

# MSc Business Analytics

## Financial Modelling and Analysis

Chapter 5.1 Finance based on blockchain technologies. Blockchain and cryptocurrency

Instructor: Roman Matkovskyy

Twitter: @matkovskyy

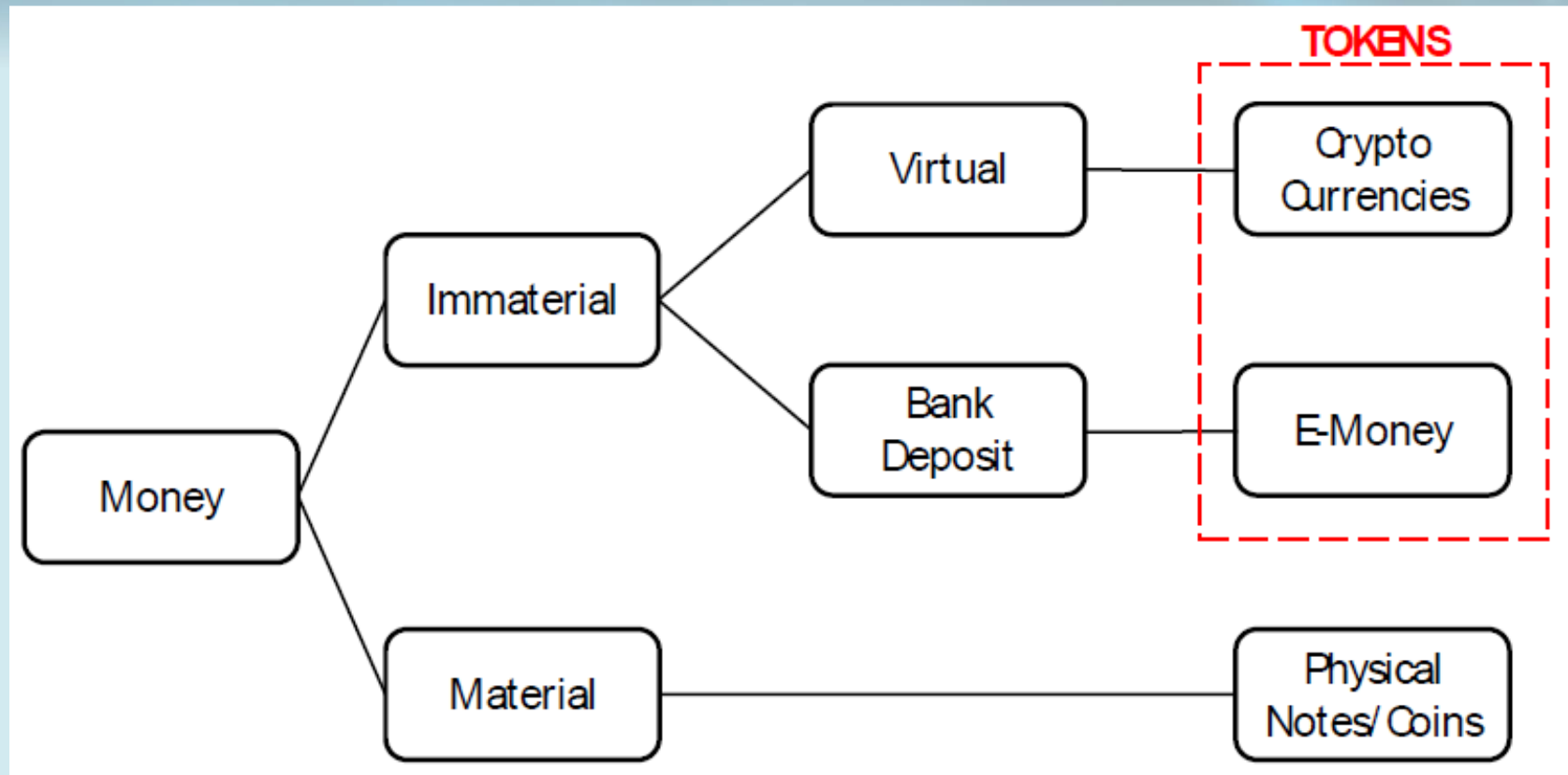
# What will we be speaking about?

- What is cryptocurrency?
- History of Cryptographic Currencies
- Transacting in Bitcoin
- The Digital Signature/Property Rights /Hash function.
- A Tamper Proof Ledger / Blockchain
- Distributed Consensus/PoW/Currency Creation (mining)
- PoW Challenges / Other types of the consensus
- Main types of digital asset: coins, stable coins, tokens
- Bitcoin/Ethereum/Cardano/Litecoin/Stellar/Monero/Solana...
- NFT
- DeFi

# Intro

- Approx. 14 years after the distribution of Satoshi Nakamoto's famous white paper (October 31, 2008), some things are clear:
  - Cryptocurrency, and the associated technology of blockchain, has staying power
  - Cryptocurrency is inherently a hard subject, as it combines the knowledge base of computer science, cryptography, finance, and economics

# Types of currencies



# What is crypto currency ?

- There is no commonly accepted definition of crypto currencies.
- The comedian John Oliver has described crypto currencies as:

**"everything you don't understand about money combined with everything you don't understand about computers."**

(Last Week Tonight with John Oliver (2018). "Cryptocurrency,"  
<https://www.youtube.com/watch?v=g6iDZspbRMg>)

# Aspects of cryptocurrencies

- Cryptocurrencies have many different aspects, and can therefore be viewed from various angles, including the
  - *financial and economic perspective,*
  - *legal perspective,*
  - *political*
  - *sociological perspective,*
  - *technical and socio-technical perspectives.*

# Failed Online Currencies: CyberCash

- Launched in 1990's that pioneered the CyberCoin
- It went public in February, 1996 (CYCH)
- Its shares rose 79% on the first day of trading!
- Problem with the currency: every user needed to obtain a certificate to verify their identity.
- In 2000, many users of CyberCash's ICVerify application fell victim to the Y2K Bug (double recording of credit card payments)
- Declared bankruptcy in 2001
- Technology was eventually acquired by PayPal (on the internet mainly is indicated VeriSign)



# Failed Online Currencies: DigiCash

- Clients were anonymous
- Patented a blind-signature scheme that has some similarity to Bitcoin's protocol
- Merchants were not anonymous and needed to register with a bank
- No user-to-user transactions
- DigiCash declared bankruptcy in 1998
- Technology eventually acquired by InfoSpace

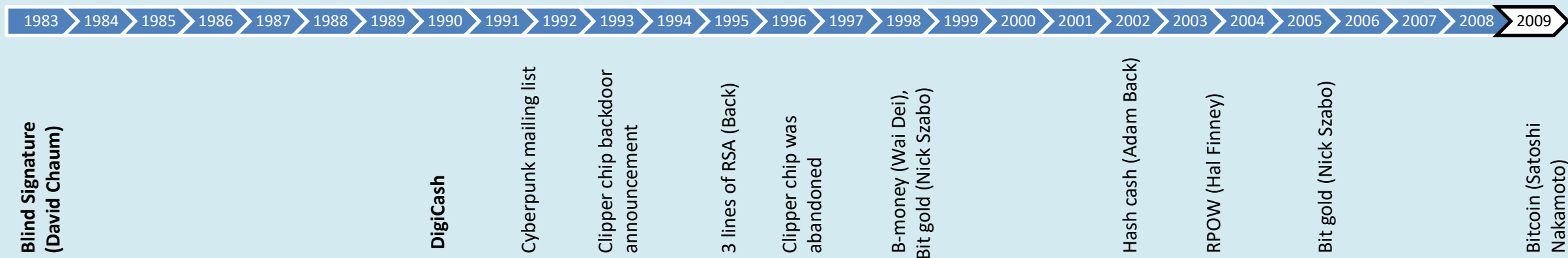


# Failed Online Currencies: Magic Money

- Created by a members of a mailing list called Cypherpunks
- Violated the patent of DigiCash
- Cypherpunks was the group out of which Satoshi emerged (the history of the movements will be later a bit)

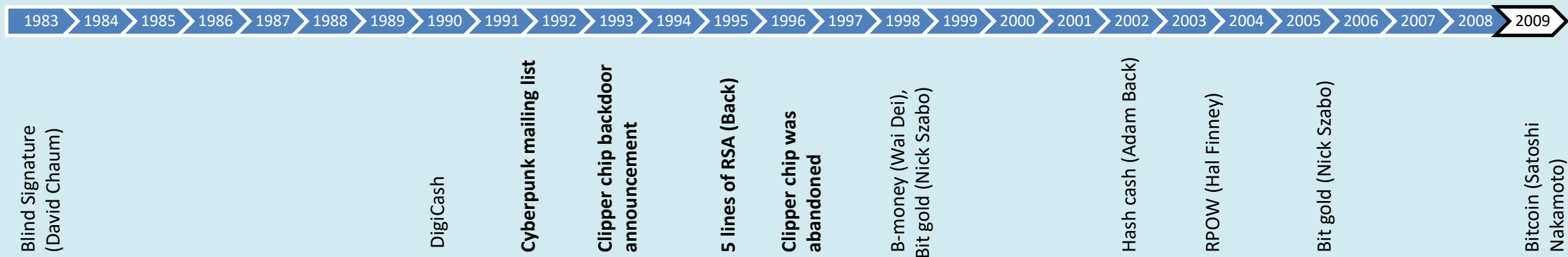
# Overall history of Cryptographic Currencies

- **The history starts in the 1980s** with **David Chaum's** work (D. Chaum. Security without identification: Transaction systems to make big brother obsolete. Volume 28, pages 1030–1044. ACM, 1985. DOI: 10.1145/4372.4373 and D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In Proc. on Advances in Cryptology, pages 319–327. Springer-Verlag, New York, 1990. DOI: 10.1007/0-387-34799-2\_25]
- Chaum **proposed a novel cryptographic scheme to blind the content of a message before it is signed.**
  - These **blind signatures** can be publicly verified.
- His digital cash allowed users to spend a digital currency in such a way that it is untraceable by another party.
- Chaum et al. (1990) added double-spending detection mechanisms.
- To commercialize his ideas of digital cash, Chaum founded DigiCash in 1990.
  - Though it failed.



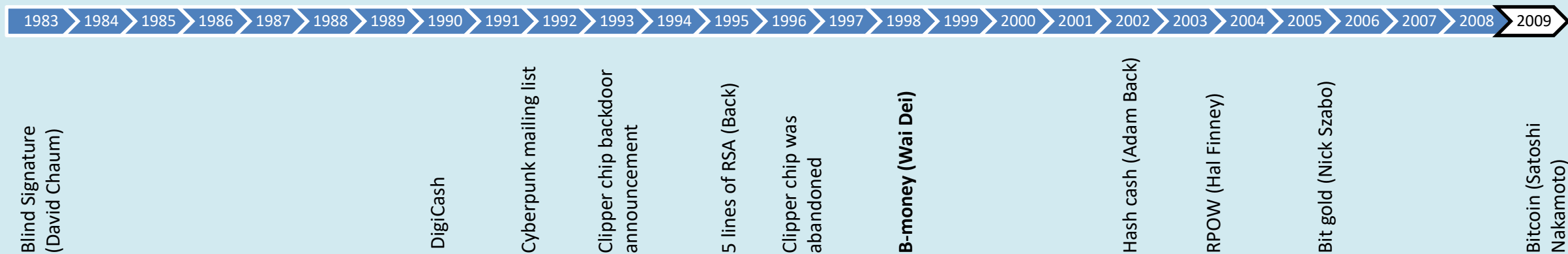
# Overall history of Cryptographic Currencies

- **The cypherpunk movement was born inspired by David Chaum's work**
- Cryptography started being used outside **the military and intelligence agencies**.
- Anonymity, pseudonymity, communication privacy, data hiding, censorship and monitoring were discussed there
- The Clipper chipset developed by the NSAA was a major issue in the mid-1990s due to its built-in backdoor.
- In 1994, Matt Blaze published a paper on vulnerabilities in Clipper Chip's escrow system. He found that the chip transmitted information that could be exploited to recover the encryption key in a specific Law Enforcement Access Field (LEAF). The chip was abandoned in 1996.
- Moti Yung and Yair Frankel in 1995 showed that key escrow device tracking can further be exploited by attaching the LEAF to messages from different devices than the originating one to bypass escrow in real time.
- Several other attacks have been published since then. **This is commonly referred to as crypto wars.** (details KEHL, D., WILSON, A., & BANKSTON, K. (2015). THE BATTLE OF THE CLIPPER CHIP AND THE WAR OVER KEY ESCROW. In DOOMED TO REPEAT HISTORY?: Lessons from the Crypto Wars of the 1990s (pp. 5–11). New America. <http://www.istor.org/stable/resrep10502.5>)
- Adam Back invented Hashcash, pioneered the use of ultra-compact code with his 5-line RSA in Perl signature file which was then printed on t-shirts to protest the United States' cryptography export regulations.



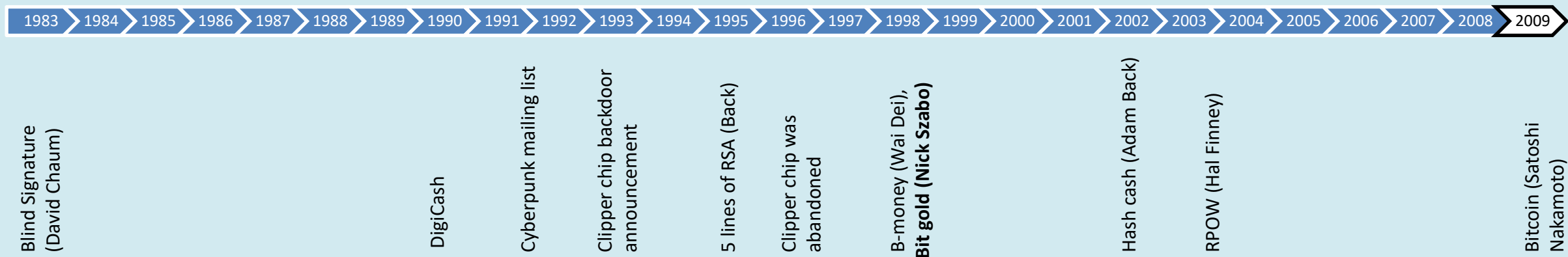
# Overall history of Cryptographic Currencies

- **b-money:** In 1998, Wei Dai proposed b-money [X. Défago, A. Schiper, and P. Urbán. Total order broadcast and multicast algorithms: Taxonomy and survey. ACM Computing Surveys (CSUR), 36(4):372–421, 2004. DOI:10.1145/1041680.1041682.], an anonymous and distributed electronic cash system.
- Two protocols were described that were based on **the assumption that an untraceable network exists where senders and receivers are identified only by digital pseudonyms such as their public keys, and that every message is signed by its sender and encrypted to the receiver.**
- B-money allowed the creation of e-money based on previously unsolved cryptographic puzzles.



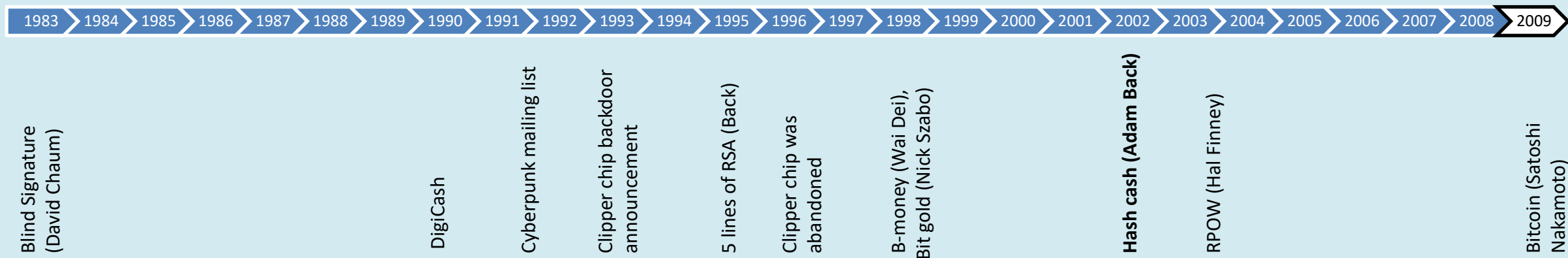
# Overall history of Cryptographic Currencies

- **bit gold**: In 1998, Nick Szabo designed a new digital currency based on cryptographic puzzles.
- Double-spending without a central authority was address by mimicing the trust characteristics of gold.
- In 2002, Szabo also presented a theory of collectibles based on the origins of money [N. Szabo. Shelling out: The origins of money. <http://nakamotoinstitute.org/shelling-out/> ].



# Overall history of Cryptographic Currencies

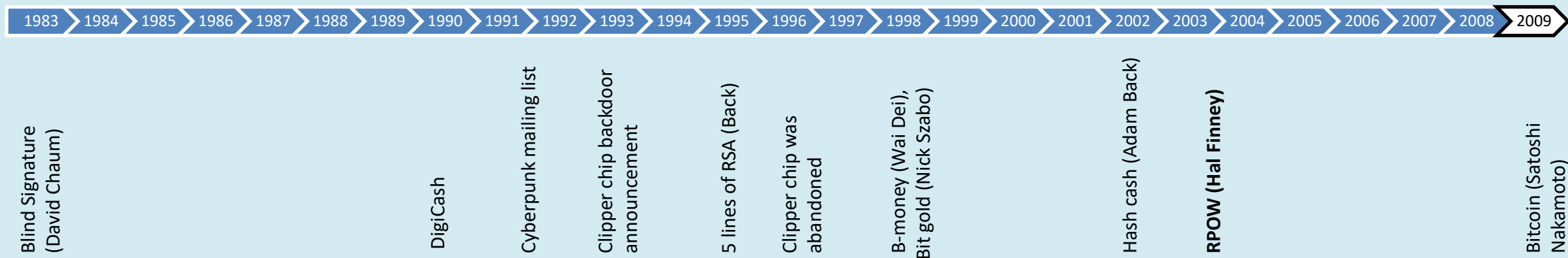
- **Hashcash:** Adam Back proposed Hashcash [A. Back et al. Hashcash-a denial of service counter-measure. <http://www.hashcash.org/papers/hashcash.pdf> , 2002], a proof-of-work (PoW) system based on cryptographic hash functions to derive probabilistic proof of computational work as an authentication mechanism.
- The purpose of the PoW was to ensure that it was computationally hard for a spam to transmit mails.
- The identity of the sender was protected, no traditional authentication checks were possible.
- Within Hashcash, this protection was realized via an additional e-mail header.
- Back's PoW was conceptually reused and developed in Bitcoin mining.





# Overall history of Cryptographic Currencies

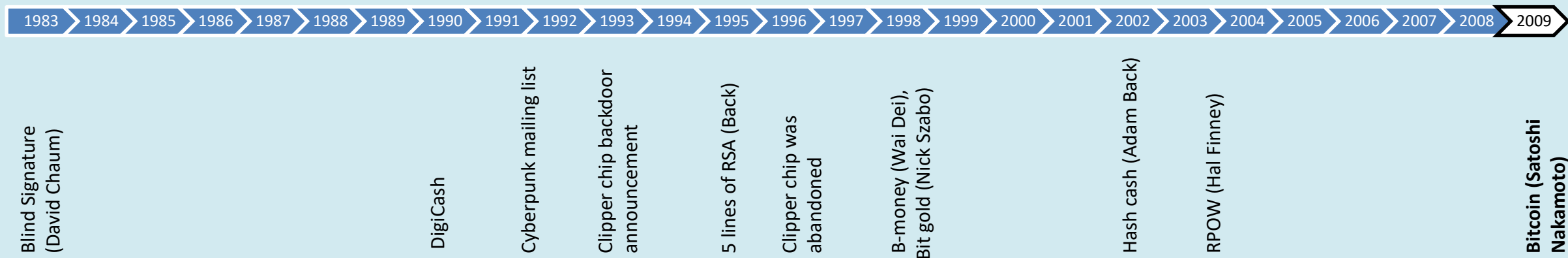
- Hal Finney presented the first currency system based on a reusable proof-of-work (**RPOW**) and Szabo's theory of collectibles [N. Szabo. Shelling out: The origins of money. <http://nakamotoinstitute.org/shelling-out/>, 2002.] in 2004 [H. Finney. Reusable proofs of work (RPOW). <http://web.archive.org/web/20071222072154/http://rpow.net/>, 2004.].
- Similar to bit gold, Finney introduced token money that was aligned with the concept of gold value.
- After the launch of Bitcoin, Hal Finney became the first user of this cryptocurrency.
  - He received a Bitcoin transaction from Bitcoin's creator Satoshi Nakamoto.





# Overall history of Cryptographic Currencies

- Between 2008 and 2009, **Bitcoin** was created by the pseudonymous developer Satoshi Nakamoto [S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf> , 2008].
- It is the first decentralized cryptocurrency that still exists. It has the highest market capitalization as of today.
- On 3.01.2009 the genesis (the first) block of the Bitcoin protocol was created, launching Bitcoin as a decentralized cryptocurrency.



# General background

- *S. Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>.*
- The original Bitcoin code is here <https://github.com/trottier/original-bitcoin>
- Those technologies that are based on the same or very similar fundamental principles as Bitcoin are commonly referred to as blockchains.
- The term **blockchain** itself was not directly introduced by Satoshi Nakamoto in the original paper, but used early on within the Bitcoin community to refer to certain concepts of the cryptocurrency (As a result, there are two common spellings of this term found throughout the literature, namely blockchain and block chain).
- Nowadays blockchain is used as a nebulous umbrella term to refer to various concepts that are related to cryptocurrency technologies.
- To date, over **22 000 different cryptocurrencies/token have been created and traded** (<https://coinmarketcap.com/>).
- Some of those currencies only had a very short lifespan or were merely conceived for fraudulent purposes, while others brought additional innovations and still have vital and vibrant communities today.
- The mechanisms and underlying principles of most of these cryptocurrencies are, to a greater or lesser extent, derived from the original Bitcoin protocol.
- Several of these incarnations may only differ from Bitcoin in their choice of certain constants such as the target block interval or maximum number of currency units that will eventually come into existence. Others have switched to alternative proof-of-work algorithms (e.g., Litecoin- <https://litecoin.org/> , Dogecoin- <https://dogecoin.com/> ), have included additional features (e.g., Namecoin - <https://www.namecoin.org/> decentralises DNS, Ethereum- <https://github.com/ethereum/yellowpaper>, Zcash <https://z.cash/> ), or have used different distributed consensus approaches (e.g., Ripple that is considered to be a crypto alternative to SWIFT).

# **TRANSACTING IN CRYPTOCURRENCY (BITCOIN)**

# Bitcoin Transactions

- A transaction tells the network that the owner of some bitcoin value has authorized the transfer of that value to another owner.
- The **new owner can now spend the bitcoin by creating another transaction** that authorizes transfer to another owner, and so on, in a chain of ownership.
- Transactions are like lines in a double-entry bookkeeping ledger. Each transaction contains one or more “inputs,” which are like debits against a bitcoin account.
- On the other side of the transaction, there are one or more “outputs,” which are like credits added to a bitcoin account.
- **The inputs and outputs (debits and credits) do not necessarily add up to the same amount.** Instead, **outputs add up to slightly less than inputs and the difference represents an implied transaction fee, which is a small payment collected by the miner who includes the transaction in the ledger.**

# Bitcoin Transactions: example of Alice, Bob and Alice

- Alice's payment to Bob's Cafe uses a **previous transaction's output as its input**.
- Alice received bitcoin from her friend Joe in return for cash.
- **That transaction created a bitcoin value locked by Alice's key.**
- **Her new transaction to Bob's Cafe references the previous transaction as an input and creates new outputs to pay for the cup of coffee and receive change.**
  - The transactions form a chain, where the inputs from the latest transaction correspond to outputs from previous transactions.
- Alice's key provides the signature that unlocks those previous transaction outputs, thereby proving to the bitcoin network that she owns the funds.
- She attaches the payment for coffee to Bob's address, thereby "encumbering" that output with the requirement that Bob produces a signature in order to spend that amount.
  - This represents a transfer of value between Alice and Bob.
- This chain of transactions, from Joe to Alice to Bob, is illustrated in the Fig.



# Transacting in Bitcoin

- First, you need a **wallet** (for instance using Blockchain.info, Coinbase,...)
  - Wallet – a place to store your bitcoin credentials: namely your private key
- Private key – a 256-bit number, expressed as a hexadecimal
  - E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA3326
  - Generated using cryptography
- When people say that they have lost their bitcoins, they mean their private key



# Transacting in Bitcoin

- Without the private key - no way to access cryptos
- If someone has your private key, or can infer it, then you have given them your bitcoins
- Your private key can generate your unique address (which is public)



# Transacting in Bitcoin

- Ways to transact in Bitcoin
  - Third-party software (example, Coinbase),
    - Provides the wallet and the access to a bitcoin exchange
  - Can separately choose a wallet and an exchange
  - You can buy with cash using a bitcoin ATM

# Transacting in Bitcoin

- Once you own bitcoin, you can:
  - purchase goods or services from other users of bitcoin using third party software, or directly
  - trade bitcoin back to dollars/euros/...
- Bitcoin is a currency, similar to any other
- It is not:
  - a stock, which is a claim to ownership in a company
  - a treasury bill, which is a claim to the income of taxpayers
- **Unless people believe that it can eventually function as a medium of exchange, in some states of the world, or store of value, bitcoin (or other similar cryptocurrencies) has no inherent value.**

# Transacting in Bitcoin

- Might Bitcoin function someday, as a generalized and global medium of exchange?
  - To really answer that question, **we need to consider what we mean by currency**

# Money: Bank money

Bank money has several notable characteristics:

- **Holding and using money requires a bank account.**
- **Any monetary transaction is a movement between bank accounts.**
  - It is identifiable and traceable and therefore can be monitored and regulated.
- **Money is a legal claim on an identifiable entity: the bank.**
  - It is a liability of the bank.
  - *A bank deposit gives the holder legal rights on the bank, and an (indirect) claim on its assets.*
- **Bank customers have the right to convert their deposit into banknotes, which are legal tender.**
  - The Central Bank issues the currency serving as a "base" for the system, giving it its legal status.
- **Bank money is a form of “private” money.**
  - It is therefore vulnerable to a loss of confidence in the issuing bank.
- **Bank money nonetheless benefits in many ways from public backing through deposit insurance and/or access to Central Bank refinancing.**

# Money: e-money

- **E-money**, which often takes the form of money on prepaid cards or stored on mobile phones, **is actually a representation of bank money.**
- The outstanding amounts of e-money are covered by existing bank accounts, so that if a provider were to fail, the user could still recover the balance in their accounts.
- **E-money**, in its current forms, **is simply a technology to access and move around money deposited in bank accounts.**
- As such, **e-money is not a new form of money, but is instead one of the modern forms that bank money takes.**

# Money: Crypto currencies

- Crypto currencies are fundamentally different than bank money or e-money.
- Like bank money, **they have no intrinsic value, are privately created, and are totally dematerialized and digital.** But each of their other characteristics are the opposite of those of existing currencies:
  - They are **purely private currencies**, are **not legal tender**, and are **not convertible at par**
  - They are **created and circulate independently of any bank**; they are **not connected to any bank account**.
  - They **do not represent a claim on any person or legal entity**. They are “outside money,” because they are created outside the banking system.
  - They have no physical, financial, or legal backing of any kind.
  - They are denominated in specific units of account, unrelated to existing currencies.

# In a nutshell

- The US dollar/euro/.. is fiat money
  - Legal tender for all debts public and private
- The requirement to accept dollars/euros/... for private debt is by “fiat”
- Backed by the power of the sovereign
- The fiat of the US/EU/... governments does extend:
  - to private businesses accepting dollars for payment
  - to all of the transactions, both legal and illegal, that take place around the world using dollars/euros/....
    - These transactions do occur, and apparently more frequently than ever (<https://scholar.harvard.edu/files/rogooff/files/c13431.pdf> )



# What Exactly is Currency?

- The self-fulfilling equilibrium:
  - Everyone agrees to take US dollars or euros etc because they believe that everyone will take US dollars/euros/etc.
- Rests on the following fundamentals:
  - Dollars/euros/.. can pay taxes and discharge debt
  - The rule of law
- Bottom line: **what makes a currency a currency are the common beliefs of the individual users**

# What Exactly is Currency?

- Directly using cash is sufficiently cumbersome that a profitable industry has arisen to allow us to avoid it
  - Nearly all merchants accept Visa and Mastercard
  - Most merchants accept 4 major credit cards: those two plus Discover and American Express
    - Very costly for the merchants due to a fee that can be over 2% of the transactions
    - By law, they are not allowed to offer a discount for cash
      - These cards are very profitable for the credit card companies
      - They are nice for consumers because consumers receive (taxfree) benefits
- Customers demand these cards, so merchants lose business if they do not accept them
- Merchants are not allowed to price discriminate, which implies that these card companies form an oligopoly.

# Cards as centralized intermediary

- Transactions are still done in terms of dollars/euros/...
- But the credit card company keeps track of the accounts and verifies the legitimacy of the transaction
- Maintains a centralized ledger
- Credit cards avoid keeping track of which customers' checks are good and which are not
- Allows internet transactions when you don't know the customer on the other side

# A short summary

- *Bitcoin is a currency* like any other
- Can function as a medium of exchange or a store of value
  - We already have the mediums of exchange – dollars, euros, ...
- The functionality of dollars/euros/... as a medium of exchange is through common beliefs
- A profitable industry of centralized intermediaries has grown up to facilitate dollar transactions without the direct use of the currency

# Why Cryptocurrency?

- Bitcoin allows:
  - online transactions (and offline transactions without cash)
  - any transaction for which a credit card is used could be a Bitcoin transaction
- It accomplishes this while still being decentralized

# Why Cryptocurrency?

- **Reason 1: A centralized intermediary has a lot of power**
- Should we worry about the potential for abuse given the near-monopoly power of intermediaries?
  - These companies might tamper with this ledger, perhaps to punish enemies or reward friends
    - Probably not: it is very profitable to be a centralized intermediary (franchise value - the present value of the future profits that a firm is expected to earn)

# Why Cryptocurrency?

- **Reason 2: You do not like centralized intermediaries for philosophical reasons**
  - i.e. you are an extreme libertarian or perhaps an anarchist
- **Reason 3: You need to hide from the centralized intermediary because you are engaged in some activity you do not want the government to know about**
  - Perhaps you do not trust the government, or you are doing something specifically against the law



# Why Cryptocurrency?

- There may be a deeper reason behind the appeal of cryptocurrency
- What if, for instance, dollars themselves were to become untrustworthy?
  - The value of the dollar rests (in part) in the hands of the Federal Reserve
  - The Federal Reserve is in principle independent
  - The value also depends on everyone's expectations

# Why Cryptocurrency? Two problems from relying on fiat money

## 1. What if there was, say, 5% inflation?

- Because of the fiat, investors need to hold cash for transaction purposes
- If there is inflation, those dollars erode in value
- Similar to a tax in that the government gets to spend the extra money it prints
- Having a competitor to dollars, residents are not trapped by the seigniorage (the difference between the value of money and the cost to produce and distribute it)

## 2. What should happens if the currency become truly unstable (for instance Venezuela 2016–present)

- Bitcoin is designed (to some extent) with protections against problems 1 & 2

# Short summary

Bitcoin is a currency like any other

- Not recognized as legal tender by any sovereign;
- Zero is always a possible answer to the question: what is its value?
- Depends on whether it can be used as a medium of exchange
- Or whether people believe it can be used as a medium of exchange
- Or whether people believe that people believe it can be used as a medium of exchange

Bitcoin derives its potential value from sources:

- Ease of transactions without relying on a centralized intermediary
- Currency that is not prone to manipulation by a central bank
- Will Bitcoin remain a niche product, or might it be widely adopted?
- It is not enough to have advantages; there must be a critical mass of users who see these advantages as important



# **THE DIGITAL SIGNATURE**

# Property Rights in Bitcoin

- Cryptocurrency must create its own system of property rights
- Must be self-enforcing, because the system is decentralized
- Who possess rights within the system, while still maintaining anonymity?
- How do you prevent this from being so cumbersome that individuals do not want to join?

# Property Rights in Bitcoin

- Bitcoin has an elegant answer!
- It dispenses with the notion of the human being in the background entirely
- **You “are” your signature**
- You can have as many signatures as you want
- Your signature has a private component (the private key), and the public component
- **The public signature is synonymous with the address**

# A digital signature

- An object with the following properties:
  - Only you can make it (unforgeability)
  - Anyone can verify it
  - It's permanent
- A digital signature:
  - A private key, generated at random
  - A protocol for affixing the private key to an electronic message (this is the actual written signature)
  - A protocol for verifying that your signature is valid
    - Without revealing your private key
    - This is where the public part of your signature comes in



# A digital signature

- It is very important that:
  - no one can forge your signature
  - no one can replicate your signature after reading a message
- Thus the creation of the signature must be random
- Affixing the signature to the message must be encrypted, which also involves randomness

# A digital signature

- Think about what makes physical signatures so difficult to forge?
  - Created by a human being
  - A built-in randomness to being human: no two humans are alike
  - No person is the same every day. One cannot replicate a signature just by seeing it.
  - Thus humanity interposes randomness at both steps of the process
- “Random-number generators”
  - Software that produces a string of random numbers
  - Computer-generated random numbers are “pseudo-random numbers”

# A TAMPER PROOF LEDGER

# The Ledger

- The ledger contains a record of all Bitcoin transactions
  - **A memory system**
- The equivalence between money and memory was proposed by economist Narayana Kocherlakota in 1998 (Kocherlakota N.R. (1998) Money Is Memory. Journal of Economic Theory 81(2), 232-251)
  - Memory is defined as knowledge on the part of an agent of the full histories of all agents with whom he has had direct or indirect contact in the past.
  - Any allocation that is feasible in an environment with money is also feasible in the same environment with memory.
  - Money is defined as an object that does not enter utility or production functions, and is available in fixed supply. From a technological point of view, money is equivalent to a primitive form of memory
- Along with the digital signature, the accurate ledger is required for the existence of property rights in Bitcoin

# Bitcoin Innovation: Incentives

- Satoshi's solution
  - In previous attempts to decentralize, creators focused on making it impossible to tamper with the ledger
  - Satoshi realized that it was sufficient (and much easier) to have incentives not to tamper with the ledger
- How to dis-incentivize participants from tampering with the ledger?
  - Answer: **By making it easy to detect that the ledger had been tampered with**
  - Any dishonest participant would then be dissuaded from even trying
- Tampering with the ledger is what, in economics, we call an “off-the-equilibrium path.”
  - No one will do it, incentives to prevent it exists

# Tampering with the Ledger

- Consider a simple example
  1. Maria creates a single MariaCoin
  2. Maria sells the MariaCoin to Sophie
  3. Sophie sells the MariaCoin to Geoff
- Thus it is clear that, at the end, Geoff is the rightful owner of MariaCoin
- But what if Bob were to come in and attempt to change the second stage: *to read that Maria sells MariaCoin to Bob, not Sophie.*
- This would undermine Geoff's ownership rights to the coin
- We need to detect possible tampering all along the chain

# Tampering with the Ledger

- Solution: We make the ledger recursive:
  1. **M**aria **C**reates a **S**ingle **M**ariaCoin <**MCSM**>
  2. **M**aria sells the **M**ariaCoin to **S**ophie <MSMS<mcsm>>
  3. **S**ophie sells the **M**ariaCoin to **G**eoFF <SSMG <msms<mcsm>>>>
- In creating this shorthand, I followed a simple algorithm. I used the first letter of each of the words.
- To detect tampering, just check if the initials match the words in the previous step



# Detecting Tampering Attempts

1. Maria Creates a Single MariaCoin

<MCSM>

2. Maria sells the MariaCoin to Sophie

<MSMS<mcsm>>

3. Sophie sells the MariaCoin to Geoff

<SSMG <msms<mcsm>>>>

1. Maria Creates a Single MariaCoin

<MCSM>

2. Maria sells the MariaCoin to Bob

<MSMB<mcsm>>

3. ~~Sophie~~ Bob sells the MariaCoin to Geoff

<BSMG <msmb<mcsm>>>>

# Short summary

- A tamper-proof ledger is a key feature of Bitcoin that enforces property rights
- How do you make a ledger tamper-proof when it is distributed?
  - You make sure any attempts will be discovered
  - By making the ledger recursive.
    - **Every entry contains a little copy of the previous entry**

# What is Blockchain?

- Blockchain is the same idea but with cryptography so that it is hard to work around
- Blockchains store large groups of transactions into blocks, not just one at a time
- The key elements
  - The linked list
  - The hash function
  - The hash pointer
  - Putting it together: Blockchain

# What is Blockchain?

- Pointer
  - A language object that stores the memory address of another value located in computer memory
- Linked list
  - A linear collection of data elements such that each element contains a pointer that points to the next
  - The elements might be in entirely different places, but they are connected by pointers
  - The pointers turn a collection of objects into an ordered list
    - Could be a list of financial transactions → a ledger!

# The Hash Function

- A function takes an input and returns an output
  - Can't have more than one output per input
  - Can have more than one input per output
- Hash function – takes an input of (virtually) any size and returns an output of a fixed size
- In this case a 256-bit number

# The Hash Function

1. Maria Creates a Single MariaCoin  
<MCSM>
  2. Maria sells the MariaCoin to Sophie  
<MSMS<mcsm>>
  3. Sophie sells the MariaCoin to Geoff  
<SSMG <msms<mcsm>>>>
- Replace the digest method with one using hash functions
  - SHA-256 - Same has function as Bitcoin
  - Takes anything and turns it into a 256-bit number
  - <https://www.movable-type.co.uk/scripts/sha256.html>



*Movable Type Scripts*

## SHA-256 Cryptographic Hash Algorithm

A **cryptographic hash** (sometimes called 'digest') is a kind of 'signature' for a text or a data file. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text. See **below** for the source code.

Enter any message to check its SHA-256 hash

Message

Hash

e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

1.410ms

Note SHA-256 hash of 'abc' should be: ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad

# The Hash Function

The ledger with hashes of the previous entry:

1. Maria Creates a Single MariaCoin

8a6daa572851240bb8bf3268e0083e02ed6008ebd8aaf3d46a47baa0738afcae

2. Maria sells the MariaCoin to Sophie

1b5be645bf51c8b9479f9f2b6d96d0d26372bbd8e0f1771a977e43023bc324ae

3. Sophie sells the MariaCoin to Geoff

be954137213e978adb80053e3f82cbe1ca9de5767392786aecdade74ce008e9  
7

The hash function of the functions of the 3 steps is:

3401cd5f6a4b18a17eb3aaa571ba55bc4bcb6d0926f03cf7e9a7f977b489aced



# The Hash Function

SHA-256 is a cryptographic hash function

- Two inputs are very unlikely to produce the same output (collision resistance)
- It must be possible to find inputs that produce the same output
- The input space is much bigger than the output space
- Hiding: given an output it is virtually impossible to reverse-engineer the input

# The Hash Function

- Even a tiny amount of tampering will produce inconsistency between the statement and the hash
- Collision-resistance and hiding means that one cannot cleverly tamper to produce the same hash
- Recursivity means one has to tamper all along the chain to not be discovered

# Hash function

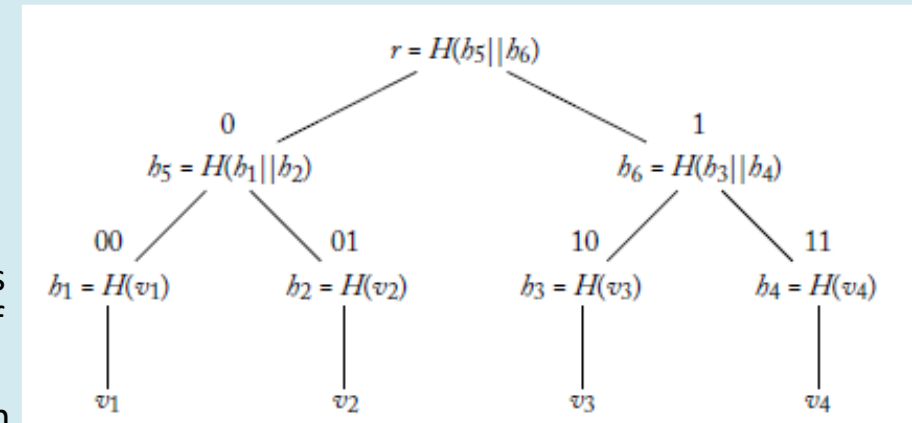
- Hash function: **A hash function  $H$  takes a message  $x$  of arbitrary but finite size and outputs a fixed size hash  $h$  (also called digest).**
- When not explicitly stated differently, we refer to a cryptographic hash function whenever the term hash function is used.
- **Cryptographic hash function:** There are four additional properties of a hash function that have to be fulfilled so that the function qualifies as a cryptographic hash function (E. Lombrozo, J. Lau, and P. Wuille. Bitcoin improvement proposal 141 (bip141): Segregated witness (consensus layer).  
<https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki>):

# Hash function, cont.

- **Easy to compute:** It is computationally easy to calculate the hash of any given finite message.  $h=H(x)$ , where  $h$  is of fixed length.
- **Pre-image resistance:** *It is infeasible to generate a message that has a given hash value.* Infeasible in this context means it cannot be achieved by an adversary as long as the security of the message is important.
  - In terms of complexity theory, this is defined as not being possible in polynomial time
  - Because of this property, **cryptographic hash functions are also called one-way functions** (Given a hash  $h$  it is infeasible to find any message  $x$  such that  $h=H(x)$ )
- **Second pre-image resistance:** *It is infeasible to find two different messages which produce identical outputs, i.e., a collision, when given as input to the hash function.*
- **Collision resistance:** *It is infeasible to find any two different messages which produce identical outputs, i.e., a collision, when given as input to the hash function.*

# Hash function : Merkle tree

- Merkle tree: A tree constructed by hashing paired data (the leaves), then pairing and hashing the results until a single hash remains, the merkle root. In Bitcoin, the leaves are almost always transactions from a single block.
- In Merkle's paper it was introduced the concept of a one-time signature scheme that relies on a "infinite tree of one-time signatures."
- This underlying concept later became known as a Merkle tree, hash tree, or authentication tree.
- Merkle trees are binary trees in which the leaf nodes are labelled with the values that need to be authenticated and each nonleaf node is labelled with the hash of the labels or values of its child nodes.
- Figure shows an example Merkle tree with  $n=4$  values and the resulting root hash or Merkle tree root  $r$ . Nodes are referenced with a binary string representing their position, e.g., node 01 is labeled  $h_2$ .
- To authenticate a value  $v_1$  and prove that it was part of a Merkle tree with root hash  $r$ , the values  $h_2$  and  $h_6$  are required. For more information on Merkle trees see (G. Becker. Merkle signature schemes, merkle trees and their cryptanalysis. Ruhr-University Bochum, Technical Report, 2008)
- R. C. Merkle. A digital signature based on a conventional encryption function. In Conference on the Theory and Application of Cryptographic Techniques, pages 369–378. Springer, 1987. DOI: 10.1007/3-540-48184-2\_32.



# Asymmetric cryptography

- The second most important primitive on which cryptographic currencies are based is asymmetric cryptography.
- Since cryptographic currency technologies mostly rely on well researched algorithms and parameters in this context (e.g., Bitcoin uses Secp256k1 [Certicom Research. SEC 2: Recommended elliptic curve domain parameters, version 2.0. [http://www.secg.org/collateral/sec2\\_final.pdf](http://www.secg.org/collateral/sec2_final.pdf), 2010.]), we will not go into detail regarding the aspects concerning this broad field of research.
- **Public-key encryption:** A public-key encryption scheme is defined as a triple of efficient algorithms (**G**; **E**; **D**) where:
  - **G** is a key generation algorithm that takes no input and outputs a key pair  $(pk; sk)$ , where  $pk$  is called public key, which can be shared publicly, and  $sk$  is called secret key, which should be kept private  $(pk; sk) \leftarrow G()$ .
  - **E** is a encryption algorithm that takes as input a public-key  $pk$  as well as a message,  $m$ , and outputs a cipher text,  $c$ , encrypted under the public-key,  $pk$ , associated with the public/secret key pair  $(pk, sk)$  of the intended recipient.  $c \leftarrow E(pk; m)$
  - **D** is a (deterministic) decryption algorithm that takes as input a secret-key,  $sk$ , as well as a cipher text,  $c$ , and outputs the message,  $m$ , that was encrypted under the public key,  $pk$ , associated with  $sk$ , or  $\perp$  (The truth value 'false') if the wrong keys have been used.  $m \leftarrow D(sk, c)$



# WHAT IS BLOCKCHAIN?



# Intro

- Blockchain technology arose with the invention of the digital currency Bitcoin in 2009
- A shared, immutable ledger that facilitates the recording of transactions in a network
- Provides the means for recording any transaction or track the movement of any asset, not just a digital currency
- Assets recorded on blockchain can be tangible (cash, gold, or real estate), or they can be intangible (intellectual property, copyrights, or licenses)

# Block Chain

- It is a linked-list
  - With a hash pointer instead of a pointer linking objects
- The objects are not individual transactions, but rather blocks with several thousand transactions
- A hash pointer is the hash function applied to the previous entry when it was created
- Technically, blockchain is not tamper proof
- It is tamper-proof in the strongest sense: no-one has an incentive to try

# Building the Blockchain

- The blockchain begins with the “stack”
  - Has projects with multiple layers of protocols
    1. Base layer (Internet)
    2. Application protocol (transaction record, consensus rule-cryptography, P2P network-nodes, mining, tokens)
    3. Application layer at the top of the “stack” (contracts, applications)
- By replicating and storing user data across a decentralized network rather than individual applications controlling access to silos of information, blockchain does two things
  - 1. Reduces barriers to entry
  - 2. Creates a potentially more competitive ecosystem of products and services

# Block Chain MariaCoin

## 1. Maria creates MariaCoin

- She creates a unique digital ID representing the coin and signs it with her private key

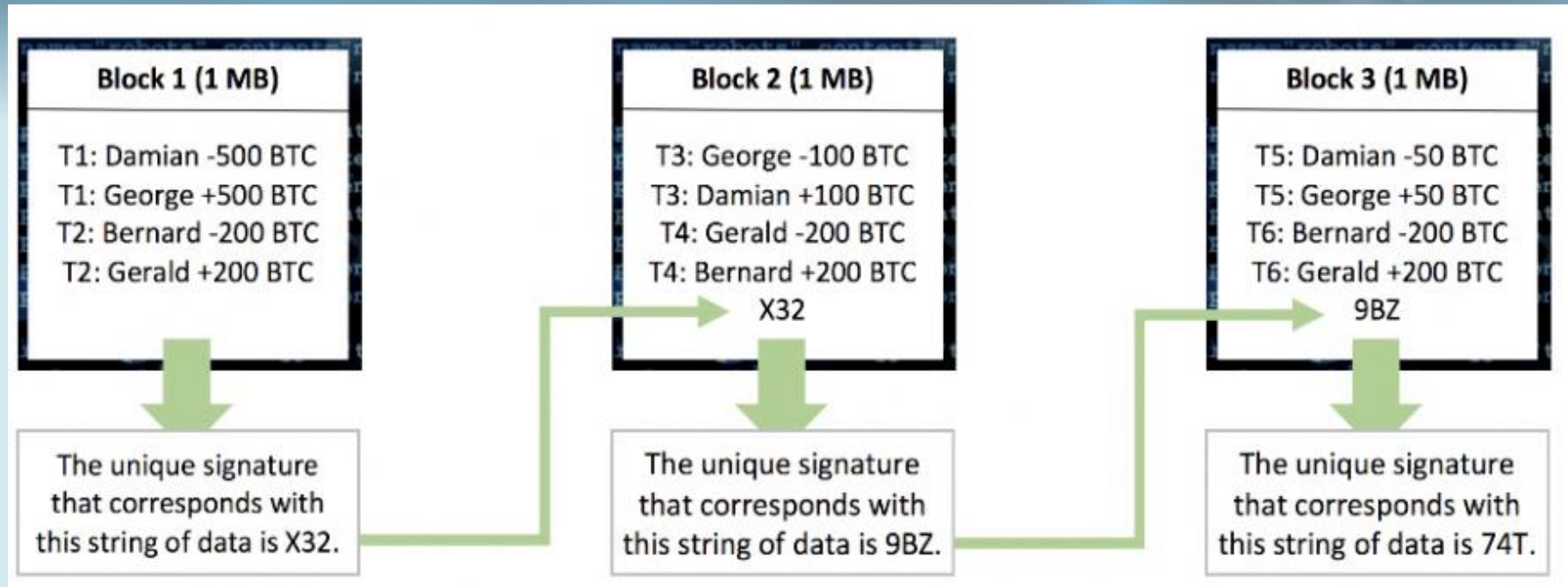
## 2. Maria writes a message “Pay Sophie with this coin.”

- **Sophie** = Sophie’s public signature
- **This coin** = a hash pointer to the coin

## 3. Maria signs the message with her private key

- Using Maria’s public key, any user can view this series of operations and verify that Sophie is the valid owner of the coin
- The ledger is secure, property rights are valid
- Sophie can repeat steps 2 and 3 to transfer the coin where she likes

# Blockchain



- The link between the blocks is cryptographic.
- Each block incorporates a coded summary of the entire preceding chain.
- As a consequence, the chain cannot be retroactively altered without such changes being immediately visible to all participants.
- The existing blockchain is thus “immutable.” This immutability is a great advantage when there is a need for full integrity and transparency in record keeping.
- It can, however, also be a source of difficulties.
- When the blockchain is used to support a payment system, immutability means that errors cannot be corrected and fraudulent transactions cannot be rectified without tampering with the protocol.

# The Double-spend Attack

Sophie can repeat the protocol to pay another user (Geoff) with the coin

AND

Can then repeat the protocol again to pay yet another user, (Mike) with the coin

- There are no safeguards in the system to prevent Sophie from spending the coin twice



# The Double-spend Attack

## JamesCoin

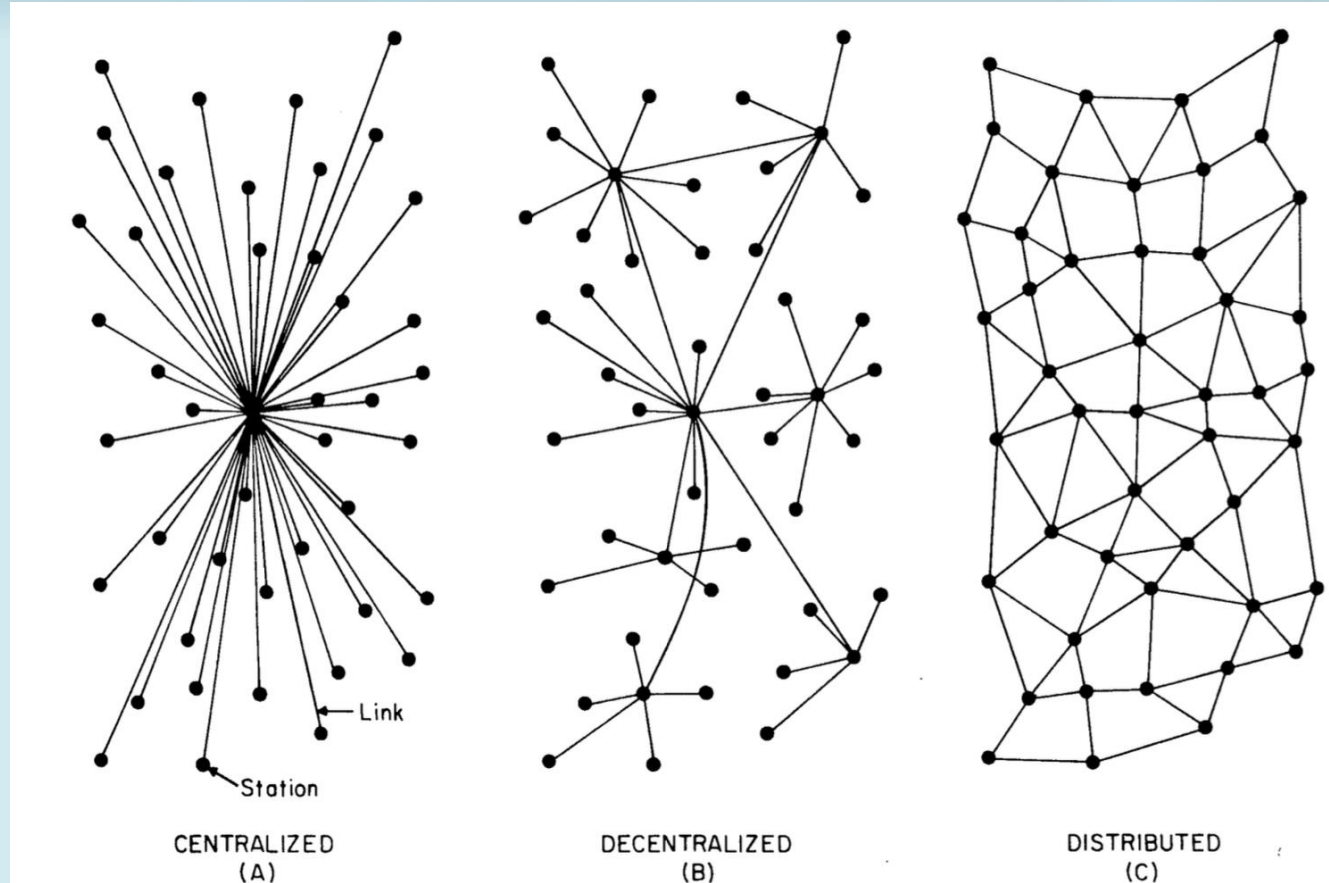
- Like MariaCoin, but with one key difference:
    - **All transactions in the ledger must be signed by James to be valid**
1. James creates JamesCoin
  2. James writes a message “Pay Sophie with this coin.”
  3. Sophie can then write a message “Pay Geoff with this coin.”
  4. Both Sophie and James sign off on this last message
    - Because James has signed the message “Pay Geoff with this coin” his software “knows” that Geoff is the valid owner
    - It will not let him sign off on a contradictory message
    - The ledger can be widely distributed, and is tamper-proof, due to blockchain technology
    - Even James himself cannot manipulate the ledger without detection
    - For these reasons, this is more decentralized than a credit card or bank





# **DISTRIBUTED CONSENSUS**

# Centralized vs decentralized vs distributed



# Distributed Consensus: What is it?

- A distributed network of systems running Bitcoin software
  - Consists of thousands of nodes (computers)
  - Each node is connected to every other node in the network
  - The system has no (built-in) central authority
  - It is fully peer-to-peer

# Distributed Consensus

- **Goal – to create a protocol that allows all nodes to agree**
  - Not sufficient
    - We want the nodes to agree on “the truth.”
    - Some nodes can be honest, some can be malicious
- Distributed consensus protocol
  - A network of nodes, each receiving a value
  - Some are malicious, some honest
  - Must terminate with all honest nodes in agreement on the value
    - The value must have been generated by an honest node

# Application to the Blockchain

- Assume that the system starts off in a good state
  - All honest nodes are in agreement on the ledger
- New transactions come in
  - Some potentially contradictory
- The distributed consensus protocol will end with a new block added to the ledger, consisting of valid transactions, on which all nodes agree

# How Do We Get There?

- Bitcoin protocol avoids assuming that any one node is honest
  - Avoids assigning stable identities to the nodes at all
- We cannot prefer any one node over the other
- How to reach consensus
  - Use randomness

# Brief Review of the Hash Pointer

- A hash pointer to a block is:
  - the output of the hash function applied to that block (“the hash”) and a pointer to that block
- Each block in the blockchain includes a hash pointer to the previous block



# Bitcoin Distributed Consensus Algorithm – First Pass

1. New transactions are broadcast to all nodes
2. Each node collects these transactions into a block
3. At a fixed interval, a random node gets to propose its block
  - Including a hash pointer to this previous block
4. All nodes check the block to make sure the transactions are valid
5. Repeat steps 1 – 4

This method avoids some obvious problems

- Not possible to spend bitcoins not belonging to you
- Not possible to deny service to a certain user whom you don't like
- That user just waits for the turn of an honest node
- It also avoids some more subtle problems

# Distributed consensus protocol

It:

- Pick nodes at random
- Makes it hard for any single node to control the blockchain
- Automatically disincentives malicious behavior

# Distributed consensus protocol: PoW

Ideally like to do is only pick honest nodes, and never pick malicious ones

- This is impossible
  - Nodes do not have identities
- What if you could somehow turn a node into an honest node?
  - Impossible for two reasons
    - There is no such thing as computer-generated randomness
    - It would require a centralized computer to generate the randomness, and everyone would need to agree on it

# Proof or Work

Two problems to solve:

1. **Generating randomness**
2. **Incentivizing honest behaviour**

- Solving one problem helps with the other:
  - If randomness is not good enough, it makes it more likely a malicious node will take over the system
  - If we incentivize honest behaviour, then fewer nodes are malicious
    - Decreasing the need for true randomness

# Proof or Work

It's worth understanding PoW for at least two reasons:

## 1. Contains some genuinely new ideas

- Many intermediaries profit off of information (Uber, Facebook, google, etc.)
- What if information could be stored and accurately maintained in a decentralized way?

## 2. On the other hand: many believe that PoW contains the seeds of

Bitcoin's downfall

# PoW Concept 1: Block Reward

- **Pick a node at random** to propose a block
- **Give the node that proposes the block some extra bitcoins to transact with**
  - a clever idea in the Bitcoin protocol thus is to use seignorage to finance the functioning of the system (seignorage is a profit made by issuing currency).
    - Because it depends on currency creation inside the system, the Bitcoin method of consensus cannot easily be transposed to other decentralized systems with no money creation.
- **As part of the block, it gets to include a transaction with these bitcoins (presumably to pay itself)**
- This acts to keep blocks honest
  - **How does block reward act to keep a node honest?**
  - The only way to receive your reward is if future nodes accept their block
    - *They do this by including a hash pointer to your block in the next block they propose*
  - If you act maliciously, extending, an orphaned fork with transactions to you or your friends
    - The next node is unlikely to accept your block

# PoW Concept 1: Block Reward

- Playing devil's advocate
  - Suppose most nodes are not honest, but rather are malicious
    - If you are malicious, the next node might choose to reward your behaviour by accepting your block
    - If you are honest, the next node might choose to punish you by accepting a different block
- Then dishonest behaviour would be rewarded, and that would be bad
- Rely on the fact that nodes behave honestly unless incentivized otherwise
  - Malicious nodes are out for their own good
- Not assuming that:
  - malicious nodes are designed for the destruction of the system



# PoW Concept 1: Block Reward

- Why is this?
- For instance: I propose a block that exhibits self-dealing
- The next node chosen to propose a block (Alice)
- Would Alice accept my block, rewarding my malicious behavior?
  - Alice also wants to receive the block reward!
    - Accepting my block makes it less likely that her block will be accepted in the next round
    - She needs to be both malicious and without self-interest
- In the background: a prevailing view that most nodes are acting honestly, because all incentives are for them to do so

# Bitcoin Mining

- Bitcoin mining is a resource-intensive activity that results in the discovery of new coins
- Thus the analogy to precious metals implicit in the word “mining”

# The Hash Puzzle

- Nodes compete to have a chance to propose the next block
- They succeed if they are the first **to solve a hash puzzle**
  - The hash puzzle is a cryptographic puzzle
- Puzzle-friendliness implies that these puzzles can be found
- The only way to solve the cryptographic puzzle is through trial and error
- The greater the computing power of the node, the more likely it is to solve the hash puzzle
- When it solves the hash puzzle, it proposes the block, with the potential to receive the block reward (if the block is accepted)
  - Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.
- It has thus “mined” new bitcoins
- Important: all nodes can verify that a given node has solved the puzzle

# The Hash Puzzle: extremely simplified example, 1

- The data:
- This is the hash of the latest block (shortened to 30 characters):
- **0000000000000001adf44c7d69767585**
- These are the hashes of a few valid transactions waiting for inclusion (shortened).
- **5572eca4dd4**
- **db7d0c0b845**
- And this the hash of one special transaction that you just crafted, which gives 25BTC (the current reward) to yourself:
- **916d849af76**

# The Hash Puzzle: extremely simplified example, 2

- Building the next block:
- Now, let's use a gross approximation of what a new block might look like (the real one uses binary format).
- It contains the hash of the previous block and the hashes of those 3 transactions:
- **00000000000000001adf44c7d69767585--5572eca4dd4-db7d0c0b845-916d849af76--**
- Now let's do mining by hand!
- Our goal is to complete this block with a nonce (a piece of garbage) such that the hash of the new block starts with **13 zeros** (considering the previous hash, it seems that **13 zeroes is the current difficulty!**).

# The Hash Puzzle: extremely simplified example, 3

- Mining (trying to finalize this block):
- Let's try with nonce=**1**, and compute the hash of the block (using the md5 hash algorithm, but Bitcoin uses double sha256!):
- **> echo "0000000000000001adf44c7d69767585--5572eca4dd4-db7d0c0b845-916d849af76--**1**" | md5sum**
- **8b9b994dcf57f8f90194d82e234b72ac**
- No luck, the hash does not start with a 0... Let's try with nonce=**2**
- **> echo "0000000000000001adf44c7d69767585--5572eca4dd4-db7d0c0b845-916d849af76--**2**" | md5sum**
- **5b7ce5bcc07a2822f227fcae7792fd90**
- No luck...



# The Hash Puzzle: extremely simplified example, 4

- ...
- If we pursue until nonce=**16**, we get our first leading zero.
- `> echo "00000000000001adf44c7d69767585--5572eca4dd4-db7d0c0b845-916d849af76--16" | md5sum`
- **03b80c7a34b060b33dd8fbbece79cee3**
- For nonce=**208**, we get two leading zeroes!
- `> echo "00000000000001adf44c7d69767585--5572eca4dd4-db7d0c0b845-916d849af76--208" | md5sum`
- **0055e55df5758517c9bed0981b52ce4a**
- So continuing like this... you can finally find a hash that has 13 leading zeroes. And you can WIN!
- But you'll have to be fast (faster than other miners)
- If someone manages to build a block before you do, you'll have to start again from the beginning with the new block's hash (the one of the winner)



# Proof of Work and Randomness

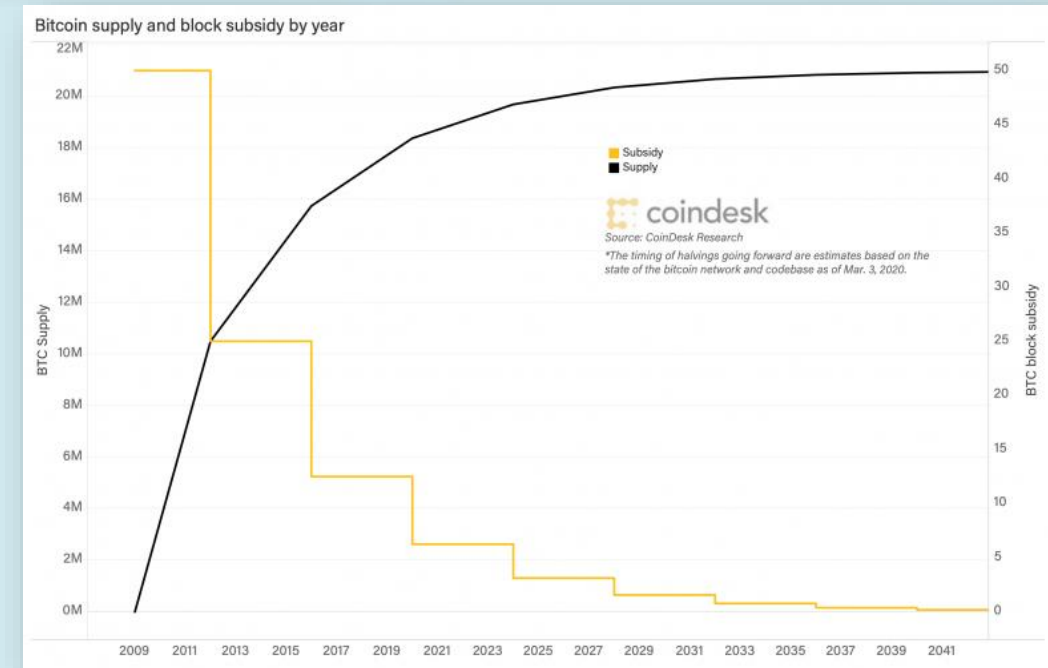
- Proof of work is therefore the solving of a hash puzzle
- For which the node is rewarded by being able to propose a block
- And for the block reward, given in bitcoins
- Notice that proof of work creates the randomness that we were missing!

# Proof of Work and Randomness

- For two competing nodes with roughly equal processing power, there is no way to predict which node will solve the puzzle first and get to propose its block
- Is block selection random?
  - **Unpredictable? Yes.**
    - Only way to predict which one will win is by having as much computing power as the two nodes combined
  - **Nondeterministic? No.**
    - A nondeterministic algorithm is an algorithm that, even for the same input, can exhibit different behaviours on different runs, as opposed to a deterministic algorithm.
  - Note: a process can be both deterministic and random (Henri Poincare in the 19th century)

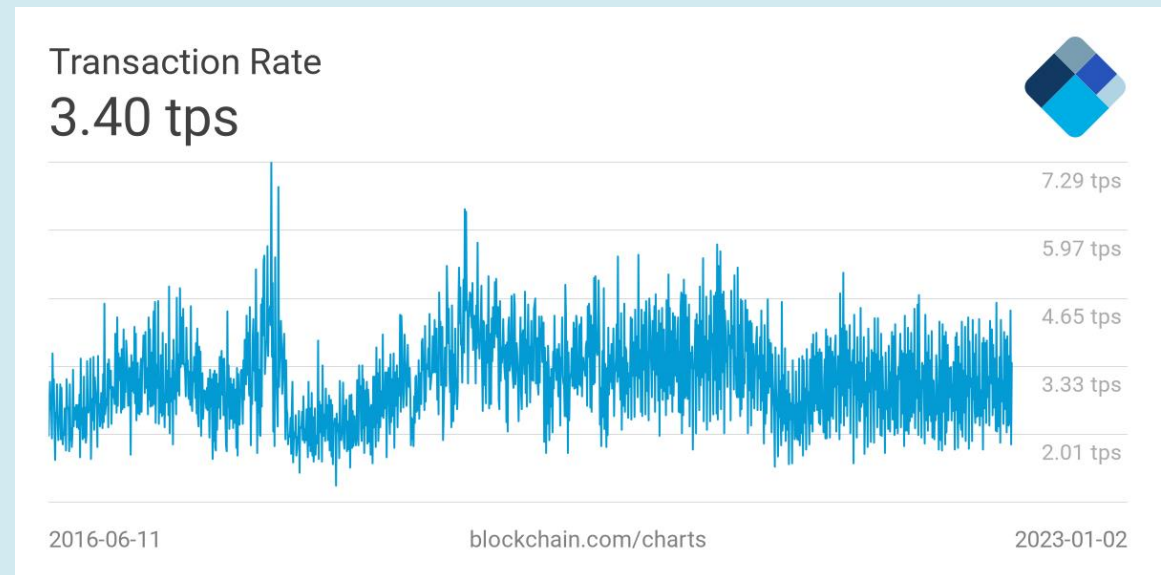
# Currency Creation

- Block rewards
  - Only way within the Bitcoin reference software for new coins to be mined
  - Even block rewards are limited
- Every 210,000 blocks, the block reward is cut in half
- Occurs every 4 years (approximately)
- Implies the total number of bitcoins will converge to 21 million
- **Bitcoin is Scarce:** Today, there are about 18.5 million Bitcoin in circulation, with approximately 2.5 million waiting to be mined (created).
  - After the last Bitcoin is mined — around the year 2140 — no additional Bitcoin will come into circulation.
- This scarcity makes Bitcoin similar to gold, except unlike gold, there are no undiscovered
- It does not imply that Bitcoin is subject to deflationary pressures
- It does imply that Bitcoin supply cannot be manipulated by a central bank.
- Bitcoin deposits that could skew the market. As Bitcoin adoption continues to grow, there will be increasing competition for a decreasing amount of new Bitcoin.



# Inefficiency of mining

- The most spectacular, and frequently mentioned, is the energy consumption.
- It is estimated that Bitcoin miners use 40.64 TWh of energy to operate annually, slightly more than Hungary, the world's 57th largest consumer of energy.
- This is also 75 times higher than the annual energy consumption of the centralized Visa network, which processed an average of 150 million transactions per day in 2016, compared to the 44 million transactions processed on the Bitcoin network for the whole of 2017 (L. Schilling, and H. Uhling, 2018).
- Later, Bitcoin processes about 200 transactions per minute, while Ethereum, which is faster, can process 1200.
- By comparison, Visa and MasterCard each process about 100,000/minute. (V. Buterin 2014).

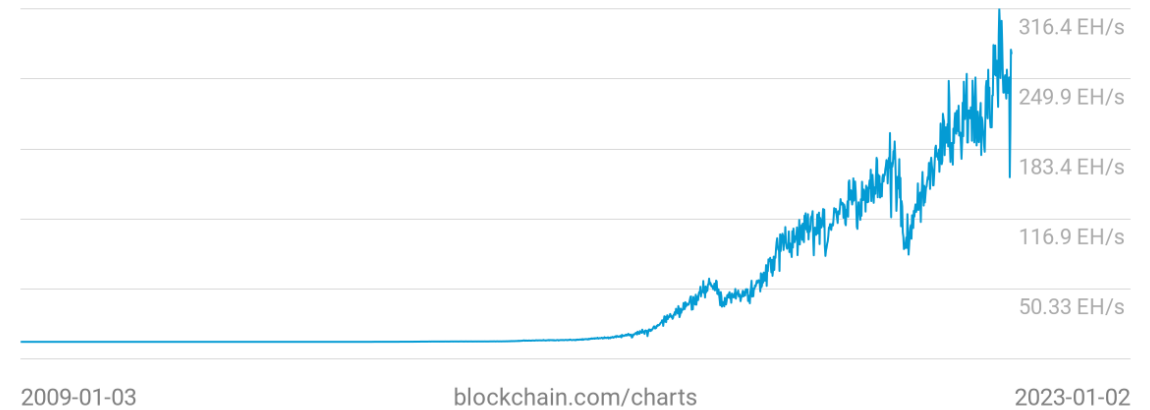


# Hash rate

- *The higher the hash rate, the more blocks are being mined which increases the chance an individual miner has to solve the block reward puzzle and receive newly mined bitcoin.*
  - **The more hashing (computing) power in the network, the greater its security and its overall resistance to attack.**
- A high hash rate is a general indication of a healthy bitcoin mining environment.
  - It means a growing number of miners are using the **most efficient mining hardware** they can afford and competing with each other to process transactions and solve the block reward puzzles.
  - This proof-of-work makes the Bitcoin blockchain secure and immutable.
- From an investor's point of view, the hash rate is an interesting metric to follow as **it shows that miners are investing in and deploying new equipment, possibly in anticipation of a rising Bitcoin (BTC) price.**
- **Advocates of the 'price follows hash' theory - the price of bitcoin follows the hash rate.**

Hash Rate

274.2 EH/s



The hashing power is estimated from the number of blocks being mined in the last 24h and the current block difficulty.

More specifically, given the average time  $T$  between mined blocks and a difficulty  $D$ , the estimated hash rate per second  $H$  is given by the formula  $H = 2^{32} D / T$

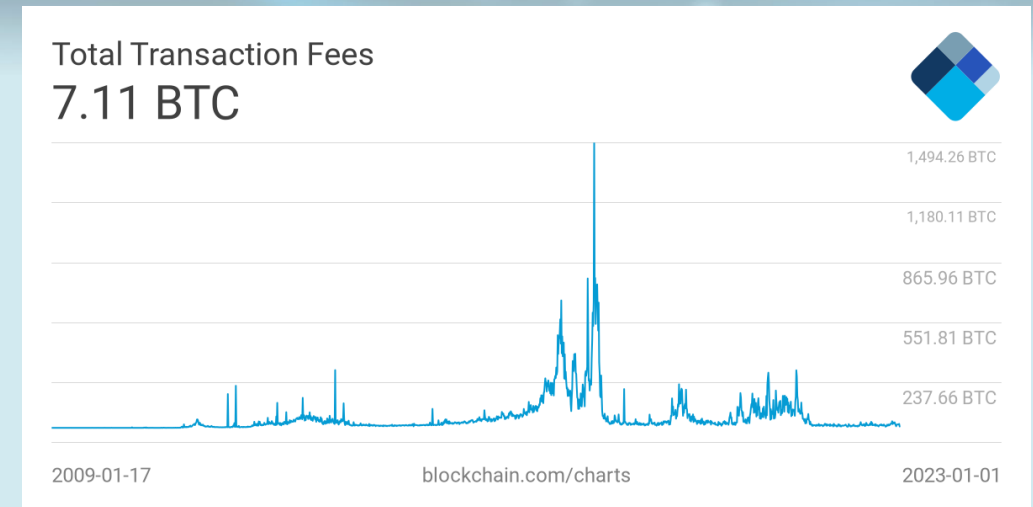
# The Transaction Fee

- The potential rewards to mining go beyond receipt of bitcoins
- Includes the receipt of transaction fees
- The node proposes transactions in which the value of bitcoins coming in exceed the value of bitcoins going out
- The remainder gets to be paid to an address of the node's choosing
- Ensures continuing incentives for trade in Bitcoin



# The Transaction Fee

- Transaction fees are based on the data volume of a transaction and the congestion of the network.
- Miners spend computing power and energy validating transactions for a financial reward
  - *with every block (a collection of transactions not exceeding 1 MB in size) added to the blockchain comes a block reward (currently 6.25 BTC), as well as all fees sent with the transactions that were included in the block.*
- Miners have a financial incentive to **prioritize the validation** of transactions that include a **higher fee**.
- **Because a block on the bitcoin blockchain can only contain up to 1 MB of information, there is a limited number of transactions that can be included in any given block.**
- When a large number of users are sending funds, there can be more transactions awaiting confirmation than there is space in a block.
- **Smaller transactions are easier to validate; larger transactions take more work, and take up more space in the block.**
  - For this reason, miners prefer to include smaller transactions.
    - A larger transaction will require a larger fee to be included in the next block.



- Fees skyrocketed in December 2017



# So:

- Proof of work incentivizes behaviour through block reward
- Creates randomization by making nodes compete to be the first to solve a hash puzzle
- Randomization only among nodes with the great computing power
- Proof of work builds in currency creation and then ensures stabilization
- Transaction fees incentivize honest trading

# Future Challenges: PoW Challenge 1: The 51% Attack

- What if a node succeeds in gaining a majority of the CPU power across all nodes?
- This node would be the first to solve all the hash puzzles
- This node could then build the longest chain in the blockchain
- The system would then revert to being centralized
  - If a node were to obtain a majority of CPU power it would have to act as a benevolent dictator
- The only possible reward to CPU power is bitcoins
- A malicious 51% attacker could include lots of payments to him- or herself
- No other nodes would actually let this attacker spend the coins
- Any such attack is limited in its profitability
- Any such attacker has an incentive to maintain trading in bitcoins

# Future Challenges: PoW Challenge 1: The 51% Attack

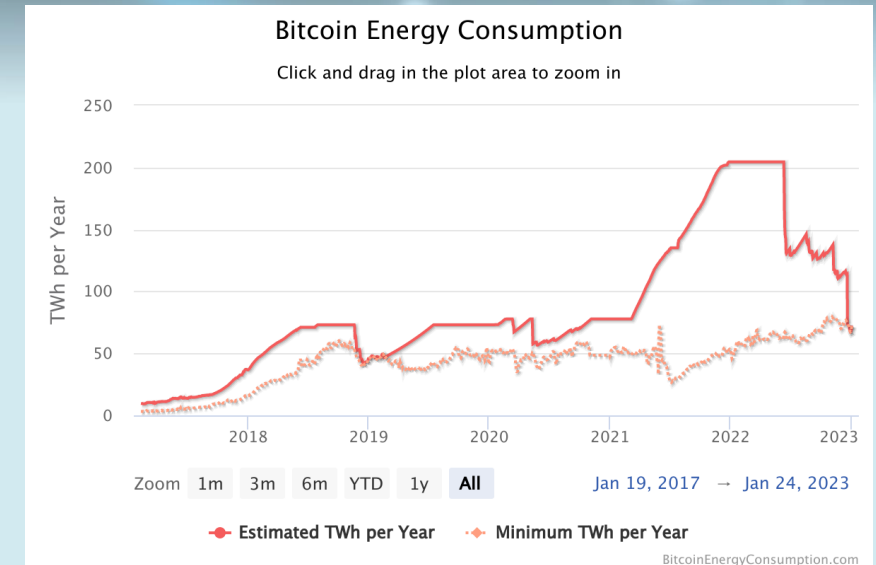
- Most bigger cryptocurrencies have sufficient mining capacity behind them, making it extremely expensive to acquire the necessary hardware to pull an attack like this off.
- Smaller cryptocurrencies have less hashing power securing the network, making it possible to simply rent hashing power from miners on a service like Nicehash for a few hours. This significantly reduces the capital costs of an attack.
- There have been a number of 51% attacks including a high profile attack against Bitcoin Gold where \$18 Million was stolen (2018, 2020)
- Krypton and Shift, two blockchains based on Ethereum suffered 51% attacks in August 2016
- The Bitcoin SV (BSV) network suffered an attack in August 2021
- Litecoin 51% attack in 2019
- Ethereum in 2020

# Related: Oligopoly Power

- A weaker version of the 51% attack is what would happen if a small number of nodes were to control all mining power
- As bitcoin mining has become industrialized, this has been occurring (see the white paper “Analysis of Large-Scale Bitcoin Mining Operations.”)
- Miners could form a cartel and charge high transaction fees
- Could be seignorage, under another name

# PoW Challenge 2: Resource Intensity

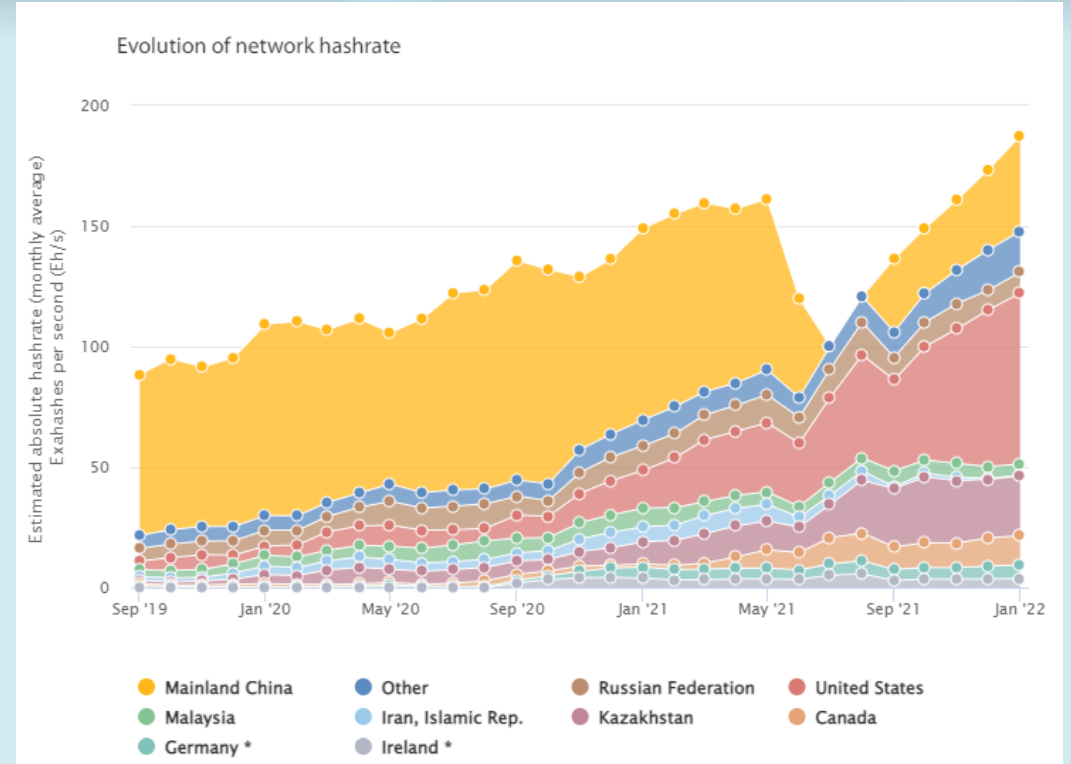
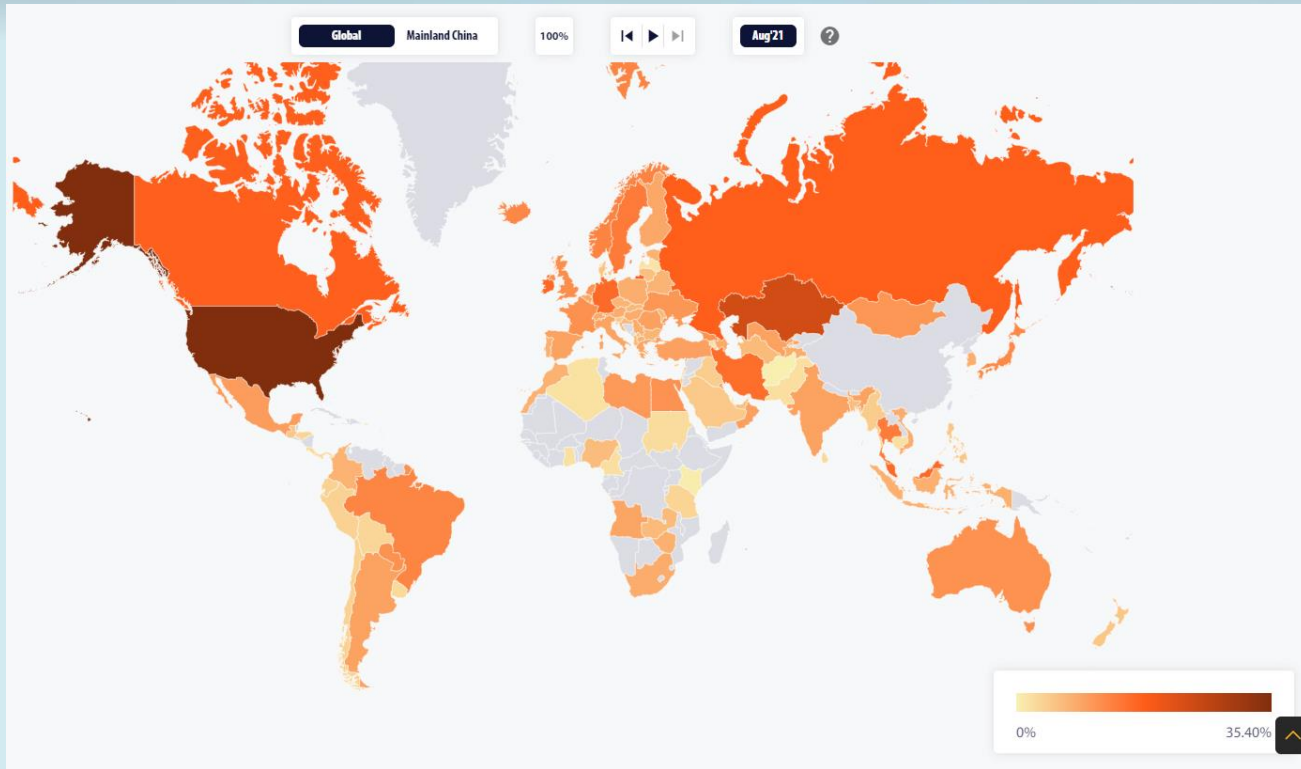
- Bitcoin mining uses lots of electricity
  - High ends of estimated amounts consumed are only 6% of the global banking sector
  - Mining takes place where energy is not a scarce resource
- A “Green” critique of Bitcoin
  - Miners are using energy for no purpose
  - PoW is a technology that enables trading in bitcoin
    - Implemented by a zero-sum game
  - As long as one believes Bitcoin is a net benefit to society, there is a net benefit to mining



Carbon Footprint	Electrical Energy	Electronic Waste
444.59 kgCO <sub>2</sub>	797.11 kWh	444.90 grams
Equivalent to the carbon footprint of 985,374 VISA transactions or 74,099 hours of watching Youtube.	Equivalent to the power consumption of an average U.S. household over 27.32 days.	Equivalent to the weight of 2.71 iPhones 12 or 0.91 iPads. (Find more info on e-waste <a href="#">here.</a> )

<https://digiconomist.net/bitcoin-energy-consumption/>

# Bitcoin mining

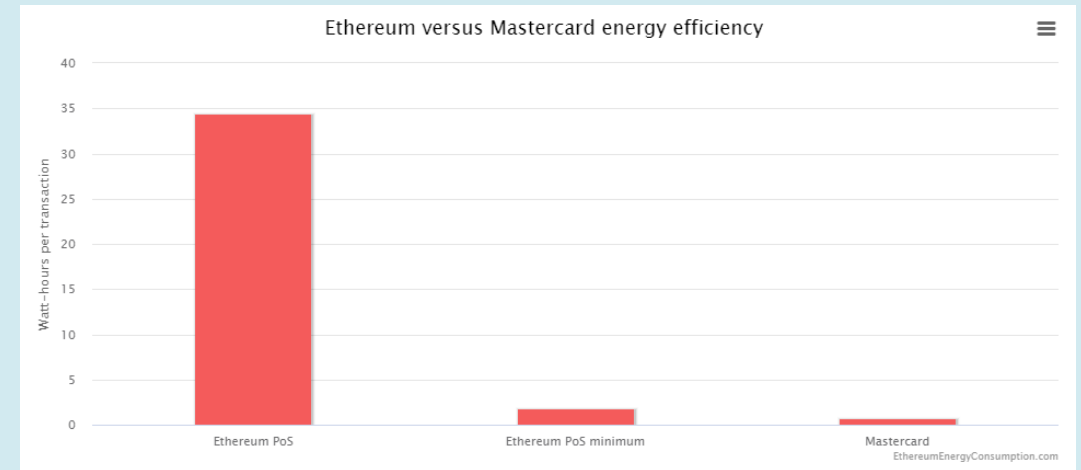


[https://ccaf.io/cbeci/mining\\_map](https://ccaf.io/cbeci/mining_map)



# Challenge 2: Resource Intensity

- Even PoS is less sustainable than some centralized solutions, like Mastercard;
- Blockchains are distributed ledgers in which data and processes are replicated over many different nodes in the network, which introduces significant data redundancy.





# PoW Challenge 3: Can the Network Scale?

- Blocks are limited in size
- Blocks can only be created about every 10 minutes
  - Implies that there are about 7 transactions per second
- Trilemma: Blockchain systems can have at most 2 of the three:
  - **1. Decentralization**
  - **2. Scalability (efficiency)**
  - **3. Security**
- Bitcoin and Ether sacrifice efficiency for the sake of security and decentralization.
- Other crypto currencies are based on different choices, often with more centralization to achieve speed. But the tradeoff seems unavoidable.



# **TYPES OF THE CONSENSUS**

# The Proof of Work (summary, discussed above)

- the first consensus mechanism introduced with Bitcoin.
- In POW, all the miners (mining is discussed later in the chapter) compete to solve a mathematical problem, and the one who solves it fastest becomes the winner.
- Soon other miners start validating it until it reaches an agreed-on percentage (51 percent or 90 percent as per the configuration).
- POW works on the “longest chain” rule;
  - in other words, if there are forks created because of different miners agreeing to different side chains, then the longest chain that moves the fastest is the most trustworthy;
  - soon others will start following that chain, and other side chains will be discarded.
- Used by: Bitcoin, Ethereum
- Advantages: Time tested, safe
- Disadvantages: Too slow, massive power consumption

# Proof of Stake

- POS consensus has nothing to do with mining, yet it still validates the blocks and adds to the blockchain.
- This collateral-based consensus algorithm **depends on the validator's economic stake in the network.**
- In other words, each validator must own some stake in the network by depositing some money into the network.
- In POS-based consensus for public blockchains, several validators take turns proposing and voting on the next block, and the weight of each validator's vote depends on the size of its deposit.
- Used by: Ethereum v.2, Cardano (ADA), Solana (SOL), Algorand (ALGO), Tezos (XTZ)...
- Advantages: Security, reduced risk of centralization, and energy efficiency
- Disadvantages: more prone to attack as there is no computational factor like with POW to keep the network safe
- In POS the entire process of validating a new block and getting a fraction of the cryptocurrency as a reward is called minting (not mining).

# Delegated Proof of Stake

- The DPoS is a variation of the POS consensus model where all the users vote to select the ones who will be the final approvers of transactions in a democratic way.
- Therefore, the DPoS algorithm creates a **voting system that is directly dependent on the delegates' reputation.**
- If an elected node misbehaves or does not work efficiently, it will be quickly expelled and replaced by another one.
- Since a DPoS system is maintained by the voters, the delegates are motivated to be honest and efficient or they get voted out.
- Used by: Terra (LUNA), TRON (TRX), Bitshares, Steem, Ark, and Lisk
- Advantages: Super-fast, scalable, and high energy efficiency
- Disadvantages: less secure than PoW

# Proof of Authority

- PoA is a modified version of POS where identity is at stake instead of monetary value.
- **The Proof-Of-Authority (PoA) is a consensus method that gives a small and designated number of blockchain actors the power to validate transactions or interactions with the network and to update its more or less distributed registry.**
- It works as follow: according to the chosen scheme, one or more validating machines are responsible for generating each new block of transactions that will be included in the Blockchain.
- The new block can be accepted directly without verification, or by unanimous vote of the block generators, or simply by a majority, depending on the configuration chosen for the Blockchain.
- A blockchain that rests on the PoA can do without using a native asset such as Bitcoin or Ether. Moreover, being a validating node does not immobilise any particular capital as in the case of Proof-Of-Stake for example.
- Used by:
  - Ethereum's Parity; players in the banking sector, such as JP Morgan with the JPMCoin, use this technology to facilitate the audit of their funds movements, mainly for accounting purposes, with reduced costs
  - Polkadot Launch phase Proof of Authority operated as a Proof of Authority (PoA) chain that is maintained by six validators belonging to Web3 Foundation. The chain will only allow users to claim DOT tokens or submit their intention to validate or nominate.
- Advantages: no mining, high in scalability and performance
- Disadvantages: a strong centralisation in the hands of a small number of actors.



# Understanding the Blockchain Ecosystem

- The dynamics of the blockchain are rooted in its ecosystem
- Consists of producers, suppliers, customers, stakeholders and competitors.
- Many smaller ecosystems also comprise blockchain
- Blockchain companies do not always easily fit into one area of the ecosystem
- The blockchain ecosystem is a living map, exhibiting constant change



# Main types of digital asset

- **Type of crypto assets :**
  - **Coin vs Token** : selecting a base coin for a fork, or a smart contract for a payment token;
  - **Crypto-assets backed by assets or not** (such as cash, gold, shares, bonds, or other real world assets);
  - Crypto-assets giving the right to use a service or access a product.
- **The key differences:**
  - **Coins are built on their own standalone independent blockchain** (Bitcoin, Ethereum, XRP, ...); **Coins can be used anywhere.**
  - **Tokens** are cryptocurrencies that **do not have their own blockchain but operate on other existing blockchain**, benefiting from its technology (for instance Ethereum standards ERC-20, ERC223(a return of funds)/ERC621(all unreleased tokens will be burned)/ERC721(unique) tokens...)
  - **Tokens are limited to a specific industry or community;**
  - **Altcoins are considered as coins** that are not Bitcoin (**forks**)

# Coin vs Token: pros and cons

Coins		Tokens	
Pros	Cons	Pros	Cons
Native to their own blockchain	More complex and expensive than creation of tokens; in-depth knowledge of blockchain and coding skills are required	Creating a token is easier and cheaper than creating a coin, as you don't have to create a new code or modify already existing one	Possible will not be having functionality we are looking for
Coins have the same characteristics as money: they are fungible, divisible, acceptable, portable, durable and have limited supply.		More different functions (Utility Tokens- provide people with access to either a product or service; Payment Tokens - to pay for goods and services)	they have certain use case only inside certain project. You can buy a token with a coin, but not vice versa.
Coin operates independently		Token has a specific use in the project's ecosystem	No values as money outside the project
Coins can be used anywhere		More secured (if one does not have resources to develop own blockchain)	Need to pay for any transaction to a blockchain owner

# Bitcoin



- In January Bitcoin price is prox. \$16-17K USD with a 24-hour trading volume of \$16,100,196,128 USD, with a market cap of \$324,524,441,025.
- It has a circulating supply of 19,251,918 BTC coins and a max. supply of 21,000,000 BTC coins.

# Main Characteristics of Bitcoin

- **Bitcoin is Independent**
- **Bitcoin is Scarce (21 million Bitcoin)**
- **Bitcoin is Verifiable**
- **Bitcoin is Portable**
- **Bitcoin is Divisible**

# Bitcoin: strengths/weaknesses

- **Strengths**

- Widespread institutional involvement making it a store of value and fiat hedge
- First mover advantage/name recognition
- Deflationary fully decentralised tokenomics

- **Weaknesses**

- High transaction fees
- Scalability issues implying slow transaction times
- Significant environmental cost due to proof-of-work concept

# Ethereum (ETH)

- Ethereum price today is \$1 200 USD with a 24-hour trading volume of \$5,238,917,682 USD, a market cap of \$153,022,408,612. It has a circulating supply of 122,373,866 ETH coins and the max. supply is not available.
- **Ethereum is an open-source, public, blockchain-based distributed ledger featuring smart contract (scripting) functionality**
- It's the **programmable blockchain**: It enables developers to build blockchain applications with business logic that execute in a trustless environment.
- Ethereum is for more than payments.
  - It's a marketplace of financial services, games and apps that can't steal your data or censor you.
- In Ethereum "smart contracts" are just pieces of code that run on the blockchain and are guaranteed to produce the same result for everyone who runs them. They automatically execute the actions necessary to fulfil an agreement between several parties on the internet
- Ethereum does not have a fixed supply because a fixed supply would also require a fixed security budget for the Ethereum network.
- Ethereum's blockchain is able to host other cryptocurrencies, called "tokens," through the use of its ERC-20 compatibility standard.
  - more than 280000 ERC-20-compliant tokens have been launched.
  - Over 40 of these make the top-100 cryptocurrencies by market capitalization, for example, USDT, LINK and BNB.



# Ethereum (ETH): strengths/weaknesses

- **Strengths**

- First mover advantage in the smart contract domain. Ethereum is the second-largest liquid digital asset (after Bitcoin).
- Most developers, nodes, and dApps of any cryptoasset
- The flexibility of Ethereum's smart contracts
- Network is Turing complete = widespread use and potential application (Solidity is a statically-typed programming language designed for developing smart contracts that run on the Ethereum Virtual Machine, also known as EVM)
  - Alan Turing created a machine that can take a program, run that program, and show some result.
  - But then he had to create different machines for different programs.
  - So he created "Universal Turing Machine" that can take ANY program and run it.
  - A programming language is called "Turing complete", if it can run any program (irrespective of the language) that a Turing machine can run given enough time and memory.

- **Weaknesses**

- Inflationary tokenomics (no fixed cap) - inflation level?
- Scalability of transactions causing high gas fees; scaling issues limit the ability of dApps to grow to some extent.
- Heavy competition from Polkadot, Cardano, Solana



# Litecoin

- Litecoin price is apprx. \$76 USD with a 24-hour trading volume of \$644,305,693, a market cap of \$5,508,154,002. It has a circulating supply of 71,977,805 LTC coins and a max. supply of 84,000,000 LTC coins.
- Litecoin (LTC) is a cryptocurrency targeted to provide fast, secure and low-cost payments by leveraging the unique properties of blockchain technology.
- It was created based on the Bitcoin (BTC) protocol, but it differs in terms of the hashing algorithm used, hard cap, block transaction times and a few other factors.
- Litecoin has a block time of just 2.5 minutes and extremely low transaction fees, making it suitable for micro-transactions and point-of-sale payments.
- This makes it an attractive alternative to Bitcoin in developing countries, where transaction fees may be the deciding factor on which cryptocurrency to support.



# Litecoin: strengths/weaknesses

- **Strengths**

- Faster transaction confirmation than Bitcoin
- Long-standing crypto-asset, solid top 10 ranking
- Quite global listing on exchanges and some adoption

- **Weaknesses**

- Limited development
- Bitcoin can be effectively solve scalability – no need of Litecoin
- The influx of stablecoins threatens Litecoin's use case as a stable medium of exchange.
- Wealth centralization is higher than in Bitcoin or Bitcoin Cash.

# Cardano (ADA)

- Cardano price is approx. \$0.26 with a 24-hour trading volume of 253.51M, a market cap of 9.16B USD. It has a circulating supply of 34.52B ADA coins and a max. supply of 45,000,000,000 ADA coins.
- Launched in September 2017 by IOHK, Cardano is a decentralized blockchain platform on open source smart contracts that works on a proof-of- stake algorithm and provides a base for the cryptocurrency ADA.
- Its first version was released in September 2017.
- The project has taken pride in ensuring that all of the technology developed goes through a process of peer-reviewed research, meaning that bold ideas can be challenged before they are validated.
- There is a maximum supply of 45 billion ADA; now there was a circulating supply of about 31 billion.
- Cardano is used by agricultural companies to track fresh produce from field to table, while other products built on the platform allow educational credentials to be stored in a tamper-proof way, and retailers to clamp down on counterfeit goods.



# Cardano (ADA): strengths/weaknesses

- **Strengths**

- Good development team
- Academic backing
- Transparent roadmap towards decentralisation, scalability, and security
- Cardano uses multiple layers
- Deflationary tokenomics, involving staking support (PoS)
  - Staking cryptocurrencies is a process that involves committing your crypto assets to support a blockchain network and confirm transactions
  - staking is a way of earning rewards for holding certain cryptocurrencies
  - First, participants pledge their coins to the cryptocurrency protocol.
  - Then, the protocol chooses validators to confirm blocks of transactions. The more coins you pledge, the more likely you are to be chosen as a validator.
  - Every time a block is added to the blockchain, new cryptocurrency coins are minted and distributed as staking rewards to that block's validator.

- **Weaknesses**

- Cardano is competing in a domain of general-purpose, PoS smart contracts (Ethereum 2, Tezos, Cosmos, Polkadot, etc)
- Cardano is still in development
- Long rollout (ETH dominates)
- Censorship can exist due to separation of computational and settlement layers
- Approx. 75% of all ADA tokens are staked

# Solana (SOL)

- Solana price is about \$13 USD with a 24-hour trading volume of \$1,462,151,864 USD. We update our SOL to USD price in real-time. Market cap of \$5,054,973,421 USD. It has a circulating supply of 367,932,725 SOL coins and the max. supply is not available.
- Solana was officially launched in March 2020 by the Solana Foundation with headquarters in Geneva, Switzerland.
- The Solana protocol is designed to facilitate decentralized app (DApp) creation. It aims to improve scalability by introducing a proof-of-history (PoH) consensus combined with the underlying proof-of-stake (PoS) consensus of the blockchain.
- One of the essential innovations is the proof-of-history (PoH) consensus and PoS. This concept allows for greater scalability of the protocol, which in turn boosts usability.
  - The proof-of-stake (PoS) consensus is used as a monitoring tool for the PoH processes, and it validates each sequence of blocks produced by it.
- Solana has short processing times the blockchain offers. Solana's hybrid protocol allows for significantly decreased validation times for both transaction and smart contract execution.



# Solana (SOL): strengths/weaknesses

- **Strengths**

- Speed and fees: Solana can process about 50,000 transactions per second with low fees (less than \$.01)
- NFTs and smart contracts : faster transaction speeds and lower fees than buyers on the Ethereum network.
- Environmental impact - Solana's PoS and PoH verification process is far less energy-intensive, potentially making the crypto a greener alternative to Bitcoin and Ethereum

- **Weaknesses**

- Still very early ecosystem
- While being extremely scalable horizontally, the cost is high demands for minimum hardware.
  - If computer hardware keeps getting better, then Solana will lead. Ethereum is designed to be able to run on a bad laptop. Not everyone can run a node as easily as with Bitcoin for instance.
- Not decentralized enough - Solana sacrifices a degree of decentralization to have faster transactions, It contributes to vulnerability to outages.
- Stability : Recent blockchain bug caused 6 hour outage
- Solana does not have a fixed number of coins. Solana started out increasing its supply by 8% annually. That inflation rate declines by 15% annually until it reaches 1.5%, where it will remain indefinitely
- Large amount of tokens owned by development team



# Chainlink (LINK)

- The Chainlink price is apprx. \$5.7 USD with a 24-hour trading volume of \$218,761,780.
- Market cap of \$5,772,641,571.
- It has a circulating supply of 467,009,550 LINK coins and a max. supply of 1,000,000,000 LINK coins.
- Chainlink (LINK) was introduced in 2017 with an Initial Coin Offering (ICO) of USD 32 million.
- Its Mainnet went live in May 2019.
- It is a decentralized and infinitely scalable network of nodes built on Ethereum (technically, it is an ERC-20 token) that provides data to any connected blockchain, allowing the integration of off-chain data into smart contracts.
  - This makes Chainlink an oracle provider that calls inputs of data from the real world into the blockchain.
- It uses the proof-of-stake (PoS) consensus mechanism, which is lighter on energy consumption than the Proof-of-Work protocol, commonly used in Bitcoin, Litecoin and Ethereum.





# Chainlink (LINK)

- What does it do?
- For instance, for a smart contract that requires the EUR/GBP exchange rate, Chainlink steps in to provide this information, after verification by its participants, who are paid in LINK tokens by the network, instead of relying only on one source.
- Requests and responses are recorded on-chain and detailed statistics are provided for further analysis, for instance by <https://www.reputation.link/> that provides information on the real-time performance of the Chainlink Network.
- So far there are about 120 data sources and 13 data providers for cryptocurrency and traditional financial market data (more than 65,000 Equities and ETFs, options etc.), proprietary and aggregated sports odds and sports results data, property on record and real-estate data, luxury goods and services' prices and collector database information



# Chainlink (LINK): strengths/weaknesses

- **Strengths**

- First mover advantage in blockchains/off-chain
- Expansive market space for use of native network in real world applications

- **Weaknesses**

- No clear roadmap
- Depends on the speed of the Ethereum network for data transfers
- Relative centralisation of stored token assets
- About 60% of the supply remains under the control of the parent company
- no restrictions about the distribution of the node operation reward

# Polkadot (DOT)

- The Polkadot price is around \$4.6 USD with a 24-hour trading volume of \$128,440,188.
- Market cap of \$5,353,255,887. It has a circulating supply of 1,152,696,297 DOT coins and the max. supply is not available.
- Polkadot (DOT) was first introduced via a whitepaper in 2016 began to be traded on exchanges in 2020-end.
- It is a proof-of-stake (PoS) agnostic blockchain that connects other different blockchains.
- In general, it is a next-generation blockchain and layer-0 protocol that combines multiple specialized blockchains into a unified and scalable network.
- Technically, it uses the concept of a relay chain (its base layer) and parachains (the blockchains that connect to the relay chain). It allows information to be seamlessly transferred between parachains and effectively solves the blockchain scalability problem.
- For instance, once Bitcoin, Monero, Ethereum or any other cryptocurrency is connected to Polkadot, investors or users will be able to move BTC into Ethereum and then clean profits via Monero or Chainlink.
- While Chainlink is built on the Ethereum blockchain, Polkadot is attempting to become a new Ethereum of sorts. As at the beginning of June 2021, there are more than 440 projects building on Polkadot.
- DOT tokens are used to provide network governance, operations, and creation of parachains through bonding.
- It is traded on Binance, Kraken, Bitfinex, Bitrex and Huobi Global, though it is not traded on Coinbase, one of the world's largest and widely accessed cryptocurrency exchanges.



# Polkadot (DOT): strengths/weaknesses

- **Strengths**

- Most widespread use of token governing cross-blockchain interoperability
- Allowing secure parallel chains for scalability and lower transaction fees
- Flexibility
- High technical prowess

- **Weaknesses**

- High fees
- Competition - Ethereum dominates in terms of adoption
- Inequality of assets owned
- hackers tried to exploit the code vulnerabilities twice and drained funds before being stopped

# Chainlink (LINK) vs Polkadot (DOT)

- Chainlink (LINK) and Polkadot (DOT) are two different blockchain currencies, using different approaches and serving different goals.
- Chainlink is a decentralized oracle, carrying outside data in and out for Dapps, while Polkadot is solving interoperability issues.
- Both cryptocurrencies are similarly ranked (Simetri assigns them a ranking of “B”, compared to “B+” and “A-” for Ethereum and Bitcoin, respectively).
- Price volatility of Polkadot is higher than that for Chainlink.
- Overall, Polkadot is being considered a strong newcomer.

# Stellar (XLM)

- Stellar price is apprx. \$0.07 USD with a 24-hour trading volume of \$185,169,859 USD, a market cap of \$1,937,360,838. It has a circulating supply of 26,132,455,230 XLM coins and a max. supply of 50,001,806,812 XLM coins.
- **Stellar is an open-source network for currencies and payments (Stellar is a system for tracking ownership).**
- Stellar makes it possible to create, send and trade digital representations of all forms of money—dollars, pesos, bitcoin, pretty much anything.
- The Stellar network has a native digital currency, the lumen, that's required in small amounts for initializing accounts and making transactions but, beyond those requirements, Stellar doesn't privilege any particular currency.
- You can create a digital representation of a U.S. dollar—on Stellar you'd call this a “dollar token”
- someone deposits a traditional dollar with you, you'll issue them one of your new tokens.
- When someone brings that “dollar token” back to you, you promise to redeem it in turn for one of the regular dollars in that deposit account.
- a 1:1 relationship between your digital token and a traditional dollar. Every one of your tokens out in the world is backed by an equivalent deposit.



# Stellar (XLM): strengths/weaknesses

- **Strengths**

- Fast cross-border payments between individuals
- Low fees
- Not-for-profit philosophy (inclusive global payment system compared to XRP)

- **Weaknesses**

- Competitor of XRP
- Small centralised development team
- Nodes are privately held for consensus algorithm



# Monero (XMR)

- Monero price is apprx. \$150 USD with a 24-hour trading volume of \$60,938,890, Market cap of \$2,747,369,202. It has a circulating supply of 18,070,965 XMR coins and the max. supply is not available.
- **Goal: to allow transactions to take place privately and with anonymity**
- XMR is designed to obscure senders, recipients and amounts through the use of advanced cryptography.
- Whereas each Bitcoin in circulation has its own serial number, meaning that cryptocurrency usage can be monitored, XMR is completely fungible. By default, details about senders, recipients and the amount of crypto being transferred are obscured.
- Past transaction outputs are picked from the blockchain and act as decoys, meaning that outside observers can't tell who signed it.
- If Sender was sending 200 XMR to Receiver, this amount could also be split into random chunks to add a further level of difficulty.



# Monero (XMR): strengths/weaknesses

- **Strengths**

- First mover privacycoin where transactions are impossible to be traced
- The transactions are not linkable
- Relatively low transaction fees
- Decentralised development and governance
- Dynamic Scalability: the blockchain doesn't have a block limit and is dynamically scalable.

- **Weaknesses**

- ~43% of hashrate of Monero is owned by 3 mining pools
- Complexity of code base: It is not beginner-friendly
- Governmental regulation is more serious
- Potential scalability issues
- There is not much digital currency wallet compatibility for Monero

# Ripple (XRP)

- XRP price is approx. \$0.35USD with a 24-hour trading volume of 777.86M, a market cap of 777.86M. It has a circulating supply of 47,736,918,345XRP coins and a max. supply of 100,000,000,000 XRP coins.
- XRP was created by Ripple to be a speedy, less costly and more scalable alternative to both other digital assets and existing monetary payment platforms like SWIFT.
- Ripple claims it's the "world's only enterprise blockchain solution for global payments."
- Unlike many other cryptocurrencies, Ripple is centralized and comes with a finite supply of currencies.
- Also, it claims to be the most scalable blockchain solution on the market.
- Difference between XRP, Ripple and RippleNet: XRP is the currency that runs on a digital payment platform called RippleNet, which is on top of a distributed ledger database called XRP Ledger.
- While RippleNet is run by a company called Ripple, the XRP Ledger is open-source and is not based on blockchain, but rather the previously mentioned distributed ledger database
- The XRP Ledger processes transactions roughly every 3-5 seconds, or whenever independent validator nodes come to a consensus on both the order and validity of XRP transactions — as opposed to proof-of-work mining like Bitcoin (BTC).



# Ripple (XRP): strengths/weaknesses

- **Strengths**

- transactions are fast and cheap.
- Higher energy-efficiency
- It can be used by small businesses and as a bridge currency for international currency transfers.
- No Mining Pools
- Enterprise-Optimized

- **Weaknesses**

- More centralization
- less secure protocol.
- Many of Ripple's banking partners only use RippleNet and not its XRP cryptocurrency.
- Ripple has attracted controversy because it's run by a private company and because of the SEC lawsuit.

# EOS

- is \$2.34 USD with a 24-hour trading volume \$225,143,009 USD. Market cap of \$2,480,163,584 USD. It has a circulating supply of 979,184,934 EOS coins and the max. supply is not available.
- EOS is a platform that's designed to allow developers to build decentralized apps (launched back in June 2018)
- EOS uses a delegated proof-of-stake consensus mechanism.
- Number of transactions: 3,000+ transactions/second



# EOS: strengths/weaknesses

- **Strengths**

- Much higher transaction speeds than main competitor Ethereum
- Negligible transaction fees
- Capacity to run industrial-scale decentralised apps

- **Weaknesses**

- Extremely few existing nodes and inherent difficulty for more
- Essentially hitherto outcompeted by Ethereum and others for dApp takeup
- Community is sour on future and project founder has left recently

# Ripple (XRP)

- XRP price is approx. \$0.61USD with a 24-hour trading volume of \$872,323,365 USD, a market cap of \$29,438,822,753 USD. It has a circulating supply of 47,736,918,345XRP coins and a max. supply of 100,000,000,000 XRP coins.
- XRP was created by Ripple to be a speedy, less costly and more scalable alternative to both other digital assets and existing monetary payment platforms like SWIFT.
- Ripple claims it's the "world's only enterprise blockchain solution for global payments."
- Unlike many other cryptocurrencies, Ripple is centralized and comes with a finite supply of currencies.
- Also, it claims to be the most scalable blockchain solution on the market.
- Difference between XRP, Ripple and RippleNet: XRP is the currency that runs on a digital payment platform called RippleNet, which is on top of a distributed ledger database called XRP Ledger.
- While RippleNet is run by a company called Ripple, the XRP Ledger is open-source and is not based on blockchain, but rather the previously mentioned distributed ledger database
- The XRP Ledger processes transactions roughly every 3-5 seconds, or whenever independent validator nodes come to a consensus on both the order and validity of XRP transactions — as opposed to proof-of-work mining like Bitcoin (BTC).





# Ripple (XRP): strengths/weaknesses

- **Strengths**

- XRP transactions are fast and cheap.
- more energy-efficient
- Ripple's payment network is already being used by financial institutions.
- XRP can be used by small business owners and consumers for secure money transfers.
- XRP can be used as a bridge currency for international currency transfers.

- **Weaknesses**

- Ripple's consensus protocol is arguably less secure than other methods of processing crypto transactions.
- Many of Ripple's banking partners only use RippleNet and not its XRP cryptocurrency.
- Ripple has attracted controversy because it's run by a private company and because of the SEC lawsuit.

# Stable Coins

- Stable coins are a new category of virtual currencies that have recently gained attention.
- They are not strictly crypto currencies, despite using a digital token, and they have very different monetary underpinnings and issuance regimes.
- In contrast to the leading decentralised digital currencies, such as Bitcoin and Ethereum, stablecoins have in-built price stability mechanism to minimize exchange rate volatility which makes digital tokens more attractive for investors.
- Stablecoins market has grown hundredfold over the last years, from \$1.4 billion at the start of 2018 to \$154 billion in December May 2021, while the US-dollar backed stablecoin Tether become the most tradable cryptocurrency with \$78.3bn market cap.
- The stable coins are of the two main types.
  - First, **Collateralized Stablecoins**, that includes **fiat-backed stablecoins** whose values are pegged to and backed by, reserves of fiat currency; **crypto-backed stablecoins** are backed by cryptocurrencies and **asset-backed stablecoins** are underpinned by reserves of assets other than fiat or cryptocurrencies, for instance by gold, diamonds, oil etc.
  - Second, **non-collateralized Stablecoins**, also known as **algorithmic stablecoins**, or **seigniorage supply coins**. They do not have any underlying asset and **their supply is “regulated” by an algorithm** or a decentralized model of governance based on holder votes.
  - There exists also **hybrid stablecoins** that combine the features of the abovementioned stablecoins, i.e., reserve backing as well as algorithms or voting to offset volatility.

# Tether

- Tether (USDT) is a cryptocurrency in the category known as stablecoins.
  - It's operated by a company called Tether, based in Hong Kong.
- Tether coins are designed to remain valued at US\$1 each.
  - It accomplishes this by backing the circulating supply of USDT with assets held in reserve.
- How does Tether work
  - Tether is unlike many other cryptocurrencies, in that its intended purpose is to remain at a consistent value. Tether does this by minting and destroying tokens.
  - New USDT enters the system when the Tether company mints it.
  - When someone wants USDT, they make a payment to Tether. The company then adds those funds to its reserves and mints new USDT for the customer.
  - USDT is removed from circulation when someone wants to redeem USDT for USD and they can sell it back to the Tether company. Redeemed USDT is then destroyed and removed from circulation.
  - This process is typically only for customers with large orders.

# Tether

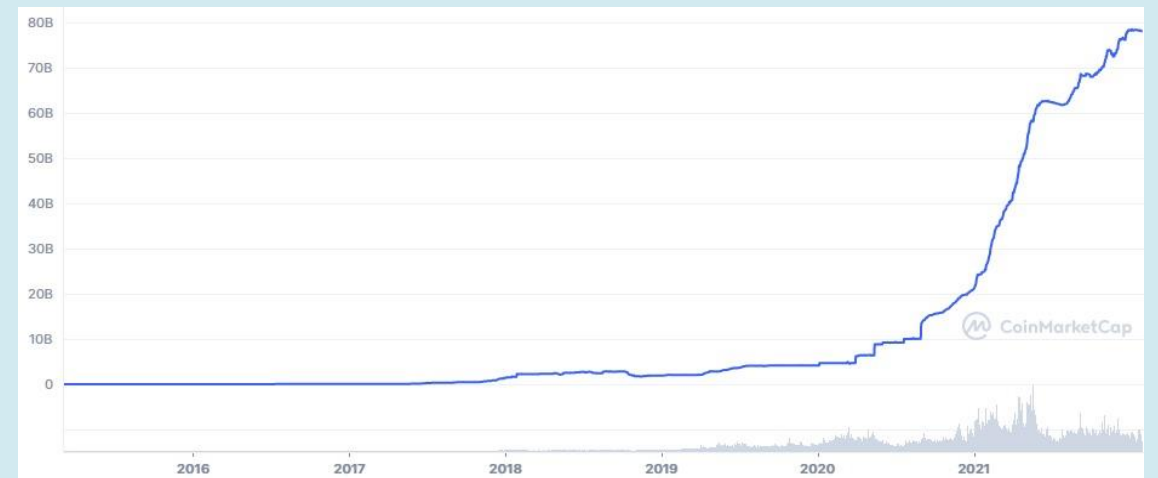
- On the technical level, the Tether coins are issued as tokens on three different blockchains. This means there are three different types of USDT in existence.

USDT type	Omni Layer USDT	ERC20 USDT	TRC20 USDT
Which blockchain it uses	Bitcoin Omni Layer	Ethereum	TRON
How to recognize its addresses	Begins with “1,” “3” or “bc1”	Begins with “0x”	Begins with “TX”

- All of them are functionally the same, but when using USDT, you must be aware of which type you’re using. The easiest way of finding out which type you have is by looking at your Tether wallet address. Each type of address will begin with different letters or numbers, which tells you what type it is.

# Tether

- Tether price today is \$1.00 USD with a 24-hour trading volume of \$38,193,480,711 USD, a market cap of \$78,146,610,374 USD. It has a circulating supply of 78,117,427,986 USDT coins and the max. supply is not available.
- USDT does not have its own blockchain — instead, it operates as a second-layer token on top of other cryptocurrencies' blockchains: Bitcoin, Ethereum, EOS, Tron, Algorand, Bitcoin Cash and OMG, and is secured by their respective hashing algorithms.



# Tether: strengths/weaknesses

- **Strengths**

- Most widely used/highest liquidity stablecoin on exchanges
- Strong record of holding currency value against the dollar
- Legal battle with New York Attorney General recently settled

- **Weaknesses**

- Stablecoin so no more designed as an investment itself than the US dollar
- Centralised supply, which can be minted whenever team decides
- Perceived unscrupulous behaviour by team, misleading about how it's backed up



# Gold backed stablecoins

- **Digix Gold Token (DGX)**
  - Digix Gold Token (DGX) is an asset-backed token and backed by the weight of gold (1DGX=1 gram of gold). It uses the PoA protocol based on Ethereum and the InterPlanetaryFiles System (IPFS)
  - Its price is apprx. \$53.98 USD with a 24-hour trading volume of \$99,817.07 USD, a market cap of \$4,138,062 USD. It has a circulating supply of 76,666 DGX coins and the max. supply is not available.
- **Perth Mint Gold Token**
  - Perth Mint Gold Token is a gold-backed stable coins supported by the Australian government.
  - Its price is approx. \$1,855.16 USD with a 24-hour trading volume of \$18,044.42 USD, a market cap of \$1,901,380 USD. It has a circulating supply of 1,025 PMGT coins and the max. supply is not available.
- **Tether Gold**
  - Tether Gold represents one troy fine ounce of gold on a London Good Delivery gold bar.
  - Its price is approx. \$1,847.04 USD with a 24-hour trading volume of \$543,662 USD, a market cap not available. The circulating supply is not available and the max. supply is not available.
- **PAX Gold**
  - PAX Gold is backed by one fine troy ounce (t oz) of a 400 oz London Good Delivery gold bar, that is stored in Brink's gold vaults.
  - Its price is approx. \$1,860.87 USD with a 24-hour trading volume of \$10,840,183 USD, a market cap of \$109,814,600 USD. It has a circulating supply of 59,012 PAXG coins and the max. supply is not available.
- **Digital Gold**
  - Digital gold enables users to purchase coverage in physical gold, via the ERC-20 Ethereum-based GOLD token.
  - Its price is approx. \$59.06 USD with a 24-hour trading volume of \$1,225,051 USD, a market cap of \$799,102 USD. It has a circulating supply of 13,530 GOLD coins and the max. supply is not available.



# NFTs

- A non-fungible token (NFT) is a unit of data stored on a blockchain that represents a unique item
  - Real-world physical items or digital assets
  - Unlike bitcoin or other cryptocurrency, not mutually interchangeable, i.e., not fungible
- Physical money and cryptocurrencies are “fungible,” meaning they can be traded or exchanged for one another.
  - They’re also equal in value—one euro is always worth another euro; one Bitcoin is always equal to another Bitcoin.
  - Crypto’s fungibility makes it a trusted means of conducting transactions on the blockchain.
- By contrast an NFT is unique; it is a one-of-a-kind piece of code, stored and protected on the blockchain.
  - Each has a digital signature that makes it impossible for NFTs to be exchanged for or equal to one another
- An NFT can represent anything that exists as or can be represented by a digital
- NFT representing ownership of a digital asset resides in a digital wallet
- Very few restrictions as to what kind of content can be "tokenized" and turned into an NFT

# NFTs, cont.

- An NFT can only have one owner at a time.
  - Each token has an owner and this information is easily verifiable.
- Each token minted has a unique identifier that is directly linked to one Ethereum address.
- ERC-721 NFT standard

# NFTs

- An NFT is created, or “minted” from digital objects that represent both tangible and intangible items, including:
  - Art
  - GIFs
  - Videos and sports highlights
  - Collectibles
  - Virtual avatars and video game skins
  - Designer sneakers
  - Music
  - Even tweets count. Twitter co-founder Jack Dorsey sold his first ever tweet as an NFT for more than £2 million.

# NFT marketplace

## OpenSea – a leader

- has all sorts of digital assets available on its platform, and it's free to sign up and browse the extensive offerings.
- It also supports artists and creators and has an easy-to-use process if you want to create your own NFT (known as "minting")

# Iconic examples

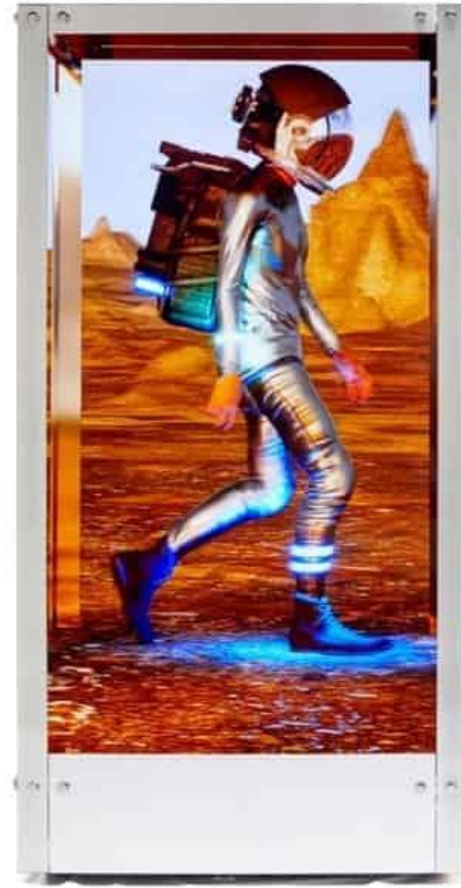
Larva Labs, CryptoPunk #7523.

The CryptoPunks is an NFT collection that consists of uniquely generated characters based on the Ethereum blockchain.

On June 2021, London's auction house Sotheby's saw CryptoPunk #7523, also dubbed "Covid Alien," sold for \$11.75 million, making it the most expensive CryptoPunk sold to date.



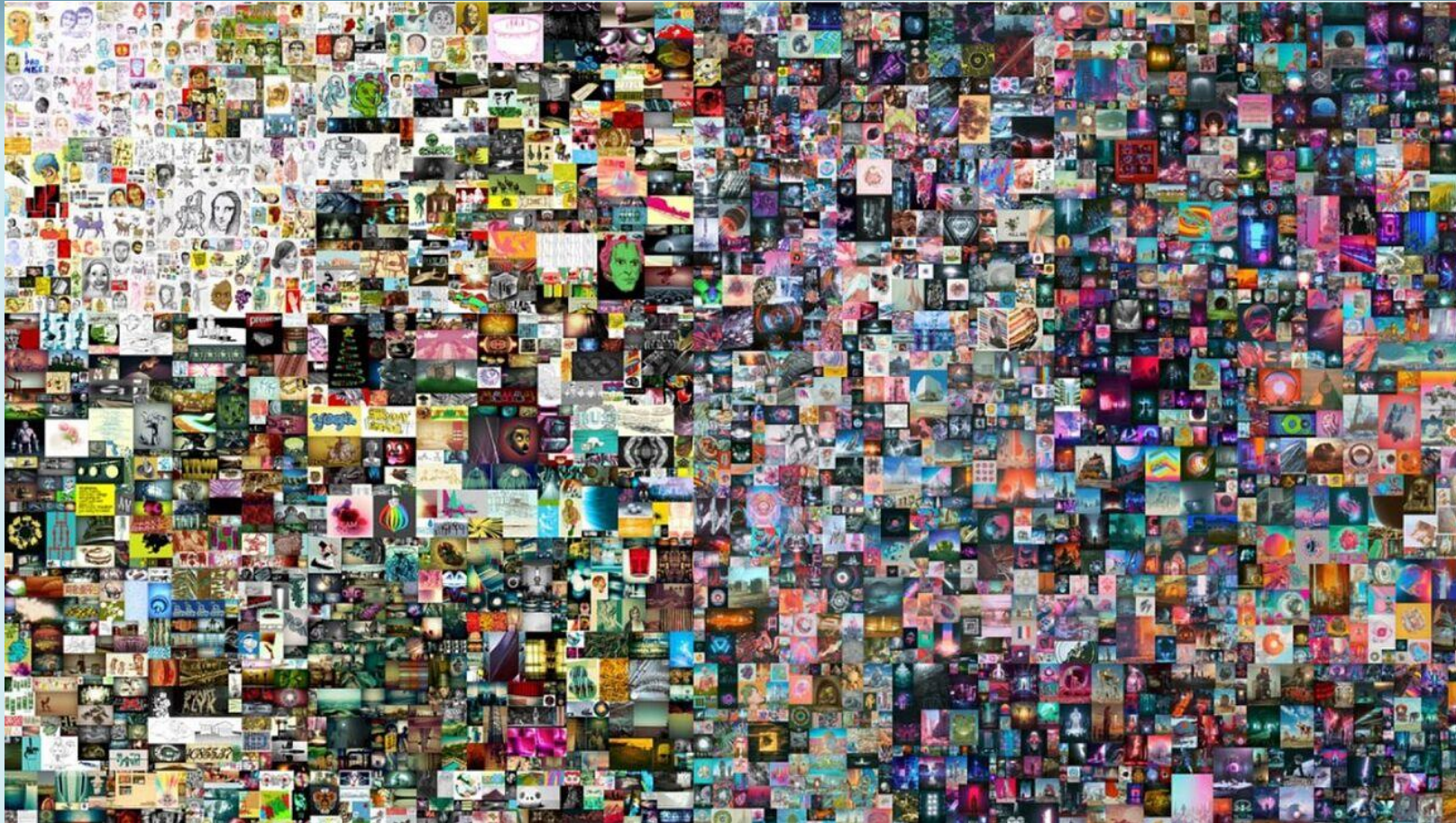
# Iconic examples



Beeple's (b. 1981) 'HUMAN ONE', it is a dynamic, life-generative sculpture, \$28,985,000 at auction.



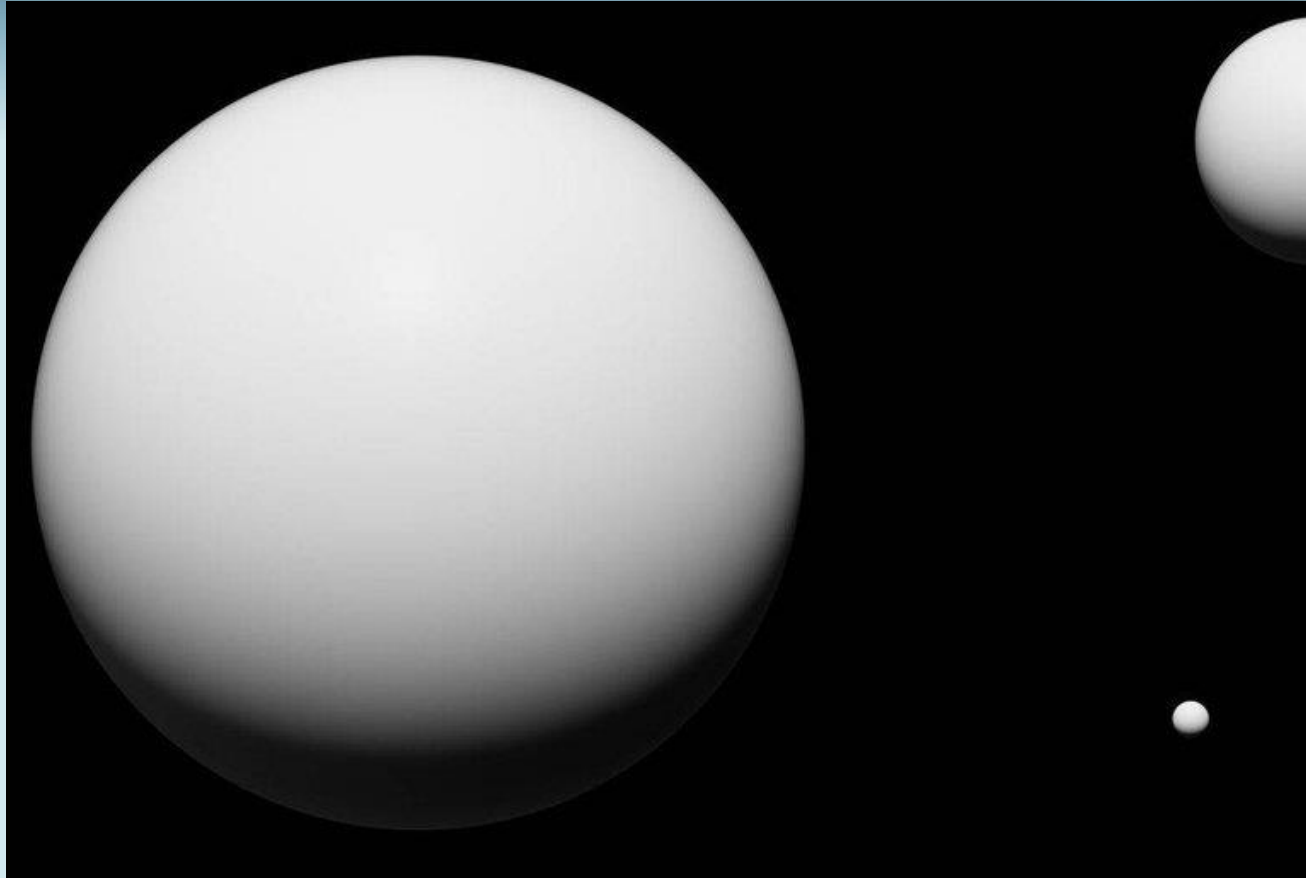
# Iconic examples



The First 5000 Days of digital artist, Beeple, 69.3 million dollars, Christies (21st of February 2021).



# Iconic examples



The Merge is a digital artwork created by an anonymous digital artist nicknamed Pak. It was sold on Dec. 6, 2021, for \$91.8 million on the NFT decentralized marketplace Nifty Gateway. However, the piece was fractionalized to 312,686 pieces distributed to 28,983 buyers. Here is that The Merge was a single artwork composed of a collection of “masses” that users could buy.

# Iconic examples

On the night of January 30, 2022, Bored Ape #232 was sold for 1080.69 ETH (\$2.85 million).

The sale happened on the NFT marketplace – LooksRare.

<https://looksrare.org/collections/0xBC4CA0EdA7647A8aB7C2061c2E118A18a936f13D/232#activity>



# DeFi

- Decentralised finance (DeFi) is a novel way of providing financial services that cuts out traditional centralised intermediaries and relies on automated protocols instead.
- In simple words, DeFi participants are part of a peer-to-peer blockchain network where assets represented in the network can be transferred automatically via so-called smart contracts.
- Mainly DeFi applications do not provide completely new financial products or services, but rather mimic within the crypto-asset ecosystem those provided by the traditional financial system.

# Overview of selected DeFi services and comparison with traditional financial services

Financial service	Decentralised finance	Traditional finance
<b>Credit</b>	<p>Smart contracts facilitate lending and borrowing. Lenders post their crypto-assets into liquidity pools, from which borrowers borrow crypto-assets posting other crypto-assets as collateral. Interest rates are often determined automatically depending on the demand and supply of liquidity.</p> <p>Largest DeFi protocols: Compound, Aave</p>	Banking
<b>Trading</b>	<p>Decentralised exchanges (DEXes) facilitate the trading of crypto-assets by matching and executing trades through smart contracts without the involvement of a (centralised) third party. Trading often happens against a liquidity pool.</p> <p>Largest DeFi protocols: Uniswap, Curve</p>	Brokers, stock exchanges, over-the-counter (OTC) markets
<b>Payments</b>	<p>Peer-to-peer transfers of value are facilitated, either directly "onchain" or via DeFi protocols that facilitate smaller value transfers offchain, before reconciling them in batches back "on-chain".</p> <p>Largest DeFi protocols: Flexa, Sablier Finance</p>	Cash, credit/debit cards, current accounts
<b>Insurance</b>	<p>Customers of insurance DeFi protocols buy tokens in exchange for cover against specific digital asset-related risks, such as cyberattacks and theft. Token holders from within the protocol decide on insurance claims by voting yes/no on payouts.</p> <p>Largest DeFi protocols: Armor, Nexus Mutual</p>	Lloyds of London insurance market, insurance firms
<b>Investment (assets and derivatives)</b>	<p>Protocols replicating asset management functions where crypto-assets from users are automatically deposited in those protocols/pools with the highest yields based on preset risk tolerance. They also include protocols creating cryptoasset indices and those creating derivatives, including synthetic assets, options or perpetual futures.</p> <p>Largest DeFi protocols: Yearn Finance, dYdX</p>	Investment funds, investment firms, investment banks

Sources: ECB

# Compound Finance - Lending

- Compound is based on the Ethereum blockchain.
- Lenders can provide loans to borrowers by locking their crypto assets in the DeFi protocol.
  - similar to depositing fiat currency into a savings account that starts earning interest immediately
- No need for negotiations.
- Compound Finance also enables you to transfer, trade, and use the money in other DeFi applications.
- The native token of the Compound network is called COMP.
- When a Lender put their cryptocurrency, they receive the native token of Compound called a “cToken.”
- The token value of the cToken is equivalent to the token that was placed in the liquid market.
- The value will increase as the interest on that cryptocurrency appreciates.
- The value of the cToken will also fluctuate with the value of the token in the market, of course.
  - For example, if you lock X amount of USDT in the protocol, you will get X amount of cUSDT tokens which will then begin growing in value.
  - These cUSDT tokens can then be used in apps on Ethereum. That way, your locked-up capital isn't truly locked up like it would be if you were to lend it to a borrower in a traditional setting. You can still use it.
  - When you need to make use of your cryptocurrency, all you need to do is pay back your cTokens, and you will receive your original tokens in return.



# Compound Finance - Borrowing

- **borrowers have to deposit collateral to get something called “borrowing power”.**
- After acquiring that power, they will be able to borrow tokens equivalent to the amount of borrowing power that they have.
- Borrowers can then borrow from that fund whenever they want, for as long as they want, at an interest rate determined by an algorithm monitoring the supply and demand of the tokens being borrowed.
- Compound operates on the principle of over-collateralization.
  - This means that users who want to borrow have to have collateral that is more than what they want to borrow, that way the lender and the system are exposed to zero risk.
- Borrowers' collateral must remain above a certain value to be viable. If it doesn't remain above that value, the collateral will be liquidated to pay back the loan.
  - When a user's collateral enters the liquidation event, other users will have the opportunity to pay the outstanding amount borrowed for a percentage of the collateral of the borrower.
  - To incentivize this purchase, users will be given an 8% discount on the collateral.
  - That is, they will get the collateral at 8% lower than the market value.

# Aave






- Aave is a decentralized lending protocol that lets users lend or borrow cryptocurrency without going to a centralized intermediary.
  - Aave is decentralized autonomous organization, operated and governed by the people who hold—and vote with—AAVE tokens.
- Aave was originally built on Ethereum, with ERC20 tokens.
- Aave expanded to other chains, including Avalanche, Fantom, and Harmony.
- Aave version1, v2 or v3 – each of which brought upgrades to the network.
  - Aave v2 remains the largest public lending market, with \$5.29 billion in TVL.
  - Aave v3 cuts transaction costs and allows the community to vote on approved stablecoins for borrowing and collateral; it has \$1.47B in TVL.
- Returns vary by asset; as of this writing, supplying ETH on Aave v2 provides an annual return of 0.7%.
- Borrowing assets similar to Compound.
- The amount to borrow depends on how much you deposit, as well as a metric called the “health factor,” which is a number that represents the safety of the asset you deposit as collateral against the borrowed assets.
- The higher that number is, the better, but keeping that number above 1 is key for the safety of your deposit.




# DeFi risks

- **DeFi is subject to some of the same vulnerabilities known from traditional finance**, which can be amplified by the specific features of DeFi (Aramonte et al. 2021; Carter and Jeng 2021; and European Commission 2022).
- DeFi lending is subject to **market, liquidity and credit risk and, as a result of leverage (leverages vary from 2x-100x)**, can exacerbate procyclicality
  - For instance, when market values begin to fall, leveraged investors may be forced to liquidate their holdings, generating large downward price spirals.
  - use of stablecoins and unbacked crypto-assets can make DeFi susceptible to spillovers from the materialisation of stablecoin risks or strong price movements of unbacked crypto-assets. For instance: the crash of the stablecoin TerraUSD exemplify these vulnerabilities

# DeFi risks, cont.

	 <b>BORROWING</b>	 <b>MARGIN TRADING</b>	 <b>PERPETUALS</b>	 <b>LEVERAGED TOKENS</b>	 <b>OPTIONS</b>
Model Type	Real Assets Trading	Real Assets Trading	Derivatives/ Synthetic assets	Real Assets Trading & Synthetic assets	Derivatives/ Synthetic assets
Leverage Level	Less than 2x	2x - 5x	5x -100x	2x -5x	0-20x
Leverage Maintenance	Variable	Variable	Variable	Constant	Variable
Leverage Adjustment	Manual	Manual	Manual	Passive and Automatic	Passive
Liquidation Risks	YES	YES	YES	NO	NO
Costs	Borrowing Interest	Borrowing Interest	Funding Rate	Borrowing Interest	Option Premiums
Expiry	NO	NO	NO	NO	YES
Current on-chain volume	HIGH	LOW	MEDIUM	LOW	LOW
Volume on Centralized Venues	HIGH	HIGH	HIGH	HIGH	MEDIUM and GROWING FAST
DeFi Platforms	Compound, AAVE, Venus	dYdX	dYdX, MCDEX, Injective Perpetual Protocol	FinNexus, Tokensets, Charm	FinNexus, Hegic, OPYN

 **FinNexus** | **Comparison of Leverages in DeFi**

## - In borrowing:

- if you are holding **\$10,000 ETH** and think it's a bullish time, you can deposit your ETH in Compound as collateral and borrow **\$5,000 USDC**, then trade for another \$5,000 ETH.
- You will get **\$15,000** exposure in ETH, which is equivalent to a **1.5x leverage**, compared with your initial capital of \$10,000.

## - in Margin Trading:

- For instance, you are longing **ETH 3x**
- You are holding **\$100 USDC**, borrowing another **\$200 USDC** and **trading for \$300 ETH** in order to take the desired ETH long position. The leverage level is  **$\$300/\$100=3x$** .
- If the price of ETH **risks by 20%**, your profit will be  **$\$300(1+20\%) - \$300 = \$60$** . You are safer from being liquidated and the real leverage level is decreased to  **$\$360/(\$360 - \$200) = 2.25x$** . In other words, you are automatically deleveraged by the ETH price rise.
- If the price of ETH drops by 20%, your loss will be  **$\$300(1-20\%) - \$300 = -\$60$** . You are in a more dangerous position as far as liquidation is concerned and the real leverage level is increased automatically to  **$\$240/(\$240 - \$200) = 6x$** . In other words, you are re-leveraged by the ETH price drops, which shows you are in a more risky position than before.
- **Perpetual contracts are similar to traditional futures contracts, but there is no expiry.**
  - **Perpetual Contracts mimic a margin-based spot market** and hence trade close to the underlying reference index price.
  - **leverages tokens VS margin trading/perpetuals** is that leveraged tokens will rebalance themselves periodically or when reaching a certain threshold, in order to maintain certain leverage

# DeFi risks, cont.

- New risks inherent to DeFi, such as **operational risks stemming from the underlying technology and governance risks**, have risen with the expansion of DeFi.
- **the absence of banks and the access to the central bank balance sheet** removes shock absorbers and buffers in the system.
- **immature and decentralised technology**, in particular pertaining to the smart contracts that enable automation
- **the vulnerability to operational risks due to the irreversibility of transactions on the blockchain** and no recourse possibilities in the absence of a central authority.

# Quick Glossary

- **Address:** A bitcoin address looks like 1DSrfJdB2AnWaFNgSbv3MZC2m74996JafV.
- **Block:** A grouping of transactions, marked with a timestamp, and a fingerprint of the previous block. The block header is hashed to produce a proof of work, thereby validating the transactions. Valid blocks are added to the main blockchain by network consensus.
- **Blockchain:** A list of validated blocks, each linking to its predecessor all the way to the genesis block.
- **Byzantine Generals Problem:** A reliable computer system must be able to cope with the failure of one or more of its components. A failed component may exhibit a type of behavior that is often overlooked—namely, sending conflicting information to different parts of the system. The problem of coping with this type of failure is expressed abstractly as the Byzantine Generals Problem

# Quick Glossary

- **Consensus:** When several nodes, usually most nodes on the network, all have the same blocks in their locally-validated best block chain. Not to be confused with consensus rules.
- **Consensus rules:** The block validation rules that full nodes follow to stay in consensus with other nodes. Not to be confused with consensus.
- **Difficulty:** A network-wide setting that controls how much computation is required to produce a proof of work.
- **Fork:** Fork, also known as accidental fork, occurs when two or more blocks have the same block height, forking the block chain. Typically occurs when two or more miners find blocks at nearly the same time. Can also happen as part of an attack.
- **Miner:** A network node that finds valid proof of work for new blocks, by repeated hashing.
- **Proof-of-Stake:** Proof-of-Stake (PoS) is a method by which a cryptocurrency blockchain network aims to achieve distributed consensus. Proof-of-Stake asks users to prove ownership of a certain amount of currency (their “stake” in the currency).
- **Proof-of-Work:** A piece of data that requires significant computation to find. In bitcoin, miners must find a numeric solution to the SHA256 algorithm that meets a networkwide target, the difficulty target.