



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).



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!



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*

Technologists are not politicians:



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

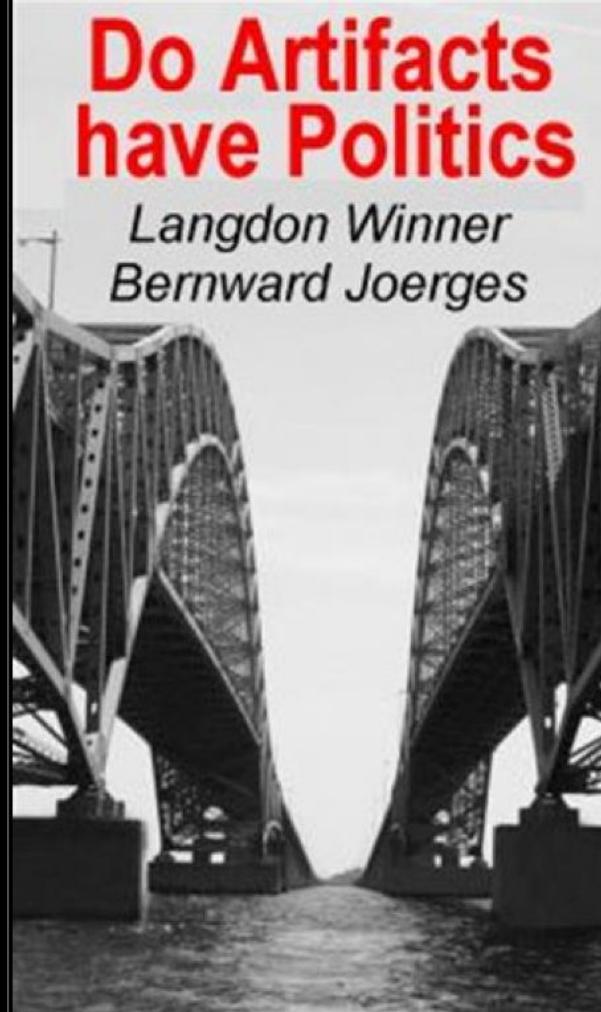


Technology is neither good
nor bad; nor is it neutral.

Melvin Kranzberg

quotefancy

Affordances



Constraints



LOW OVERPASS BRIDGES



HAUSSMANIAN BOULEVARDS



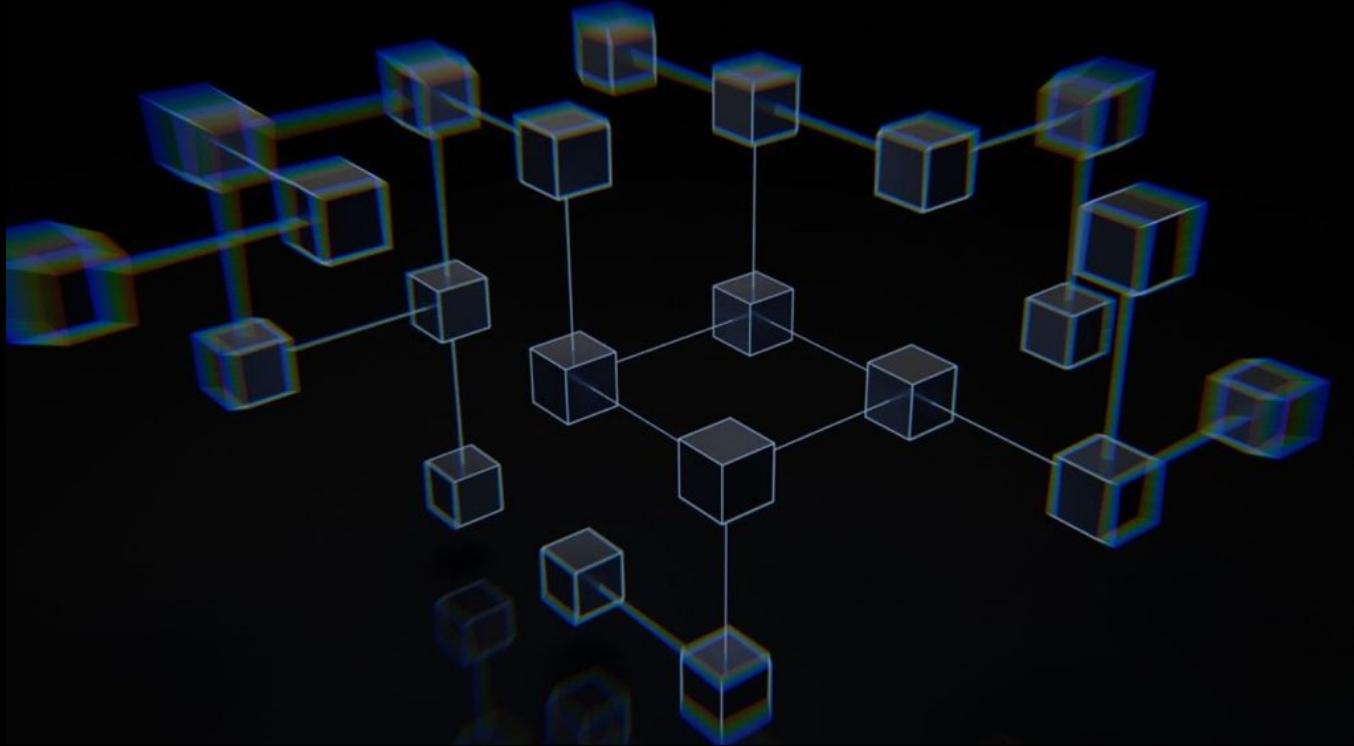
SPEED BUMPS



DIGITAL ARTEFACTS HAVE POLITICS



DIGITAL ARTEFACTS ALSO HAVE POLITICS



BLOCKCHAINS HAVE POLITICS



BLOCKCHAINS HAVE POLITICS



*How to engineer blockchain systems
that provide the right mix of affordances and constraints ?*

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?

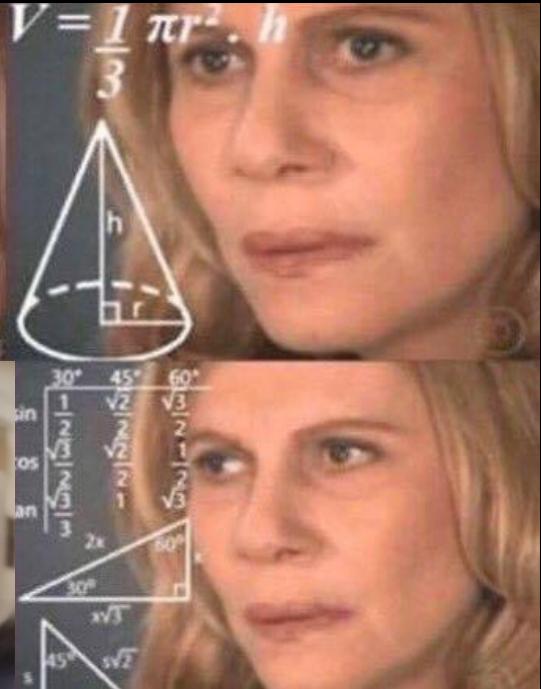
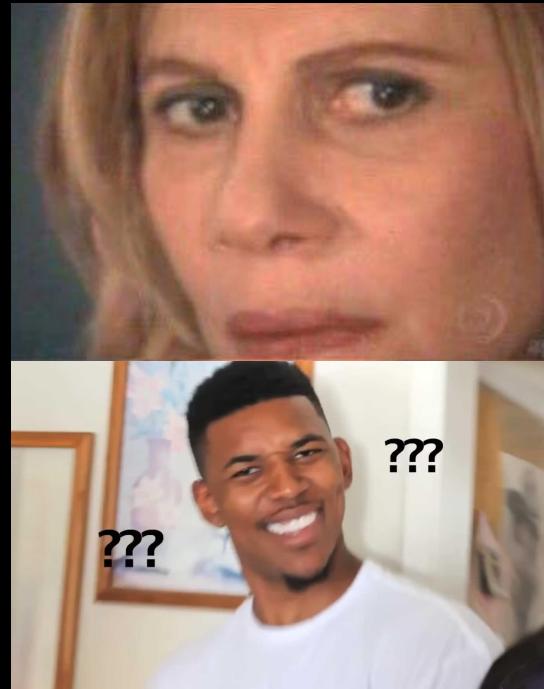
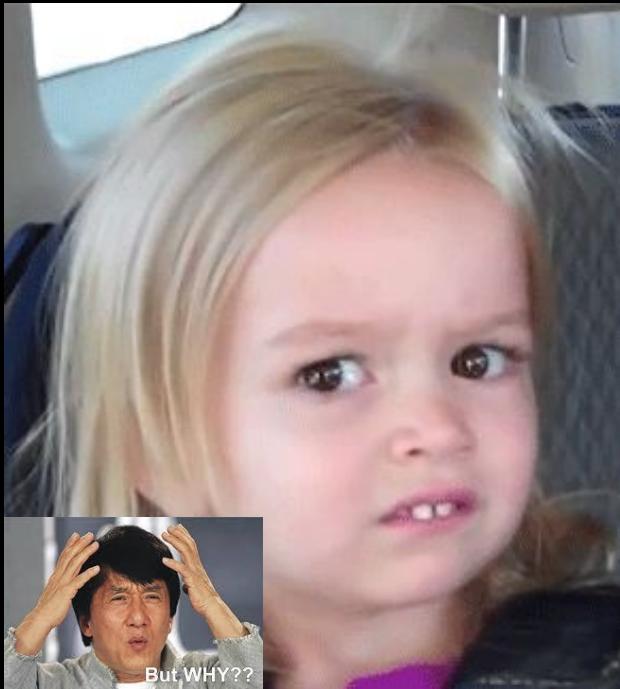
Defining governance

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

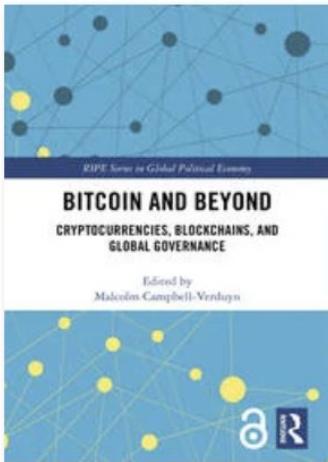
HU University of Applied Sciences
Utrecht, the Netherlands
john.vanmeerten@student.hu.nl

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

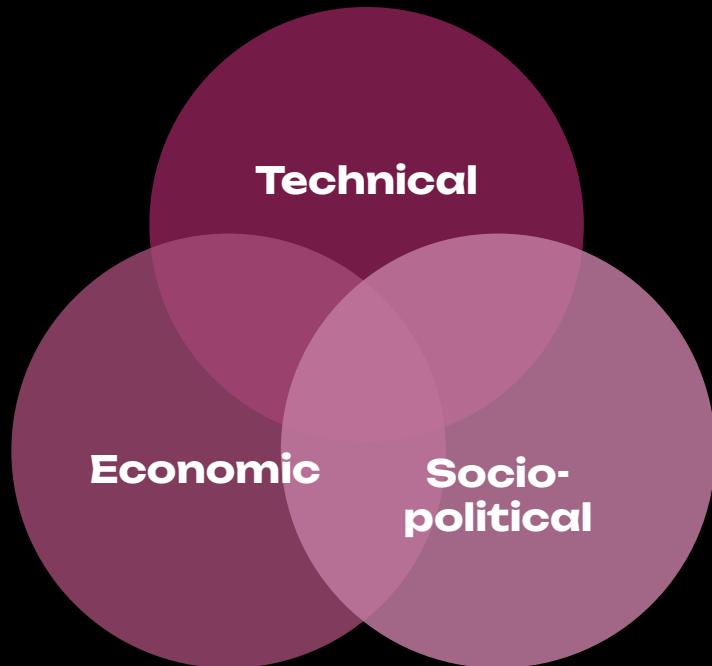
Gabriella Laatikainen  , Mengcheng Li, Pekka Abrahamsson

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



BLOCKCHAIN AS... TRUSTLESS TECHNOLOGY

Antonopoulos:

"Shift from trusting people ... to trusting math"

"Don't trust, Verify"

The Economist:

"Trust Machine"

Werbach:

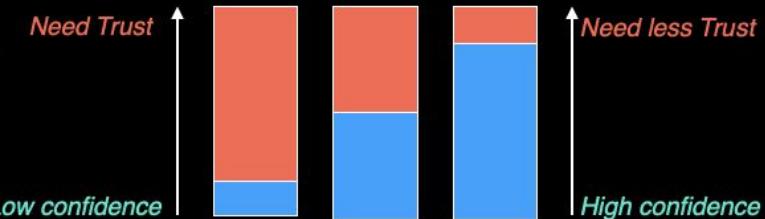
"Trustless Trust"



... 07E 6 89019A12 AB CD45CD
18018F07 078F0780 807 F07EF7E
D56D45C3BC34BC B A 23AB3 B23AB34
9 890 F089018F08F0 F 890 F078
F0 80 EF0 F078F67 F 67 7E56D
B24B 423B A A 29A1891890
EF67E5 45DE5CD4BD45C 4BC4BC345
34B23AB23BC3AB 3 29A129A
F078F67F075 E EF6D 6DE5 D5DE5C
D45CD4CD45 D 4BC34B3 B2 AB A2
BF07EF78F0 8 08F078F67F67E 6 5 7
1B 4B34B29A29A19 0 8 0 078F6
6 F078F078018907801 E 89078
67EF7EF67E 08F07E56 6
23AB B29A23

*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... CONFIDENCE MACHINE

CONFIDENCE FACTORS

(1) Mathematics & Cryptography

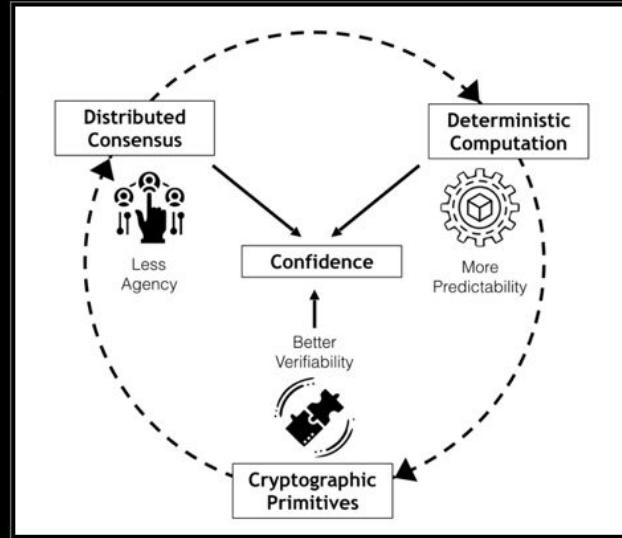
- Hashing functions, Public-Private Keys

(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

THE RULE OF CODE

"This dark, exhilarating work is the most important book of its generation about the relationship between law, cyberspace and social organization."



CODE AND OTHER LAWS OF CYBERSPACE

LAWRENCE LESSIG

CODE
IS
LAW

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

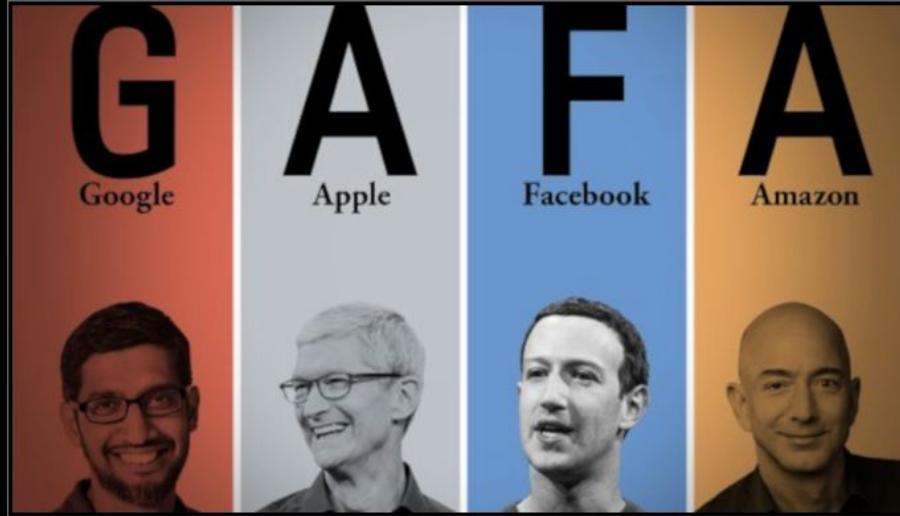
Independent judiciary ensures equality and fairness of law between people & public officials

BY
RULE ~~OF~~ LAW



INSTRUMENTALISATION OF LAW
AS A TOOL OF POLITICAL POWER

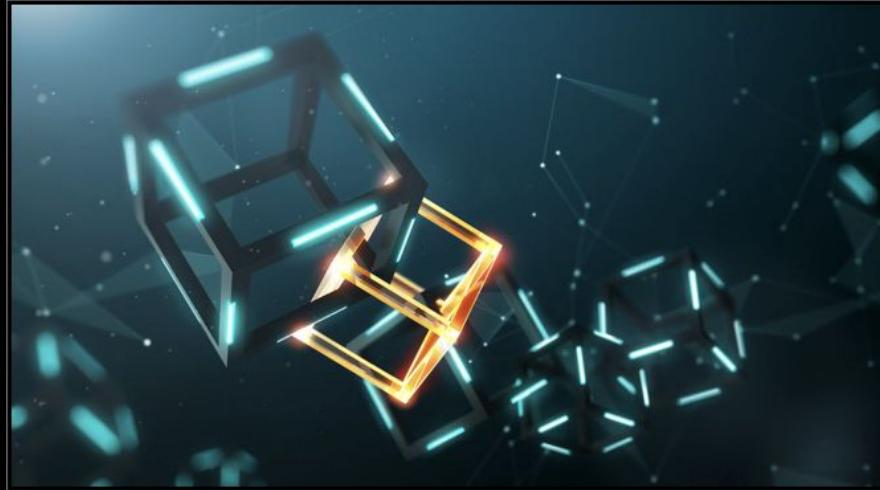
RULE BY CODE



DIGITAL FEUDALISM
FUNCTIONAL SOVEREIGNTY

INSTRUMENTALISATION OF CODE
AS A TOOL OF POLITICAL POWER

OF
RULE BY ~~CODE~~ CODE



TECHNICAL SOVEREIGNTY

No ONE IS ABOVE THE CODE

CODE IS LAW : BLOCKCHAIN AS CONFIDENCE MACHINE



BRINGING TRUST BACK IN



BLOCKCHAINS AS SOCIO-TECHNICAL SYSTEMS

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

BLOCKCHAIN GOVERNANCE

GOVERNANCE

BY the infrastructure



(on-chain governance)

OF the infrastructure



(off-chain governance)

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 ?

Case Study Introduction

Lecture 2

Lovisa Björna & Tara Merk

Meet Parallel Finance

parallel / README.md

Preview Code Blame 57 lines (41 loc) · 3.05 KB

Raw ⌂ ⌄ ⌅ ⌆ ⌇ ⌈ ⌉ ⌊ ⌋ ⌃ ⌁ ⌂ ⌄ ⌅ ⌆ ⌇ ⌈ ⌉ ⌊ ⌋ ⌃ ⌁

Files

master

Go to file

- .githooks
- .github
- .maintain
- docs
- integration-tests
- node
- pallets
- precompiles
- primitives
- resources
- runtime
- scripts
- support
- .dockerignore
- .editorconfig
- .gitignore

PARALLEL FINANCE
BRING DEFI TO THE MAINSTREAM

last commit september 2024 tag v3.1.3 Substrate 3.0.0 CI failing codecov 51% docker pulls 8.3k license GPL-3.0

X Follow @ParallelFi Telegram Medium Forum chat widget disabled

A decentralized lending & staking protocol built on top of the Polkadot ecosystem

[Website](#) | [White Paper](#) | [API Docs](#) | [Chat](#)

ParaFi over time

Milestones Achieved

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

Oct, 2022

Dec, 2024

Sept, 2024

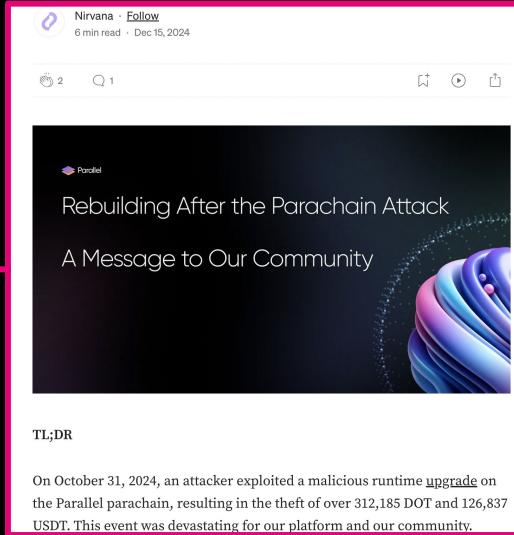
Today

Important Notice: Closure of Polkadot Parallel Money market on September 22th

Nirvana · Follow
2 min read · Sep 19, 2024

Dear Parallel Community,

We are pleased to announce that Parallel's Polkadot Parallel Money market has been a great success and will officially close on September 22th, 2024.



TL;DR

On October 31, 2024, an attacker exploited a malicious runtime [upgrade](#) on the Parallel parachain, resulting in the theft of over 312,185 DOT and 126,837 USDT. This event was devastating for our platform and our community.



@ParallelFi

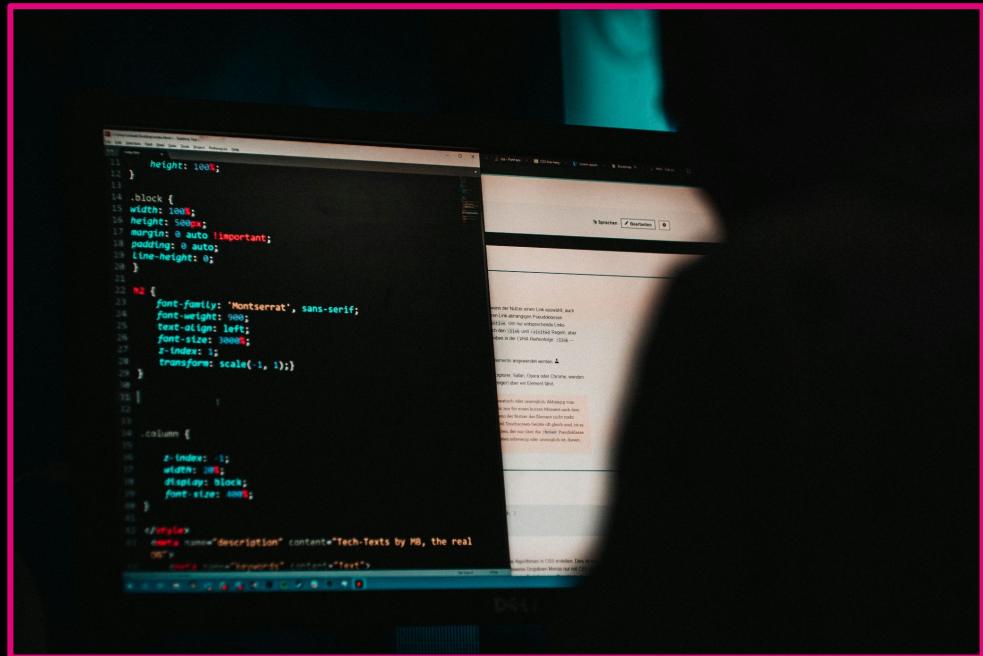
This account doesn't exist

Try searching for another.

What happened?

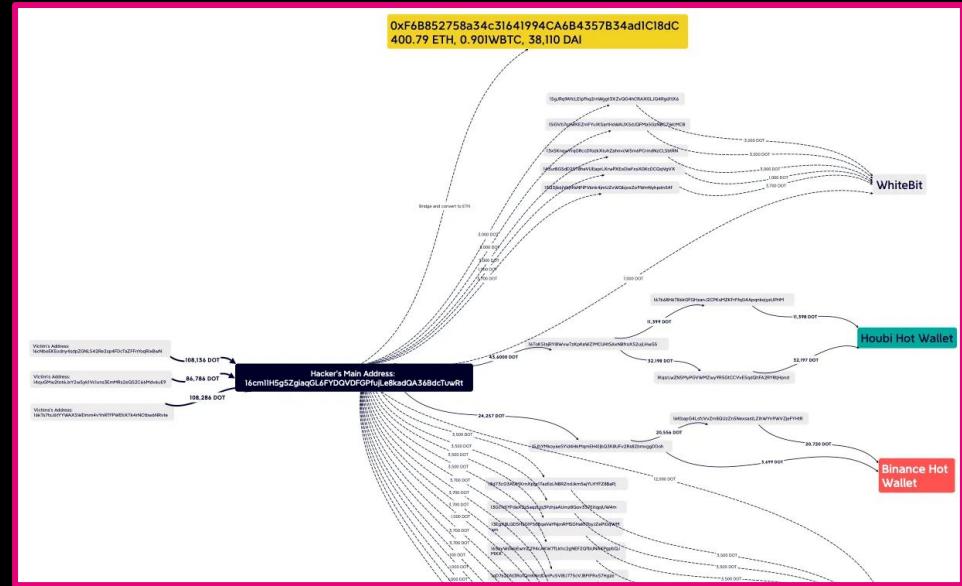
Halloween 2024...

- 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.

Alice und Bob ✅
@alice_und_bob

🚨 DOT Community: We need your help!
200k DOT are at risk of being stolen! 🚨

An attacker compromised Parallel governance and is unbonding 200k DOT. We might have a chance to stop them!

OpenGov Ref 1322 will restake the DOT to give the defenders a chance to regain control of the chain.

We need 100m DOT support (7% of the supply) to get the proposal through.

Please VOTE and SHARE this message!

This is our chance to show that the Polkadot ecosystem can do better!

 polkadot.subsquare.io/referenda/1322



Round 1: The community rallied together!

Executed

#1322 Referendum #1322: Rebond DOT from Parallel Fi accounts - Description below

Proposer:  RTTI-5220 (POLKADOT) in Democracy | 29th Nov '24

Description AI Summary Timeline Evaluation On Chain Info ...

Goal of the Proposal:

- To rebond all balances related to the attack.
- The approach does not impact the sovereignty of the funds but delays availability of funds
- It allows the Parallel team to win time and explore alternatives to regaining control of their parachain governance.

Context:

An account took control over Parallel Fi governance, upgraded the parachain's runtime and used it to transfer out over DOT and USDT. The account executed a malicious runtime upgrade, introducing a custom "sudo" pallet, granting themselves administrative privileges

Show More

No Expert Review Available! An Expert adds their valuable review for this post! An expert? [Add your Review!](#)

→

Proposal Passed 3 of 3

Summary Passed ⓘ

100.0% Aye 0.0% Nay

Ayes(246) 117.20M DOT Nays(9) 4.11K DOT

Support 130.00M DOT Issuance 1.54B DOT

**With 28 days more time,
what would they do?**

Parallel finance pushes for runtime upgrade

The screenshot shows the Polkassembly OpenGov interface. On the left, there's a sidebar with navigation links like Home, Discussions, Calendar, Delegation, Batch Voting, Preimages, and Bounties. A 'Report an issue' button is also present. The main content area displays a proposal titled '#1339 Critical Runtime Upgrade to Prevent Further Exploitation'. The proposal is marked as 'Executed' and was proposed by Para in Democracy on 7th Dec '24. It has three tabs: Description (selected), AI Summary, Timeline, Evaluation, On Chain Info, and Stats. The 'Description' tab contains an 'Incident Overview' section detailing a malicious upgrade that transferred over 312,185 DOT and 126,837 USDT. The 'Timeline of Events' section includes dates like 4/14/2024 and 10/31/2024. To the right, a box says 'No Expert Review Available!' and encourages adding a review. Below that, a summary card shows the proposal 'Passed' with 99.3% Aye and 0.7% Nay. The summary also lists 144 Ayes (49.12M DOT), 11 Nays (351.35K DOT), 16.41M DOT support, and 1.54B DOT issuance. At the bottom, a 'Voting Details' section with a 'View Vote History' link is shown.

& 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!

This screenshot shows the Polkassembly OpenGov interface. The left sidebar includes navigation links for Home, Discussions, Calendar, Delegation, Batch Voting (highlighted), Preimages, Bounties, Tracks, Treasury, and Root. A 'Report an issue' button is also present. The main content area displays proposal #1326 titled "Parallel Finance Guilty - Request for Investigation". The proposal was proposed by 16cm_TuwRt on November 29, 2024, and is categorized under 'community'. It has tabs for Description, AI Summary, Timeline, Evaluation, On Chain Info, and Stats. The description section notes that the proposer is responsible for a whitelist call proposal regarding Parallel Finance governance takeover, as noted in Refendum #1322. It expresses concern about the current vote process and emphasizes that they should not return control to the Parallel Finance team. The proposer clarifies that they are fearful of being discovered and removed from their Polkaidentity information on Subscan. Evidence suggests Parallel Finance may have begun executing a rug pull as early as April, though the investigation only covers activities starting from April due to time constraints. The proposal is effective around Parallel Finance block 6990839-2, on October 31, 2024. A note states that the proposer will list the following addresses at first: Parallel Finance I (PFI), the technical and general council account controlled by Yubo pBBDTWhQx0uTCvVSSOTSVYDcAC523iDZYNSg+T8uiyvbxBh.

This screenshot shows the Polkassembly OpenGov interface. The left sidebar is identical to the previous screenshot. The main content area displays proposal #1458 titled "Parallel Finance Round Two; Is Polkadot Tech-fellows over-involved?". The proposal was proposed by 16cm_TuwRt on February 26, 2024, and is categorized under 'Democracy'. It has tabs for Description, AI Summary, Timeline, Evaluation, On Chain Info, and Stats. The description section states that the proposer has seized 200,000 DOT since parallel finance submitted a technically flawed whitelist referendum - #1445. A link is provided: https://polkadot.subscan.io/referenc/2490323i-9. It notes that it was quite a shock to discover that a staking project was so unfamiliar with the Polkaid staking mechanism. The proposer updates about Parallel Finance news: In their medium Parallel Finance decided not to return all DOT to users. They will open swap pairs for cDOT/PARA and cDOT/DOT. That said, we can't guarantee the conversion price, but we will do our best to provide liquidity for you. Twitter On 2025/02/25, Parallel Finance recently decided to change its CEO to Tom Tou. Twitter On 2025/02/22, Parallel Finance recently decided to shut down its main service in under five months by 2025/8/1 (you sure you can recover by Aug?). No comment. Desperate move.

**Back to the hack:
did the community win?**

Round 2:

The screenshot shows the Polkassembly interface. On the left is a sidebar with navigation links like Home, Discussions, Calendar, Delegation, Batch Voting (with 188 notifications), Preimages, and Bounties. The main content area displays a proposal titled "#1424 Emergency Response Plan for Securing 200,000 DOT". The status is "Executed". The proposer is Parallel Finance 3 in Democracy, dated 9th Feb '25. Below the title are tabs for Description, AI Summary, Timeline, Evaluation, On Chain Info, and Stats. The "Description" tab is selected. It contains a "Context" section where the attacker's malicious actions are described. The "Summary" section shows a green arc indicating 100.0% Aye votes (243.37M DOT) and 0.0% Nay votes (63.86K DOT). The "Voting Details" section includes a chart showing the distribution of support.

#1424 Emergency Response Plan for Securing 200,000 DOT

Proposer: Parallel Finance 3 in Democracy | 9th Feb '25

Description AI Summary Timeline Evaluation On Chain Info Stats

Context

Following the execution of Referenda 1339, the attacker has maliciously added their key as a proxy to the newly established sudo key, effectively freezing all associated PARA funds under the account. As a result, the new sudo key is unable to send transactions, while the attacker retains sudo ownership. Meanwhile, the attacker has initiated unbonding on all six of our accounts, putting 200,000 DOT at risk. We currently have only 16 days left to act, making it crucial to pass this referendum as soon as possible.

This referendum represents the first step of a two-part rescue plan. The first step is to break the chain and transfer funds to an account that no one controls. The second step will involve submitting another proposal to return the funds to users after securing them. Our team has been collaborating closely with Parity and srlabs, who have provided valuable feedback and a thorough review for this referendum.

The accounts at risk:

- 14quGMw2tot6JxY2wSyk1Vc1uns3EmMRs2eQS2C66Mdv6uE9 (22.649 DOT)
- 19cnUyebu52RUt4Rt67brDmmnVdaDD37dxKbaJ7tuLnLf (74.614 DOT)
- 16kTs7tsJ6tYYWAXSWDmm4vNrtFPWEhXtk4rNCtbw6NRvt (1.566 DOT)
- 16ZbwPMyrp9yTbPSdQm9btzcNVKKQ5MHcMQp4rA1ztF4sBA (101.322 DOT)
- 1dMif8G4irXsdPSkvF87uBfajahh2EvC9fPnsi9tv4i1yKC (3.413 DOT)

Proposal Passed 3 of 3

Summary

100.0% Aye 243.37M DOT 0.0% Nay 63.86K DOT

Ayes(168) Support 214.92M DOT Issuance 1.54B DOT

Voting Details View Vote History

10% 10% 10% 0% 0%

Attacker outsmarted the solution from Round 1 😳

Parallel finance issues root proposal to break the chain!

Executed

#1424 Emergency Response Plan for Securing 200,000 DOT

Proposer:  Parallel Finance 3 in Democracy | 9th Feb '25

Description AI Summary Timeline Evaluation On Chain Info Stats

Context

Following the execution of Referenda 1339, the attacker has maliciously added their key as a proxy to the newly established sudo key, effectively freezing all associated PARA funds under the account. As a result, the new sudo key is unable to send transactions, while the attacker retains sudo ownership. Meanwhile, the attacker has initiated withdrawals on all six of our accounts, putting 200,000 DOT at risk. We currently have only 16 days left, making it crucial to pass this referendum as soon as possible.

This referendum represents the first step in our part rescue plan. The first step is to break the chain and transfer funds to an account that no one controls. The second step will involve submitting another proposal to return the funds to users after securing them. Our team has been collaborating closely with Parity and srlabs, who have provided valuable feedback and a thorough review for this referendum.

The accounts at risk:

- 14quGMw2tot6JxY2wSyk1Vc1uns3EmMRs2eQS2C66Mdv6uE9 (22.649 DOT)

Quote Share Copy

No Expert Review Available! An Expert adds their valuable review for this post! An expert? Add your Review!

→

Proposal Passed 3 of 3

Summary

Passed

100.0% Aye 243.37M DOT Nays(8) 63.86K DOT Support 214.92M DOT Issuance 1.54B DOT

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

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?

Primavera De Filippi it's a coup d'état ;)

it's even more legit than the DAO hack, in terms of "stealing" / "not stealing"

PF exploiting governance apathy rather than a tech bug :) 4:55 PM

soooooo crazy 4:40 PM

4:51 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 criticizes 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.”

The screenshot shows the Polkassembly OpenGov interface. On the left, there's a sidebar with navigation links like Home, Discussions, Calendar, Delegation, Batch Voting (with a new badge), Preimages, Bounties, Tracks, Treasury, All, and Root. A 'Report an issue' button is also present. The main content area displays a proposal titled '#1458 Parallel Finance Round Two; Is Polkadot Tech-fellows over-involved?'. It was proposed by '16cm1_TuwrT' on 26th Feb '25. The proposal status is 'Timed Out'. Below the title, it says 'Just information: We have seized the 200,000 DOT since parallel finance submit a technically flawed whitelist referenda - 1445.' followed by a link: <https://polkadot.subscan.io/extrinsic/24903231-9>. There's also a note about Parallel Finance not returning cDot to users and shutting down its main service. At the bottom, it says 'No comment. Desperate move.' To the right, there's a summary section with a progress bar showing 0.0% Aye and 100.0% Nay, and a note that the proposal timed out because the decision deposit was not placed in time. Another box indicates 'No Expert Review Available!' with a call to action to add a review.

| Ayes | DOT | Nays | DOT | Issuance | DOT |
|---------|--------|------|--------|----------|-----|
| 15 | 7.47K | 32 | 19.49M | 1.5 | 1.5 |
| Support | 26.72K | | | | |

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?



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.**

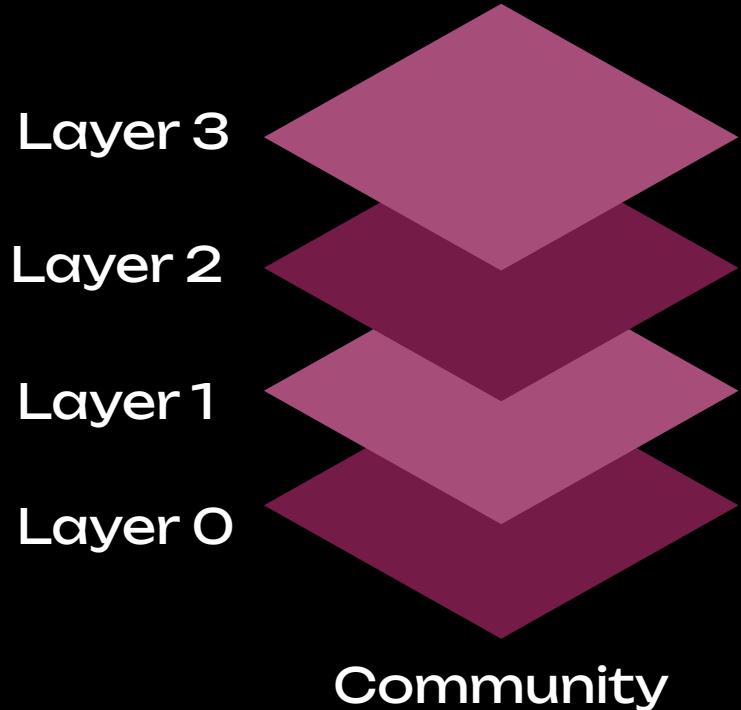
Layer 3: Smart contracts and dApps defining use-case logic.

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?



Nansen Research Discover ▾ Search reports and topics Alpha Zone Analysts My Reading List Log in ↗

Polkadot

Polkadot: The Ultimate Layer-0?

Osgur Murphy 0 Kane Apr 15, 2022



TLDR
Key Terms
Introduction
Substrate
Customizable
Security
Parachain Auctions Explained
Winners of the first 14 Parachains

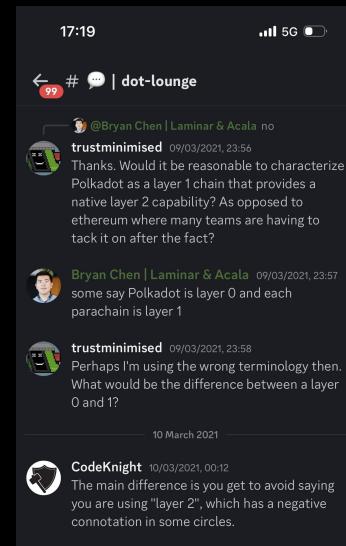


BLOG EDUCATION

Why is Polkadot Called a Layer Zero?

ELIZABETH BROWNING, DISTRACTIVE MAY 26, 2023 13 MIN READ

SHARE



17:19 # dot-lounge

99 @Bryan Chen | Laminar & Acala no trustminimised 09/03/2021, 23:56 Thanks. Would it be reasonable to characterize Polkadot as a layer 1 chain that provides a native layer 2 capability? As opposed to Ethereum where many teams are having to tack it on after the fact?

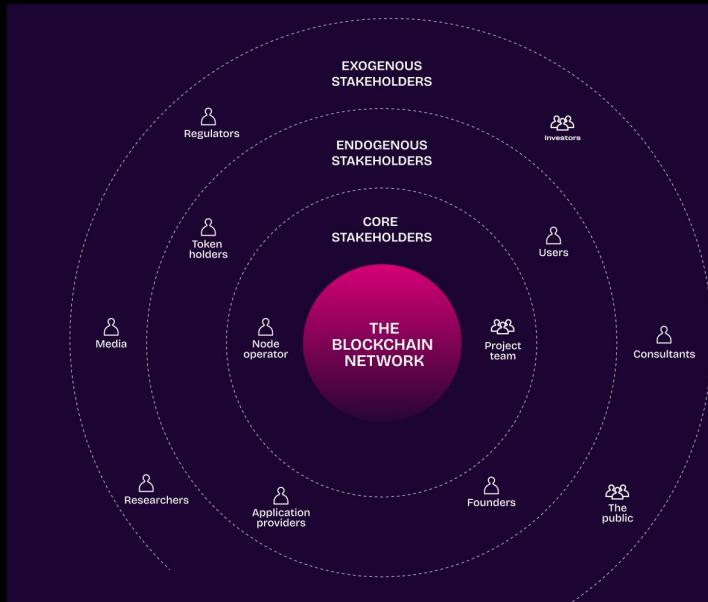
@Bryan Chen | Laminar & Acala 09/03/2021, 23:57 some say Polkadot is layer 0 and each parachain is layer 1

trustminimised 09/03/2021, 23:58 Perhaps I'm using the wrong terminology then. What would be the difference between a layer 0 and 1?

10 March 2021

CodeKnight 10/03/2021, 00:12 The main difference is you get to avoid saying you are using "layer 2", which has a negative connotation in some circles.

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)



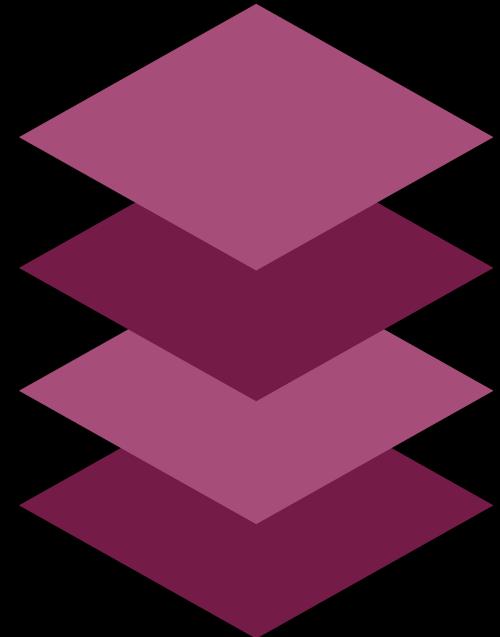
Where is governance enforced?

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.



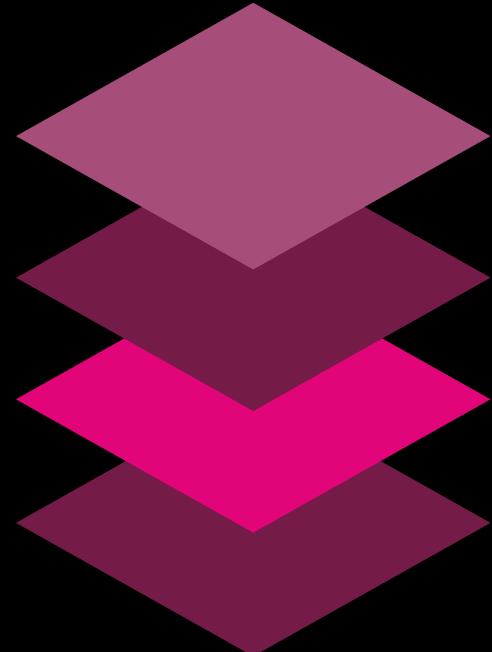
Layer O Governance

- **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 O platforms).



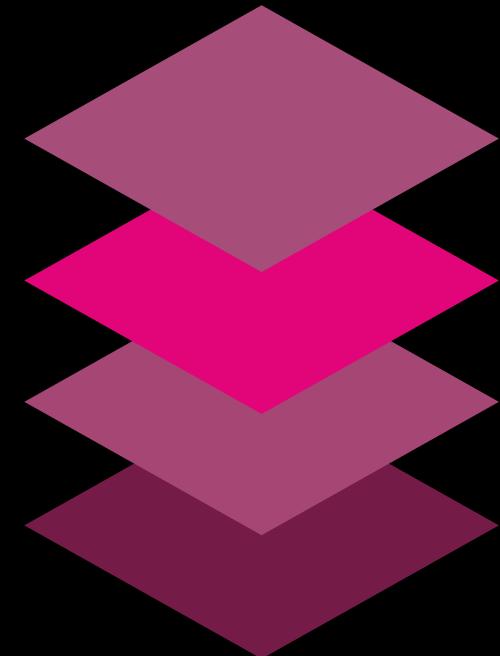
Layer 1 Governance

- **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)



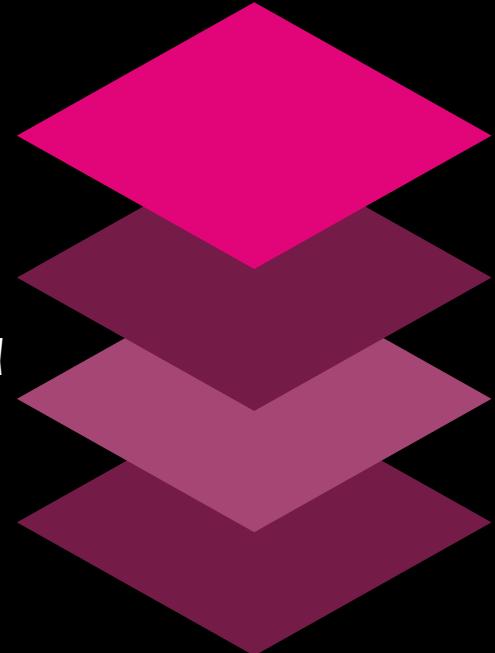
Layer 2 Governance

- **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



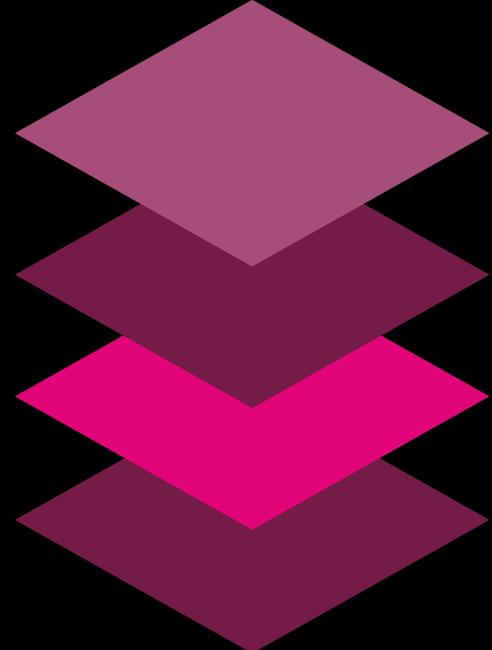
Layer 3 Governance

- **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.



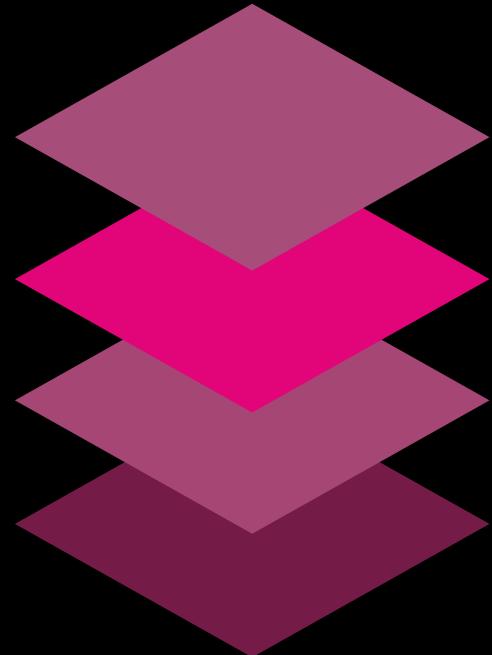
Platform Layer

- **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.



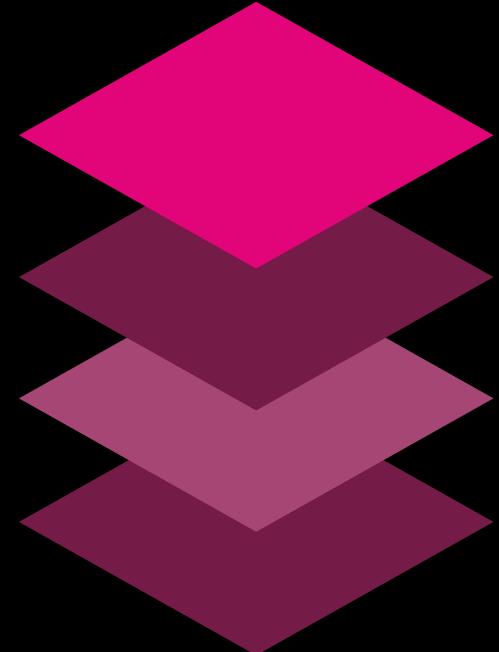
Data Layer

- **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.



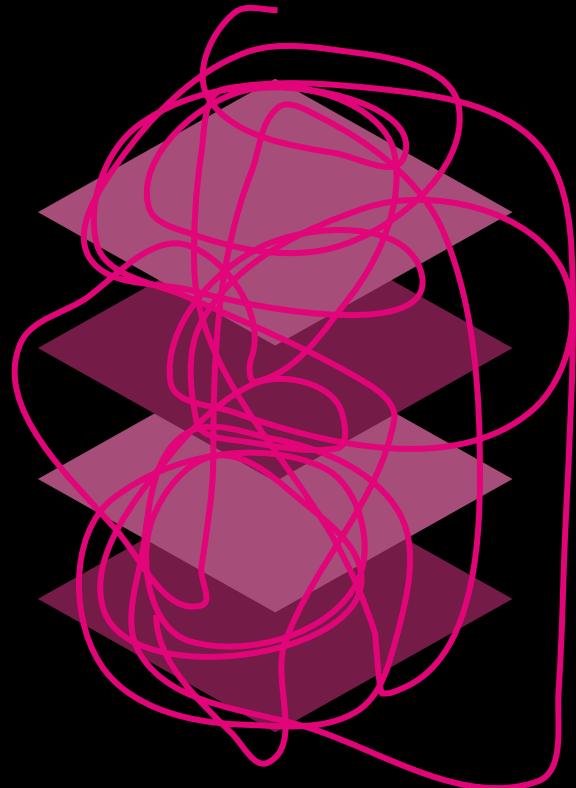
Communication

- **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.

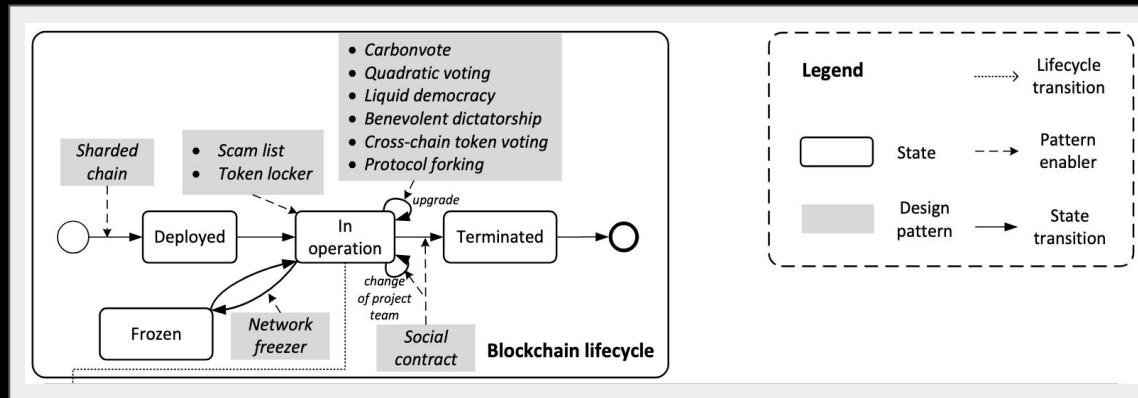


Community Layer

- **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



Governance Mechanisms & Trade-Offs

Lecture 4

Tara Merk

Designing blockchain governance is like creating the perfect recipe



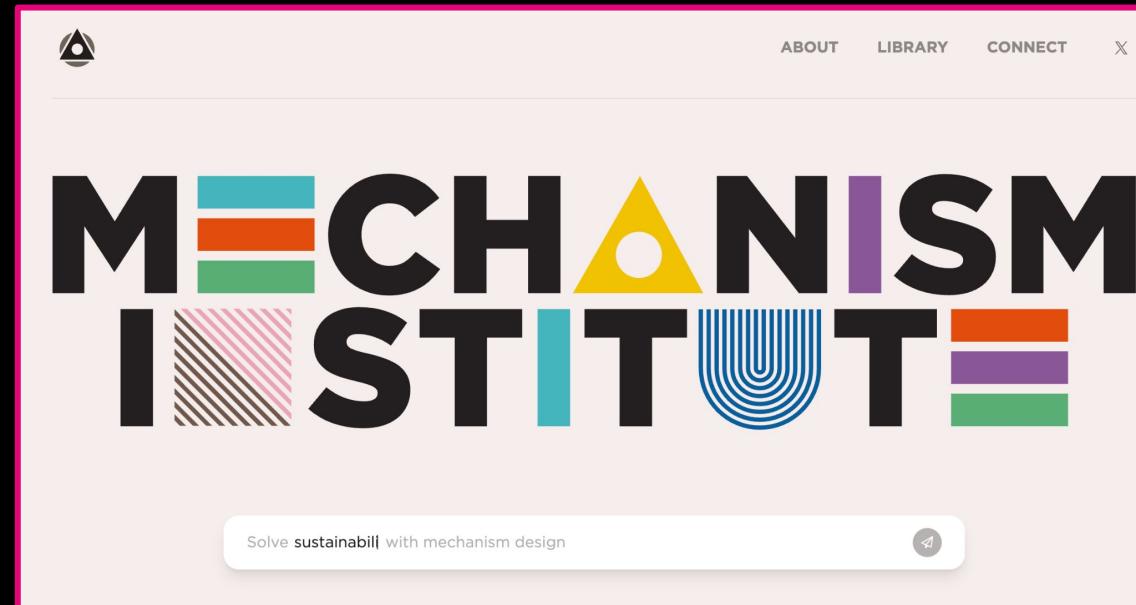
wikiHow to Cook Good Food

Governance mechanisms are like the ingredients to a tasty dish



Depending on the ingredients you chose
you will get different flavors

What ingredients are available?



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

Mechanisms affect different aspects of governance design



Different mechanisms also create different flavors of governance

Expediency



Participation

Immutability



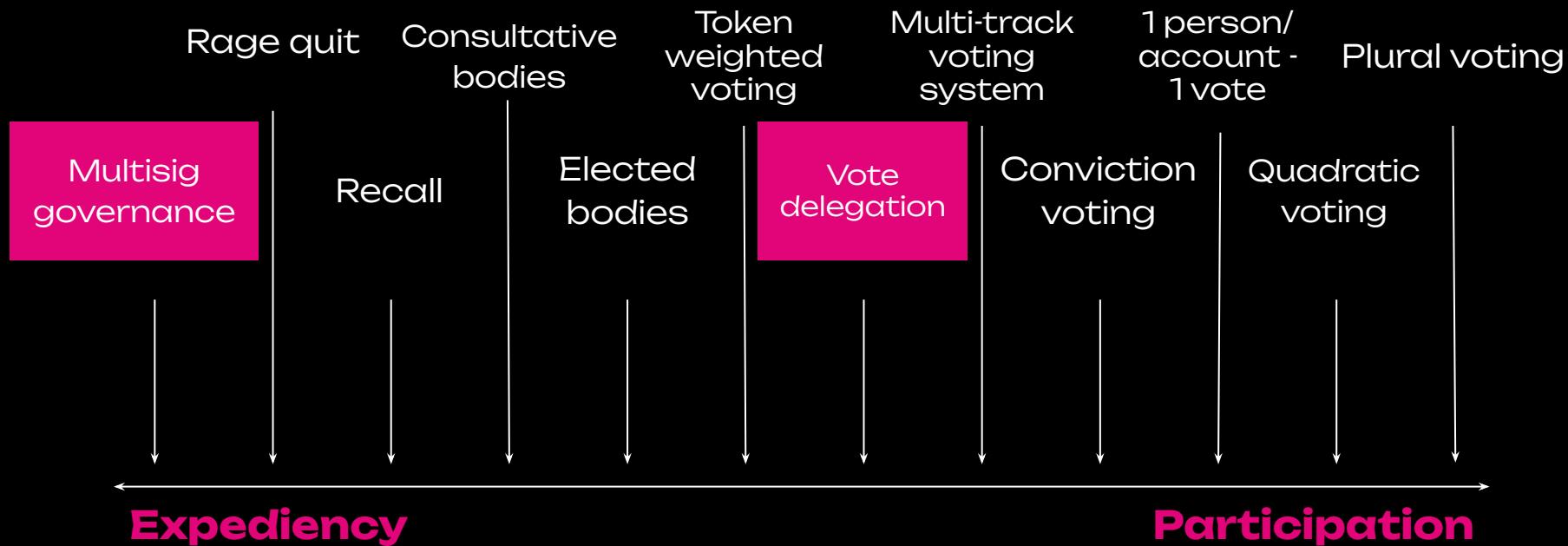
Adaptability

Determinism



Discretion

Pick your ingredients



Case study: Multisig governance



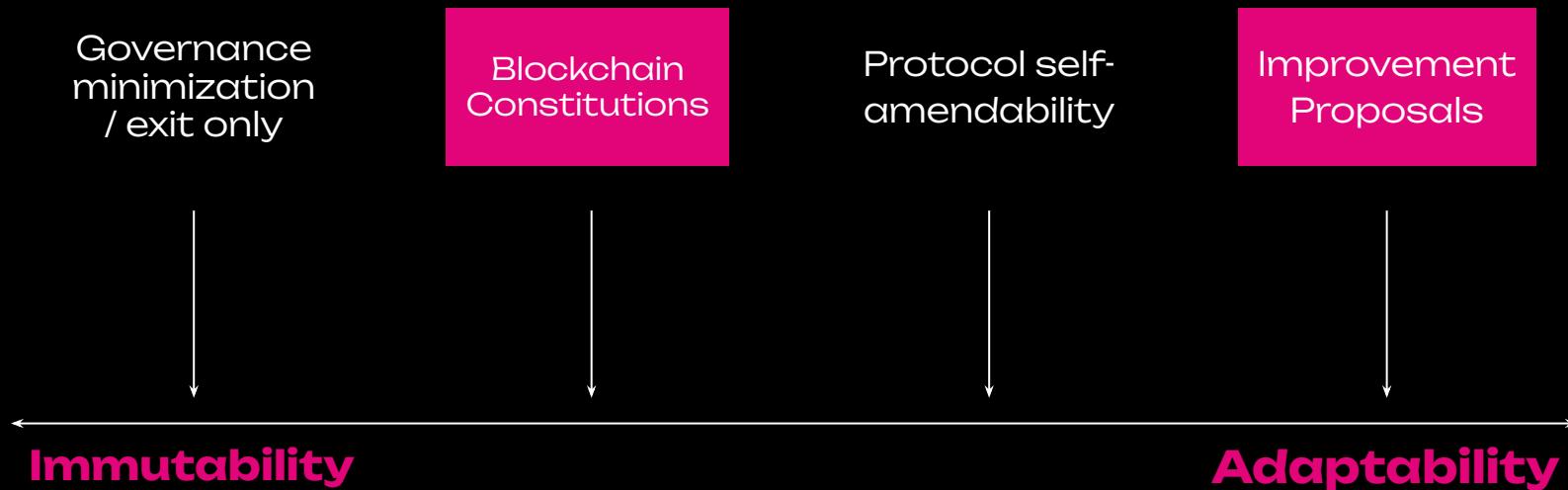
Example: Polygon Protocol Council emergency updates

Case study: Vote delegation



Example: Cardano's DRep system

2: Pick your ingredients



Case study: Blockchain constitutionalism

 **Working Constitution of the Optimism Collective**

 Policies and Templates

 system 

6  Apr 2022

The Optimism Collective is a large-scale experiment in decentralized governance. Our Vision is to sustainably fund those public goods that improve upon the well-being of the Collective and its members. This Working Constitution enshrines governing provisions and principles that, we hope, are calibrated to the ambition of this Vision. It lays the foundation for a fair, democratic model of decentralized governance that's built to last.

1. **This is a “Working” Constitution.** It is exceedingly unlikely that a fixed model of governance will suffice. The Optimism Collective, defined at the outset of this experiment, can appropriately navigate the challenges ahead by being a working constitution.

Constitutions of Web3

* * *

Table of Contents

- I. Introduction
- II. Essay
- III. Constitutions
- IV. Guide
- V. Template

By Joshua Tan, Max Langenkamp, Anna Weichselbraun, Ann Brody, and Lucia Korpas

- [Introduction](#)
- [Part I: Digital Constitutionalism and Web3](#)

[Analyzing DAO Constitutions](#)
[Towards Computational Constitutionalism](#)

The full, comment-enabled version of the paper, including template, [here](#).



**BLOCKCHAIN
CONSTITUTIONALISM:
THE ROLE OF LEGITIMACY
IN POLYCENTRIC SYSTEMS**

Authors: Primavera de Filippi, Morshed Mannan, Kelsie Nabben, Sofia Cossar, Jamila Kamalova, Tara Merk

Example: Optimism's working constitution

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:BIP-1
Status: Replaced
Type: Process
Created: 2011-09-19
Superseded-By: 2
```

Preview Code Blame 85 lines (54 loc) · 4.84 KB ·

[Raw](#)

Ethereum Improvement Proposals (EIPs)

ATTENTION: The EIPs repository has recently undergone a separation of ERCs and EIPs. ERCs are now accessible at <https://github.com/ethereum/ercs>. All new ERCs and updates to existing ones must be directed at this new repository. The editors apologize for this inconvenience.

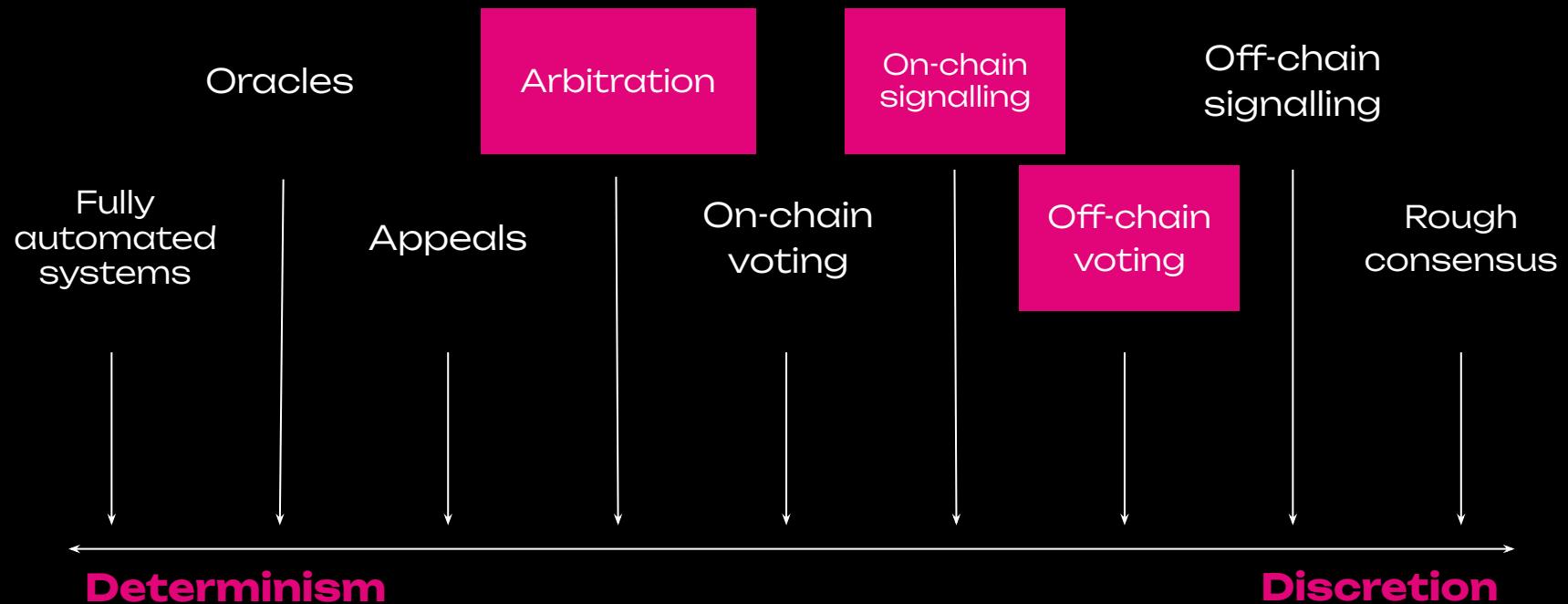
The goal of the EIP project is to standardize and provide high-quality documentation for Ethereum itself and conventions built upon it. This repository tracks past and ongoing improvements to Ethereum in the form of Ethereum Improvement Proposals (EIPs). [EIP-1](#) governs how EIPs are published.

The [status page](#) tracks and lists EIPs, which can be divided into the following categories:

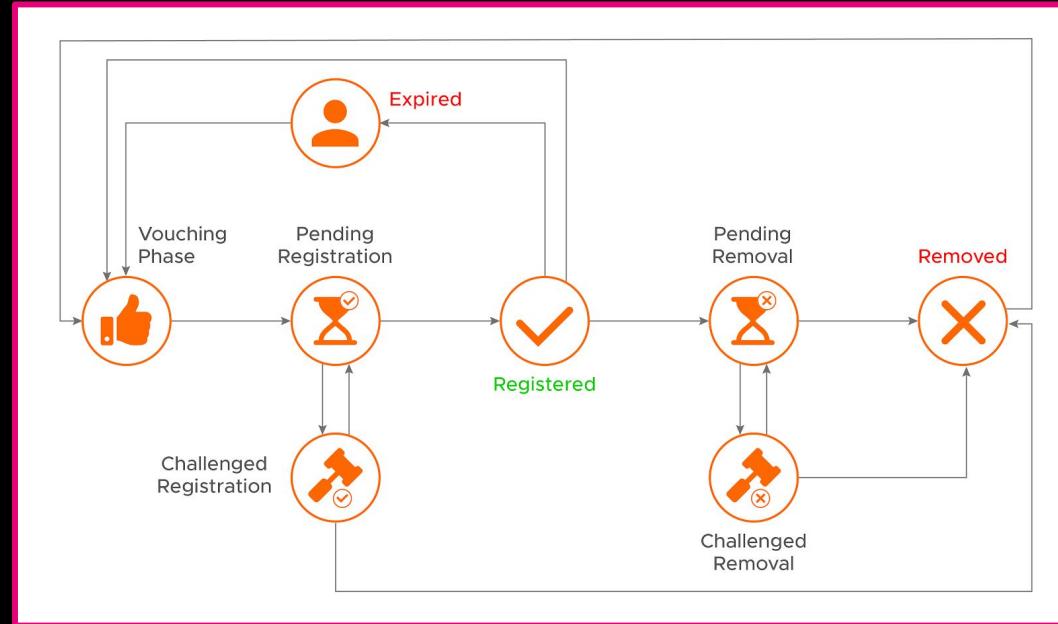
- [Core EIPs](#) are improvements to the Ethereum consensus protocol.
- [Networking EIPs](#) specify the peer-to-peer networking layer of Ethereum.
- [Interface EIPs](#) standardize interfaces to Ethereum, which determine how users and applications interact with the blockchain.

Example: BIPs and EIPs

2: Pick your ingredients

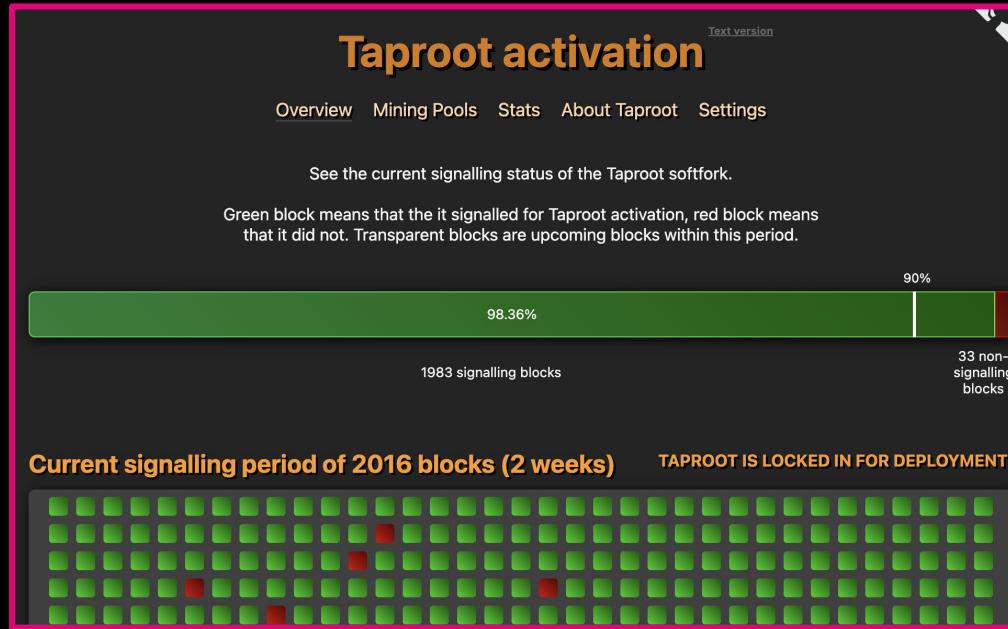


Case study: Arbitration



Example: Proof of Humanity Courts

Case study: On-chain signalling



Example: Bitcoin miner signalling

Case study: Off-chain voting

The screenshot shows a dark-themed web application interface for off-chain voting. At the top left is a yellow lightning bolt icon next to the word "snapshot". On the right is a "Connect wallet" button. A sidebar on the left has three icons: a bar chart, a line graph, and a plus sign. The main content area shows a "Closed" status above the title. The title is "5.4.2] [Social] Funding Request: ENS Public Goods Working Group Term 5 (Q1/Q2)". Below the title is a small circular icon with "ENS by avsa.eth" and a "Share" button. To the right of the title is a "Information" section containing details like Strategie(s), IPFS, Voting system, Start date, End date, and Snapshot count. Further down is a "Results" section showing a horizontal bar chart of the vote distribution.

Information

- Strategie(s) #bafkrei
- IPFS #bafkrei
- Voting system Single choice voting
- Start date Mar 13, 2024, 10:06 PM
- End date Mar 18, 2024, 10:06 PM
- Snapshot 19,428,696

Results

| Vote | Value | Percentage |
|---------|----------|------------|
| For | 1.3M ENS | 89.05% |
| Abstain | 144K ENS | 10.01% |
| Against | 14K ENS | 0.94% |

Example: Snapshot

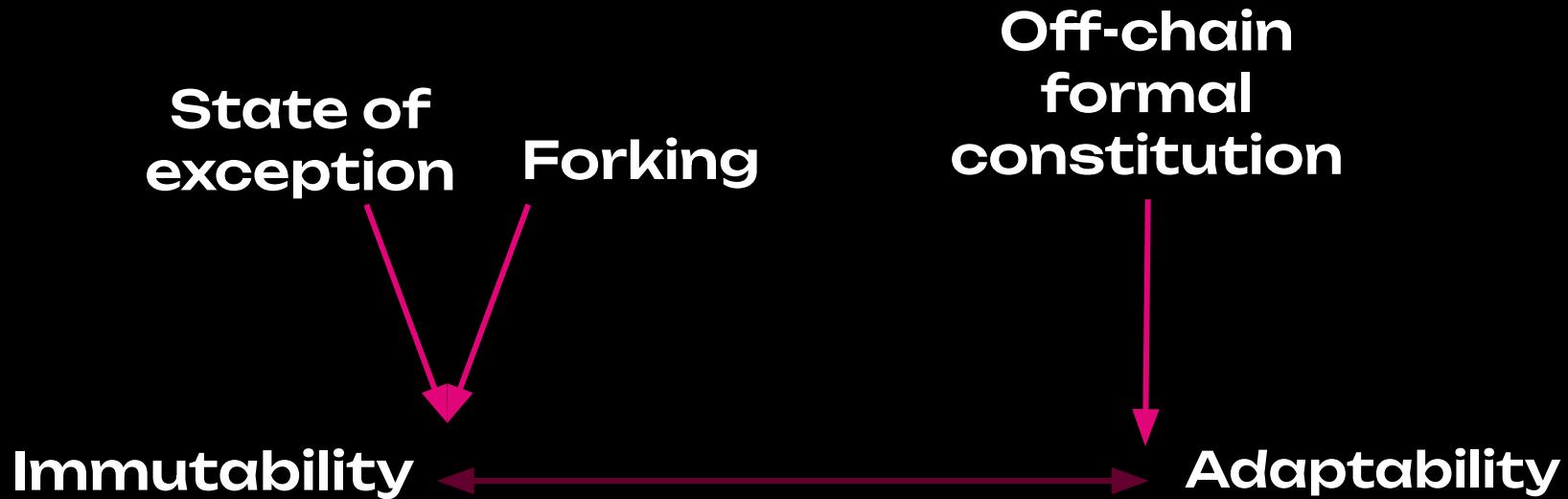
Blockchain governance secret sauce



Keep strong flavors in check



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!



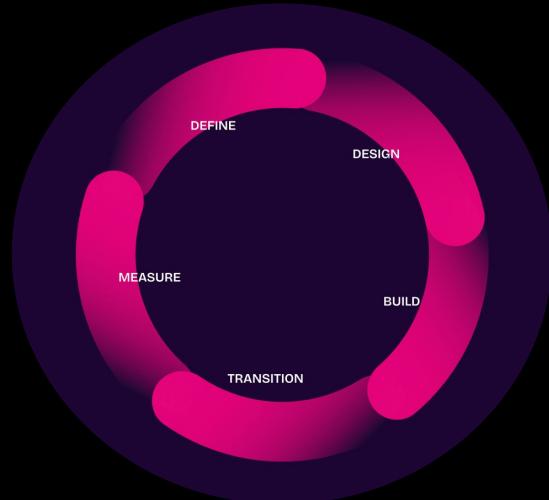
Governance Lifecycle

Lecture 4

Felix Beer

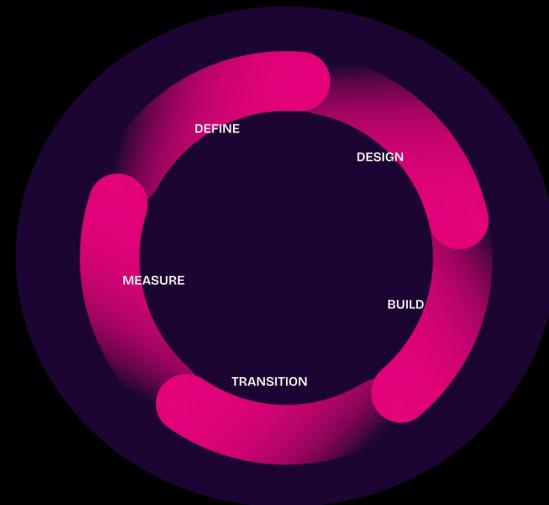
The **lifecycle** perspective

- 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



Blockchain Legality & Regulation

Lecture 6

Primavera de Filippi

“NO BLOCKCHAIN IS AN ISLAND”



New avenues for 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

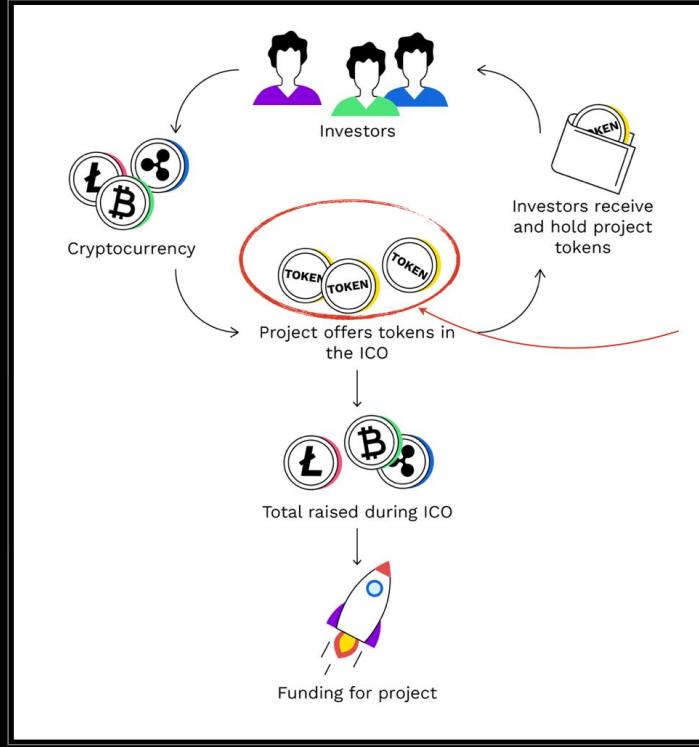


INITIAL COIN OFFERING

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:

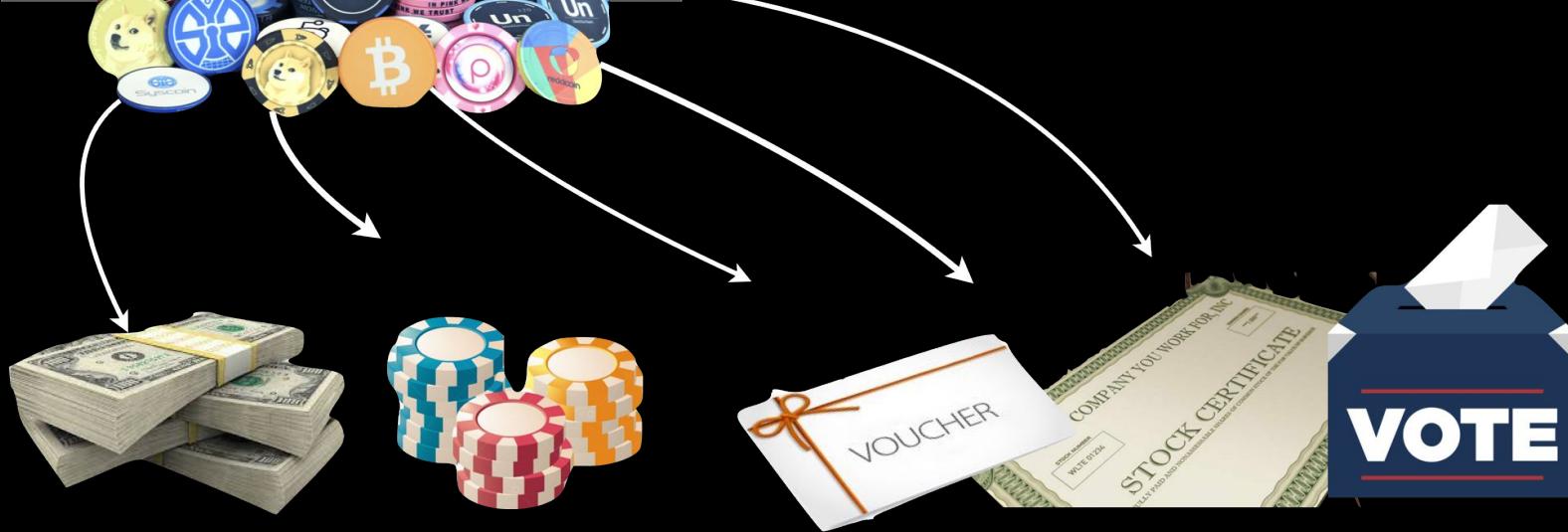
- *the original function of the token (why it was issued)*
- *the practical applications of that token
(beyond the control and intention of the issuer)*

FUNCTIONAL EQUIVALENCE

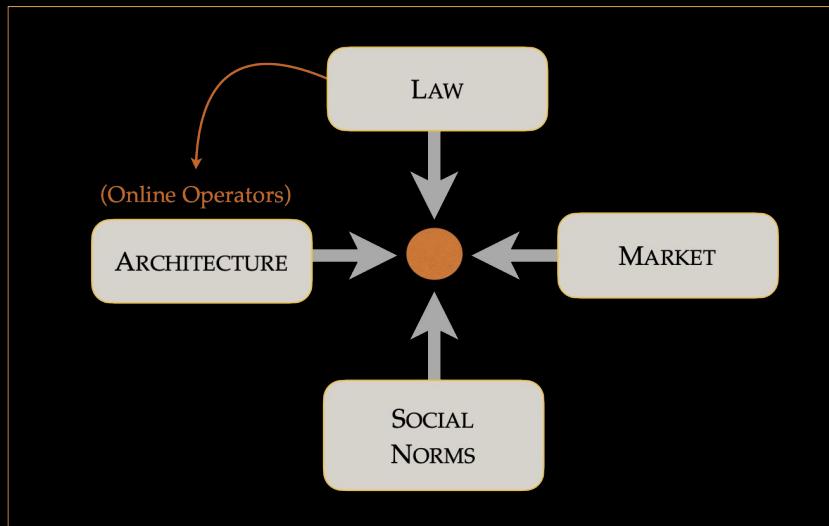


Many tokens usually qualify as multiple classes:

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



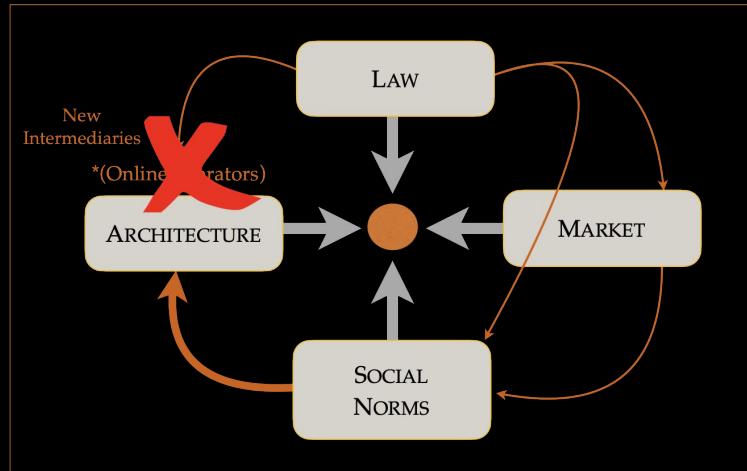
4 LEVERS OF REGULATION ON THE INTERNET



Lawrence Lessig

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

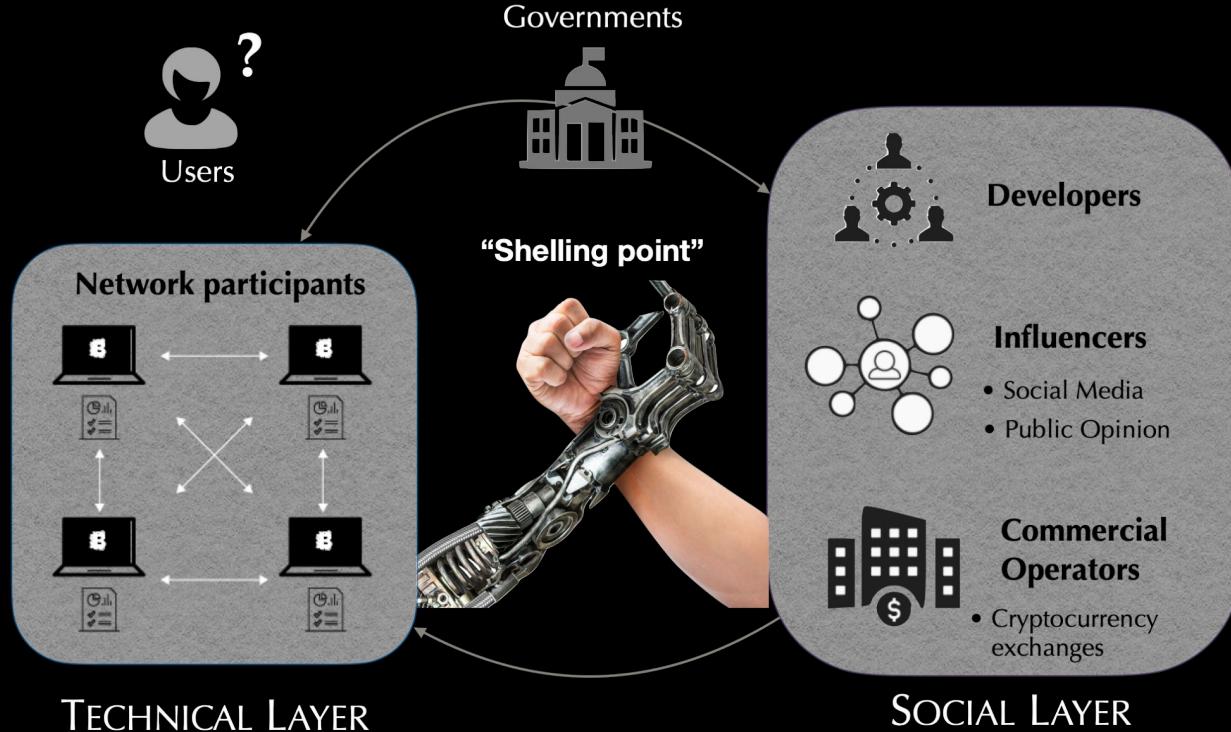
4 LEVERS OF REGULATION ON THE BLOCKCHAIN



Lawrence Lessig

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

BLOCKCHAIN BETWEEN REGULATION & GOVERNANCE



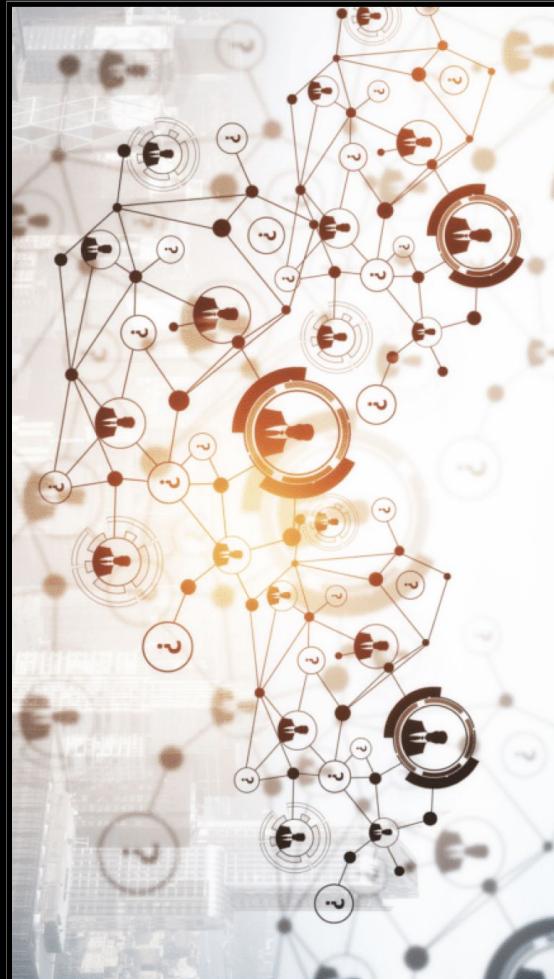
USERS

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



INFOMEDIARIES



- ❖ Obligation to filter Internet traffic (e.g. China)
- ❖ Slow down traffic towards a specific blockchain
- ❖ De-referencing of illicit blockchain apps
- ❖ No advertisement for these apps (e.g. ICOs)

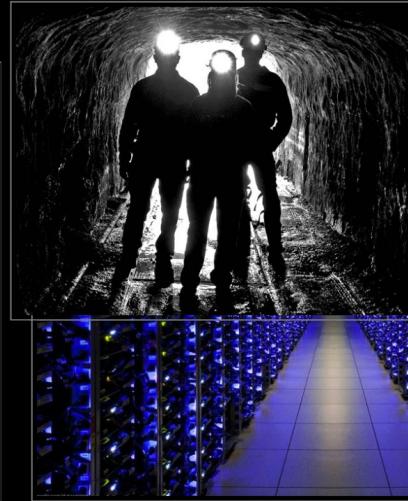
NEW INTERMEDIARIES

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

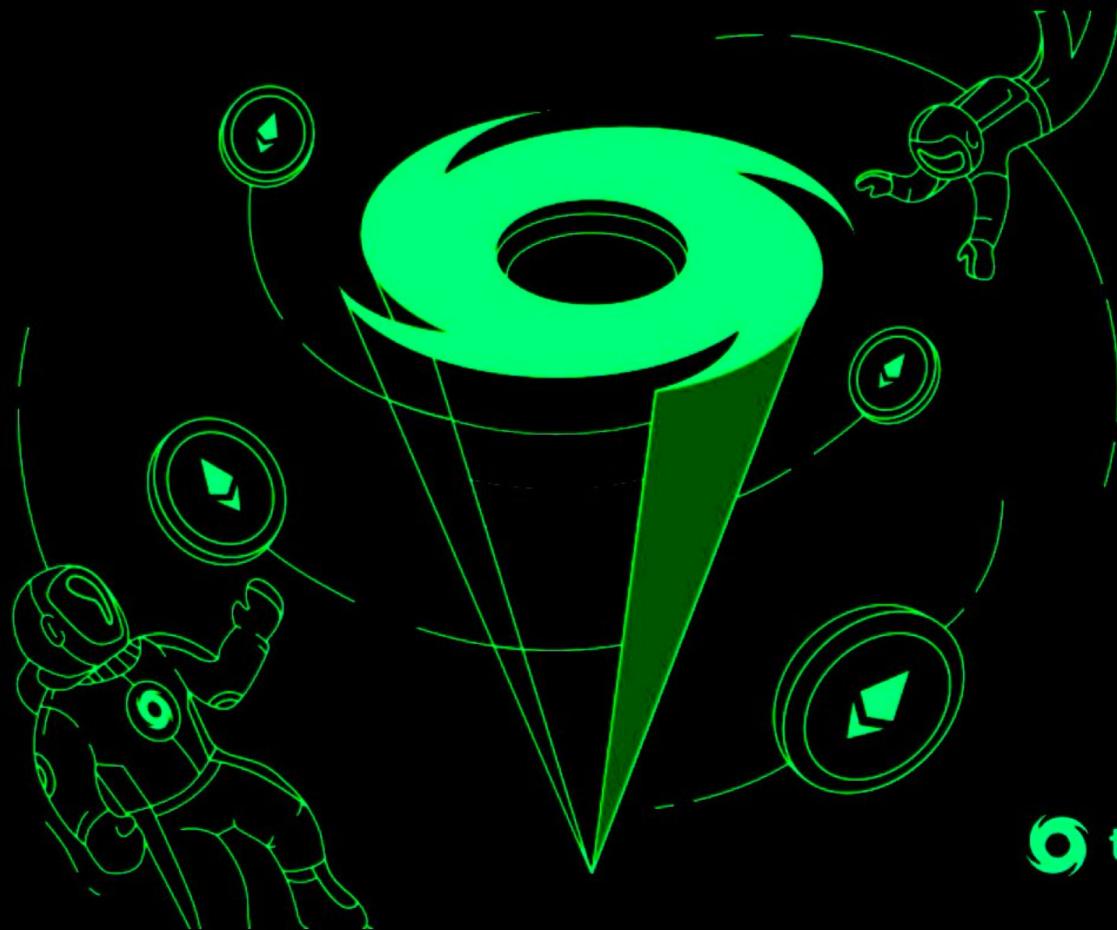
BACKDOORS

- ❖ Obligation to introduce *backdoors* in the code in order to provide “veto right” to public authorities
 - ❖ 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

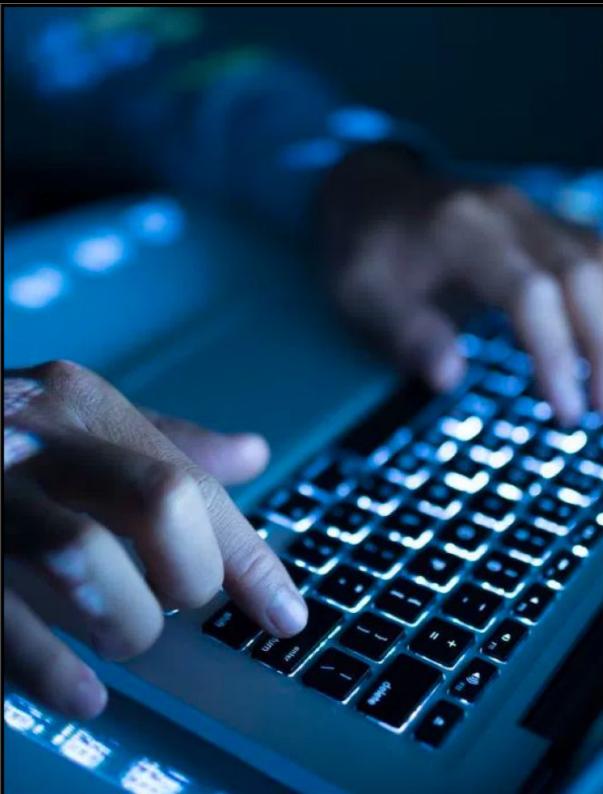
NO LEGAL ENTITY
JUST A SMART CONTRACT

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)

CHILLING



U.S. Persons
(Strict liability)

EFFECTS



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!



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 ?

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

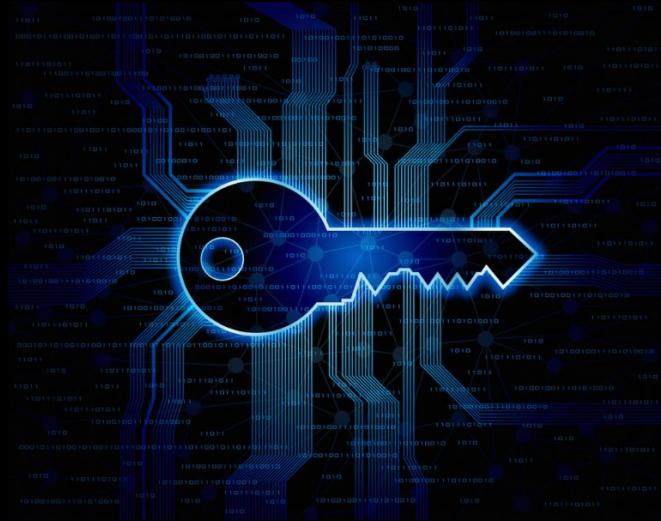
(1) Ensure the alignment of management team and investors with long-term success
(2) Prevents ppl to engage into speculative practices such as “pump and dump”.



- 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



PROOF OF RESERVE

—REAL-TIME AUDITING—

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

KEYLESS WALLETS

—NO CUSTODY—

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



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)

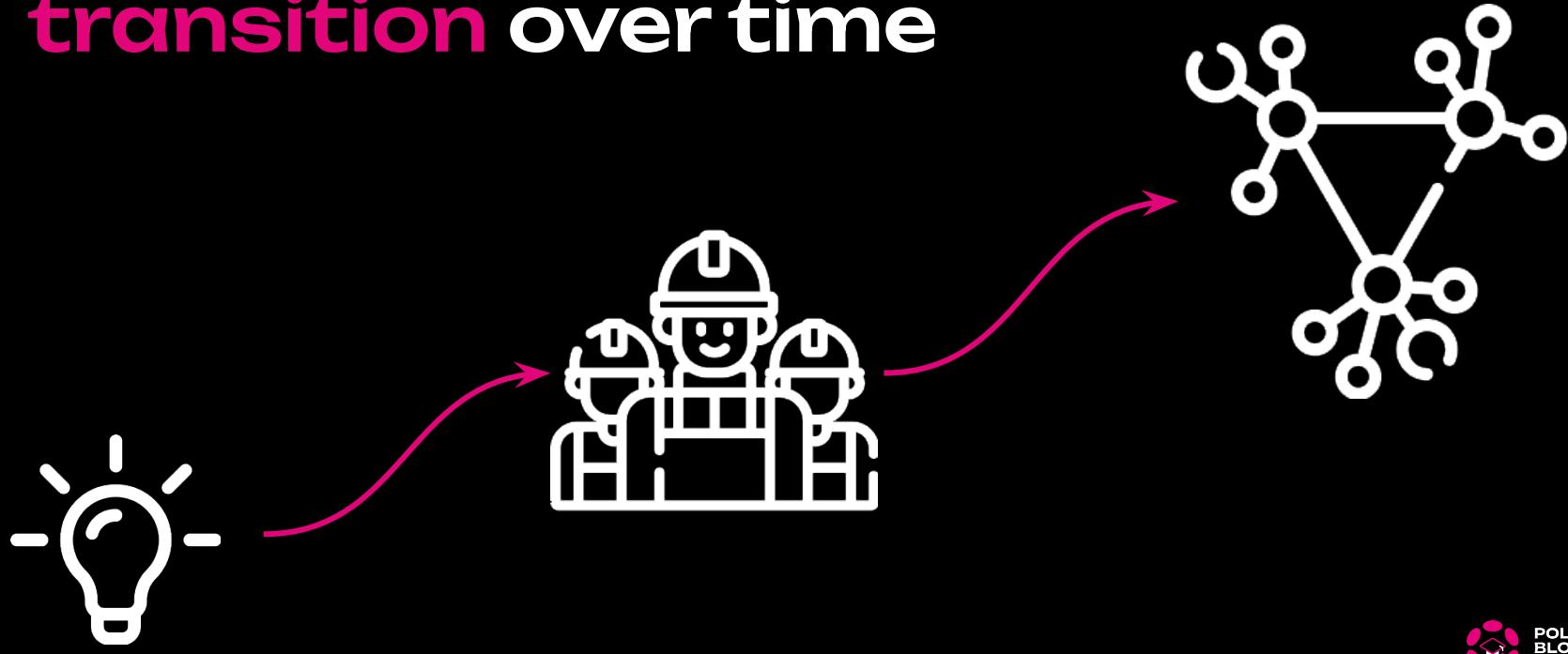


(Progressive) Decentralization & Exit to Community

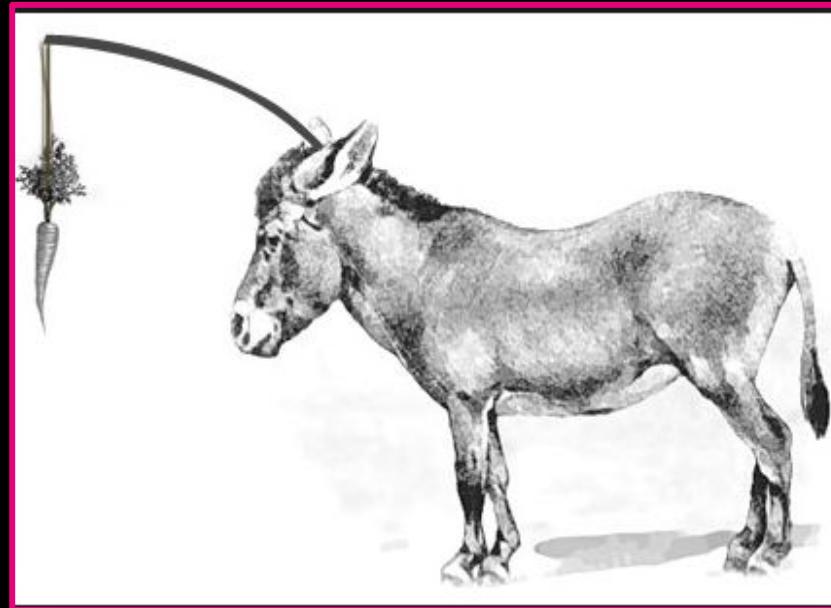
Lecture 7

Tara Merk

Many blockchain projects start
with **centralized governance** and
transition over time

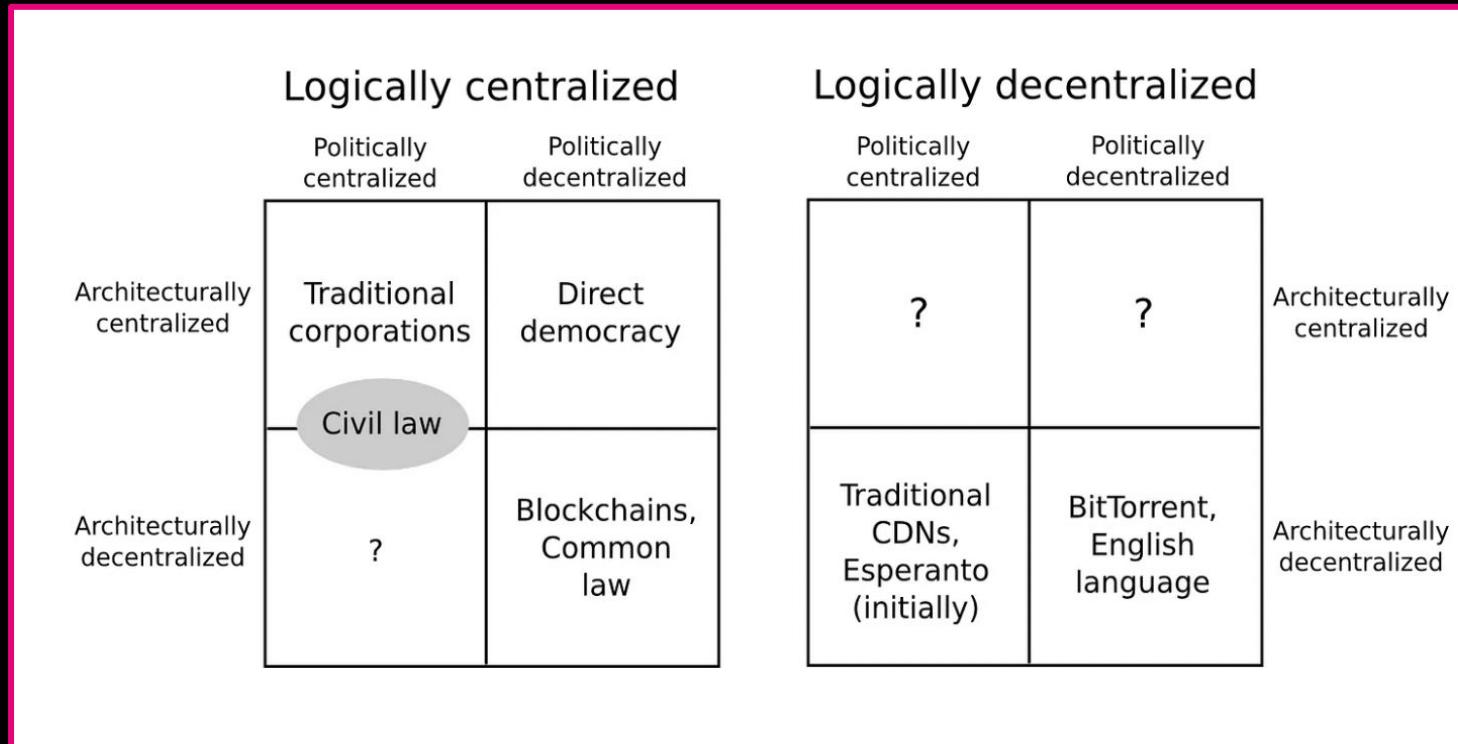


Decentralization is the holy grail



But: what is decentralization, actually?

Definitions of Decentralization



More definitions of Decentralization

The screenshot shows a journal article from the Internet Policy Review. The header includes the journal logo (a stylized 'R' inside a hexagon), the title 'INTERNET POLICY REVIEW', and the status 'OPEN ACCESS'. Below the header is a navigation bar with categories: DIVERSITY, GOVERNANCE, INFRASTRUCTURE & STANDARDS, INFORMATION & DATA, INNOVATION, and more. The main content area displays the following information:

- Volume 10, Issue 2 | Concepts of the digital society**
- Decentralisation: a multidisciplinary perspective**
- Authors: 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](https://doi.org/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 technosocial 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

More definitions of Decentralization

Sufficient Decentralization: A Playbook for web3 Builders and Lawyers

By [Marc Boiron](#), Chief Legal Officer at dYdX Trading¹

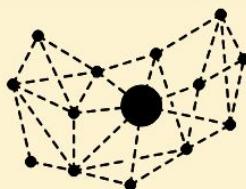
Introduction

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

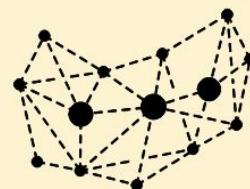
Who has read/ write access?

Principle 1: Consider the level of decentralisation



Permissioned
private
blockchain

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



Permissioned
public
blockchain

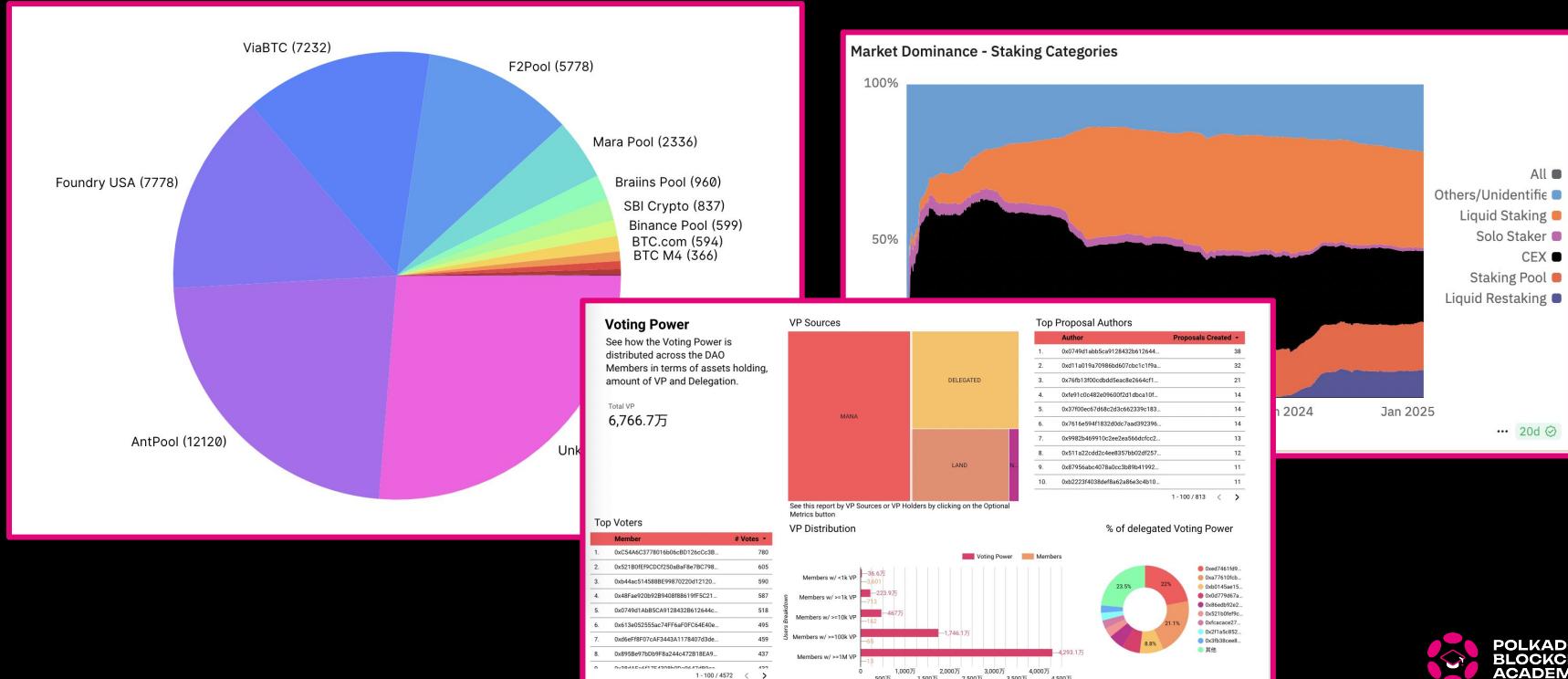
- Governing structure: A consortium of multiple authorities.
- Decentralisation level: Medium.



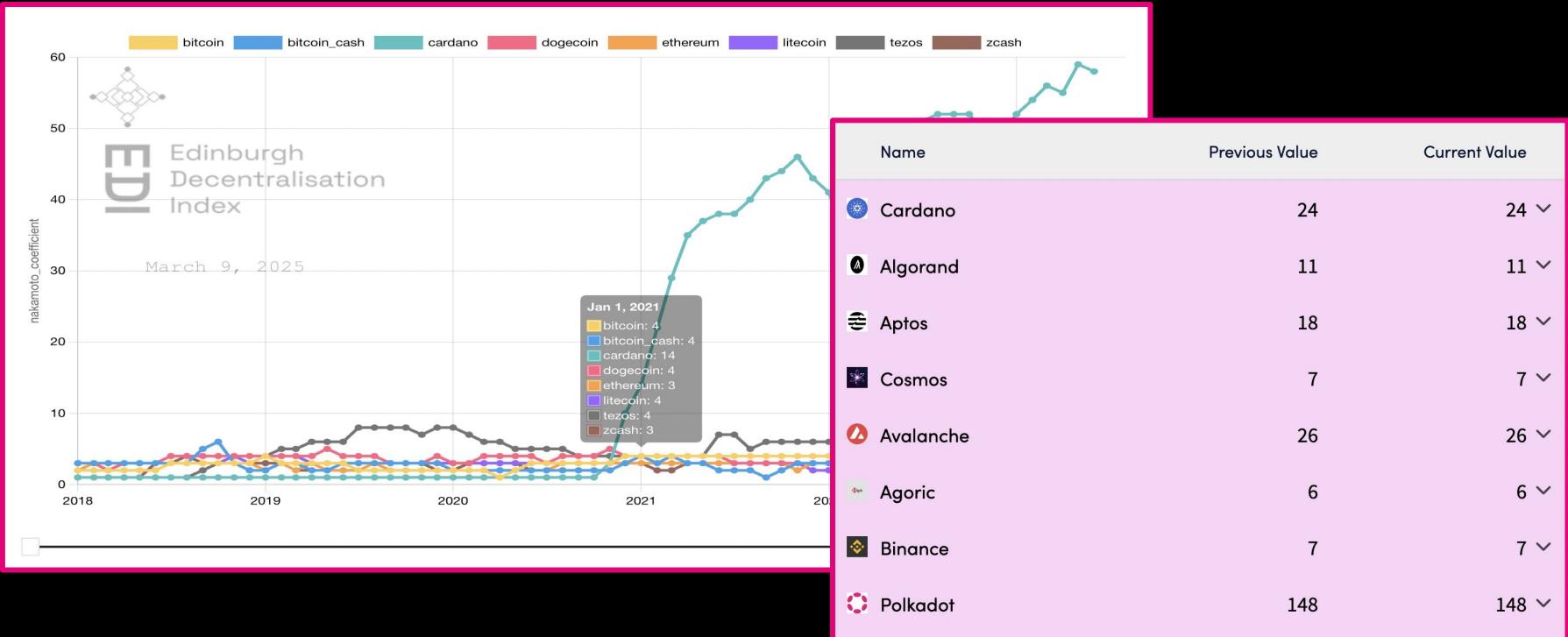
Permissionless
public
blockchain

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

What is the mining/staking/ voting distro?



Nakamoto coefficient



Optimism CoP measurement



CPI



Concentration of Power Index

Explore Index →

in DAOs {

Tracking and analyzing the distribution of influence
within decentralized governance structures }

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

Toward Equitable Ownership and Governance in the Digital Public Sphere

Connor Spelliscy
Sarah Hubbard
Nathan Schneider
Samuel Vance-Law



Exit to Community Stories & Strategies

A library of community ownership

GEORGETOWN LAW TECHNOLOGY REVIEW

EXIT TO COMMUNITY: STRATEGIES FOR MULTI-STAKEHOLDER OWNERSHIP IN THE PLATFORM ECONOMY

Morshed Mannan* & Nathan Schneider**

CITE AS: 5 GEO. L. TECH. REV. 1 (2021)

Learning from experience



Progressive decentralization

The screenshot shows a web browser window with the alózcrypto logo in the top left corner. The main title 'Progressive Decentralization: A Playbook for Building Crypto Applications' is displayed in a large, bold, dark font within a yellow header bar. Below the title, the author's name 'Jesse Walden' is shown. Underneath the author's name are several small, light-colored circular tags containing category names: COMPANY BUILDING, DECENTRALIZATION, GLOSSARIES & TERMINOLOGY, and PROGRESSIVE DECENTRALIZATION. At the bottom of the page, there is a date '1.9.20'.

The screenshot shows a web browser window with the alózcrypto logo in the top left corner. The main title 'Progressive decentralization: a high-level framework' is displayed in a large, bold, dark font within a yellow header bar. Below the title, the authors' names 'Jad Esber and Scott Duke Kominers' are shown. Underneath the authors' names are several small, light-colored circular tags containing category names: COMPANY BUILDING, DECENTRALIZATION, GUEST POSTS, MENTAL MODELS & FRAMEWORKS, PROGRESSIVE DECENTRALIZATION, and RESEARCH. At the bottom of the page, there is a date '1.12.23'.

A blockchain specific playbook

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 only thing 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

Where does the transition **end**?

Where does the transition end?

The screenshot shows the homepage of the Internet Policy Review journal. At the top, there's a navigation bar with categories: DIVERSITY, GOVERNANCE, INFRASTRUCTURE & STANDARDS, INFORMATION & DATA, INNOVATION, and INTELLECTUAL. Below this is a teal header bar with the journal's name and some icons. The main content area features an article by Balázs Bodó, Jaya Klara Brekke, and Jaap-Henk Hoepman. The article title is "Decentralisation: a multidisciplinary perspective". It includes author details, a DOI (10.14763/2021.2.1563), and a peer-reviewed status. There's also a section for an abstract.

The screenshot shows a Medium post titled "The Meaning of Decentralization" by Vitalik Buterin. The post has 24K views and 92 comments. The text discusses the concept of decentralization in the context of blockchain technology, mentioning that it is often viewed as a blockchain's entire purpose. A quote from the post is highlighted in a pink box: "Sufficient Decentralization: A Playbook for web3 Builders and Lawyers".

Sufficient Decentralization: A Playbook for web3 Builders and Lawyers

By [Marc Boiron](#), Chief Legal Officer at dYdX Trading¹

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.

Understanding decentralization

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



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.

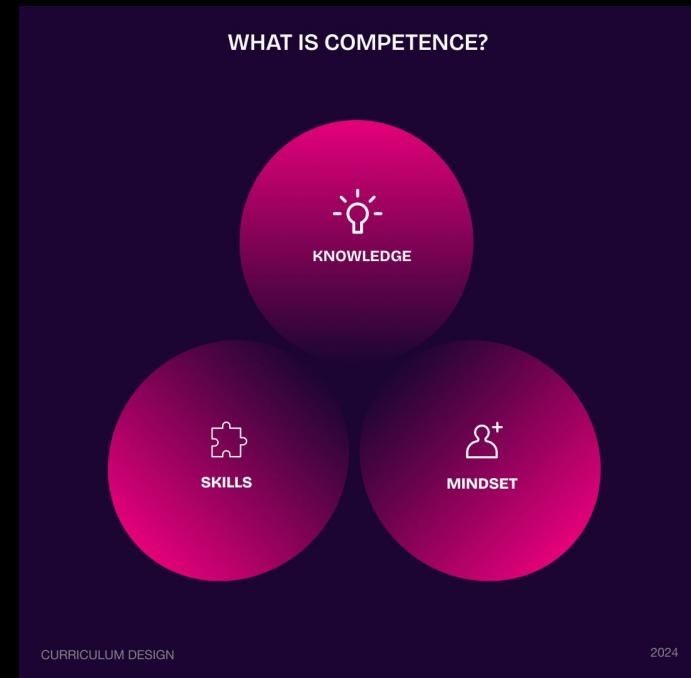
Blockchain governance literacy

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**)



2024

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

?

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

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

Technical Proficiency

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

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

Legal & Regulatory
Literacy

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

Adaptive Governance Innovation

Objective: Steering governance evolution through continuous experimentation and learning.

Adaptive
Governance
Innovation

Skills: Evaluate systems, lead experiments, refine models

Knowledges: Impact evaluation, scenario planning, adaptive design

Mindsets: Futures thinking, continuous learning

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**.

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?



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.