



THE UNIVERSITY
of EDINBURGH



A Stratified Approach to Blockchain Decentralisation

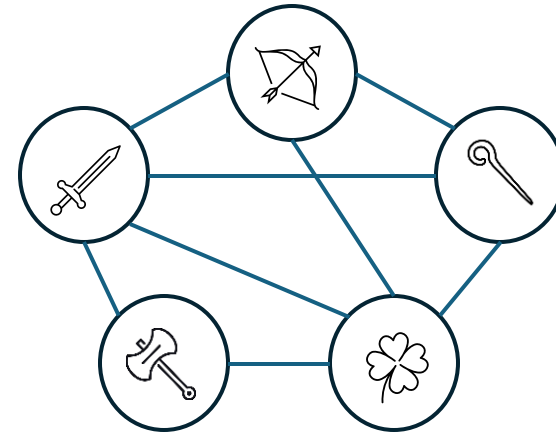
Aggelos Kiayias, University of Edinburgh and Input Output

Joint work with **Cristina Ovezik** and **Dimitris Karakostas**

Centralised vs Decentralised systems



- A **single party** has full control over the system (“rules them all”)
- If it misbehaves or crashes, the system is compromised, e.g.:
 - Censorship
 - Inconsistency
 - Data loss / unavailability



- A number of **independent parties** collectively control the system and guarantee its properties
- If only few nodes are malicious / faulty, the system remains operational
 - No single points of failure

Decentralization spectrum

- Decentralization as an **objective of blockchain** systems
- **Not a binary** property
- Degree of decentralization impacts a blockchain's **security, fairness and even legal status**

Decentralisation / Centralisation



Examples of centralised system failure

BBC Sign in Home News Sport Weather iPlayer Sounds

NEWS

Home | InDepth | Israel-Gaza war | War in Ukraine | Climate | UK | World | Business | Politics | Culture

Technology

CrowdStrike IT outage affected 8.5 million Windows devices, Microsoft says



EPA

Joe Tidy
Cyber correspondent, BBC News

20 July 2024

16,900 flights cancelled over 72h

BBC Menu

NEWS

Technology

Cloudflare apologises for outage which took down X and ChatGPT



GETTY IMAGES

Liv McMahon
Technology reporter

18 November 2025

A number of high-profile websites, including X and ChatGPT, went down for many people on Tuesday, due to problems affecting major internet

20% of global web traffic for 4+ hours

BBC Menu

NEWS

Business | Economy | Technology of Business | AI Bus

Post Office Horizon scandal: Why hundreds were wrongly prosecuted



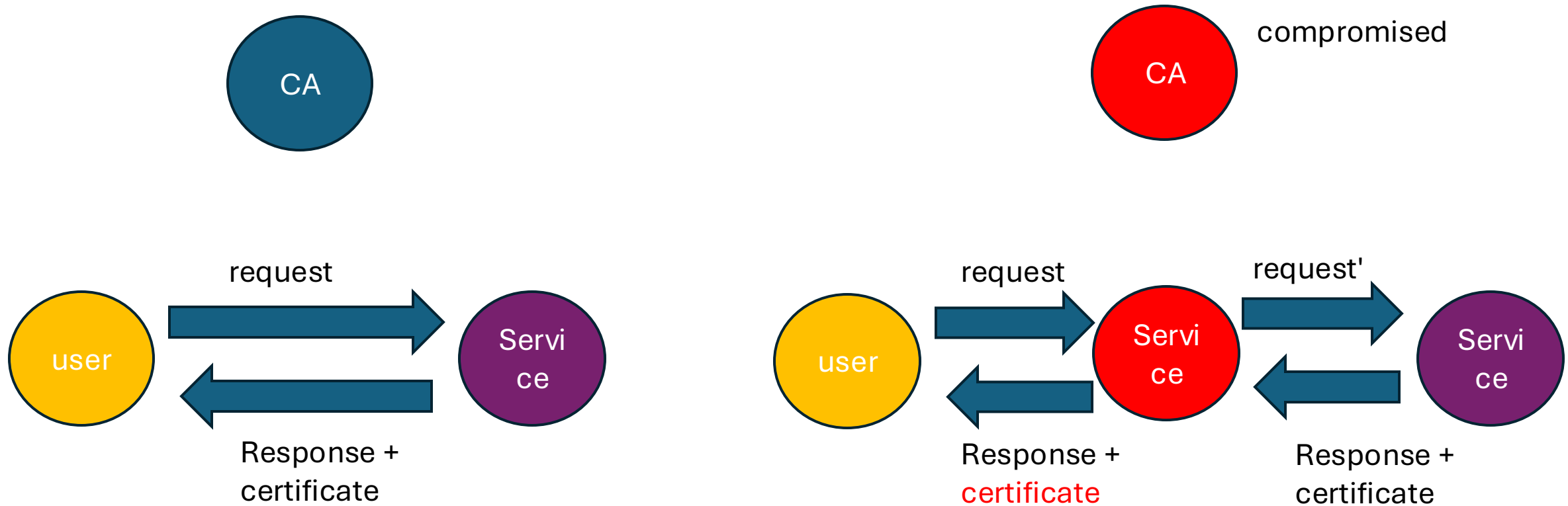
PA MEDIA

22 April 2021
Updated 9 October 2025

The Post Office Horizon scandal has been called the UK's most widespread miscarriage of justice, after hundreds of people were wrongly prosecuted due to faulty software which suggested money was missing from their branch accounts.

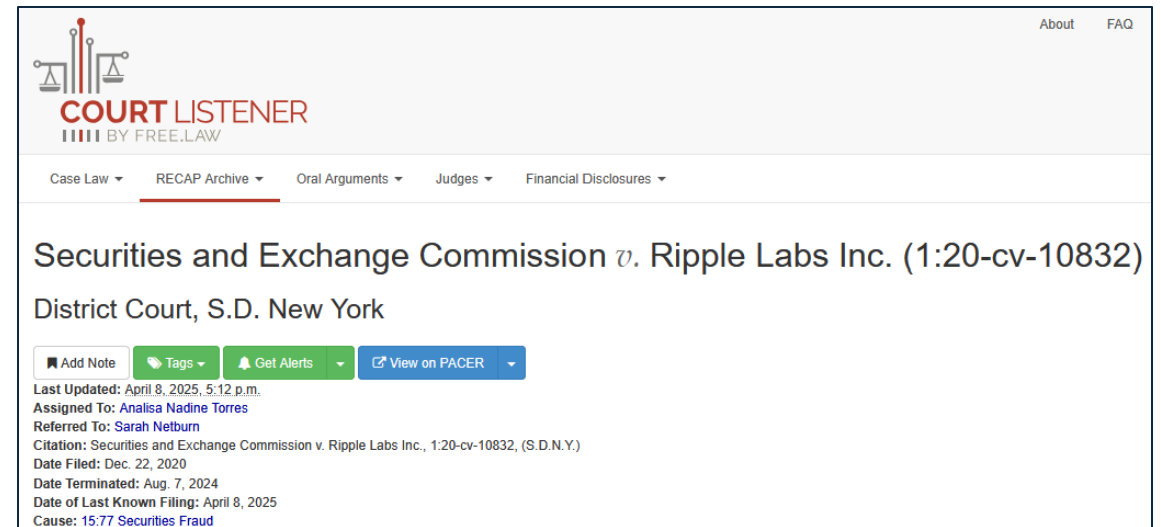
900 falsely accused

Certificate authority compromises



Case study: SEC vs. Ripple Labs lawsuit

- SEC' allegation: XRP is a security
- Ripple's defence: decentralised network
- Court proceedings point to lack of clear methodology for determining blockchain decentralisation



Sources: <https://www.courtlistener.com/docket/19857399/securities-and-exchange-commission-v-ripple-labs-inc>
<https://storage.courtlistener.com/recap/gov.uscourts.nysd.551082/gov.uscourts.nysd.551082.796.33.pdf>

SPOFs and Layers in IT Systems

Single Points of
Failures = SPOF

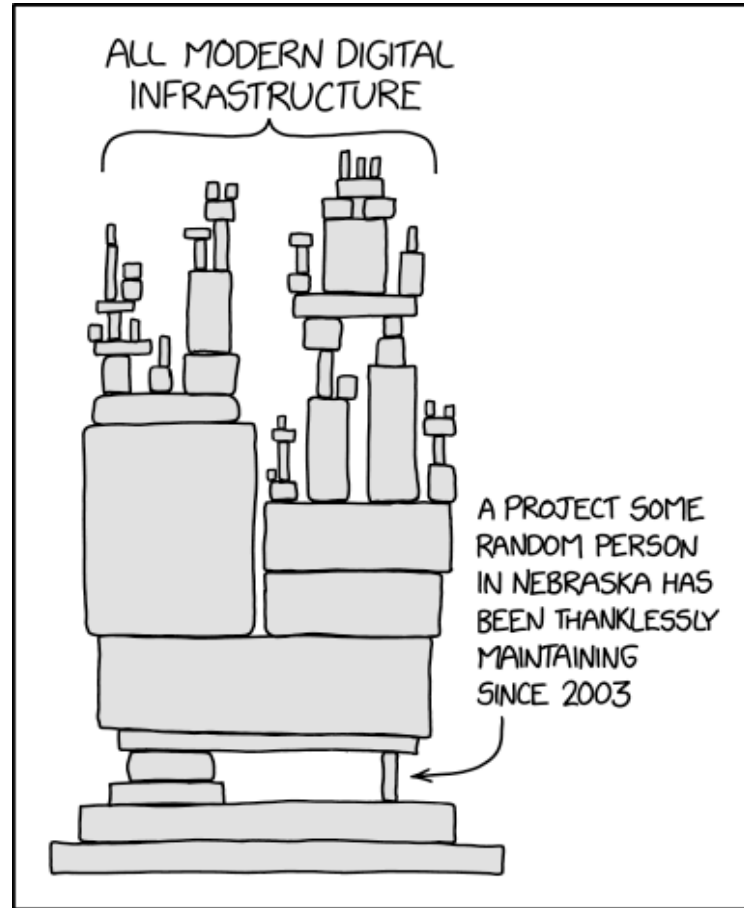


Image credit: <https://xkcd.com/2347/>

Blockchain systems are multilayered

- Bitcoin example from 2019
 - > 100 block producers
 - But 70% of mining coming from China (geographical centralization)
- FTX example from 2022
 - Built on top of Ethereum
 - 60 % of tokens owned by a single address (centralization of wealth)



Understanding SPOFs

- We usually understand **single points of failure** (SPOFs) in the context of catastrophic failures
- However: any **desirable system property** should be subjected to SPOF analysis
- Relevant blockchain properties:
 - **Safety**: a “bad” thing never happens
 - **Liveness**: a “good” thing will eventually happen

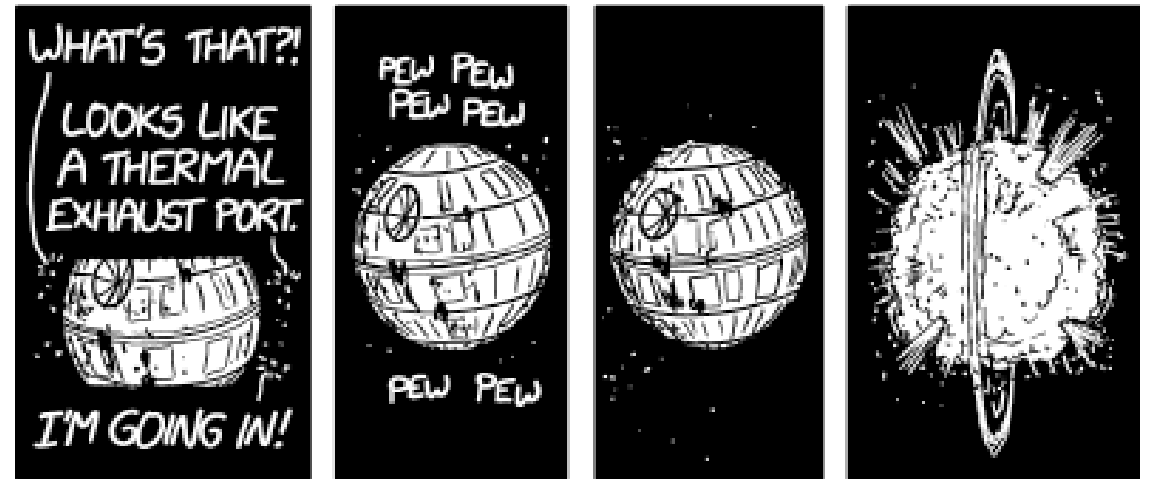
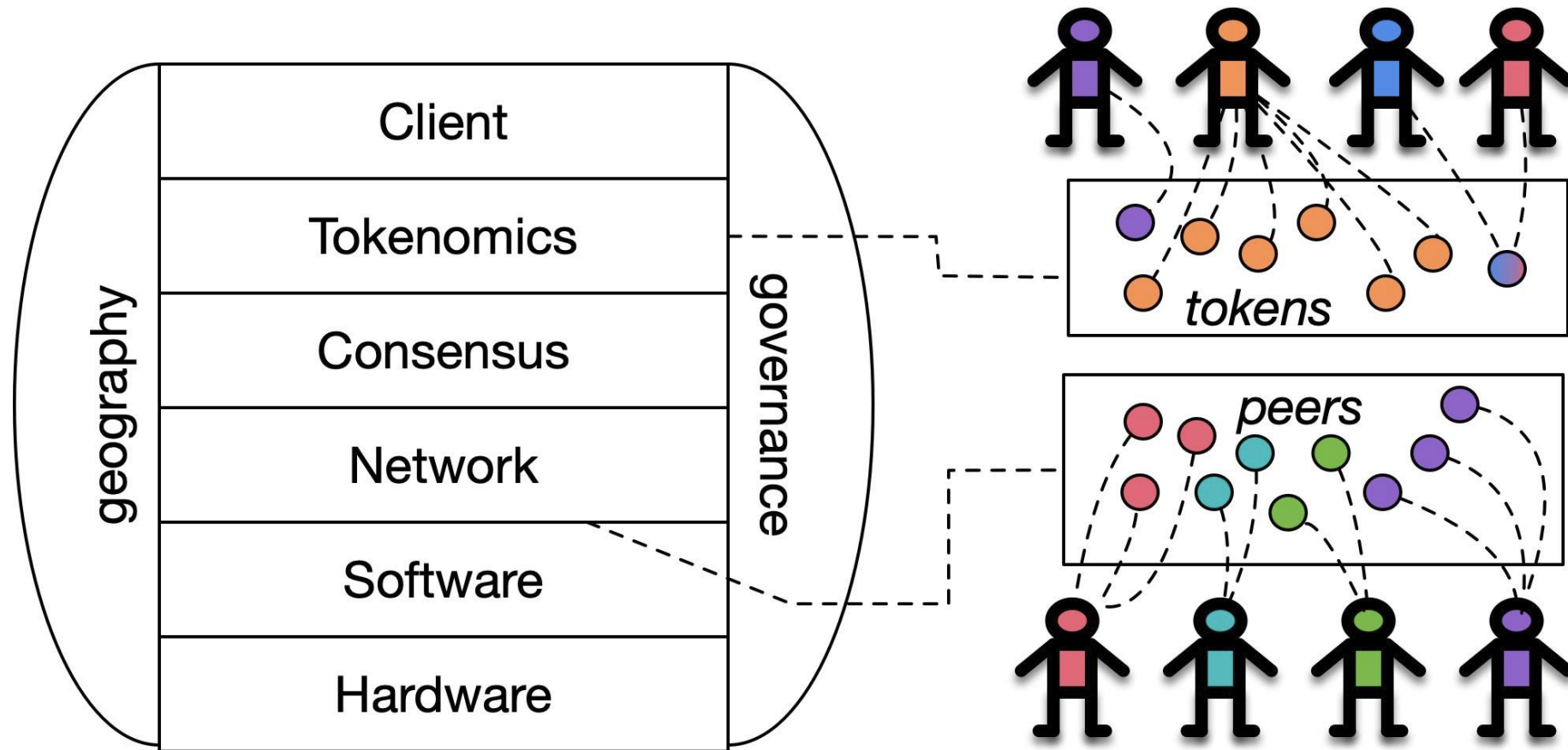


Image credit: <https://xkcd.com/2425/>

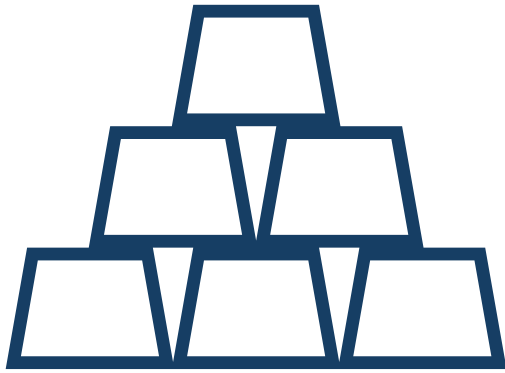
Methodology – Main thesis

- There are **8 layers of** blockchain systems where **(de)centralisation** can occur
- **Centralisation** in some layer **threatens** desirable system properties, such as **safety, liveness, privacy and price stability**

Methodology - Layers



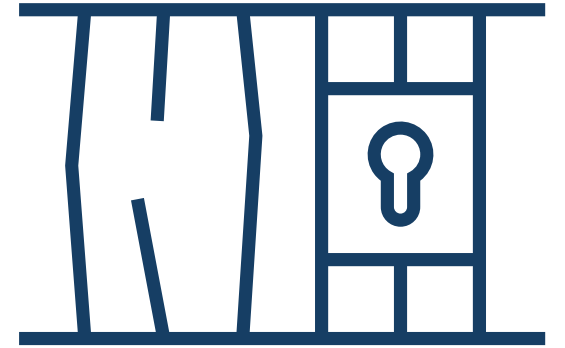
For each layer



resource



relevant
parties



properties
at risk

Open ended questions

- What are the right metrics for measuring decentralization in a layer?
 - Which resource distributions are good ? Which ones should be avoided?
- How to combine metrics across layers?
- How to account for resource units that are decentralized themselves?