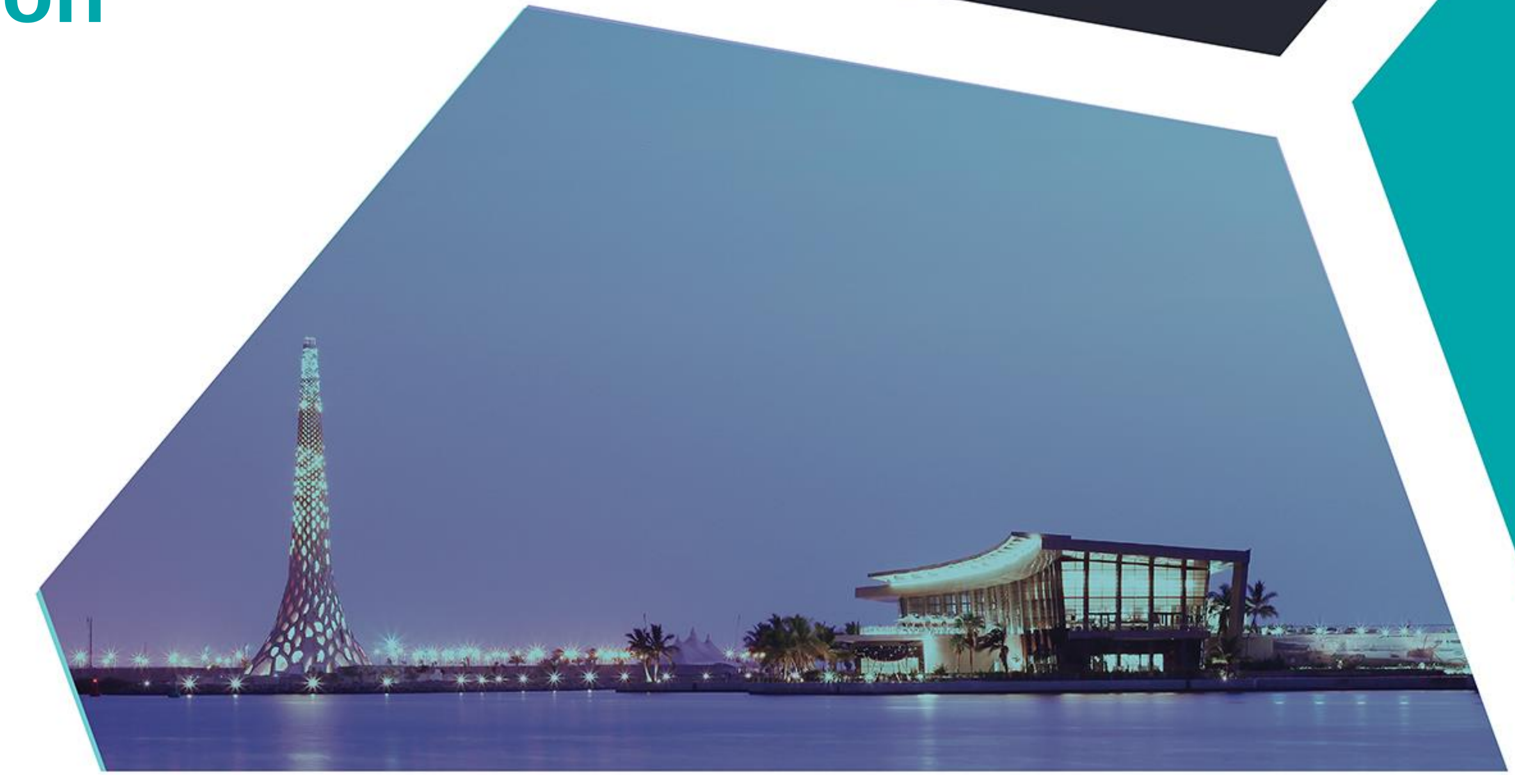
The Convergence of Fintech and Cybersecurity: Regulation, Security and Innovation

CONSOB, Rome

14 Nov. 2024

Dr. Roberto Di Pietro

Full Professor in Cybersecurity
IEEE Fellow, ACM DM, MAE
Jean-Claude Laprie Award recipient



Roberto Di Pietro, IEEE Fellow, ACM DS, MAE

Vision: To achieve excellence in cybersecurity research addressing both fundamental and applied challenges in the field, as well as to have impact and to generate innovation.

Currently

- Full Professor in Cybersecurity @KAUST-CEMSE, Saudi Arabia
- PI of the Cybersecurity Research and Innovation Lab @ KAUST (https://cri-lab.net)

Past

- Professor in Cybersecurity at HBKU-CSE, Doha, Qatar
- Global Head Cybersecurity Research @ NOKIA Bell Lab (3 Depts, 50+ HR)
- Professor at University of Padua
- Seconded National Expert at EUROJUST (DPO)
- United Nations Agencies consultant (cybersecurity)
- ICT Officer - Ministry of Defense (10+ years)

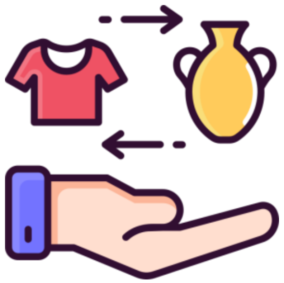
Main Research Domain: **Distributed Systems Security**

Outline

- Introduction
- Cryptocurrencies Genesis
  - *E-Cash*
- Incumbent Security issues
  - *Bitcoin*
  - *Ethereum*
- Cryptocurrencies Latest Evolution
  - *Layering*
- Security & Privacy Case Study: Polkadot
- RWA & Stablecoins
- Conclusion

Non è possibile visualizzare l'immagine.

The Evolution of Currency



Barter System

First type of exchange
(appeared with humas, still in use)

Metal Coins

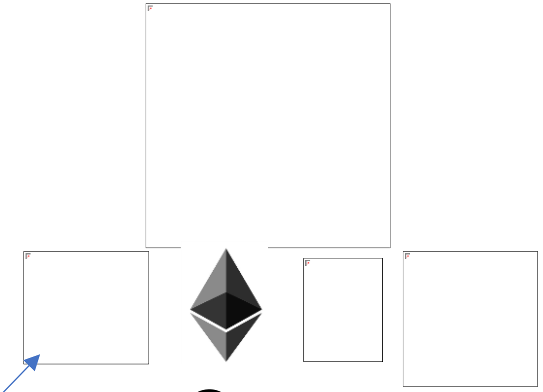
King Alyattes of Lydia
(~550 BCE)

Paper

Tang dynasty China
(7th century)

Electronic

50's, the Diners Club card



Crypto

Satoshi Nakamoto (?)
2008

A global Financial Revolution is Taking Place…

What is a Cryptocurrency

What is money?

- Store of value
- Medium of exchange
- Unit of account

Cryptocurrency:

A Cryptocurrency is a **digital asset** designed to work as a medium of exchange using cryptography to secure user transactions and control the minting (creation of additional unit of the currency)

Fiat Currencies

- Regulated (legal course)
- Widely accepted
- Stable (+/-)

🙂 ✓

- Slow Transactions
- Inflation
- Subject to Government Control

🙁 ✗

Cryptocurrencies

- Fast Transactions
- Worldwide Transactions
- Pseudo-anonymity
- No Third-parties

🙂 ✓

- Volatile
- Unregulated
- Not Universally Accepted

🙁 ✗

History of Cryptocurrencies

1983

Ecash (David Chaum)

Anonymous cryptographic electronic money

2008

Bitcoin (Satoshi Nakamoto)

First decentralized cryptocurrency

2015

Ethereum (Vitalik Buterin)

Smart contracts, decentralized apps

2020

Polkadot (Web3 Foundation)

First platform supporting parachains

2023

Facing the Future…

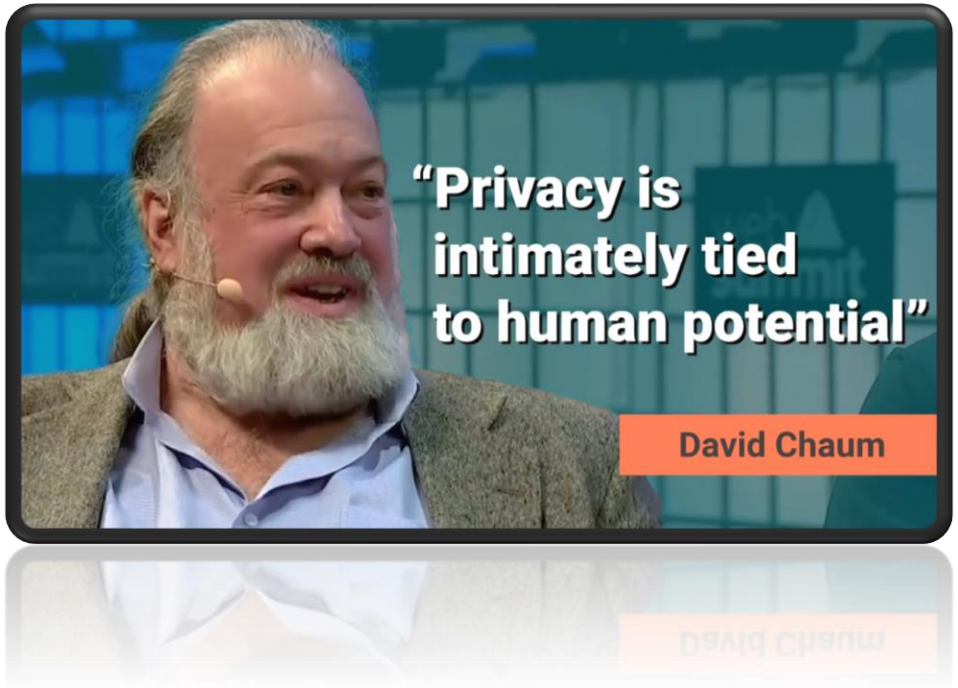
E-Cash (1983)

- First privacy preserving payment method
- Based on **“Blind Signatures”**
- Involves a “Bank”, merchants and users
- Users must have accounts in the Bank, with FIAT currencies
- Users can withdraw e-cash from the Bank and spend it later with any merchant; merchant can cash (deposit) the spent amount at the Bank
- No double-spending

Though…

- DigiCash files for **bankruptcy** in late 1998

Chaum, D., 1983.
Blind signatures for untraceable payments.
In Advances in Cryptology: Proceedings of Crypto 82 Springer US.

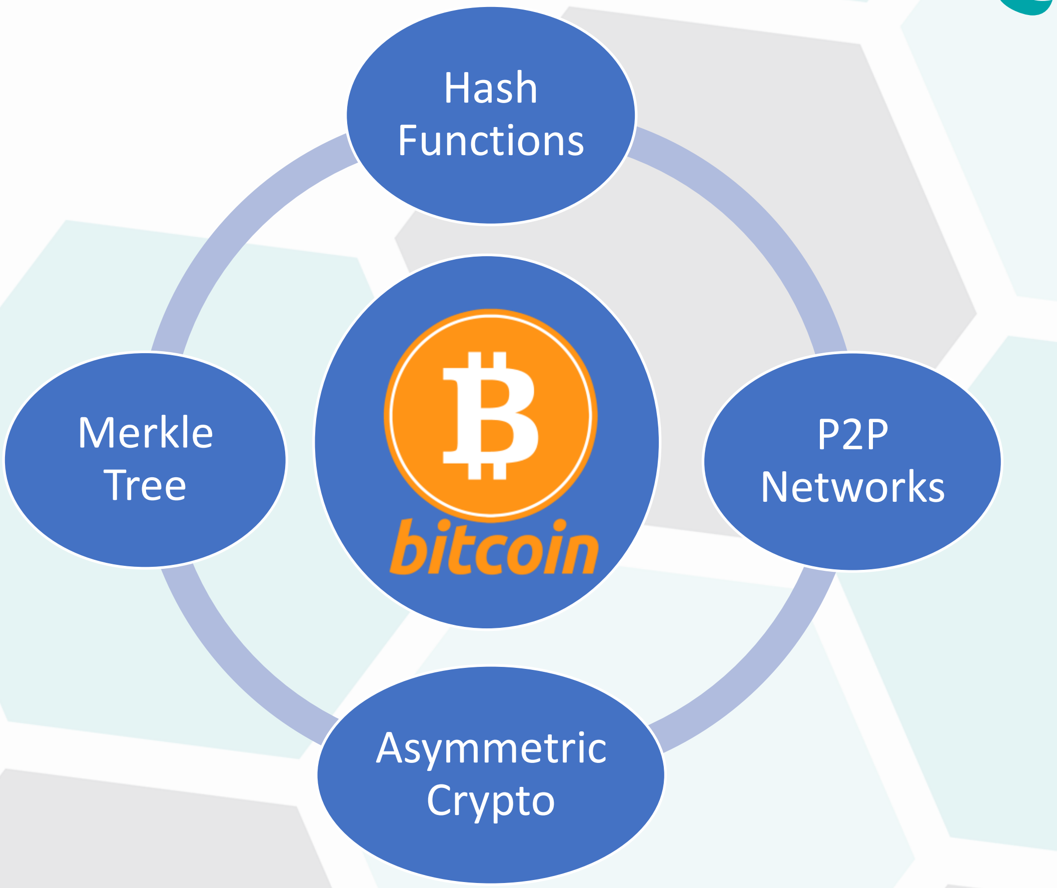


Bitcoin (2008)

First platform to implement:

- Completely digital money
- Public ledger
- Decentralized ledger
- Immutable ledger
- No central authority

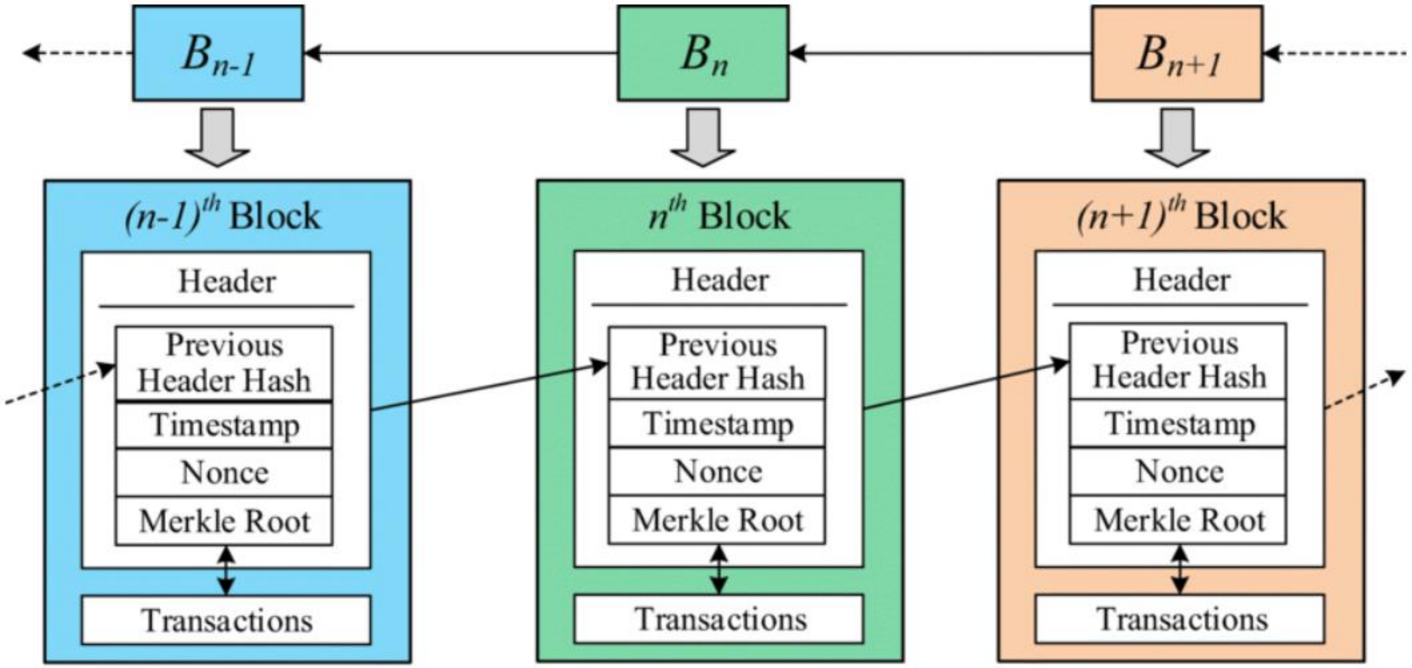
Nakamoto, S., 2008.
Bitcoin: A peer-to-peer electronic cash system.
Decentralized business review.



Enabling Technologies
(none of them new –wrt BTC)

Bitcoin Architecture

- The consensus is based on Proof of Work (PoW)
- A copy of the ledger is maintained in every full-node
- A new block is created every 10 minutes (on average)



Bitcoin Security Issues

- **Privacy**: Bitcoin isn’t anonymous! (provides just pseudo-anonymity)
  - *User De-anonymization: The attacker tries to link a public key to a physical person. Usually performed with off-chain data*
  - *Address Clustering: Correlate multiple public keys to the same entity*

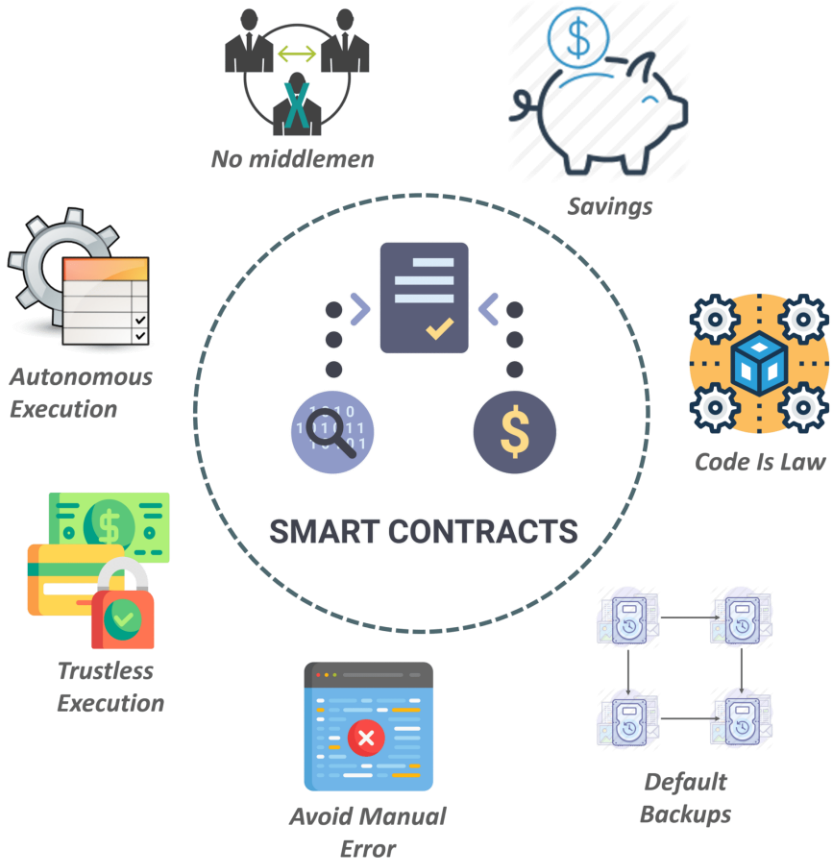
- **Protocol hacks**:
  - *Double-spending: malicious users attempting to deceive the system by spending the same BTC more than once (How: Forking…).*
  - *51% attacks: The attacker controls more than half of the total computational power of the system.*

- **Network attacks**: P2P networks are vulnerable!
  - *Eclipse attack: By monopolizing the connections of a victim node, the attacker can control the blockchain view of this node.*
  - *Routing attack: intercept the network transmitted messages and tamper with them (BGP hijacks, partitioning attack, delay attack)*

Ethereum (2015)

Ethereum: a platform to build powerful decentralized applications (DApps).

- Consensus based on **Proof of Stake** (PoS)
- A new block every **15 seconds** (on average)
- **Infinite** supply (inflationary…)
- Turing completeness
- **Smart Contracts** support (**Solidity**)
- Decentralized Apps (**DApps**) support
- Improved **Scalability**



Ethereum Security Issues

Smart Contract Security:

- *<u>Reentrancy Attacks</u>: recursive calls in a malicious contract that drain the balance of the honest contract that invokes it.*
- *<u>Frontrunning</u>: Takes advantage of network latency and useful information from TXs in the MemPool to gain profit (transaction re-ordering)*
- *<u>Integer Overflow and Underflow</u>: common attack in many programming languages. From version 0.8, the Solidity compiler automatically checks for overflows and underflows.*

H. Chen, M. Pendleton, L. Njilla, and S. Xu.
A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses.
ACM Comput. Surv. 53, 3, Article 67 (May 2021)

What else?

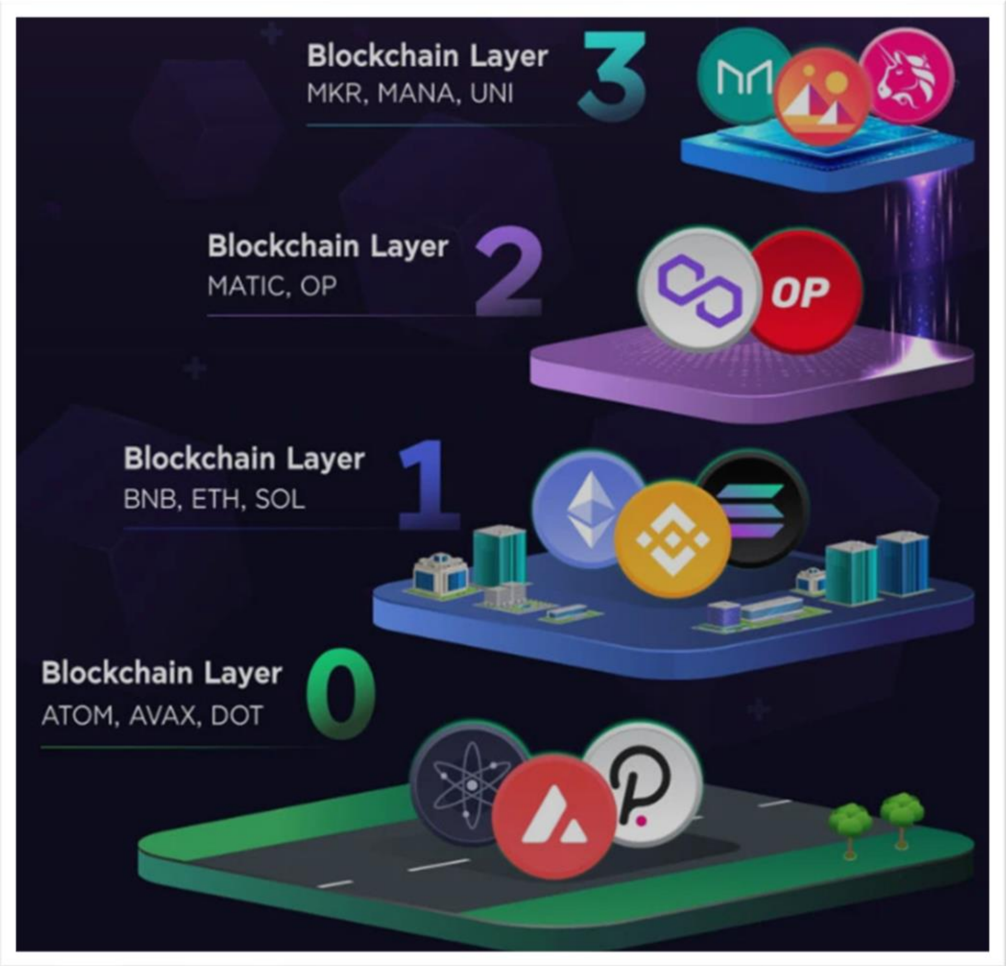
Dozens of other major exploits!

“It takes a week to learn Solidity, and three years to avoid writing critical vulnerabilities on a regular basis”

Recent Evolution of Cryptocurrencies

Multi-layer model

- Level 3: hosts decentralized applications (DApps) and user-facing applications
- Level 2: offers better scaling capabilities and third-party integration.
- Level 1: also called “implementation layer”, maintains dispute resolution, consensus mechanisms, and blockchain programming.
- Level 0: provides the underlying infrastructure for blockchain, including foundational elements like hardware, network protocols, and cross-chain interoperability communication.



The DeFi Landscape: New Services, old Problems

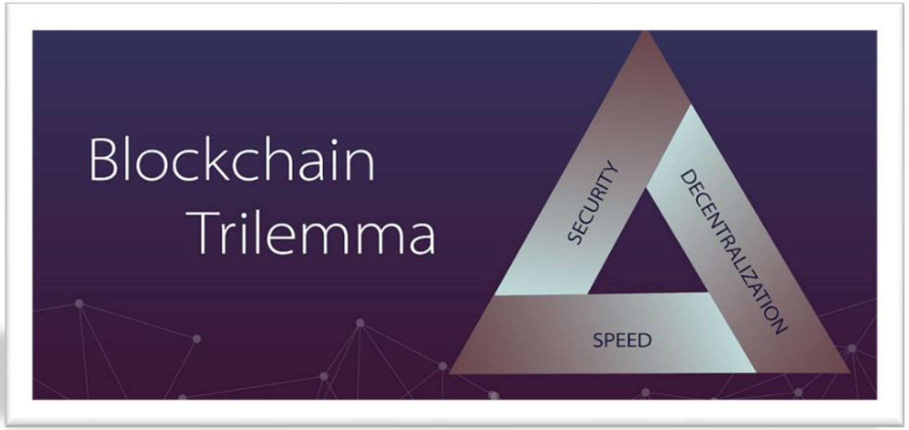
New Platforms covering Several Use Cases

- Decentralized Exchanges (DEXs)
- Tokenization of Assets
- Asset management
- Bridge protocols
- Stablecoins
- Marketplaces
- Insurance
- Payments
- Credit

The Blockchain Trilemma

Usually, blockchains lose security when scalability is enhanced, and lose speed when decentralization is higher.

Different consensus algorithms prioritize each of the three directions, but no existing method optimizes all of them.



New DeFi applications: Challenges and Threats

DeFi Security Challenges

- **Centralization**: DeFi is still reliant on some centralized components, such as price feeds and liquidity pools.
- **Oracle APIs**: manipulation of information received from external sources might result in system failure and theft.
- **Protocol Interactions**: interoperability of DeFi protocols offers enhanced functionality, but also expose a web of intricate dependencies.
- **Governance**: The weight of a vote is proportionate to the number of governance tokens that the voter holds.

DeFi Biggest Threats

- **Asset Custody**: Both online wallet and other custodial services have proven to be highly susceptible to hacks.
- **Cross-Chain Security**: Bridges are an attractive target because they often feature a central storage point of funds that back the “bridged” assets on the receiving blockchain.
- **Governance**: the skyrocketing Total Value Locked (TVL) of DeFi protocols makes governance attacks highly profitable

Bridge Attacks: real-world Examples

Ronin Network - March 22

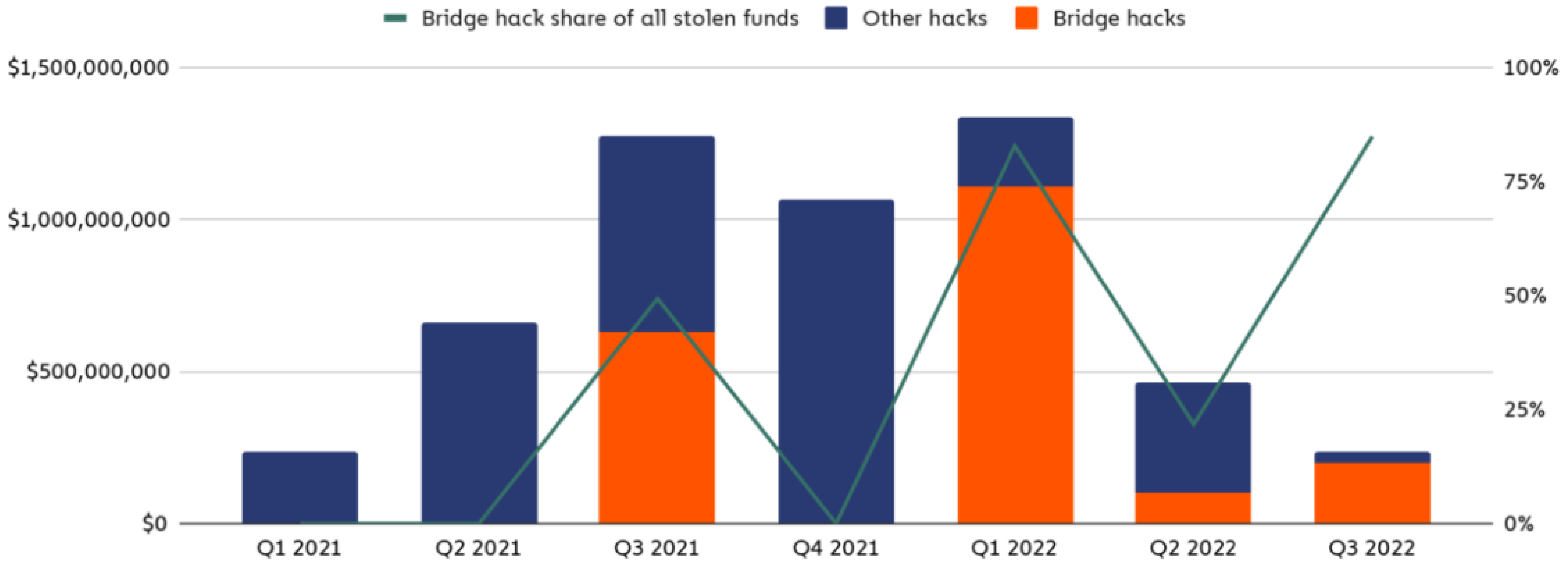
Hacked private keys… fraudulent withdrawals from the Ronin bridge contract

Result: $620 Million loss

BSC Bridge - Feb 22

A vulnerability of the protocol allows attacker to mint 120K wETH with no corresponding ETH backing on Ethereum.

Result: $568 Million loss



Public Ledger: A Trove of Data

- As of March 2023, there are 8,832 active cryptocurrencies currently available in the market
- Lack of peer-reviewed research paper to describe their architecture and assess their security
- Academic research mainly focuses on Bitcoin and Ethereum only…

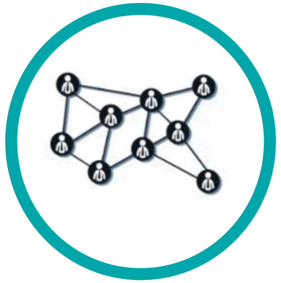
Public Ledger Analysis

- Public ledgers offer an incredible opportunity for the research community.
- Graph analysis widely used to assess Bitcoin and Ethereum security and privacy (2 out of 8,832)

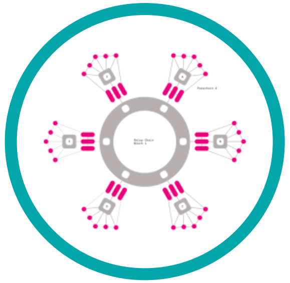
What about the other 8,830?

Let’s start with **Polkadot!**

Polkadot



Novel Protocols
lay foundation for a truly decentralized Web.



Sharded Multichain transfer of arbitrary data across heterogenous blockchains.

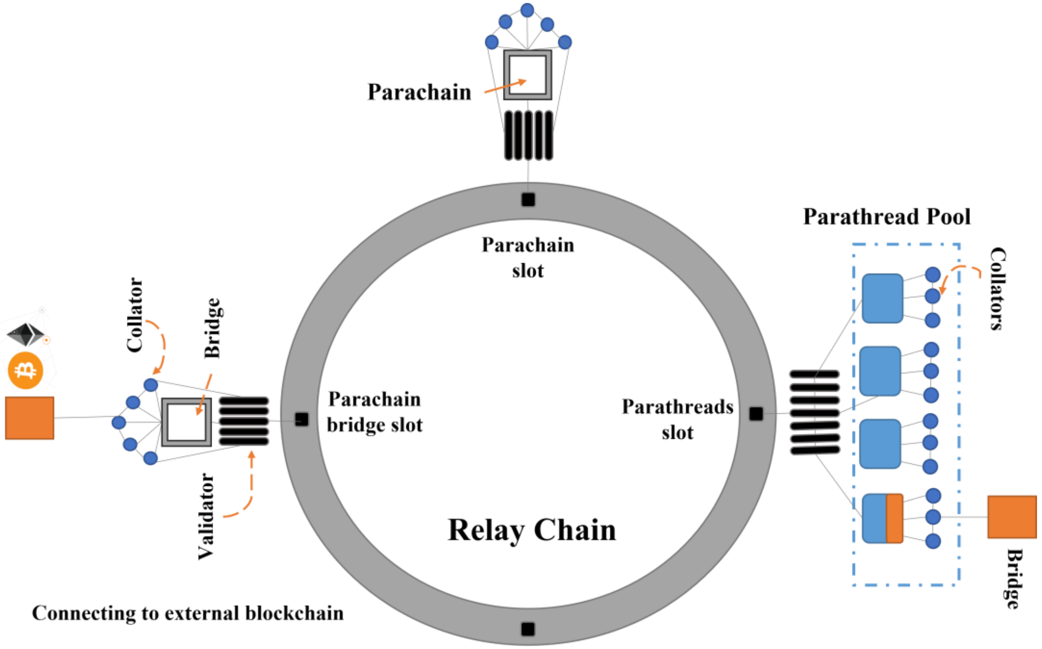
Promising features & use-cases: scalability, interoperability, shared security.

Polkadot Architecture

Nodes & Roles:

- A Validators
- B Collators
- C Nominators

- A Maintainers of Relay Chain
- B Maintainers of Parachains
- C Participants of **Nominated Proof of Stake** (NPoS) consensus



Structures:

1. Relay Chain
2. Parachain
3. Bridge
4. Parathread

1. **Pooled security**
2. Customizable logic and uses
3. Interoperate with external chains
4. Parathread pool

Polkadot Research Opportunities

Several research directions:

- Architectural analysis: Polkadot is discussed in the grey-literature only
- Graph Analysis: Transaction system modeling using graph analysis
- Privacy: What is the privacy level of the network?

Polkadot – Architecture and Contradictions

Motivations: Novelty of multi-chains. Need to investigate their design and processes

Contributions: First systematic study about Polkadot, involving architecture analysis and protocol limitations

Abbas, H., Caprolu, M. and Di Pietro, R., 2022, **Analysis of Polkadot: Architecture, internals, and contradictions.** In 2022 IEEE International Conference on Blockchain (Blockchain) (pp. 61-70). IEEE.

Results:

***Validators*:**

- Active set is limited (currently 297)
- Competition forces a high minimum stake requirement (Around 1.8 million DOT, $32.4 million, in April 2022)

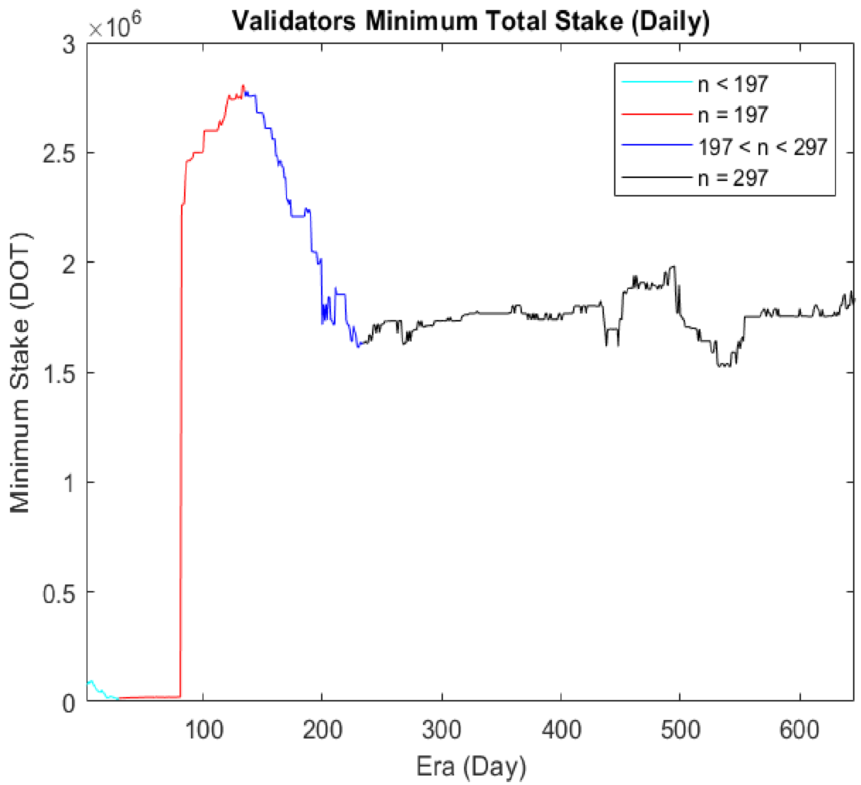
***Nominators*:**

- Active set is limited
- Suspicious commissions
- Nominators suffer major slashing with minimal self-stake validators

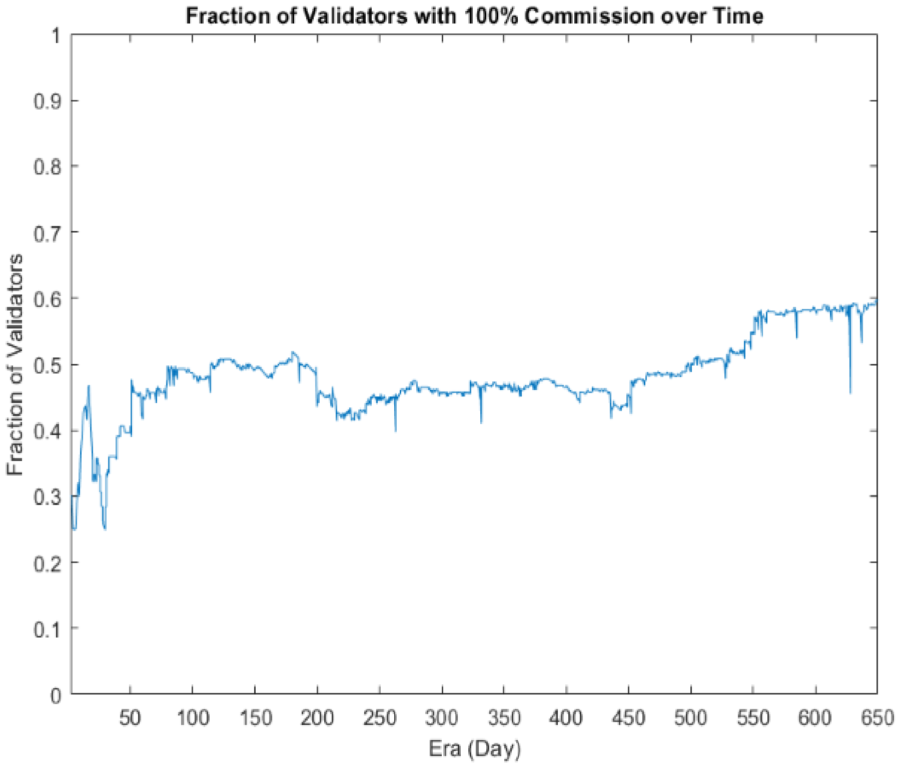
***Governance*:**

- Heavy concentration of power
- Council is restricted to 13 members
- Competition forces a high minimum stake requirement (Around 9.5 million DOT, $171 million, as of April 2022)

Polkadot – Architecture and Contradictions



- The minimum validator stake varies with the number of active validators (> 1.8 M Dot ~ 7M USD !)

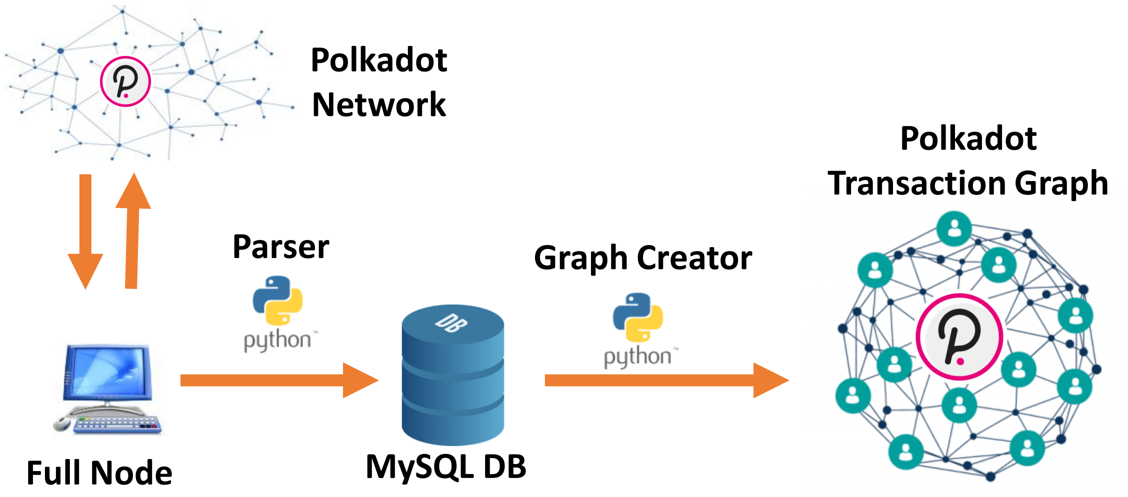


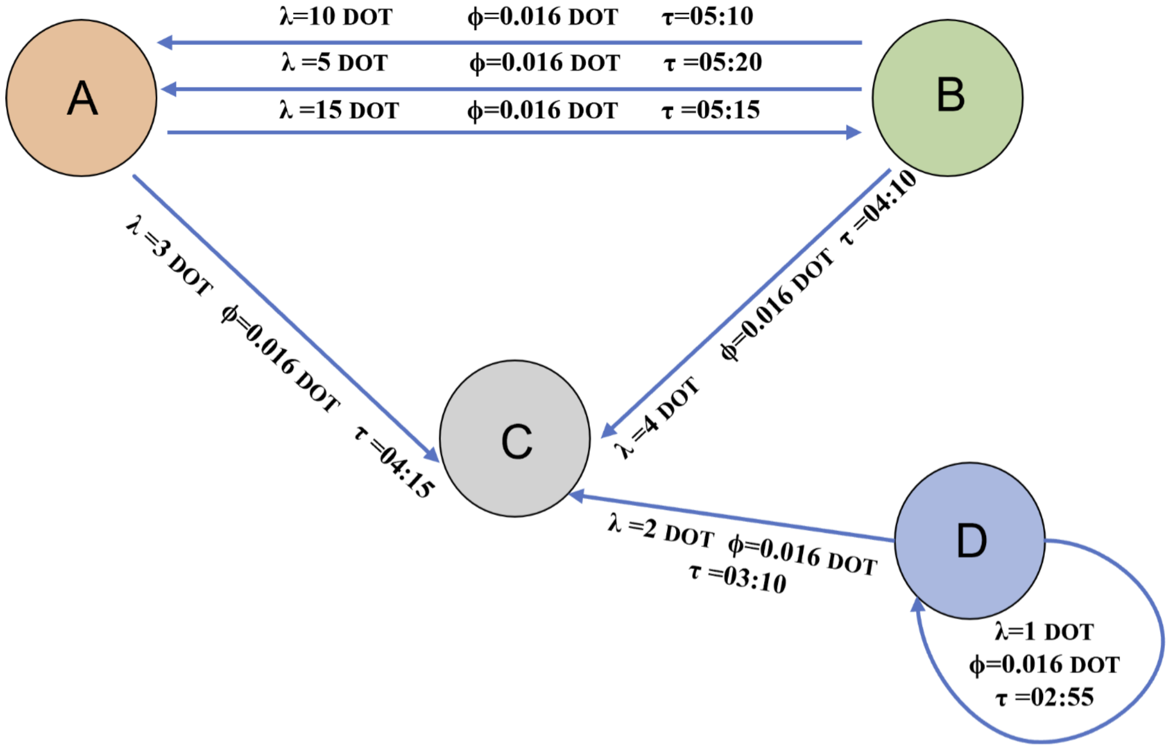
- Increasing over time, currently exceeding 60%
(why nominators do nominee such greedy supporters?)
- Typically, such validators provide the minimal self-stake (such as 1 DOT only) and are also backed by a few nominator accounts.

Polkadot – Transaction Graph Analysis

Motivations: Leverage graph theory to analyze the Polkadot environment and measure its network

Methodology: Starting from a Polkadot full node, build TX graph using on-chain data and analyze it

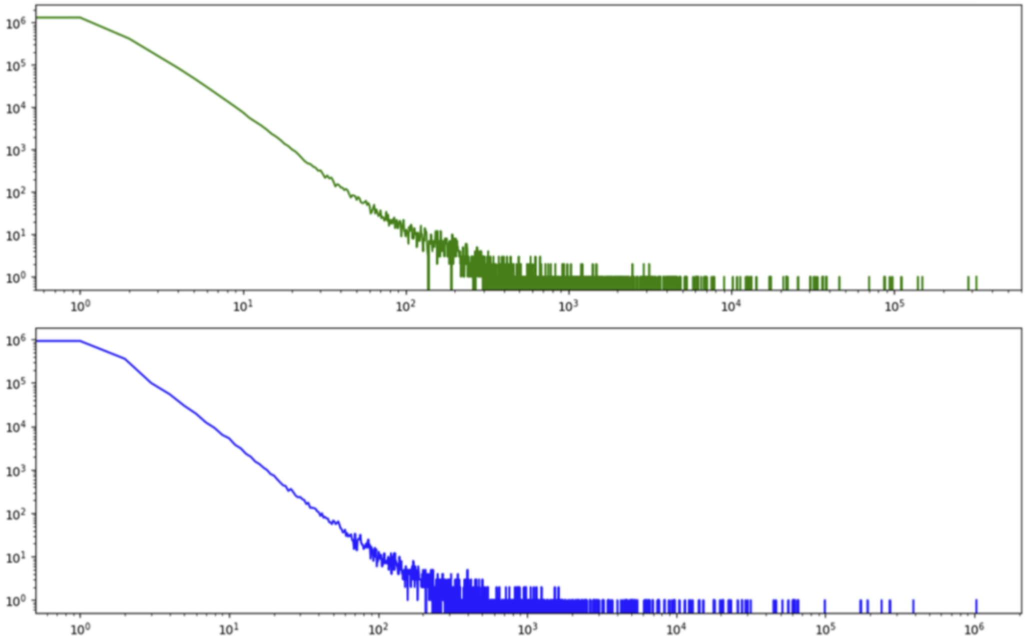




A
B
C
D
λ=10 DOT ϕ=0.016 DOT τ=05:10
λ =5 DOT ϕ=0.016 DOT τ =05:20
λ =15 DOT ϕ=0.016 DOT τ =05:15
λ =3 DOT ϕ=0.016 DOT τ =04:15
λ =4 DOT ϕ=0.016 DOT τ =04:10
λ =2 DOT ϕ=0.016 DOT τ =03:10
λ=1 DOT ϕ=0.016 DOT τ =02:55

Abbas, H., Caprolu, M. and Di Pietro, R., 2023
Understanding Polkadot Through Graph Analysis: Transaction Model, Network Properties, and Insights.
International Conference on Financial Cryptography and Data Security (FC) 2023

Polkadot – Transaction Graph Analysis - Results

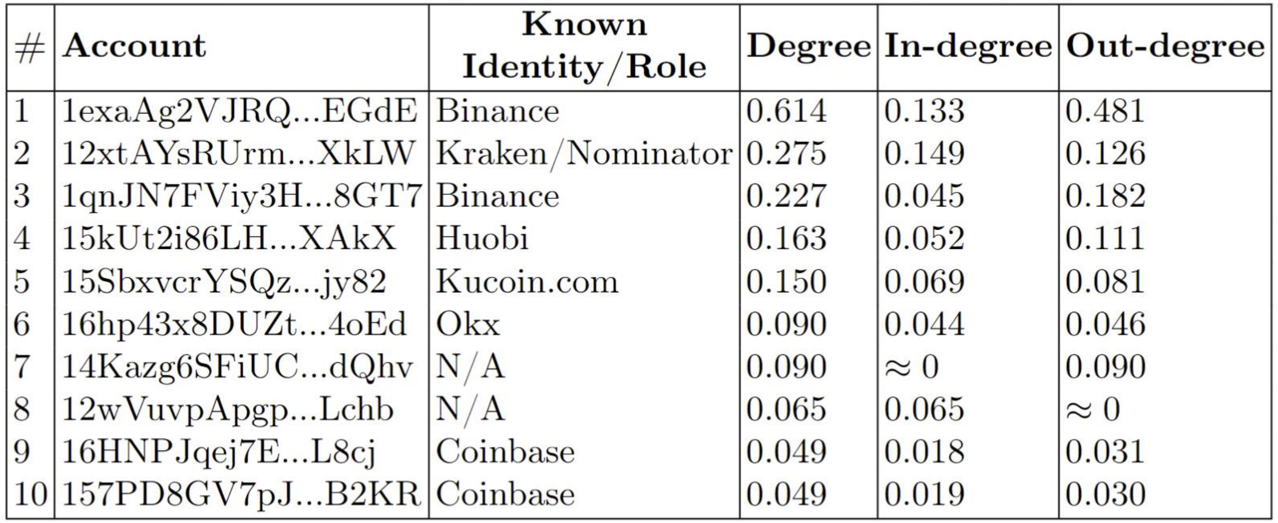


Crypto Exchanges largely dominate the network!

Nodes Analysis

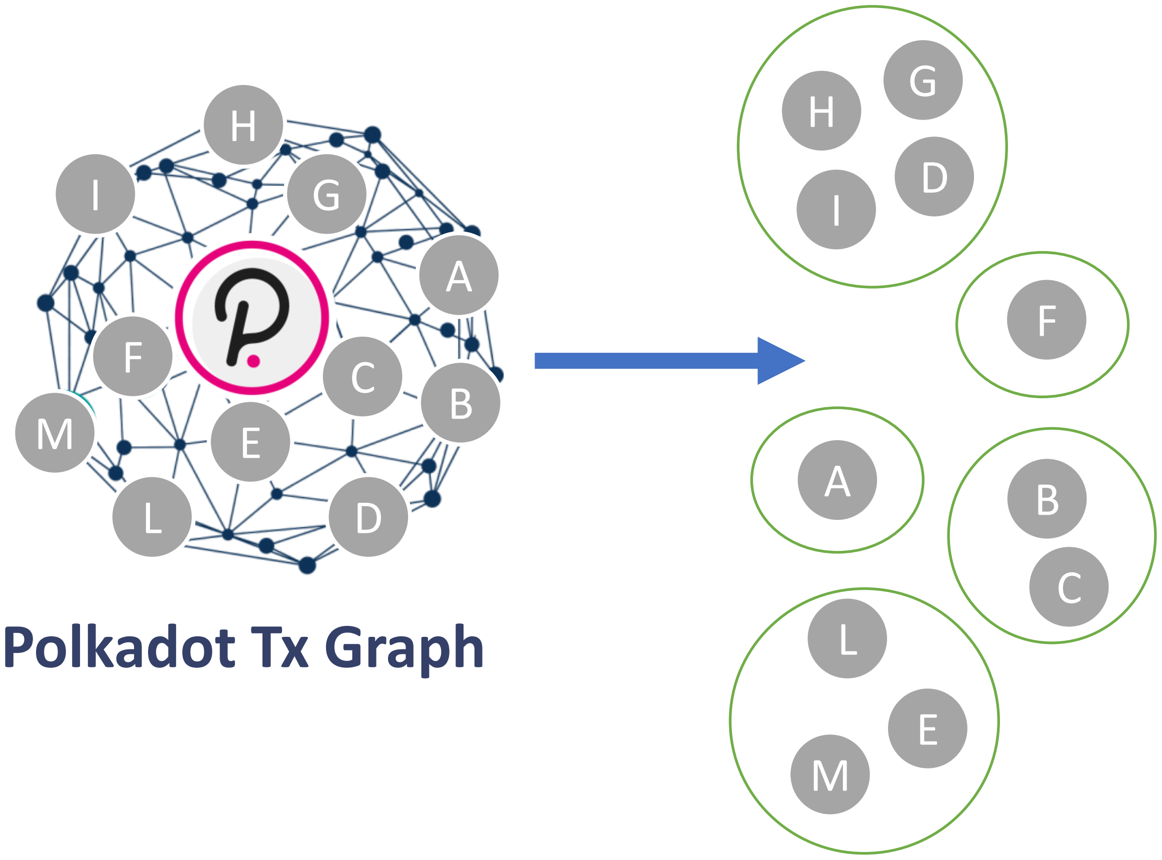
- The number of high-degree nodes is much smaller (…power-law) than low-degree ones
- A few accounts only own balances in the range 500K to over 50M
- ≈ 1M accounts (out of 1,042,149 active accounts) hold small balances (0-499K)

Table 3: Top-10 Most Important Nodes Evaluated By Degree Centrality



#	Account	Known Identity/Role	Degree	In-degree	Out-degree
1	1exaAg2VJRQ...EGdE	Binance	0.614	0.133	0.481
2	12xtAYsRUrm...XkLW	Kraken/Nominator	0.275	0.149	0.126
3	1qnJN7FViy3H...8GT7	Binance	0.227	0.045	0.182
4	15kUt2i86LH...XAkX	Huobi	0.163	0.052	0.111
5	15SbxvcrYSQz...jy82	Kucoin.com	0.150	0.069	0.081
6	16hp43x8DUZt...4oEd	Okx	0.090	0.044	0.046
7	14Kazg6SFiUC...dQhv	N/A	0.090	≈ 0	0.090
8	12wVuvpApgp...Lchb	N/A	0.065	0.065	≈ 0
9	16HNPJqej7E...L8cj	Coinbase	0.049	0.018	0.031
10	157PD8GV7pJ...B2KR	Coinbase	0.049	0.019	0.030

Polkadot – User Account Clustering



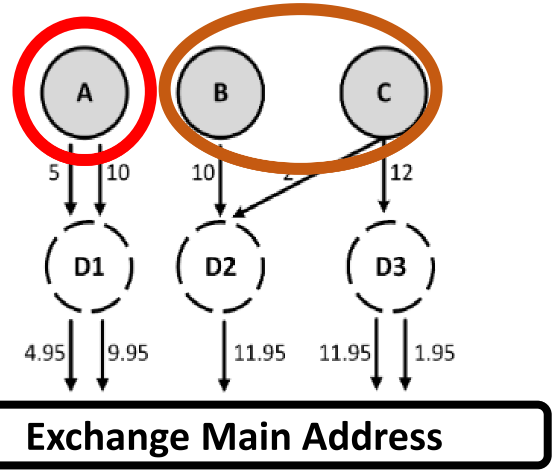
Polkadot Tx Graph

Account Clusters

Caprolu, M. and Di Pietro, R., 2023
Account Clustering in the Polkadot Network: Heuristic, Experiments, and Insights.
IEEE International Conference on Blockchain and Cryptocurrency (ICBC)

Research Question: Do Crypto Exchanges undermine user's privacy?

Methodology: Detect Deposit Addresses (DA), verify their reuse, cluster accounts with common DA



Polkadot – User Account Clustering

Binance

- 70K+ DA Detected
- 8K+ DA Reused
- 22K+ User addresses

↓

clustered in 8,355 clusters

Kraken

- 22K+ DA Detected
- 1.6K+ DA Reused
- 3.7K+ user addresses

↓

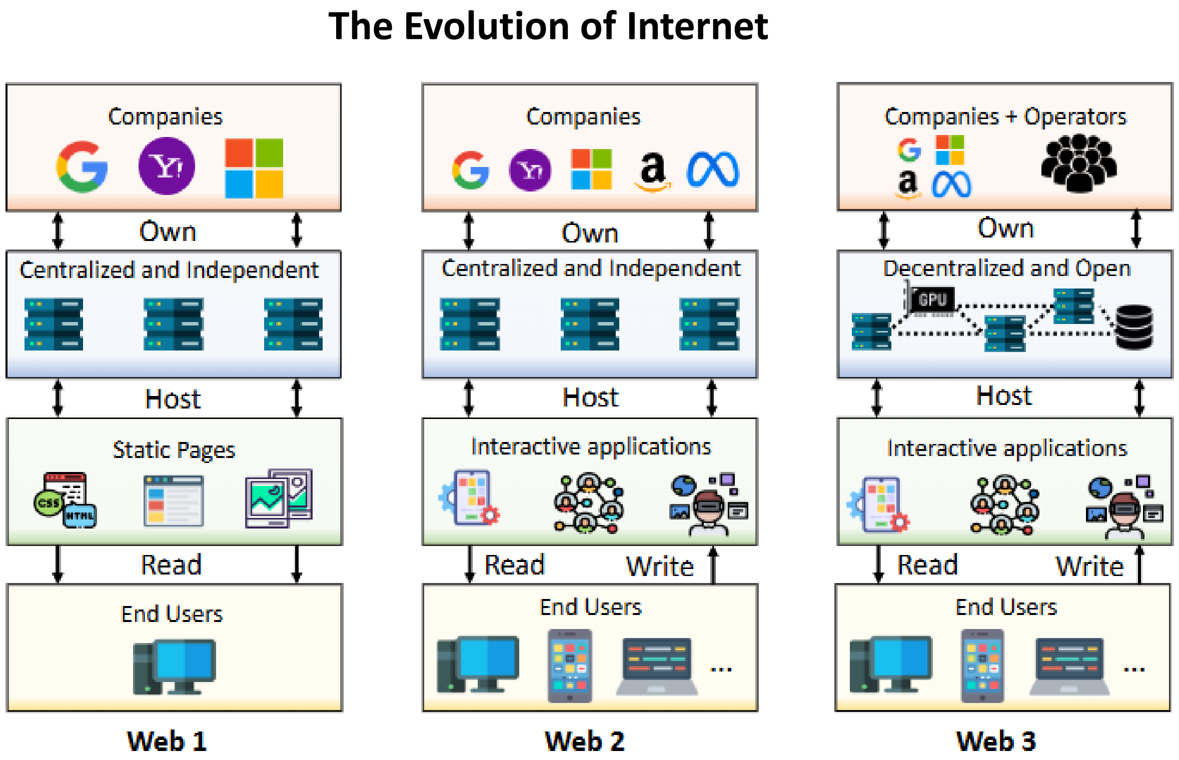
clustered in 1,516 clusters

~25% of all the Binance/Kraken were customers in the Polkadot Blockchain

↓

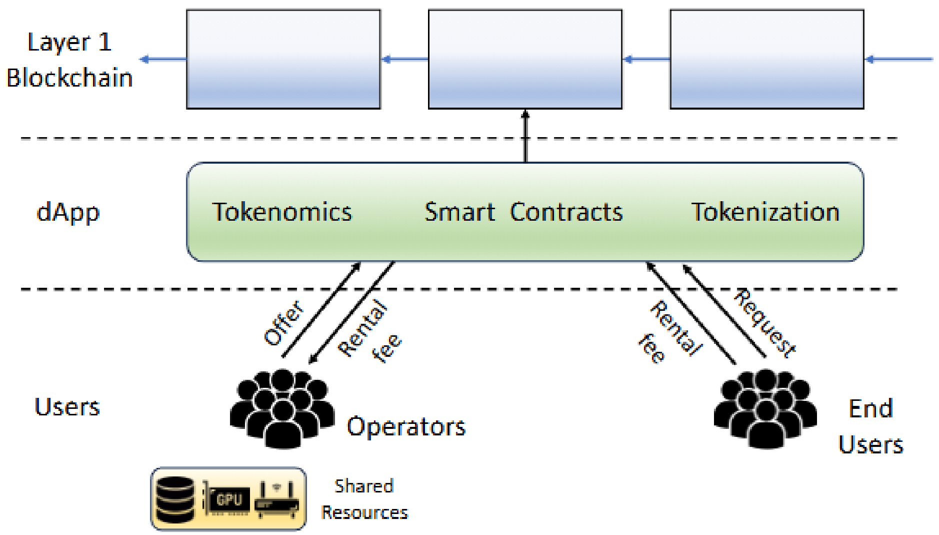
Privacy is in jeopardy!

Decentralized Physical Infrastructure Networks (DePIN)



DePIN Paradigm

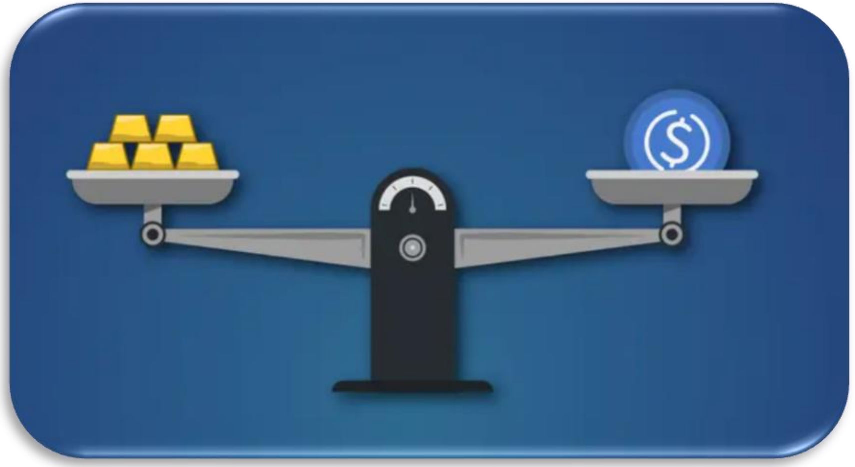
- Running on top of a **blockchain** network
- **Tokenization** of resources (IoT sensors, computation, Internet access, etc.)
- **Tokenomics** models to incentivize participation



Stablecoins

Stablecoins bridge the gap between traditional finance and the decentralized world.

- Cryptocurrencies designed to maintain a stable value by pegging to a reserve of assets (e.g., fiat currency, commodities, etc.)
- Combines the benefits of cryptocurrency with the stability of traditional currency.



Different types of stablecoin:

- <u>Fiat-Collateralized</u>: Backed by a 1:1 reserve of fiat currency (e.g., Tether (USDT), USD Coin (USDC))
- <u>Crypto-Collateralized</u>: Backed by a basket of other cryptocurrencies with over-collateralization to account for market volatility. (e.g., DAI)
- <u>Algorithmic</u>: Use algorithms and smart contracts to control supply and demand, without any backing asset. (e.g., Terra (LUNA))

Stablecoins Security

In an ever-evolving market, ensuring stablecoin security is essential for long-term adoption and trust

Major risks for Stablecoin:

- Dependence on trust in the issuer
- Over-collateralization risks (in crypto-backed types)
- …

Risks generated by stablecoins:

- Escaping monetary policy (sovereignty)
- Devaluing national currency (favoring the pegged one)
- General risk to the financial system (change of pegging target)

Conclusion

- Cryptocurrencies are not a recent innovation. The first one, Ecash, dates back to 1988 (and built on the shoulders of giant…).
- After Bitcoin, a global financial revolution began to change the financial world, culminating in the current multi-faceted DeFi landscape.
- The new DeFi applications inherit issues and vulnerabilities of previous blockchain-based systems, bringing also novel threats and challenges.
- The entire DeFi ecosystem is posing serious threats to the security and privacy of million of users (with very few scientific contributions addressing this issue).

Conclusion

- Innovation is progressing at exponential pace with a move towards tokenization of Real World Assets (RWA)

- Crypto has moved from being nerd staff to a class of assets on its own

- DeFi and stablecoins could pose a serious threat to the current financial system

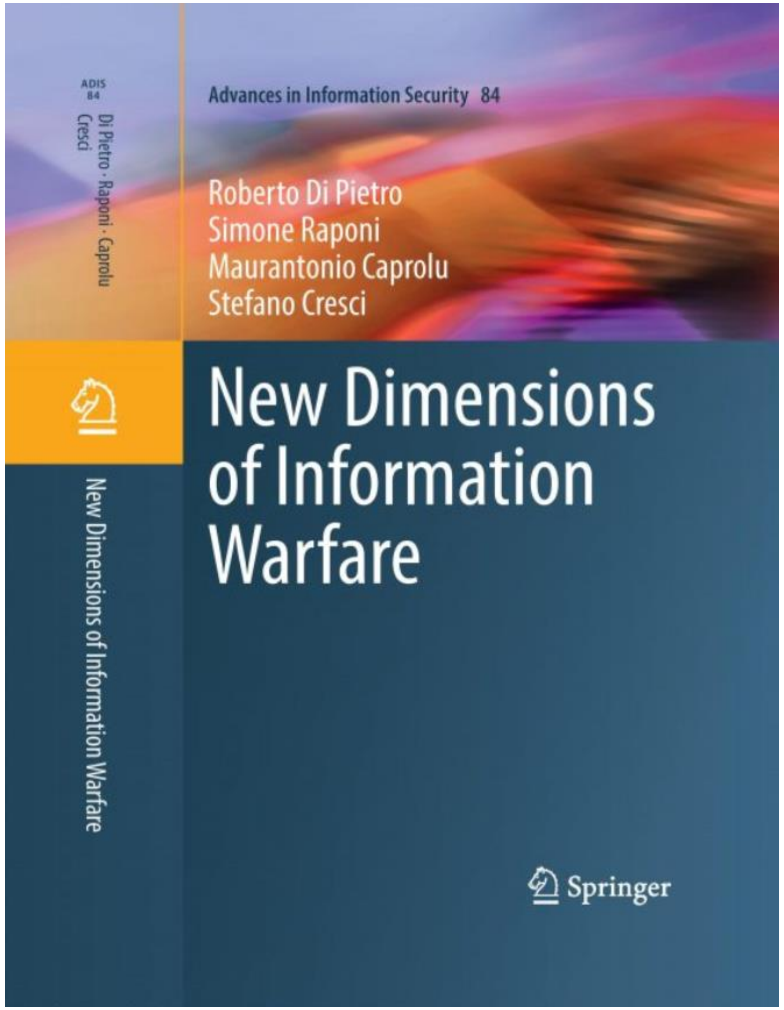
- Need for a sound, scientific multidisciplinary approach (e.g. finance, economics, technology, psychology, CS) to run a sound SWOT analysis.

New Dimensions of Information Warfare

"The digital revolution has changed Information Warfare. Not its core objective (information dominance), but the dimensions along which the cited concept is affirmed, adding a few ones that have been so far quite neglected"

Chapters:

- *Society*
  - Information Disorder
- *Economy*
  - ***Cryptocurrencies***
  - ***Fintech***
- *Infrastructures*
  - Critical Infrastructures
  - Business Entities


ADIS 84
Di Pietro · Raponi · Caprolu
Cresci
Advances in Information Security 84
Roberto Di Pietro
Simone Raponi
Maurantonio Caprolu
Stefano Cresci
New Dimensions of Information Warfare
New Dimensions of Information Warfare
Springer

Thank you!

Follow-up to:

roberto.dipietro@kaust.edu.sa