A Primer on Blockchain Economics

ECOM215

Dr. Daniele Bianchi[1]

[1]School of Economics and Finance
Queen Mary, University of London

Summary

In this lecture, we introduce the economic foundations of blockchain technology and the implications of blockchain adoption and development for economic practice. We will particularly emphasise key economic aspects of Blockchain, such as disintermediation, competition, cost efficiency, consensus formation, and scalability.

Contents

Building consensus in decentralised networks

Consensus in blockchain networks

An integral part of economic development is the digitisation of information.

↪ Digitised information drastically increases the quantity and quality of economic activities and business organisations.

An example of the impact of digitised information is the "sharing economy"

↪ On-demand labour gets instantaneous payments instead of relying on long-term employment contracts.

However, successful platforms and organisations still heavily depend on existing centralised parties like banks and payment systems.

↪ The lack of trust among players in an open system can hinder economic growth.

Consensus in blockchain networks

Blockchain addresses the lack of trust in peer-to-peer interactions by reorganising an economic system into a decentralised network.

A decentralised consensus mechanism allows agents to interact safely without relying on a centralised third party.

↪ The economic system can be more robust to external shocks and/or internal corruption.

↪ Better coordination between individuals and groups, thus increasing productivity.

In blockchain technology, consensus refers to the rules and protocols agreed upon by the agents for conflict resolution and network governance.

Consensus in blockchain networks

Blockchains can be permissionless (public) or permissioned (private).

The distinction has more to do with who participates in the **consensus** formation rather than the users of a particular blockchain.

↪ **Permissionless** blockchains allow any node in the network to be a recordkeeper/validator based on the rules dictated by a pre-specified protocol.

↪ **Permissioned** blockchains are mostly proprietary (enterprise applications). Network maintenance usually relies on a single or a small group of entities.

Consensus in blockchain networks

In Economics, consensus represents the information basis for agents, who may have different beliefs and preferences, to agree on the state of the world or to behave according to a common set of rules.

↪ Traditionally, centralised parties such as courts, governments, and notary agencies provide such consensus.

↪ This is often labour-intensive, time-consuming, and prone to tampering, corporate capture, and monopoly power.

Blockchains provide a decentralised way of generating consensus. *Decentralisation* pertains to how consensus is generated and stored.

↪ E.g., in Bitcoin, the proof-of-work protocol postulates that newly appended blocks are stored on multiple (if not all) nodes representing network participants' computers.

Consensus in blockchain networks

Fundamentally, blockchains are distributed systems in which independent nodes have to collaborate with one another.

A trusted environment is one in which transactions can be carried out in a fault-tolerant way.

Some nodes might often act rogue, especially in architectures that allow anyone to join the network.

Fault tolerance $\Longrightarrow$ minimises the risk that one or more network nodes fail and exhibit inconsistent or fraudulent behaviour (e.g., sending conflicting information to the different parts of the system).

Digression: Byzantine general's problem

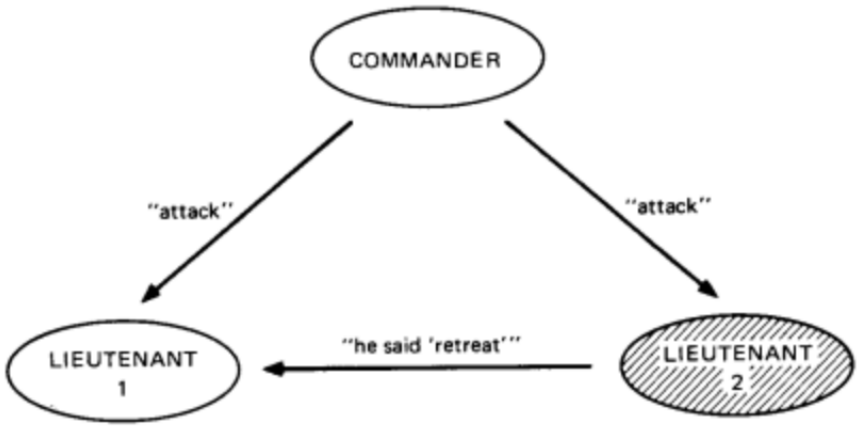
A **Byzantine general's problem** refers to a condition in a distributed computer system in which components may fail, and imperfect information exists about whether a component has failed.

Consider a fortress surrounded by generals of the Byzantine Empire. They are geographically separated and can communicate only through messengers. They need to decide to either retreat or attack.

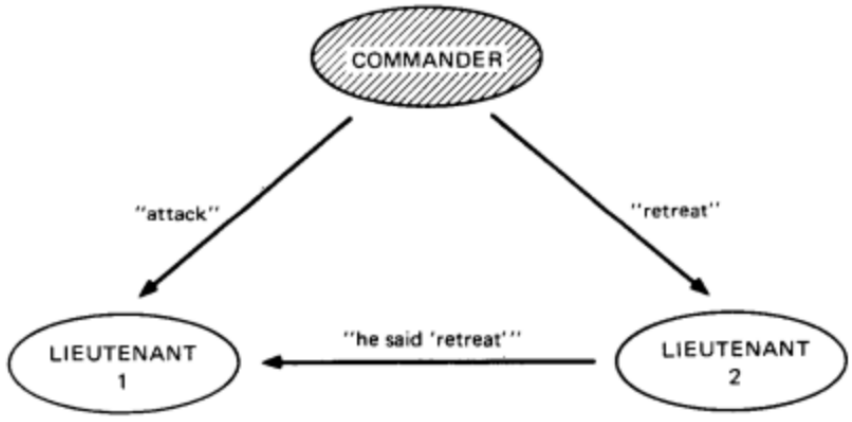
To succeed, all the generals should agree on one common decision: attack or retreat. Any attack by only a few generals would worsen the situation rather than a coordinated attack or retreat.

The complexity increases as there are "traitors" (or points of failure) who would do their best to stop generals from reaching an agreement.

Digression: Byzantine general's problem



(a) Lieutenant point of failure



(b) Commander point of failure

In a peer-to-peer system, preventing malicious attempts to tamper with the transactions or balances can be challenging.

Blockchain prevents these attacks with a consensus protocol (e.g., Proof-of-Work, Proof-of-Stake).

The Blockchain trilemma

Consensus generation

Earlier attempts at cryptocurrencies lacked a proper incentive system for decentralised nodes to record transactions properly.

Consensus protocols are essentially the rules by which agents interact in distributed computing and network systems.

↪ For blockchains, the best-known consensus protocol is proof-of-work (PoW), which is behind Bitcoin design.

Satoshi Nakamoto introduced the concept of "mining", in which independent computers spend resources and compete for the right to record new blocks of transactions.

↪ The winner gets rewarded with fees and newly generated Bitcoins.

↪ Miners have incentives to act honestly, as rewards are paid only if subsequent miners endorse the record.

Consensus generation

Coupling the right incentives with existing cryptographic solutions makes Bitcoin a valid form of payment within the network.

Economics allows us to formally discuss the incentive mechanism within and outside Bitcoin.

↪ We can leverage concepts such as equilibrium (or multiple equilibria), incentive compatibility, and mechanism design.

↪ These help to understand the mechanics underlying consensus protocols.

Proof-of-Work (PoW) protocol

Proof-of-Work represents the predominant protocol for generating decentralised consensus.

Miners (recordkeepers) compete for the right to update the public ledger with a block of transactions.

↪ The competition involves solving cryptographic puzzles, mimicking a mining activity's effort.

The winner gets a fixed amount of Bitcoin plus a transaction fee.

↪ The reward is halved every four years (deflationary supply).

Proof-of-Work (PoW) protocol

Once a solution is found, the result is inserted into the block header, and the new block is immediately propagated to the network.

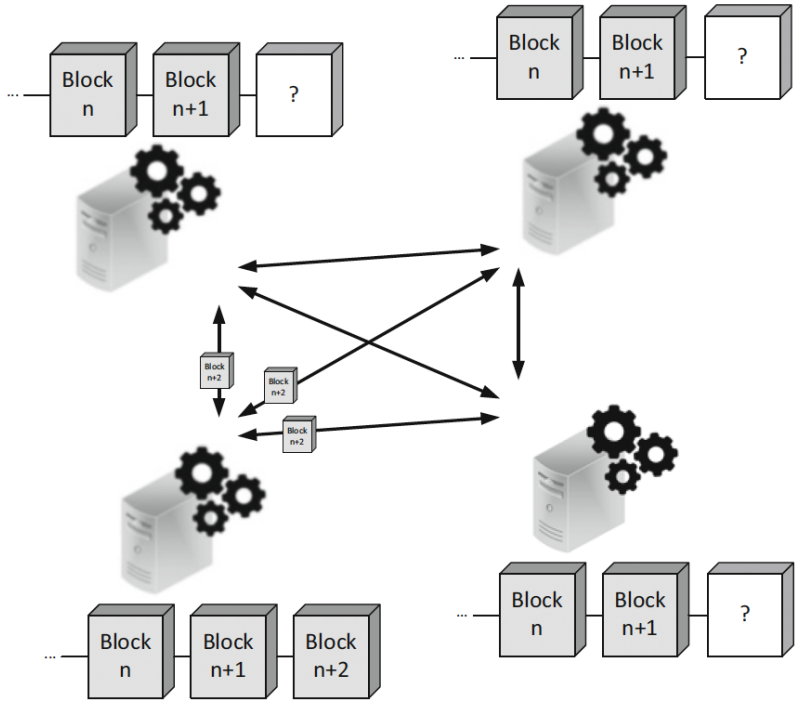


Figure: The miner in the lower left corner finds the next block $n + 2$ and broadcasts it to the network. Source: Xu et al. 2019 "Architecture for Blockchain Applications".

Proof-of-Work (PoW) protocol

The other nodes in the networks receiving the new block verify it and then include it in their replica of the blockchain data structure.

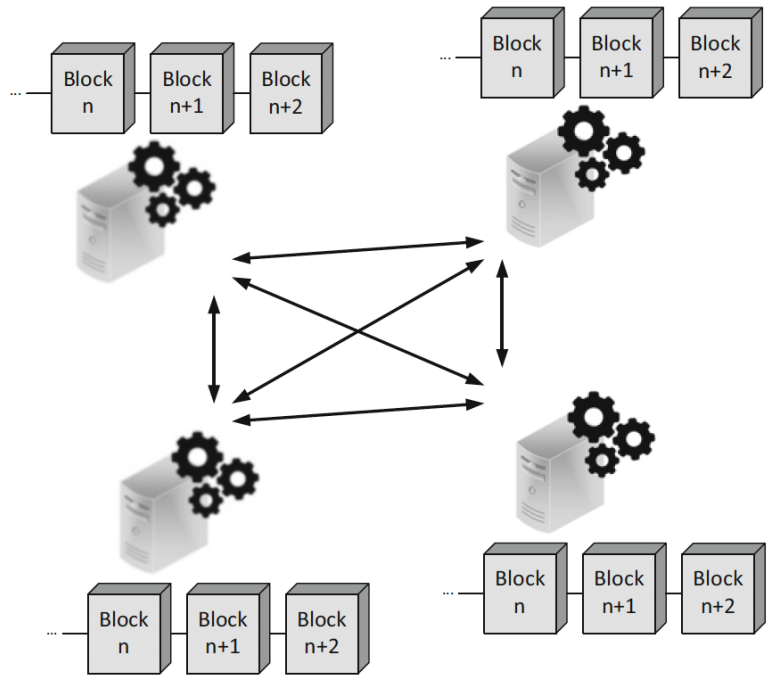


Figure: Other nodes append the block to their local copy of the blockchain data structure. Source: Xu et al. 2019 "Architecture for Blockchain Applications".

Proof-of-Work (PoW) protocol

Two common features in PoW protocols.

(1) The difficulty of the cryptographic puzzles dynamically adjusts, limiting the speed of block generation and, thus, recording.

↪ Miners are in an arms race $\Longrightarrow$ more computational power improves the chance of winning the recordkeeping, not the social surplus.

(2) In addition to getting newly minted native tokens, miners often also receive fees for their service.

↪ The transition between mining rewards to a full market fees system is an inherent risk of Bitcoin.

Longest chain rule $\Longrightarrow$ Nakamoto envisioned that the winning miner would append to the longest chain when appending blocks.

Proof-of-Work (PoW) protocol

The network computational power grows with the complexity required to mine a new block.

Figure: The estimated number of terahashes per second the bitcoin network performs in the last 24 hours vs network difficulty. Source: `Blockchain.com`.

Proof-of-Work (PoW) protocol

Determining the optimal fee structure based on transaction volume is an interesting problem.

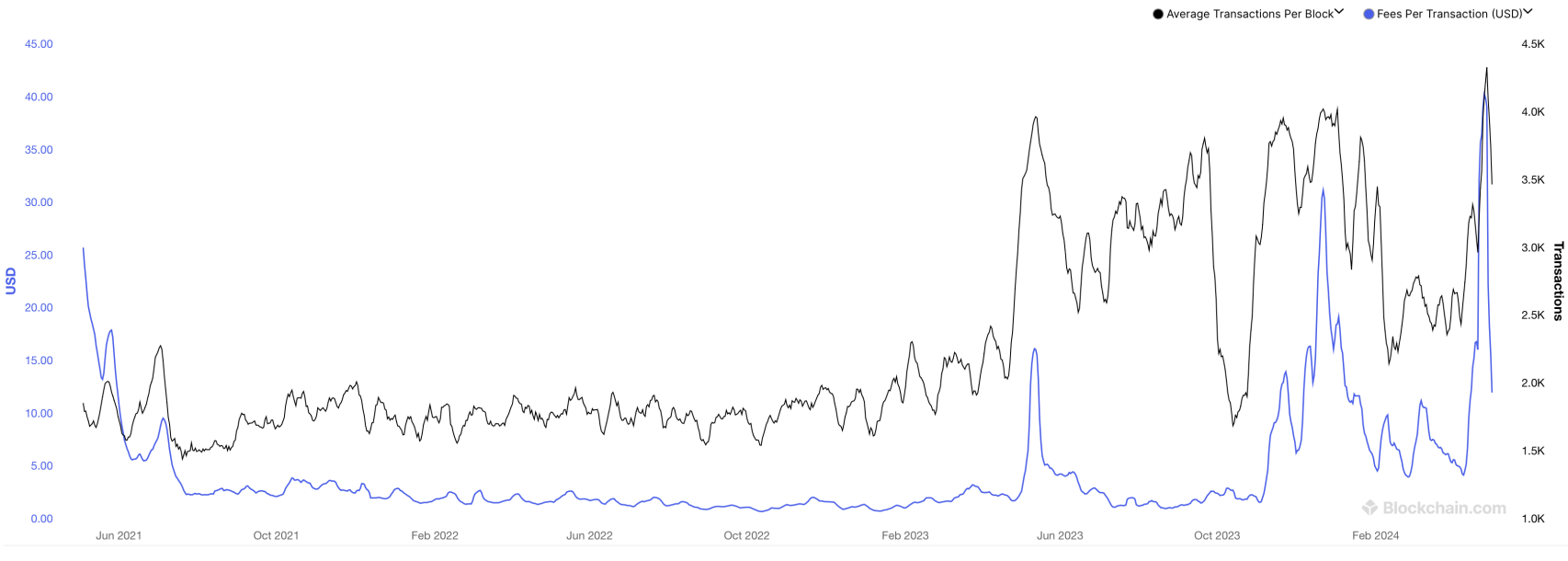


Figure: Fees per transaction in USD vs average transactions per block. Source: `Blockchain.com`.

Alternative protocols

PoW is the most used protocol for decentralised consensus among permissionless Blockchains.

However, PoW has a series of shortcomings, such as energy consumption, which have spurred the development of alternative consensus protocols.

Another popular alternative to PoW is Proof-of-Stake (PoS).

- ↪ In PoS protocol, the recordkeeper is chosen based on a combination of random selection and wealth.
- ↪ Miners need to prove the ownership (or stake) of a certain amount of native tokens to have the right to mine blocks.

Roughly speaking, PoW offers good security and decentralisation but lacks scalability. PoS is more scalable but lacks decentralisation.

The Blockchain trilemma

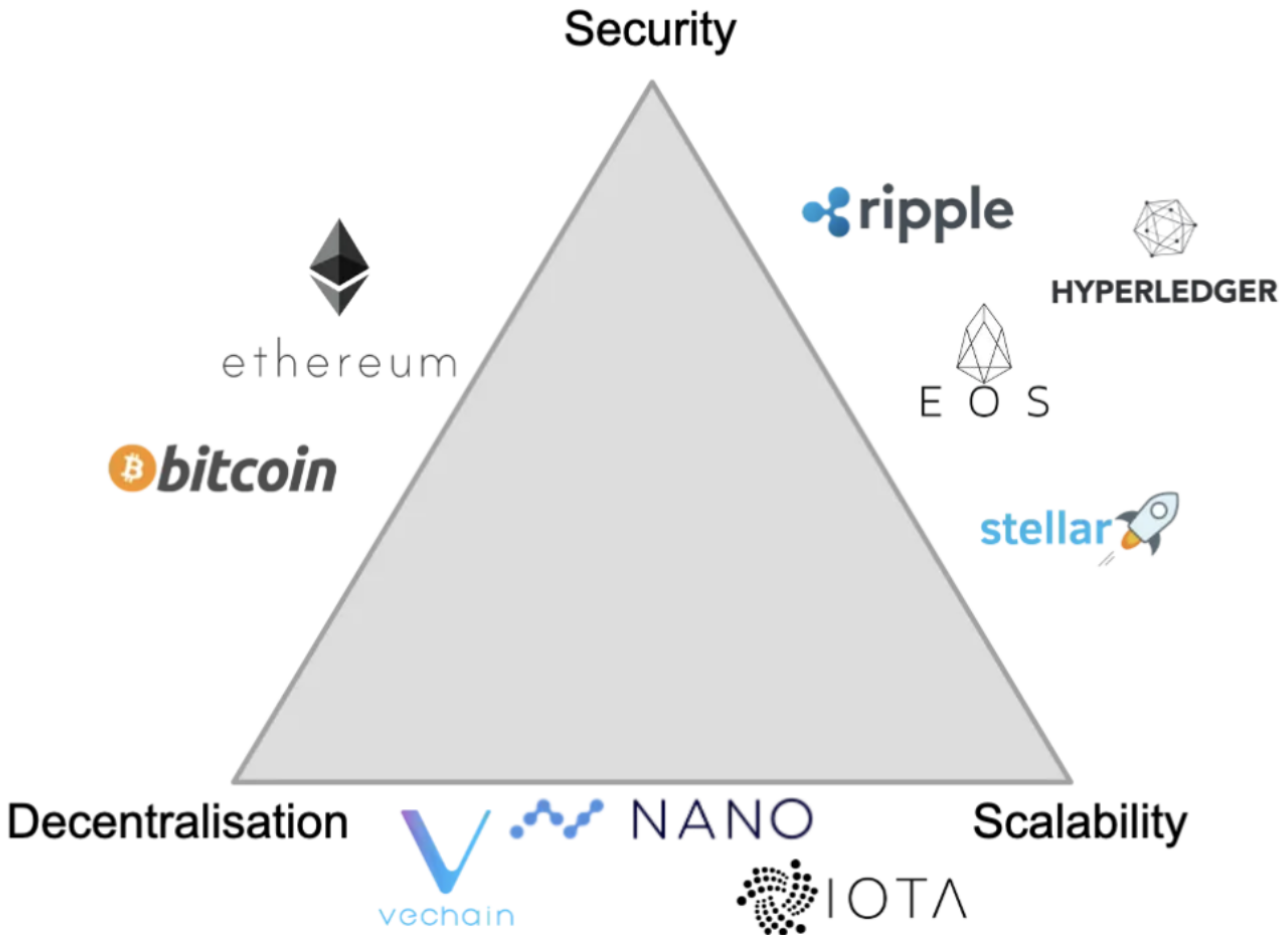


Figure: The blockchain trilemma with examples of blockchains which excel in a particular property.

The Blockchain trilemma

The Blockchain trilemma refers to the trade-off between 3 critical aspects of blockchain technology: Security, scalability, and decentralisation.

Blockchain developers often have to trade between decentralisation, security, and scalability.

↪ It is generally accepted that a public blockchain can only truly achieve 2 of the three benefits at any given time.

↪ Bitcoin runs on a blockchain network that prioritises decentralisation and security, which poses scalability challenges.

The "Blockchain Trilemma" is one of the larger hurdles for blockchain to achieve mass adoption.

The Blockchain trilemma

The Blockchain trilemma posits that blockchains cannot simultaneously achieve scalability, decentralization, and security.

Trade-offs:

- ↪ **Decentralisation:** When a blockchain network involves many participants, we can expect any consensus on transactions or upgrades to the blockchain to take time (sacrificing scalability).
- ↪ **Security:** While increasing hash power in mining under the PoW consensus improves security, it also increases mining costs. It may force smaller, less efficient mining set-ups to exit $\Longrightarrow$ less decentralisation.
- ↪ **Scalability:** One way to increase a network's scalability is to reduce the number of nodes. However, this reduces the censorship resistance and security of the blockchain.

Benefits of decentralisation

The Benefits of decentralisation

In a traditional finance/banking system, only a centralised authority can record transactions and update account balances.

↪ Centralised systems such as governments and large IT firms have traditionally supplied trusted systems and digital platforms/exchanges.

Why do we need decentralised consensus, then?

Decentralisation has three core benefits:

↪ Increases the resilience of an economic system.

↪ Increases competition and the overall system efficiency.

↪ Incentivises interactions transparency and value sharing.

Resilience

By having irreversible records distributed through the network, blockchain helps mitigate the effect of "points of failure" which could prevent the network from functioning.

↪ Once data has been written to a blockchain, it is nearly impossible to alter the records without consensus from the network.

Because hash-pointers are immutable (with time stamping), no single party can change the historical transaction record or the sequence of events recorded on the distributed ledger.

↪ Caveat: storing duplicate copies of the entire history of transactions could be costly.

Resilience

How about hacks, though? Some major hacking events.

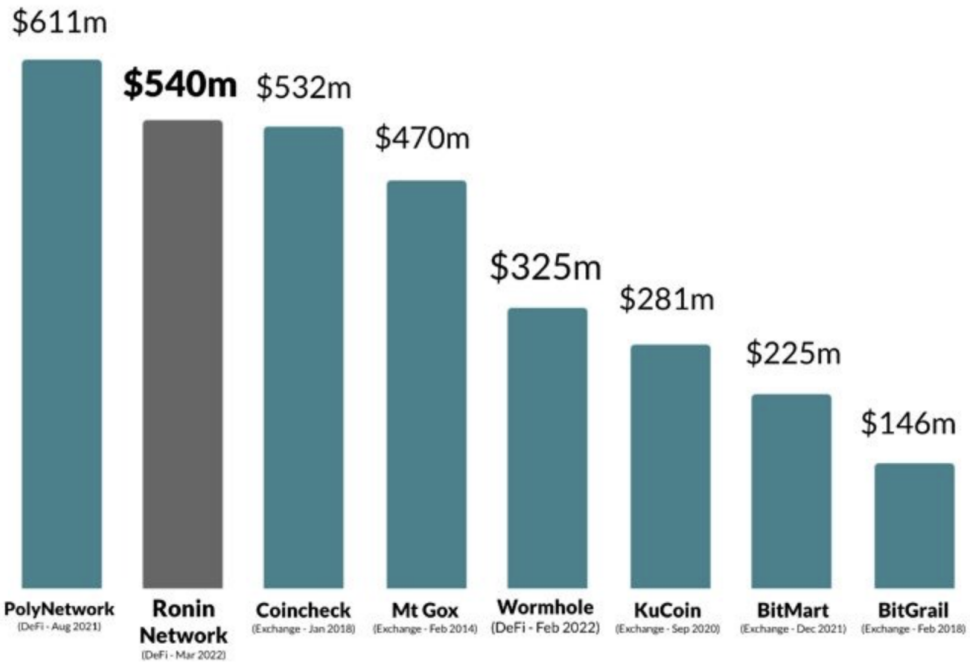


Figure: Observed hacking events (as of 03/2022) raise the question of whether systems are truly decentralised rather than whether decentralised systems are truly resilient.

Competition

A popular argument favouring blockchain is that enabling peer-to-peer transactions eliminates the need for intermediaries such as banks, payment processors, and even some legal services.

However, assuming disintermediation is the main benefit of decentralisation is misleading. The real advantage of (a public) blockchain is openness.

$\hookrightarrow$ More competition in providing service, reducing intermediaries' rent.

That does not imply that a decentralised system is perfectly competitive; there could still be local monopolies, especially for miners and large owners.

People discussing competition in blockchain usually have permissionless blockchains in mind.

Competition

Blockchain technology can increase competition by introducing new business models and reducing barriers to entry.

Driven purely by the incentives embedded within their protocol, permissionless platforms enjoy the benefits of a shared network without the main cost: Market Power.

↪ When people talks about "censorship resistance", is market power that they really have in mind.

↪ Interoperability across blockchains is key to increasing competition within blockchain technology.

A permissionless blockchain can be used to bootstrap a digital platform without the need for a central intermediary.

Key economic issues

Key economic issues

The specific design of a consensus protocol to balance security, decentralisation, and scalability can have important socio-economic implications.

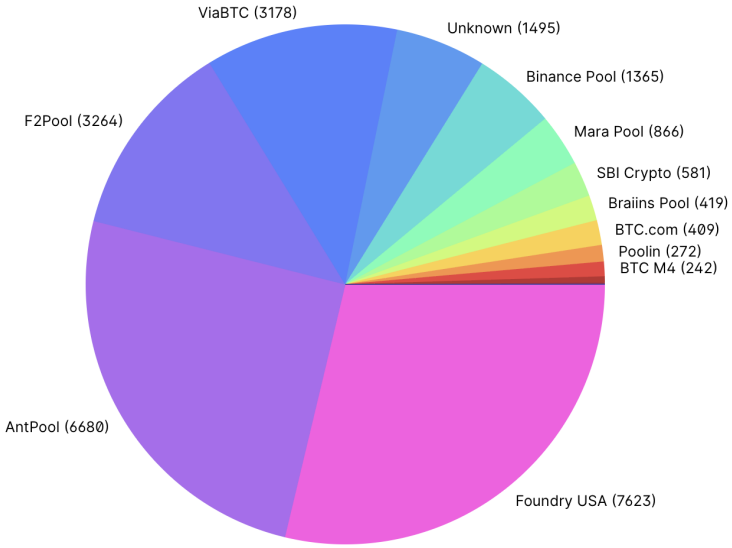
Overconcentration, sustainability, and adoption are all crucial considerations for designing consensus protocols.

↪ All three aspects have received particular attention from regulators and policymakers but for different reasons.

Security is also a crucial aspect of consensus protocol design but is less intertwined with socioeconomic implications.

Overconcentration

Mining tends to be controlled by a few entities...



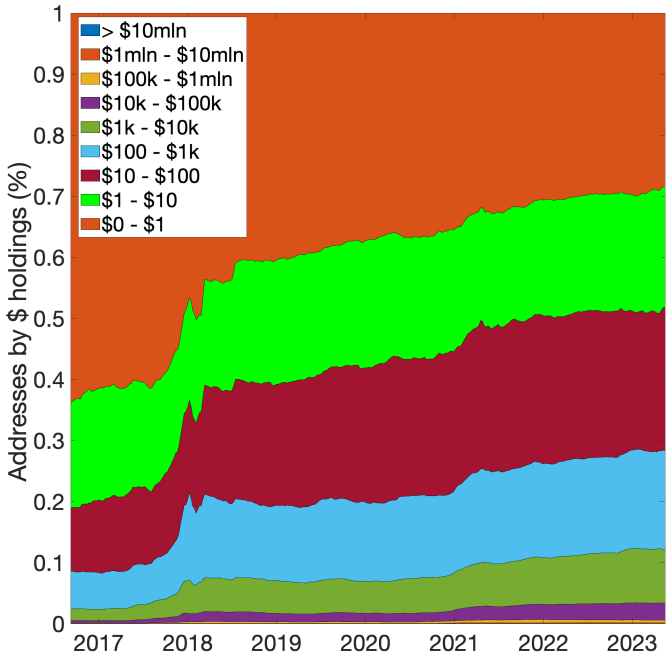
Summary of Mined Blocks

Miner / Pool	Percent	Blocks Mined
Foundry USA	28.742%	7623
AntPool	25.187%	6680
F2Pool	12.307%	3264
ViaBTC	11.983%	3178
Unknown	5.637%	1495
Binance Pool	5.147%	1365
Mara Pool	3.265%	866
SBI Crypto	2.191%	581
Braiins Pool	1.580%	419
BTC.com	1.542%	409
Poolin	1.026%	272
BTC M4	0.912%	242
Ultimus	0.392%	104
1THash	0.068%	18
Solo CKPool	0.015%	4
Zulu Pool	0.004%	1
KanoPool	0.004%	1

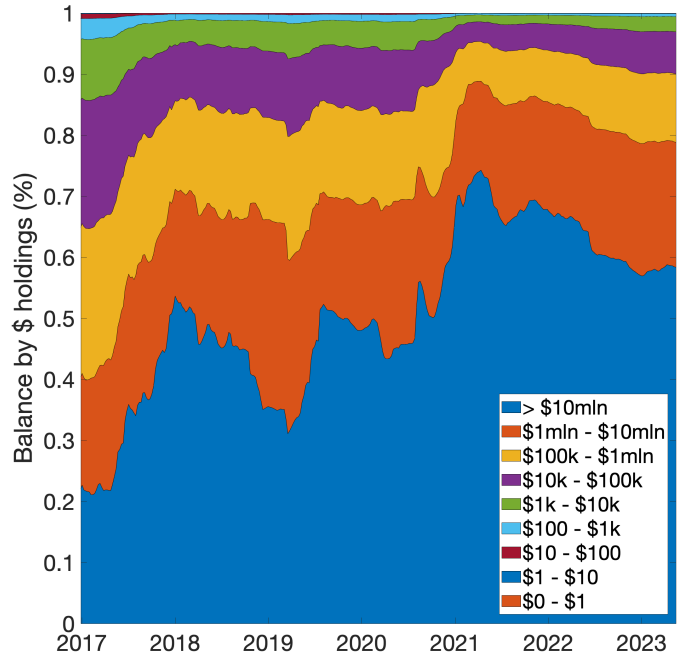
Figure: The graphs show the market share of the most popular Bitcoin mining pools. It should only be used as a rough estimate and, for various reasons, will not be 100% accurate. Blocks grouped into the 'Unknown' category do not mean an attack on the network. It simply means we have been unable to determine the origin. Source: `Blockchain.com`

Overconcentration

... and ownership/wealth is highly concentrated as well.



(c) Addresses by holdings (%)



(d) Balance by holdings (%)

Figure: The distribution of BTC addresses by holdings (left panel) and the distribution of BTC supply by holdings (right panel). The sample is from January 2017 to May 2023.

Overconcentration

Some interesting facts from the previous figure (as of May 2023):

1. Almost 70% of the addresses own less than \$100, while only 1% own more than \$100k, and 0.1% of addresses holding more than \$10mln.
2. Large addresses account for most of the Bitcoin supply. Addresses holding more than \$100k hold approximately 90% of the supply.
3. The concentration of wealth increased over time, with only 20% of the BTC supply held in the largest addresses ($> \$10 mln$) in 2017, compared to 60% in May 2023. This is a x3 increase in six years.

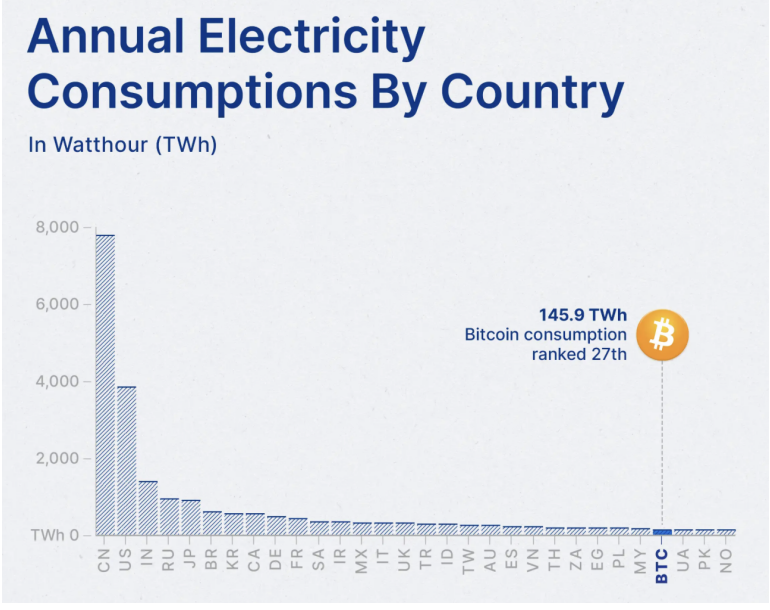
Overall, $\approx 95\%$ of the accounts holds $\approx 10\%$ of the supply.

$\hookrightarrow$ Rather substantial wealth concentration.

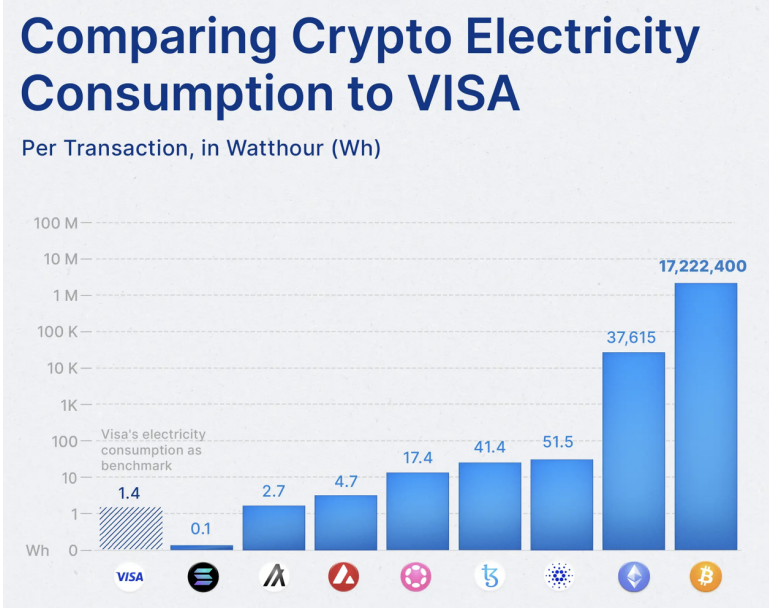
$\hookrightarrow$ Careful though, some addresses may be institutional investors, miners, or exchanges offering custodian services.

Energy consumption and sustainability

One of the issues that arguably received the most attention is the sustainability of PoW blockchains.



(e) BTC Mining energy consumption

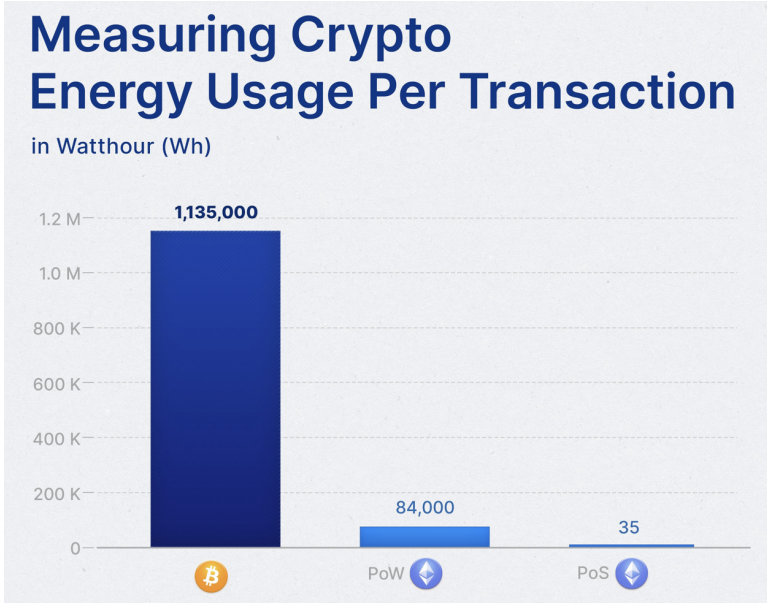


(f) BTC mining vs other payments

Figure: The energy consumption of BTC mining vs major countries (left panel) and vs other payment methods (right panel), as of January 2022. Source: `Crypto.com`.

Energy consumption and sustainability

Again, this is a manifestation of the Blockchain trilemma. There might be more sustainable consensus protocols, though, such as Proof-of-Stake.



(g) BTC vs ETH energy consumption

Figure: The energy consumption of BTC mining vs ETH mining as of November 2023. Source: `Crypto.com`.

Energy consumption and sustainability

Can Bitcoin growth be sustainable?

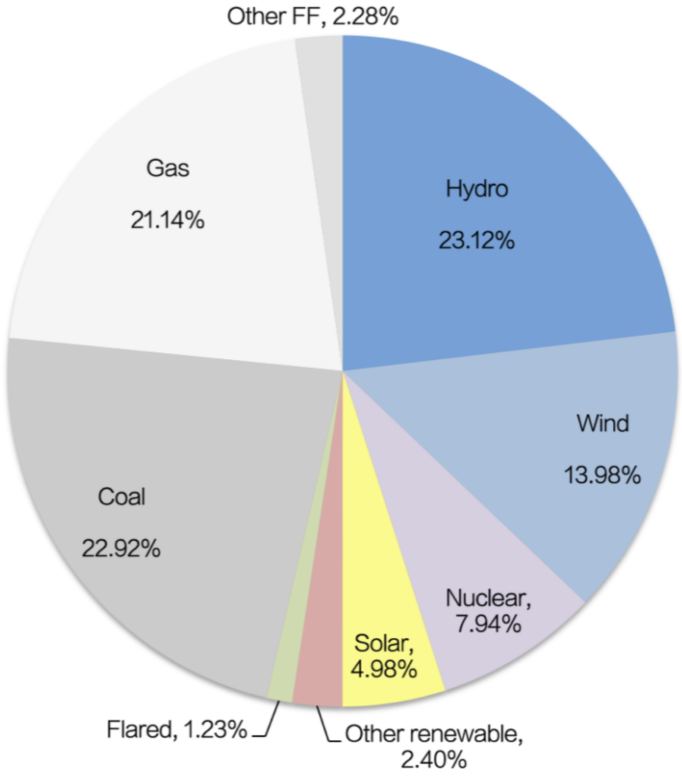


Figure: Bitcoin mining energy sources as of March 2023. Source: `batcoinz.com`.

Another option is carbon offsetting $\Longrightarrow$ tokenised carbon credits.

Adoption

Blockchains's scalability is reflected by endogenous user adoption.

↪ Without mass user adoption, most blockchain applications cannot survive in the long run.

There is evidence that limited adoption arises endogenously in PoW blockchains.

↪ Increased transaction demand increases the fees, which induce recordkeepers to enter the network.

↪ The increased network size delays transaction confirmation and increases the effort needed to solve the cryptographic puzzle.

Again, this reflects the Blockchain trilemma, as increased security means more security but also limited adoption, *unless other solutions are implemented (e.g., Layer-2 protocols such as Lightning network).*

Adoption

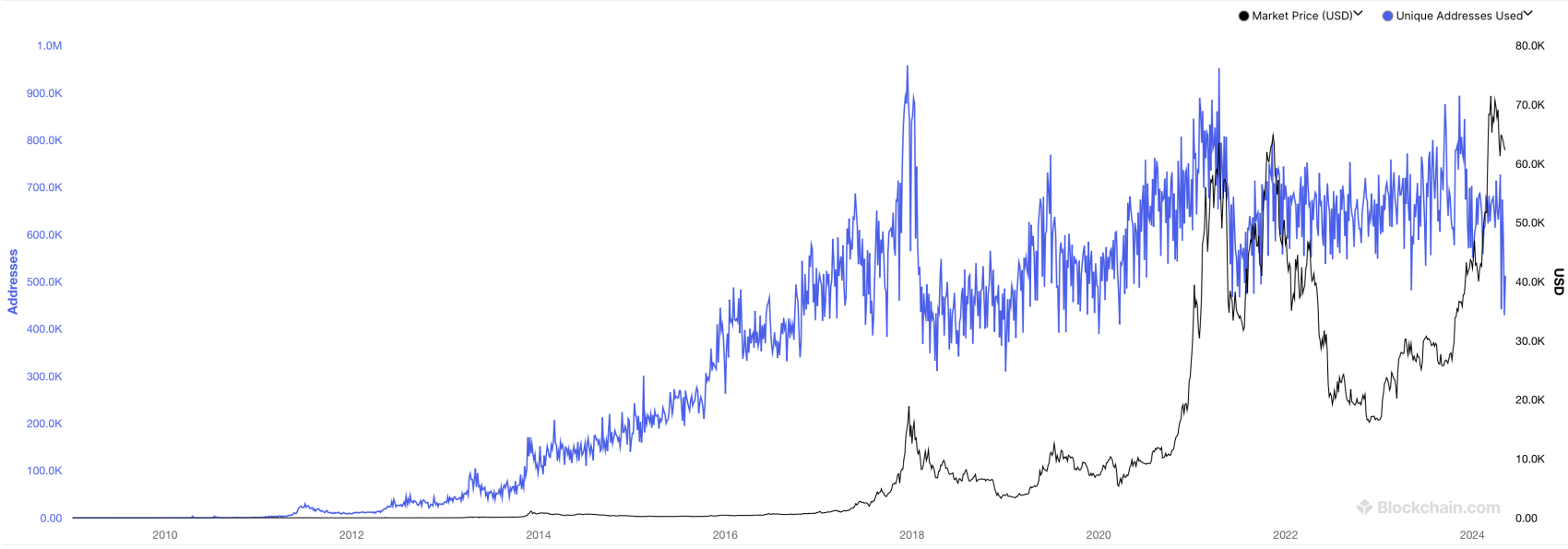


Figure: Bitcoin unique addresses used vs Bitcoin price. Source: `Blockchain.com`.

What did we learn?

Consensus protocols are key for the security and transparency of the blockchain.

- ↪ Consensus protocols determine how network participants interact in the blockchain.
- ↪ Common protocols are Proof-of-Work (e.g., Bitcoin) and Proof-of-Stake (e.g., Ethereum).
- ↪ There are differences between the two regarding decentralisation and energy consumption.

Blockchain trilemma: there is a seemingly unsolvable trade-off between scalability, security, and decentralisation.

Key economic issues are (1) the tendency of concentration of ownership and mining, (2) the sustainability of some consensus protocols, such as PoW, and (3) the adoption of blockchain on a large scale.