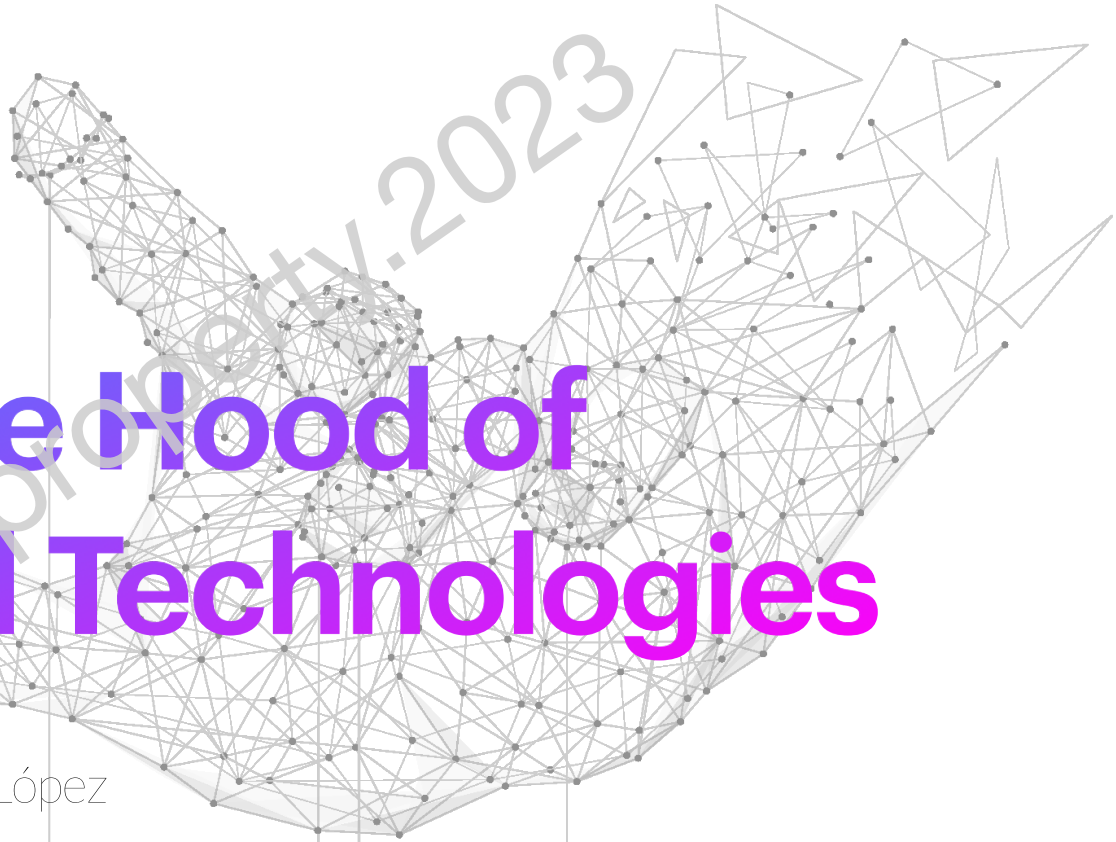
Under the Hood of Decentralized Technologies

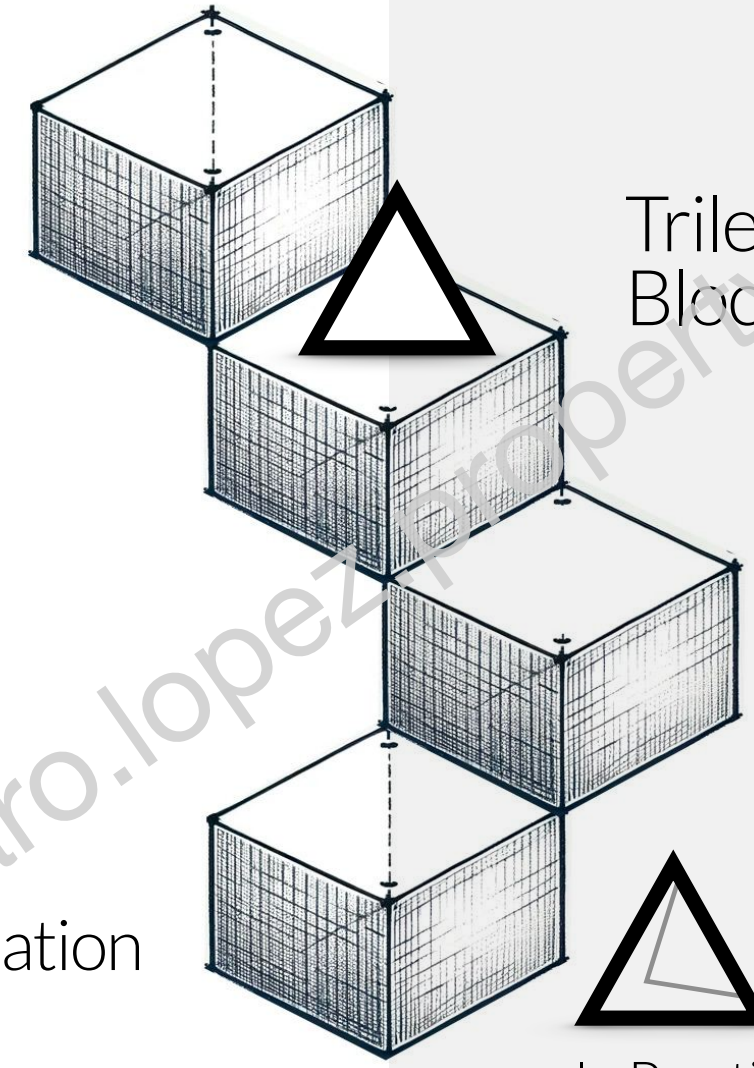


Álvaro López

Is decentralization an illusion?

28th October 2023
Biznaga Fest, Málaga

Decentralization ecosystem



Trilemma of Blockchain

Scalability challenges and gains

Security on ~~De~~centralization

In Practice!

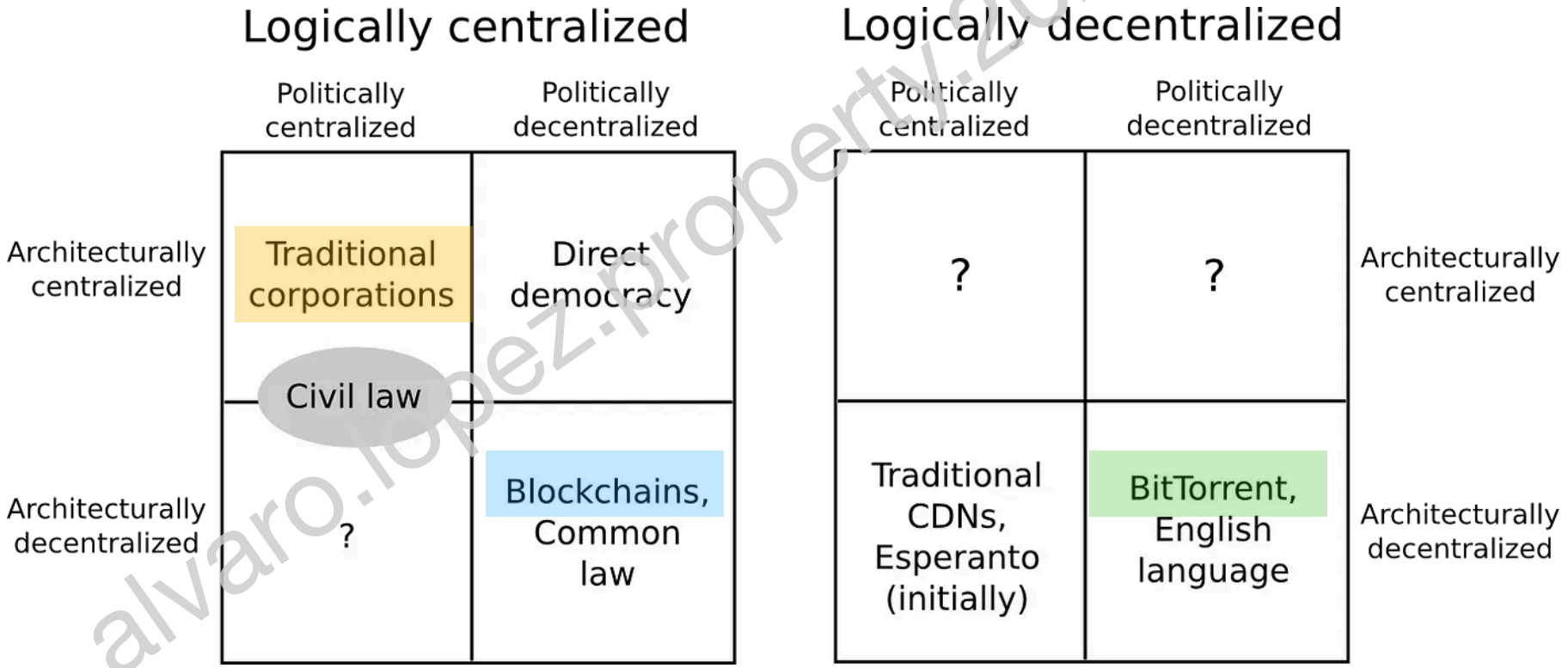
1of6

Decentralization ecosystem

Decentralized technology concepts, (de)centralization paradigm, Blockchain the modern distributed system.

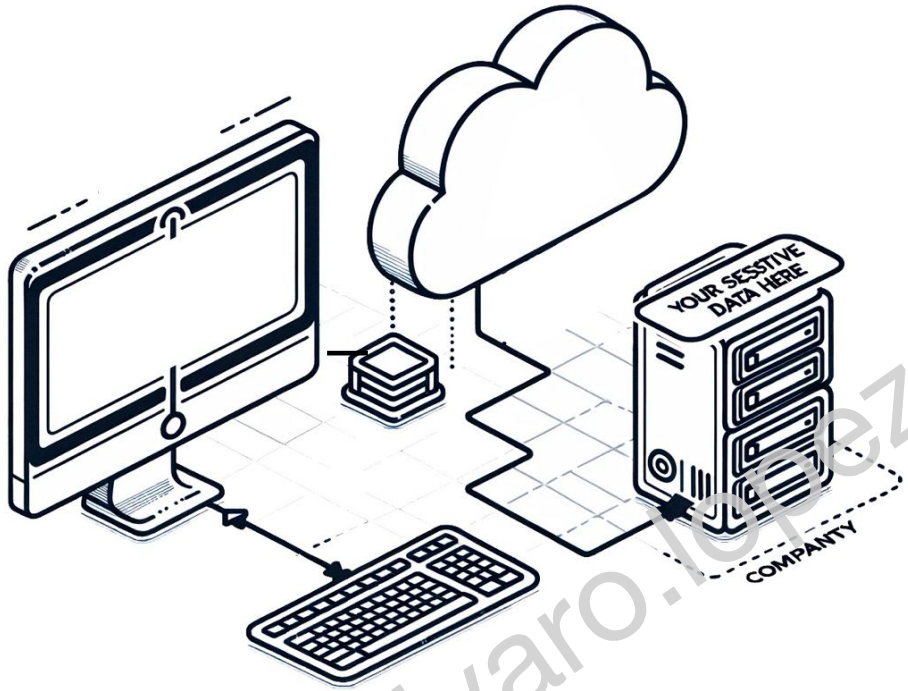
Decentralization *is also a key concept in organizational structures, governance models, and other systems where power and control can be distributed.*

Vitalik Buterin
[1]



[1] Vitalik Buterin The meaning of decentralization https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

Is *centralization* a real-life issue?



AirEuropa [3] 23andMe® Globalcaja Clínic Barcelona

No

⬆ Centralization is undoubtedly an effective way to manage organizations or network

Yes.

⬇ Risk of data breaches or ransomware attacks

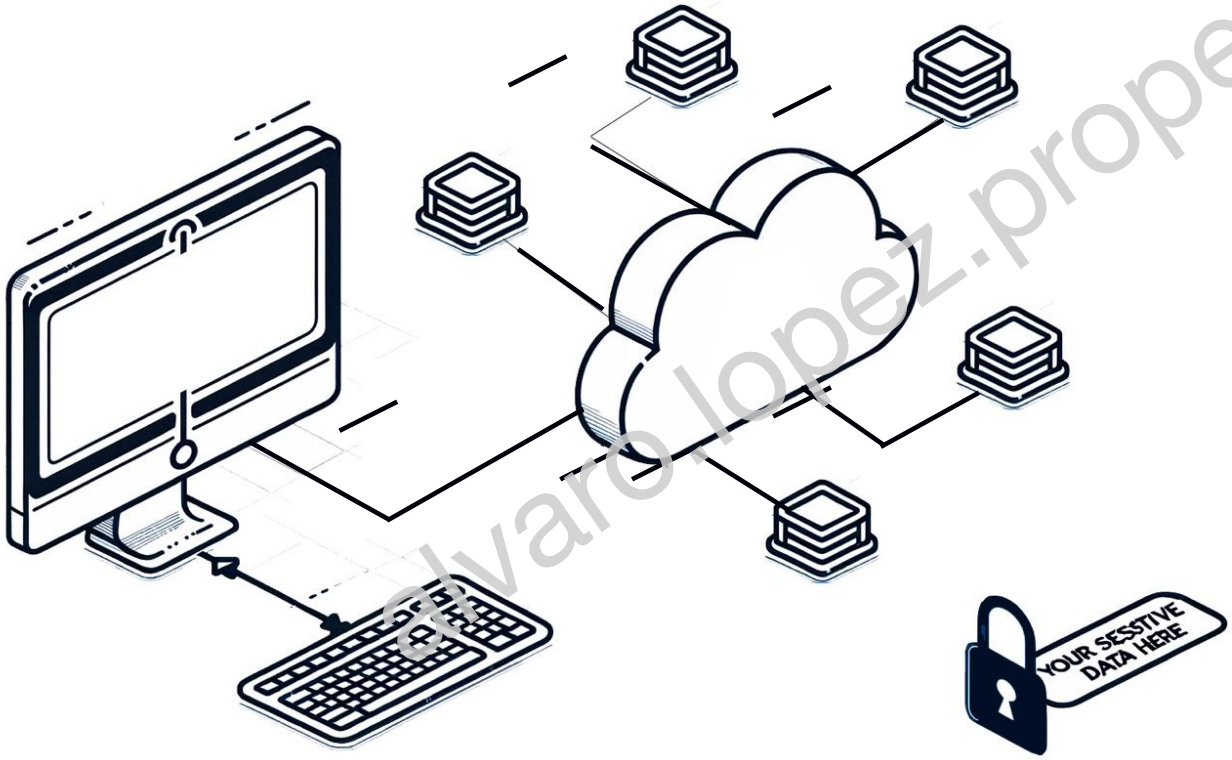
*Countries have suffered the most **attacks** on airlines [2], financial institutions, significant places, and hospitals during the last year.*

[2] Payments method leaked (airEuropa) https://www.xataka.com/seguridad/air-europa-sufre-ciberataque-pide-a-todos-sus-clientes-que-cancelen-sus-tarjetas-credito

[3] Millions of DNA information leak (23andme) https://blog.23andme.com/articles/addressing-data-security-concerns

Ok, so ...what does *decentralization* resolve?

- Decentralization is here to stay



- **Trust**. Consensus mechanisms ensure trust in distributed information

- **Self-custody**: individual ownership and control of digital information

.. are *real-life* examples of decentralization ratified?

W3C®

ENS vitalik.eth (0xd8dA6BF..045)

- **Decentralized identities**
  - Self-sovereign identifies (SSI) with DIDs
  - Sovrin (Hyperledger), Microsoft ION (BTC), uPort (ETH), Blockstack...
- **Domain Names decentralization**
  - ⬆ DNS vs ENS
  - ENS (Ethereum Name Service .eth), Handshake, Blockstack, r/ENS...
- **Financial decentralization**
  - ⬆ transparency, accessibility, inmutability in financial transactions
  - Bitcoin, Ethereum, Stablecoins,
  - Lightning Network (BTC), Raiden Network (ETH)...

⬇ Crypto exchanges are not decentralized, **only DEX!**

UNISWAP PancakeSwap Curve

Microservices architecture

Container orchestators

where is Blockchain in the **ecosystem of distributed systems**?

Edge computing

Serverless computing

Blockchain

Consensus mechanisms

bitcoin

P2P networks

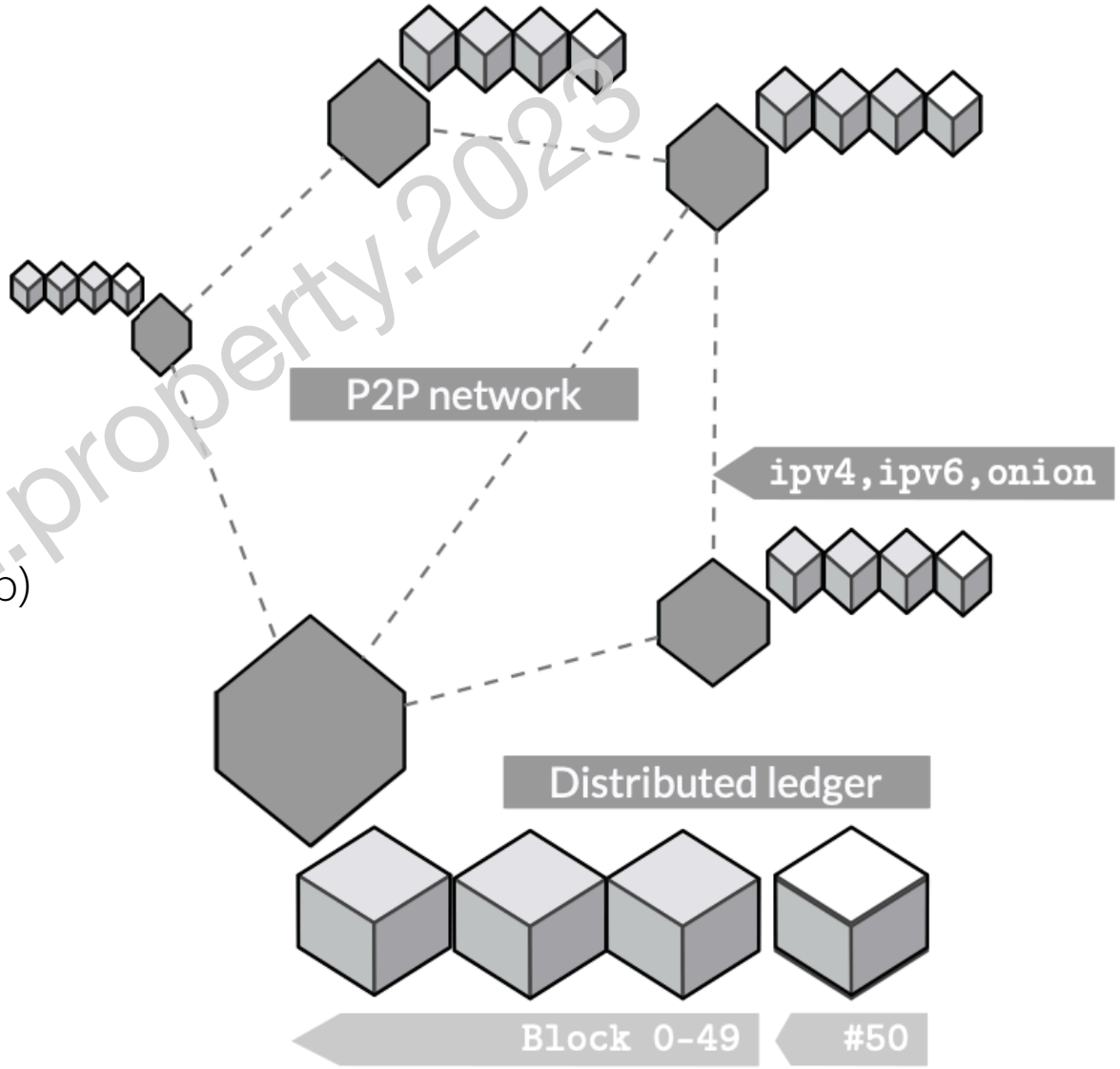
Signal

IPFS

BitTorrent

Blockchain

- **Peer-to-peer network**
  - Reachable nodes (BTC ~17k [4])
  - ⬆ Fault-tolerance
- **A distributed ledger**
  - Nodes + copy of the ledger (BTC ~500Gb)
  - ⬆ Redundancy
- **No control entity, just consensus !**
  - ⬆ Trust model
  - ⬇ **Low-rate transaction per second (TPS)**



[4] Reachable nodes by main crypto blockchains | Bitcoin: ~17k (source: https://bitnodes.io) | Ethereum: 7k (source: https://www.ethernodes.org)

[5] *LaTex* table built with source from **Bitcoin** (BTC): blockchain.com | **Ethereum** (ETH): etherscan.io or etherscan.io/chart2/size | **Litecoin** (LTC): litecoinblockhalf.com | **Bitcoin Cash** (BCH): blockchair.com | **Cardano** (ADA): cardanoscan.io | **Hyperledger** : hyperledger.org | **IBM Blockchain** : ibm.com/blockchain | **Quorum**: consensys.net/quorum | **Chainlink**: chain.link | **Factom**: www.factomprotocol.org

[5]

Project	Blockchain type	Size (GB)
Bitcoin	Public	350
Ethereum (archive)	Public	7 TB
Ethereum (geth full node)	Public	400-500
Litecoin	Public	40
Bitcoin Cash	Public	200
Cardano	Public	12
Hyperledger	Permissioned	Varies
IBM Blockchain	Permissioned	Varies
Quorum	Permissioned	Varies
Chainlink	Public	(Ethereum)
Factom	Public	10

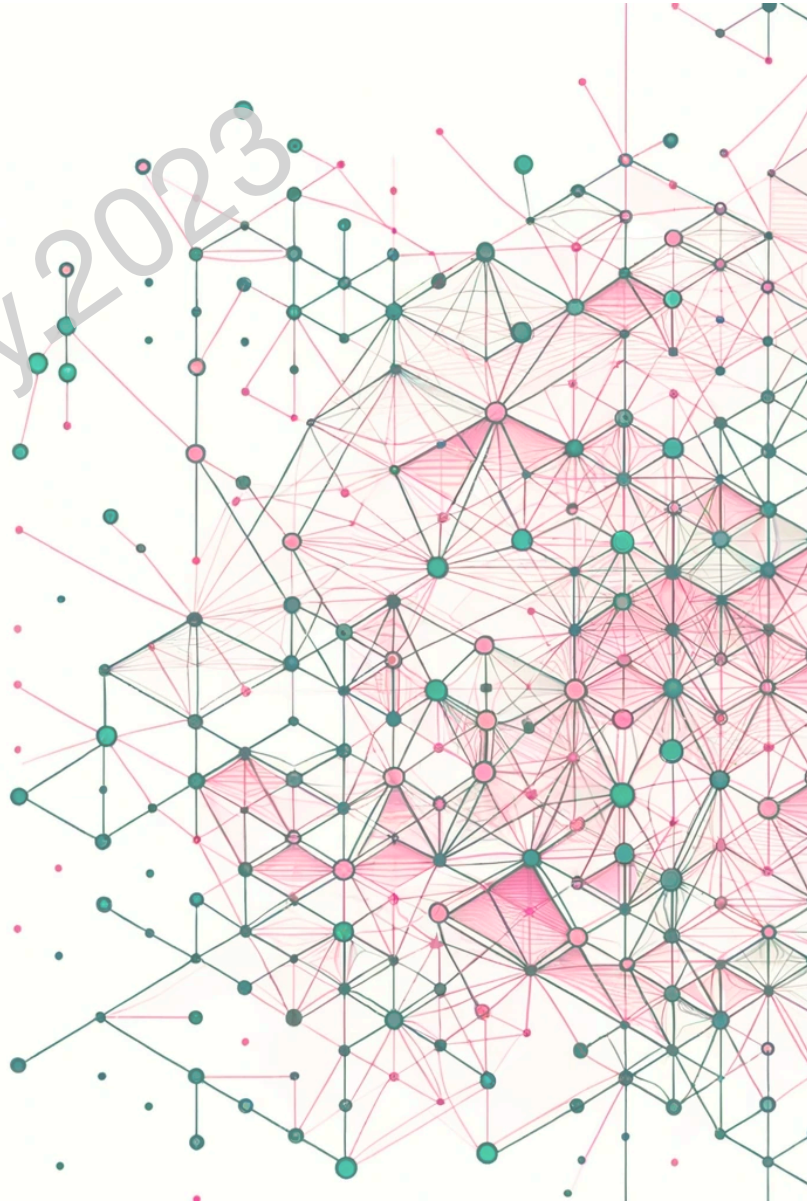
Bitcoin first real-world blockchain application

Bitcoin: A Peer-to-Peer Electronic Cash System

[5]

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

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

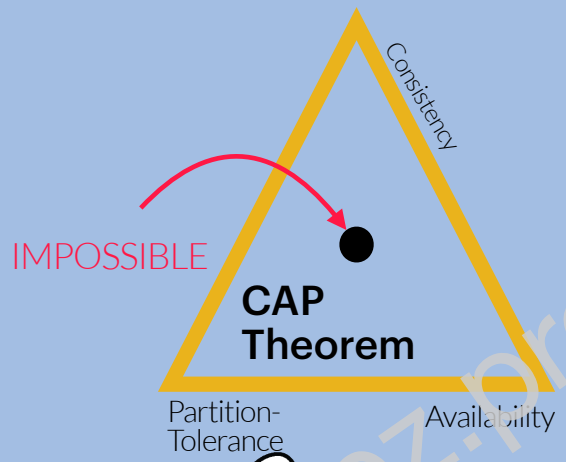


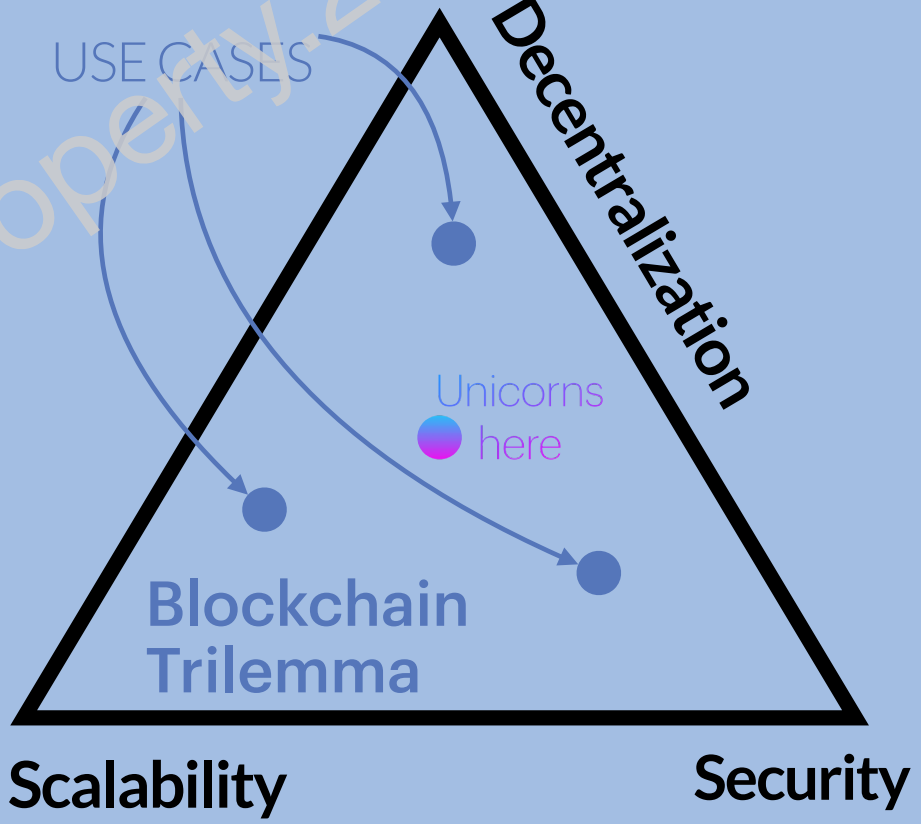
[5] Bitcoin -whitepaper- https://bitcoin.org/bitcoin.pdf

Triangle of Balance

Blockchain scalability, decentralization and security trade-offs.

How to **balance** these concepts?





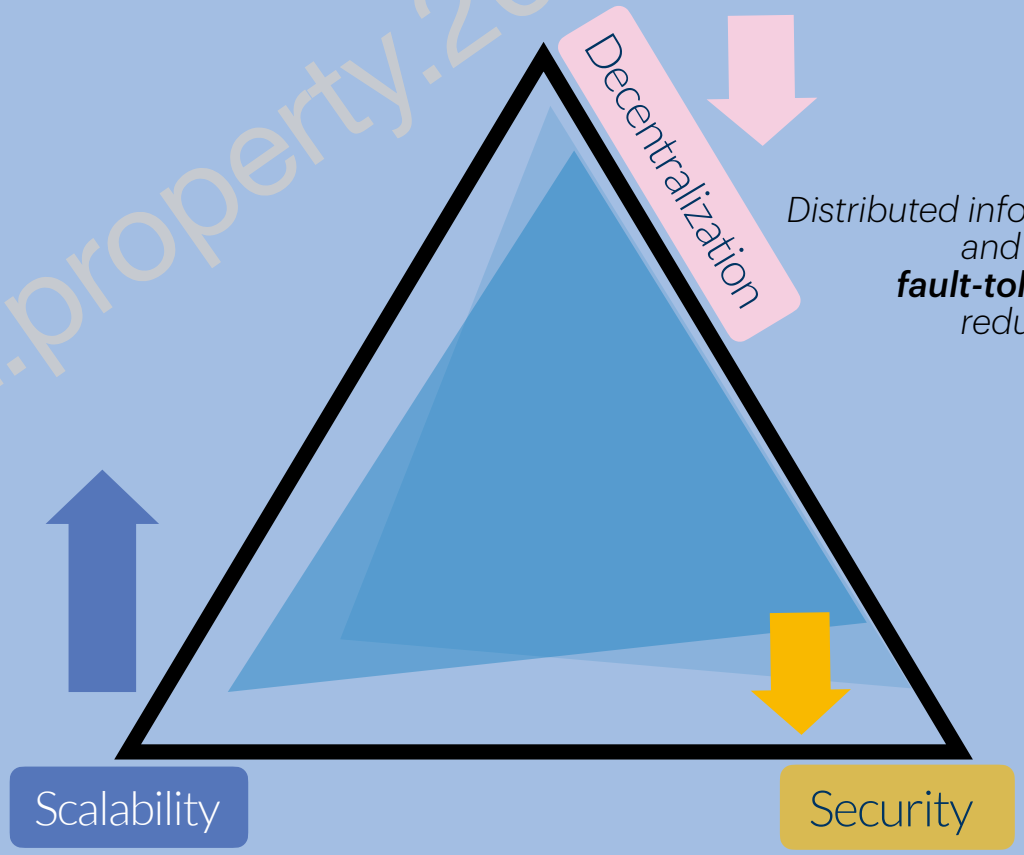
The cost of scalability

Decentralization

Security

Scalability

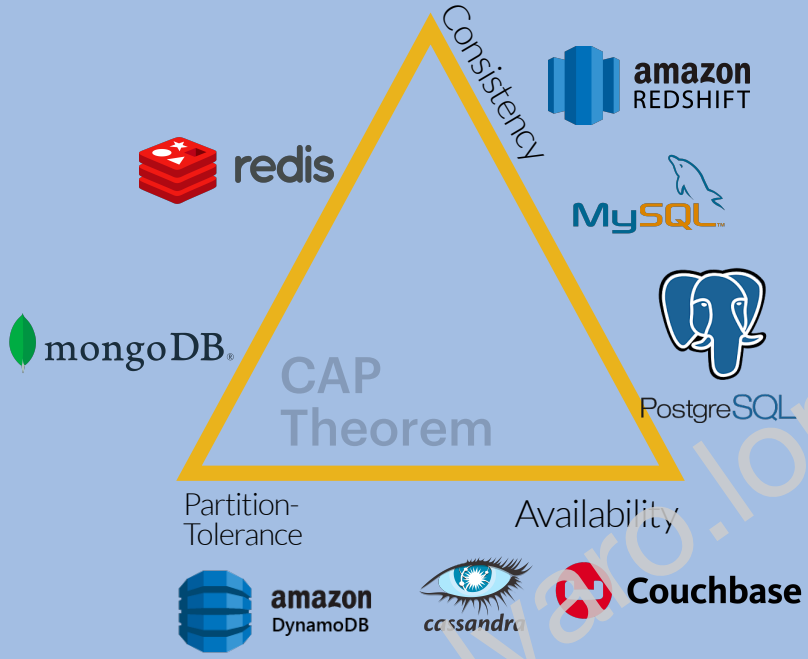
- Centralization risk
- Loss of privacy
- Untested software vulnerabilities
- Increase attack surface

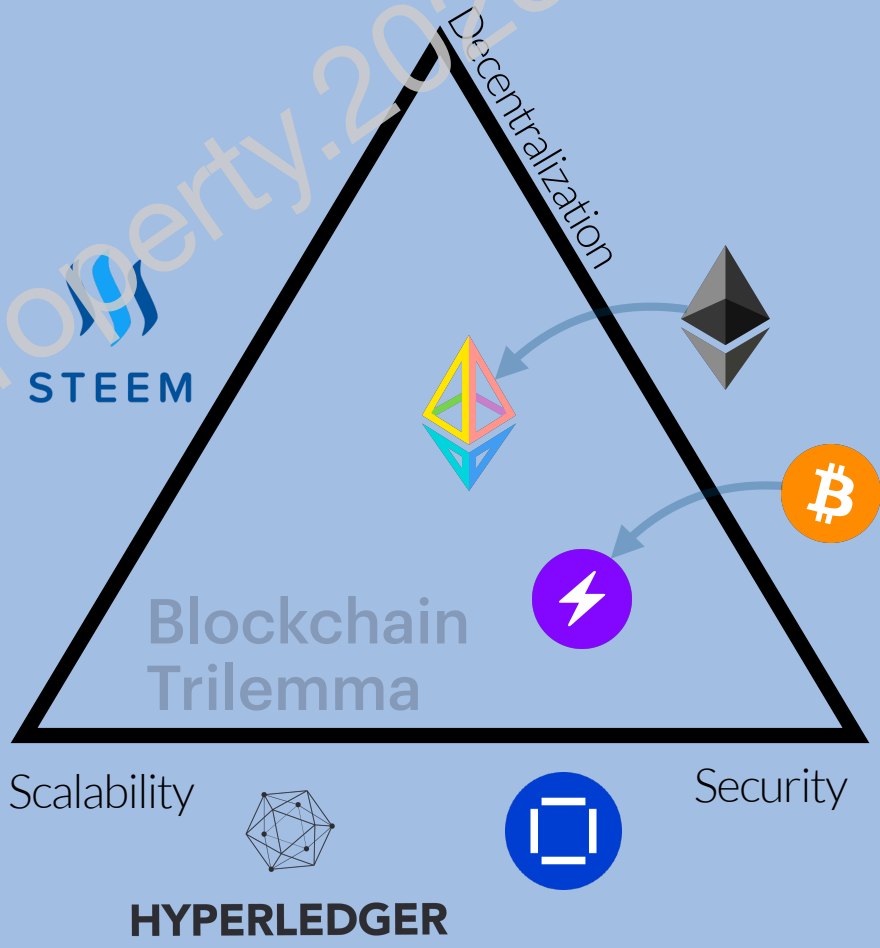


Distributed information and control, ***fault-tolerance****, redundancy*

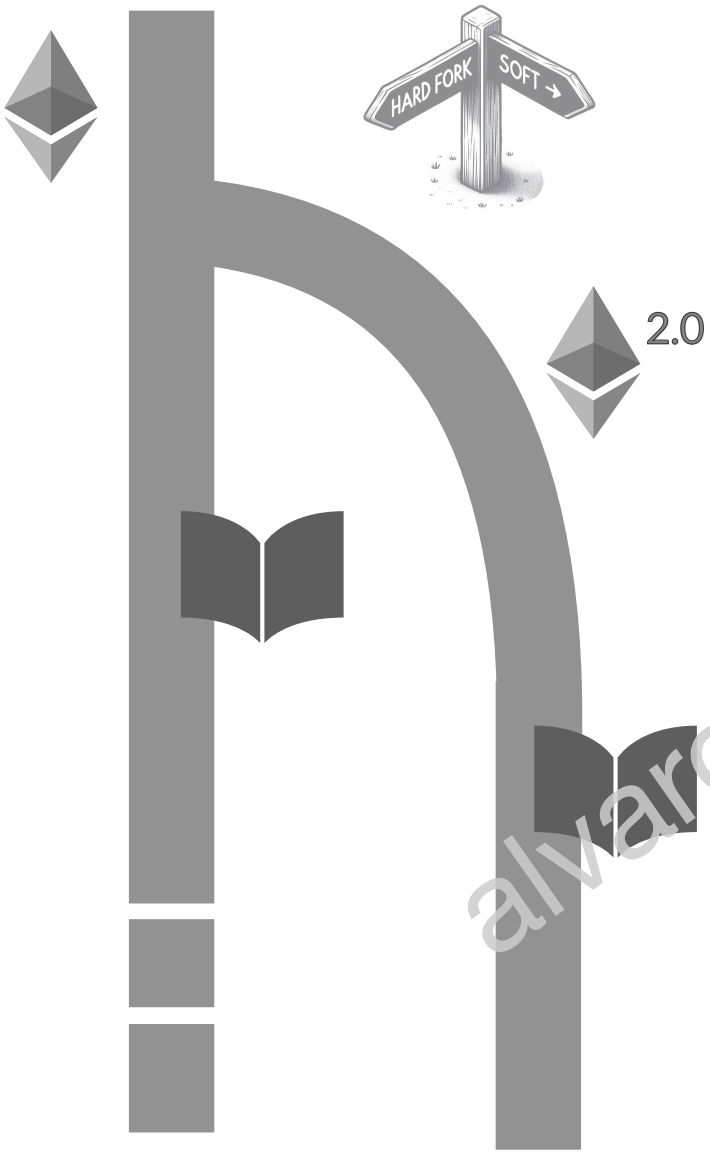
Increasing workload along performance: ***TPS, throughput, latency***

Trust *model, sensitive information, the integrity of the network*





3of6 Forks and Proposals



Improvement Proposals

Stagnant Standards Track: Core

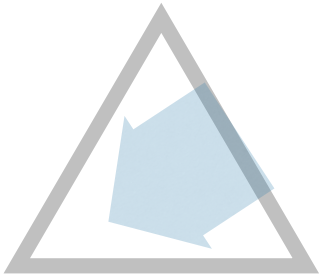
EIP-2537: Precompile for BLS12-381 curve operations

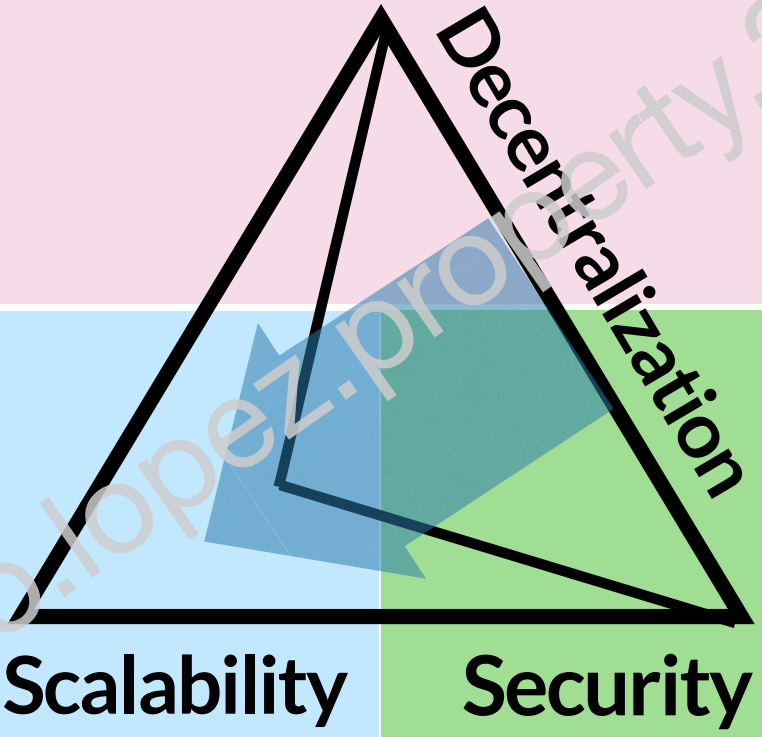
```
BIP: 141
Layer: Consensus (soft fork)
Title: Segregated Witness (Consensus layer)
Author: Eric Lombrozo <elombrozo@gmail.com>
        Johnson Lau <jl2012@xbt.hk>
        Pieter Wuille <pieter.wuille@gmail.com>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0141
Status: Final
Type: Standards Track
Created: 2015-12-21
License: PD
```

4of6

Solving for Scalability

how crypto-cruisers tackle the scalability issues ...





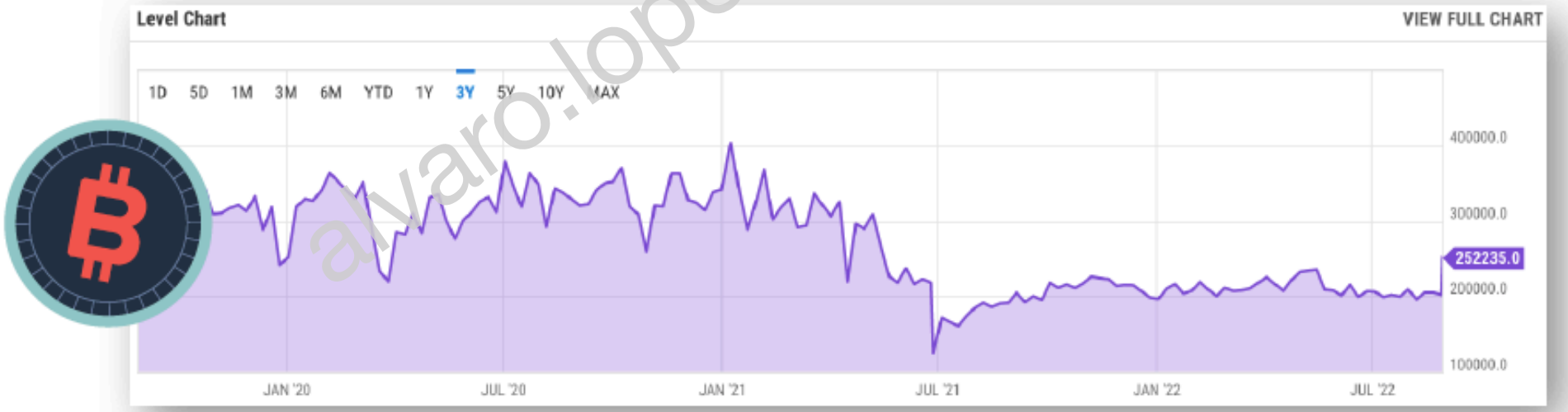
Scalability | Security | Decentralization

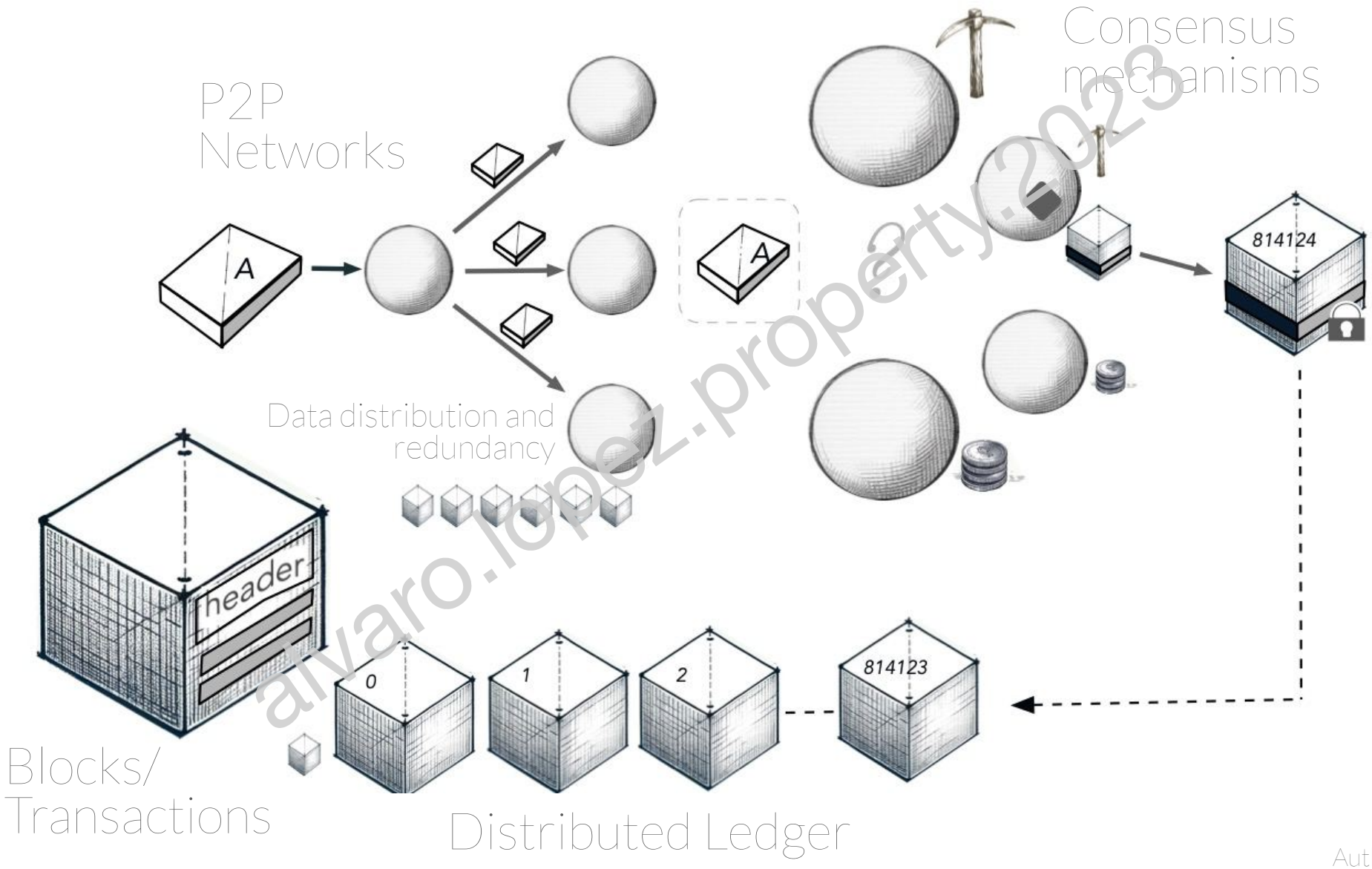
The Blockchain cryptos suffer the most known **scalability challenges**

- Data distribution and redundancy
- Consensus mechanisms

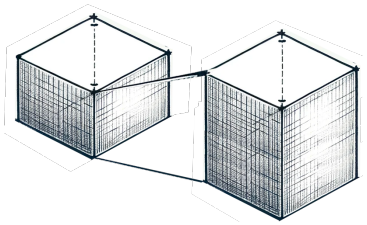
Low
TPS

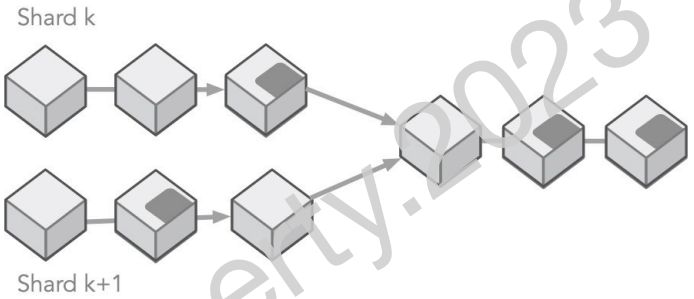
6–7	20	450	24,000



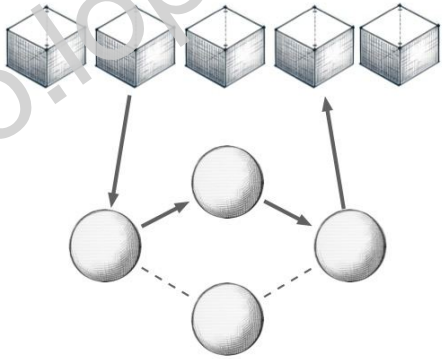


Author: @bluebycode





Enhancing **data size**, network **partitioning**, employing **side chains** **optimizing consensus** mechanisms.

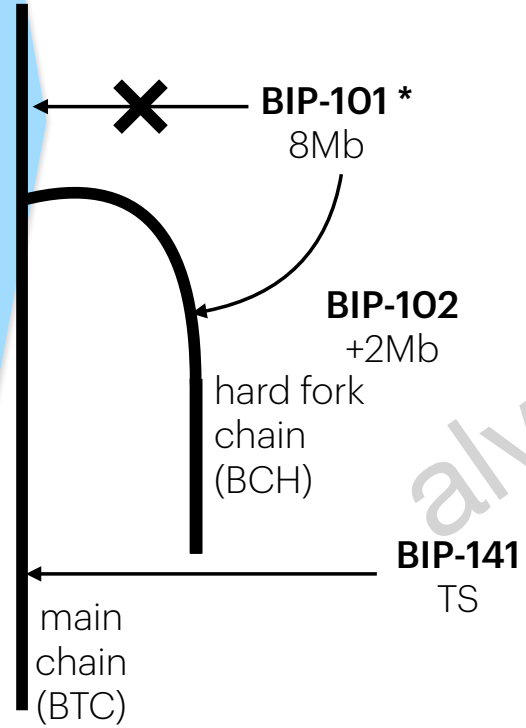


Higher TPS
Lower latency

Seize on **block and transaction** sizes increase the throughput

Scalability | Security | Decentralization

- BTC 1Mb (NOT APPLIED)
- BTC Cash 32 Mb (Hard fork)

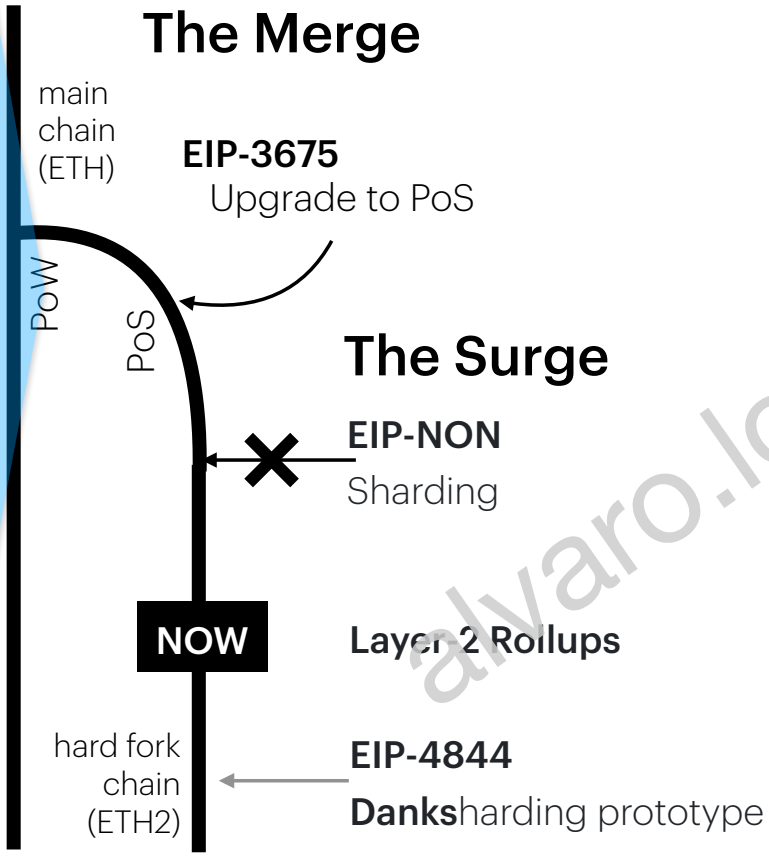


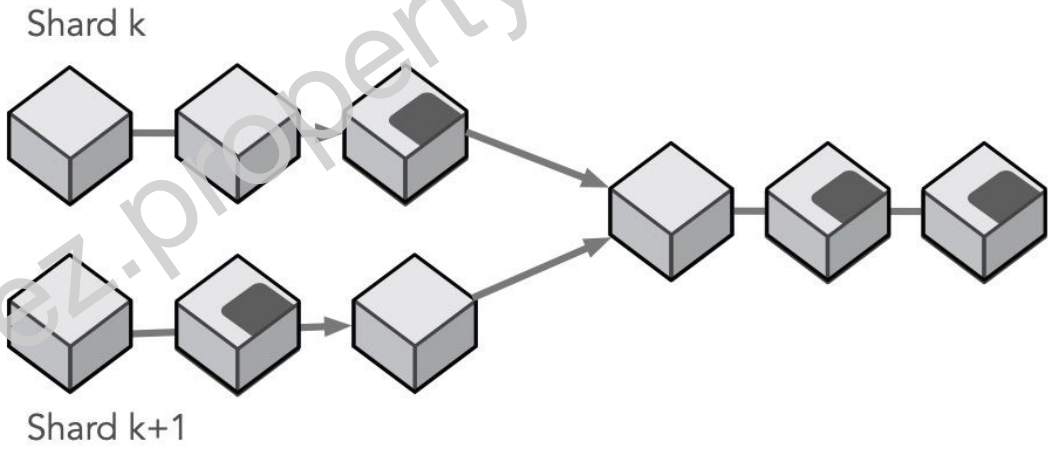
- BTC witness (signatures) decoupled from transaction
- ETH gas ("compute unit") limitation and cost affect the transaction number in a block indirectly

- Larger blocker => more storage => fewer nodes => Centralization risk
- DDOS attacks

Scalability | Security | Decentralization

Dividing the network into shards increase the throughput distributing into **parallel** processing workload

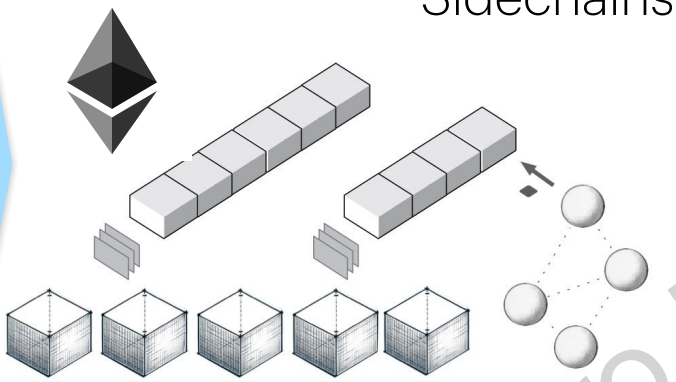




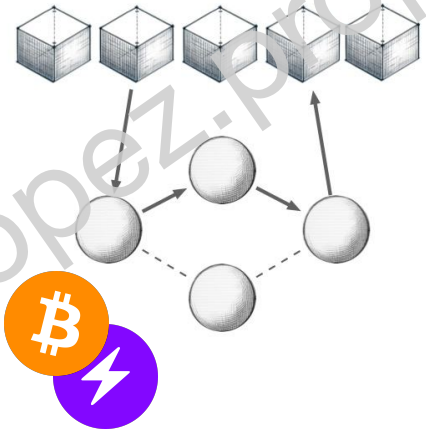
- Split networks, fewer nodes
- Centralization risk (C)
- 51% attack by manipulation (S)

Scalability | Security | Decentralization

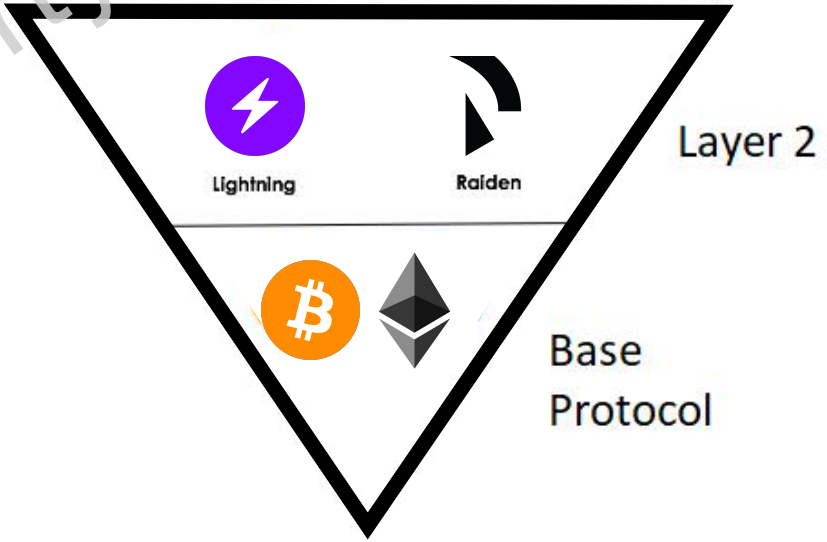
Offload transactions to **auxiliary chains** achieve **significantly higher** transactions per seconds



Sidechains



Layer-2 chains



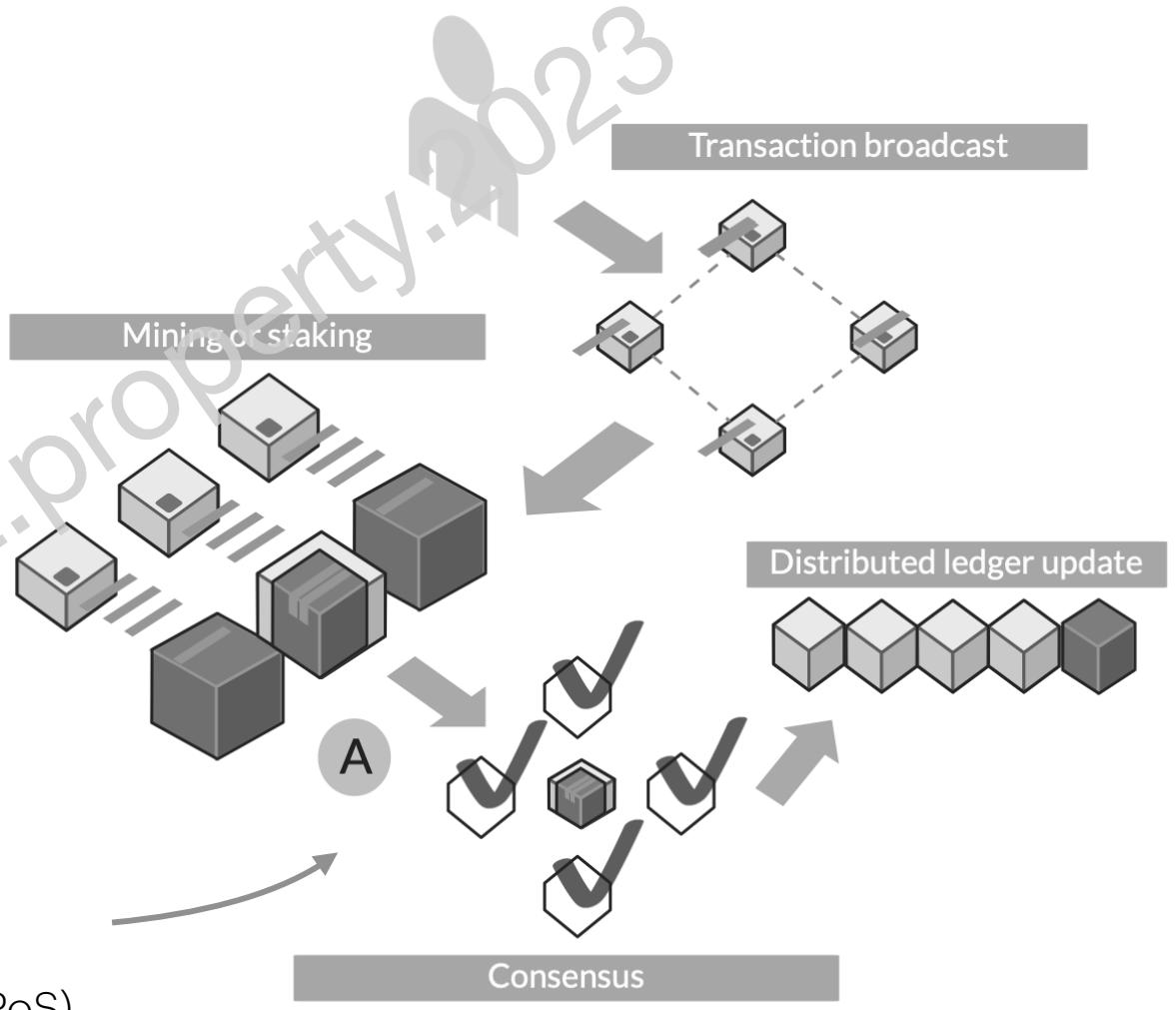
- Untested software => New vulnerabilities (S)
- Trust on ¿centralized? solutions => Centralization risk (C)

[6] Layer 2 solutions are built on top of the underlying blockchains, which are referred to as Layer 1 (Source: ListedReserve.com)

Scalability | Security | Decentralization

The **consensus** mechanisms and **incentivation** most responsibles of low scalability

- Consensus (PoW, PoS)
- Incentivation (fee)
  - Fees priorization and higher confirmation times => Network congestion

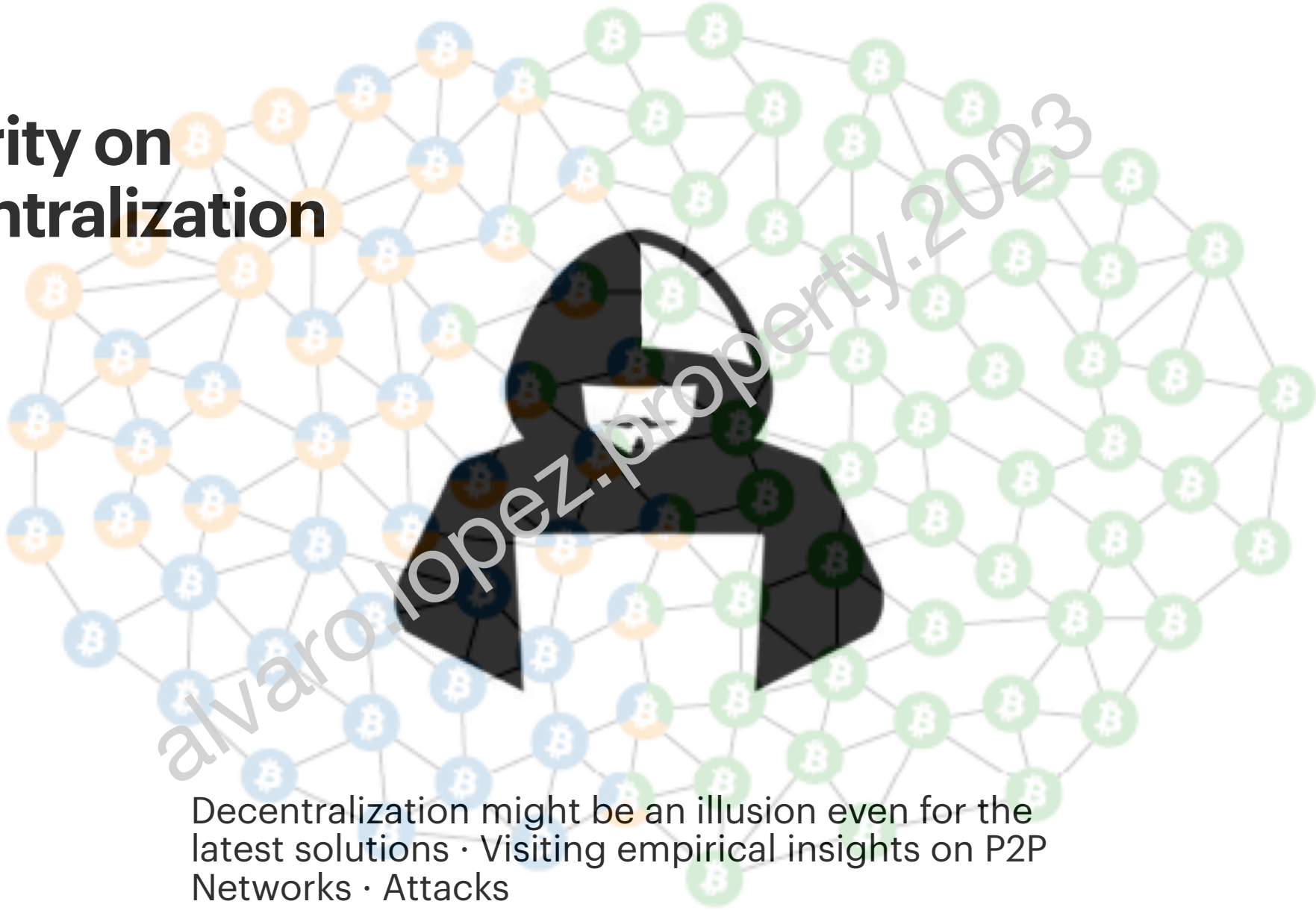


(A) Fees priorization creates network congestion (PoW)

(A) Limited validators cause higher confirmation times (PoS)

5of6

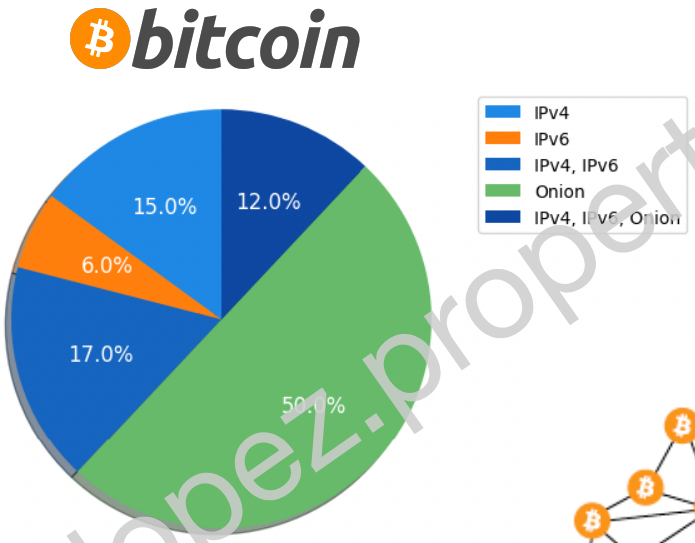
Security on ~~D~~ecentralization



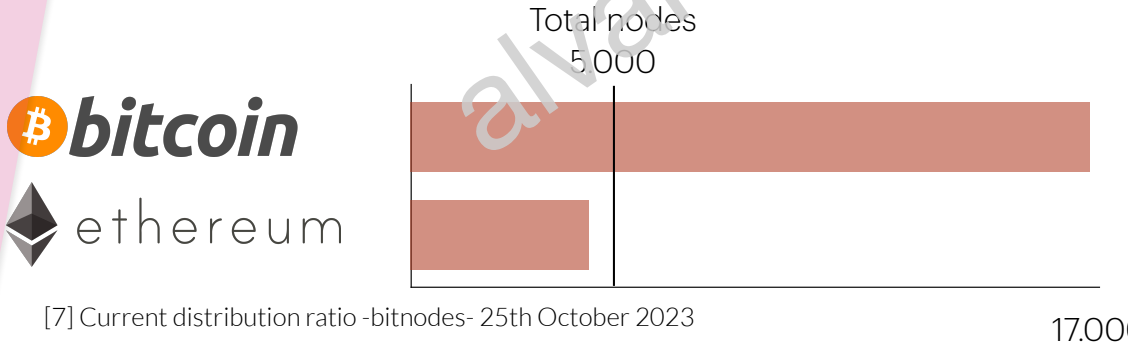
Decentralization might be an illusion even for the latest solutions · Visiting empirical insights on P2P Networks · Attacks

Great cohesion on P2P networks

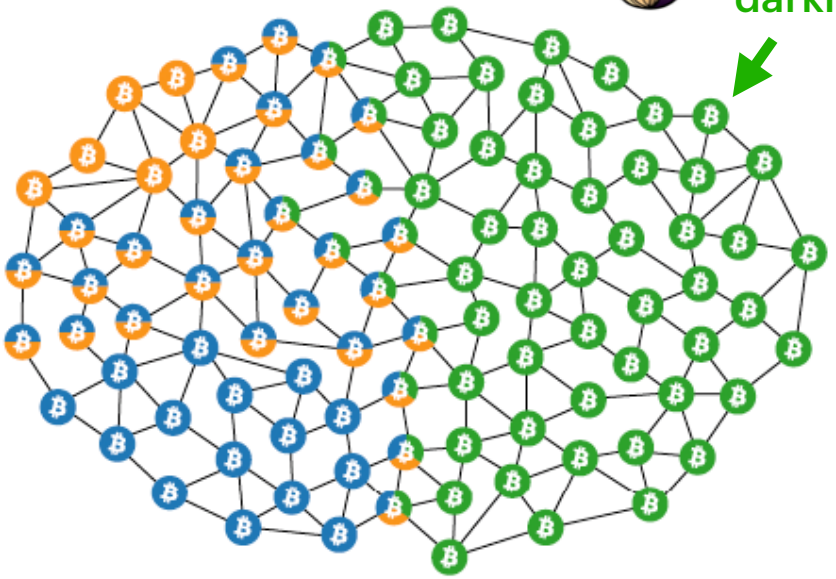
- Good network cohesion
  - 15% **IPv4**, 6% **IPv6**
  - 17% **IPv4**+**IPv6**
  - 50% **Onion**
  - 12% **IPv4**+**IPv6**+**Onion**
- Half the network in darknet



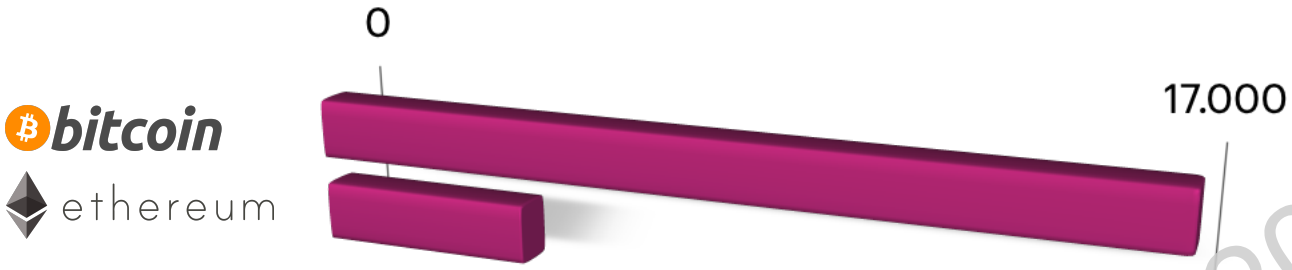
[7]
IPv4: -3.6% / IPv6: -1.6% / .onion: +3.1%



[7] Current distribution ratio -bitnodes- 25th October 2023



Bitcoin *network distribution* ***ipv4, ipv6,*** *and* ***Tor*** *cohesion*



BITNODES

Bitnodes estimates the relative size of the Bitcoin peer-to-peer network by finding all of its reachable nodes.

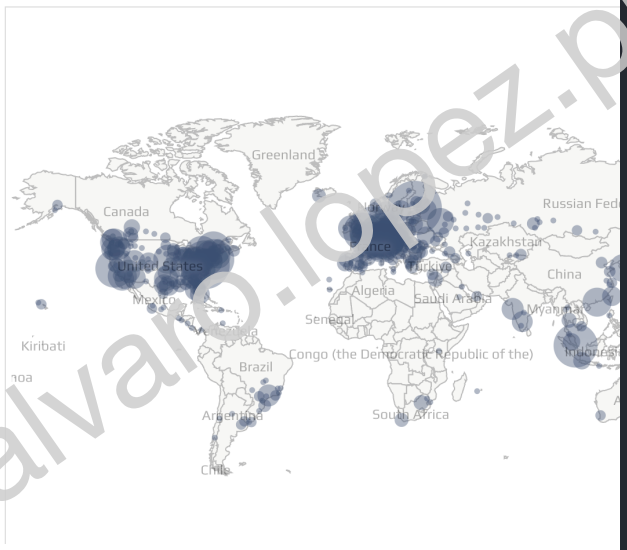
REACHABLE BITCOIN NODES

17049 NODES CHARTS

IPv4: +0.3% / IPv6: +2.1% / .onion: +4.0%

Top 10 countries with their respective number of reachable nodes are as follows.

RANK	COUNTRY	NODES
1	n/a	10839 (63.58%)
2	United States	1570 (9.21%)
3	Germany	1309 (7.68%)
4	France	441 (2.59%)



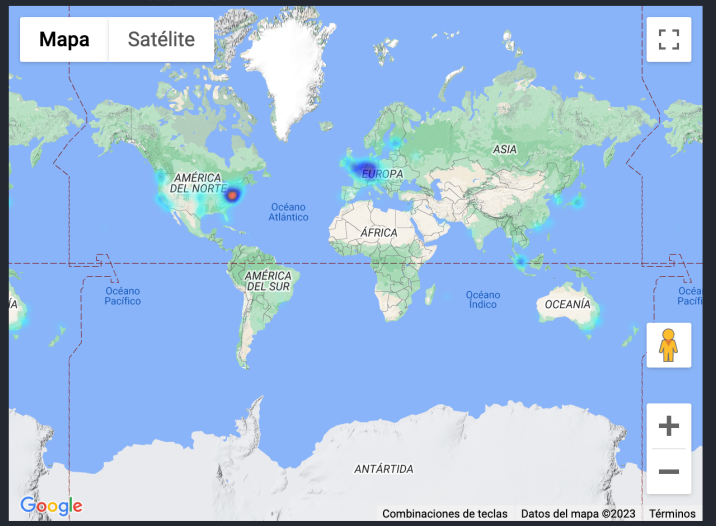
ethernodes.org Home Browse The Merge Search node by IP or pu

Ethereum Mainnet Statistics

Clients Countries Sync Status OS Network Types History

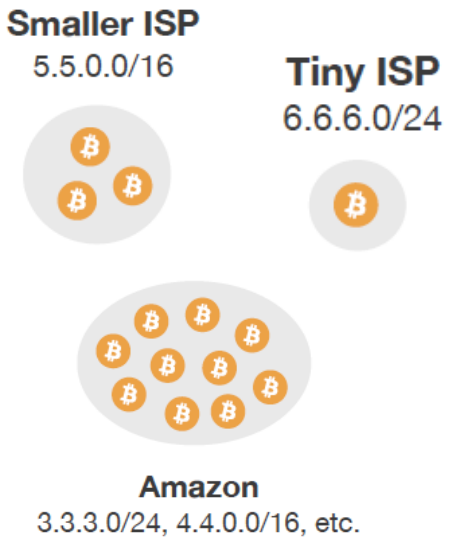
COUNTRIES

Total	3992 (100%)
United States	1591 (39.85%)
Germany	508 (12.73%)
United Kingdom	188 (4.71%)
France	148 (3.71%)
Netherlands	135 (3.38%)
Canada	131 (3.28%)
Singapore	123 (3.08%)
Australia	122 (3.06%)
Finland	93 (2.33%)

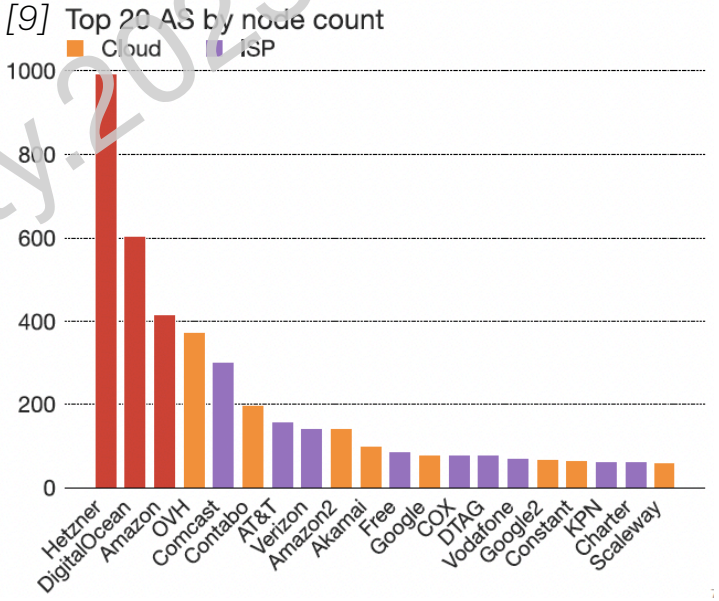


[8] Bitcoin nodes bitnodes.io | Ethereum nodes ethernodes.org

Are P2P networks **under the control** of AS, ISP and Cloud providers?



Ahaam!!, **decentralization** might be an illusion?



- AS, ISP and Cloud control: *AmazonWS, Azure, Google Cloud* (25% of BTC nodes)
  - ⬇ Centralization risk

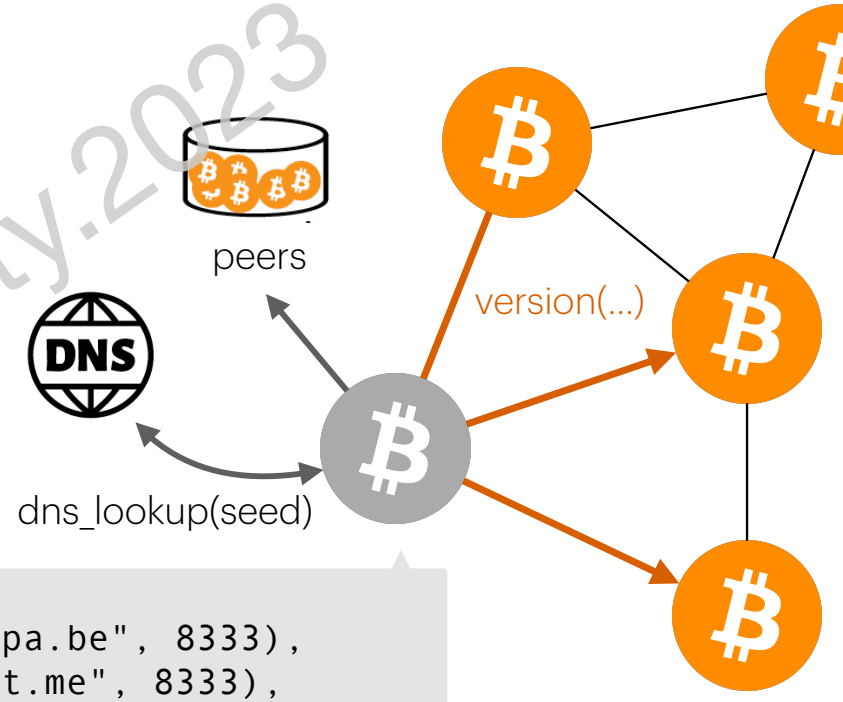
AS+ISP focus of attack targeting?

- More than 50% of AS contain only one single node, contributing a total of 7,6% nodes
- Top 1% AS contribute with more than 50% of the nodes
- Three providers host 25% of nodes

[9] *Bitcoin P2P Network Insights @ Advanced BitCoin Conference 2023 (https://t.co/BgjNWzk9Rb) source:* ⭐⭐⭐⭐ *Virtu*

P2P Network **onboarding with discovery** brings security risk

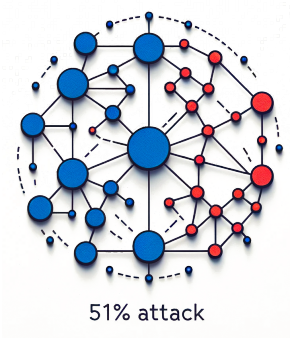
- DNS seeds (default way to bootstrap nodes)
  - DNS lookup: availability on advertised nodes + tcp sock
  - Bitcoin
- DHT (distributed hash tables)
  - Ethereum

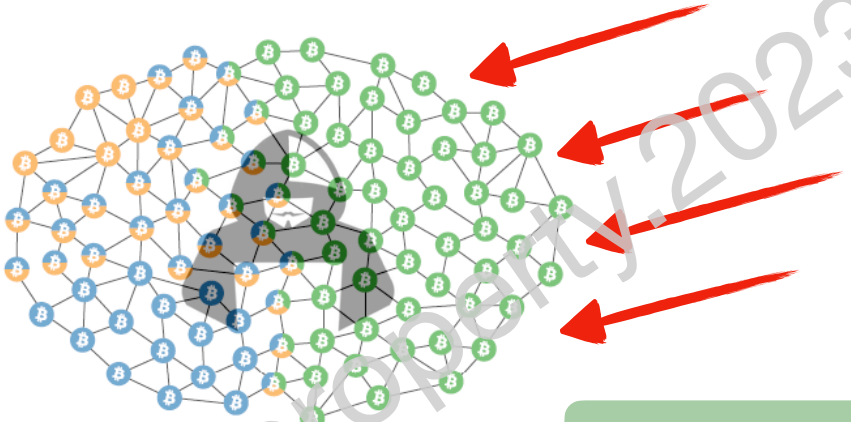



```
("seed.bitcoin.sipa.be", 8333),
("dnsseed.bluematt.me", 8333),
("dnsseed.bitcoin.dashjr.org", 8333)
. . .
```


[10] Bitcoin Seeds https://github.com/bitcoin/bitcoin/blob/1b2460bd5824170ab85757e35f81197199cce9d6/src/chainparams.cpp#L112
[11] Bitcoin Protocol https://developer.bitcoin.org/reference/
[12] Bitcoin Message Structure https://en.bitcoin.it/wiki/Protocol_documentation#Message_structure

Attacks motivation on nodes distribution





Take the control

Denegation

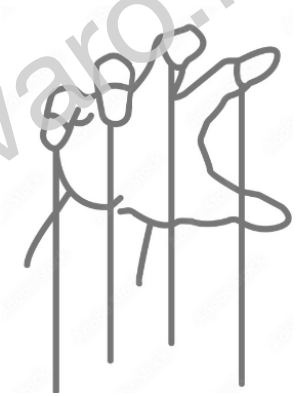
- Centralization risk
- Sybil and eclipse attacks

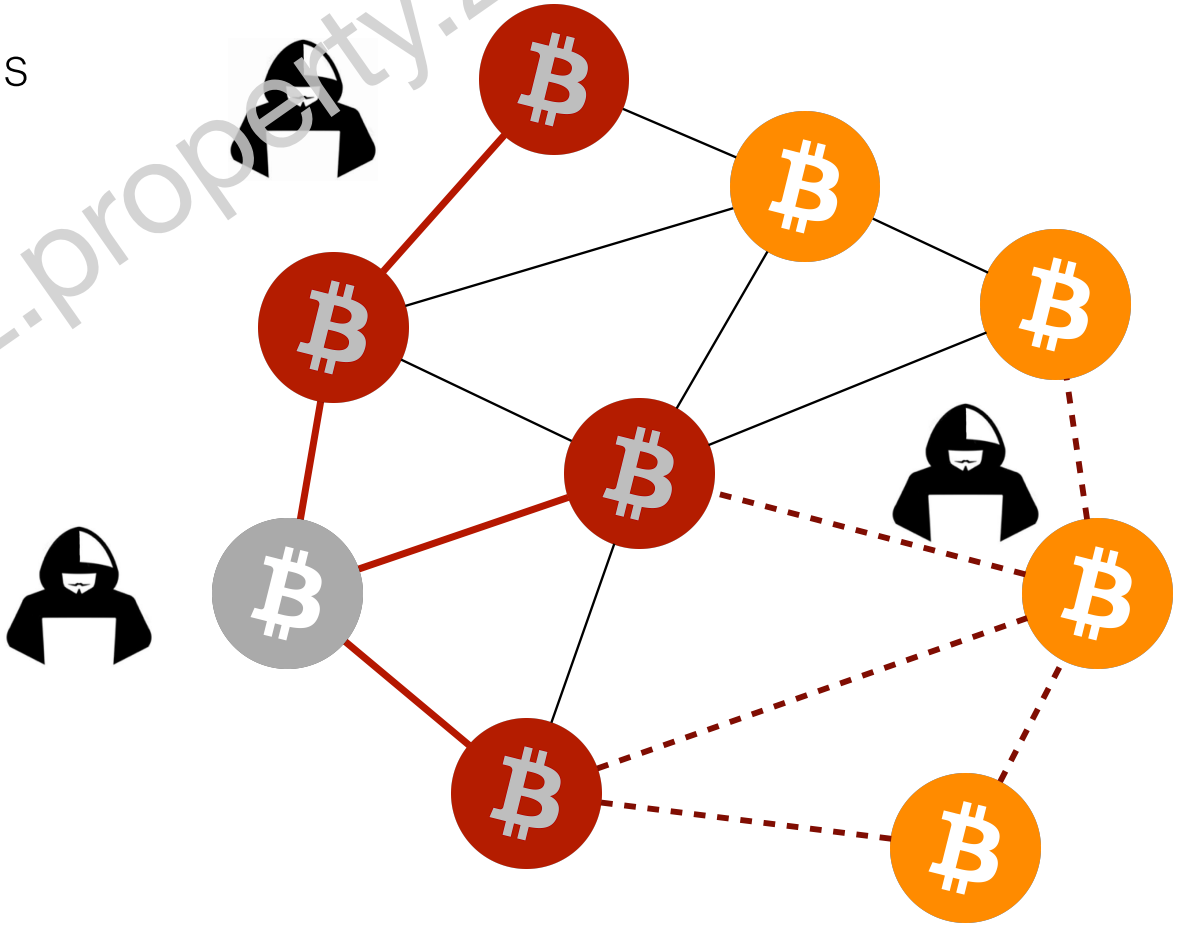
- DDoS
- Exploit vulnerabilities

Take the control

- 51% attacks —> take over consensus
- Sybil attacks —> fake nodes
- Eclipse attacks —> node isolation

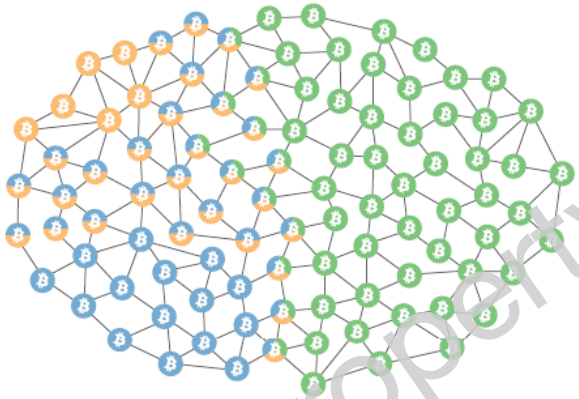
- Centralization risk—> control centralization





Scalability | **Security** | Decentralization

To ***prevent a disaster***, let's work together and take action now!



Take the control

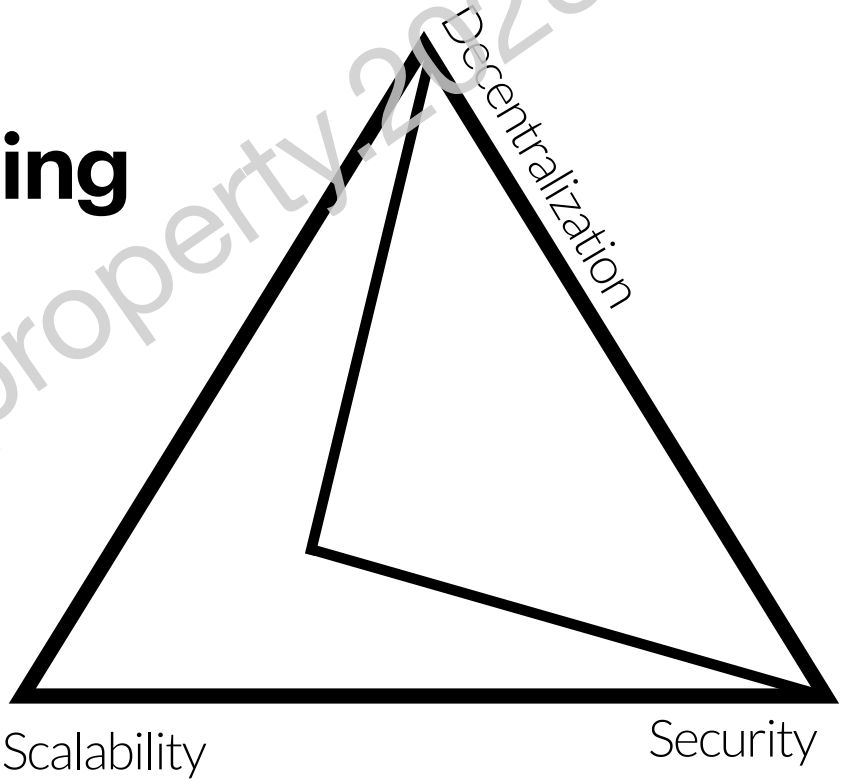
Denegation

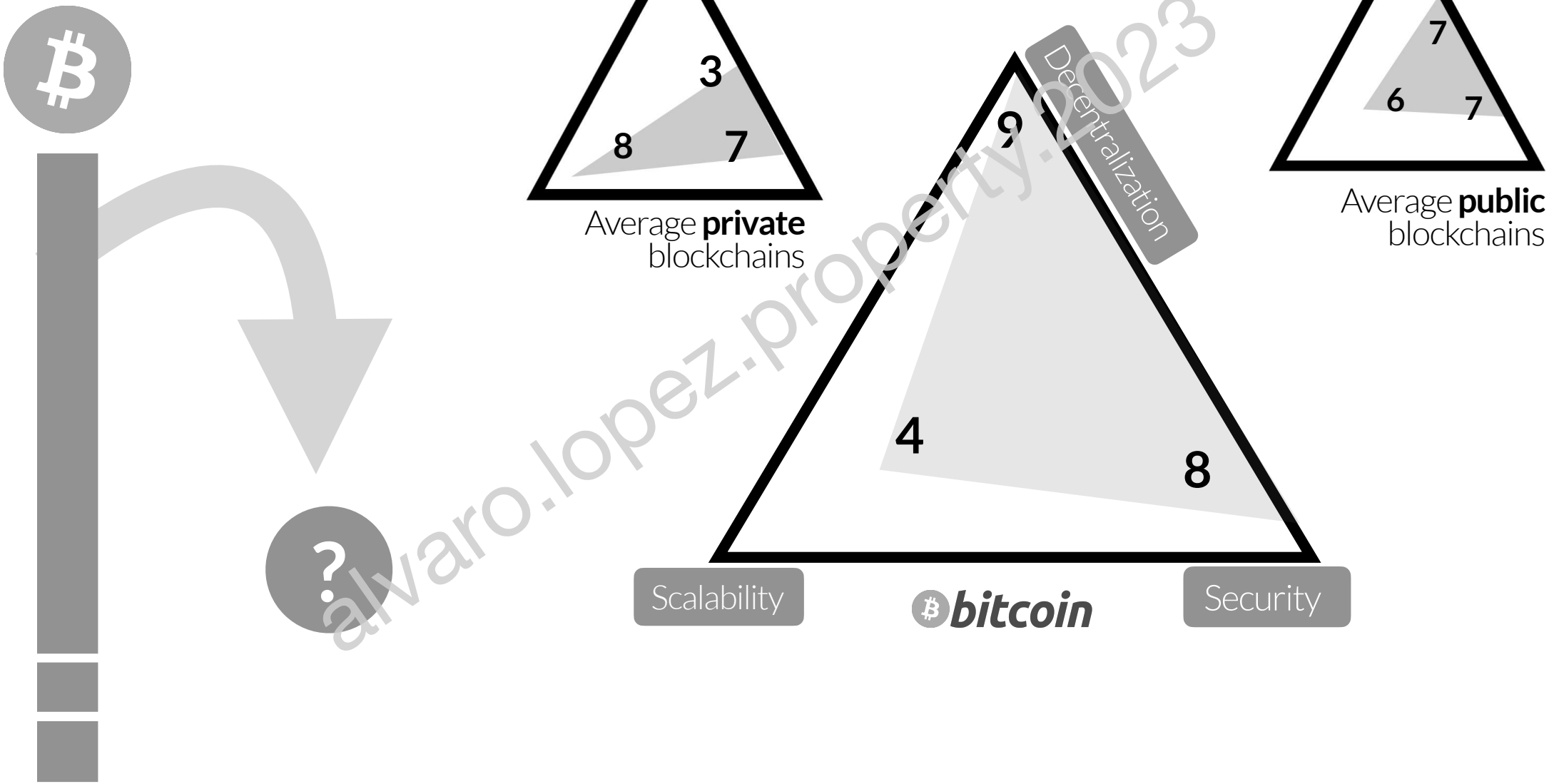
- Transparency and audit companies
- Staking strategies
- Infrastructure diversification

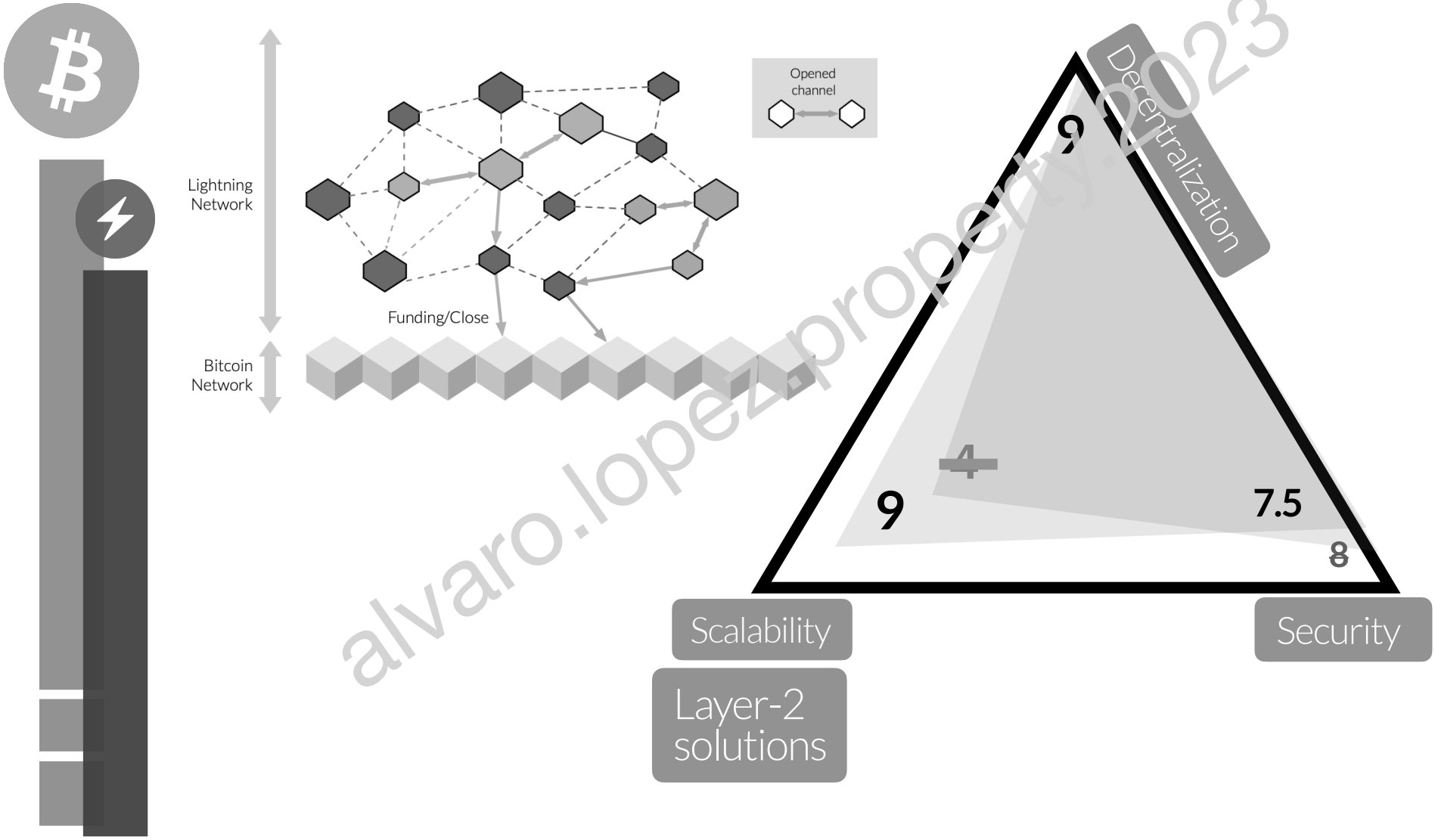
- Upgraded software
- White/Blacklisting
- Peer verification (handshake)
- Redundancy

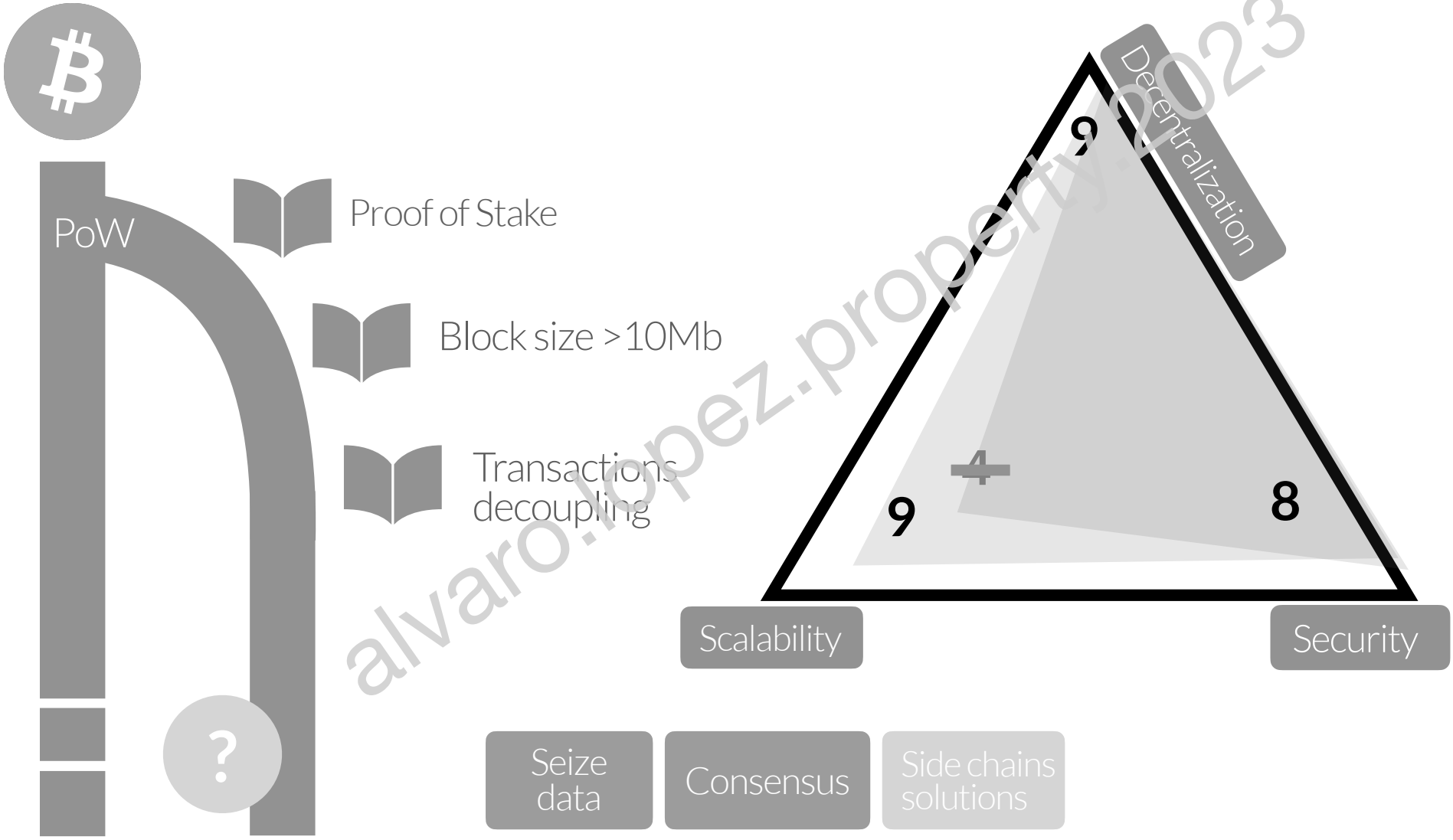
6of6

Putting everything Into practice









Resources

Bitcoin Development

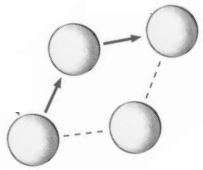
- Mastering The Bitcoin, *Andrea M. Antonopoulos* https://github.com/bitcoinbook/bitcoinbook
- Lunaticoin Podcasts https://lunaticoin.com/
- Estudio Bitcoin - Spanish community to get start and dive in Bitcoin https://estudiobitcoin.com/

The Lightning Network

- Mastering the Lightning Network, *Antonopoulos, Osuntokun, Pickhardt,* https://github.com/lnbook/lnbook
- How the Lightning Network works by Lightning Labs, https://docs.lightning.engineering/the-lightning-network/overview
- Setup a local Lightning Network cluster with Polar https://docs.lightning.engineering/lapps/guides/polar-lapps/local-cluster-setup-with-polar

Ethereum (roadmap)

- Vision https://ethereum.org/en/roadmap/vision/
- The path to The Merge (protocol 2021) https://trent.mirror.xyz/82eyq_NXZzzqFmCNXiKJgSdayf6omCW7BgDQIneyPoA
- What is dancharking (roadmap 2022) https://members.delphidigital.io/reports/the-hitchhikers-guide-to-ethereum



P2P Networks Insights

- Empirical insights into BTC P2P network (virtu) @ Advancing Bitcoin Conference 2023, London UK https://t.co/BgjNWzk9Rb
- Bitcoin P2P Networks https://developer.bitcoin.org/devguide/p2p_network.html
- Ethereum P2P Networks (Networking Layer) https://ethereum.org/en/developers/docs/networking-layer/

researchers & companies

Fortris

Digital assets treasury operations and **custody** management

NuCypher

Cryptographic infra for privacy preserving applications

decentralized SECURITY

Cybersecurity researching on Blockchain Ecosystems

OAK

Security **auditing** on decentralized-technologies

Enroll in Blockchain path

Blockchain Technologies

University Extension Course

NICS Lab research group of the University of Malaga

NICS LAB

UNIVERSIDAD DE MÁLAGA

blockchain@nics.uma.es

- Aertec, the UMA and Telefónica Tech develop a software project based on blockchain technology applied to the aeronautical industry (April 2022) https://www.aeropolis.es/boletin/en/aertec-the-uma-and-telefonica-tech-develop-a-software-project-based-on-blockchain-technology-applied-to-the-aeronautical-industry/

- "Advanced Custody Wallet with Miniscript and Timelocks" *Álvaro López, Antonio Tóvar, Diego García, Juan Carlos Delgado, Miguel Ángel Fortes* (9th November 2023) XVI JITEL Telematic Engineering Conferences. (https://web.salleurl.edu/docsmkt/agenda-jitel-2023.pdf)

Cybersecurity challenges Let's **Team up!** 💪

- R&D Engineering Fortris
- Videogames & API Security+Scalability
- PhD Research (University of Málaga)
  "Decentralized security architectures and self-sovereign identities"

DALL·E

linktr.ee/bluebycode