BLOCKCHAINGOV

POLKADOT BLOCKCHAIN ACADEMY

Blockchain Governance Module

PBA Lucerne

06.04. – 07.04.2025

Welcome!
Kick-Off Meeting

Agenda

- Meet the faculty
- What is this about?
- Why does it matter?
- Educational goals
- Module overview
- Module logistics
- Q&A

Meet the faculty

Primavera de Filippi

Tara Merk

Lovisa Björna

Felix Beer

BLOCKCHAINGOV

BLOCKCHAIN-POWERED DISTRIBUTED GOVERNANCE
FOR COMMUNITIES, INSTITUTIONS AND THE WORLD.

We are a 5-year long, transdisciplinary research effort aimed at restoring trust in institutions at the community and global levels, by promoting better on chain and off chain distributed governance practices. We are funded by the European Research Council (grant ID: 865856).

cnrs CERSA EUI erc

www.blockchaingov.eu

Our educational goal

Promote governance literacy

- Equip blockchain technologists with the necessary competences to design and implement effective governance, both on-chain and off-chain.
- Contribute to the professionalization of blockchain governance as a recognised field of expertise.

Learning outcomes

1. Understand the key governance principles, mechanisms and trade-offs;
2. Develop a strategy for progressive decentralization;
3. Design and implement effective governance innovations;
4. Navigate their political, regulatory and ethical implications;
5. Measure and improve the impact of governance systems.

Why
What
Who
Where
When
How

TIME	DAY 1	DAY 2
09 AM	Kick-Off Presentation	Lecture 5 “Blockchain Legality & Regulation” (Primavera)
10 AM	Lecture 1: “Introduction to Blockchain Governance” (Primavera)	Lecture 6 “Blockchain Governance Competencies” (Primavera)
11 AM	Case Study Presentation (Tommi? Tara? Lovisa?)	Fish Bowl “The Future of Governance” (Primavera, Tara, Lovisa, Felix, Nathalie, Tommi)
12 AM	Lecture 2: “Blockchain Governance Architecture” (Felix & Lovisa)	Wrap-Up & Feedback Form
01 PM	Lunchbreak	Lunchbreak
02 PM	Lecture 3: “Blockchain Governance Mechanisms & Trade-Offs” (Tara)	
03 PM	Exercise	
04 PM	Lecture 4: “DAO Governance” (Felix)	
05 PM	Wrap-Up + Q&A	
06 PM	Office Hour	

Module Logistics

- All course materials are in the symposium that you have received.
- Also available in our Element channel.
- Office Hours from 5-6PM.

Get in touch!

Lovisa Björna

Email:
lovisa@polkadot.academy

Felix Beer

Email:
felix@polkadot.academy

Q & A

Thanks & Enjoy!

BLOCKCHAINGOV

Introduction to Blockchain Governance

Lecture 1

Primavera de Filippi

In a world increasingly governed by technology

those who build and control the technology, govern the world

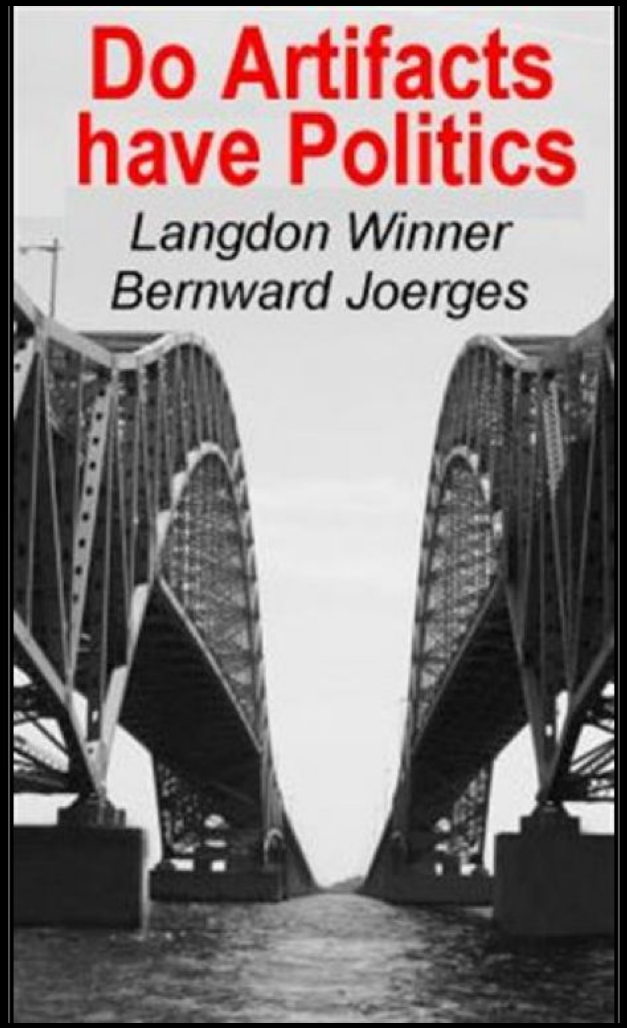
POLKADOT
BLOCKCHAIN
ACADEMY

Technologists are not politicians:

1. Not elected through democratic mechanisms
2. Not trained to think about politics and governance

POLKADOT
BLOCKCHAIN
ACADEMY

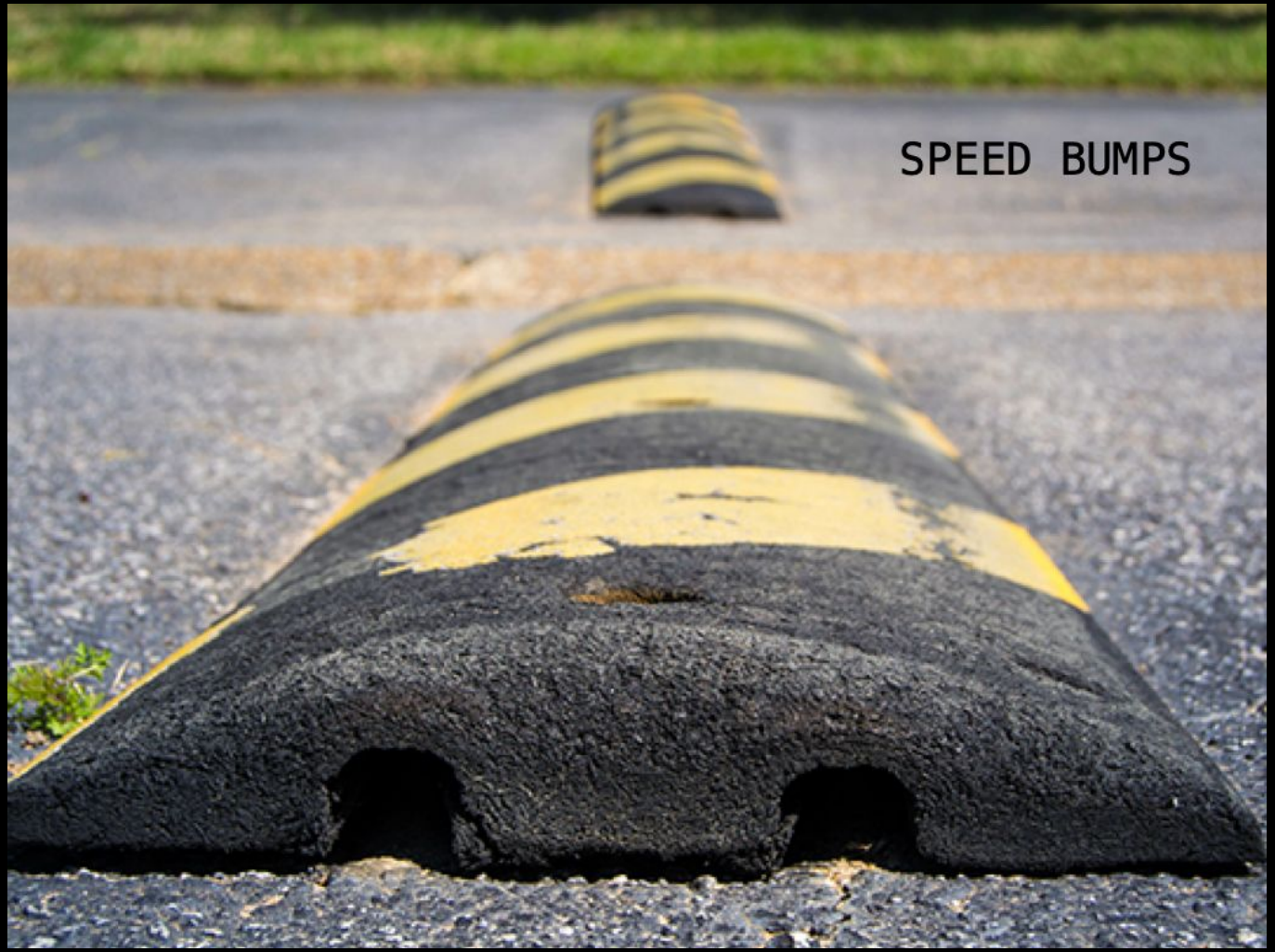
Affordances



Constraints

POLKADOT BLOCKCHAIN ACADEMY

POLKADOT
BLOCKCHAIN
ACADEMY



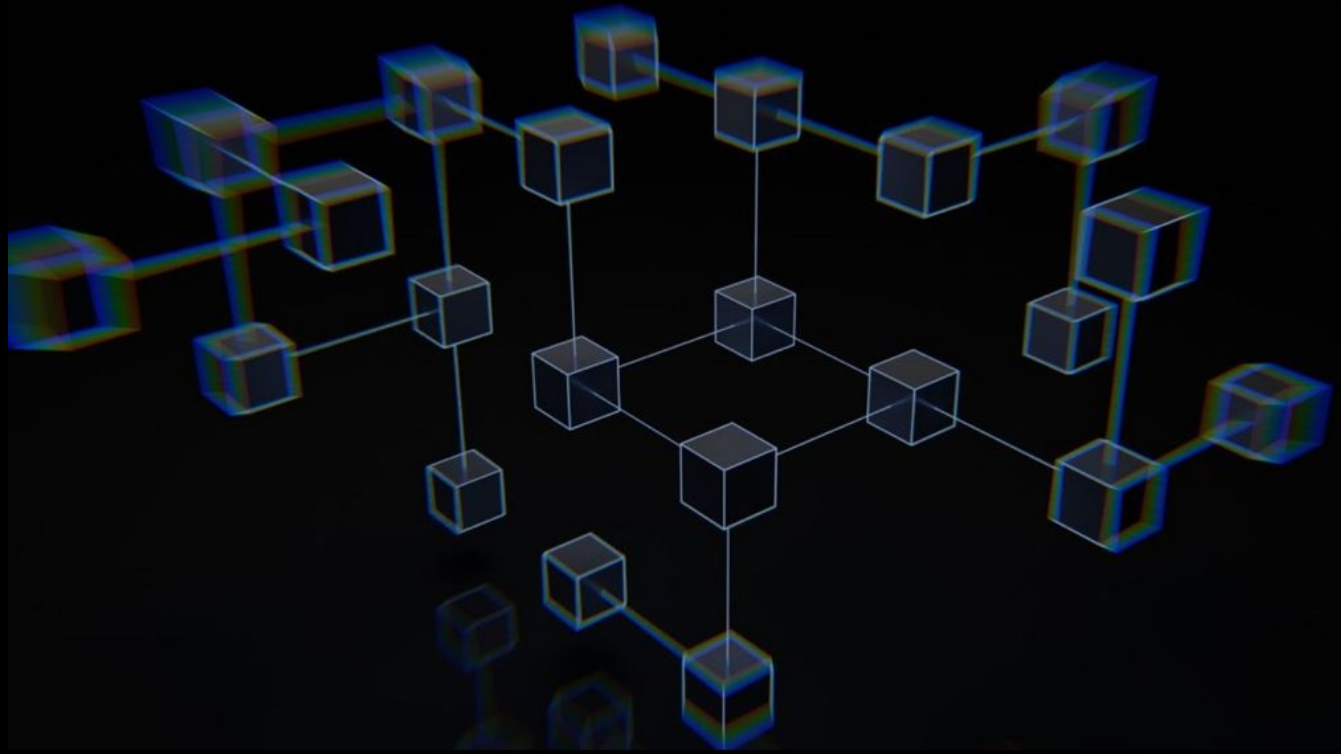
POLKADOT
BLOCKCHAIN
ACADEMY

Digital Artefacts Have Politics

POLKADOT BLOCKCHAIN ACADEMY

DIGITAL ARTEFACTS ALSO HAVE POLITICS

POLKADOT BLOCKCHAIN ACADEMY



Blockchains Have Politics

POLKADOT BLOCKCHAIN ACADEMY

Blockchains Have Politics

POLKADOT BLOCKCHAIN ACADEMY

How to engineer blockchain systems

that provide the right mix of affordances and contraints ?

POLKADOT
BLOCKCHAIN
ACADEMY

Blockchains require governance

- Governance is an universal feature of all blockchains, whether explicitly designed or not;
- Blockchain networks can be thought of as decentralised decision making systems;
- Effective governance is crucial for aligning and coordinating diverse stakeholders in a blockchain network;
- Without governance leadership, blockchain systems struggle to succeed, evolve and adapt.

What is governance?

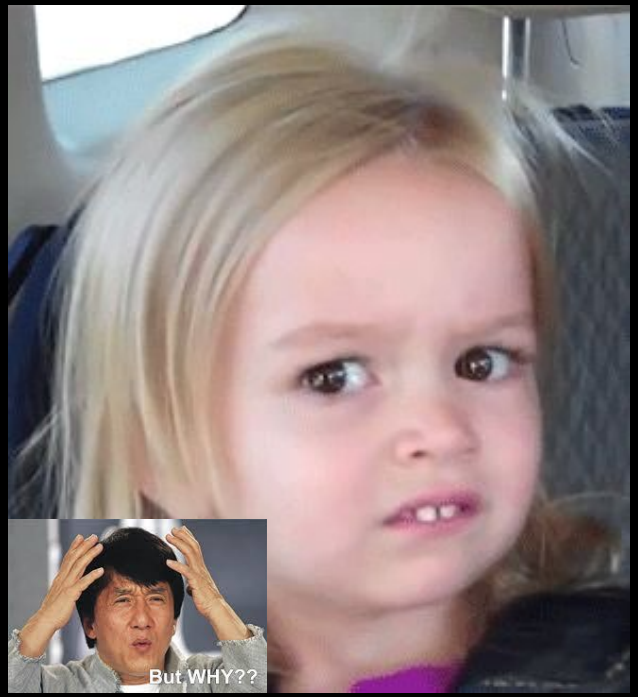
Defining governance

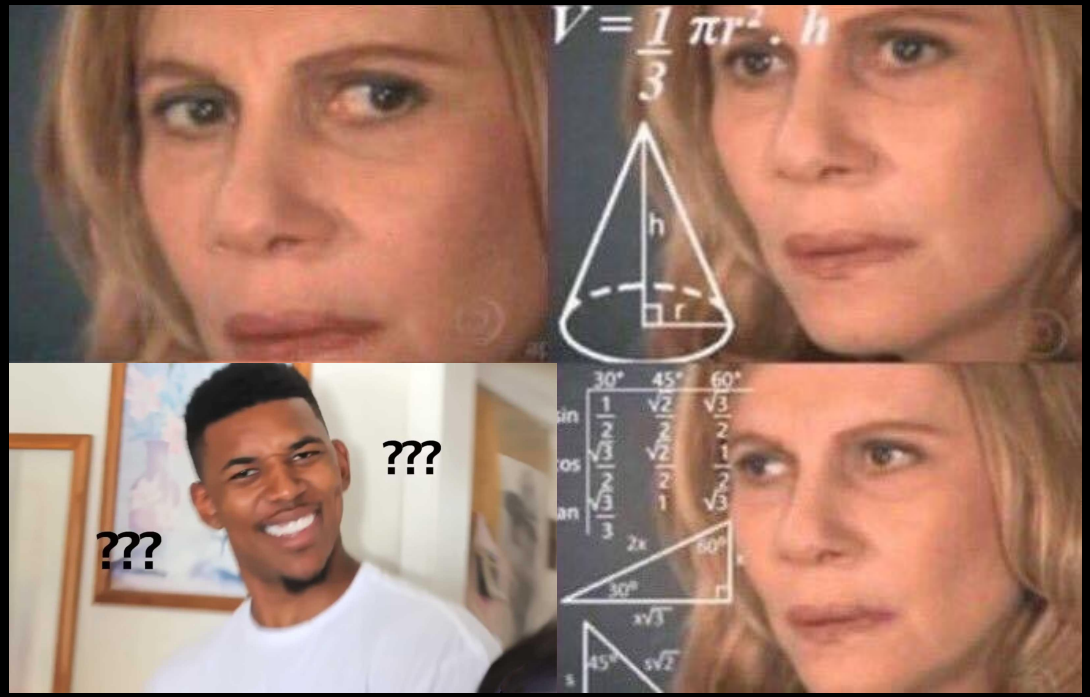
Governance refers to the regulation of decision-making processes among actors towards shared objectives that lead to the development, reinforcement, or reproduction of social norms and institution

"Governance describes the norms, structures, and processes by which individuals and groups with ongoing relationships bargain about how to make decisions within an organisational formation — such as a community, market or government" (Bevir, 2012).

Bevir, M. (2012). Governance: A Very Short Introduction. Hampshire, UK: Oxford University Press.

What the **** is blockchain governance?





Blockchain governance is ...

- A term associated with many topics, meanings, and interpretations;
- A concept characterised by a lack of a commonly recognised definition;
- A nascent yet rapidly evolving field of research and practice;
- An interdisciplinary discourse including computer science, law, political science, sociology, policy and cybernetics.

Blockchain governance is ...

- “Blockchain governance is the mechanism by which design changes are enacted and regulated on a blockchain.”

Decision Rights and Governance within the Blockchain Domain: a literature analysis

Completed Research Paper

Koen Smit
HU University of Applied Sciences
Utrecht, the Netherlands
koen.smit@hu.nl

Jalal el Mansouri
HU University of Applied Sciences
Utrecht, the Netherlands
jalal.elmansouri@student.hu.nl

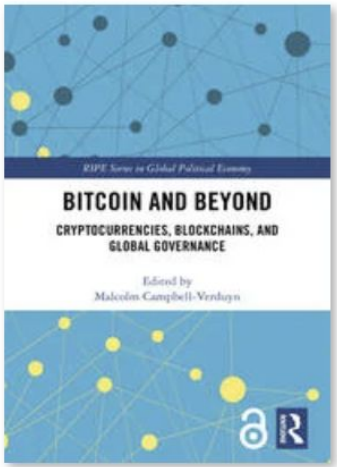
Sabri Saïd
HU University of Applied Sciences
Utrecht, the Netherlands
sabri.said@student.hu.nl

John van Meerten
HU University of Applied Sciences
Utrecht, the Netherlands
john.vanmeerten@student.hu.nl

Sam Leewis
HU University of Applied Sciences
Utrecht, the Netherlands
sam.leewis@hu.nl

Blockchain governance is ...

- "Blockchain governance is about determining who has authority (internal and external actors); how these actors are endowed (e.g., ownership rights vs. decision authority), in what form (formal and informal governance forms/structures), and at which level."



Chapter

The internal and external governance of blockchain-based organizations

Evidence from cryptocurrencies

By *Ying-Ying Hsieh*, *Jean-Philippe (JP) Vergne*, *Sha Wang*

Blockchain governance is ...

Defining Blockchain Governance: A Framework for Analysis and Comparison

Rowan van Pelt, Slinger Jansen, Djuri Baars & Sietse Overbeek

Pages 21-41 | Published online: 09 Mar 2020

- "Blockchain Governance describes the means of achieving the direction, control and coordination of stakeholders within the context of a given blockchain network to which they jointly contribute"

Blockchain governance is ...

- “Blockchain Governance encompasses technical and social means to make decisions on the different levels (e.g., individual, community, organizational, national, international) related to actors, roles, rights, incentives, responsibilities, rules, and the business, technological, legal, and regulatory aspects of a blockchain system during its whole lifecycle.”

A system-based view of blockchain governance

Gabriella Laatikainen, Mengcheng Li, Pekka Abrahamsson

Different dimensions of governance

1. **Decision rights** denote the authority, responsibility, and capability of involved individuals in a blockchain that how decisions are made and monitored and which stakeholders' interests should be prioritised. The allocation of decision rights indicates the network's degree of decentralization.

2. **Accountability** means that those responsible for the different phases of the blockchain lifecycle should be identifiable and answerable for their decisions. This governance dimension promotes the efficient use of resources and transparent performance monitoring.

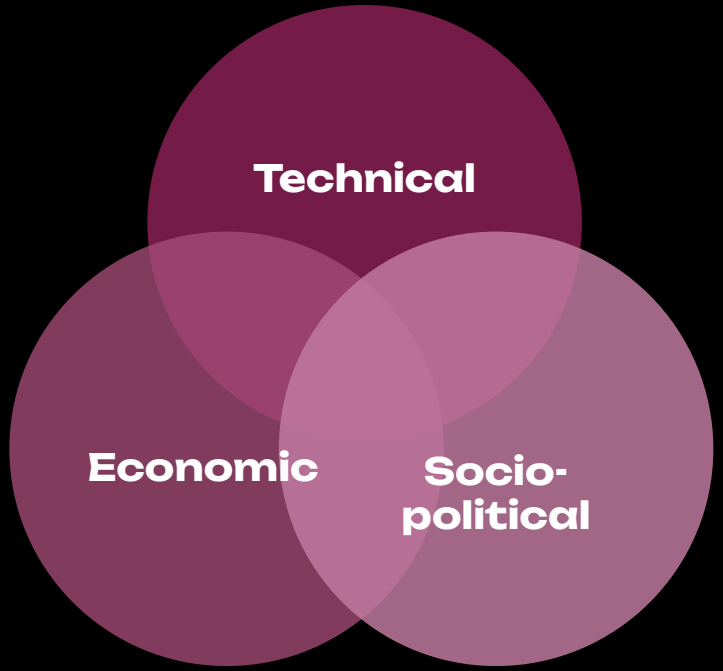
3. **Incentives** play a dual role, attracting participation in governance activities and guiding collective decision-making towards shared objectives.

Different scopes of governance

1. **Technical aspects:** code upgrades, protocol changes

2. **Economic aspects:** token issuance, monetary policy

3. **Social/political aspects:** community coordination, conflict resolution



Different functions of governance

Governance functions

- **Upgradability:** Governance mechanisms facilitate the continuous evolution of blockchain systems, allowing for the integration of new functionalities to adapt to changing needs.

- **Resilience:** Governance equips blockchain networks with the flexibility to adapt to evolving demands and environments, enabling the rectification of vulnerabilities. This ensures the ongoing relevance and operational efficiency of the network.

Governance functions

- **Legitimacy:** Effective governance practices lend legitimacy to a blockchain network by instituting clear, transparent rules and procedures that earn the recognition and respect of its stakeholders.

- **Security:** A strong governance framework significantly boosts the security measures of blockchain networks, safeguarding them from potential attacks and reinforcing the trustworthiness and integrity of the data stored on-chain.

Governance functions

- **Compliance:** Governance ensures blockchain networks adhere to legal and regulatory standards, enhancing credibility and safeguarding against legal risks. This alignment with laws and guidelines fosters a trustworthy and secure environment for users and stakeholders.

Consequences of poor governance

Hard Forks / Chain Splits

- Example: Contentious disagreements can lead to rival blockchains.

Underfunded Public Goods

- Lack of mechanisms to fund protocol maintenance or improvements.

Loss of Community Confidence

- Users and investors may leave if decision processes seem unfair or chaotic.

Regulatory & Legal Exposure

- Without clarity on decision-making, the project can run afoul of changing regulations.

Key Concepts

TRUST &
CONFIDENCE

Antonopoulus:
"Shift from trusting people … to trusting math"

"Don't trust, Verify"

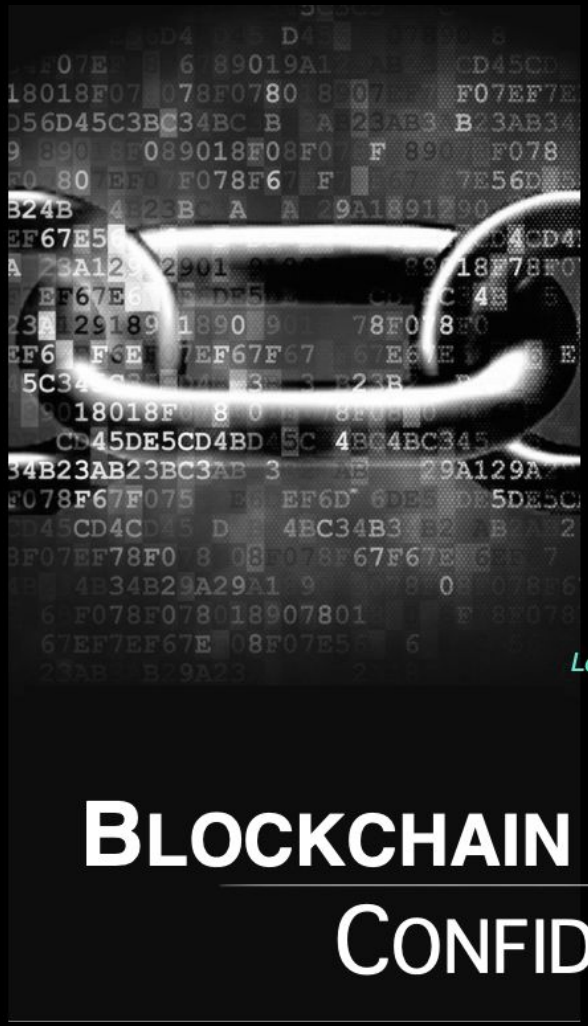
The Economist:
"Trust Machine"

Werbach:
"Trustless Trust"

BLOCKCHAIN AS… (negative definition)

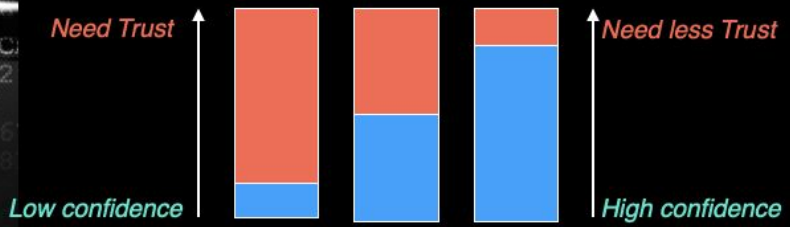
TRUSTLESS TECHNOLOGY

POLKADOT BLOCKCHAIN ACADEMY



*It is **not** about **eliminating trust** altogether,*
*but rather about **maximizing confidence,***
*in order to indirectly **reduce the need for trust.***

- *The **higher** the **predictability** of the system,*
- *The **higher** the **confidence** in the system,*
- *The **lower** is the **need for trust** in the system.*



BLOCKCHAIN AS... (positive definition)

CONFIDENCE MACHINE

POLKADOT BLOCKCHAIN ACADEMY

Confidence Factors

(1) ***Mathematics & Cryptography***

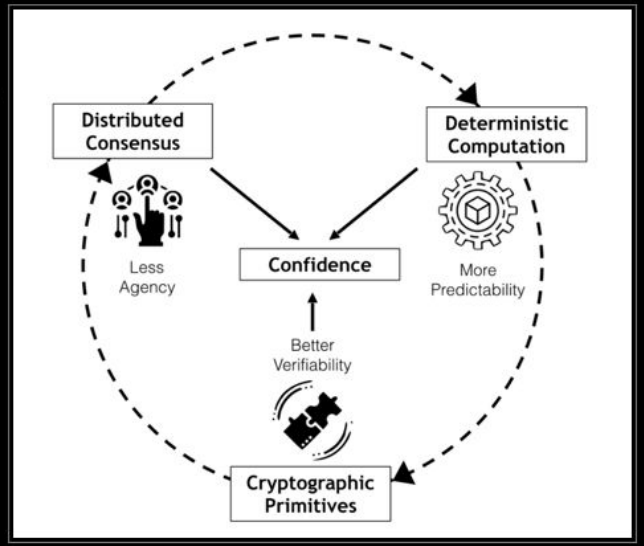
- *Hashing functions, Public-Private Keys*

(2) ***Economic incentives & Game Theory***

- *Utility function*
- *Distributed Consensus*

(3) ***Expert systems***

- *Open Source code*
- *Public verifiability of every operation*

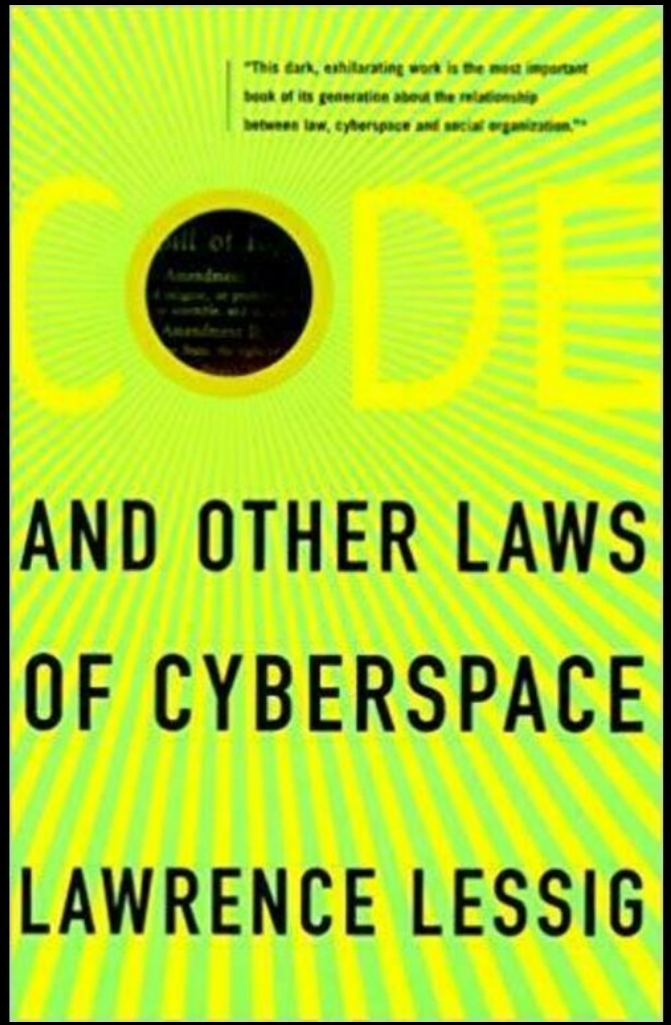


Blockchain as... (positive definition)

Confidence Machine

POLKADOT BLOCKCHAIN ACADEMY

THE RULE OF CODE



CODE IS LAW

POLKADOT BLOCKCHAIN ACADEMY

Rule of Law

Access to Legal Remedy

Access to timely justice mechanisms for grievance remedies and peaceful resolutions

Transparency of Law

Laws must be clear, precise, affordable and accessible while protection fundamental rights

Equality under the Law

All are equal under the law: it applies equally to all—governments, citizens, companies, etc

Independent Judiciary

Independent judiciary ensures equality and fairness of law between people & public officials

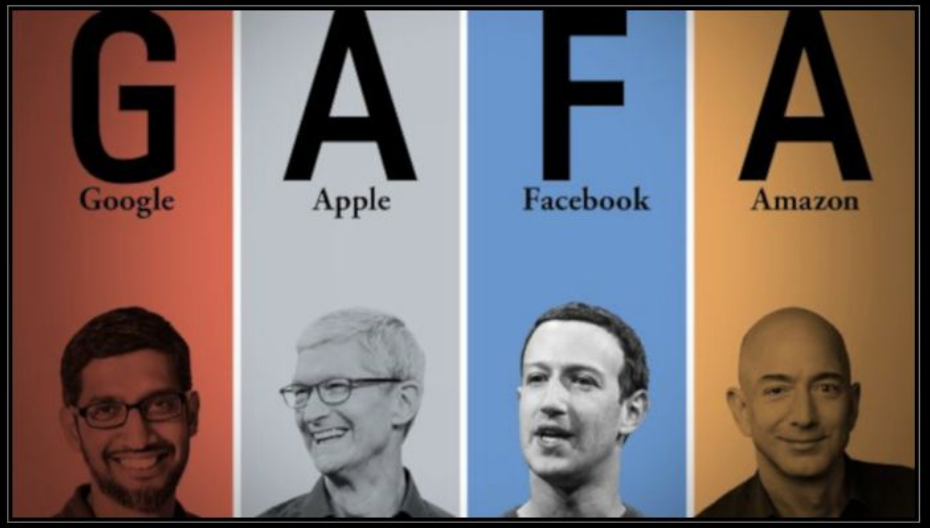
POLKADOT BLOCKCHAIN ACADEMY

RULE ~~OF~~ BY LAW

INSTRUMENTALISATION OF LAW
AS A TOOL OF POLITICAL POWER

POLKADOT BLOCKCHAIN ACADEMY

Rule by Code

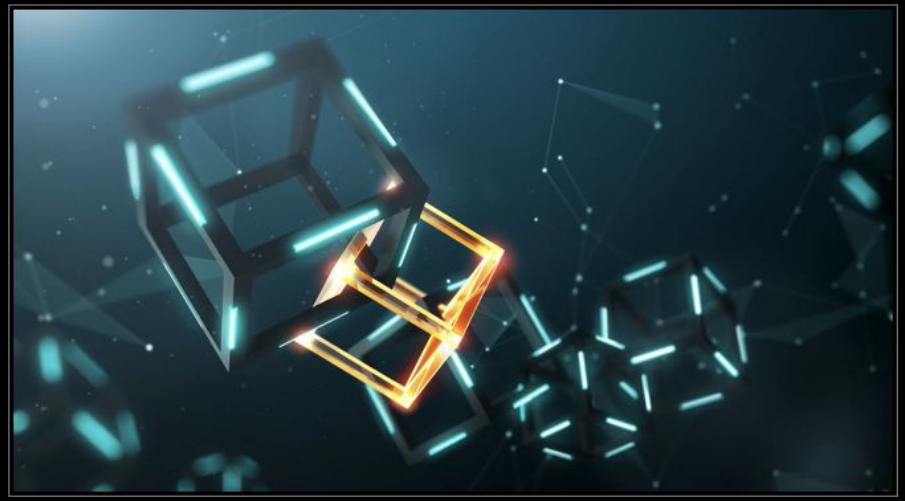


Digital Feudalism
Functional Sovereignty

Instrumentalisation of Code
as a tool of political power

POLKADOT BLOCKCHAIN ACADEMY

Rule ~~by~~ of Code



Technical Sovereignty

No One is Above the Code

POLKADOT BLOCKCHAIN ACADEMY

Code is Law : Blockchain as Confidence Machine

POLKADOT
BLOCKCHAIN
ACADEMY

Bringing Trust back in

Blockchains as Socio-Technical Systems

Confidence of on-chain rules depends on the *trust* of underlying off-chain processes

POLKADOT BLOCKCHAIN ACADEMY

Blockchain Governance

Governance

BY the infrastructure

(on-chain governance)

OF the infrastructure

(off-chain governance)

POLKADOT BLOCKCHAIN ACADEMY

ON-CHAIN Governance refers to a decision-making process where protocol changes and updates are proposed, voted on, and implemented directly through the blockchain itself, using smart contracts and token-based voting mechanisms

VS

OFF-CHAIN Governance involves making decisions about blockchain protocols through discussions, debates, and consensus-building that occurs outside the blockchain, typically through forums, social media, or in-person meetings, before implementing the agreed-upon changes

Exogenous governance refers decisions made outside the blockchain system (e.g., the media, general public) but impacting managerial decision-making within the system

VS

Endogenous governance describes governance practices inside the system, done by the community and for the community.

Exercise

1. Collective brainstorming:

    a. what are the main governance issues that you have encountered?
    b. what is your preference for blockchain governance? on-chain or off-chain?
    c. do you think governance should play a larger role in the context of blockchain systems, and why ?

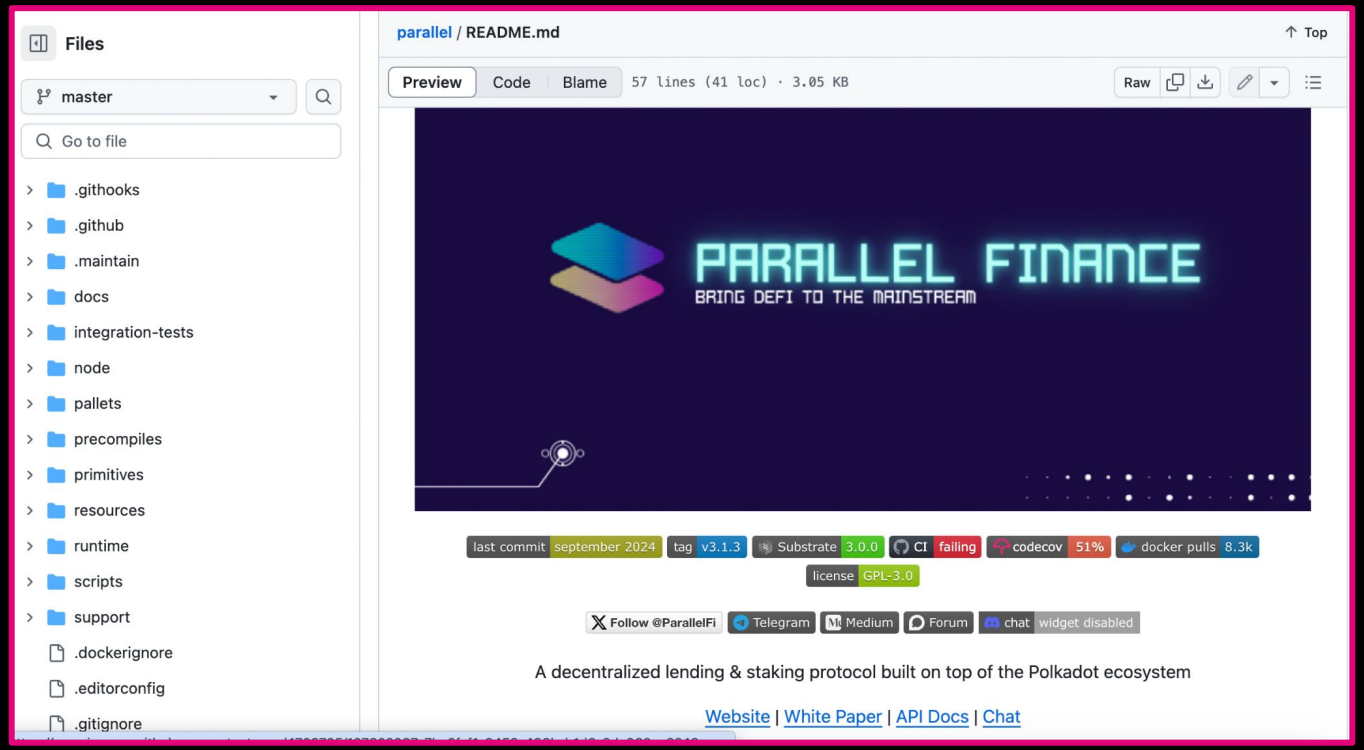
BLOCKCHAINGOV

Case Study Introduction

Lecture 2

Lovisa Björna & Tara Merk

Meet Parallel Finance



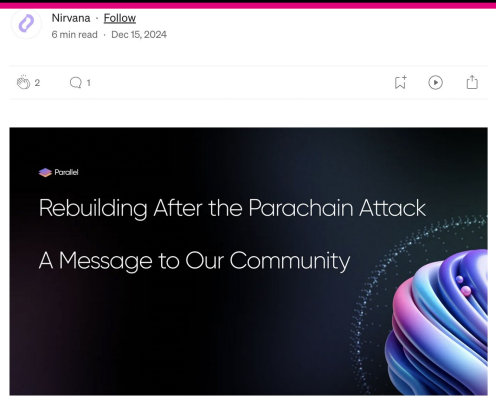
ParaFi over time

Milestones Achieved

- Highest TVL among all parachains.
- Highest number of XCM transfers.
- 44,000 token holders.
- 29.4 Million DOT crowdloaned via Parallel.
- 1.63 Million DOT staked via Parallel liquid staking.

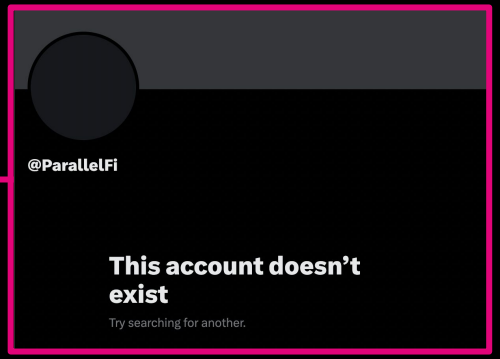
Oct, 2022

Dec, 2024



Sept, 2024

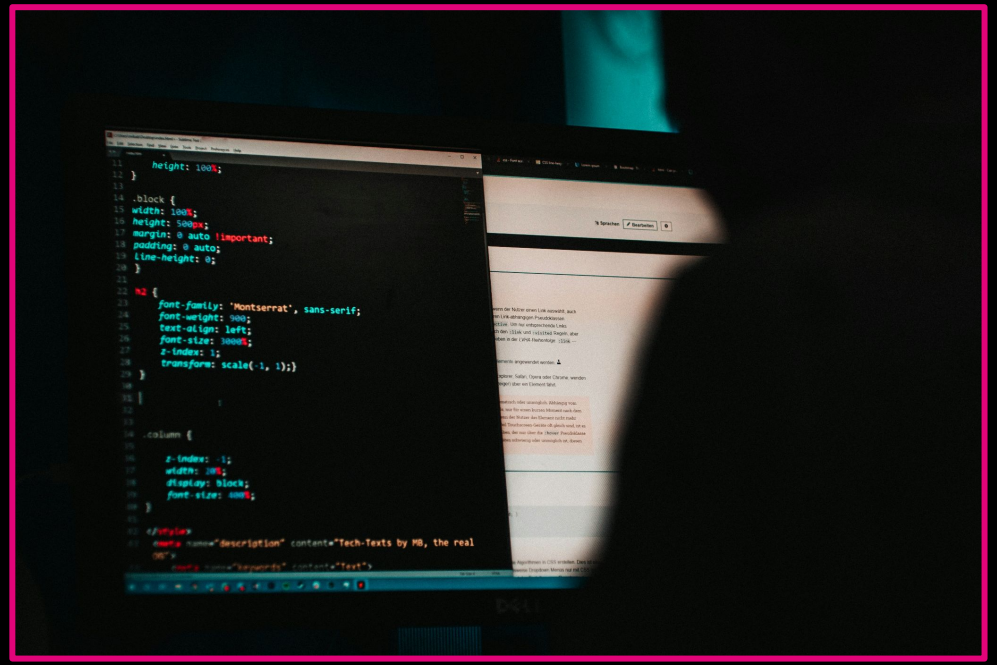
Today



What happened?

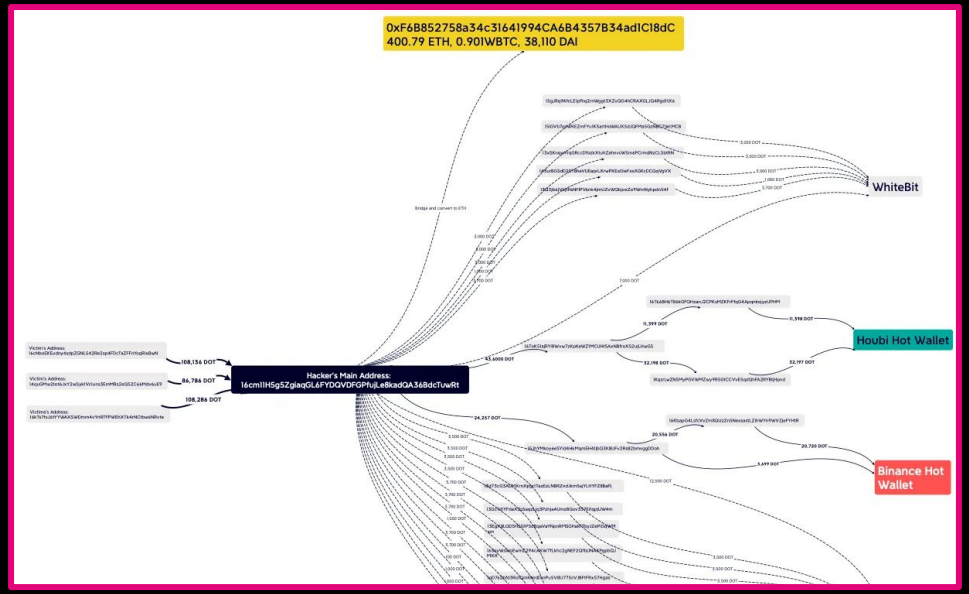
Halloween 2024...

- Hacker submits a malicious runtime upgrade to the Parallel Finance Parachain governance
- They vote for their own proposal (Attacker approved of attack 🤝)
- The proposal creates a “sudo” pallet i.e. a type of account with super privileges
- The module becomes active on Nov 7th

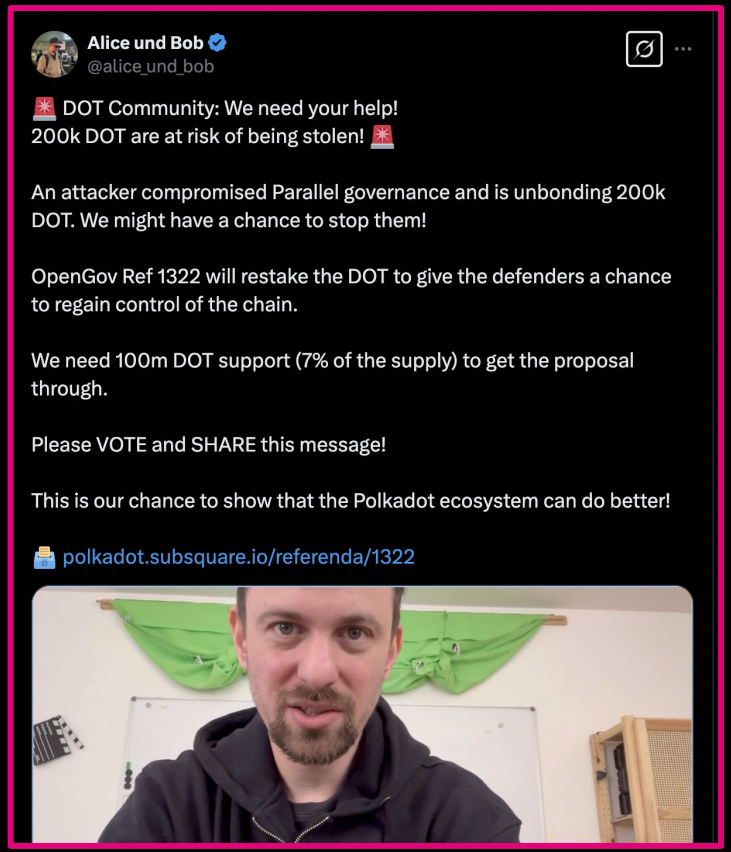


Next...

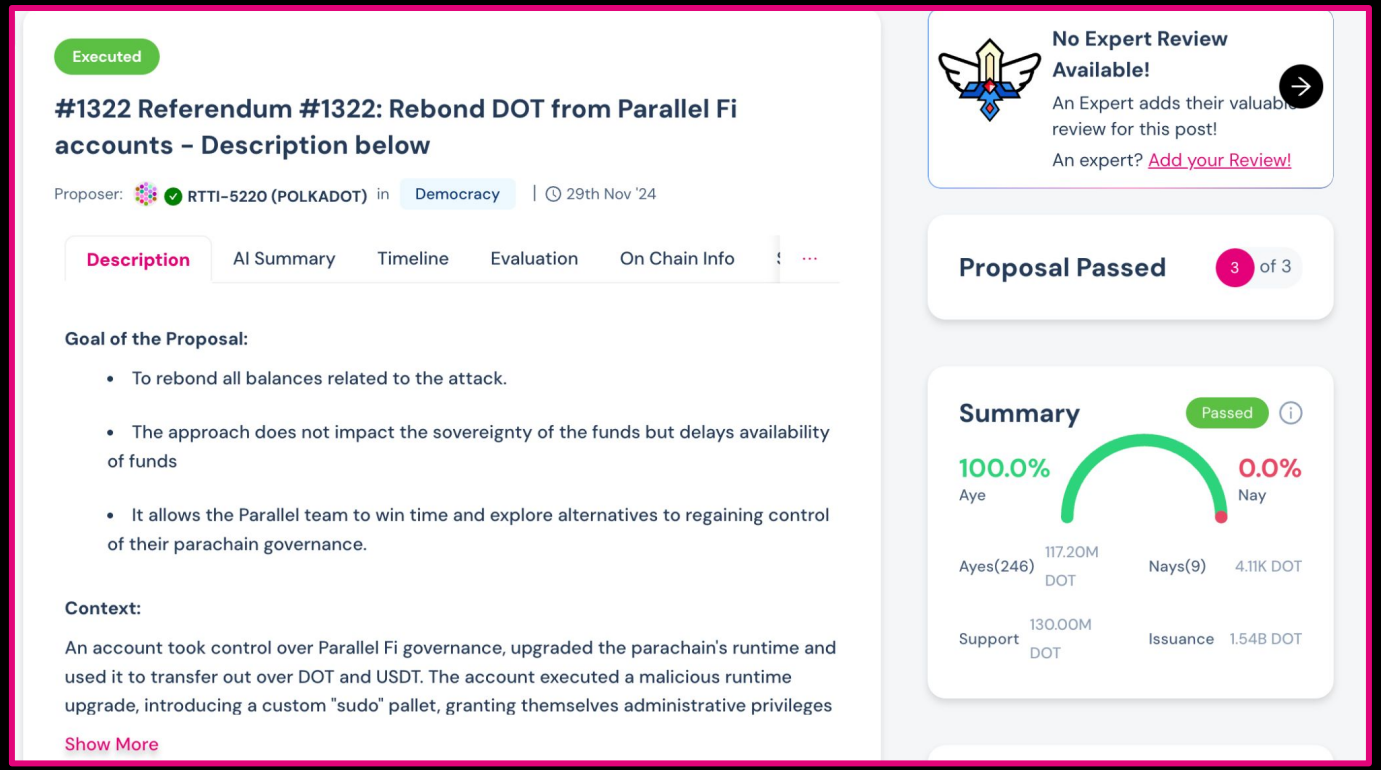
- They disabled governance
- Unstaked funds were immediately moved out of the network. The attacker successfully transferred over 312,185 DOT and 126,837 USDT.
- Part of the funds (200.000DOT) required unstaking from the Polkadot network, causing delays and attracting attention.



Ecosystem agents alerted the community, Parallel were still asleep at the wheel.

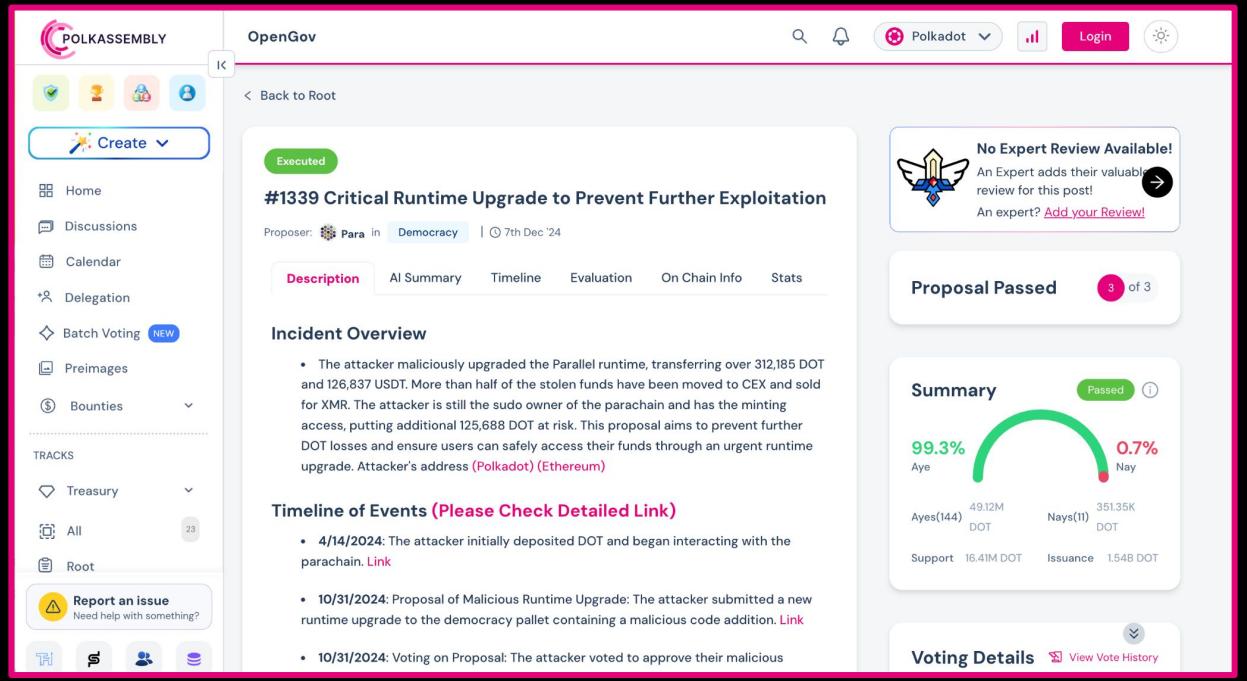


Round 1: The community rallied together!



With 28 days more time, what would they do?

Parallel finance pushes for runtime upgrade



& it goes through!

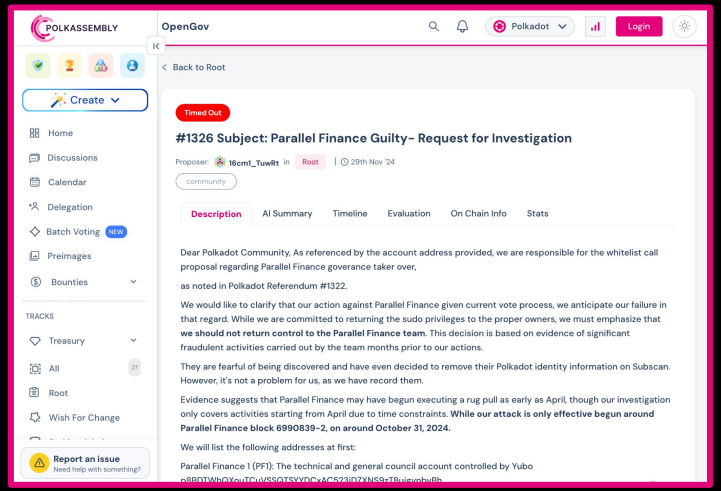
Interlude:
the hacker has something to say...

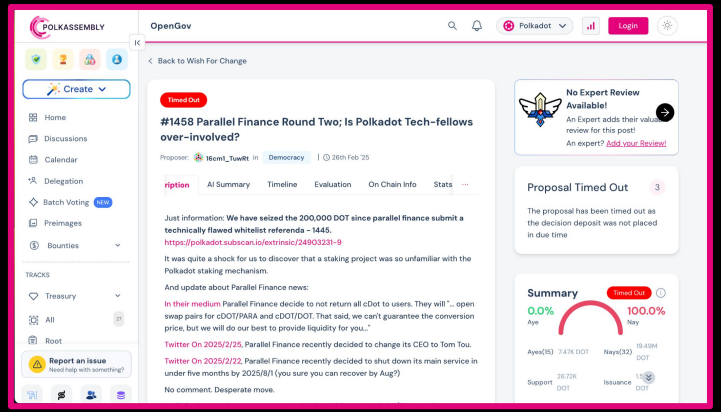
In Parallel...

The attacker started giving background of the purpose of the attack by criticizing Parallel's historic management of the chain.

In referenda **#1326** the attacker presents "evidence of significant fraudulent activities" and claims that the CEO had a previous **criminal record.**

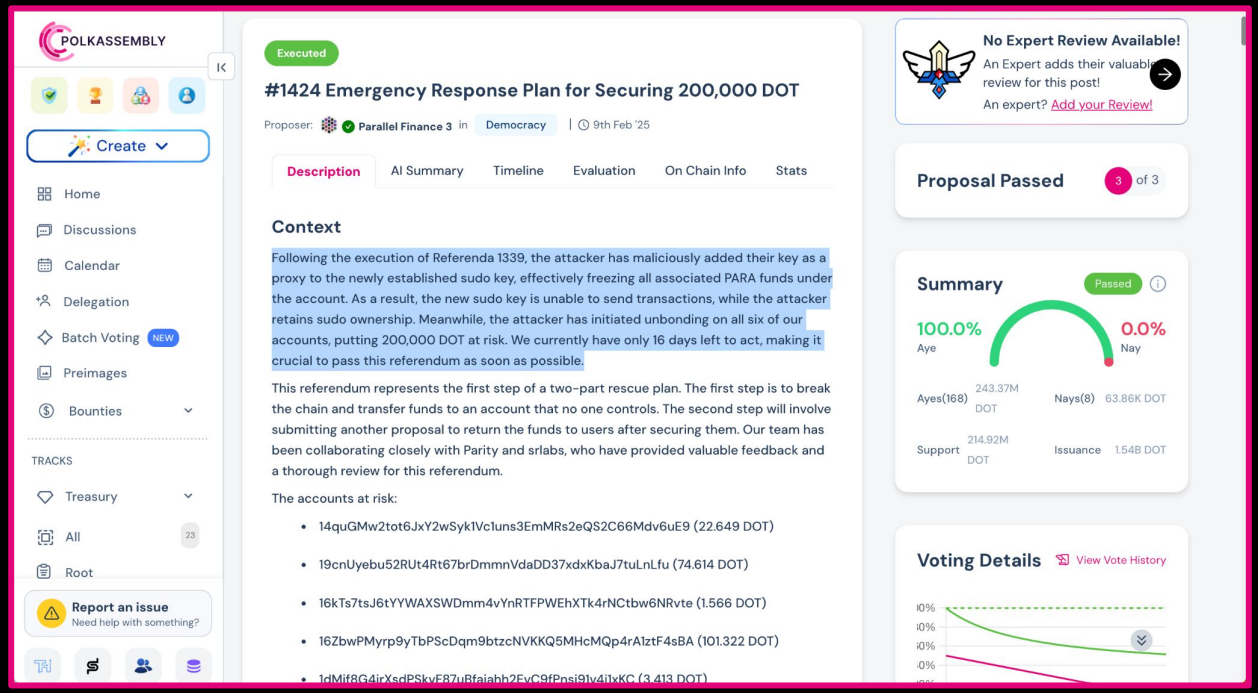
Basically, he's arguing that the ParallelFi team are the criminals, not him!





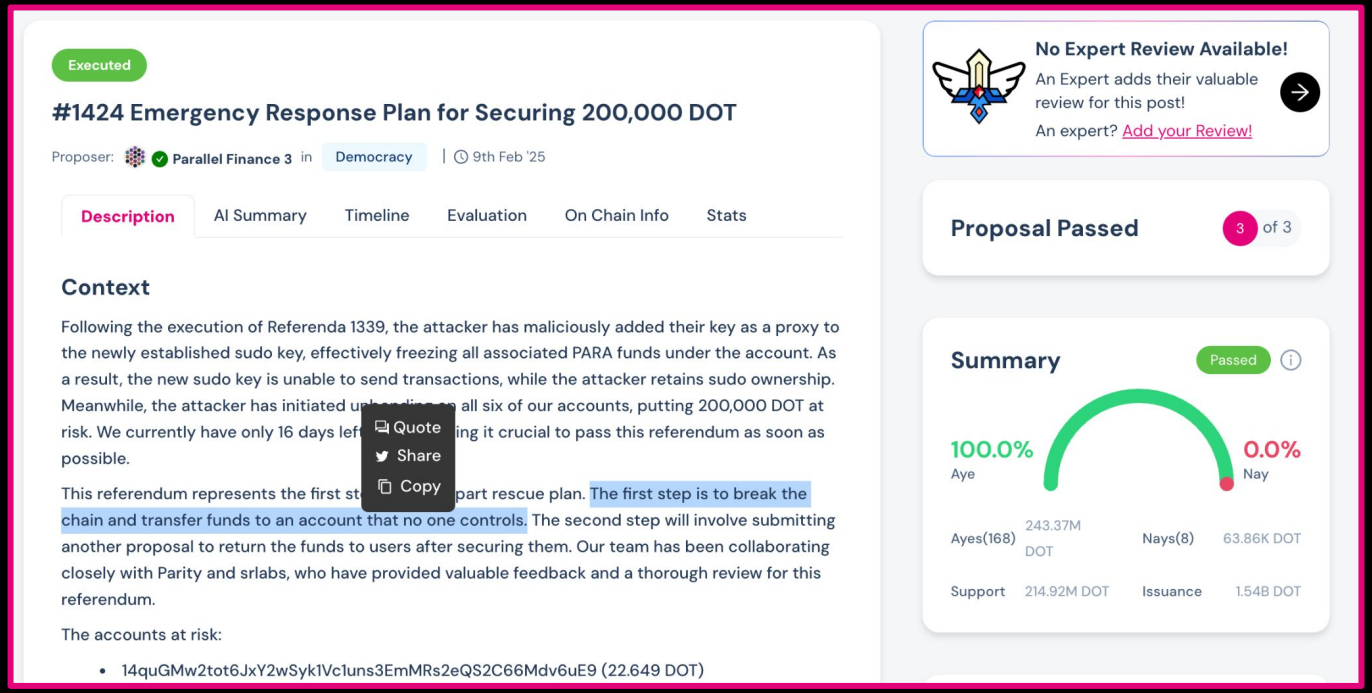
Back to the hack: did the community win?

Round 2:



Attacker outsmarted the solution from Round 1 😵‍💫

Parallel finance issues root proposal to break the chain!



They also began taking off-chain action

How to Recover Stolen Funds?

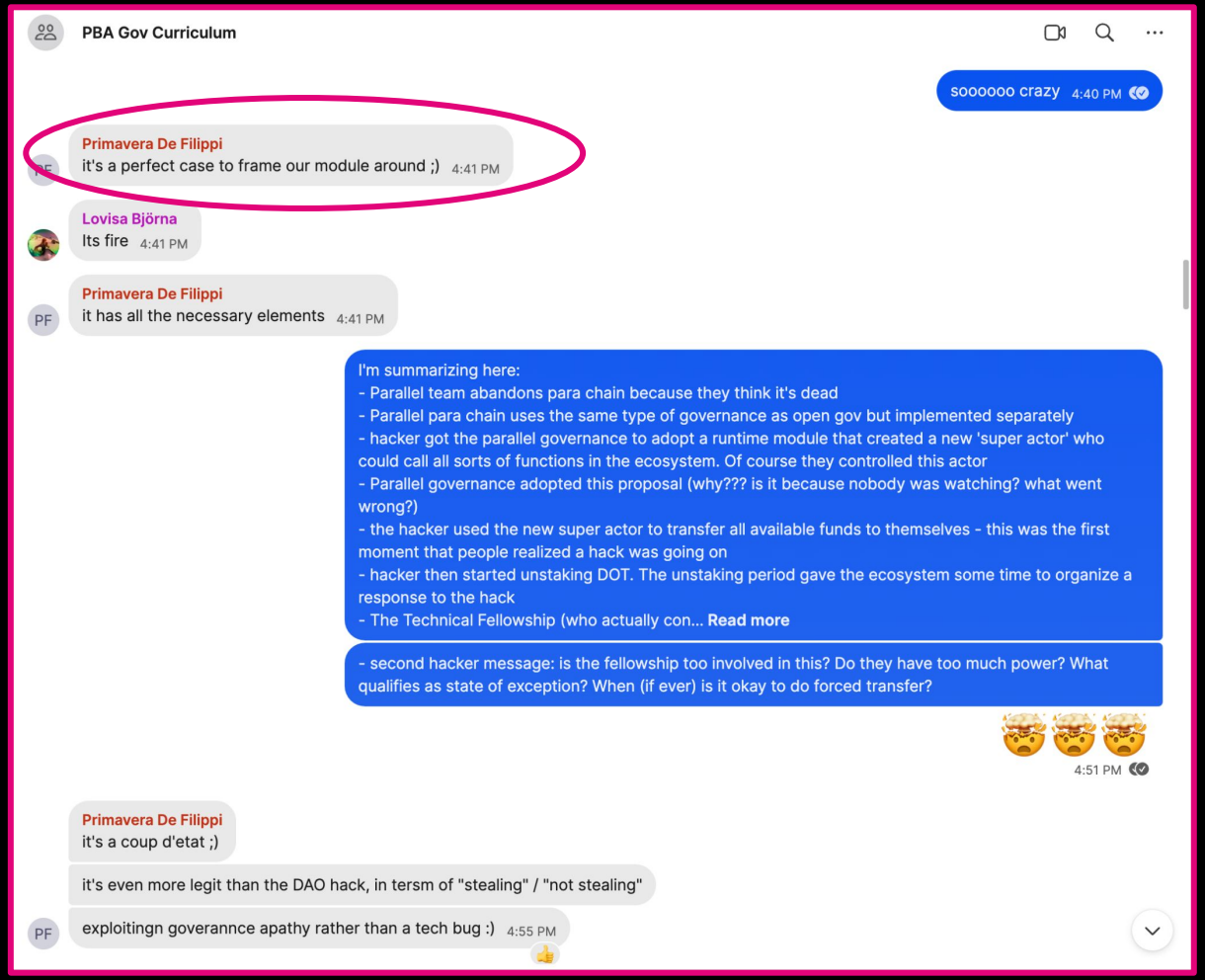
- **Exchange Blocking:** After collaborating with law enforcement and security firm, we successfully engaged over 55 exchanges to actively block and freeze funds from attacker's addresses. For full transparency, we includes an analysis from SlowMist.
- **Negotiation:** Despite multiple attempts to communicate with the attacker, we have received no response.
- **Law Enforcement:** Every action the attacker takes leaves a trail, and eventually, the net will close. A generous bounty will be offered for information that results in the attacker's capture.

The attacker had one more trick in store.

Via a less-known mechanism called “fast unstake” the attacker managed to unbond the funds **before the referendum was executed.** Leaving the community confused and sad...

Hacker: 3M USD
Parallel Finance: 0 USD

In summary


PBA Gov Curriculum
sooooo crazy 4:40 PM
Primavera De Filippi
it's a perfect case to frame our module around ;) 4:41 PM
Lovisa Björna
Its fire 4:41 PM
Primavera De Filippi
it has all the necessary elements 4:41 PM
I'm summarizing here:
- Parallel team abandons para chain because they think it's dead
- Parallel para chain uses the same type of governance as open gov but implemented separately
- hacker got the parallel governance to adopt a runtime module that created a new 'super actor' who could call all sorts of functions in the ecosystem. Of course they controlled this actor
- Parallel governance adopted this proposal (why??? is it because nobody was watching? what went wrong?)
- the hacker used the new super actor to transfer all available funds to themselves - this was the first moment that people realized a hack was going on
- hacker then started unstaking DOT. The unstaking period gave the ecosystem some time to organize a response to the hack
- The Technical Fellowship (who actually con... Read more
- second hacker message: is the fellowship too involved in this? Do they have too much power? What qualifies as state of exception? When (if ever) is it okay to do forced transfer?
4:51 PM
Primavera De Filippi
it's a coup d'etat ;)
it's even more legit than the DAO hack, in tersm of "stealing" / "not stealing"
exploitingn goverannce apathy rather than a tech bug :) 4:55 PM

Interesting aspects about this case

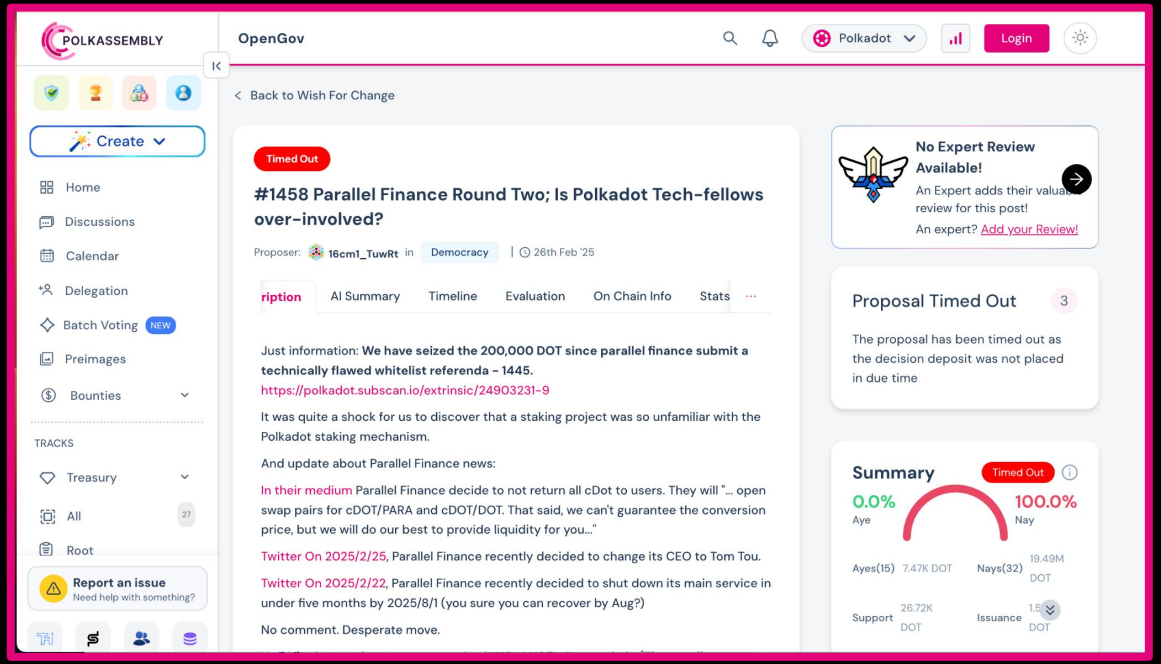
The Technical Fellowship **always had the ability to force-transfer the funds**—meaning they could have directly moved the stolen assets back to safety.

Instead, they **chose not to use this power**, opting instead to lock the funds and enable Parallel's governance to resolve the issue itself.

Notable is also that as a final statement the hacker **critizes the overinvolvement** of the technical fellowship.

Why would TF give such a generous response to a struggling parachain?

The blockchains immutability has **“not been respected.”**



What now?

The attacker is **still the owner** of the Parachain and the democracy and technical committee pallets are still disabled. Preventing any other actors from performing any upgrades.

Parallel's leadership resigned & deleted their governance records.

How much worth is ideological conviction?

Open questions

1. Should the Technical Fellowship have stepped in?
2. Was this hack wrong? It passed through governance correctly...
3. What mistakes allowed this to happen? Who's to blame? The team? The gov design (of Polkadot? Or Parachain)? The hacker? The community (who kept their tokens on Parallel)? The Technical fellowship?
4. What's the role of external agents (exchanges, law enforcement, etc)?
5. How could this be mitigated?
6. What would have been a good response to implement in the 28 day window period? Why? How?

BLOCKCHAINGOV

Governance Architectures

Layers, Stakeholders & Power Dynamics

Lecture 3

?

What is governance architecture?

Each layer of the blockchain serves a distinct purpose. — Layer 0 connectivity, Layer 1 manages the core protocol, Layer 2 enhances performance, and Layer 3 brings blockchain to users.

Governance architecture plays a key role across these layers, **guiding how changes are made**, **who participates in decisions**, and how **decentralized coordination is maintained.**

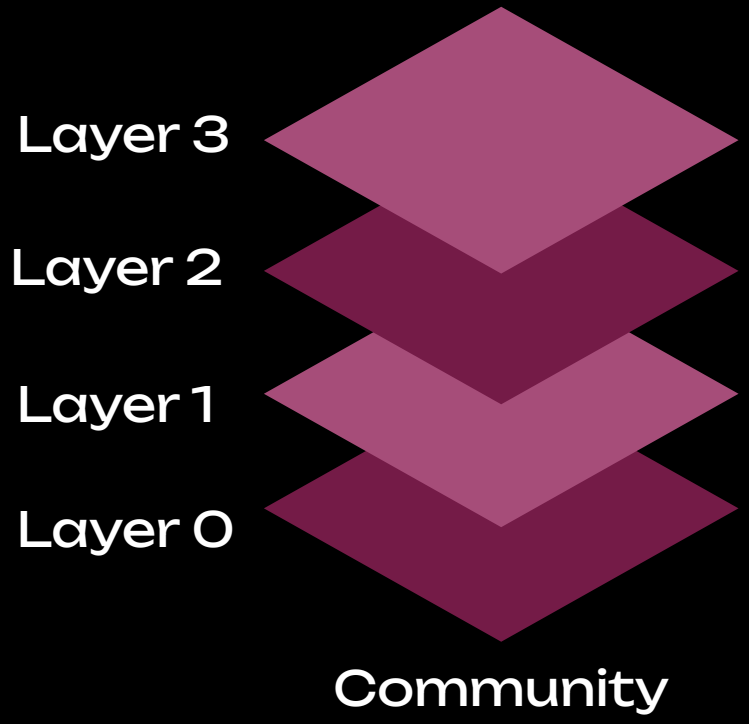
Layer 3: Smart contracts and dApps defining use-case logic.

Layer 2: Scalability & transaction management

Layer 1: Handles consensus, protocols, programming, and dispute resolution.

Layer 0 : Structures, stores, and governs access to on-chain data.

Community: Stakeholders shaping governance through norms and coordination.

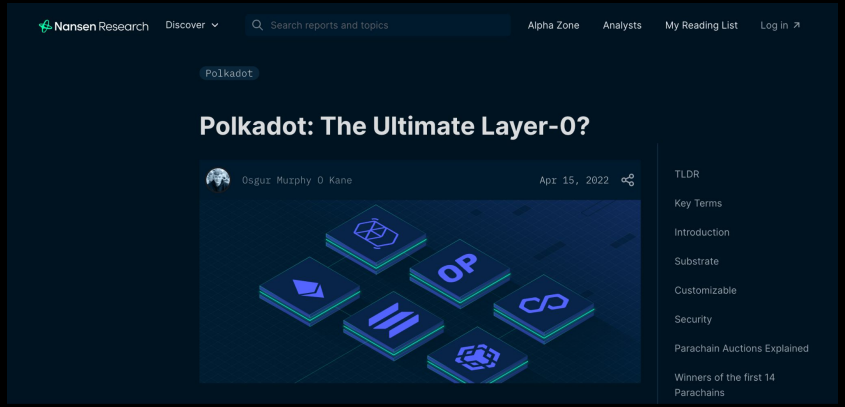


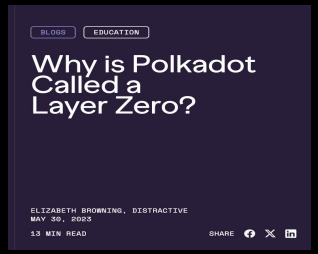
Where is governance enforced?

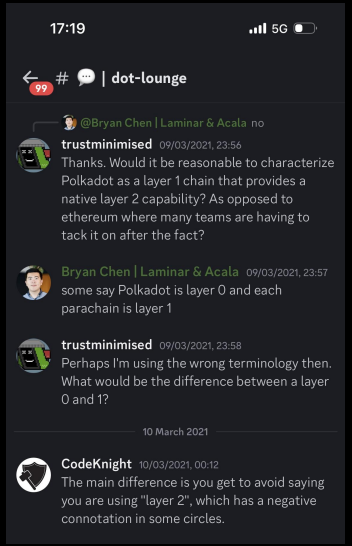
Each layer in the **blockchain stack** has its own set of stakeholders, influencing governance, security, development, and user adoption.

Understanding these stakeholders is crucial for **assessing power dynamics** and decision-making processes across decentralized ecosystems. (I.e. start understanding applied blockchain governance)

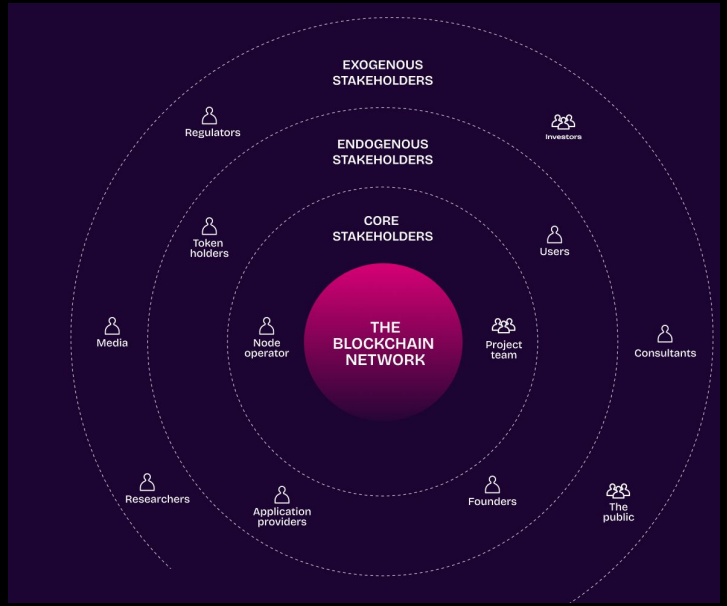
Polkadot as layer 0?







Who is involved in governance?



Who is involved in governance?

Layer 2, Layer 3
Sets dApp rules, manages app-level governance

Stakeholders	Decision rights	Accountability	Incentives
Project team	Platform development: Blockchain infrastructure setting; Consensus mechanism; Incentive mechanism; Project management: Conflict resolution rules; Formal communication channel; Onboarding & exit rules; Risk management.	Institutional means: Real-world identity verification; Traceable code contributors; Standardised documentation; Technical means: Address-based on-chain identity; Ledger-enabled operation logs.	Increase of market values; Block rewards; Transaction fees; Service fees.
Node operator	Replica storage; Block validation; Improvement proposal voting; Forking (instance installation).	Technical means: Address-based on-chain identity; Ledger-enabled operation logs; Institutional means: Real-world identity verification.	Block rewards; Transaction fees.
User	Transaction submission; Improvement proposal voting.	Technical means: Address-based on-chain identity; Ledger-enabled operation logs; Institutional means: Real-world identity verification.	Achievement of personal goals: Personal investment; On-chain trading; Data storage.
Application provider	Blockchain adoption; Improvement proposal voting. Onboarding & exit rules.	Institutional means: Real-world identity verification; Commercial agreement.	Increase of market values; Service fees.
Regulator	Risk assessment & measurement: Regulatory policy; Audit trail.	Institutional means: Legal regulation; Real-world identity verification; Technical means: Address-based on-chain identity; Ledger-enabled operation logs.	Taxes and fees.

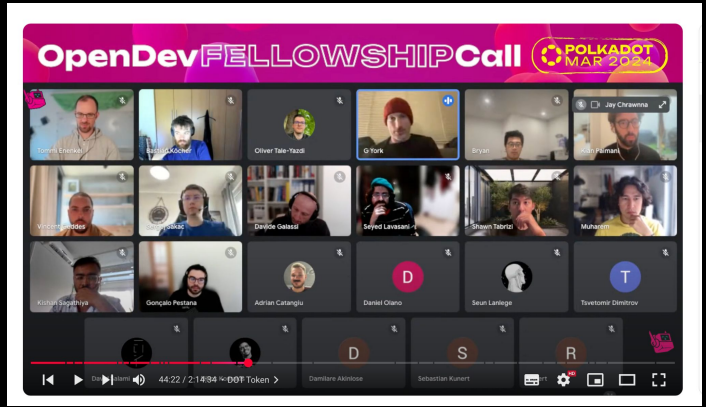
Stakeholder	Relevant Layers	Governance Impact
Developers	Layer 0, Layer 1	Propose and implement protocol upgrades
Validators / Miners	Layer 1	Enforce or vote on protocol changes
Token Holders	All Layers	Control treasury, governance outcomes via on-chain voting
App Builders / Protocol Teams	Layer 2, Layer 3	Set dApp rules, manage app-level governance
Users / Community Members	All layers	Influence through community input,
Foundations / Core Teams	All Layers	Initiate governance models, manage early direction

Who is involved in governance?

Blockchain governance must be viewed as an **ecosystem** where each stakeholder's decisions impact the others.

Decentralised coordination; no single actor has complete control.

Importance of **communication channels** for collaborative decision-making (e.g. on-chain voting, off-chain forums, social media, dev calls)



POLKADOT BLOCKCHAIN ACADEMY

Where is governance enforced?

Platform Layer: Core protocols, consensus rules, and infrastructure powering the blockchain.

Data Layer: Structures, stores, and governs access to on-chain data.

Application Layer: Smart contracts and dApps defining use-case logic.

Community Layer: Stakeholders shaping governance through norms and coordination.

Layer 0 Governance

- **Decisions Enforced:** Network architecture,Interoperability protocols, Validator coordination
- **Mechanisms:** Native token governance, Codebase updates, Off-chain coordination
- **Typical Stakeholders:** Core infrastructure developers,Foundations or ecosystem councils,Relay chain/node operators, Token holders (in interoperable Layer 0 platforms).

Layer 1 Governance

- **Decisions Enforced:** Consensus rules, Protocol upgrades. Network parameters
- **Mechanisms:** On-chain proposals, Token/validator voting, Client updates
- **Typical Stakeholders:** Core protocol developers,Validators / miners, Node operators, Token holders (with governance rights)

Layer 2 Governance

- **Decisions Enforced:** Rollup design,Settlement logic, Bridge/sequencer rules
- **Mechanisms:** Smart contract upgrades,Protocol DAOs, Community proposals
- **Typical Stakeholders:** Layer 2 dev teams,Sequencer operators or verifiers, Token holders (if applicable), users providing liquidity or staking

Layer 3 Governance

- **Decisions Enforced:** App features & logic, UI/UX decisions, Token economics.
- **Mechanisms:** App DAOs,Snapshot voting,Off-chain forums.
- **Typical Stakeholders:** App developers and designers, Community contributors and moderators, Token holders (platform-specific), End-users.

Platform Layer

- **Decisions Enforced:** Peer-to-peer communication rules, transaction propagation, network parameters (e.g., block propagation times).
- **Mechanisms:** Client implementations, network-level policies.
- **Typical Stakeholders:** Developers, node operators, infrastructure partners.

Data Layer

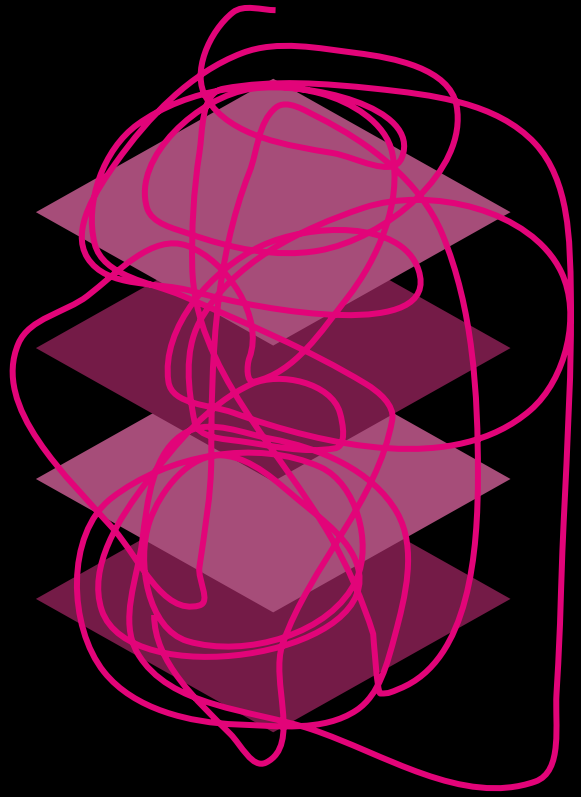
- **Decisions Enforced:** Rules encoded in contracts (token standards, governance tokens, DeFi protocols).
- **Mechanisms:** On-chain voting (DAO governance), permission settings in smart contracts.
- **Typical Stakeholders:** dApp developers, token holders, end-users.

Communication

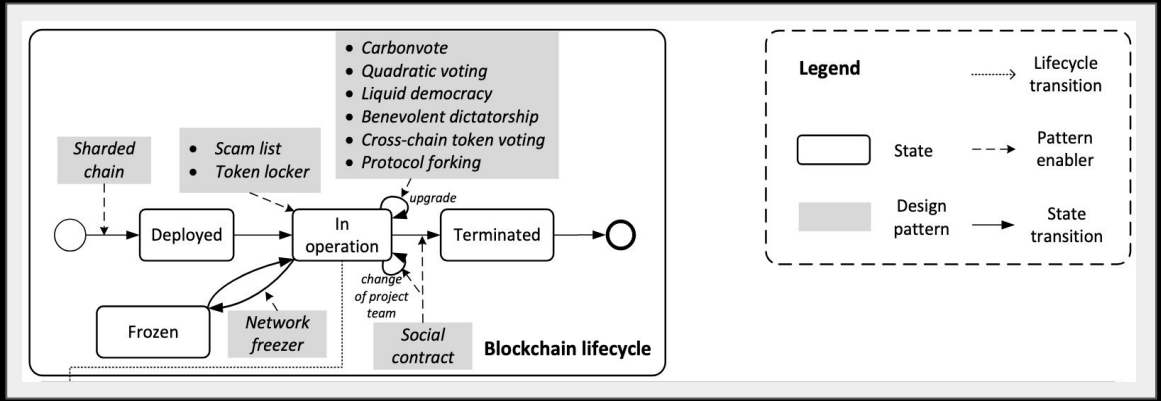
- **Decisions Enforced:** Peer-to-peer communication rules, transaction propagation, network parameters (e.g., block propagation times).
- **Mechanisms:** Client implementations, network-level policies.
- **Typical Stakeholders:** Developers, node operators, infrastructure partners.

Community Layer

- **Decisions Enforced:** Community standards, marketing strategies, ecosystem funding, conflict resolution.
- **Mechanisms:** Social media, forums, dev meetings, conferences, legal/regulatory frameworks.
- **Typical Stakeholders:** Entire community, external regulatory bodies, foundations, influencers. + Any other way you can think of people getting together and scheming.



When is governance applied?



Exercise

Step 1 : Make a list of all the stakeholders and their roles in the Parallel hack

Step 2: Group them into categories of:

- Exogenous / Endogenous
- What layer are they operating on?
- Categorize them by level of power in two categories:

1. **Most powerful on paper**

2. Most powerful in practice

BLOCKCHAINGOV

Governance Mechanisms & Trade-Offs

Lecture 4

Tara Merk

Designing blockchain governance is like creating the perfect recipe

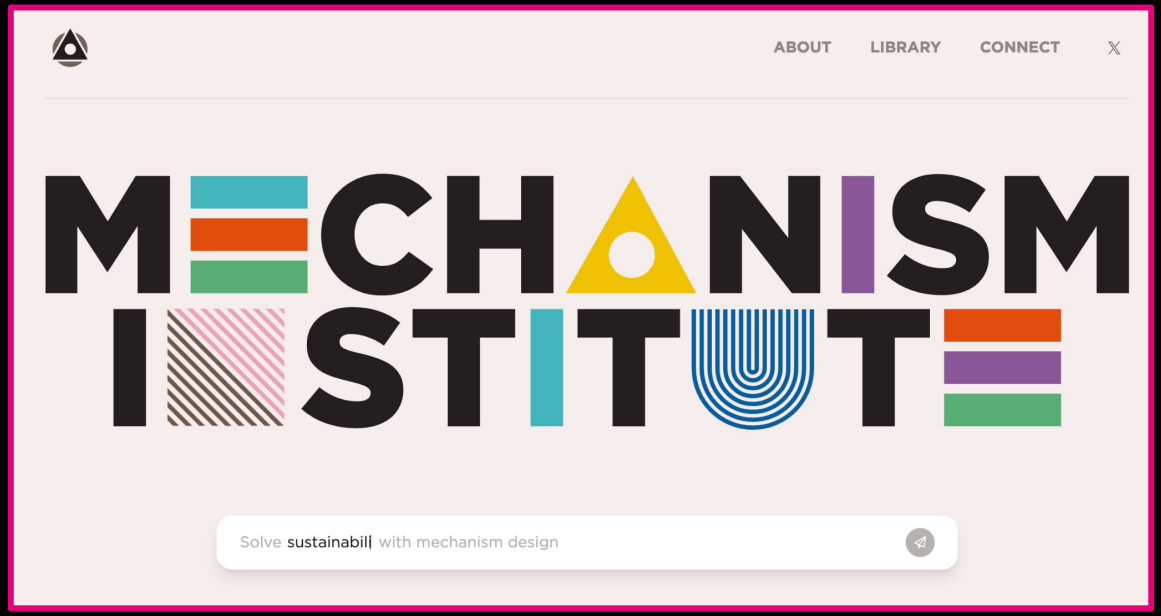
POLKADOT BLOCKCHAIN ACADEMY

Governance mechanisms are like the ingredients to a tasty dish

Depending on the ingredients you chose
you will get different flavors

POLKADOT
BLOCKCHAIN
ACADEMY

What ingredients are available?



Check out the MI library to get a glimpse of what's out there

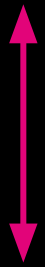
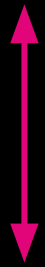
POLKADOT BLOCKCHAIN ACADEMY

Mechanisms affect different aspects of governance design

Product mechanism

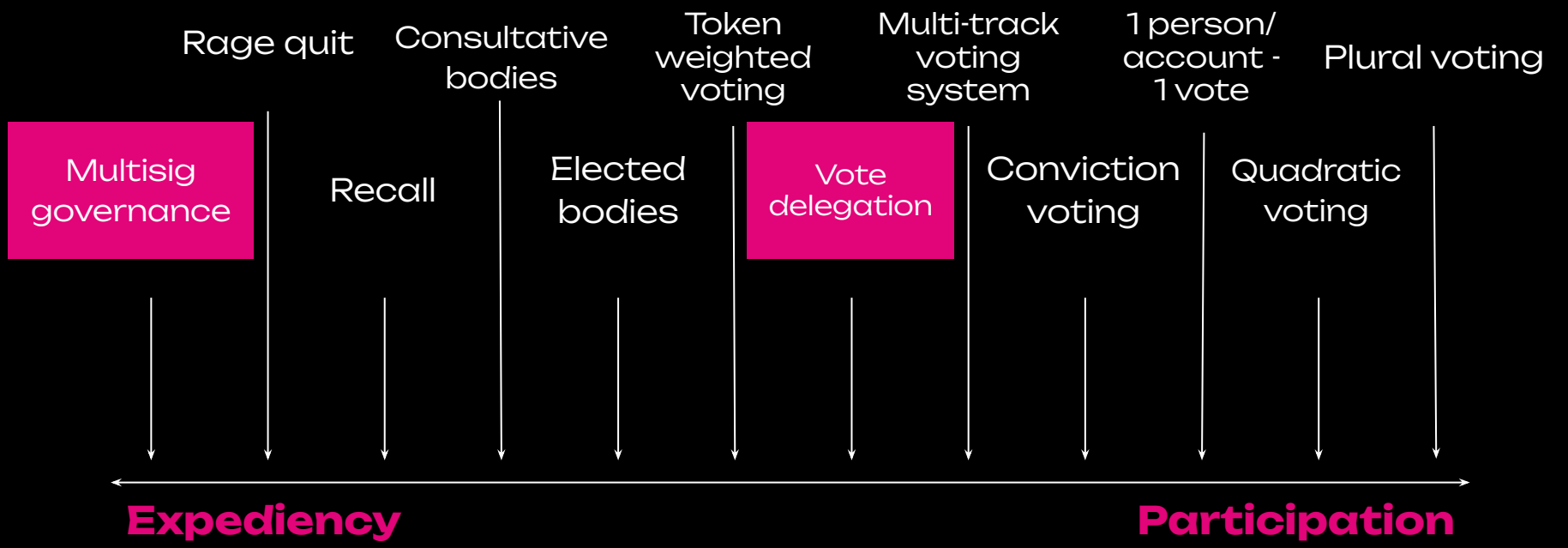
Process mechanism

Different mechanisms also create different flavors of governance

Expediency	Immutability	Determinism
		
Participation	Adaptability	Discretion

POLKADOT BLOCKCHAIN ACADEMY

Pick your ingredients



POLKADOT BLOCKCHAIN ACADEMY

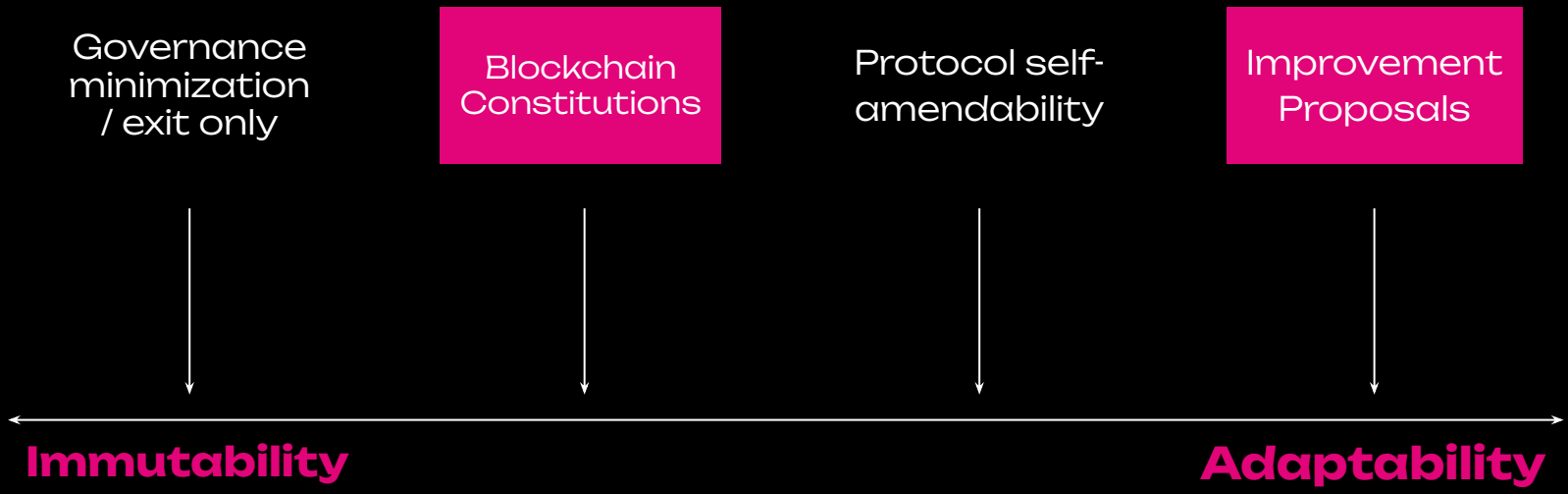
Case study: Multisig governance

Example: Polygon Protocol Council emergency updates

Case study: Vote delegation

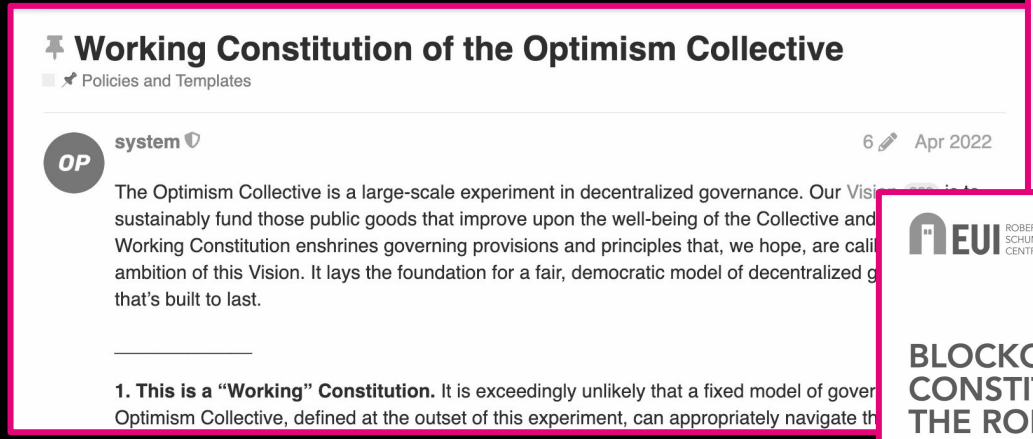
Example: Cardano's DRep system

2: Pick your ingredients



POLKADOT BLOCKCHAIN ACADEMY

Case study: Blockchain constitutionalism



Example: Optimism's working constitution

POLKADOT BLOCKCHAIN ACADEMY

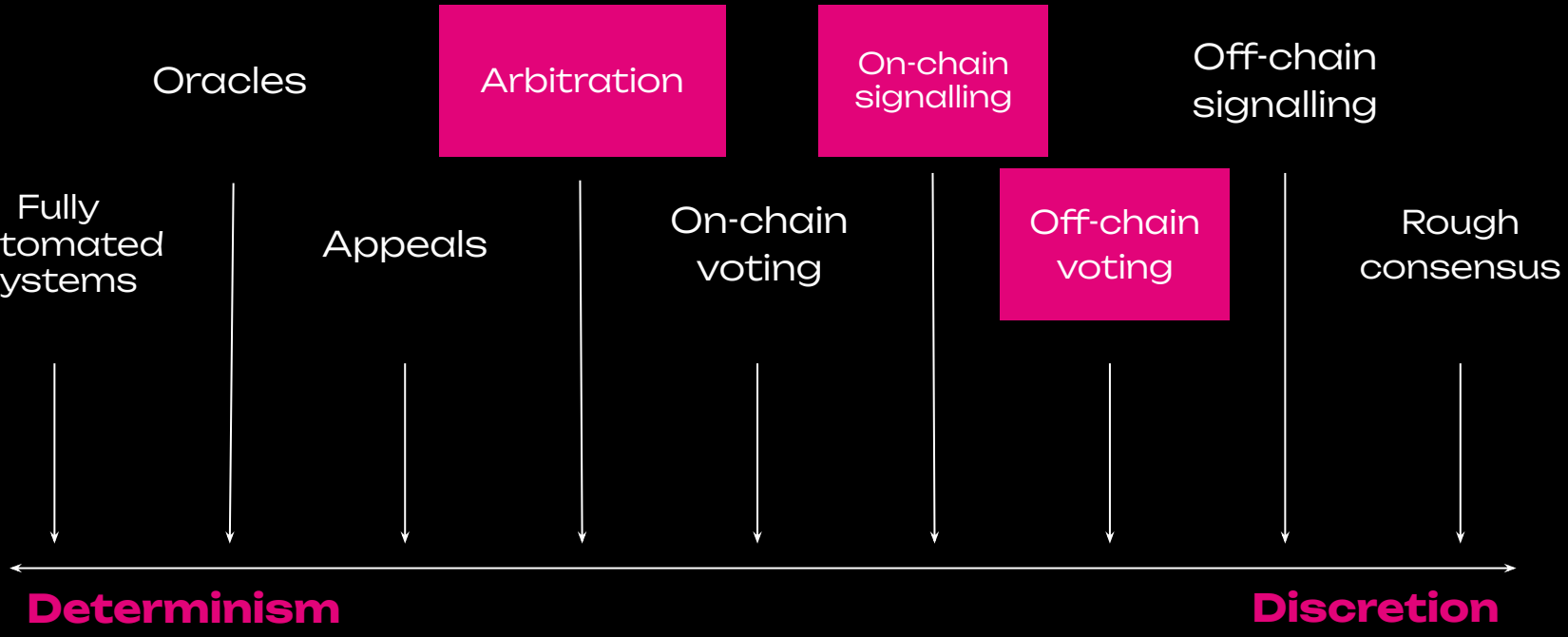
Case study: Improvement proposals

```
BIP: 1
Title: BIP Purpose and Guidelines
Author: Amir Taaki <genjix@riseup.net>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BI
Status: Replaced
Type: Process
Created: 2011-09-19
Superseded-By: 2
```

Example: BIPs and EIPs

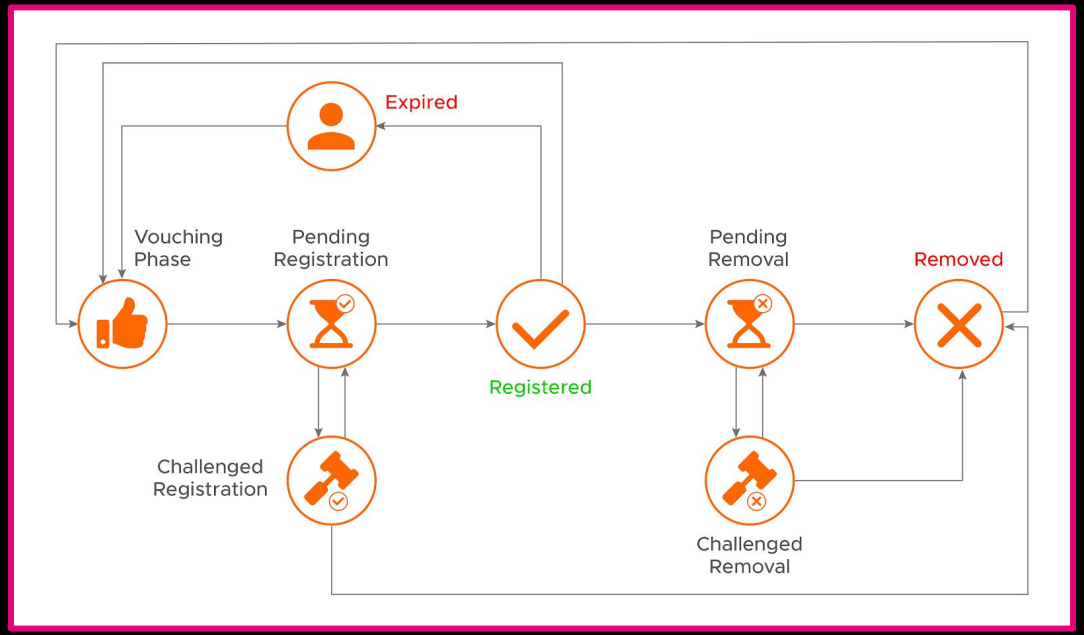
POLKADOT BLOCKCHAIN ACADEMY

2: Pick your ingredients



POLKADOT BLOCKCHAIN ACADEMY

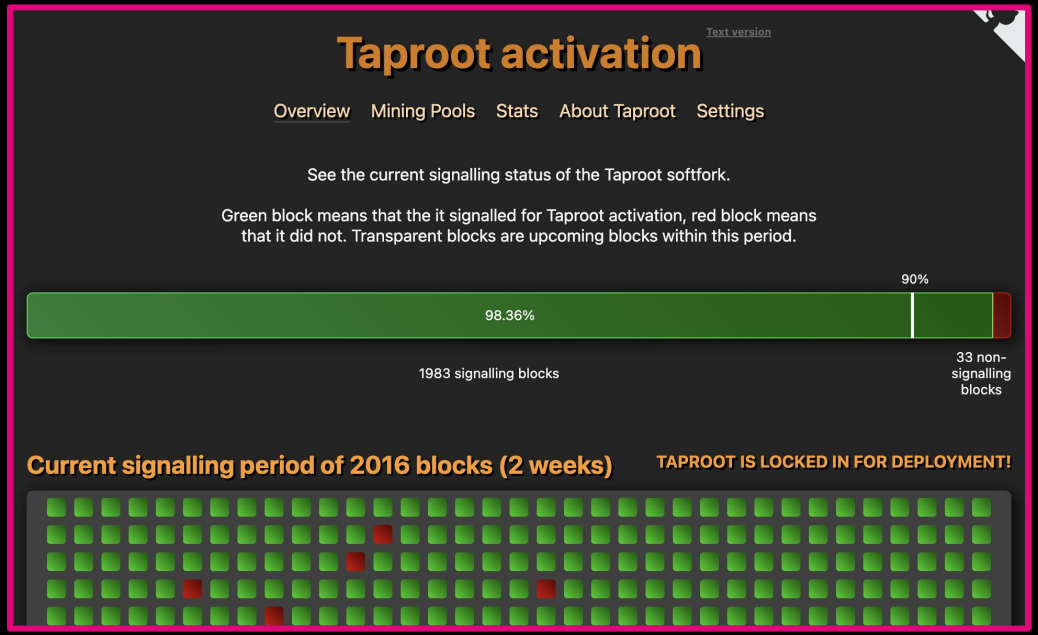
Case study: Arbitration



Example: Proof of Humanity Courts

POLKADOT BLOCKCHAIN ACADEMY

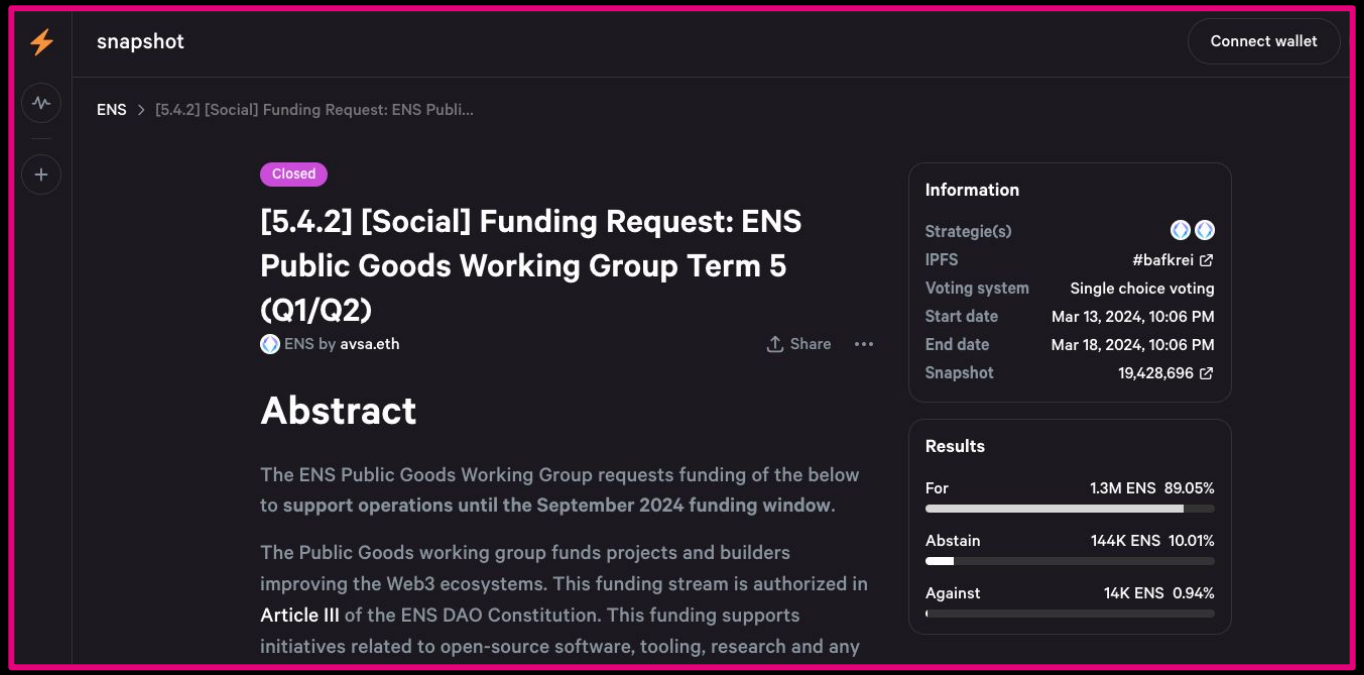
Case study: On-chain signalling



Example: Bitcoin miner signalling

POLKADOT BLOCKCHAIN ACADEMY

Case study: Off-chain voting



Example: Snapshot

POLKADOT BLOCKCHAIN ACADEMY

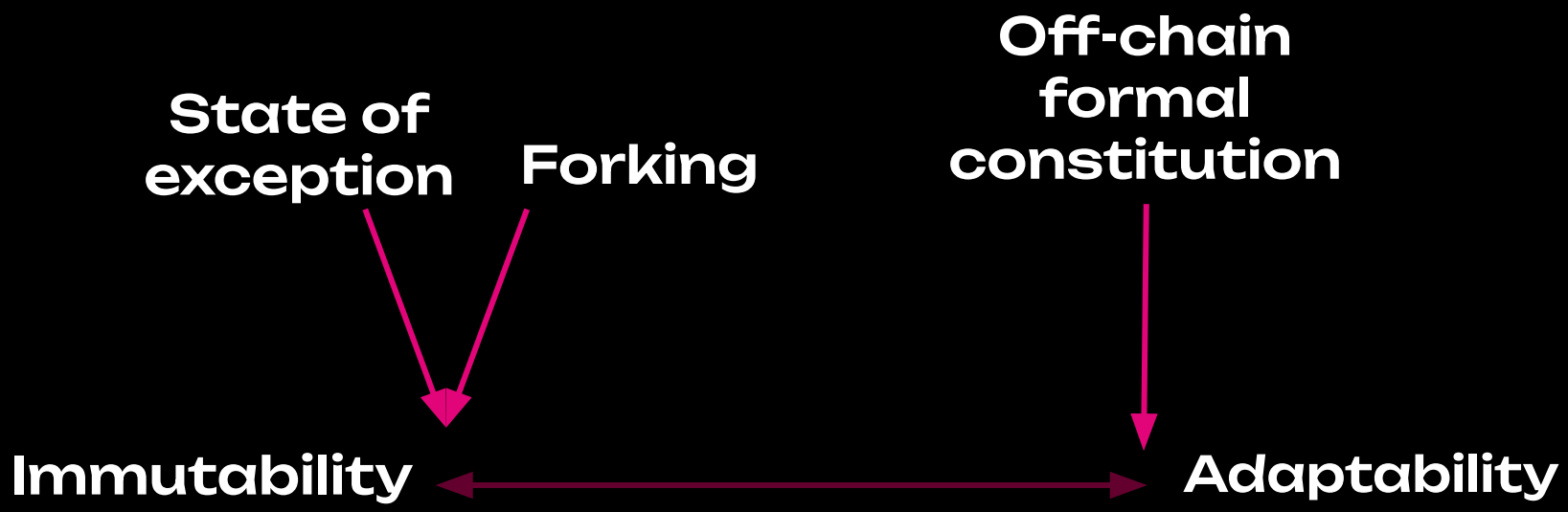
Blockchain governance secret sauce

POLKADOT BLOCKCHAIN ACADEMY

Keep strong flavors in check

POLKADOT BLOCKCHAIN ACADEMY

Keep strong flavors in check



Keep strong flavors in check

Exercise

1. Which mechanisms were exploited in this hack? Are they more product or process oriented?
2. Which mechanisms could have prevented this attack? Which mechanisms could have reduced its severity?
3. Would it be desirable to implement such mechanisms? Why? Why not?
4. Argue your case and let's vote!

BLOCKCHAINGOV

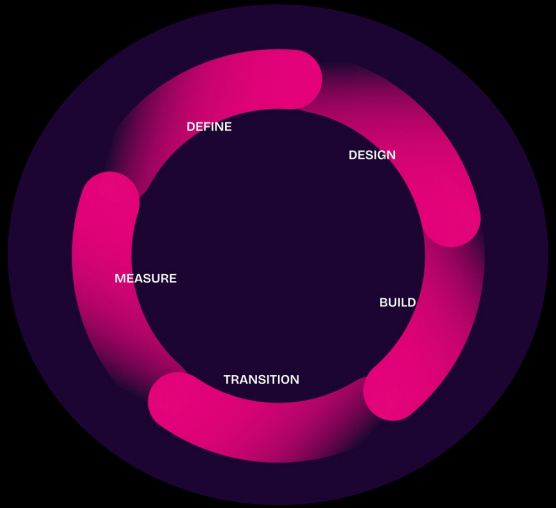
Governance Lifecycle

Lecture 4

Felix Beer

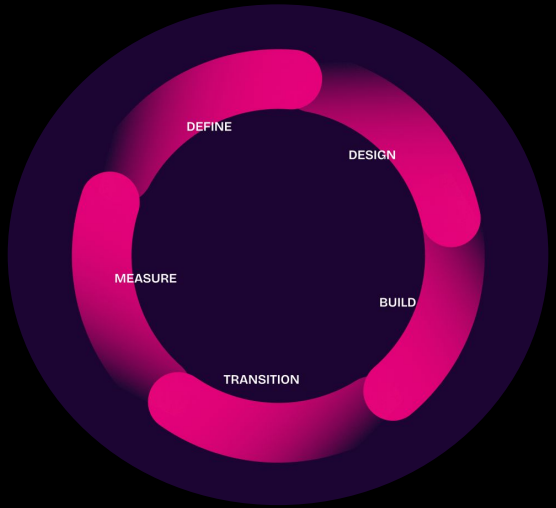
The lifecycle perspective

- A strategic framework for structuring governance intervention in distinct phases.
- A lens similar to agile product management.
- An iterative approach focused on continuous learning and adaptation.



The lifecycle stages

1. Problem Identification & Agenda Setting
2. Proposal Drafting
3. Consensus Building
4. Implementation & Deployment
5. Monitoring & Evaluation
6. Iteration or Sunset



1. Identify problem

Problem Scoping: Identify governance challenges (e.g., security risks, low voter engagement, lack of protocol sustainability).

Stakeholder Input: Engage the community to understand diverse perspectives and priorities.

Agenda Setting: Prioritize governance issues based on impact, feasibility, and urgency.

2. Draft proposal

Drafting the Proposal: Outline the problem, goals, intervention details, implementation plan, and expected impact.

Expert Consultation: Validate technical, legal, and economic implications with domain experts.

Community Review: Open proposal for discussion and feedback on governance forums or DAOs.

3. Build Consensus

Proposal Submission: Submit the refined proposal to the appropriate governance process (e.g., DAO vote, core dev consensus, on-chain referendum).

Discussion & Debate: Encourage constructive debate to surface trade-offs, risks, and alternative solutions.

Voting Process: Conduct formal governance voting (e.g., token-based voting, reputation-weighted voting, council decisions).

4. Deploy Solution

Technical Development: Implement changes in code (for protocol updates) or governance structures (for governance rule changes).

Security Audits: Conduct extensive testing (e.g., testnets, simulations, code reviews) to prevent unexpected failures.

Progressive Deployment: Use phased rollouts, upgrade coordination, and back-out mechanisms to ensure stability.

5. Monitor Outcomes

Impact Assessment: Analyze key performance indicators (KPIs) and real-world effects of the intervention.

Stakeholder Feedback:

Continuous Learning: Document lessons learned for future governance improvements.

6. Iterate or Terminate

Iterative Refinement: If unintended consequences arise, prepare new governance proposals to fix or improve the intervention

Sunsetting Changes: If the intervention is no longer useful, governance mechanisms should allow for deprecation or removal.

Governance Evolution: The governance process itself may need adaptations based on learnings from past decisions.

Exercise

BLOCKCHAINGOV

Blockchain
Legality & Regulation

Lecture 6

Primavera de Filippi

“No Blockchain is an Island”

New avenuesfor ~~regulation~~? intervention

2 TYPES OF EQUIVALENCE:

FUNCTIONAL EQUIVALENCE

*As regards the tools available to comply with specific **legal rules** (e.g. electronic contracts, e-sig)*

REGULATORY EQUIVALENCE

*As regards the means available to achieve a **regulatory objective** (e.g. lower risks, transparency)*

Functional Equivalence

Functional equivalence allows the establishment of equivalence between two technological artefacts:

- *One that is already covered within the realm of a legal rule*
- *Another that is not (yet) encompassed by it (e.g., written signatures and electronic signatures).*

Regulatory Equivalence

Regulatory equivalence establish the equivalence between:

- *the policy objectives of specific legal provisions, and*
- *the implications of adopting a particular technological artefact as an alternative way to achieve regulatory compliance.*

FUNCTIONAL EQUIVALENCE

Applying existing legal rules

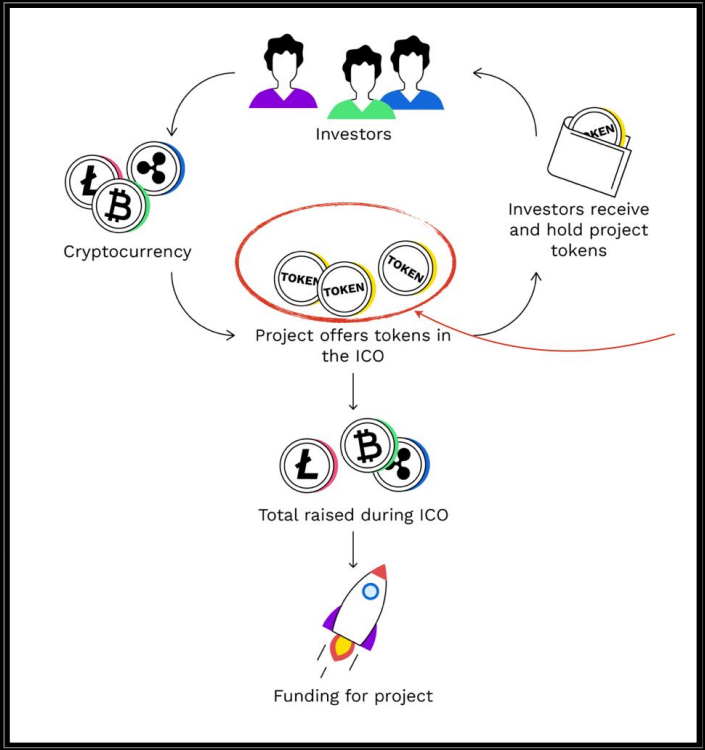
to novel technologies that serve equal functions

Initial Coin Offering

IPO vs. ICO

- Issue shares of a company
- Centralized by stock exchange
- Heavy regulated by authorities

- Issue cryptocurrency tokens
- Operated via a smart contract
- Unregulated ?



Legal Qualification ?

Legal qualification must take into account:

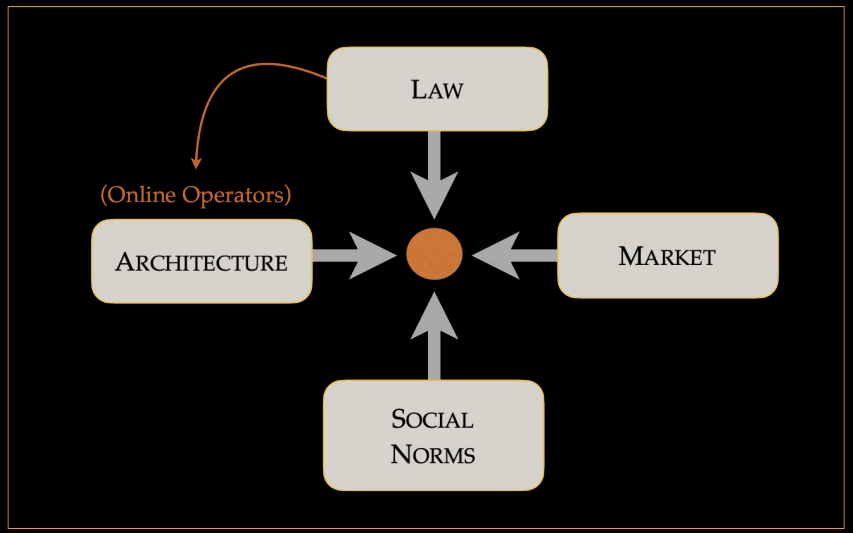
- *the original function of the token (why it was issued)*
- *the practical applications of that token (beyond the control and intention of the issuer)*

Functional Equivalence

Many tokens usually qualify as multiple classes:

- Payment tokens
- Utility tokens
- Governance tokens
- Investment tokens
- Asset-backed tokens

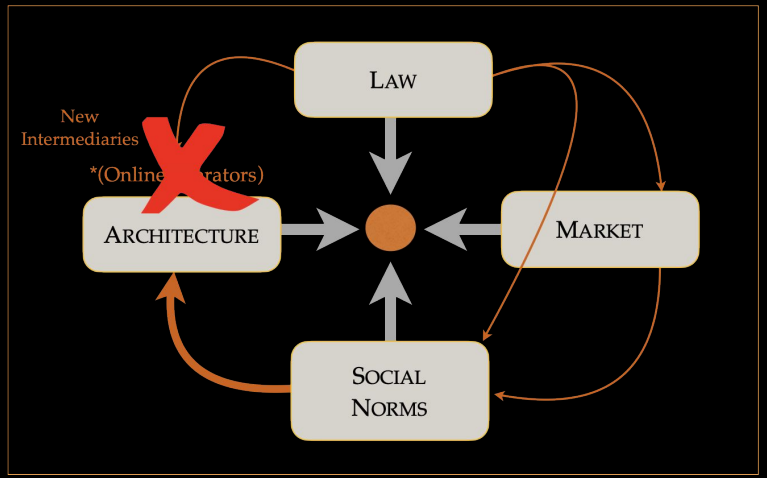
4 Levers of **Regulation** On the Internet



Lawrence Lessig

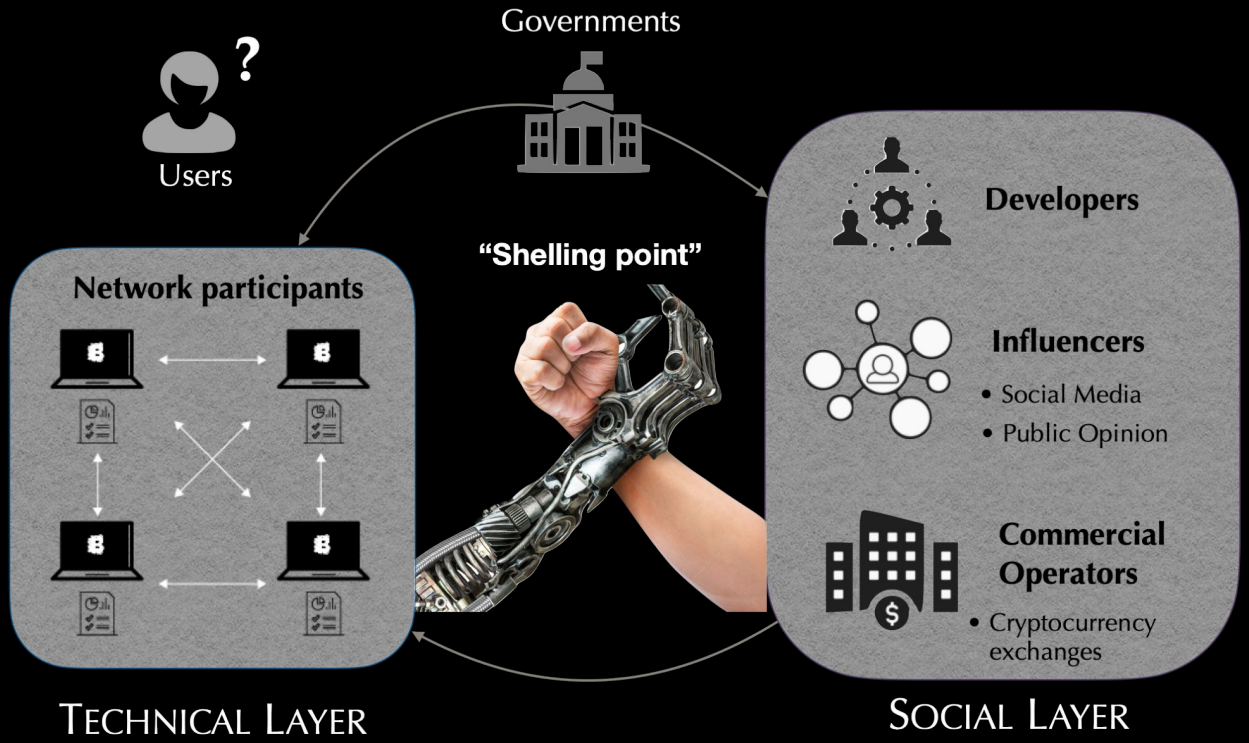
Code: And Other Laws of Cyberspace (New York: Basic Books, 1999), 123

4 Levers of **Regulation** on the Blockchain



Lawrence Lessig
Code: And Other Laws of Cyberspace (New York: Basic Books, 1999), 123

Blockchain between Regulation & Governance



Users

Criminalisation

- Prohibit the use of a particular blockchain
- Prohibit the use of specific blockchain apps
- Legal liability for providing financial resources to illicit applications deployed on a blockchain.

Limitations

- Problematic (cf. online piracy)
- Transnationality of blockchain networks
- Pseudonymity of users

Old Intermediaries

Internet Access Providers

- Obligation to filter Internet traffic (e.g. China)
- Slow down traffic towards a specific blockchain

Infomediaries

- De-referencing of illicit blockchain apps
- No advertisement for these apps (e.g. ICOs)

New Intermediaries

Cryptocurrency Exchanges and Commercial Operators

- Obligation to comply with regulatory constraints
- Possible to block or censor specific transactions

Mining Pools Miners

- Obligation to ignore / censor specific transaction
- Economic incentives (e.g. taxation)

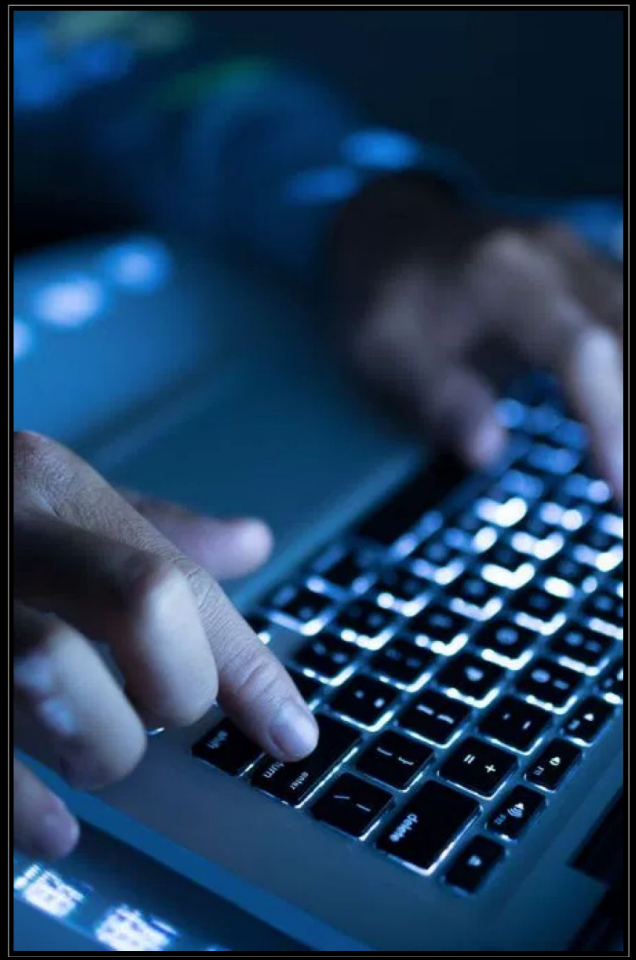
Developpers

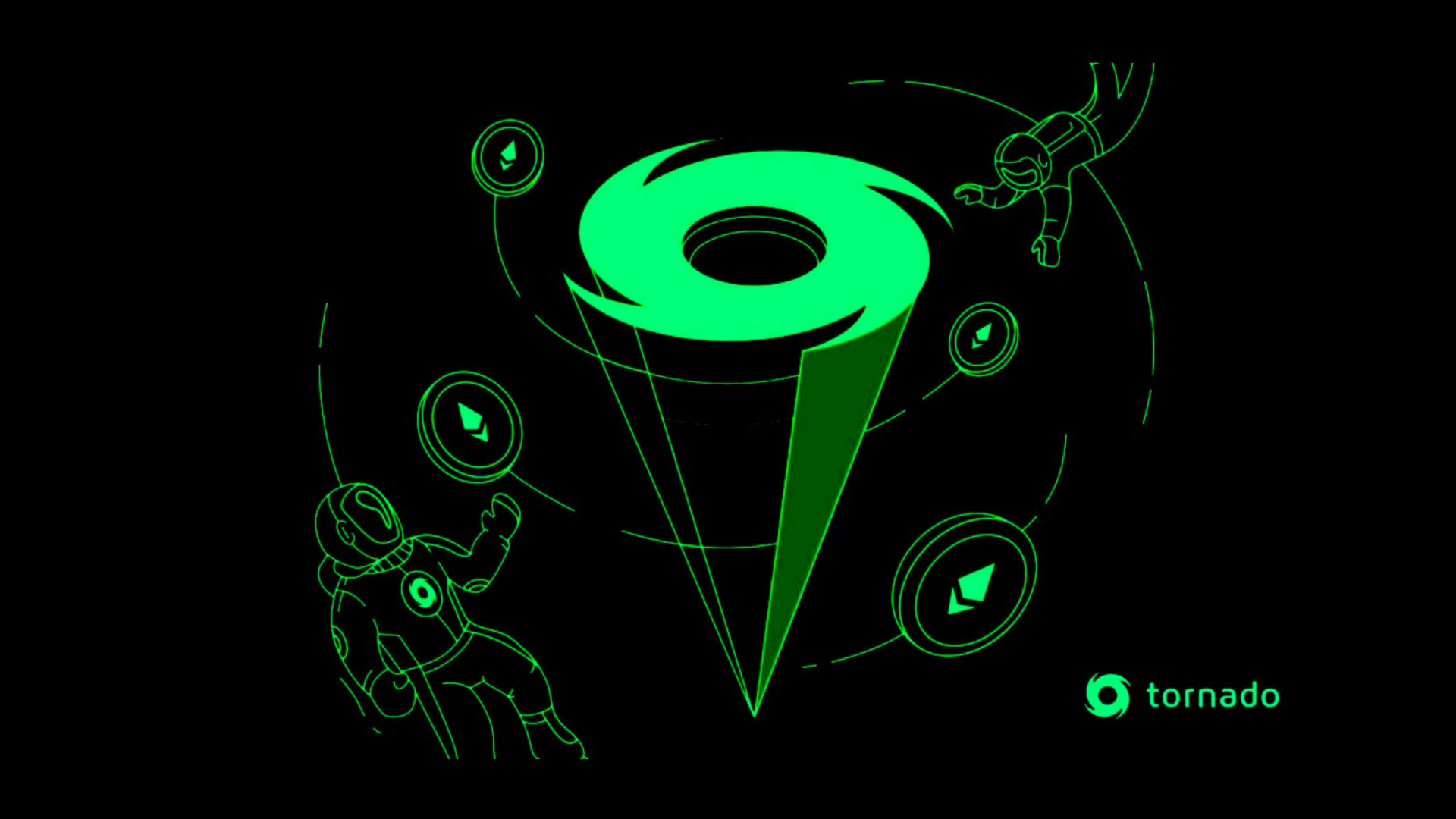
Backdoors

- Obligation to introduce *backdoors* in the code in order to provide "veto right" to public authoriies
  - Loss of guarantees of execution
  - Risk of creating new vulnerabilities

Fiduciary Liability Regime

- *Fiduciary duties* towards users (Walsch)
  - Could jeopardise the liability regime of OpenSource
- *Vicarious liability for illicit applications*
  - Visa's for registering legitimate applications?
  - Risk of encouraging the anonymity of apps



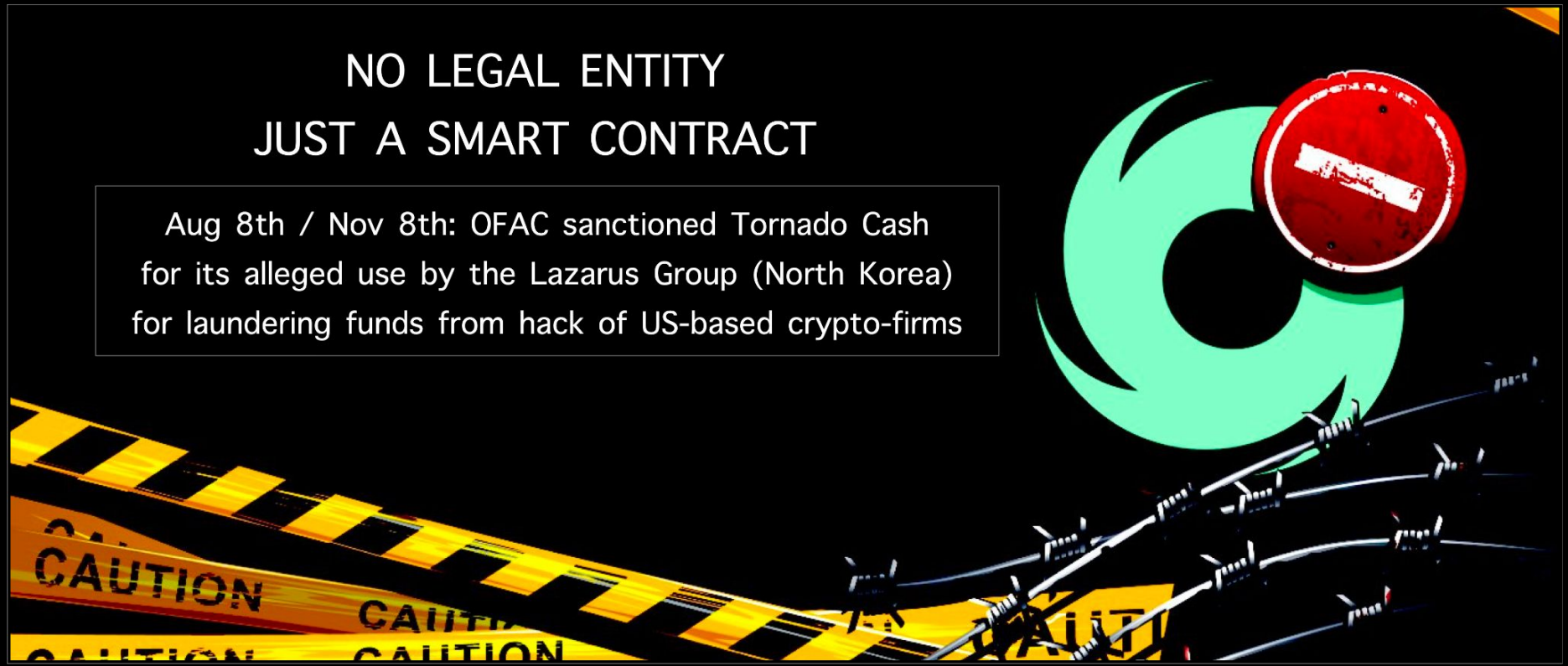

tornado

OFAC Sanctions

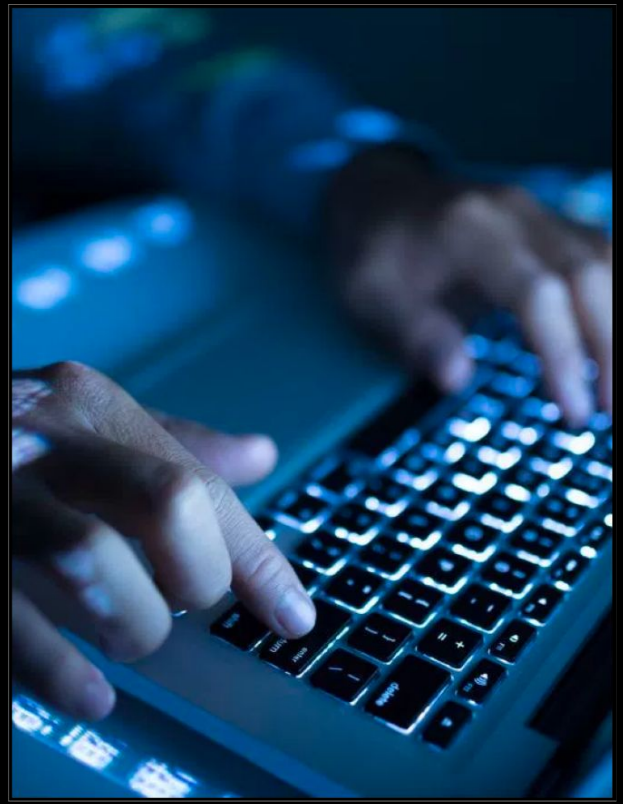
NO LEGAL ENTITY

JUST A SMART CONTRACT

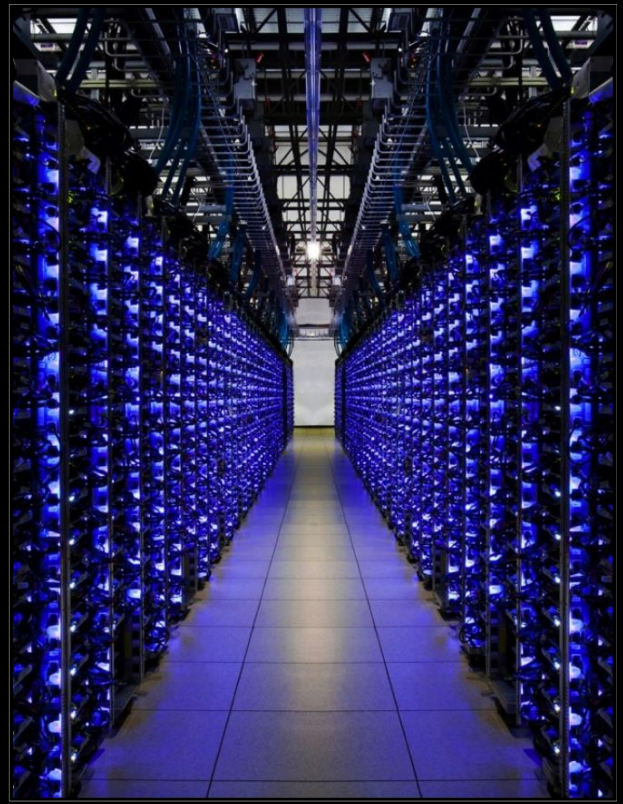
Aug 8th / Nov 8th: OFAC sanctioned Tornado Cash
for its alleged use by the Lazarus Group (North Korea)
for laundering funds from hack of US-based crypto-firms



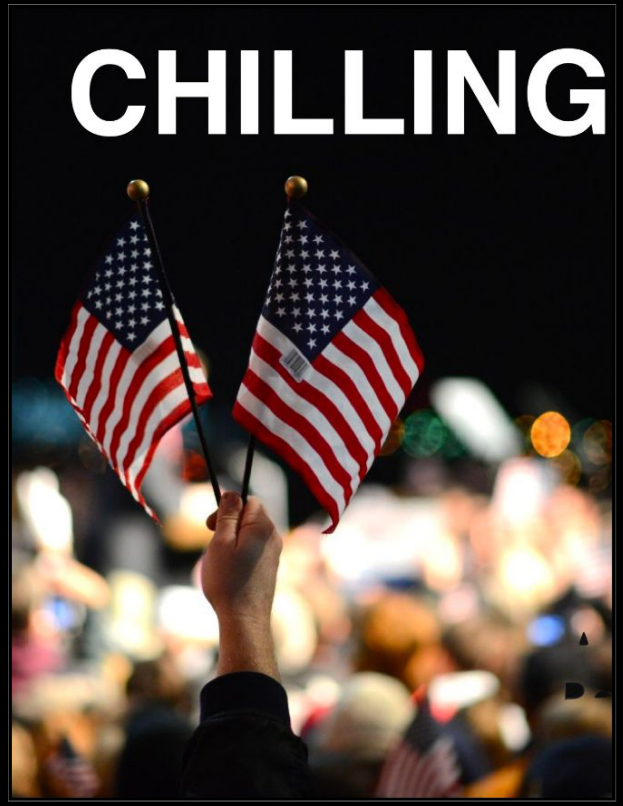
U.S. Persons
(Strict liability)



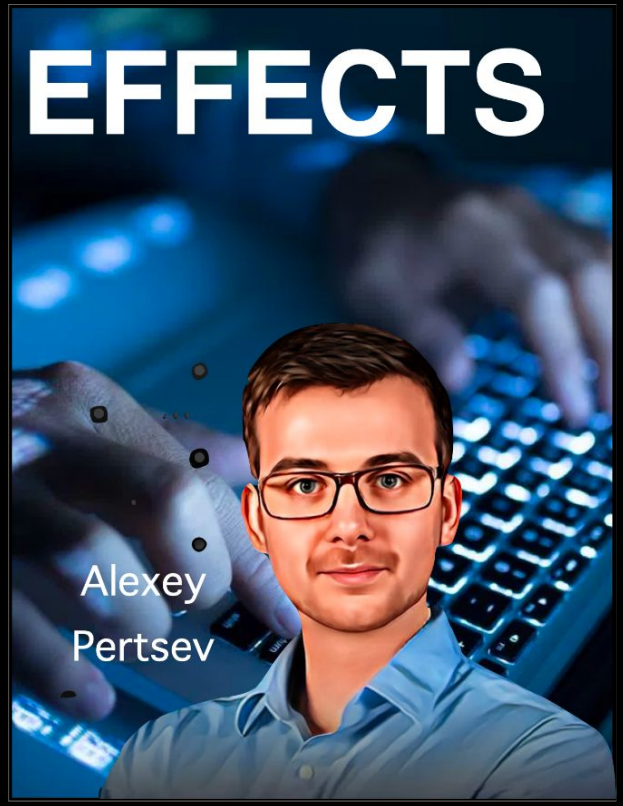
Core Developpers
(Legitimate vs illegitimate uses)



Miners and Validators
& Crypto-exchanges
(Vicarious liability)

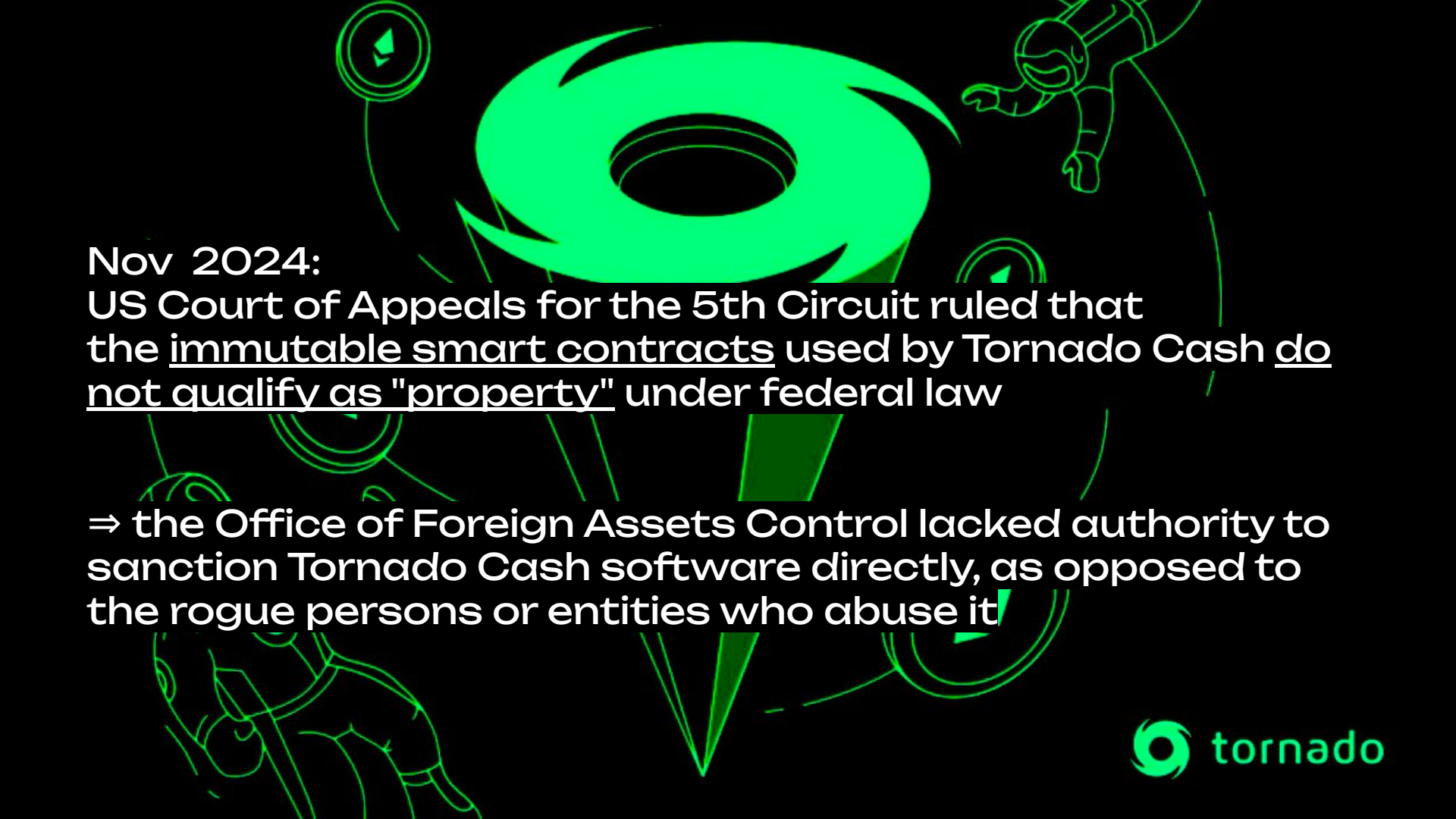


U.S. Persons
(Strict liability)



Core Developpers
(Legitimate vs illegitimate uses)

Miners and Validators
& Crypto-exchanges
(Vicarious liability)



Nov 2024:
US Court of Appeals for the 5th Circuit ruled that the immutable smart contracts used by Tornado Cash do not qualify as "property" under federal law

⇒ the Office of Foreign Assets Control lacked authority to sanction Tornado Cash software directly, as opposed to the rogue persons or entities who abuse it

tornado

Exercise

Exogenous governance of Parallel Finance

1.-How can governments prevent / dissuade / punish

2. -What avenues for regulation?
    - - Law ?
    - - Market mechanisms ?
    - - Social norms ?
    - - Tech infrastructure ?
3. - Who are the actors that can exert pressure ? On whom ?

POLKADOT BLOCKCHAIN ACADEMY

Regulatory Equivalence

From Legal Constraints
to Technical Guarantees

"Don't trust, Verify"

Regulatory Equivalence

*Goal is to **alleviate the regulatory burden** on specific tech solutions*

by demonstrating their ability to achieve specific regulatory objectives

*through **technological guarantees** rather than paper-based formalities.*

Principle-based Regulatory Approach

Security laws designed to limit the risk of investors in investment contracts

From a Regulatory Equivalence perspective:

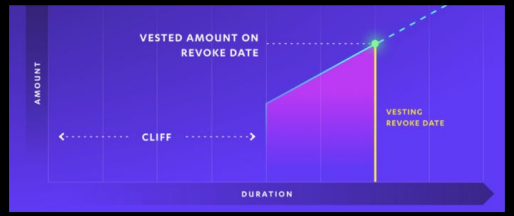
★ similar risks should be treated in a similar manner

- If ICOs pose similar risks to IPOs (in degree and in kind), they should be subject to similar laws

- If they don't want to fall within existing regulations ICOs must provide lower risks than IPOs

- Escrow System

Progressive disbursing of funds based on Milestones, so that both investors and token issuers are protected



- Locking / Vesting periods

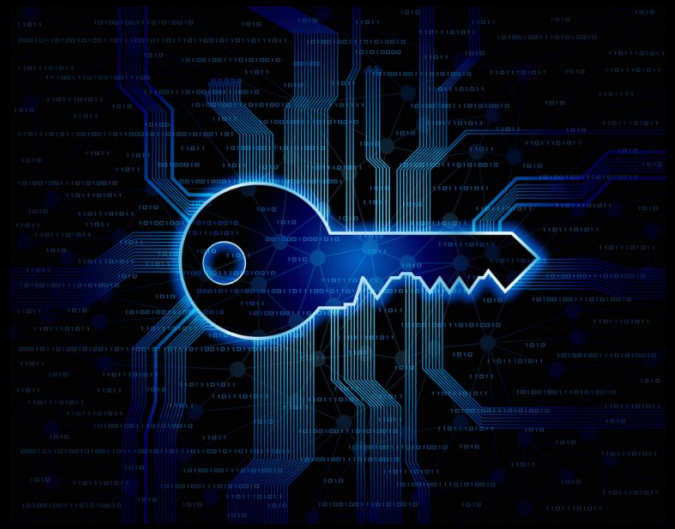
(1) Ensure the alignement of management team and investors with long-term success

(2) Prevents ppl to engage into speculative practices such as "pump and dump".

- Speculative capping

e.g. by offering a constant supply of tokens at pre-determined price (decided by smart contract) regardless of current market price

Technical Accountability



Keyless Wallets

—NO CUSTODY—

Provide service to customers without holding their funds
Thus removing counter-party risks of centralised entity

Proof of Reserve

—REAL-TIME AUDITING—

Prove the full reserve of funds in custody
reducing the need for additional audits.

Regulatory Compliance

Real Time Audits

Identity Management

Automated Reporting

Guarantee of Execution

Exercise

BRAINSTORMING

1.- Other examples of regulatory equivalence ?
2.- What are the technological guarantees of blockchain that can contribute to better regulatory compliance?
3.- What are the challenges that blockchain systems meet when trying to comply with regulations designed for centralised entities?

(try to apply it to the case study)

POLKADOT BLOCKCHAIN ACADEMY

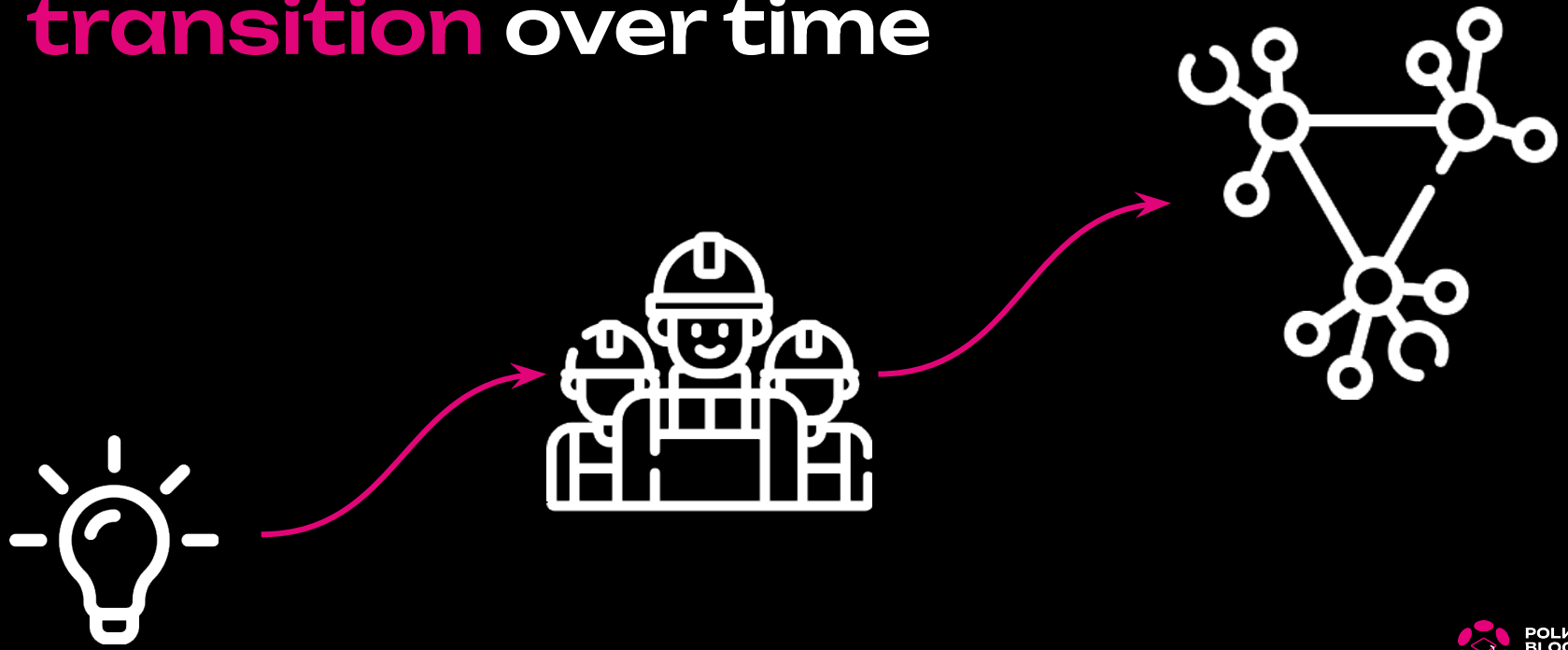
BLOCKCHAINGOV

(Progressive) Decentralization & Exit to Community

Lecture 7

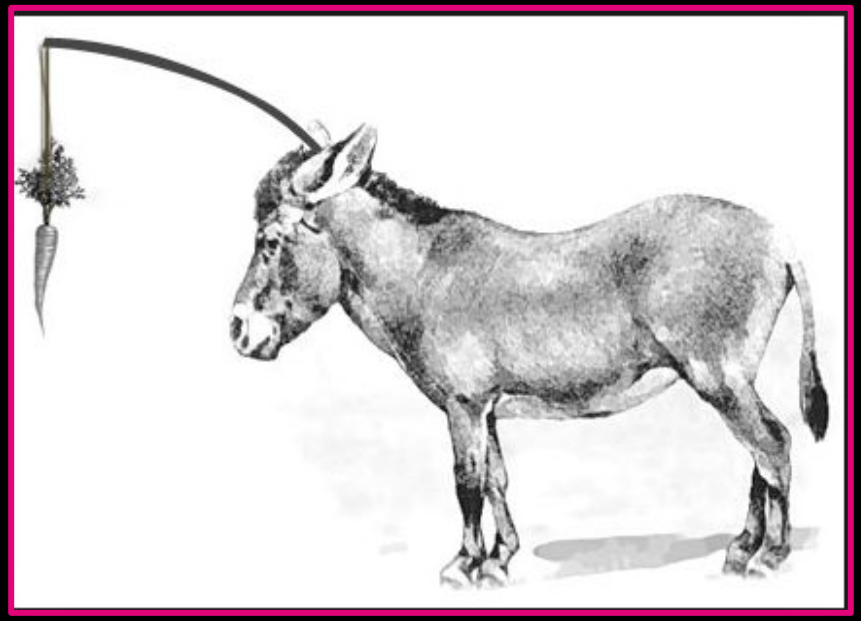
Tara Merk

Many blockchain projects start with centralized governance and transition over time



POLKADOT BLOCKCHAIN ACADEMY

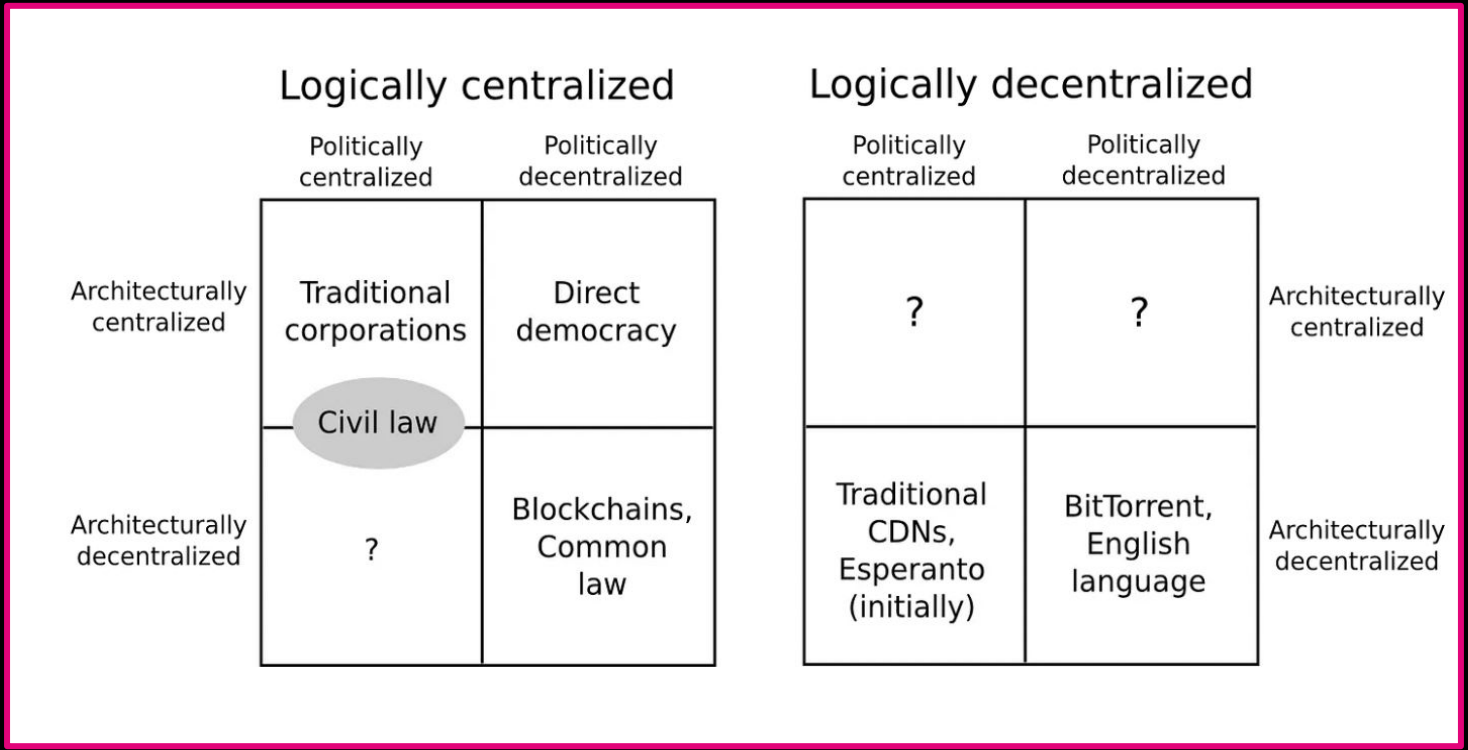
Decentralization is the holy grail



But: what is decentralization, actually?

POLKADOT BLOCKCHAIN ACADEMY

Definitions of Decentralization



POLKADOT BLOCKCHAIN ACADEMY

More definitions of Decentralization

INTERNET POLICY REVIEW

OPEN ACCESS

DIVERSITY GOVERNANCE INFRASTRUCTURE & STANDARDS INFORMATION & DATA INNOVATION INT

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Volume 10, Issue 2 | Concepts of the digital society

Decentralisation: a multidisciplinary perspective

Balázs Bodó, *Institute for Information Law, University of Amsterdam, Amsterdam, Netherlands, bodo@uva.nl*
Jaya Klara Brekke, *Department of Geography, Durham University, United Kingdom, j.k.brekke@durham.ac.uk*
Jaap-Henk Hoepman, *Institute for Computing and Information Sciences, Radboud University , Nijmegen, Netherlands, jhh@cs.ru.nl*

PUBLISHED ON: 16 Jun 2021 DOI: 10.14763/2021.2.1563

ABSTRACT

Decentralisation as a concept is attracting a lot of interest, not least with the rise of decentralised and distributed techno-social systems like Bitcoin, and distributed ledgers more generally. In this paper, we first define decentralisation as it is implemented for technical architectures and then discuss the technical, social, political and economic ideas that drive the

POLKADOT BLOCKCHAIN ACADEMY

More definitions of Decentralization

Sufficient Decentralization: A Playbook for web3 Builders and Lawyers

By Marc Boiron, Chief Legal Officer at dYdX Trading[1]

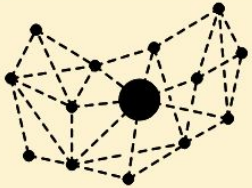
Introduction

Web3 builders have focused on the concept of “sufficient decentralization” ever since staff at the U.S. Securities and Exchange Commission introduced the concept in 2018. It led builders to focus on distributing the efforts of driving profits in a crypto-asset from a centralized company to unaffiliated community members working towards a common goal.

Operationalizing and measuring decentralization

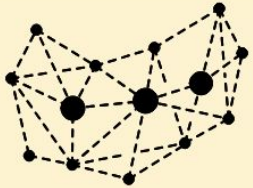
Who has read/ write access?

Principle 1: Consider the level of decentralisation



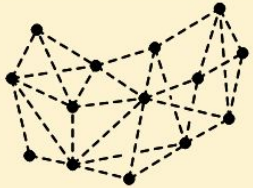
Permissioned private blockchain

- Governing structure: A single source of authority.
- Decentralisation level: Low.



Permissioned public blockchain

- Governing structure: A consortium of multiple authorities.
- Decentralisation level: Medium.

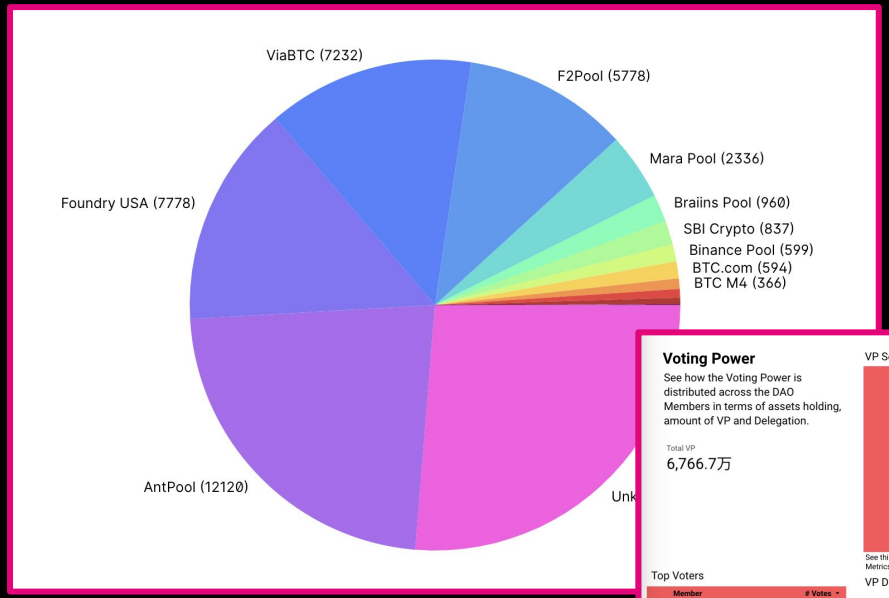


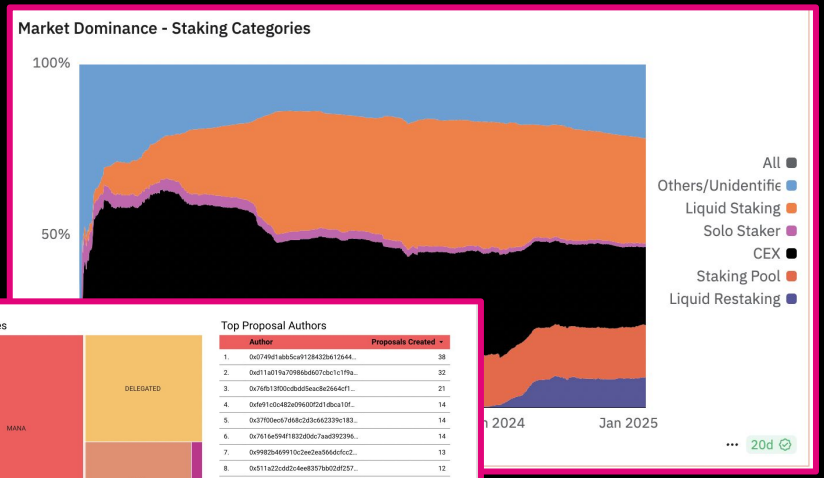
Permissionless public blockchain

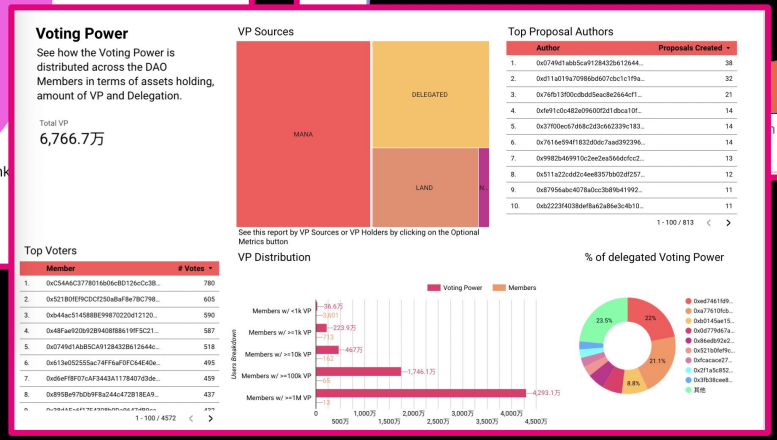
- Governing structure: No clear authority.
- Decentralisation level: High.

POLKADOT BLOCKCHAIN ACADEMY

What is the mining/staking/ voting distro?

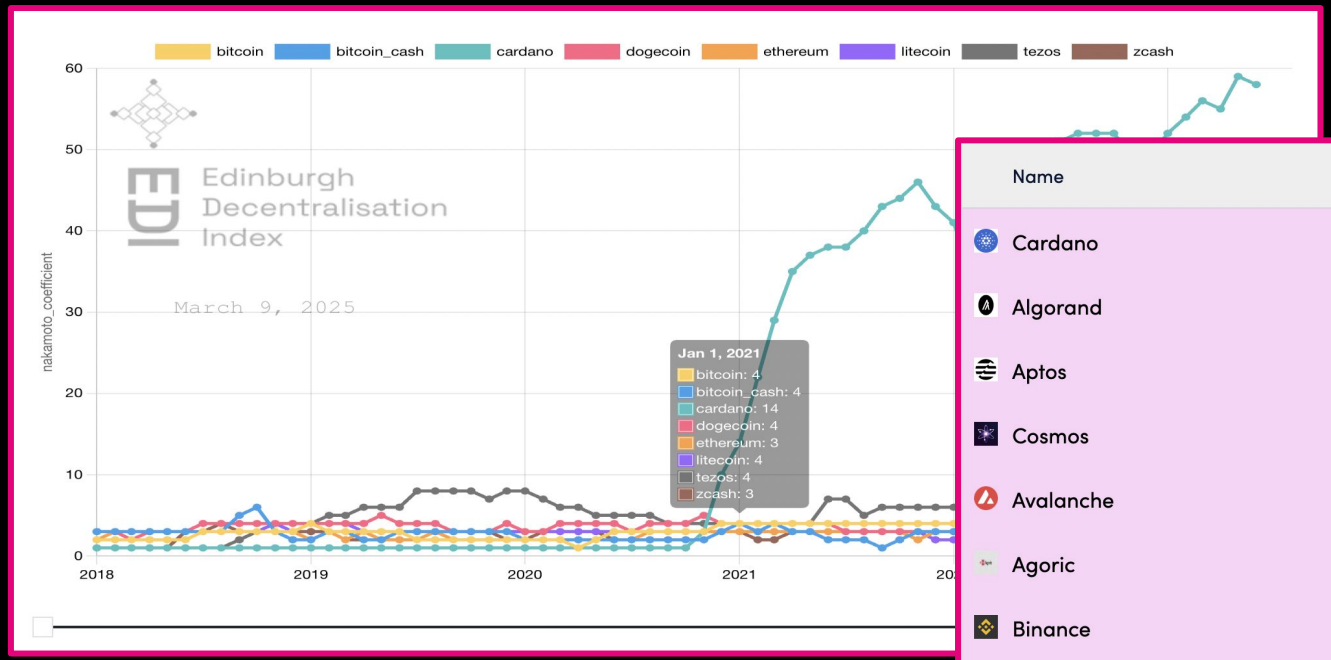






POLKADOT BLOCKCHAIN ACADEMY

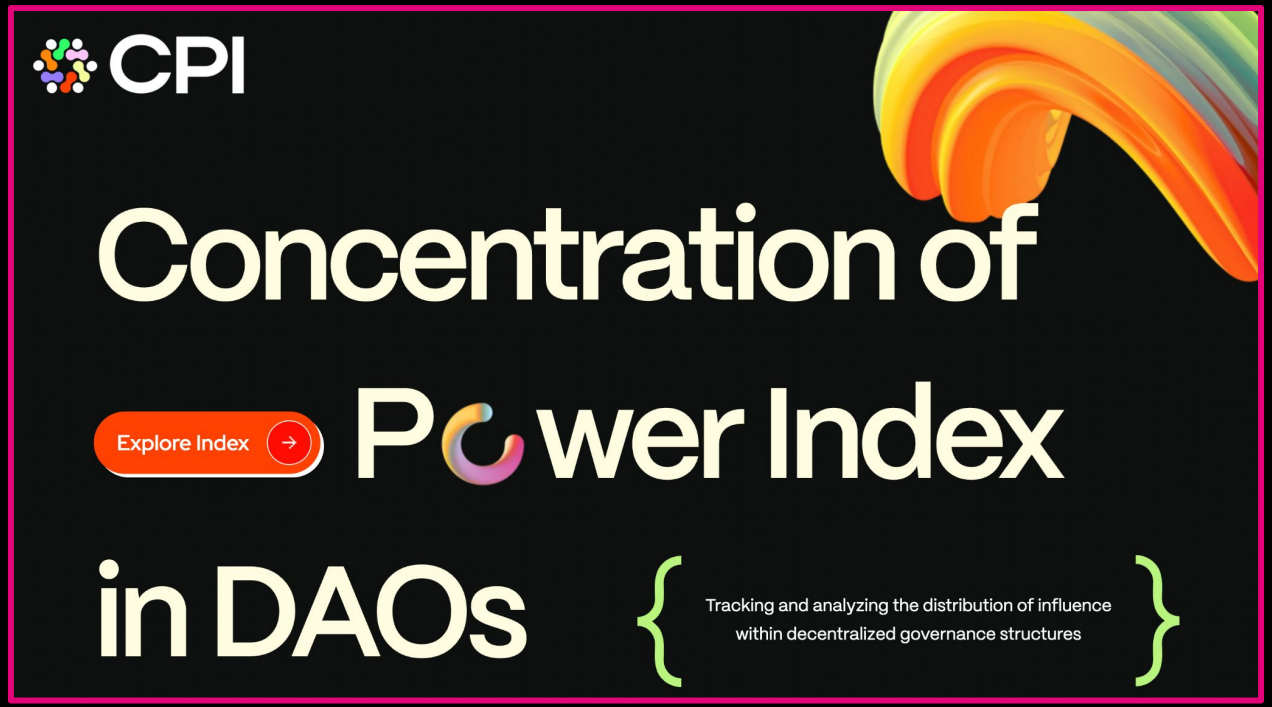
Nakamoto coefficient



Name	Previous Value	Current Value
Cardano	24	24
Algorand	11	11
Aptos	18	18
Cosmos	7	7
Avalanche	26	26
Agoric	6	6
Binance	7	7
Polkadot	148	148

POLKADOT BLOCKCHAIN ACADEMY

Optimism CoP measurement



POLKADOT BLOCKCHAIN ACADEMY

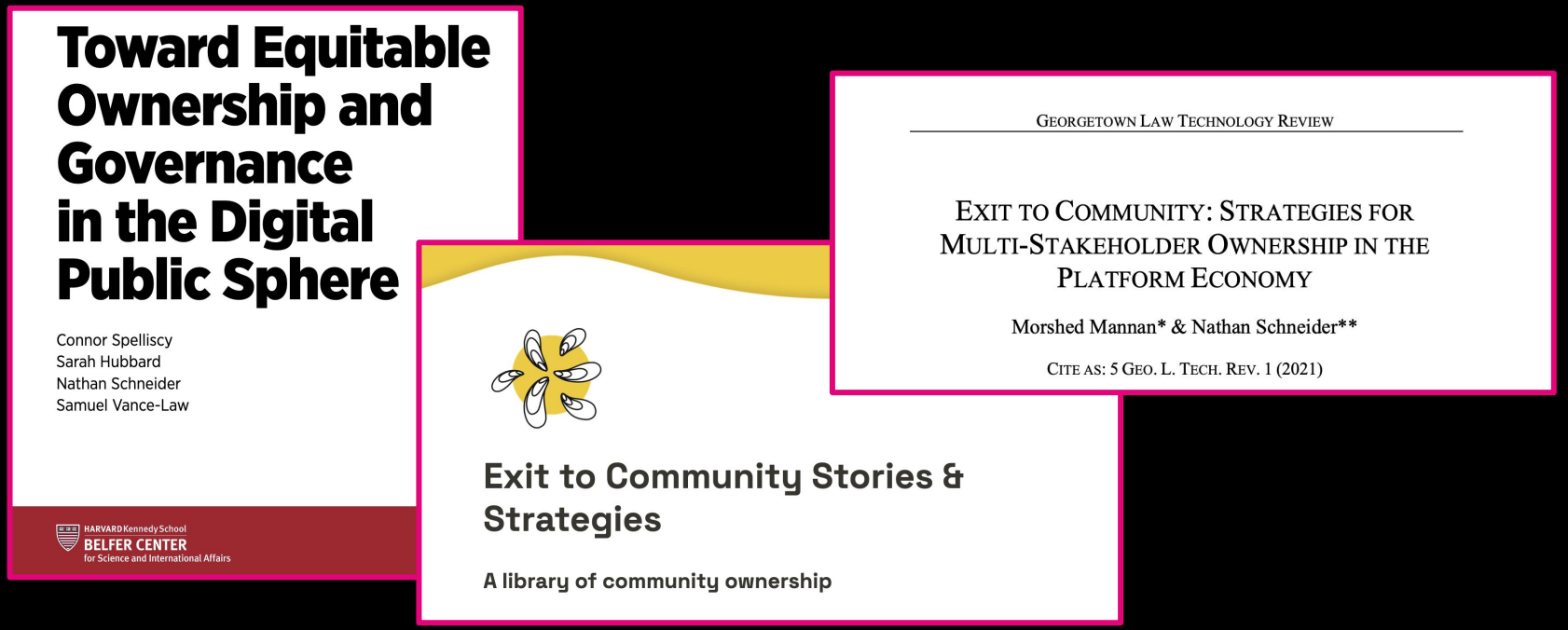
Legal assessments

What are some of the factors to consider in assessing whether a digital asset is offered as an investment contract and is thus a security? Primarily, consider whether a third party – be it a person, entity or coordinated group of actors – drives the expectation of a return. That question will always depend on the particular facts and circumstances, and this list is illustrative, not exhaustive:

1. Is there a person or group that has sponsored or promoted the creation and sale of the digital asset, the efforts of whom play a significant role in the development and maintenance of the asset and its potential increase in value?
2. Has this person or group retained a stake or other interest in the digital asset such that it would be motivated to expend efforts to cause an increase in value in the digital asset? Would purchasers reasonably believe such efforts will be undertaken and may result in a return on their investment in the digital asset?
3. Has the promoter raised an amount of funds in excess of what may be needed to establish a functional network, and, if so, has it indicated how those funds may be used to support the value of the tokens or to increase the value of the enterprise? Does the promoter continue to expend funds from proceeds or operations to enhance the functionality and/or value of the system within which the tokens operate?
4. Are purchasers "investing," that is seeking a return? In that regard, is the instrument marketed and sold to the general public instead of to potential users of the network for a price that reasonably correlates with the market value of the good or service in the network?
5. Does application of the Securities Act protections make sense? Is there a person or entity others are relying on that plays a key role in the profit-making of the enterprise such that disclosure of their activities and plans would be important to investors? Do informational asymmetries exist between the promoters and potential purchasers/investors in the digital asset?
6. Do persons or entities other than the promoter exercise governance rights or meaningful influence?

Frameworks for thinking through transition management

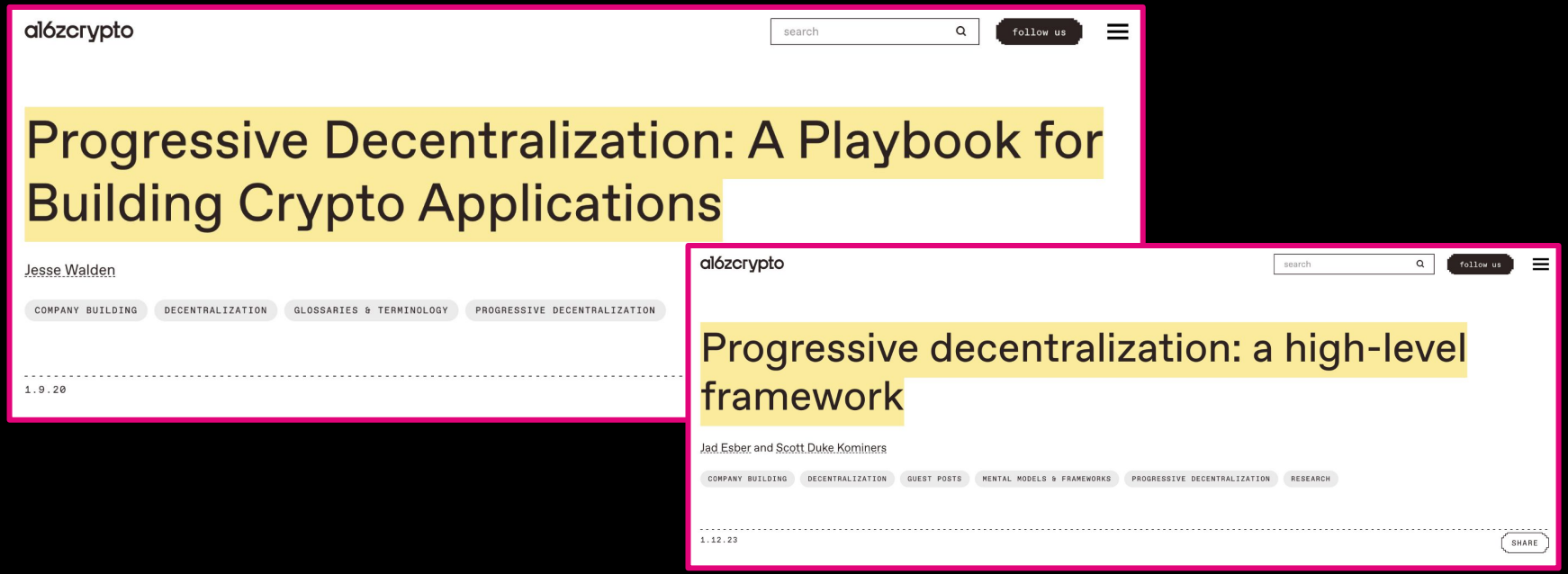
Exit to Community



Learning from experience

POLKADOT BLOCKCHAIN ACADEMY

Progressive decentralization

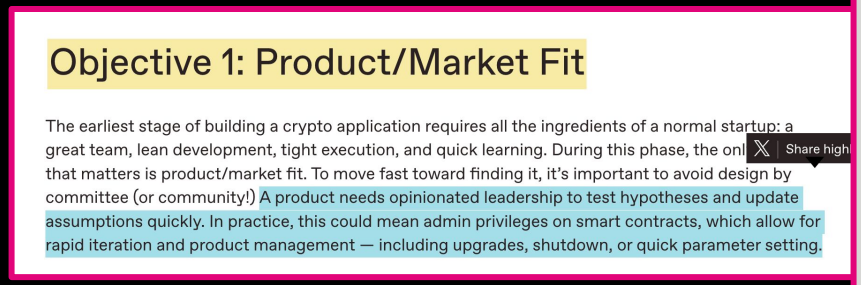


A blockchain specific playbook

POLKADOT BLOCKCHAIN ACADEMY

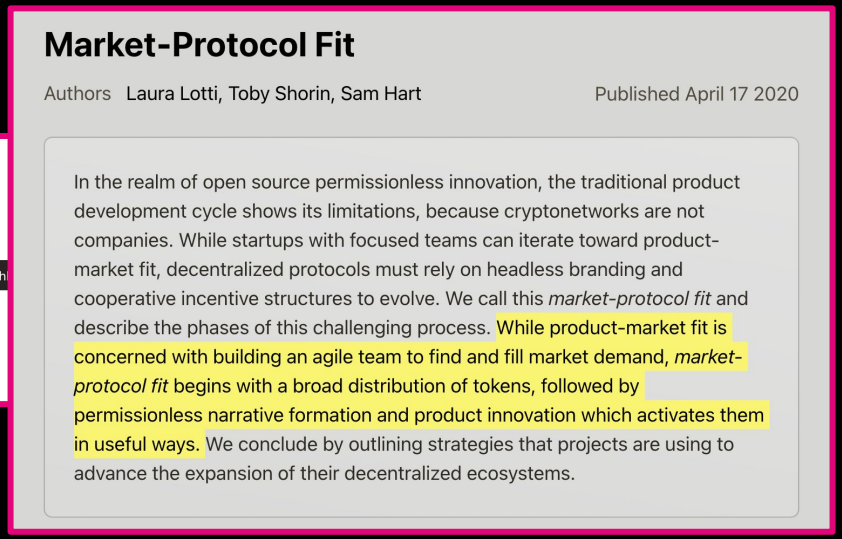
When should the transition start?

When does the transition start?



Objective 1: Product/Market Fit

The earliest stage of building a crypto application requires all the ingredients of a normal startup: a great team, lean development, tight execution, and quick learning. During this phase, the onl Share high that matters is product/market fit. To move fast toward finding it, it's important to avoid design by committee (or community!) A product needs opinionated leadership to test hypotheses and update assumptions quickly. In practice, this could mean admin privileges on smart contracts, which allow for rapid iteration and product management — including upgrades, shutdown, or quick parameter setting.



Market-Protocol Fit

Authors Laura Lotti, Toby Shorin, Sam Hart

Published April 17 2020

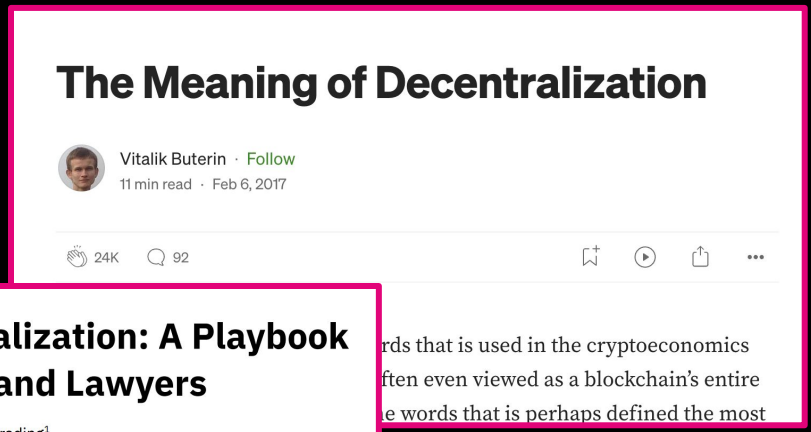
In the realm of open source permissionless innovation, the traditional product development cycle shows its limitations, because cryptonetworks are not companies. While startups with focused teams can iterate toward product-market fit, decentralized protocols must rely on headless branding and cooperative incentive structures to evolve. We call this *market-protocol fit* and describe the phases of this challenging process. While product-market fit is concerned with building an agile team to find and fill market demand, *market-protocol fit* begins with a broad distribution of tokens, followed by permissionless narrative formation and product innovation which activates them in useful ways. We conclude by outlining strategies that projects are using to advance the expansion of their decentralized ecosystems.

Product-market vs market-protocol fit

POLKADOT BLOCKCHAIN ACADEMY

Where does the transition end?

Where does the transition end?



Understanding decentralization

POLKADOT BLOCKCHAIN ACADEMY

Exercise

1. When and where did centralization/ decentralization matter in the case of the Parallel Hack
2. Should the Technical Fellowship have seized control of the Parallel network? Why? Why not? Write a blog post convincing the community of your opinion

BLOCKCHAINGOV

Blockchain Governance Competencies

Lecture 6

Felix Beer

Governance talent gap

- Blockchain technologists often lack governance expertise despite technical and business acumen.
- Ecosystems struggle to implement effective governance and decentralization.
- There is a major gap in professional training focused on blockchain governance.
- This educational gap hinders resilience and long-term evolution, making governance literacy a critical capacity for the Web3 space.

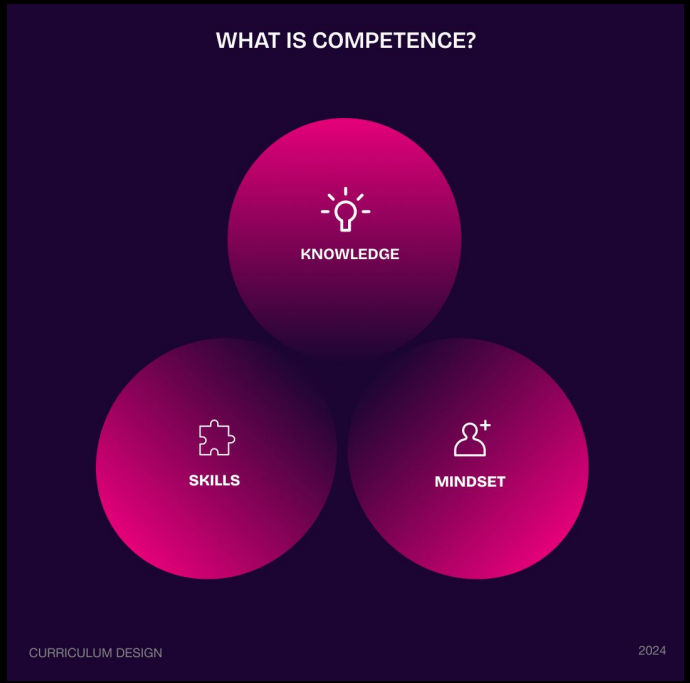
Blockchain governance literacy

A collection of distinct yet interrelated competencies that together empower individuals and collectives to:

1. Understand and contextualize the politics and history of web3 governance;
2. Strategize for progressive decentralization;
3. Design and deploy governance models, both on-chain and off-chain;
4. Navigate their legal, regulatory, and ethical implications;
5. Enhance impact through continuous evaluation and upgrades

What is competence?

1. **Knowledge** is composed of facts, concepts, and theories which are foundational for the understanding of a given subject. **(What I understand)**
2. **Skills** are defined as the ability and capacity to carry out processes and use the existing knowledge to achieve results. **(What I do)**
3. **Mindsets** describe the disposition and mindsets to act or react to ideas, persons or situations. **(What I believe)**



POLKADOT BLOCKCHAIN ACADEMY

Governance competence framework

The Blockchain Governance Competence Framework includes **seven clusters**:

- Decentralized Governance Fundamentals
- Technical Proficiency
- Mechanism Design & Implementation
- Stakeholder & Change Management
- Legal & Regulatory Literacy
- Distributed Community Leadership
- Adaptive Governance Innovation
- ?

POLKADOT BLOCKCHAIN ACADEMY

Decentralized Governance Fundamentals

Objective: Understand core theories, models, and discourses shaping Web3 governance.

Skills: Analyse, evaluate and communicate governance models and their trade-offs

Knowledges: Theories and discourses of decentralised governance

Mindsets: Systems thinking, critical awareness

Decentralized Governance Fundamentals

POLKADOT BLOCKCHAIN ACADEMY

Technical Proficiency

Objective: Navigate the technical foundations that enable and constrain blockchain governance.

Skills: Consensus mechanisms, smart contracts, protocol upgrade, governance tooling

Knowledges: Interpret, test or contribute to on-chain governance (e.g. protocol changes)

Mindsets: Engineering mindset

Mechanism Design & Implementation

Objective: Understanding core theories and discourses around web3 governance.

Skills: Design, implement, and iterate governance mechanisms

Knowledges: Voting models, proposal systems, tokenomics

Mindsets: Design thinking

Mechanism Design & Implementation

Stakeholder & Change Management

Objective: Understanding core theories and discourses around web3 governance.

Skills: Facilitate engagement, manage conflict, drive change

Knowledges: Stakeholder roles, decentralization pathways, power dynamics

Mindsets: Ecosystem thinking

Stakeholder & Change Management

POLKADOT BLOCKCHAIN ACADEMY

Legal & Regulatory Literacy

Objective: Understanding core theories and discourses around web3 governance.

Skills: Assess risk, translate legal impact, engage with policymakers

Knowledges: Regulatory frameworks, compliance law, DAO legal models

Mindsets: Responsibility and accountability mindset

POLKADOT
BLOCKCHAIN
ACADEMY

Distributed Community Leadership

Objective: Cultivate decentralised community self-governance

Skills: Facilitate debates, align perspectives, and nurture participatory culture

Knowledges:

Mindsets: Trust building mindset, participatory mindset

Distributed Community Leadership

POLKADOT BLOCKCHAIN ACADEMY

Adaptive Governance Innovation

Objective: Steering governance evolution through continuous experimentation and learning.

Skills: Evaluate systems, lead experiments, refine models

Knowledges: Impact evaluation, scenario planning, adaptive design

Mindsets: Futures thinking, continuous learning

Adaptive Governance Innovation

POLKADOT BLOCKCHAIN ACADEMY

Governance as ecosystem capacity

Blockchain governance is **not centralised** in any one person. It is a **distributed capacity** of the ecosystem itself.

✅ To build resilient systems, we must think of governance not as a role—but as a distributed, evolving **capacity of the whole ecosystem.**

POLKADOT BLOCKCHAIN ACADEMY

Professional pathways

🔧 **Governance Facilitator:** Bridges technical and social domains. Moderates discussions, guides proposals, and ensures inclusive and transparent processes.

📐 **Mechanism Designer:** Architects voting systems, incentive structures, and DAO logic. Applies game theory, behavioral insight, and design thinking.

📊 **Governance Analyst:** Collects, interprets, and visualizes data on participation, power dynamics, and outcomes. Tracks governance health and risks.

⚖️ **Legal & Compliance Steward:** Navigates regulation, risk, and responsibility. Brings legal clarity and ethical sensitivity to decentralized systems.

🌱 **Community Steward:** Nurtures cultural cohesion, psychological safety, and contributor pathways. Builds community memory and continuity.

Exercise

1. **Individual exercise (15 min)**
   a. Rate yourself (Beginner → Expert) in each cluster
   b. Identify strengths and growth areas
   c. Choose one cluster to develop further in the future
   d. Define 2–3 concrete learning or contribution actions
2. **Group discussion (20 min)**
   a. What are your learning goals?
   b. What are key challenges and opportunities for acquiring governance expertise?
   c. How can you help build governance literacy in your blockchain ecosystem?

BLOCKCHAINGOV

Fish Bowl:
The Future of Blockchain Governance

Fishbowl Exercise

1. Roles: Six discussants and audience
2. Rules:
    a. One chair is always kept empty;
    b. Any member of the audience can, at any time, occupy the empty chair and join the fishbowl;
    c. When this happen, an existing member of the fishbowl must voluntarily leave the fishbowl and free a chair.