristics of a blockchain are: **Immutability, decentralisation and safety.**

Key Points: Immutability

- Transactions are permanently recorded, immutable, and cannot be changed by anyone.
- The data stored in each block is visible to everybody, yet not changeable.
- When a new block is stored, it transforms into “stone” and becomes part of the blockchain timeline.
- Each new block is given a timestamp with the exact date and time it was recorded.
- No single person or group of people have control, rather all together, collectively.

➔ Interview with the guy behind ‘’timestamping’’ - Scott Stornetta. Watch it here.
  - Article here

Key Points: Decentralisation

- Each computer or group of computers is in a different geographic location and are operated by separate individuals or groups of people.
- These computers that makeup the network are called nodes.
- This method aids in the establishment of a precise and straightforward sequence of events.

Key Points: Safety

- Each new block stored in the blockchain is saved chronologically and linearly.
- Each block has its own hash, as well as the hash of the previous block and the time stamp.
- A math function converts digital data into a string of numbers and letters, resulting in hash codes.

➔ BLOCK = HASH (previous block)+ Timestamp

Advantages and Disadvantages

Pros

- Accuracy of the Chain
- Cost Reductions
- Decentralisation
- Efficient Transactions
- Private Transactions
- Secure Transactions
- Transparency
- Banking the Unbanked

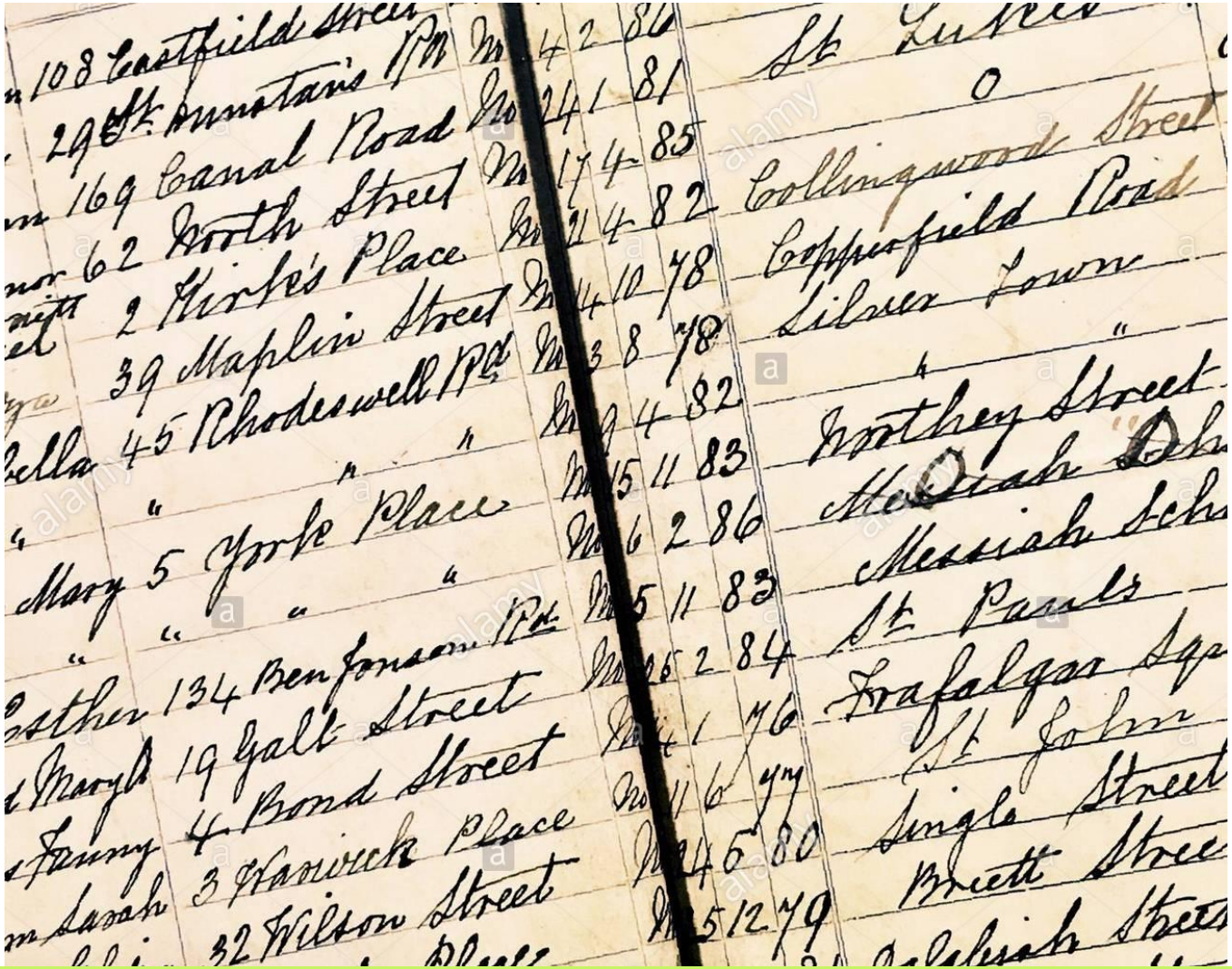
Cons

- Technology Cost
- Speed Inefficiency
- Illegal Activity
- Regulation

Ledger

A ledger records activity, ownership and transfer of value between stakeholders.


DATE September 17, 2015
DAILY GOALS 1800 calories
FOOD VALUE REMAINING
oatmeal -150 1650
banana -80 1570
turkey sand. -500 1070
granola bar -170 900
salad + ranch -700 200
walk 3 miles +300 500
WATER
EXERCISE walk 3 miles
NOTES super tired + cranky today!

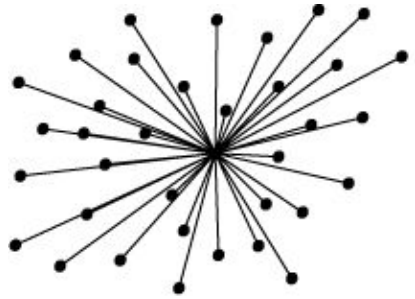

108 Eastfield Street
29 St. Dunstan's Pl
169 Canal Road
62 South Street
2 Hirst's Place
39 Maplin Street
45 Rhodeswell Pl
" " "
Mary 5 York Place
" " "
Esther 134 Ben Jonson Pl
Mary 19 Galt Street
4 Bond Street
3 Warwick Place
32 Wilson Street
St Lukes
Collingwood Street
Copperfield Road
Silver Town
Northey Street
Messiah Sch
St Pauls
Trafalgar Sq
St John
Single Street
Brett Street

Public Ledger

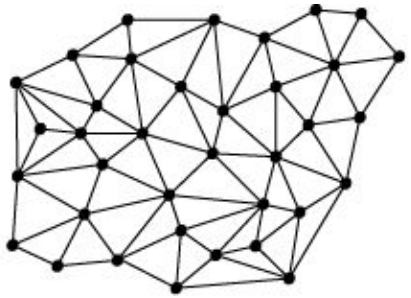
- A public ledger is a record-keeping system.
- The ledger maintains participants' identities anonymously (pseudonymously)
- It records all the transactions executed between network participants.
- Scaling and security concerns are one of the challenges for public ledgers.
- Similar to the bank records, the transaction details on a public ledger can be verified and queried by the two transacting participants. Their identities remain unknown.

Centralised vs Distributed (Decentralised)

- A **centralised ledger** (owned/ controlled)
  - The general ledger is the backbone of any accounting system which holds financial and non-financial data.
  - Example: A general ledger contains all the accounts for recording transactions relating to a company's assets, liabilities, owners' equity, revenue, and expenses.
- A **distributed ledger** (not owned)
  - A database that lives across a network of multiple sites, geographies or institutions.
  - Each participant may each have their own identical copy of the ledger.

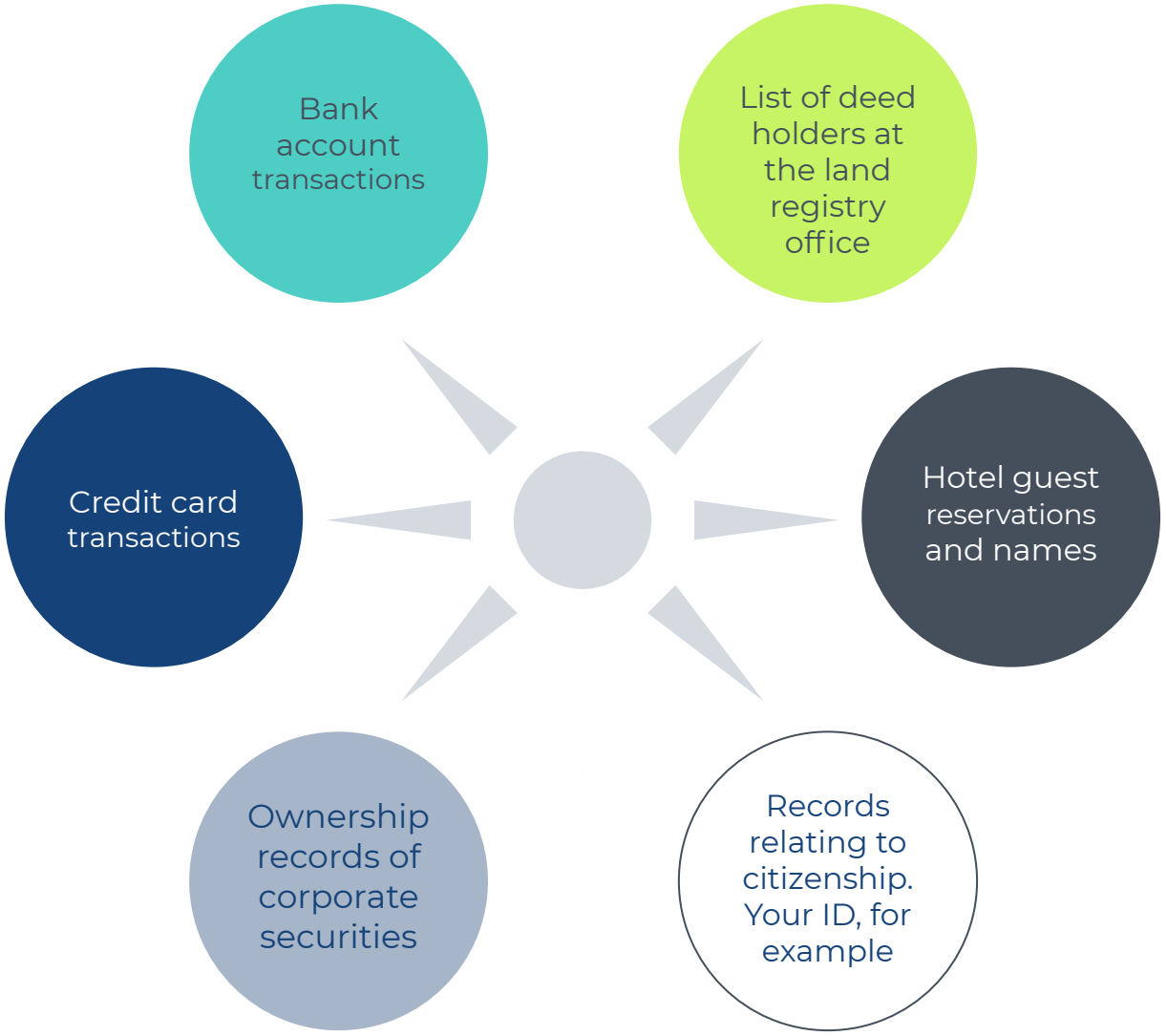


centralised

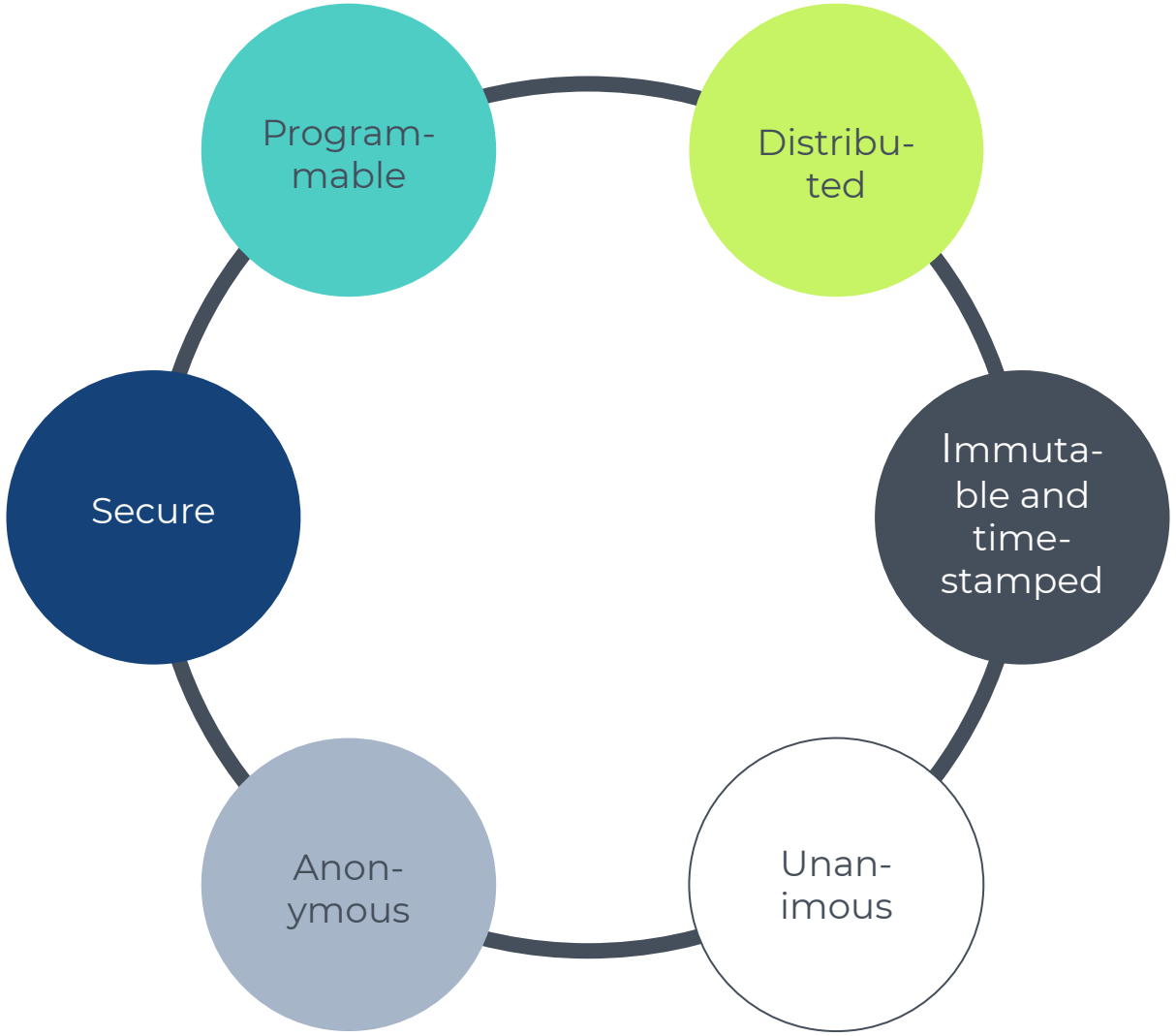


distributed

Centralised Ledger Examples



Distributed Ledger Technology (DLT)



Ledgers and Ownership

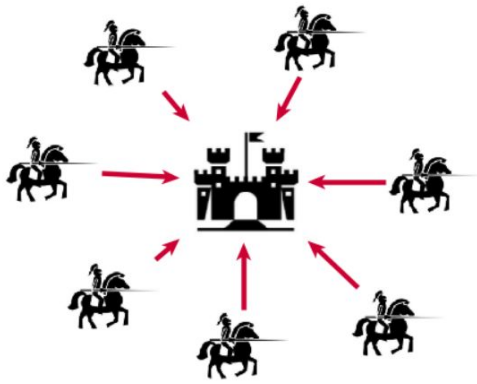
- Nodes are devices in charge of handling transactions and keeping track of all records, including those of ownership.
- Anyone can become a node by downloading the free open-source Bitcoin programme.
- No single node prevails over the others. None is trusted, and all nodes are treated equally.

Question:

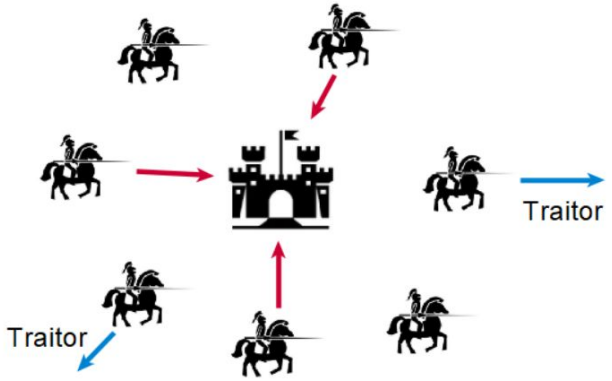
- What problem does blockchain solve?

Byzantine Generals Problem

- The main challenge that distributed networks are faced with is consensus.
- In the event of a faulty or defective component, the network needs to manage the failure and prevent any damage.
- A failed processed could be triggered by a component that crashes, reboots or shuts down, or even behaves byzantine.
- This problem is best known as “problem of the Byzantine Generals”.



Coordinated attack leading to victory



Uncoordinated attack leading to defeat

Byzantine Generals Problem p.2

- In the case of Bitcoin, the entire network of nodes needs to agree on the validity of transactions.
- There is always a risk of misinformation or miscommunication between users, whether accidental or deliberate, which is why consensus is key.
- Distributed Ledger Technology, and several other types of computer networks, would fail to function properly.
- The loyalty of more than 50% of the nodes that constitute the blockchain network is key to reach **consensus** and, thus, provide a solution to the problem.

Blockchains

Blockchain Platforms

- Each blockchain has its own:
  - **Governance (rules)**
  - **Consensus (way of validation)**
  - abilities/ best use cases

More blockchain platforms [here]

Last update: Jan-2021	Bitcoin BTC	Ethereum ETH	Ripple XRP	Cardano ADA	Cosmos ATOM	Polkadot DOT
Main Website	bitcoin.org	ethereum.org	ripple.com	cardano.org	cosmos.network	polkadot.network
Blockchain Generation	1st gen	2nd gen	1st gen	1st gen	3rd gen	3rd gen
Consensus Mechanism	PoW	PoW	RPCA	PoS	BPoS	NPoS
Consensus energy consumption	High (small state)	High (half of Bitcoin)	Low	Low	Low	Low
Block Time	600s	14s	4s	20s	7s	6s
Transactions Per Block/Second ~	2.700 4,5 TPS	70 5 TPS	6.000 1.500 TPS	5.000 250 TPS	10.000 (Hub) 1.420 TPS	6.000 (Relay) 1.000 TPS
Deposit Times (by Kraken)	40 minutes	5 minutes	near-instant	10 minutes	near-instant	2 minutes
Transaction Fee ~ (as of Jan 2021)	$ 8	$ 4	$ 0.0X	$ 0.0X	$ 0.0X	$ 0.0X
Smart Contracts	Yes (Script)	Yes (Solidity EVM)	No (planned)	No (planned)	Yes (WASM, EVM)	Only parachains (WASM, EVM)
Decentralized Apps (dApps)	No	Yes	No	No	Yes	Yes
Decentralized Exchange (DEX)	No	Yes	No	No	Yes	Planned
Decentralized Finance (DeFi)	No	Yes	No	No	Yes	Planned
On-chain Governance	No	No	No	No	Yes	Planned
Human Readable Addresses	No	Yes	No	No	Yes	Planned
Digital Identity Management	No	Yes	No	No	Yes	Planned
Data Oracles	No	Yes	No	No	Yes	Planned
Data Privacy	No	No	No	No	Yes	Planned
Distributed Cloud Storage	No	Yes	No	No	Yes	Planned
Distributed Cloud Computing	No	Yes	No	No	Yes	Planned
Interoperability	No	No	No	No	Yes (IBC)	Yes (ICMP)
Cross-chain communication	No	No	No	No	Yes (IBC peg zones)	Planned (XCMP bridges)
Scalability Options	None (planned lightning)	None (planned ETH 2.0)	No (only by channels)	None (planned Hydra)	Zones	Parachains (shards-like)
Chains Security Model	N/A	N/A	N/A	N/A	Zone sovereignty	Relay sovereignty
Automated Slashing	N/A	N/A	N/A	N/A	Yes (by protocol)	Yes (fisherman)
						You need to buy a

Cryptography

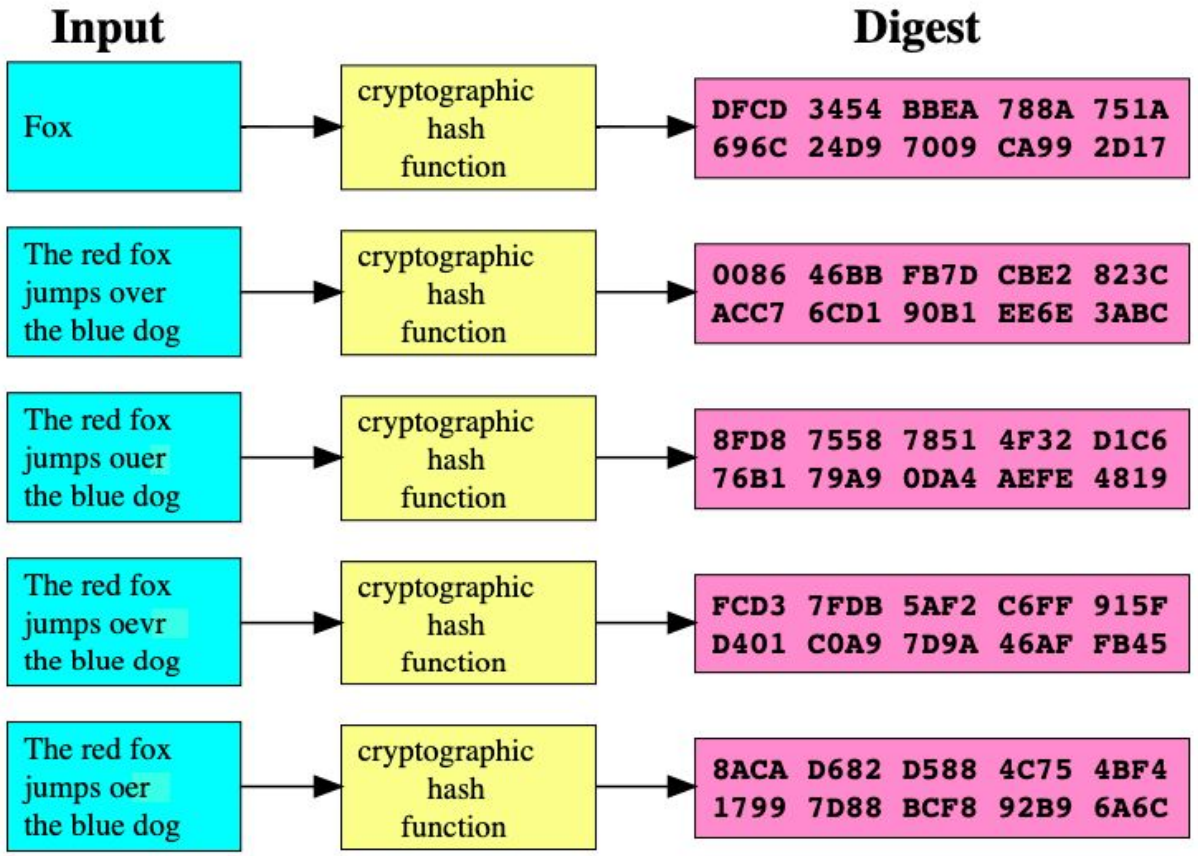
What is a Hash?

Hash

A hash is a function that transforms a string of letters and numbers into a fixed-length encrypted output.

Key Points

- A cryptographic hash function is a mathematical process that transforms identical data into a unique, fixed-size code, which is widely used to verify data authenticity.
- Any data alteration, whether accidental or malicious, would fully alter the hash code.

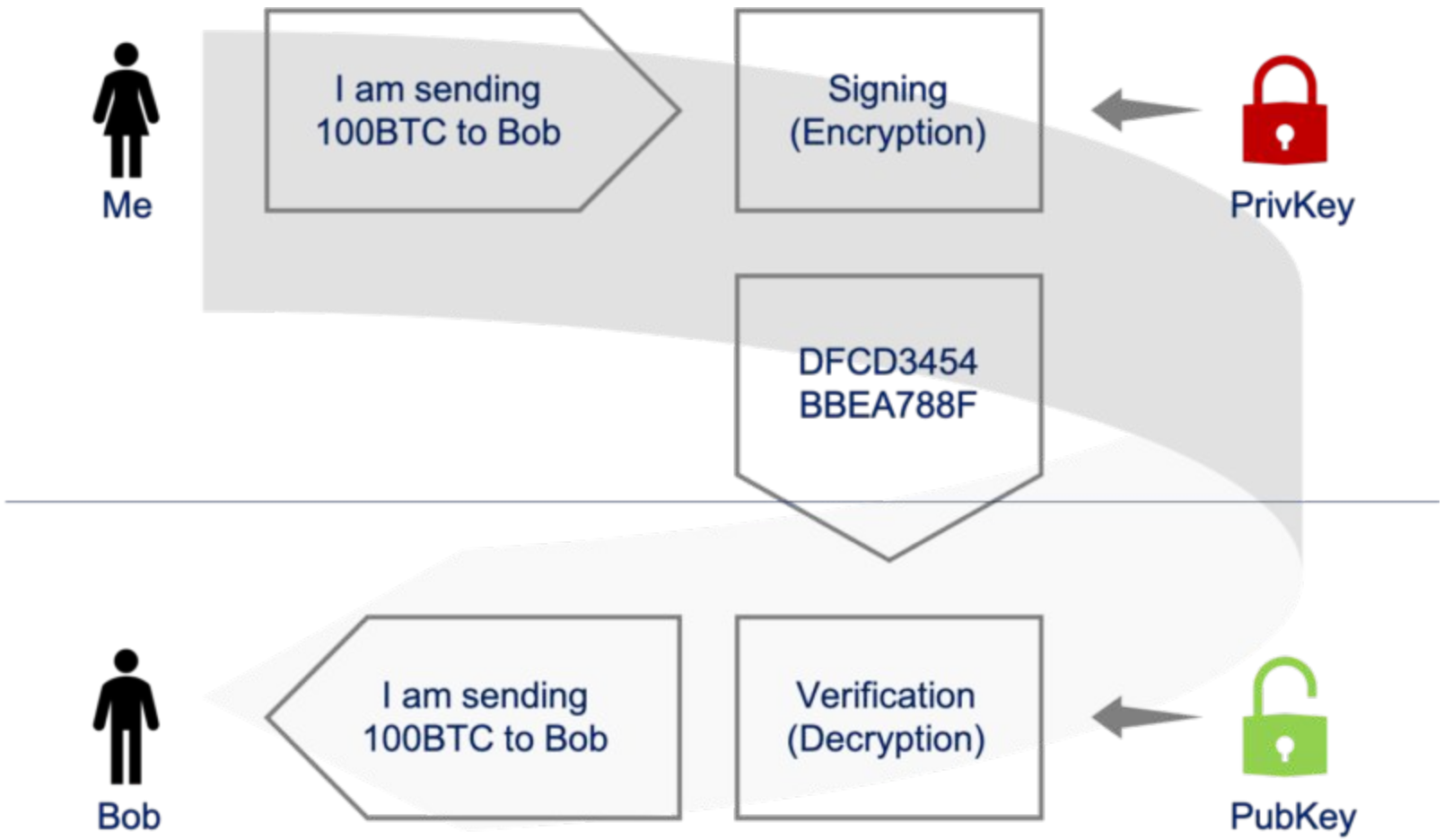


Cryptographic hash functions

- Password storage is the most coord storage is the most common use for a Hash
- Hash functions are one of the ground pillars of the blockchain technology and ensure immutability.
- Solving the hash starts with the data available in the block header.
- Each block header contains:
  - Version number
  - Timestamp
  - Hash of previous block
  - Hash of the Merkle Root
  - Nonce
  - Target Hash
- Fun Fact: Satoshi wanted to avoid confusion in Bitcoin addresses, so he removed O0lI characters.

Bitcoin Hash Keys

- A **Private key (Privkey)**
  - It is initially generated at random, and is kept secret at all times.
  - It is used to transfer bitcoins from one owner to the other. The original owner has to digitally sign off the transaction to validate it.
  - The digital signature of a transaction confirms ownership and can be used to check that the transaction is genuine.
- The **Public key (Pubkey)**
  - The public key is generated from the private key using a unique hash function.
  - It is used by the new owner to verify the digital signature of a transaction.


Me
I am sending
100BTC to Bob
Signing
(Encryption)
PrivKey
DFCD3454
BBEA788F
Bob
I am sending
100BTC to Bob
Verification
(Decryption)
PubKey

≠

Uses for Blockchain

Question:

- What are some uses of blockchain?

What are some uses of blockchain?

- Currency (Session 2 & 3)
- Digitalised Commodities
- Record keeping
- Process monitoring
- Quality Assurance

Some Companies Currently Using Blockchain

Bank and Finance	HSBC	BBVA	Barclays	VISA	Intesa Sanpaolo
Supply Chain	AB InBev	Walmart	DB	Ford	Unilever
Healthcare	Pfizer	Change Healthcare	FDA	CDC	DHL
Insurance	AEGON	Prudential	MetLife	AIA	AIG
Energy	SIEMENS	Shell	Adnoc	CNE	Tennet
Real Estate	Westfield	JLL	Brookfield	Coldwell Banker	LINK
Trade	ANZ	Bank of China	SEB	Scotiabank	MIZUHO
Government	Government of Dubai	MAS	Seoul	Lantmäteriet	Uganda National Drug Authority
IoT	Smart Electric Power Alliance	McKesson	Van Dorp	Commonwealth Bank	Maersk
Travel	ETIHAD Airways	Singapore Airlines	DELTA	British Airways	Lufthansa

Uses for Blockchain

- Blockchain (in conjunction with “smart contracts”) has many other applications outside the crypto world. It can help address more complex issues. For example:
  - **Public Records:**
    - Land titles, Criminal records, Voter records, Court records
  - **Private Records:**
    - Wills, Trusts
  - **Other uses:**
    - Certifications, Medical records, etc.

Other uses: Ownership and Compensation

- **Song/ Art registration**
- Ownership is registered permanently therefore no need for record labels to have a share of the artist's work.
- Smart Contracts technology allows artists to set automated payments to them based on licenses they design themselves.

Other uses: Academic Certificates

- Ease of Publication & Distribution
- Independent validation
- Immutable Records
- Reduced time and cost to issue (and re-issue) certificates
- Data is accessible, even if the university or the institution’s website is no longer accessible.
- Employers can verify job applications instantly, ensuring that a candidate is presenting valid academic certifications.

Other uses: Real Estate Management

- Property owners could digitally prove and transfer ownership immediately without the need to pay and wait for third-party verification.
- A “digital ownership certificate” cannot be replicated, making selling or advertising properties you don’t own almost impossible, reducing property fraud.
- Faster mortgage process and transfer of ownership.
- Credit history, income could be checked immediately, saving time spent dealing with banks, attorneys, and intermediaries.
- Homeowners may show that they own the property and have lived there for a certain amount of time.
- Digital IDs may be attributed to properties, which would include the chain of ownership, a list of repairs, and other relevant information.

Other uses: Supply Chain Shipping

- Allows digitisation of the supply chain process
- Reduce the time spent in transit and during the shipment process, by tracking the paper trails of shipping containers.
- Enhance product accountability and protection while lowering costs and complexity
- Reduce fraud and defects in product quality by improving stock control.

Other uses: Solar Energy Management

- Energy buying and selling is decentralised and direct among participants, ensuring independence from a third-party power supplier.
- Transaction data is stored, as well as the amount of electricity produced per participant in a network.
- A community or an area may set up a solar-powered energy trading system and keep track of transactions between residents.
- Instead of selling excess energy back to the power provider, users can exchange it among themselves.
- Participants can sell their excess energy to whom they decide and decide its price.

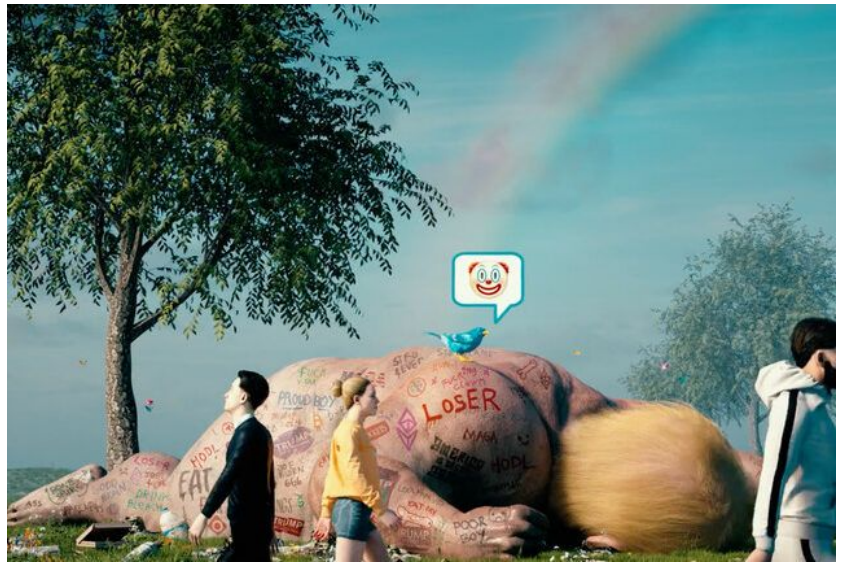
NFT

A non-fungible token (NFT) is a digital file stored on a blockchain that certifies its uniqueness.

Dogecoin's NFT

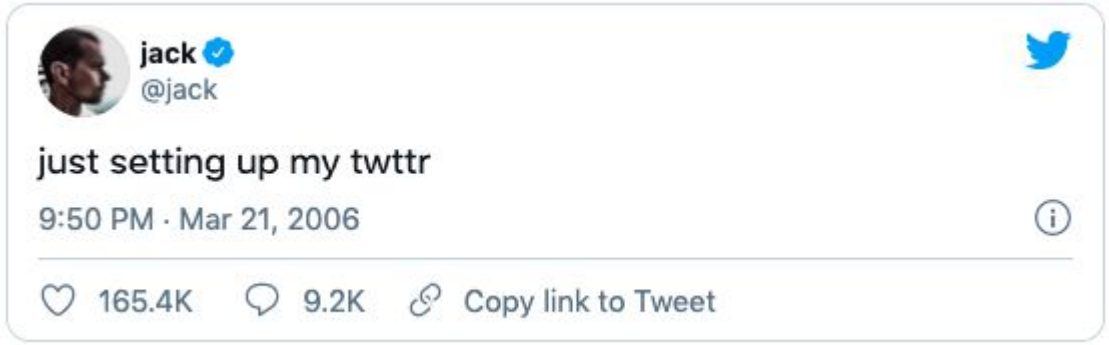
https://www.cryptokitties.co/
https://crypto.com/nft/marketplace

Logan Paul Pokémon card: $20,000

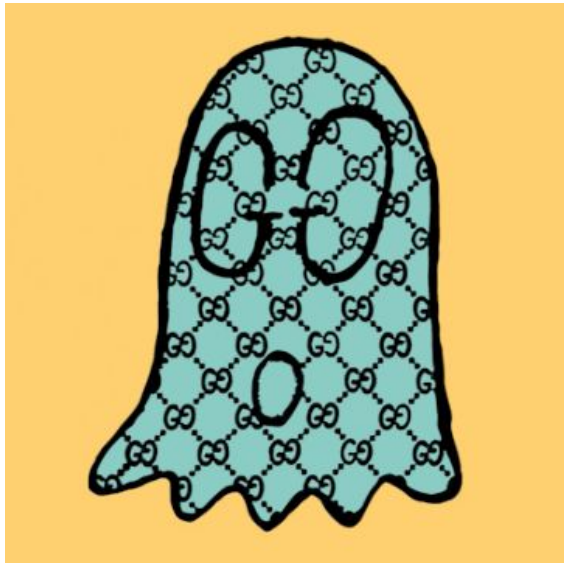


Beeple Video: $69 million

Dude with Sign: launching 1st NFT on 23th April 2021



Twitter's Founder 1st Tweet: $2.5 million



Gucci Ghost: $3,600

What are NFTs?

- NFTs are non-fungible digital tokens that run, mostly, on the Ethereum blockchain using smart contracts.
- CryptoKitty is the first NFT, with each kitty being an ERC-721 token.
- They can be used to share digital assets and use the blockchain to check their validity.
- While anyone can access copies of these digital products, NFTs are monitored on blockchains to provide the owner with a proof of ownership that is distinct from copyright.

But Why buy NFTs?

- Artwork NFTs are comparable to autographed art pieces.
- Non-fungible basically means that it’s one-of-a-kind and can’t be replaced by anything else.
- A bitcoin, for example, is fungible, meaning you can exchange one for another and get exactly the same thing.
- A digital file, including the art that comes with an NFT, can be replicated as many times as you want.
- NFTs are built to give you something that can’t be copied: ownership of the work.
- To put it another way, anybody can buy a Picasso print, however, the original can only be owned by one person.

ReCap

- Blockchain is:
  - a record keeper
  - digitased ledger
  - chronological
  - immutable
  - can be decentralised or centralised
- Where does blockchain differ from a database:
  - records are built by consensus
  - enable trust
- You need a private key and a public key to ‘sign’ blockchain

Keywords

- Blockchain
- Blocks
- Nodes
- Ledger
- Centralised
- Decentralised
- Byzantine Generals Problem (BGP)
- Consensus
- Proof of work
- Hash
- Private key
- Public Key
- Digital signature

Thanks!

See you in our next session.
Any questions so far?

Session 2

Agenda

- **Bitcoin**
  - Key Points
- **History of Bitcoin**
- **How Bitcoin works**
  - Mining
    - Key Points
    - How mining works
    - Proof of Work Problem
    - 51% Attack
    - Mining Farms
  - Halving
    - Key Points
    - Future of Halving
- **Bitcoin Price**
  - Supply and Demand
  - Competition
  - Cost of Production
  - Availability
  - Regulations
  - Forks & Governance Stability
  - Forks
    - Bitcoin Forks
    - Soft Fork vs Hard Fork
    - Hard Forks
- **Bitcoin Metrics**
  - Top 5 Cryptocurrencies
  - Bitcoin Price
  - Market Capitalisation
  - Cryptocurrencies in the Market
  - Total Bitcoin Supply
  - Future Bitcoin Supply
- **Lightning Network**
- **Fun Facts**
  - Who is Satoshi Nakamoto?
  - Bitcoin Bible
  - Bitcoin Pizza Day
  - Liberland
  - Digicash

?

What is Bitcoin

Bitcoin

A type of digital currency that functions independently of a central bank and maintains a record of transactions while also generating new units of currency through the computational solution of mathematical problems.

It’s a new online currency that’s been developed. It’s just like actual money, except you can’t see it, hold it or spend it on anything. […] You can mine it. […] There is a limited amount and we find it not by tunneling into the earth, but by using a computer to solve complex mathematical problems.

Sheldon Cooper, The Big Bang Theory
Watch it here and here

Key Points

- Created anonymously in 2009 by Satoshi Nakamoto
- “Bitcoin” the blockchain vs. “bitcoin” the coin
- The first block was called genesis block
- In 2021 Bitcoin remains the world’s leading Cryptocurrency, followed by Ethereum (ETH) and Binance (BNB)
- It is a decentralised currency, which means they are not issued by any entity and cannot be outlawed.
- Bitcoin transactions cannot be reversed, they are immutable.
- Large amounts of bitcoin are held by whales.
- Some people like to hodl bitcoin since they consider it a rare commodity.

Bitcoin’s Governance

- There’s a limited amount of Bitcoin.
- When Bitcoin was founded, the creator only made 21 million of it.
- Right now, over 18 million Bitcoin are in circulation.
- The number or bitcoin “released” through mining reduces over time.
- Over time, the computation becomes harder to solve.
- Predictively, it will take until 2041 for all bitcoin to be mined.
- A new Bitcoin block is build every 10 minutes.

Bitcoin Characteristics

- Bitcoin addresses are a long strings of up to 35 alphanumeric characters.
- You keep bitcoin in a wallet
- Under this address, know as a key, the identities of the sender and recipient are kept anonymous.
- If you lose your key, you've lost your bitcoins!
- It is believed that aprox 20% of all the bitcoin supply is "lost".
- Bitcoin is highly volatile.
- It is created through mining.

Key Points p.3

- Bitcoin can be regarded as one of the most significant technical breakthroughs of the twenty-first century.
- One of bitcoin is called a “Satoshi byte” – 1 Satoshi byte is worth 0.00000001 bitcoin
- Bitcoin ATMs are now available worldwide.
- Fun fact: The FBI is the owner of one of the world’s biggest Bitcoin wallets (1.5% of all bitcoins)

“*Bitcoins are amounts associated with addresses, unique strings of letters and numbers. “1Ez69SnzzmePmZX3WpEzMKTrcBF2gpNQ55” represents nearly 30,000 Bitcoins seized during the Silk Road bust—worth about $20 million at the time—that were auctioned off by the U.S. government on 1 July 2014*”.

Is Bitcoin anonymous?

- Bitcoin is completely transparent. Thus, it would be ironic for it to also be anonymous.
- Instead, it is pseudonymous. This means it’s anonymous, but only up to a certain degree.
- “Bitcoin is designed to allow users to send and receive payments with an acceptable level of privacy as well as any other form of money. However, Bitcoin is not anonymous and cannot offer the same level of privacy as cash”

Is Bitcoin money?

- Properties of money:
  - Money is a store of value
  - Money is a unit of account
  - Money is a medium of exchange
- There are many arguments about whether Bitcoin is money or not
- Essentially, for something to be classified as money, it needs to be considered “legal tender”.
- While some countries now recognise bitcoin as legal tender, the majority of countries still regard it as a commodity.

History of Bitcoin

2008

- Registration of the domain bitcoin.org
- Satoshi Nakamoto publishes the white paper:
  Bitcoin: A Peer-to-Peer Electronic Cash System

2009

- Mining of Block 0 - **Genesis** Block of Bitcoin
- First Bitcoin transaction takes place:
  Satoshi Nakamoto sends 50 Bitcoins to Hal Finney

2010

- Code for mining bitcoin is released to the public
- First real world bitcoin transaction:
  Laszlo Hanyecz buys a pizza with Bitcoin

2011

- Bitcoin Price reaches parity with USD in February:
  1 BTC = 1.10 USD
- Wikileaks accepts Bitcoin donations

2012

- First Bitcoin Halving event
- Bitcoin Foundation is established to accelerate its global growth

2013

- Bitcoin Market capitalization reaches 1 Billion USD
- World’s first Bitcoin ATM

2014

- PayPal announces the integration of Bitcoin as valid currency

2015

- Bitcoin Lightning Network established
- Ethereum goes live with 72 million coins

2016

- Craig Wright claims to be Satoshi himself stating that this is “only the beginning”
- 3.6 million Ethereum are stolen
- Second Bitcoin halving event

2017

- Hard Fork, splitting into two Blockchains
- Bitcoin Cash is created
- Japan recognizes Bitcoin as a legal tender
- Bitcoin reaches $20,000

2018

- First Lightning Network Released
- Bitcoins Price crashes to $3,300

2019

- More than 5,000 Bitcoin ATMs around the world

2020

- COVID-19 makes Bitcoin price crash due to the pandemic
- Bitcoin recovers and reaches all-time high of $28,000+ in December

2021

- Elon Musk and Tesla announce Bitcoin investment and acceptance of payment
- Bitcoin reaches new all time high of $60,000 in April

2022

- Future?

How Bitcoin works

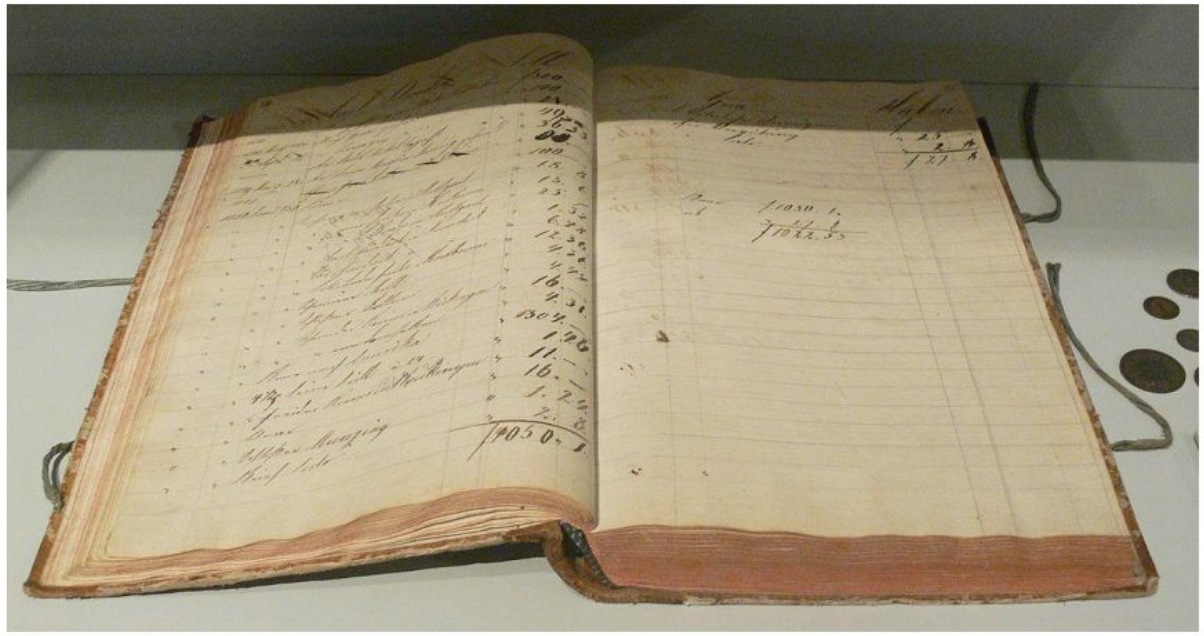
Mining

Is the process of generating new bitcoins through computational algorithms.

Mining

- The term “mining” is a poor analogy for what “miners” do.
- It would make a lot more sense if you think of the miners as bookkeepers.

Think **attributing** to **record keeping** & ***verifying***...



...not this.

Key Points

- Bitcoin mining process serves two purposes:
- It creates new bitcoins in each block
- And confirms transactions
- Bitcoin mining requires a lot of energy, hardware and bandwidth.
- As a result, if you intend to do this at home, the cost of electricity would almost certainly outweigh the value of the bitcoins you will mine.
- To mine successfully, you need to have a high “hash rate,” which is measured in terms of megahashes per second (MH/s), gigahashes per second (GH/s), and terahashes per second (TH/s).

How mining works

1. Miners gather and broadcast their transactions in a block, which they then verify are legitimate.
2. They apply the previous block's header's cryptographic hash function to the new block.
3. Then, they try to solve the Proof of Work dilemma.
4. Winning/Losing – The winning block is broadcast to all other clients as a verified transaction block. The client nodes check that the hash matches the required pattern and accept the new block, which is then added to the existing blockchain that they all maintain.
5. Notice that blockchain refers to a series of blocks (!)

Proof of Work Problem

- To prevent wasteful or malicious use of the device, miners must demonstrate that they have placed considerable effort into solving complex mathematical problems.
- The time and energy required to run the computer hardware and solve complex equations is part of said effort.
- How it works:
  a. Hash of Last Block Header + Block of New Transactions + Random Number (Nonce = 32-bit number)
  b. Apply Cryptographic Function (SHA-256) to the above data
  c. Hash is compared to a predetermined value.
     i. Less than this value = Prize.
     ii. Not less = Guess Nonce Again & Repeat
     iii. Winning Block Verified by Nodes as a Block and broadcasted to the network

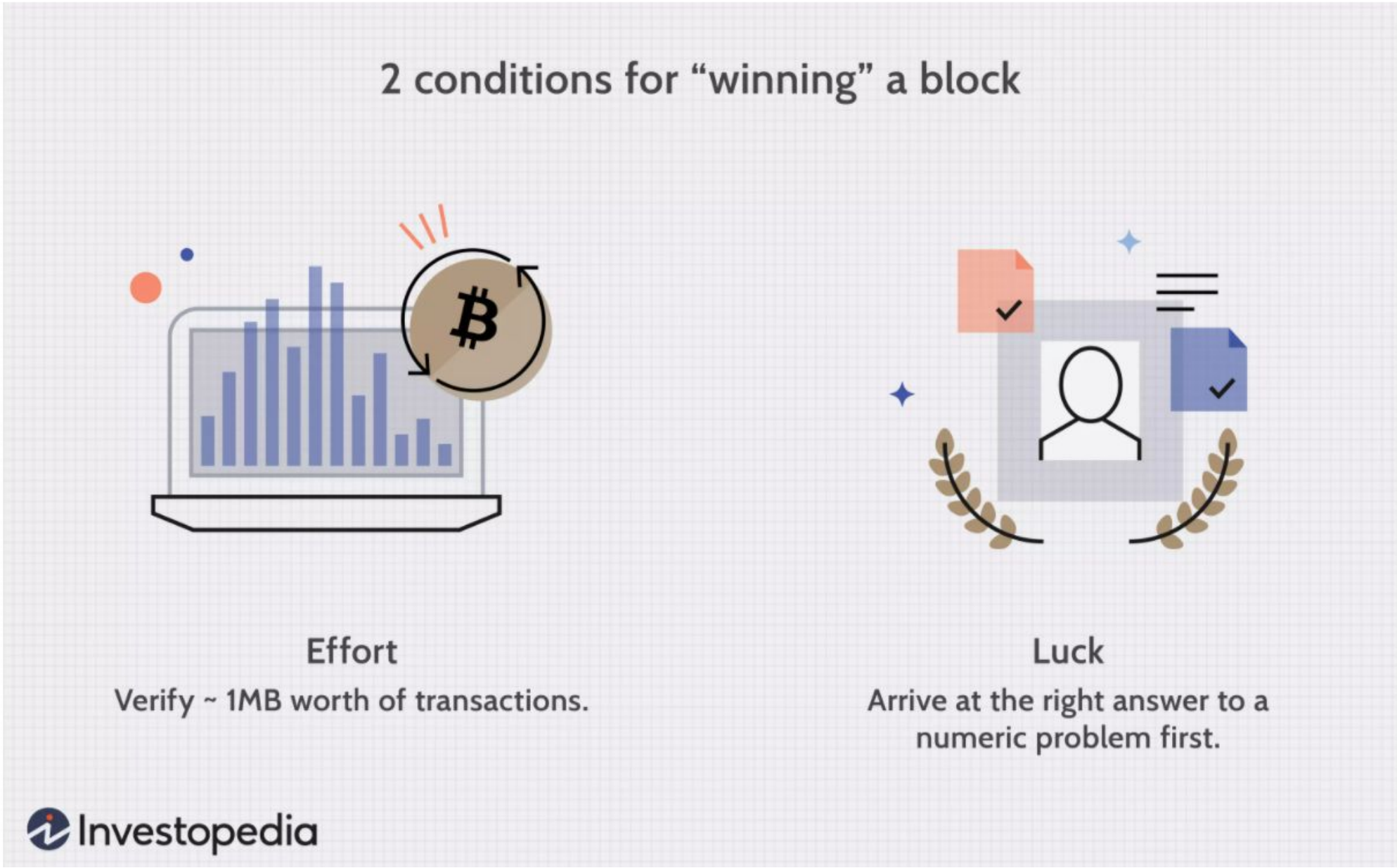
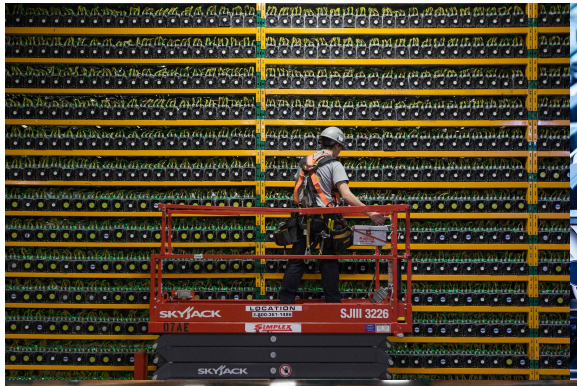


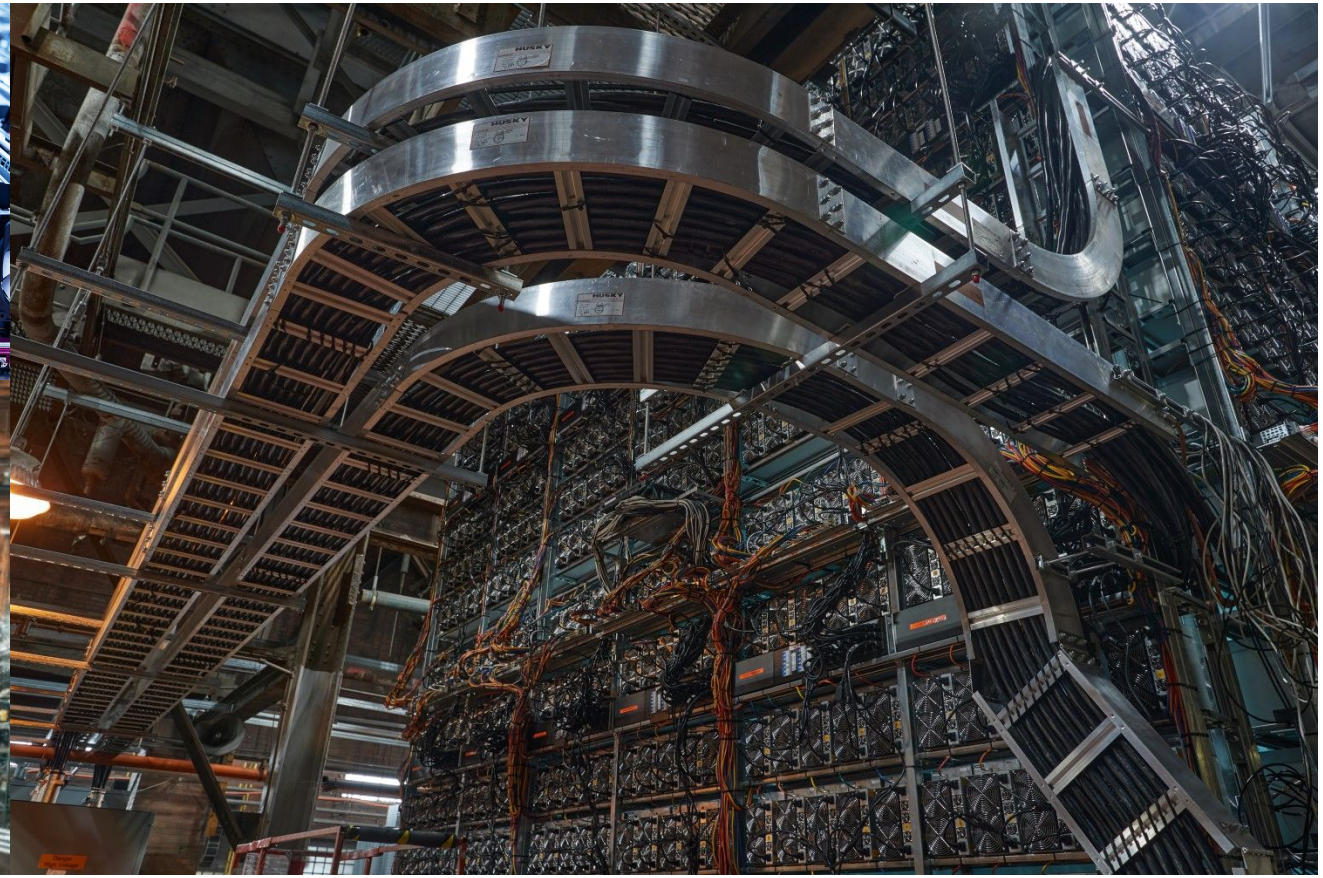
Image by Sabrina Jiang © Investopedia 2021

51% Attack

- When a 51% attack occurs on a blockchain, a single person or organisation gains control of the majority of the hash rate, potentially disrupting the network.
- In this was the case, the attackers would have enough power to exclude or change the order of transactions on purpose.
- They would also be able to stop new transactions from being confirmed, effectively halting transfers between any or all users.
- They could potentially double-spend coins, as they could undo transactions that had already been made while in charge of the network.

Crypto Mining Farms





Halving

When the reward for mining Bitcoin transactions is cut in half, it is known as a Bitcoin halving.

Key Points

- The block reward offered to Bitcoin miners for processing transactions is cut in half every 210,000 blocks mined, or approximately every four years.
- Inflation and the pace at which new Bitcoins enter circulation are both cut in half as a result of the halving.
- Both recent halvings have been linked to extreme boom and bust cycles, with prices ending up higher than they were before the event.
- The reward for each block mined in the chain was 50 Bitcoins in 2009. After the first halving, it was 25, then 12.5, and as of May 11th, 2020, it was 6.25 Bitcoins per block.

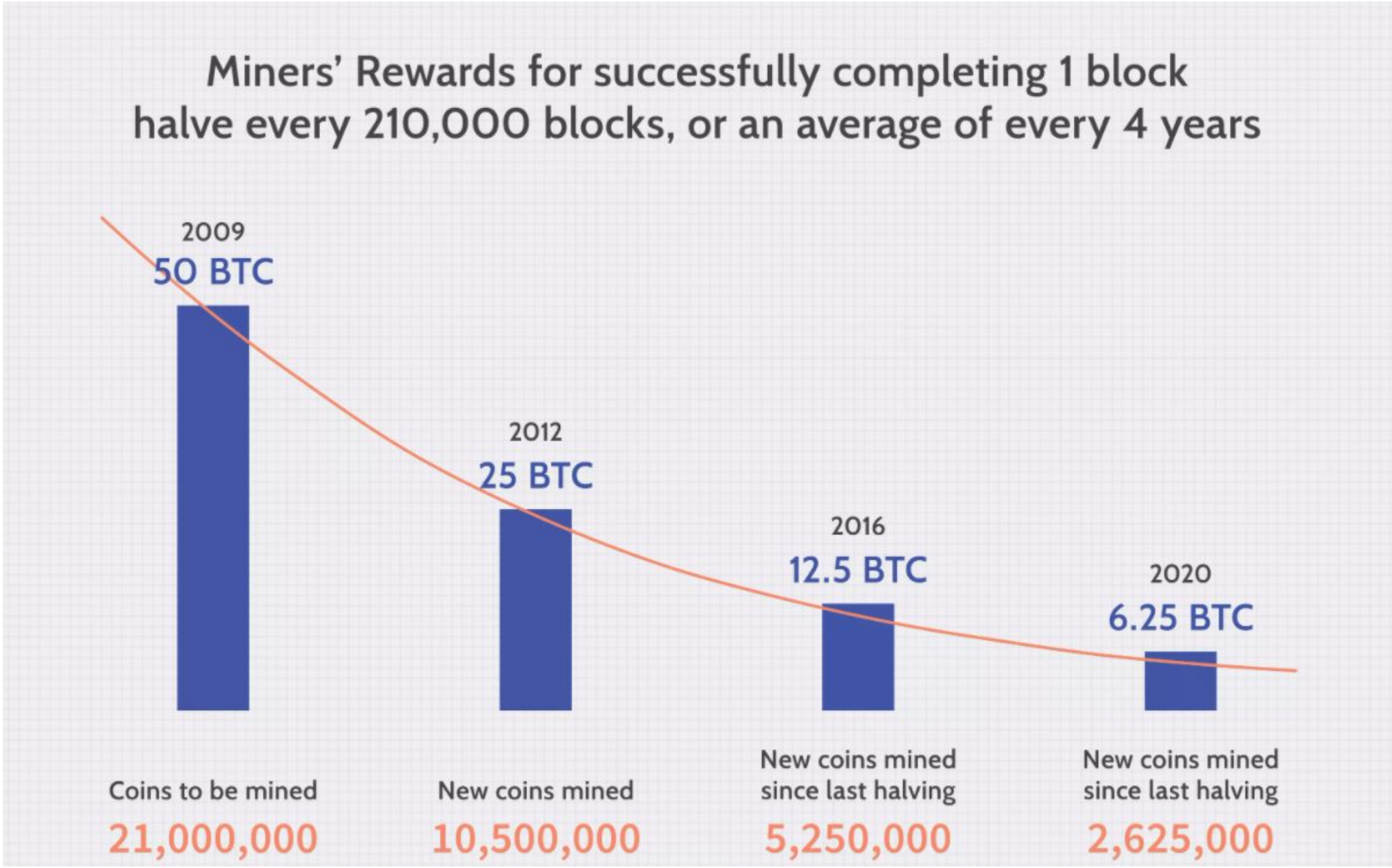


Image by Sabrina Jiang © Investopedia 2021

Future of Halving

- A halving event is important, because it means another reduction in the limited supply of Bitcoin.
- Bitcoin has a maximum supply of 21 million coins.
- This system will be in place until about the year 2140.
- After that, miners will be paid fees for processing transactions.
- These payments ensure that miners continue to be motivated to mine and maintain the network.
- The theory is that after the halvings are completed, there will be enough competition for these fees to keep them minimal.

Bitcoin Price

Bitcoin Price

- The price of bitcoin is influenced by the following factors:
  - Supply and demand
  - Cost of production (mining process)
  - Rewards to miners
  - Exchanges
  - Regulations
  - Internal governance
  - Whale movement
  - Pump and dump activity
  - Media exposure

More info here

Supply and Demand

- The supply of bitcoin is impacted in different ways.
- First, as miners process blocks of transactions, new bitcoins are added into the market, and the rate at which new coins are introduced is programmed to slow down over time.
- Growth decreased from 6.9% in 2016, to 4.4% during 2017 to 4.0% in 2018.
- This can lead to situations where demand for bitcoins grows faster than supply, causing the price to rise.
- The halving of block rewards provided to bitcoin miners has slowed the development of bitcoin circulation.

Supply and Demand p.2

- Second, the amount of bitcoins that the system allows to exist can have an effect on supply (21 million can be ever mined).
- In December 2020, the supply of bitcoin reached 18.587 million, accounting for 88.5% of the total supply of bitcoin accessible.
- Once the full amount of bitcoins is in circulation, prices will depend on its practicality, legal status and popularity compared to other cryptocurrencies.

Competition

- As of March 2021, bitcoin remains the dominant cryptocurrency in terms of market capitalization.
- Altcoins such as Ethereum (ETH), Tether (USDT), Binance Coin (BNB), Cardano (ADA) and Polkadot (DOT), are among the main rivals of bitcoin.
- A vast competition is always good news for investors as it keeps costs down.
- Bitcoin, fortunately, benefits from its popularity, which gives it an advantage over its rivals.

Cost of Production

- Bitcoins and other cryptocurrencies are expensive to produce – by far, the most important factor is the electricity consumption.
- Bitcoin miners compete against each other in a race to solve a difficult cryptographic math problem. The first one to do so is rewarded with a block of newly minted bitcoins as well as any transaction fees accrued since the last block was discovered.
- In order to maintain the block time, the math problem has to be of a certain complexity, but the sharp competition increases said complexity even more, making it, in exchange, more expensive.

Availability on Currency Exchanges

- The more successful an exchange becomes, the more likely it is to attract new users.
- By using its market clout, it can potentially set the rules on how other cryptocurrencies are added in the future.

Regulations and Institutional Acceptance

- Because of the rapid increase in popularity of bitcoin and other cryptocurrencies, regulators are debating how to define them.
- This can have two effects on markets.
- Growing demand:
- Bitcoin is accessible to buyers who otherwise would not be able to afford to buy one
- Driving institutional acceptance
- Tesla and other Fortune 500 businesses add Bitcoin to their balance sheets
- Visa, Mastercard and PayPal add support for crypto payments

Forks and Governance Stability

- Software updates might frustrate the bitcoin community since they take a long time to address and need to be consensus-driven.
- The number of transactions that can be processed is determined by block size, and, currently, bitcoin software can only process about three transactions per second.
- Bitcoin is notorious for its slow transactions, which can push investors towards other faster cryptocurrencies. With the demand of cryptocurrencies, this concern has grown in the recent years
- A modification to the laws controlling the underlaying software, are called “Forks”

Forks

Bitcoin forks are splits in the transaction chain that occur as a result of differing user views on transaction history.

Bitcoin Forks

- A Bitcoin fork changes the rules that Bitcoin must fulfil.
- Miners of that particular Bitcoin blockchain can opt to obey one set of rules or opt for the other ones, with the new rules implemented.
- Without sacrificing the original product, forks allow for a different development structure within the Bitcoin framework.
- As Bitcoin became more popular, the original 1-megabyte blocks, proved to be restricting.
- If a larger block undergoes a fork, it will result in a completely new and independent cryptocurrency.

Bitcoin Forks p.2

- Forks are similar to institutional splits, with one portion of a corporation going in one direction and the other moving in the opposite one.
- Just a few of the nearly 100 bitcoin forks that have occurred to date have managed to gain traction in the altcoin market.
- Bitcoin Cash, Bitcoin SV, and Bitcoin Gold are three of the most well-known.
- Each of them operates independently and follows its own set of rules.
- They are cryptocurrencies, but they are not identical to Bitcoin.

Soft Forks vs Hard Forks

Soft Forks

- Instead of modifying the final product, a soft fork modifies the Bitcoin protocol.
- The soft fork can be used in both directions.
- This ensures the old nodes in the system would accept the new protocol.
- It also means that no new product is being released.

Hard Forks

- Hard forks are newer Bitcoin versions that are entirely different from the original.
- After a hard fork, there are no transactions or interactions between the two forms of Bitcoin.
- They are distinct from one another, and the transformation is permanent.

Bitcoin Hard Forks

Source: Bitcoinmarketjournal.com

BITCOIN MARKET JOURNAL

Bitcoin Metrics

Top 5 Cryptocurrencies

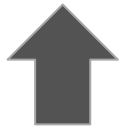
Rank	Name	Symbol	Market Cap	Price	Circulating Supply
1	Bitcoin	BTC	$1,134,372,691,934	$60,722.49	18,681,262 BTC
2	Ethereum	ETH	$249,958,303,587	$2,165.13	115,447,306 ETH
3	Binance Coin	BNB	$88,672,745,247	$573.81	154,532,785 BNB *
4	XRP	XRP	$67,489,683,924	$1.49	45,404,028,640 XRP *
5	Tether	USDT	$45,367,503,967	$0.9995	45,388,521,921 USDT *

Print Date: April 13th 2021 - **Source**: CoinMarketCap.com

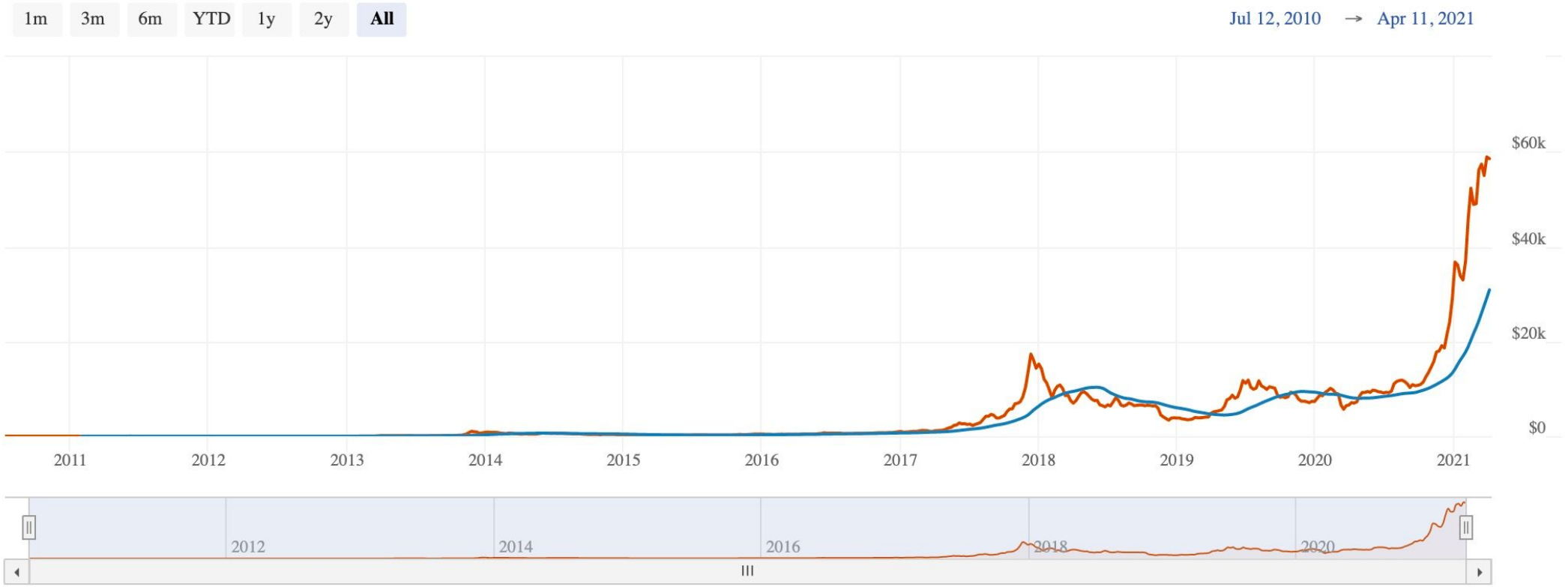
Top 5 Cryptocurrencies

Rank	Name	Symbol	Market Cap	Price	Circulating Supply
1	Bitcoin	BTC	$1,053,726,193,586	$56,390.87	18,686,112 BTC
2	Ethereum	ETH	$255,627,883,497	$2,212.63	115,531,294 ETH
3	Binance Coin	BNB	$78,139,050,564	$509.27	153,432,897 BNB *
4	XRP	XRP	$62,203,606,102	$1.37	45,404,028,640 XRP *
5	Dogecoin	DOGE	$51,732,847,963	$0.4002	129,251,963,658 DOGE

Print Date: April 19th 2021 - **Source**: CoinMarketCap.com



Bitcoin Price



- Daily bitcoin price and 200-day simple moving average. Market is polled every 10 minutes and a daily median is calculated. Historical price goes back to 2010.

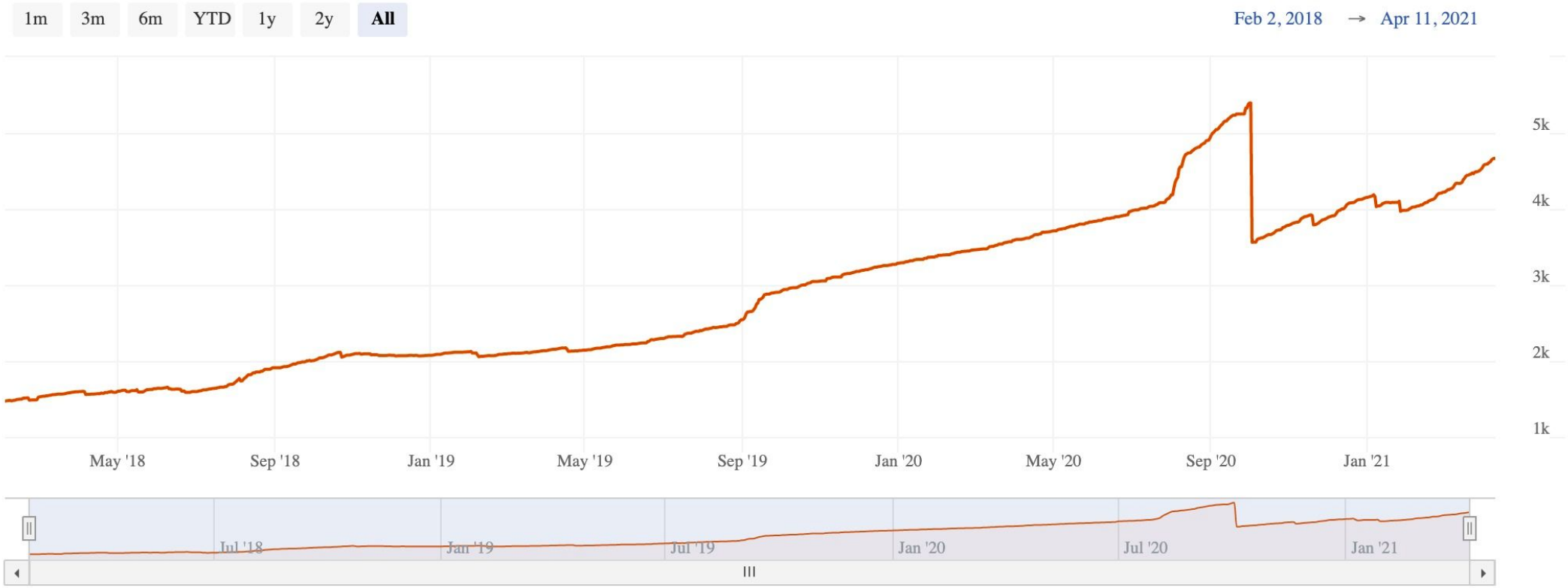
Print Date: April 13th 2021 - **Unit**: US Dollars - **Source**: BitcoinAverage.com / CoinMarketCap.com

Market Capitalization

- Bitcoin market capitalization and market dominance. Capitalization = total supply * price.

Print Date: April 13th 2021 - **Unit**: US Dollars, Percent of Total Capitalization - **Source**: BitcoinAverage.com / CoinMarketCap.com

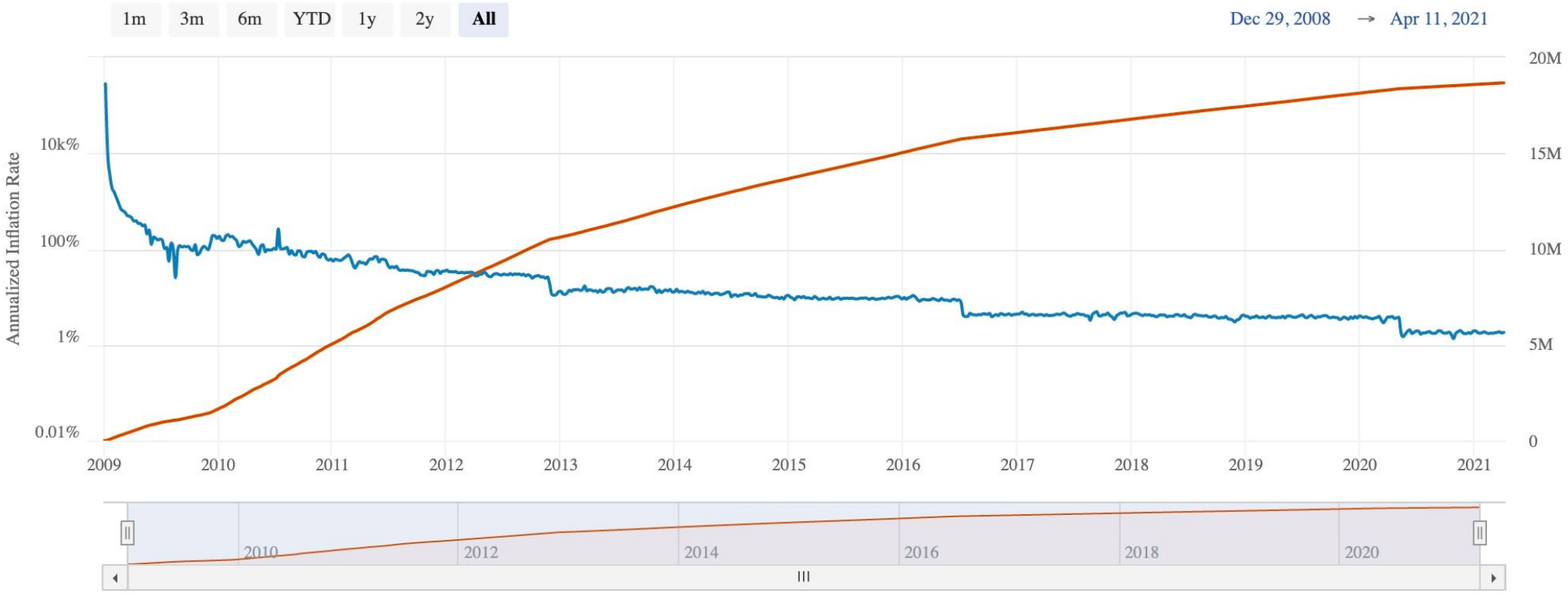
Cryptocurrencies in the Market



- Number of different crypto currencies / coins in the market.

Print Date: April 13th 2021 - **Unit**: Currencies - **Source**: CoinMarketCap.com

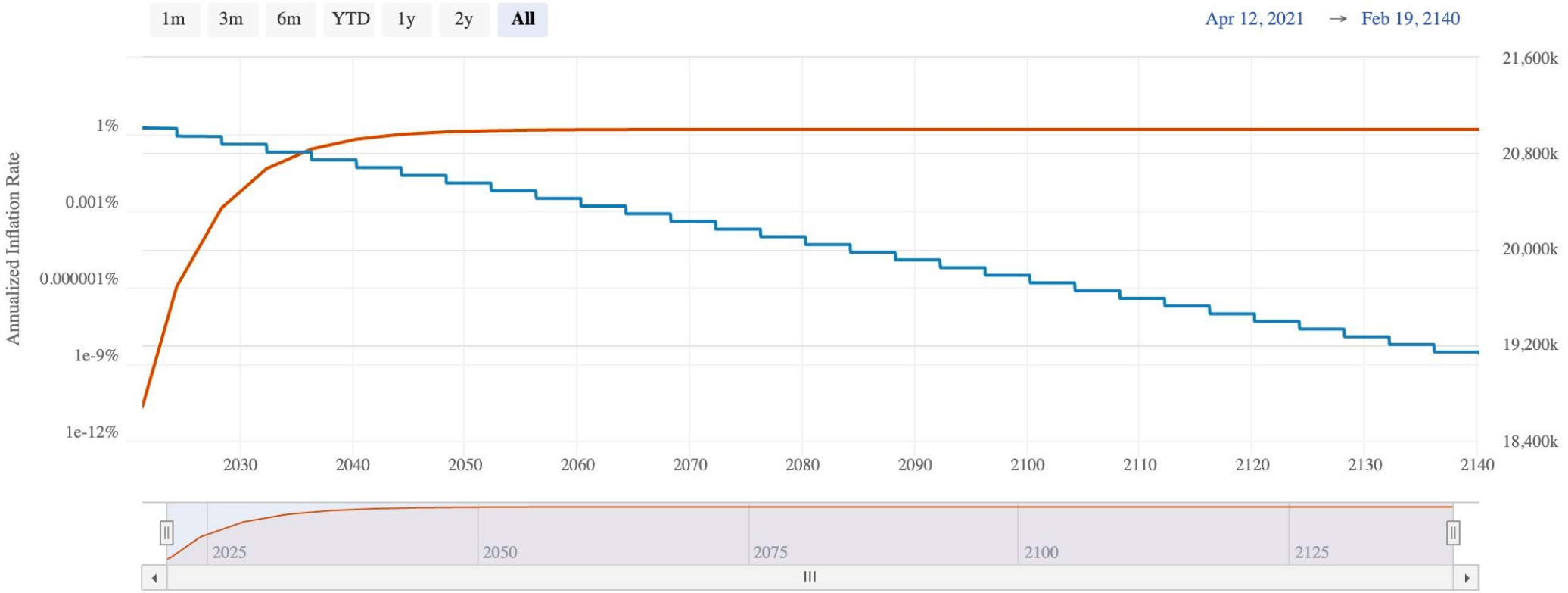
Total Bitcoin Supply



- Total bitcoin supply issued through block rewards which halve every 210,000 blocks. Inflation rate is annualized.

Print Date: April 13th 2021 - **Unit**: Inflation Rate, Bitcoin - **Source**: BitcoinVisuals node (bitcoind)

Future Bitcoin Supply



- Estimate of the future bitcoin supply curve, assuming 10 minute blocks. Bitcoin is issued through block rewards which halve every 210,000 blocks. Inflation rate is annualized.

Print Date: April 13th 2021 - **Unit**: Inflation Rate, Bitcoin - **Source**: BitcoinVisuals node (bitcoind)

Lightning Network

The lightning network is a bitcoin second layer solution that employs micropayment channels to increase the blockchain’s ability to process transactions quicker.

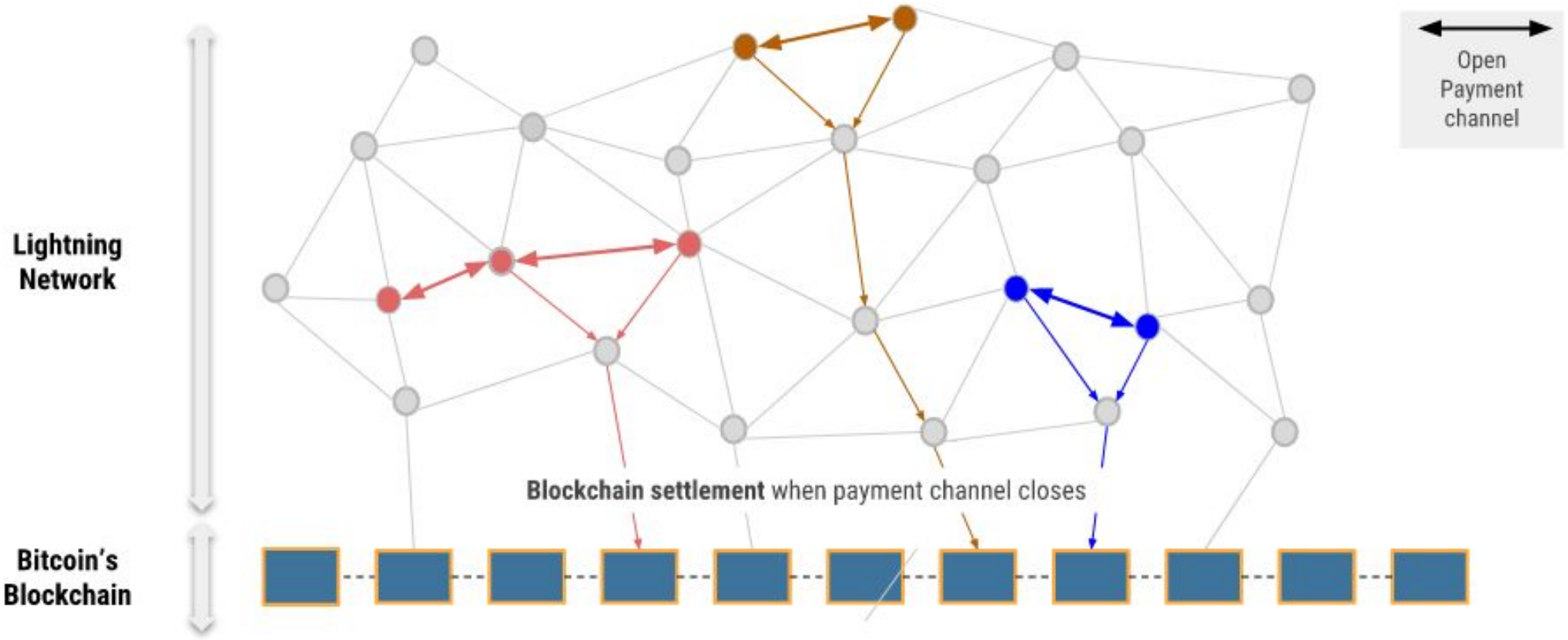
Key Points

- The idea behind it is that not every single transaction on the Blockchain needs to be recorded.
- The Lightning Network opens a channel when two people make multiple transactions between them.
- The Blockchain then only records the opening of said channel.
- Participants can make as many transactions as they want until one of the members decides to close the channel.
- The final balance of the transactions done while the channel was open, will be recorded in the Blockchain.

How does it work: Payment Channel

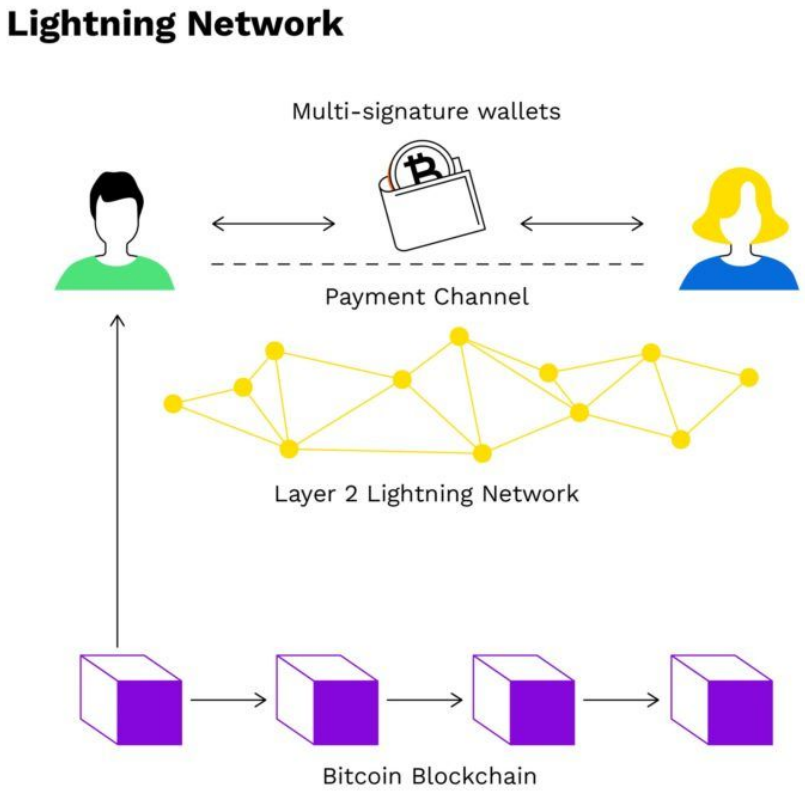
- When a payment channel is opened, the funds that are going to be transferred are locked in it, like in a vault.
- To open said channels, the participants have to commit a certain amount of Bitcoins.
- The two parties exchange a “promise of ownership” for that quantity of bitcoins.
- The channel can be closed at any time, would one of the participants wish to do so.
- Once the channel is fully closed, the final balance is recorded into the Blockchain.

Lightning Network & Payment Channels



Source: TheBlockPro.com

Lightning Network

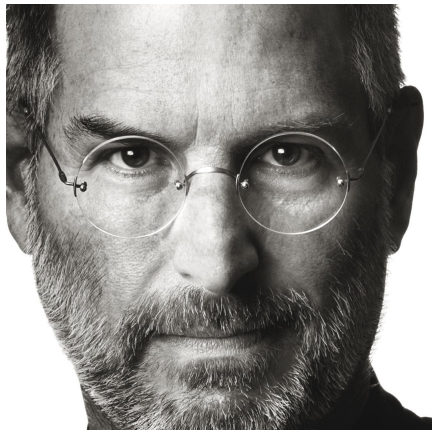


Source: Blockgeeks.com

Fun Facts!

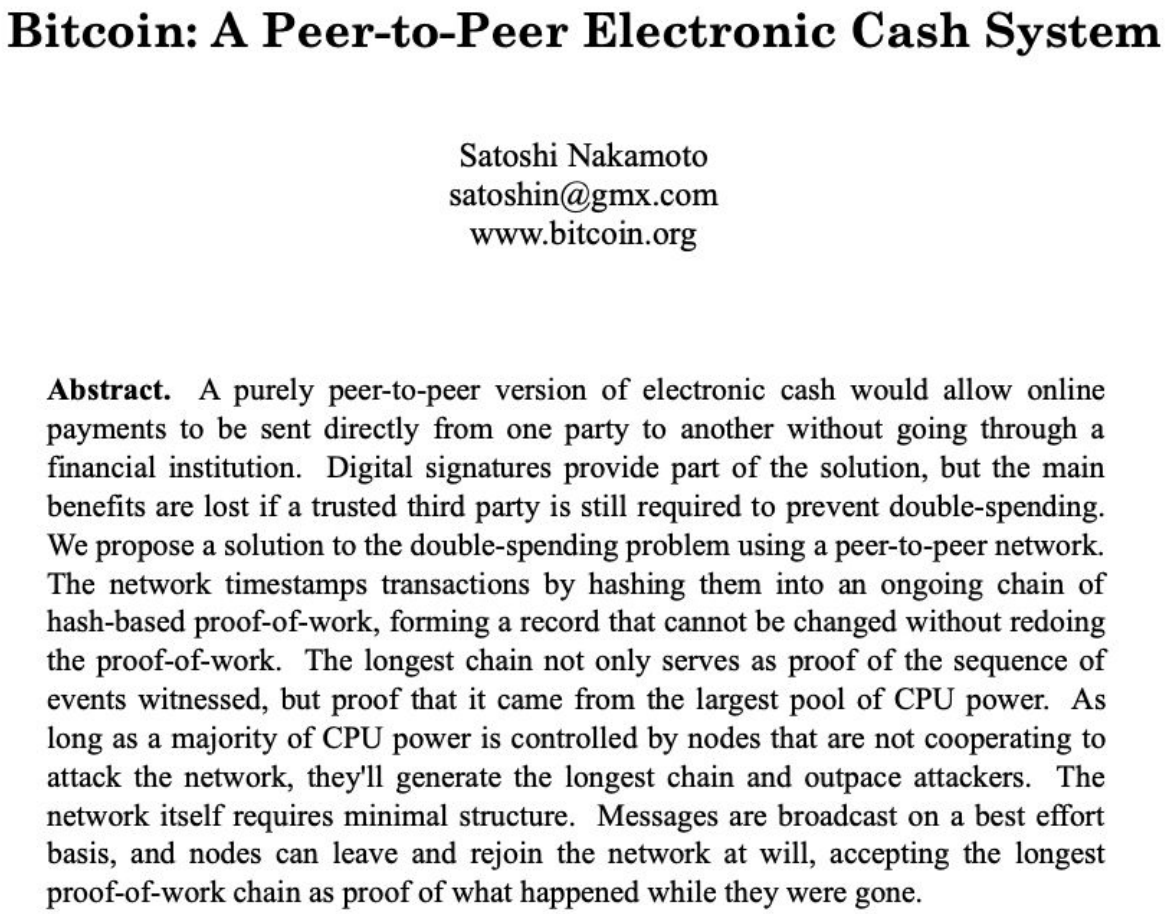
Who is Satoshi Nakamoto ?

- Anonymous creator of Bitcoin
- Could have been any person, group of people, financial institution or even a government.



Bitcoin Bible

- Satoshi Nakamoto produced the original whitepaper in 2009.
- It's called "Bitcoin: A Peer-to-Peer Electronic Cash System
- You can find it online here



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bitcoin Pizza Day - 22nd May

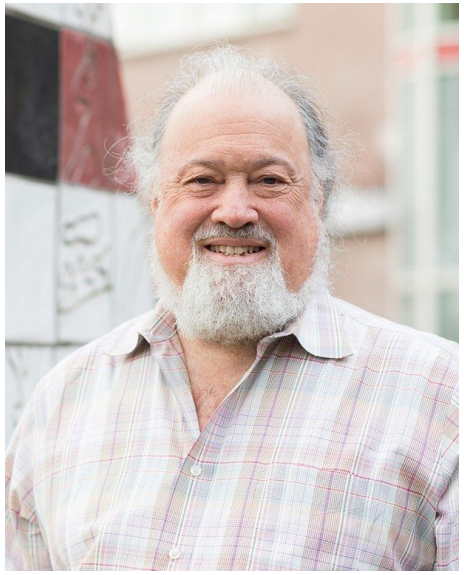
- On May 22, 2010, the first real- world transaction with bitcoin happened.
- Laszlo Hanyecz, a programmer from Florida, traded 10,000 bitcoins for two Papa John's Pizzas.
- At that particular time, 10,000 Bitcoins were worth approx. $41.
- Now, these 10,000 Bitcoins are worth over $64 million.

Liberland

- In April 2015, Vít Jedlička, founded Liberland.
- It’s a micronation between Croatia and Serbia.
- The founder is a politician, publicist, activist and, now, president of Liberland.
- Bitcoin is the official currency of Liberland.
- It has since then been removed from google maps, but you can still find it here.

Digicash

- Digicash was the first cryptocurrency to ever exist.
- In 1989, David Chaum created Digicash based on cryptographic protocols.
- Unfortunately, it wasn’t popular enough and never got materialised.



ReCap

- Governance
- Proof of Work (Pow)
- Consensus
- Mining
- Farms
- Block
- Halving
- Forks/Forking event
- 51% attack

Keywords

- Bitcoin is:
  - a cryptocurrency and blockchain
  - has a limited supply
  - governed by a whitepaper by Satoshi Nakomoto
  - uses PoW as a consensus
  - bitcoin is mined mostly in farms nowadays
  - a new block happens every 10 minutes (LN tries to improve this)
  - Reward halves every 210,000 blocks mined, apx every 4yrs
  - price is volatile
  - supply and demand is a key factor to price going up
  - resources heavy
  - subject to several forks (Bitcoin Cash / Bitcoin SV)

Thanks!

See you in our next session.
Any questions so far?

Session 3

Crypto & Altcoins

Agenda

- **Altcoin**
  - Key Points
- **Best Known Altcoins**
  - Ethereum
  - Monero
  - Bitcoin Cash
  - Litecoin
  - Ripple
  - Binance Coin
  - Dogecoin
- **KPIs for Cryptocurrencies**
  - Market Capitalization
  - Volume (24h)
  - Transaction Volume
  - Exchange Rate
  - Average Confirmation Time
  - Network Hash Rate
  - Hashrate Distribution
  - Number of Users
- **Financial Services**
  - Foundational Financial Services of Crypto
  - Crypto Exchanges
    - Key Points
    - How it works
    - Special Considerations
    - Most Popular Crypto Exchanges
  - Crypto Wallets
    - Key Points
    - Hardware Wallets
    - Paper Wallets
    - Desktop Wallets
    - Mobile Wallets
    - Online/ Web Wallets
    - Cold vs. Hot Storage
    - Custodial vs. Non-Custodial
  - Merchant Processors
    - Key Points
    - Likely Initial Areas of Adoption

Altcoin

Altcoins are all other alternative cryptocurrencies other that are not bitcoin.

Key Points

- An “alt-coin” is a form of payment that is based on the basic concepts of Bitcoin but differs or improves in its execution.
- Many people have developed their own “alt – currencies,” with their own laws and networks.
- Some older concepts, such as Ripple, have been enhanced by blockchain innovation and have grown into their own entities.
- While some are minor tweaks to the Bitcoin protocol with a small audience, others are intriguing sources of innovation.
- Although Bitcoin is the king, several alt-coins have received a lot of acceptance.
- These new coins have different attributes and generate their own blockchains that are independent to the Bitcoin blockchain, using the original open source software with a few modifications.

Best Known Altcoins

- Currently more than 5,000 altcoins
- Some of the best-know coins are: Ethereum (ETH), Litecoin (LTC), Cardano (ADA), Polkadot (DOT), Bitcoin Cash (BCH), Stellar (XLM), Chainlink, Binance Coin (BNB)

Ethereum (ETH)

- Ethereum is one of the most popular and globally funded projects.
- Ethereum's goal is to establish a decentralised range of financial opportunities that anyone in the world, regardless of nationality, ethnicity, or beliefs, can use for free.
- The Ethereum blockchain may run any decentralised application's programming code.
- Rather than having to create a new blockchain for each new application, Ethereum allows developers to create several applications on a single platform.
- Ether is the cryptocurrency of Ethereum. It is mined and fuels the network.

Monero (XMR)

- Monero saw the light in 2014, initially as a fork of Bytecoin.
- Monero allows its users to select to selectively disclose their transactional history to selected parties.
- It has always focused on providing strong privacy while offering optional transparency.
- Monero has a dynamic fee mechanism and a changeable block size.
- It employs an encrypted public ledger, which allows anyone to send or record transactions while keeping the source, amount, and destination hidden from outside observers.

Bitcoin Cash (BCH)

- Bitcoin Cash was created as a result of a fork from Bitcoin.
- It was established in 2017
- This blockchain’s block size is 8 MB.
- Miners can earn more transaction fees if there are more transactions in a block.
- Approximately 2 million transactions may be handled each day, compared to 250k transactions per day for Bitcoin.

Litecoin (LTC)

- Litecoin is an open-source software project and a peer-to-peer cryptocurrency.
- Starting in October 2011, it was an early bitcoin spinoff or cryptocurrency.
- Litecoin is nearly identical to Bitcoin.
- In comparison to Bitcoin’s 10 minutes, the Litecoin Network promises to process a block every 2.5 minutes.
- As a result, Litecoin can confirm transactions significantly more quickly than Bitcoin.

Ripple (XRP)

- Ripple is a distributed open source protocol that supports tokens representing fiat cash, bitcoin, commodities, or other units of value such as frequent flier miles or mobile minutes.
- It was launched in 2012 and is based on a distributed open source protocol.
- Ripple claims to be able to facilitate “secure, instantaneous, and almost free worldwide financial transactions of any size with no chargebacks.”
- The native cryptocurrency of the Ripple Ledger is XRP.

Binance Coin (BNB)

- Binance Coin (BNB) is a the official cryptocurrency of the Binance crypto exchange.
- Binance Exchange is one of the most popular crypto exchanges in the world,
- Binance accepts and trades other major cryptocurrencies like, such as Bitcoin, Ethereum, Litecoin, etc.
- BNB was launched in 2017 and worked with the ERC-20 token on the Ethereum blockchain before becoming the native currency of Binance’s own blockchain, the Binance Chain.

Dogecoin (DOGE)

- Dogecoin was created as a fun and unconventional payment system.
- The logo of Dogecoin is the face of the Shiba Inu dog from the “Doge” meme, reinforcing the “fun” concept behind DOGE
- Launched in 2013, it quickly became a fan favourite
- Dogecoin’s block time is 1 minute as opposed to Litecoin’s 2.5 minutes.

Stablecoin

Stablecoins are a type of cryptocurrency whose value is determined by another more stable asset, such as gold or fiat currency.

Key Points

- There is usually an Usually, the entity behind a stablecoin will set up a "reserve" where it securely stores the asset or basket of assets backing the stablecoin – for example, $1 million in an old-fashioned bank (the kind with branches and tellers and ATMs in the lobby) to back up one million units of a stablecoin.
-
- This is one way digital stablecoins are pegged to real-world assets. The money in the reserve serves as collateral for the stablecoin – meaning whenever a stablecoin holder wishes to cash out their tokens, an equal amount of whichever asset backs it is taken from the reserve.
-
- Cryptocurrency's unpredictability comes in contrast to the generally stable prices of fiat money, such as U.S. dollars, or

Key Points

- Originally, stablecoins were primarily used to buy other cryptocurrencies, like bitcoin, because many cryptocurrency exchanges didn’t have access to traditional banking.
- They are more useful than country-issued currencies because you can use them 24 hours a day, seven days a week, anywhere in the world – without relying on banks. Money transfers take seconds to complete.
- Another useful feature of stablecoins is that they can work with so-called smart contracts on blockchains, which, unlike conventional contracts, require no legal authority to be executed.
- This makes stablecoins programmable in ways that dollars can’t be.
- Worried that stablecoins could pose risks to the financial

Stablecoins vs Altcoins

Stablecoins

- Instead of modifying the final product, a soft fork modifies the Bitcoin protocol.
- The soft fork can be used in both directions.
- This ensures the old nodes in the system would accept the new protocol.
- It also means that no new product is being released.

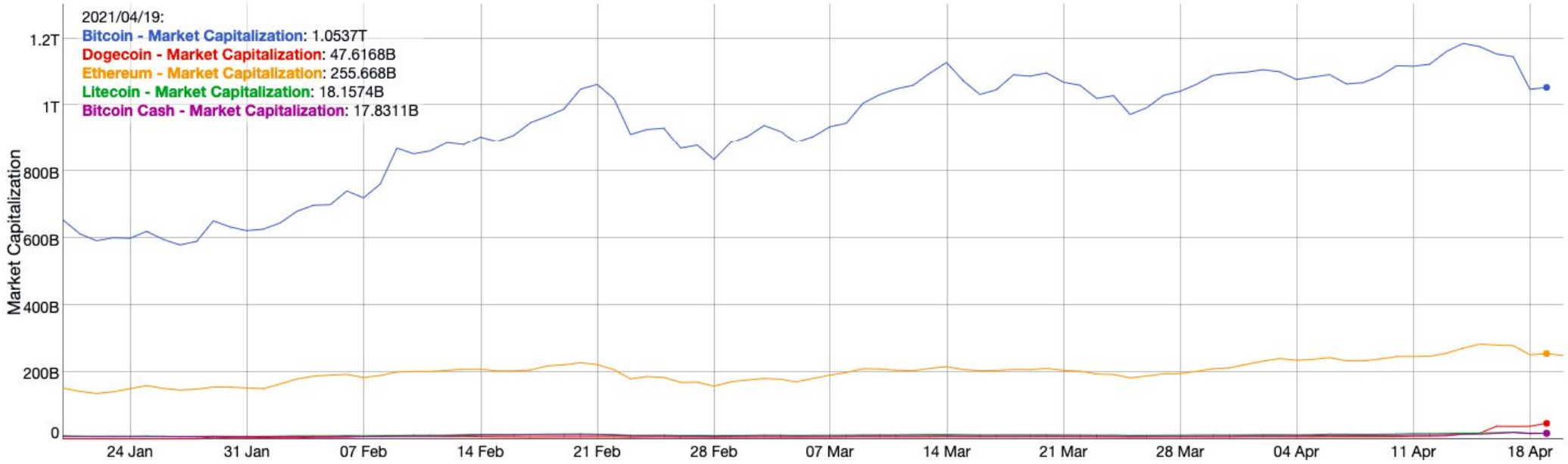
Altcoins

- But one key drawback is that cryptocurrencies' prices are unpredictable and have a tendency to fluctuate, often wildly.
-
-

KPIs for Cryptocurrencies

Market Capitalization

- Market capitalisation is a term that calculates and tracks a cryptocurrency's market worth.
- This metric compares the current value of each coin to major conventional (fiat) currencies.
- It is determined by the current price * by the circulating supply.



Print Date: April 20th 2021 - **Source**: bitinfocharts.com

Volume (24h)

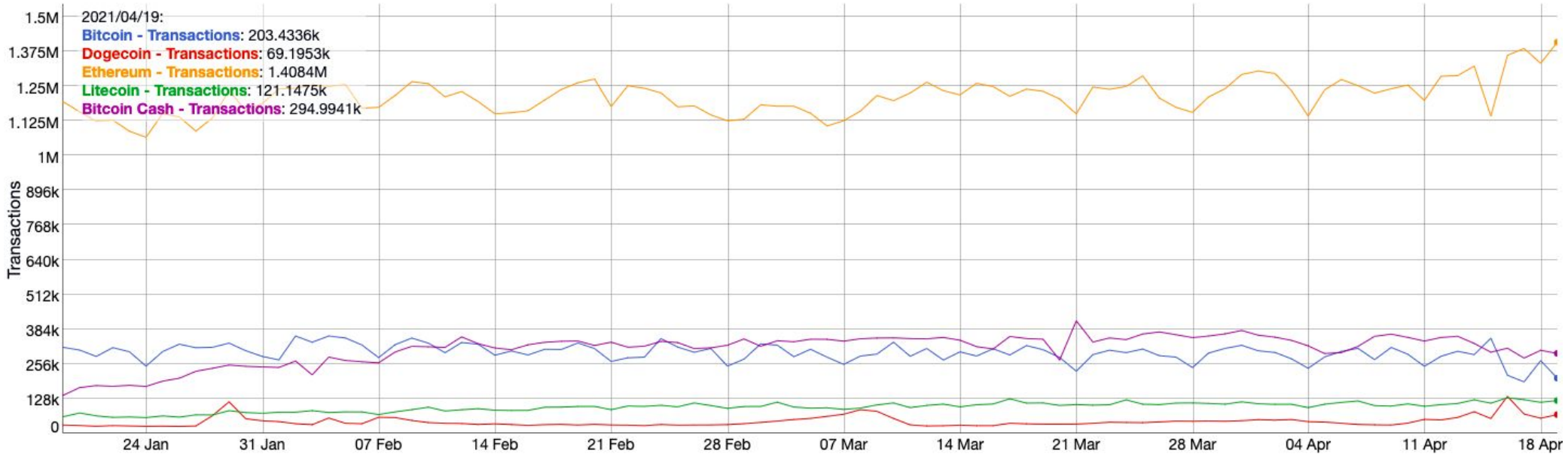
- The trading volume measures the number of coins that have been traded and/ or exchanged in that particular time period, usually 24 hours.
- The 24-hour trading volume of a cryptocurrency refers to how much of a coin's value has been bought and traded in a single day.

Rank	Name	Symbol	Market Cap	Price	Circulating Supply	Volume(24h)
1	Bitcoin	BTC	$1,028,572,732,106	$55,043.30	18,686,612 BTC	$66,335,775,788
2	Ethereum	ETH	$245,925,502,650	$2,128.46	115,541,464 ETH	$35,370,127,224
3	Binance Coin	BNB	$76,532,374,694	$498.80	153,432,897 BNB *	$6,211,435,761

Print Date: April 20th 2021 - **Source**: CoinMarketCap.com

Transaction volume

- Measures the number of transactions that have happened over time as well as the amount of coins involved in said transactions.



Print Date: April 20th 2021 - **Source**: bitinfocharts.com

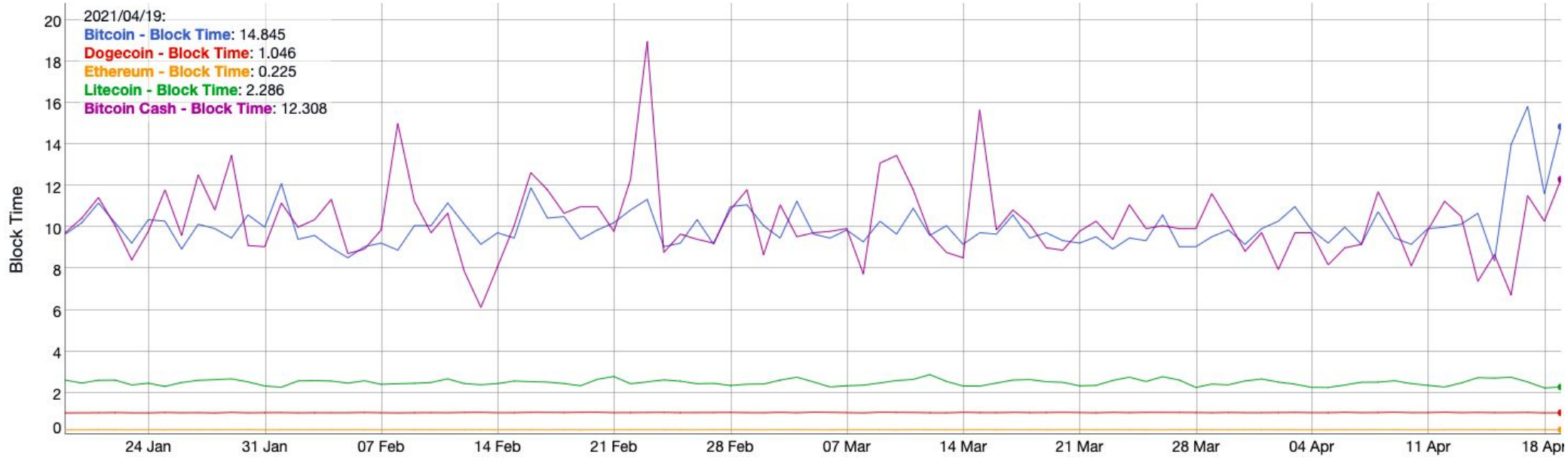
Exchange Rate

- The value of one currency in relation to another.
- An exchange rate is the rate at which one national currency is exchanged for another.
- Exchange rates can be fiat vs. fiat, crypto vs. fiat or crypto vs. crypto.

Print Date: April 20th 2021 - **Source**: Google.com

Average Confirmation Time

- The average confirmation time, also known as block time, is the time it takes for a transaction to be confirmed on the blockchain.
- The confirmation time of Bitcoin is about 10 minutes. Newer cryptocurrencies have a much lower block time.



Print Date: April 20th 2021 - **Source**: bitinfocharts.com

Network Hash Rate

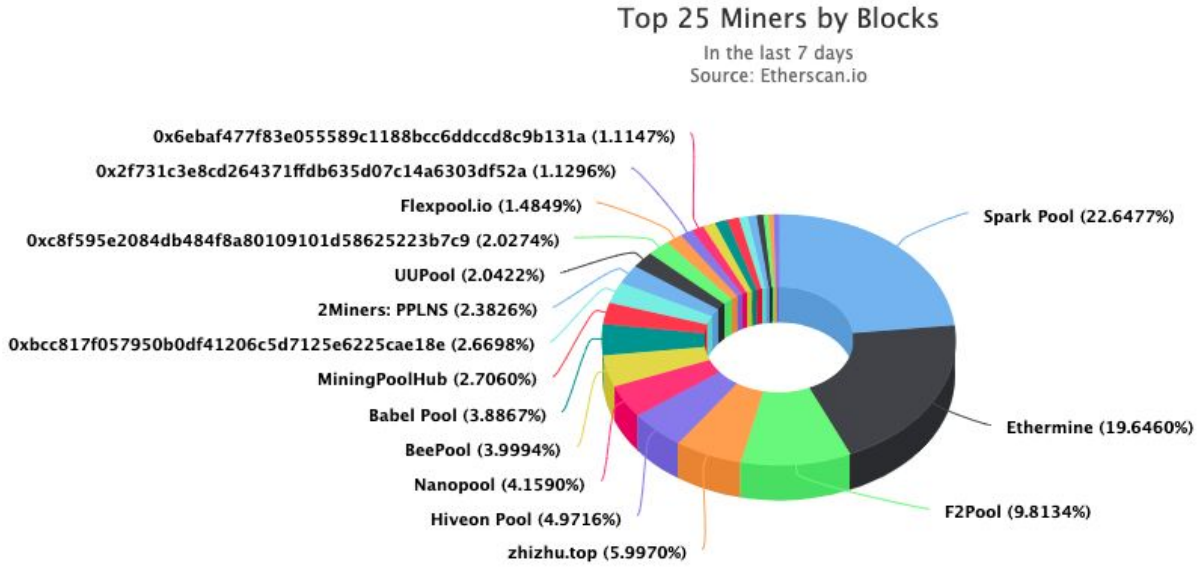
- This metric is the network's processing power.
- It gives an indication of the current difficulty in the mining process.
- Difficulty refers to the complexity to generate a SHA-256 hash for a candidate block.

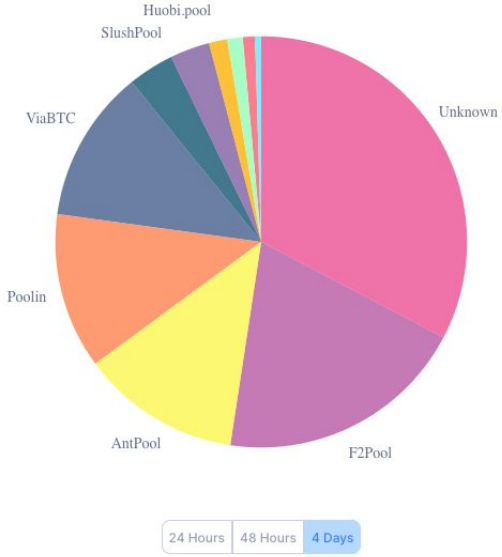
Date	Value
April 19, 2021	151.23M
April 18, 2021	154.29M
April 17, 2021	164.85M
April 16, 2021	172.58M
April 15, 2021	165.79M
April 14, 2021	169.40M
April 13, 2021	169.73M
April 12, 2021	171.70M
April 11, 2021	171.87M
April 10, 2021	167.60M
April 09, 2021	165.62M
April 08, 2021	166.12M
April 07, 2021	164.70M
April 06, 2021	163.71M
April 05, 2021	161.53M
April 04, 2021	162.23M
April 03, 2021	165.39M
April 02, 2021	163.51M
April 01, 2021	164.90M

Print Date: April 20th 2021 - **Source**: ycharts.com

Hashrate Distribution

- With the Hashrate Distribution you can identify the biggest mining pools and their contribution to the whole blockchain.
- This metric is never 100% accurate and it should only be used as a rough estimate.

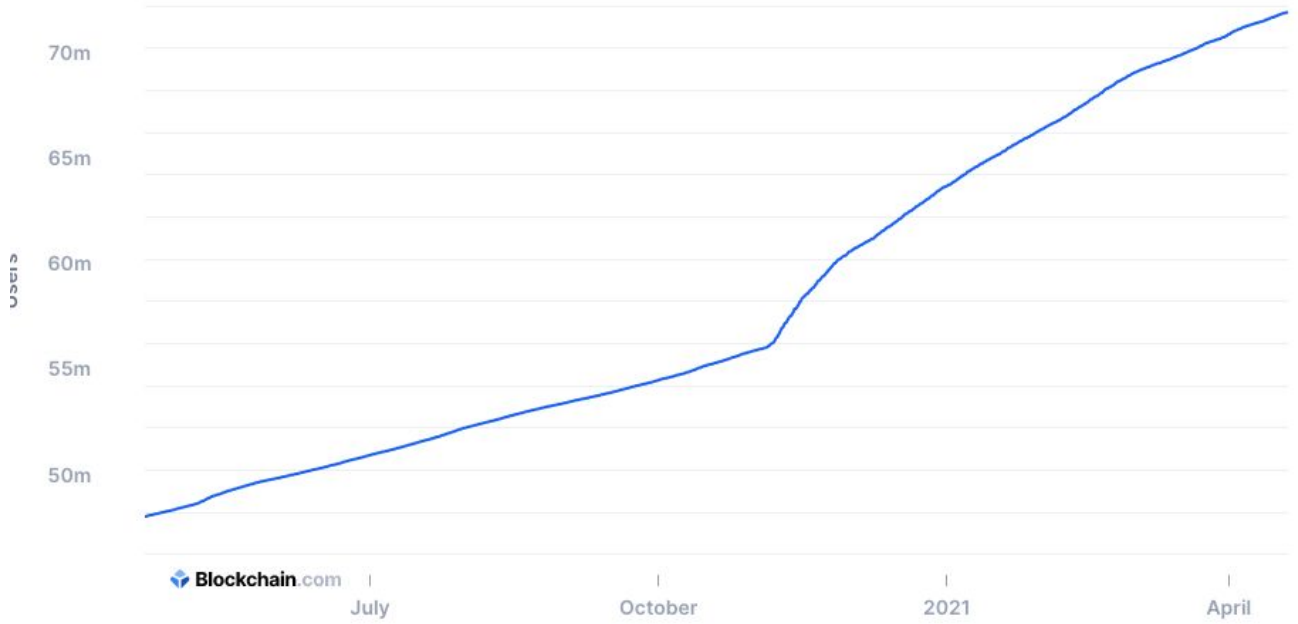




Print Date: April 20th 2021 - **Source**: etherscan.io/ blockchain.info

Number of Users

- Probably the most important parameter, ins the popularity of a cryptocurrency.
- Although the number of users can only be measured by the downloads of wallets, it’s a pretty good indicative of the user acceptance.
- Users can have one or more wallets, from any provider, so these number can never be absolute.



Print Date: April 20th 2021 - **Source**: blockchain.com

Financial Services

Foundational Financial Services of Crypto

- The following are the basic components of cryptocurrency financial services:
  - Cryptocurrency Exchanges
  - Crypto Wallets
  - Merchant Processing Services
- Once properly established and integrated, they will become the core of the payment system.

Crypto Exchanges

It’s an online marketplace where traders can buy and sell cryptocurrencies using fiat and/or digital currencies.

Key Points

- A crypto currency exchange is an online platform where you can exchange and trade cryptocurrencies.
- It acts as an intermediary between buyers and sellers, or to use crypto terminology, between a “maker” and a “taker.”
- A bitcoin or crypto exchange works like a stockbroker, you open an account and you can deposit money via bank transfer and other popular deposit methods.
- It works similarly to exchanging money at a bank or exchange bureau: you will pay a currency conversion fee and, in exchange, you will get your new currency.

How it works

- The first step to start trading and exchanging cryptocurrencies is to open an account with a selected crypto exchange and pass the verification process.
- After this initial authentication process, verified users can fund their crypto exchange to start using the digital platform.
- You can deposit funds with different payment methods, check your exchange to see which ones are available for you.
- In order to withdraw funds, you can do so by choosing from one of the available payment methods.

Special Considerations

- **Fees**
  - Some crypto exchanges might charge fund transfer fees, when making deposits and withdrawals. This also depends on the payment method chosen to transfer funds.
  - In cases where your own currency is not accepted, you might have to pay conversion fees.
  - As a general rule, most of the crypto exchanges have transaction fees, that apply after each completed buy and sell order.
- **Important:** Crypto exchange is NOT a crypto wallet.
  - The crypto exchange is a trading platform, the crypto wallet is a digital storage service only.
  - Most crypto exchanges also offer wallets, but they might charge a fee for this addition service.

Most Popular Crypto Exchanges

Crypto Wallets

A cryptocurrency wallet is a storage system that holds your public and/or public keys. It can be a physical device, digital program or paid online service.

A wallet is software that holds all your addresses. Use it to send bitcoins and manage your keys. [...] A wallet is simply a collection of addresses and the keys that unlock the funds within.

Antonopoulos, Mastering Bitcoin

Key Points

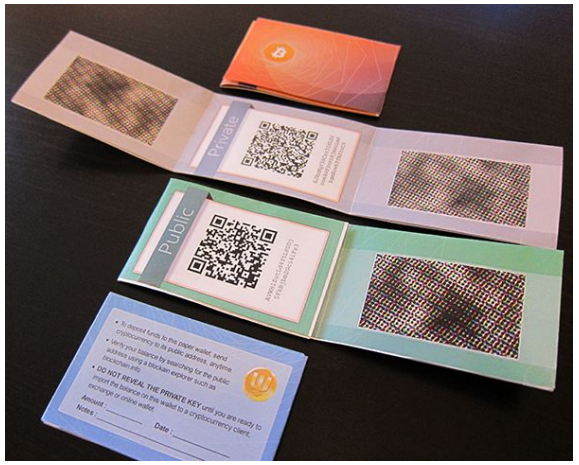
- Since cryptocurrencies are fully digital, you will never be able to hold a physical bitcoin or altcoin, so, in order to store them, you will need a private key.
- Crypto wallets don’t really store your cryptocurrencies; instead, they store your private key, which gives you access to all of them.
- There are **5 types of crypto wallets**:
  - Hardware wallets
  - Paper wallets
  - Desktop Wallets
  - Mobile Wallets
  - Web Wallets.

Hardware Wallets

- A physical piece of hardware that can be used to store your cryptocurrencies.
- Hardware wallets are also referred to as cold storage and non-custodial.
- It is the safest type of wallet as it’s an offline storage.
- You plug it to your computer when you need to manage your funds.

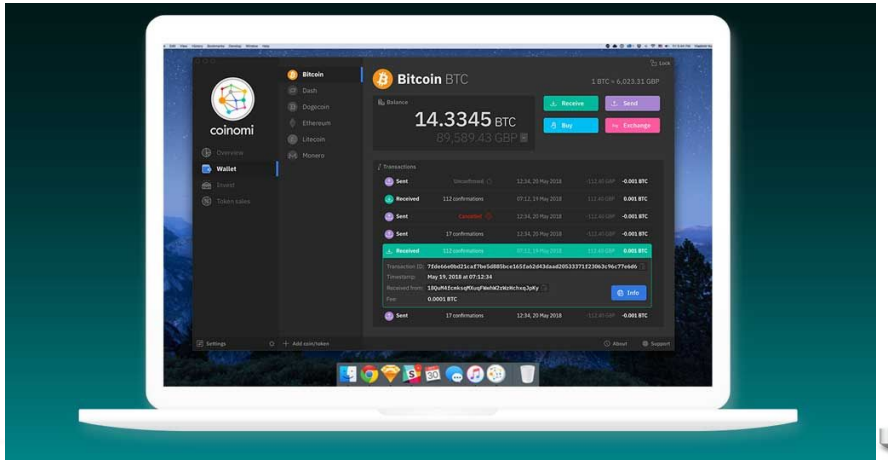
Paper Wallets

- A paper wallet is a printed version of your key, which contains the key itself and a QR code, which is used for transactions.
- It’s also an offline storage wallet, and, thus more secure than online options, but it’s also easy to loose and it an fade with time.
- It is now an outdated type of wallet.



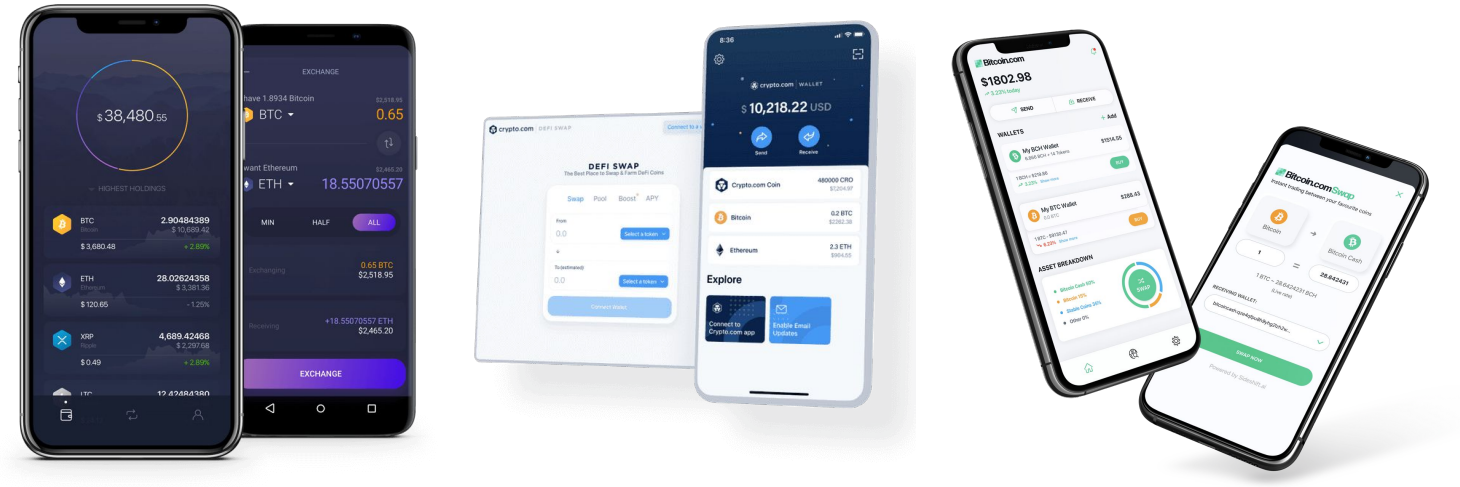
Desktop Wallets

- Desktop wallets are installed on your computer, need internet access and provide control over you wallet from your device.
- They work as an address for the user to send and receive crypto.
- You can also store your private key.



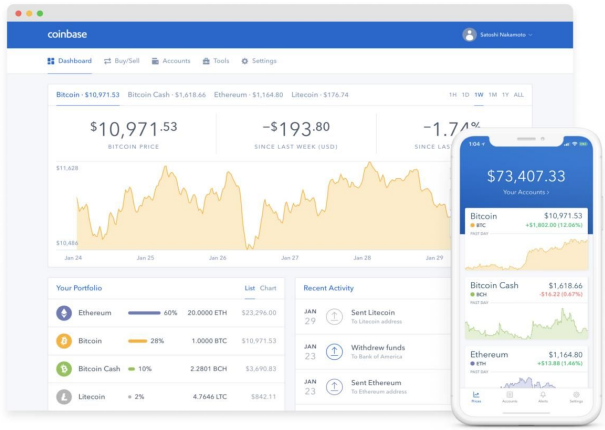
Mobile Wallets

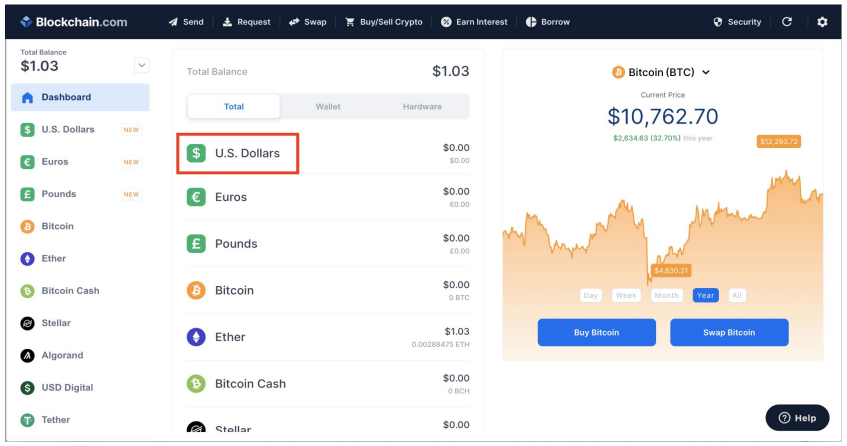
- Mobile wallets or wallet apps, are wallets downloadable on your mobile phone.
- Most desktop and online wallets come with the mobile app as well.
- Some crypto exchanges include a mobile wallet, and vice-versa.
- Since it’s an online platform, it’s a custodial wallet and hot storage.

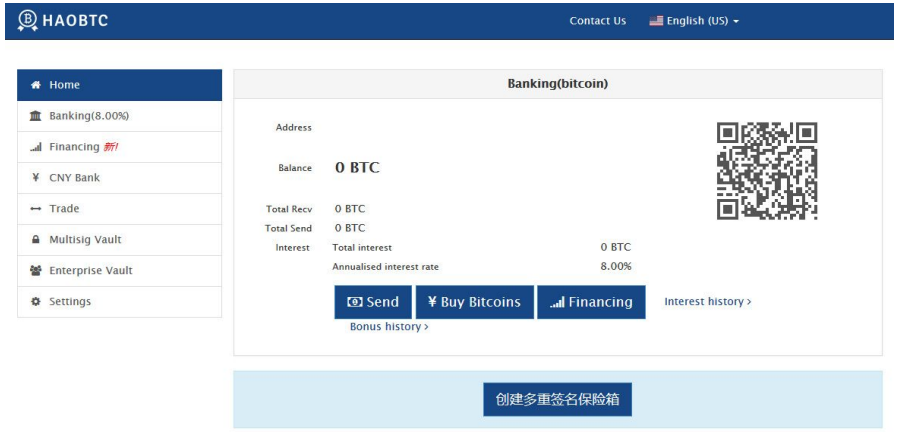


Online/ Web Wallets

- With online wallets, you don’t need to download any software to your computer or phone, meaning you can connect anywhere, anytime.
- Unfortunately, the main drawback is that it’s more vulnerable to hacking, than other wallets.







Cold vs Hot Storage

Cold Storage

- It is disconnected from the internet, completely offline, making it the safest crypto wallets.
- Cold storage wallets include: Hardware wallets (physical devices, like a pen drive) and paper wallets.

Hot Storage

- Hot wallets are the best option if you’re currently trading or exchanging crypto.
- Connected to the internet
- Hot wallets are vulnerable to online hacking, change in regulations and technical difficulties.

Custodial vs Non-Custodial Wallets

Custodial

- A custodial wallet keeps your private keys and digital assets safe, meaning you can always recover. It offers a backup.
- If you lose your private key, you can always recover it.
- It offers, for most parts, free and instant transactions.

Non-Custodial

- No one else, except you, own your private key.
- It is the safest way of owning crypto, since it’s not connected to the internet, safe from external cyber attacks.
- But a lost wallet, also means total loss of your funds and crypto.
- Non-custodial wallets are cold storage, like hardware and paper wallets.

Merchant Processors

Merchant processors allow business to accept cryptocurrencies as payment method.

Key Points

- They are the equivalent to fiat currency merchant processors (First Pay, WorldPay, Elavon, Authorize.net, Square, etc) for the most popular payment methods (Visa, Mastercard, American Express, etc).
- They include the integration into the business' website and shopping cart, and the conversion into legal tender after the purchase.
- Common payment systems use a "pull" mechanism, in which they take funds from your account and route them via a vast and complicated network.
- With bitcoin payments it's different, as only two parties have access to the transaction and only at the time that it's being made. This is called a "push" mechanism.

Likely Initial Areas For Adoption

- **Online Products:** affordable merchant fees for vendors
- Sensitive Products: HIV tests, pregnancy tests, pornography, etc.
- **High-Risk Vendors:** giving access to their credit card/credit line to “risky” vendors.
- **International Customers:** chargeback frauds are avoided due to the irreversible nature of cryptocurrency transactions.
- **Open Bazaar :** It’s a peer to peer e-commerce application, that it’s expected to grow in popularity paving the way for similar e-commerce sites.

Thanks!

See you in our next session.
Any questions so far?

Session 4

Agenda

- **Decentralized Finance**
  - Key Points
  - DeFi vs Traditional Finance
  - Most Popular DeFi Applications
  - DeFi and Ethereum
  - Ethereum DeFi Map
- **Smart Contracts**
- **Initial Coin Offering**
  - Key Points
- **Banking**
  - Central Banks vs Cryptocurrencies
  - Central Bank Digital Currency
    - Key Points
    - Key Differences
- **Crypto Regulations**
  - Key Points
  - USA
  - EU
    - EU - Malta
    - Malta - Key Regulatory Timestamps
    - Malta - Notable Blockchain Companies
    - Other European territories
  - UK
  - Central and South America
  - Asia
- **Connecting BC and Crypto Companies**
  - Quantum Supremacy
  - AI
  - IoT
  - Big Data
  - Blockchain Landscape
- **Quiz Time**

§

Decentralized Finance

DeFi

Decentralised finance, or DeFi, tries to re-create conventional financial instruments by removing intermediaries through technology.

Key Points

- Decentralised finance uses blockchain technology to offer traditional financial services.
- In DeFi, blockchain expands its uses from simple transactions to more complex services.
- You might have heard the term “Open Finance” before, which was the first aim to implement the concept of DeFi.
- Most DeFi applications are built on the Ethereum blockchain, the world’s second-largest cryptocurrency platform.

DeFi vs. Traditional Finances

DeFi

- You are the sole owner of your money
- You control where your money goes and how it's spent.
- Transactions happen within minutes
- Your activity remains pseudonymous
- Open 24/7
- It is built on transparency

Traditional Model

- Your money is held by a company or third party
- You have to trust the bearer of your money
- Transactions are partially processed manually, which delays them.
- You might be denied certain financial services due to your origin, identity, etc.
- Financial institutions are closed books

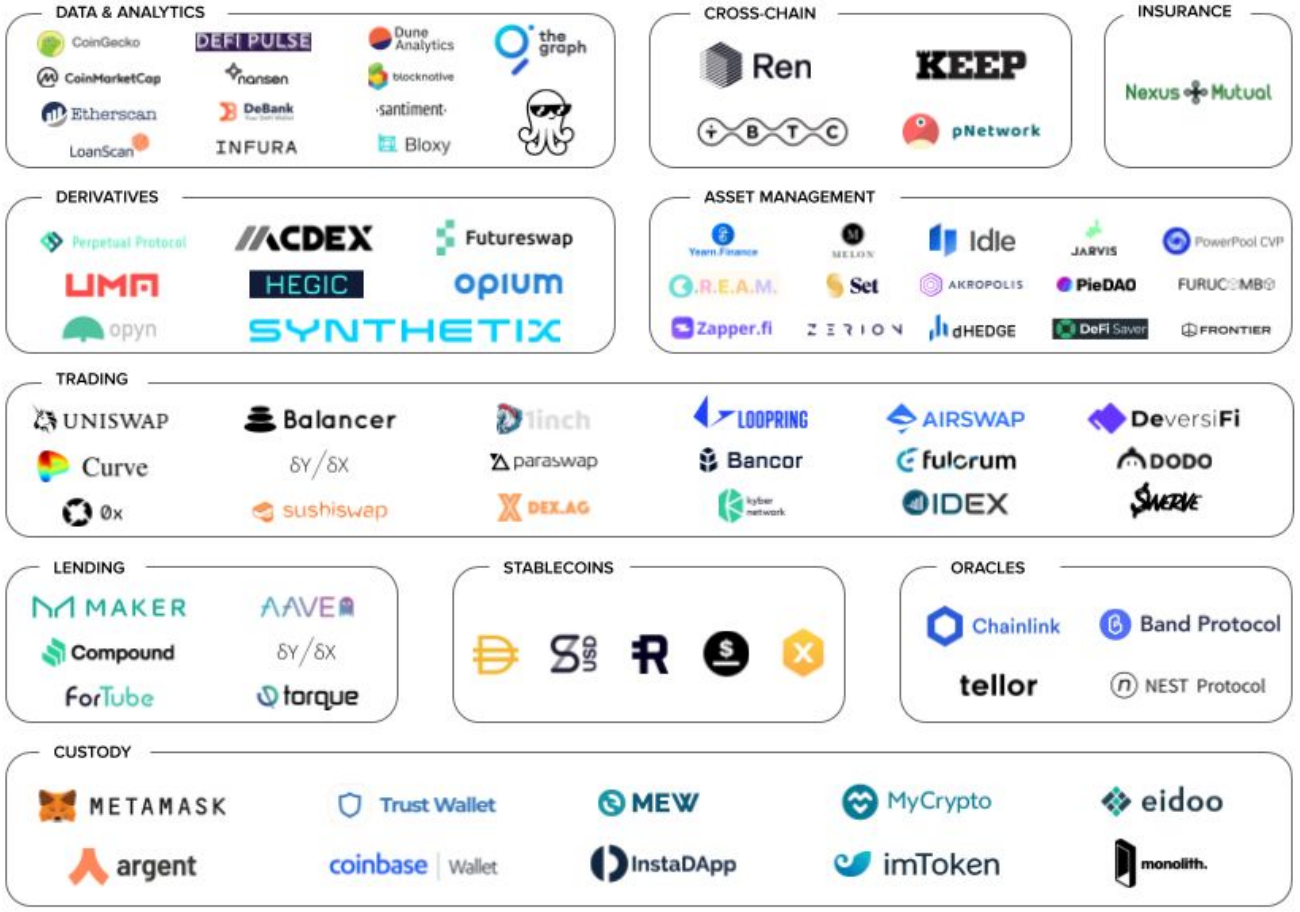
Most Popular DeFi applications

- **Decentralised exchanges (DEXs):** Users are connected directly with one another, there is no need for intermediaries in order to exchange money.
- **Lending platforms:** Lenders and borrowers of cryptocurrencies are connected via smart contracts.
- **“Wrapped” bitcoins (WBTC):** A way of sending bitcoin to the Ethereum network so the bitcoin can be used directly in Ethereum’s DeFi system.
- **Prediction markets:** Betting markets for future events, such as elections. The goal is to create reliable predictions, without interference of intermediaries and/ or manipulations.

DeFi and Ethereum

- DeFi runs in the Ethereum Blockchain.
- Ethereum's platform uses smart contracts, which execute transactions automatically when certain predetermined conditions are met.
- No one owns Ethereum or the smart contracts that live on it.
- Since most of Ethereum's products will never take custody of your funds, it allows complete financial freedom, leaving you in control.

Ethereum DeFi Map



Source: Reddit

ethereum

Smart Contracts

A smart contract is self-executing piece of code that enforces transactions verifiable on the Ethereum blockchain.

Key Points

- Smart contracts are a key element of the Ethereum network and essential for the blockchain.
- Most of the contractual clauses are, partially or fully, self-executing, self-enforcing, or both.
- The main goal is to provide a superior security and a cheaper alternative to traditional contractual laws.
- These contracts are autonomous, decentralised and transparent, meaning they are irreversible and unmodifiable once deployed.

%

Initial Coin Offering

ICO

Initial Coin Offerings (ICO) are a popular fundraising method used primarily by crypto and blockchain startups.

Key Points

- It’s usually launched by a crypto company looking to raise funds to create a new coin, app, or service.
- Supporters of the project buy some of the project’s tokens (coins) with fiat- or digital currency in exchange of the newly-created coins.
- It works similarly to a company shares sold to investors during an Initial Public Offering (IPO).
- As in any investment, some ICOs have yielded massive returns for investors but others have turned out to be a fraud or have failed.

Key Points p.2

- ICOs differ from crowdfunding in that crowdfunding is mainly done from donations, while the backers of ICOs are motivated by a prospective return on their investments.
- ICOs are also called “crowdsales.”
- Since ICOs are, mainly, completely unregulated, investors need to do research and be cautious when investing in new coins.
- The best way to stay ahead of new ICOs is to stay informed and follow the latest news.


$
Banking

Central Banks vs Cryptocurrencies

- In each country there is a financial entity that defines and supports the monetary system of their nation. That is a central bank.
- The most common functions handled by Central Banks are: monetary stability, financial stability, regulation, policy operations management and financial infrastructure provisioning.
- Since cryptocurrencies are not issued by a state (or central bank), they are not considered legal tender.
- Most of cryptocurrencies provide a very light set of central banking functions like setting monetary policy, payment/transfer services and issuance/distribution of new ‘coins’/units.

Central Banks vs Cryptocurrencies

Central Bank General Functions	Central Bank Detailed Functions	Cryptocurrencies
Monetary Stability Functions	Monetary Policy	Monetary policy fixed at inception, but can be changed by majority of miners.
	Exchange Rate Policy	No
Financial Stability & Regulatory Functions	Prudential Policy Supervision	No
	Supervision/ Oversight	No
Policy Operation Functions	FX Intervention	No
	FX Reserves *	No
	Lender of Last Resort	No
Financial Infrastructure and Provision Functions	Currency Provision	Yes, through block rewards
	Banking/ account management services	No
	Payment system (inter-bank)	Yes
	Settlement system of central bank money	Cryptocurrencies have a built in payment system that, from one point of view, merges a variety of traditional payment and settlement systems.
	Other settlement systems	
	Registry Provision	No

Central Bank Digital Currency

Digital currency issued by a central bank

Key Points

- Central bank digital currencies (CBDC) are also known as digital fiat currencies.
- CBDC is aimed to be a high-security digital instrument.
- It is a means of payment, a unit of account, and a store of value, just like normal currencies.
- Like paper currency (or coins), each unit of CBDC is uniquely marked to prevent counterfeit.
- Currently most central banks are looking into digital currencies, which CBDCs mostly remaining in the hypothetical stage.
- China issued the first ever digital currency, done by a major economy, the digital RMB.

Key Differences

- The main difference is the governance: a CBDC is centrally controlled, whilst cryptocurrencies use a blockchain or other distributed ledger technology.
  - CBDC does not use blockchain technology
- Like any third party-controlled digital asset, the main risk of CBDCs is that the issuer/ authority of the Central Bank Digital Currency can manipulate, add or remove money from anyone's account remotely with the flip of a switch.
  - Cryptocurrencies are protected against this kind of threat by ensuring that more than 50% of the mining power is in agreement before proceeding with any action.

Crypto Regulations

Key Points

- For a currency to be considered legal tender, it has to be recognised by another nation-state, preventing cryptocurrencies to be formally recognised as currency.
- Even if it’s not a currency for legal purposes, cryptocurrencies almost certainly are property /assets instead.
- In 2013, The U.S. Treasury classified bitcoin as a “convertible decentralised virtual currency”.
- In September 2015, it as was also classified as a commodity by the Commodity Futures Trading Commission, CFTC.
- Per IRS, bitcoin is taxed as a property.

USA

- According to IRS – “virtual currency” is considered property for tax purposes.
- Buying cryptocurrency with USD is not a taxable event.
- Income and expenses generated in cryptocurrencies are taxed and as per regular standards.
- Crypto earned through mining is treated as ordinary income. i.e. you have to report the value at the time you are awarded the coin.
- Keep and eye on Wyoming (Caitlin Long – LN) ‘#Wyoming will recognize #DAOs as a new type of LLC, effective July 1!’

EU

- In 2014 bitcoin was classified as a convertible decentralised virtual currency by the European Central Bank (ECB).
- Since a regulatory regime was still not in place, the European Banking Authority advised European banks not to deal in virtual currencies just yet.
- In 2015 it was dictated that VAT/GST is not applicable to the conversion between traditional fiat currency and bitcoin.
- As of 2020 Crypto exchanges and wallet providers must be under the “Anti-Money Laundering Directive”.
- Small European nations such as Malta, Cyprus, Austria and Estonia, are embracing new technological trends and pacing the future of blockchain and cryptocurrencies.

EU - Malta

- Cryptocurrencies are recognised by the government as “a medium of exchange, a unit of account, or a store of value”, but not as legal tender.
- The financial regulator in charge of cryptocurrency exchanges in Malta is the Malta Financial Services Authority, or MFSA.
- There is no specific cryptocurrency tax legislation, nor is VAT applicable to transactions exchanging fiat currency for crypto.
- Three new laws are enabling blockchain based businesses: The Malta Digital Innovation Authority Bill, The Technology Arrangements and Services Bill and the Virtual Financial Assets Bill.
- The Malta Gaming Authority has expressed interest in integrating and allowing the use of cryptocurrencies by MGA licensees.

Malta - Key Regulatory Timestamps

- **2018:** parliament passed three bills establishing a comprehensive regulatory foundation for blockchain and digital currencies.
- Malta is promoted as the “Blockchain Island”
- **2020:** With only 26 of the initial 83 companies applying for licence, and none granted to date, all signs point to the fact that many entities found the VFA’s requirements too demanding.

Malta - Initial “Blockchain Island” Enthusiasm

Joseph Muscat @JosephMuscat_JM · Mar 23, 2018

Welcome to #Malta @binance. We aim **to** be the global trailblazers in the regulation of blockchain-based businesses and the jurisdiction of quality and choice for world class fintech companies -JM @SilvioSchembri

World's Biggest Cryptocurrency Exchange Is Heading to Malta

Binance, the world's largest cryptocurrency exchange by traded value, is seeking a fresh start in the Mediterranean.

bloomberg.com

246 1.8K 3.8K

Silvio Schembri @SilvioSchembri · Apr 13, 2018

Welcome to #Malta . The Blockchain Island. @binance @cz_binance @JosephMuscat_JM

30 223 839

Malta - Popular Blockchain Companies (with hesitation)

- **Binance / Binance Labs:** Established in 2017, Binance is a global-reaching digital currency exchange. It is also maintaining its own digital currency BNB and proprietary blockchain. Binance is no longer based in Malta as of today (year 2021)
- **Pacific:** Pacific offers a blockchain-powered payments system for social media and e-commerce that utilises smart QR codes.
- **Changelly:** Changelly is a popular crypto-exchange that allows for the purchase and exchange of more than 150 digital currencies and digital assets.

Malta - Notable Blockchain Companies p.2

- **Komodo Platform:** Komodo Platform is a popular and open smart-chain platform built on a multi-chain architecture.
- **BitPay:** Established in 2014, BitPay is a digital currency and digital assets exchange.
- **Chillz:** Fan Tokenisation
- **Stobox:** Stobox, which was founded in 2018, is a platform enabling small and medium-sized businesses to issue digital securities.

Other European territories

- **Slovenia:** Mining and businesses selling goods/ services in bitcoin are taxed.
- **Switzerland:** Bitcoin businesses may need a banking licence and are subject to anti-money laundering regulations.
- **Norway:** Bitcoin is an asset and falls under the sales tax regulation.
- **Sweden:** Subject to Financial Supervisory Authority regulations and treated as currency exempt of VAT.
- **Germany:** “Unit of account” and can be used for tax and trading.
- **Russia:** The use of other currencies beside the Ruble, is illegal. Crypto is considered a high risk asset

UK

- For the purpose of taxation, crypto assets are considered property.
- A capital gains tax (CGT) liability may become due if a gain is made on disposal.
- The CGT threshold for UK taxpayers is £12,300 per tax year, as at 6 Apr 2020.
- Airdrops and forks are mentioned in the guidance.
- Much like shares, crypto assets can be pooled.

Central and South America

- **Argentina, Brazil and Chile:** bitcoin and other cryptocurrencies are legal, but unregulated.
- **Bolivia:** Bitcoin activities were banned by the Central Bank of Bolivia in 2014. 60 cryptocurrency promoters were arrested in May 2017
- **Ecuador:** The government banned bitcoin and other cryptocurrency activities in 2014, however use of Bitcoin still grows until now.
- **El Salvador:** In 2021, El Salvador becomes the first country to adopt bitcoin as currency.

Asia

- **Lebanon** and **Jordan** have issued warnings on the use of Bitcoins, but it is still legal.
- **Japan** recognises cryptocurrencies as a method of payment.
- **Singapore** recognises cryptocurrency transactions as barter sales for tax purposes
- Cryptocurrencies are illegal in **Kyrgyzstan** and **Bangladesh**
- **India** bans the purchases/ sales of crypto but expressed believe in blockchain technologies
- In early January 2018, **China** took a hostile position for local miners. This hostility has continued and during the year 2021, the government has shown a very negative approach towards crypto.

Connecting

Blockchain & Crypto Companies

Quantum Supremacy

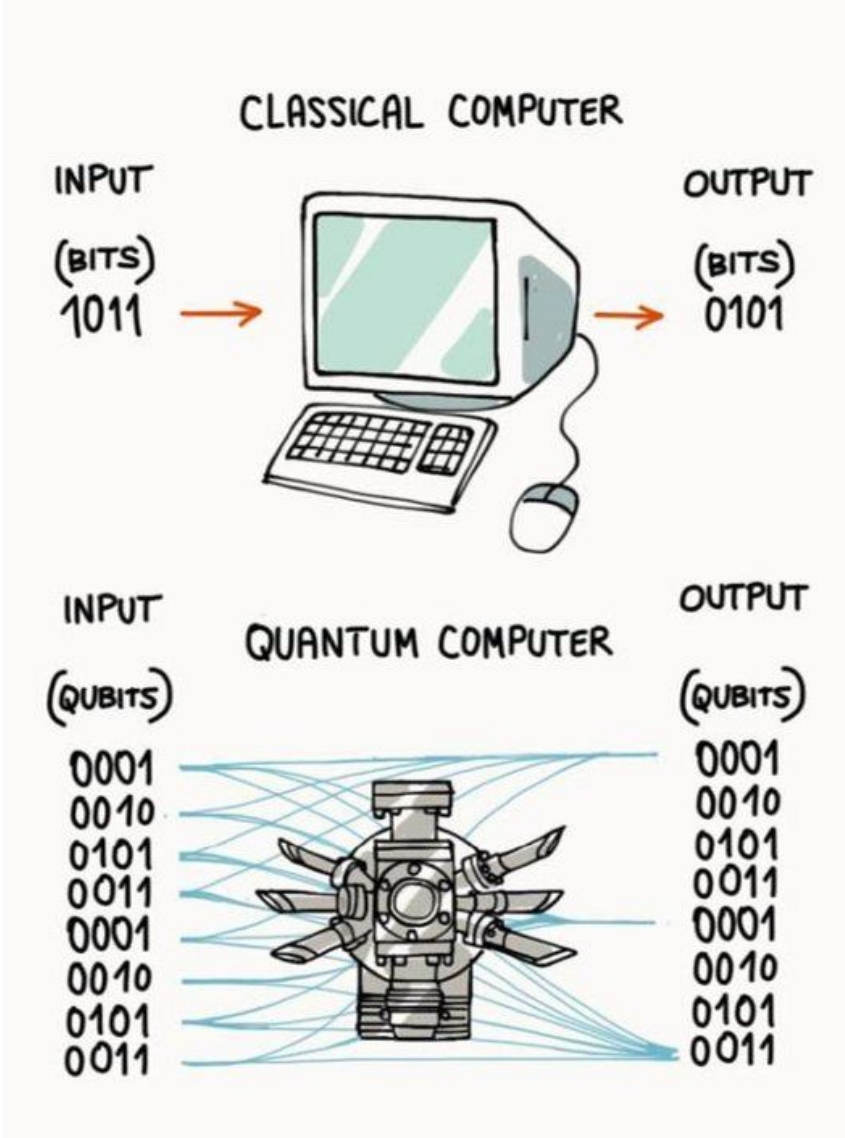
Quantum supremacy, or quantum advantage, is the idea that a computer based on quantum physics can solve a problem in record time, something that no conventional computer could do in a reasonable amount of time.

Key Points

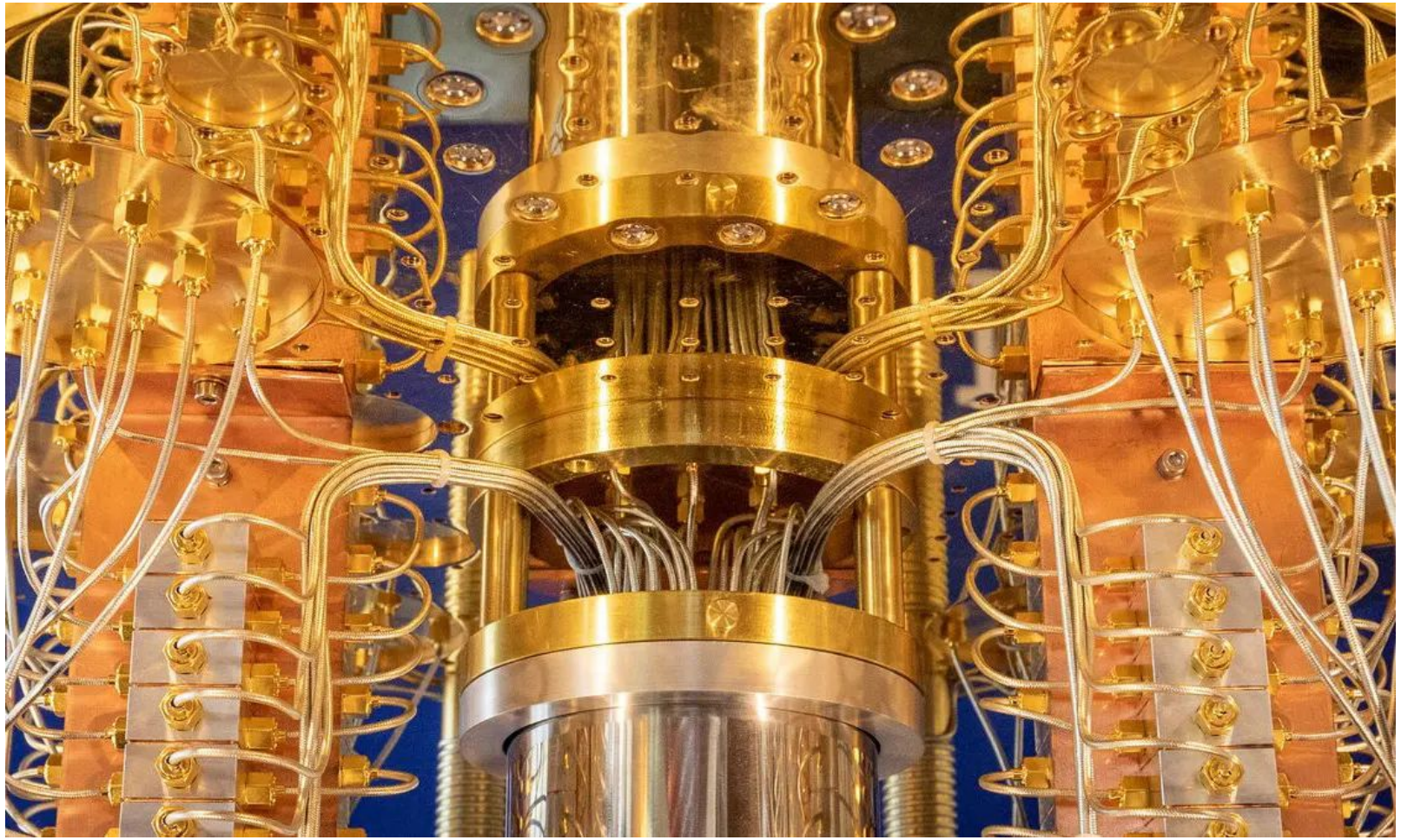
- Quantum computing wants to utilise the “all possible directions” idea in order to get lots of computations done in parallel, at the same time.
- Google claims that their quantum computer has completed a computation in a couple of seconds, compared to thousands of years for a regular computer.
- Quantum computing challenges blockchain speed, which is know to be notoriously slow
- Challenges PoW/PoS
- It is currently in its early stages of research
- Vitalik (Ethereum) resists it for now
- Interesting reads on the topic can be found here and here

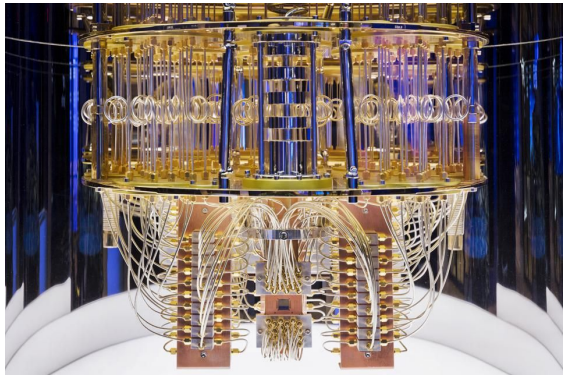
Quantum Computing

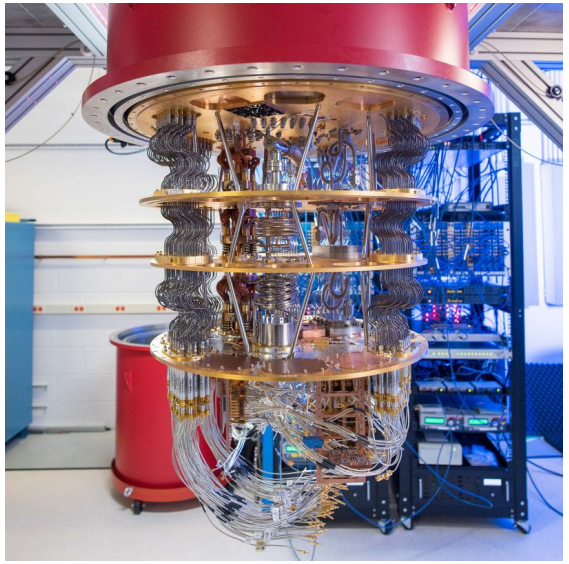
- Traditional computers use 1 and 0 to break through operations, quantum computers, on the other hand, use quantum bits or qubits.
- The special particularity of qubits is that they have a third state called “superposition”, which allows them to represent a 1 or a 0 at the same time.
- With the superposition, a quantum computer allows two qubits to represent four scenarios at the same time.



Quantum Computing







AI

Artificial intelligence uses computers to mimic human intelligence. AI models differentiate themselves from traditional computers, as they “learn! by improving as they are fed with new data. Like a human brain, an AI model can be developed and improved.

AI uses on Blockchain

- Artificial Intelligence models can be used to analyse, classify and make predictions from the information fed to them (data).
- Blockchain allows for collaborative and secure data sharing since information can’t be altered once stored in the blockchain.
- This translates into more authentic and close-to-reality results.
- In order for AI models to remain effective and updated, their database needs to be filled with quality information. Unfortunately, the amount of data on the internet is not always trustful.
- Machine learning is a subdivision of artificial intelligence and it is used to extract insights from data.
- In general, larger (and better) datasets help create more efficient machine learning models.

Practical Example: at the Doctor's

- At the doctor's office, the AI assistant, that is expertly trained, has ingested millions of medical periodicals to this date.
- It would not be humanly possible for any doctor to keep up with all the latest medical breakthroughs and advances.
- Important question: who provides the training to this AI Doc?
  - Professional, unbiased and reliable training is key
  - If, for example, it's been trained by one Big Pharma company, it wouldn't be reliable.
  - Blockchain technology ensures objective and unaltered training.

IoT

The Internet of Things, or IoT, refers to the billions of physical internet – connected devices and capable of collecting and transmitting data without the need for human interaction.

The IoT Network

- All our electronic devices are fitted with chips, sensors, etc, each transmitting data to the IoT network.
- Security has always been a major concern, that has hindered the large-scale deployment of IoT.
- Vulnerable IoT devices make it easier for cybercriminals to target them.
- The existing centralised systems that authenticate, authorise and connect different nodes won’t be able to keep up with the ever growing network of IoT devices. Blockchain and its decentralised network, will help alleviate that burden.

How Can Blockchain Help IoT

- IoT security and scalability challenges can be addressed with blockchain technology.
- By eliminating the single point of control, you also eliminate the single point of failure. Blockchain doesn’t allow one organisation to control the data generated by the IoT.
- The idea is to give each device, at their creation point, an identity (chip, serial number, etc) that allows the device to be tracked and verified throughout their whole life cycle within the Blockchain.
- With blockchain technology, transactions can be coordinated in a fraction of the time among billions of devices.

Applications of IoT and blockchain

- **Freight transportation**
  - With blockchain, temperatures, position, arrival times and shipping status of containers can be continuously be tracked as they move.
- **Component tracking and compliance**
  - For safety and regulatory purposes, components can be tracked as they go into an aircraft, automobile, or other products is critical for both safety and regulatory compliance.
- **Log operational maintenance data**
  - Critical machines can be tracked for their safety and maintenance if connected to the blockchain.

IoT Examples

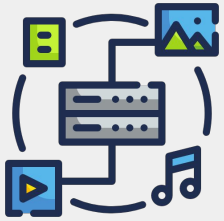
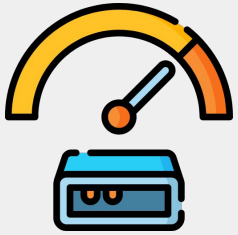
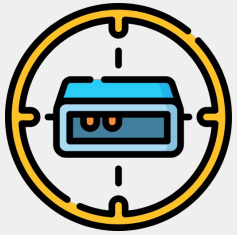
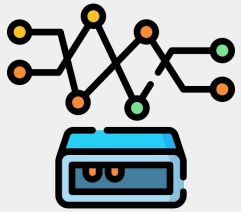
Big Data

Big Data is a large amount of data that traditional databases can’t capture, manage, or process because of its size or type.

Key Points

- Big data is composed of structured, semistructured and unstructured data collected by organisations and companies for information and/ or other advanced analytics applications.
- Big data is often characterised by the 6Vs:
  - **Volume:** large volumes of data
  - **Variety:** wide variety of data types
  - **Velocity:** the speed at which the data is generated, collected and processed.
  - **Veracity**, **value** and **variability** are the other key characteristics.

6 Vs of Big Data

Volume	Variety	Velocity	Veracity	Value	Variability
The amount of data from myriad sources	They types of data: structured, semi-structured, unstructured.	The speed at which big data is generated.	The degree to which big data can be trusted.	The business value of the data collected.	The ways in which the big data can be used and formatted
					

Key Points

- Big data is mainly used to improve operations, provide better customer service, create personalised marketing campaigns and increase profitability.
- Big data can come from many different sources, mainly through the IoT devices and other, more traditional methods, such as business transaction systems, customer databases, medical records, internet clickstream logs, mobile applications, social networks, etc.

Big Data and Blockchain

- Blockchain adds another security layer to the Big Data analytics process.
- Blockchain-generated Big Data is
  - Safe: it cannot be manipulated or altered.
  - Valuable: it is structured, abundant and complete.
- **“If Big Data is the quantity, blockchain is the quality”**

➔ The real question now is who will be the first company to develop the most appropriate and blockchain-trained AI machine.

Blockchain Landscape

Created by and for the DLT community, live market landscape with the blockchain technical foundation.

Forbes' Blockchain Top 50 - 2021

- Read the full article here

Forbes' Blockchain - Key Leaders

Blockchain "will fundamentally change financial systems in the next 10, 15 years. A blockchain technology will be applied in many areas because it is about trust, credit, security—the security of data and the privacy of data."

—**Jack Ma** *Cofounder of ANT Group and founder of Alibaba*

"The crypto economy is what we're driving toward. It's a new economy that starts off primarily online, but it's also accessible to people in emerging markets. It's more global. It's more fair. It's more free. It's more efficient."

—**Brian Armstrong**
Coinbase CEO and cofounder

"By tracking hundreds of fresh food items, including leafy greens, meat and seafood on the blockchain, Walmart has made it easier to identify the origin of potentially contaminated products—a benefit to not only the retailer but also the FDA."

—**Archana Sristy**
Walmart Senior Director—Software Engineering, Blockchain Platforms

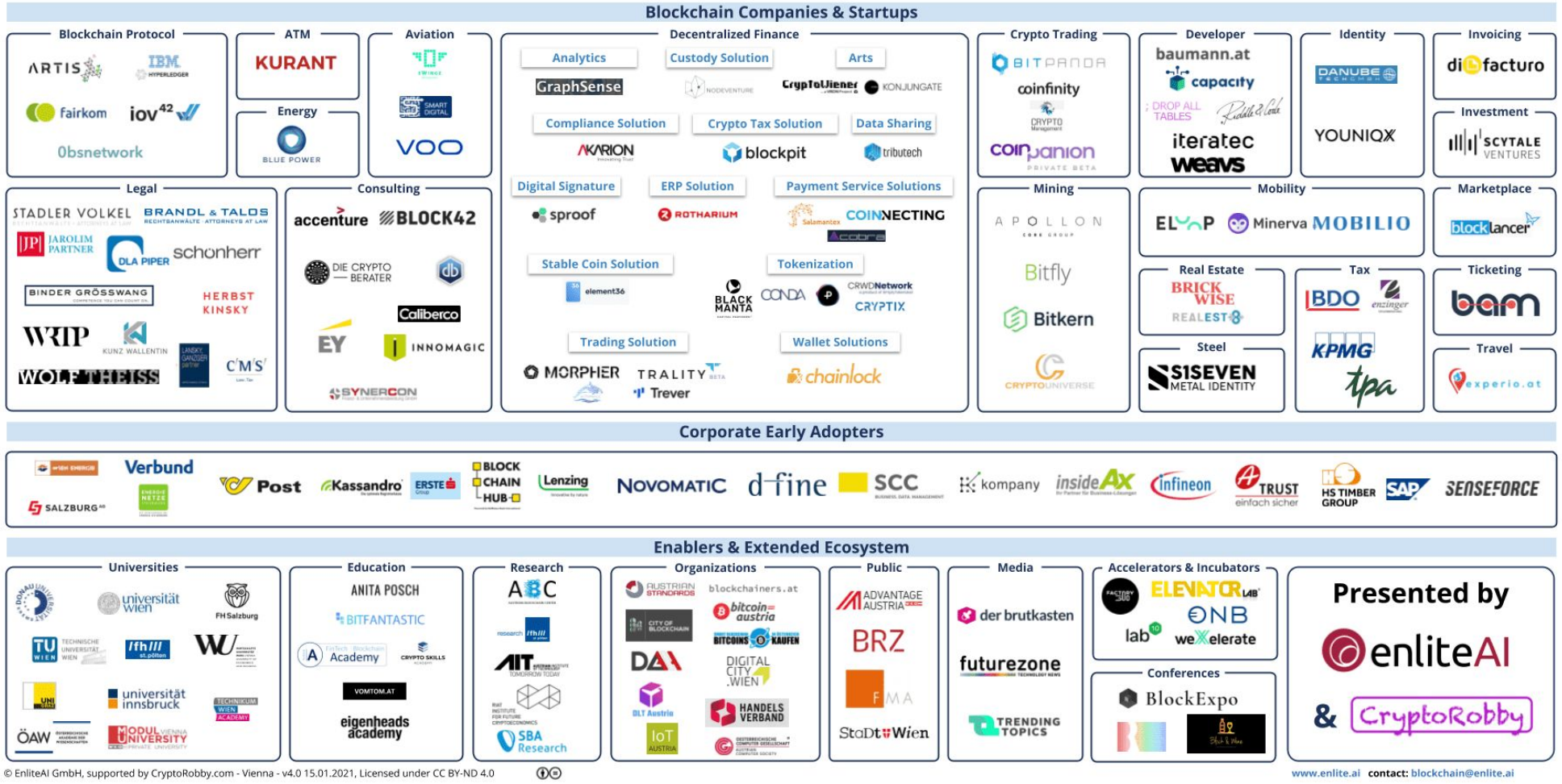
"The tokenization process is efficient for assigning title to real physical goods. By making that process more efficient, it allows for more liquidity, more investment and opening up those assets to a broader range of investors."

—**Jeanine Hightower-Sellitto**
CEO of Atomyze, a partner of Nornickel

"The reason I have so much passion for Bitcoin is largely because of the model it demonstrates: a foundational internet technology that is not controlled or influenced by any single individual or entity."

—**Jack Dorsey**
Square CEO and cofounder

Austria’s Blockchain Landscape 2021



Source: enlite.ai

Blocktech in Financial Services

Source: The Block

Blockchain Marketing Technology Landscape q1 2019

Quiz Time

When was the Genesis Block mined?

A. 2009
B. 2010
C. 2011
D. 2012

Where are private keys located?

A. In a wallet
B. Attached to a bitcoin
C. In a transaction
D. In a block

What is the role of digital signatures in Bitcoin?

A. To associate bitcoins with their owners
B. To provide transaction verification
C. To provide decentralized trust in the system
D. All of the above

What does P2P stand for?

A. Password to Password
B. Peer to Peer
C. Product to Product
D. Private Key to Public Key

What is the most secure method of generating private keys?

A. Generating keys offline
B. No method is truly secure, except generating keys through an exchange
C. Generating keys through a trusted third-party
D. Generating keys by using a web service

What are the best methods for “cold storage”?

A. Hardware wallets
B. Removable media or USB flash drives
C. Paper wallets
D. A combination of using the full and web Bitcoin clients

What is the purpose of the blockchain?

A. To provide transparency of transactions
B. Record all valid transactions
C. It is a means to provide distributed consensus of valid transactions
D. Full anonymity of transactions

What is a miner?

A. A type of blockchain
B. An algorithm that predicts the next part of the chain
C. A person doing calculations to verify a transaction
D. Computers that validate and process blockchain transactions

What are some of the main goals of altcoins?

A. To provide centralized alternative currencies
B. To create the same currency in an alternative name
C. To create an alternative network to Bitcoin
D. To introduce new features

How do you calculate market capitalization?

A. A cryptocurrency's current supply * by the highest exchange rate to date
B. A cryptocurrency's current number of nodes * by the current exchange rate
C. A cryptocurrency's current supply * by the current exchange rate
D. A cryptocurrency's maximum expected supply * by the current exchange rate

Which of the following are Key Performance Indicators (KPIs) for assessing digital currencies?

A. Average confirmation time
B. Hashing algorithm used
C. Merchant Acceptance
D. Network Hash rate

Which country's government aims to turn the country into a blockchain/ cryptocurrency hub?

A. China
B. Greece
C. Cyprus
D. Malta

What is the term for when a blockchain splits?

A. A fork
B. A merger
C. A sidechain
D. A division

What is a smart contract?

A. Artificial intelligence assisted contract
B. A cloud-based contract
C. A computer protocol
D. An auto-generated work contract

Thank you!

Thank you very much for your attention.

www.encryptedreviews.com

References

- Cointelligence
- Blockonomi
- Blockgeeks
- Coincentral
- Coinmarketcap
- Investopedia
- Bitpanda
- Wikipedia
- Thebalance
- Visualcapitalist
- EUblockchainforum
- Coindesk
- Youtube
- Ethereum
- Tradeblock
- Blockchain
- Gemini

Need MORE? Who to Watch & Follow

Podcasts/Youtube

- Ivan on Tech
- Krown's Crypto Cave
- Unchained Podcast
- Coindesk Podcasts

Resources

- Coindesk Research Hub
- Trading View
- Bitcoin Forum

Crypto Twitter is REAL!

Appendix

Quiz Answers

- **When was the Genesis Block mined?** 2009
- **Where are private keys located?** In a wallet
- **What is the role of digital signatures in Bitcoin?** - All of the above
- **What does P2P stand for?** - Peer to Peer
- **What is the most secure method of generating private keys?** - Generating keys offline
- **What are the best methods for “cold storage”?** - Hardware wallets
- **What is the purpose of the blockchain?** - all the options
- **What is a miner?** - Computers that validate and process blockchain transactions

Quiz Answers pt.2

- **What are some of the main goals of alt- coins?** - To create an alternative network to Bitcoin, To introduce new features
- **How do you calculate market capitalization?** - A cryptocurrency' s current supply * by the current exchange rate
- **Which of the following are Key Performance Indicators (KPIs) for assessing digital currencies?** - Average confirmation time, Network Hash rate
- **Which country's government aims to turn the country into a blockchain/ cryptocurrency hub?** - Malta
- **What is the term for when a blockchain splits?** - A fork
- **What is a smart contract?** - A computer protocol