Primavera De Filippi

CERSA / CNRS / Université Paris II
Harvard Law School

@yaoeo

Wessel Reijers

European University Institute

@WesselReijers

Blockchain as a Confidence Machine

The Problem of Trust & Challenges of Governance

Introductory Remarks

2008 Financial Crisis: Dawn of a Crisis of Trust?

Blockchain Technology as Potential Solution

TRUSTLESSNESS

Forbes

Mar 31, 2019, 08:32pm EDT | 3,275 views

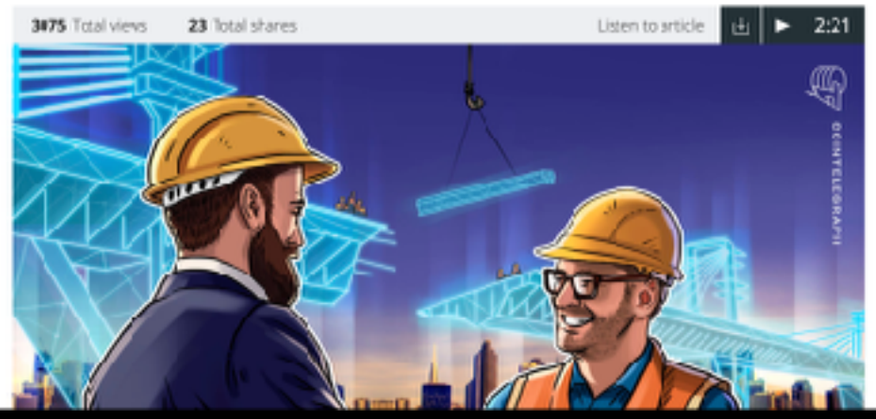
Building Trust In The Trustless: Blockchain's Best Asset Is Holding It Back

Jemma Green Contributor ©
Crypto & Blockchain

ANDREY SHEVCHENKO DEC 08, 2020

RSK launches Powpeg, a trustless Bitcoin bridge architecture

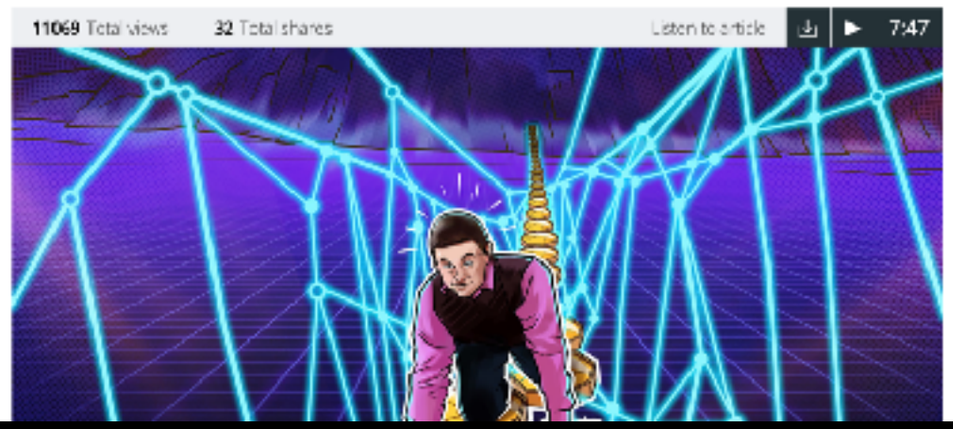
The pegging process no longer relies on functionaries holding custody of bridged funds.



ANTÓNIO MADEIRA NOV 19, 2020

Who watches the watchmen? Crypto may not be as trustless as it seems

Crypto is often seen as trustless and failproof. But as more regulation, venues and developers come aboard, just how trustless is it really?



Structure

1.

Trust and confidence are distinct phenomena

2.

Blockchain technology as a confidence machine

3.

Distributed trust still needed, challenges of governance

Trust

vs.

Confidence

Two Concepts

Trust, "treuwaz": strength, consolation

Confidence, "com-fidere":
together, having faith or believing

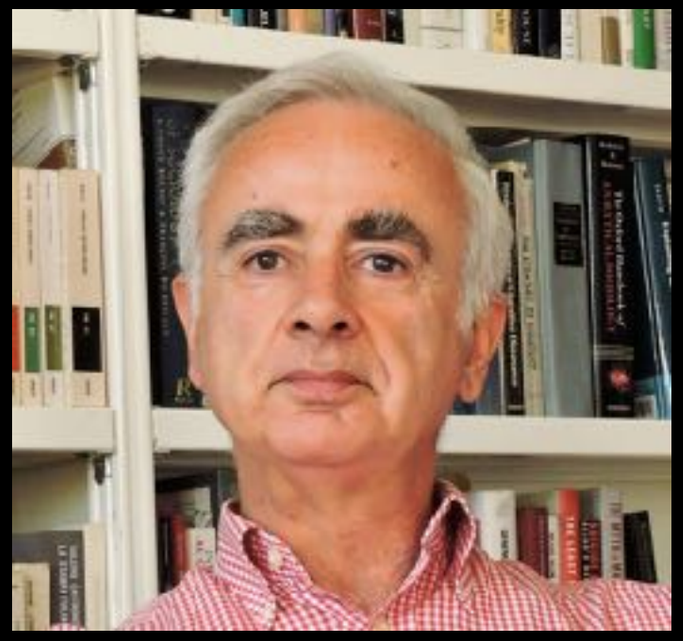
Trust

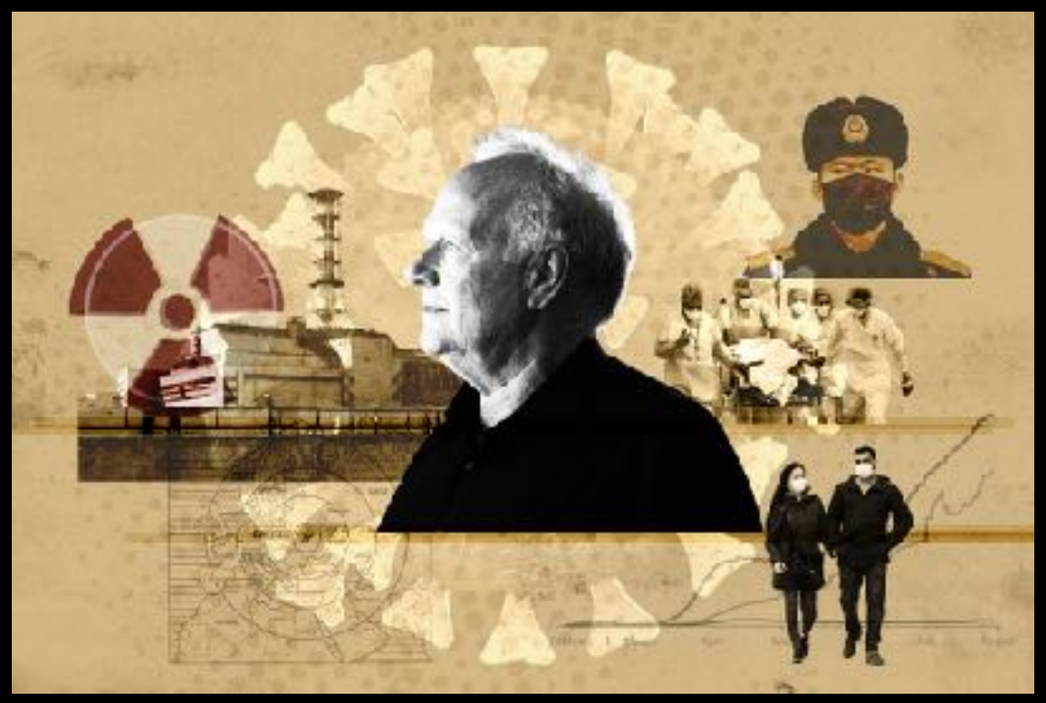
Multifaceted, complex social phenomenon

Vulnerability, Expectation (probability)

Trust helps 1) delegating tasks, 2) ensuring their proper performance

Flipside: uncertainty, risk society





A psychological attitude or mood

Rational choice

Tacit acceptance

Predictability
Reliability

Access points
Designers

Interaction
Others

Where Does Trust...

Come From?

CONFIDENCE

No assumption of risk and vulnerability or free choice between alternatives

Simmel: "Weak inductive knowledge"

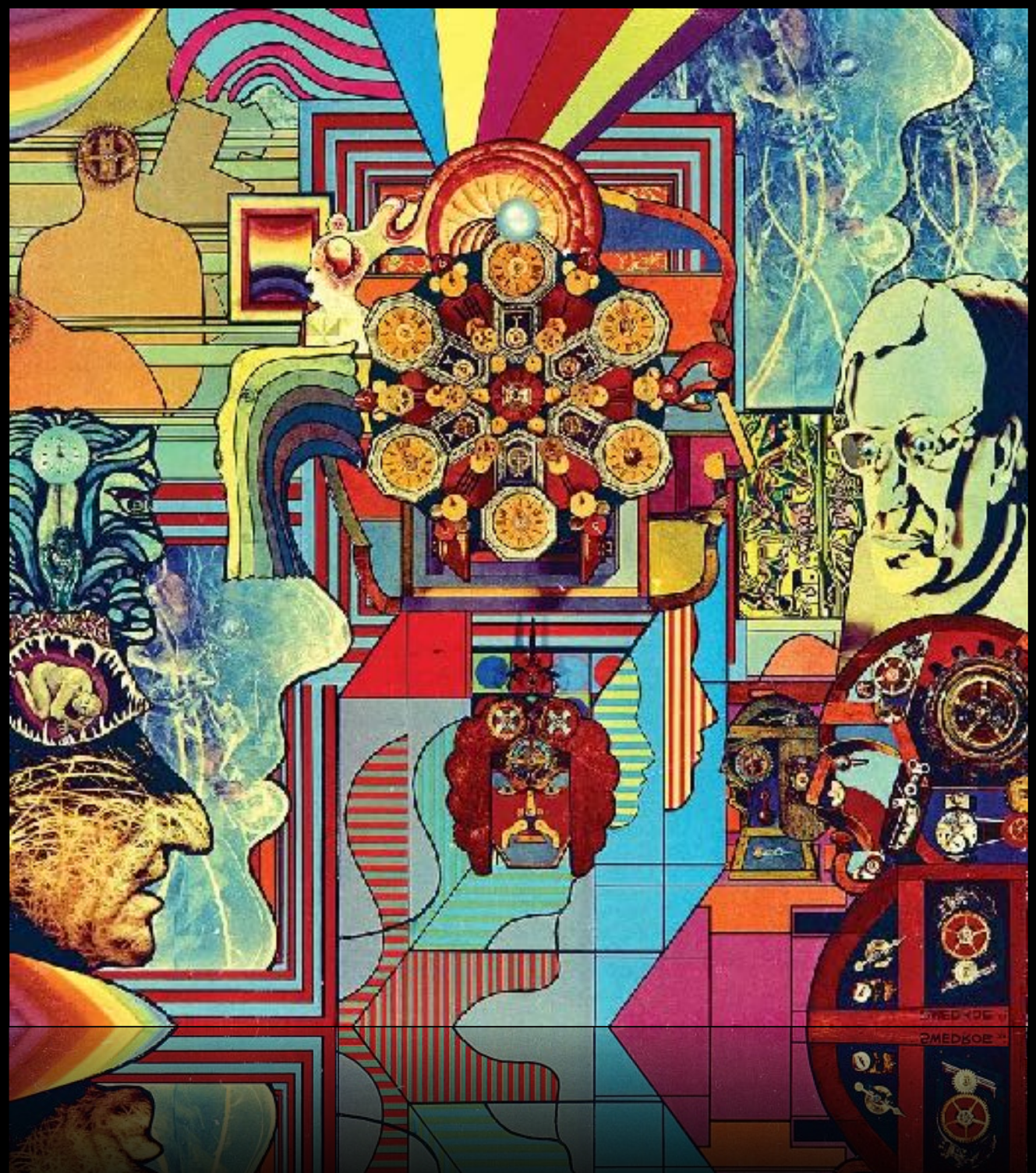
Acting on assumption that system lacks agency to betray expectations

Confidence

One does not decide to be confident, one "is" confident

Confidence implies a lack of agency, e.g., through role expectations

Trust is addressable, confidence is not



Interplay between trust & Confidence

Trust in agents boosted by confidence in (sub-)systems

Confidence often dependent on trust in higher level actors or institutions; expert systems

Blockchain

As A

Confidence Machine

Replacing Trust with Confidence

Luhmann:
"The more complex a system is, the longer it takes to build expectations about the operations of that system"

Hume:
"Governments and other complex institutional arrangements should not be trusted at the outset"

Hardin:
"Need checks & balances and transparency requirements to allow for the emergence of more trustworthy systems"

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

"Don't trust, Verify"

The Economist:
"Trust Machine"

Werbach:
"Trustless Trust"

BLOCKCHAIN AS... (negative definition)

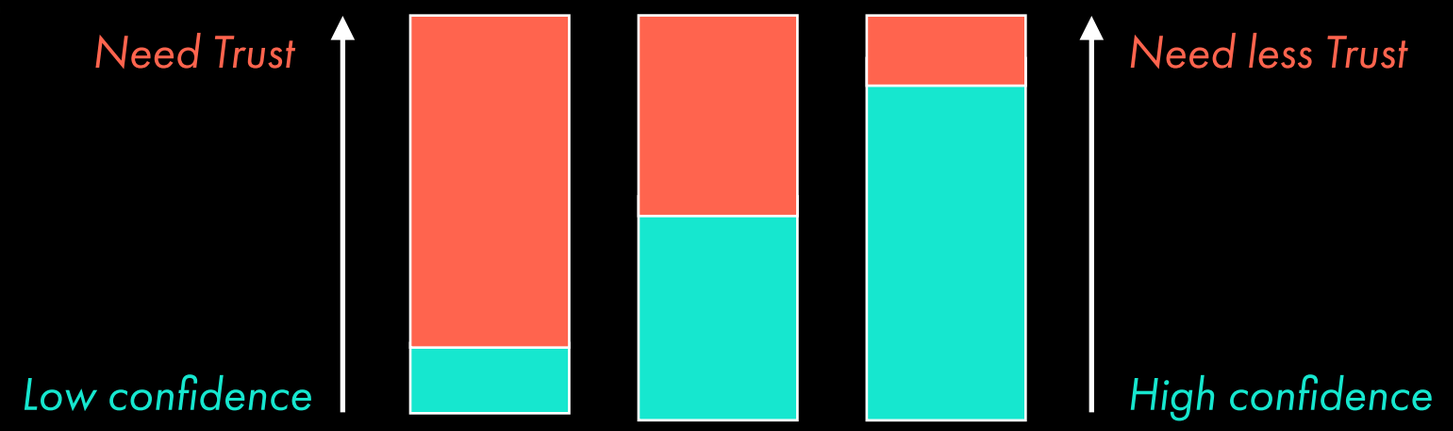
TRUSTLES TECHNOLOGY

*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

Confidence Factors

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

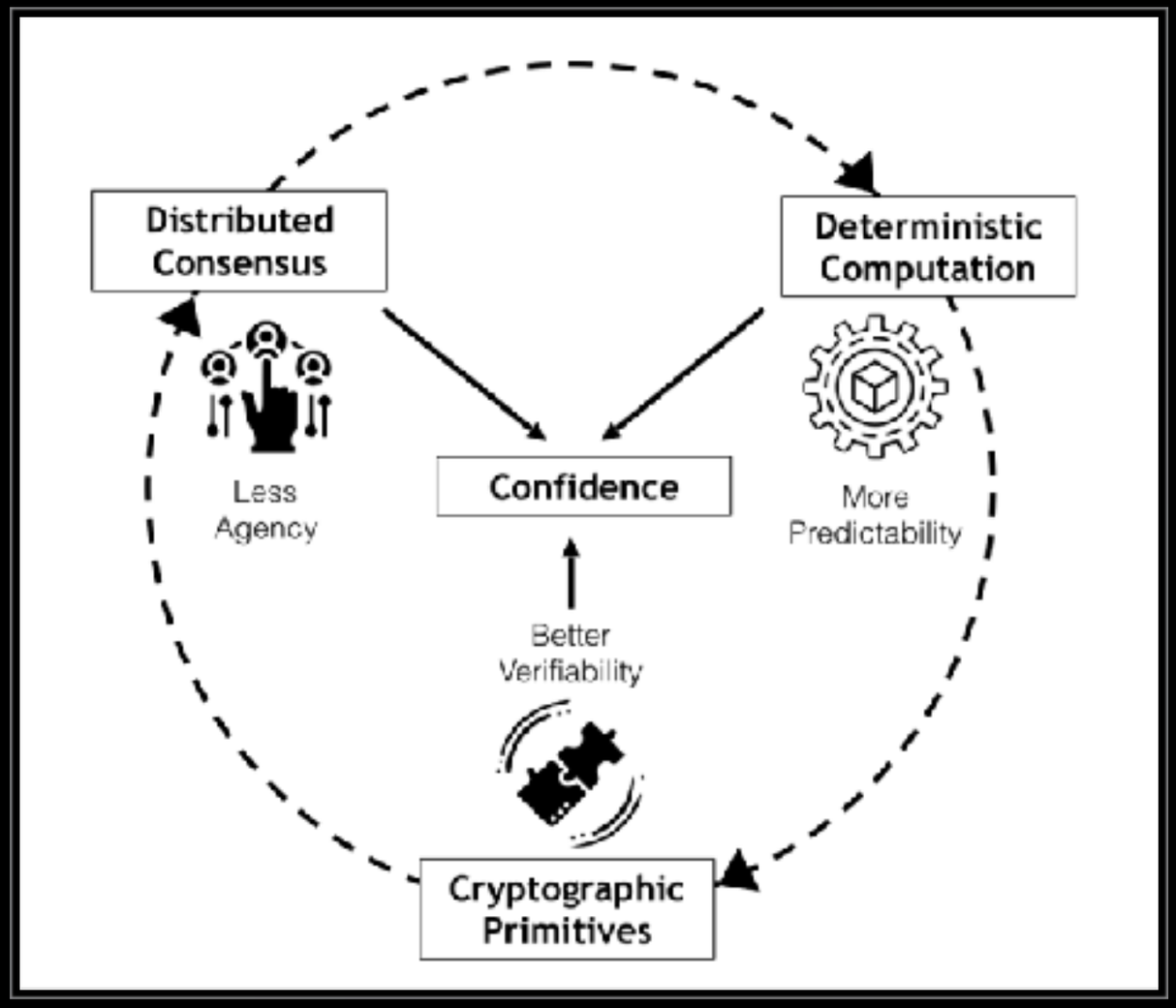
- *Hashing functions, Public-Private Key, etc.*

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

- *Utility function*
- *Distributed Consensus*

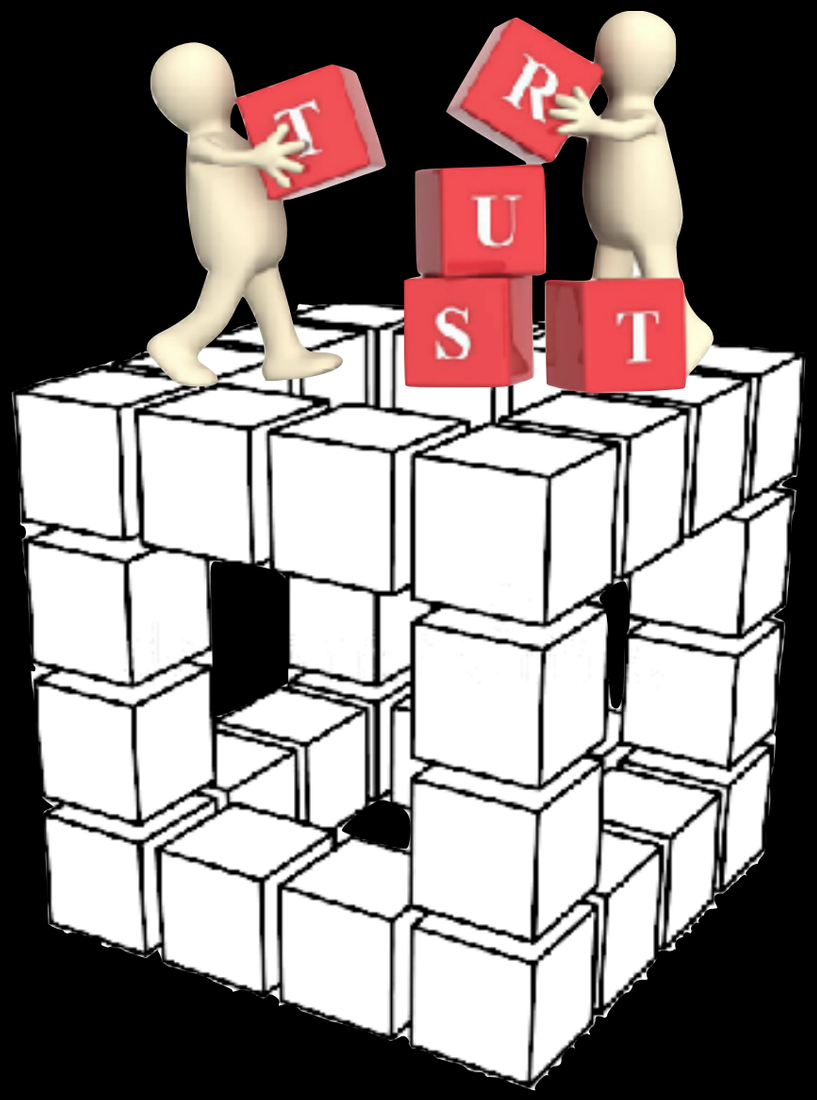
(3) ***Expert systems***

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



Blockchain as... (positive definition)

Confidence Machine



TRUST
IN INSTITUTIONS

CONFIDENCE
IN TECHNOLOGY

BLOCKCHAIN AS... (positive definition)

CONFIDENCE MACHINE

Bringing Trust back in

Blockchains as Socio-Technical Systems

Confidence *in the* ***technology*** *requires* ***Trust*** *in the* ***operators*** *of the technology*

1. Developpers

Core Developpers

Open Source contributors

Technocratic Governance

- Decision on who can push to a repository
- Technical decisions are political decisions
- Contentious issues (e.g. forks)

2. Maintainers

Miners

Validators

Network Governance

- Distributed consensus
- Hashing power as political power
- Validators as legitimate counter-power

3. End-Users

Users

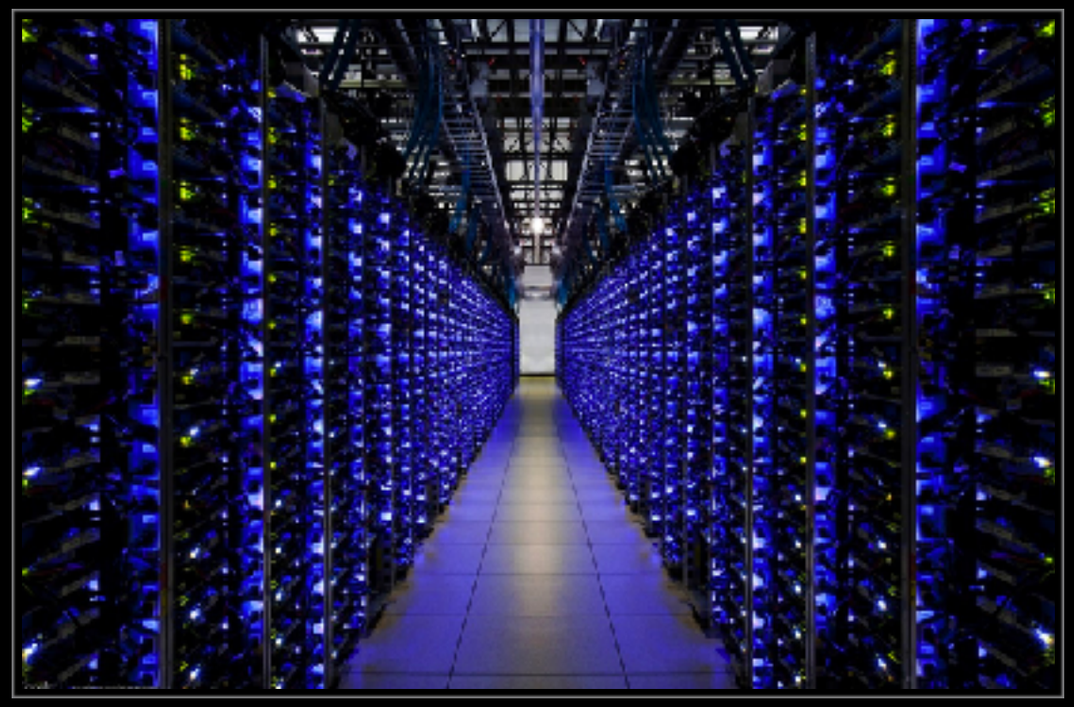
Token holders

Plutocratic Governance

- Exit vs. Voice
- Market-based influence (e.g. “whales”)
- Token-based governance (e.g. Carbon voting)

4. New Intermediaries

Super Nodes



Mining Pools

— Cryptocurrency exchanges, Blockchain explorers,
— DApps interfaces, Custodian wallets,
— Commercial service providers, etc.

Delegated Governance

- Centralized Points of Failure & Control
- Invisible powers that can influence the network

5. Experts

Founders

Influencers

Meritocratic Governance

- Tech-savvy individuals are more respected
- Founders hold strong influence in the governance
- Most vocal individuals can influence the public opinion

6. Laws & Regulations

Policy Makers

Regulators

Exogenous Governance

- Provide legitimacy to specific blockchain applications
- Indirectly influence the decision-making of endogenous actors
- Directly regulate the operations of new intermediaries

The Rule of Code

vs.

The Rule of 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

RULE ~~OF~~ BY LAW

INSTRUMENTALISATION OF LAW

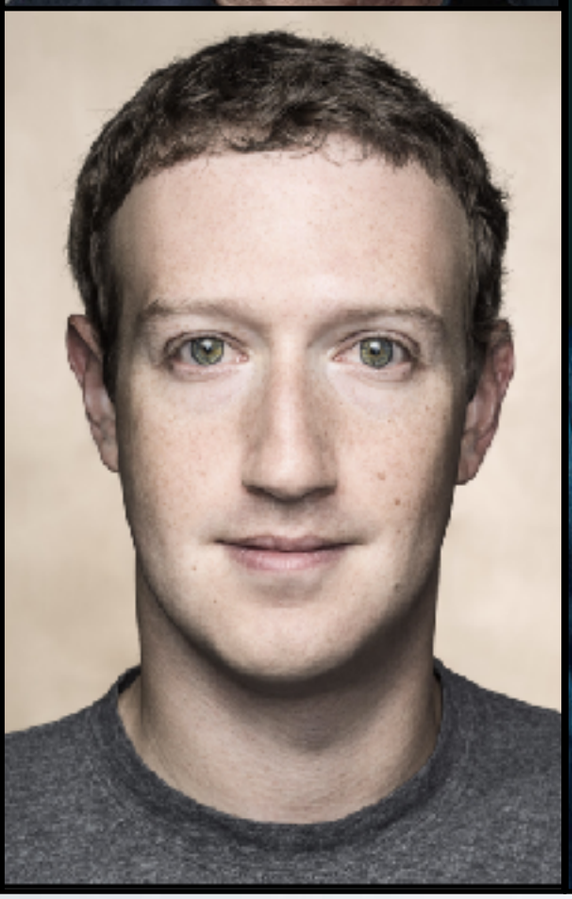
AS A TOOL OF POLITICAL POWER

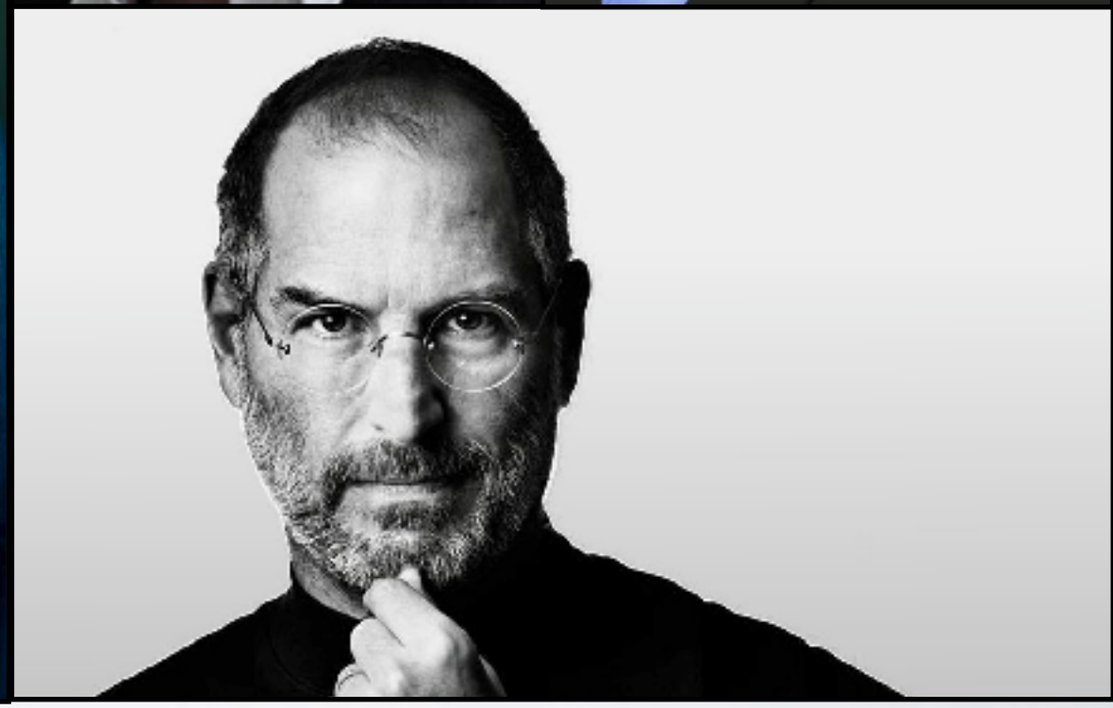
JP Barlow

Timothy May

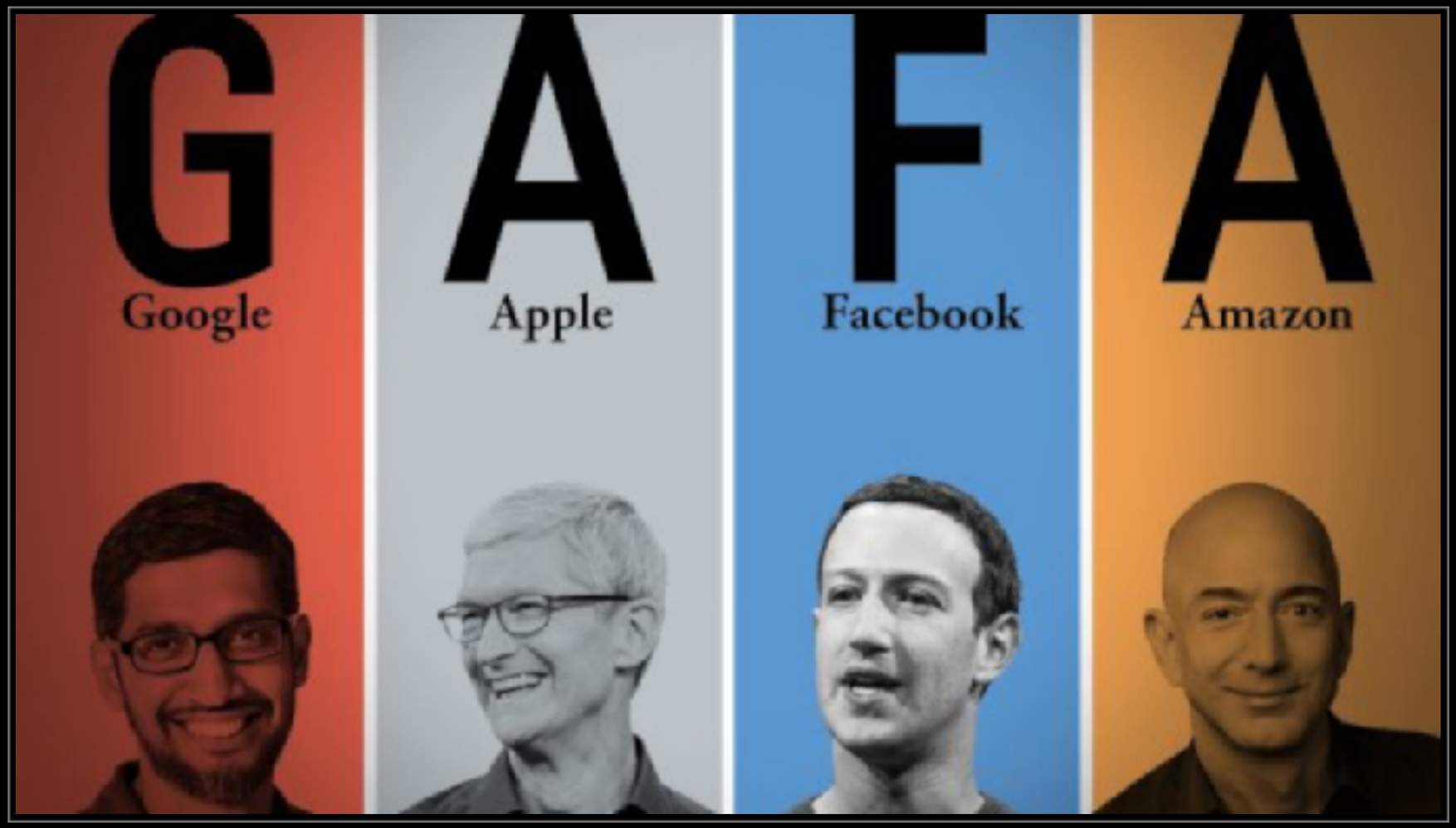
Cyberspace

as an independent space that cannot be Regulated





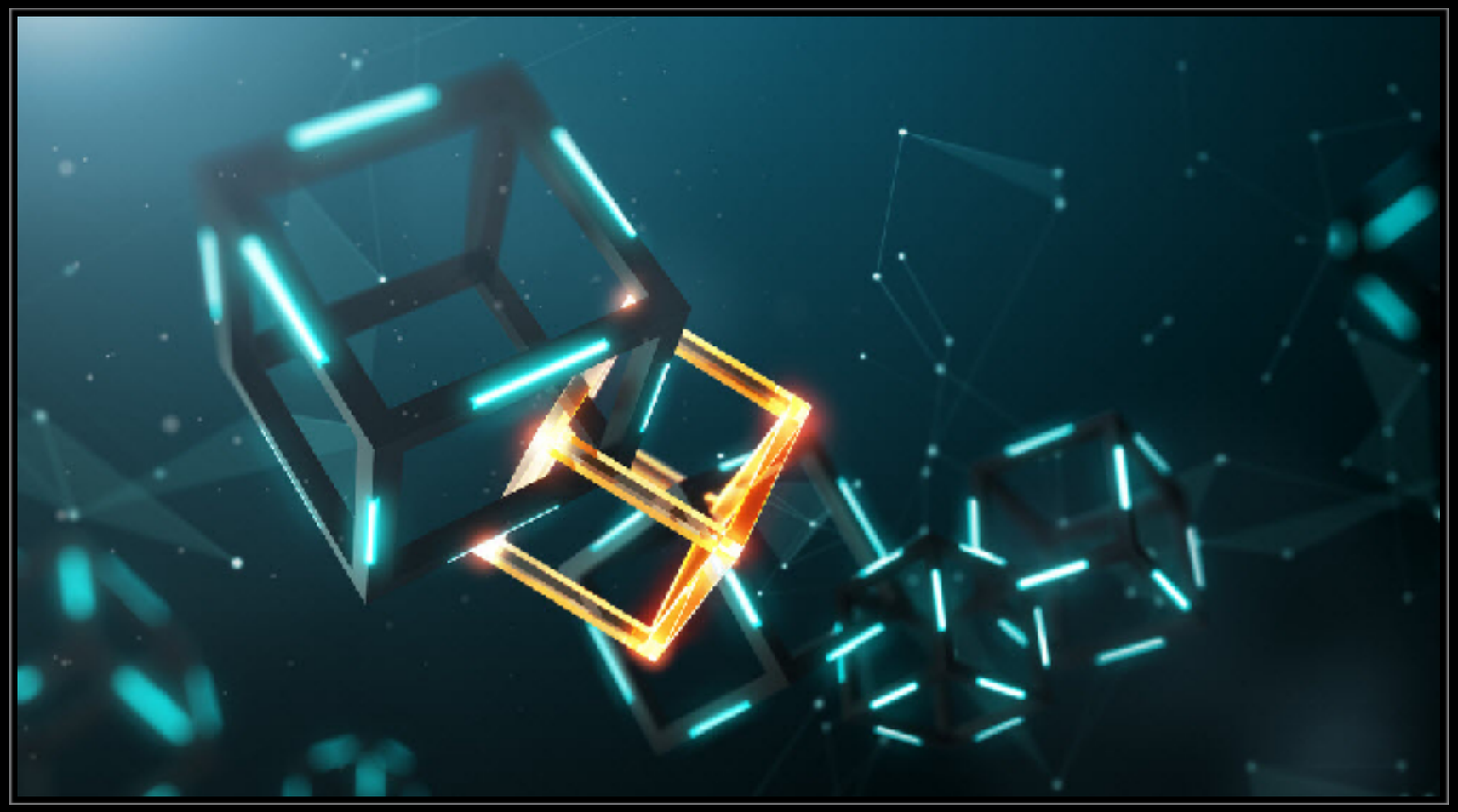
Rule by Code



Digital Feudalism
Functional Sovereignty

Instrumentalisation of Code
as a tool of political power

Rule ~~by~~ of Code



Technical Sovereignty

No One is Above the Code

UNREGULABILITY ?

“ALEGALITY”

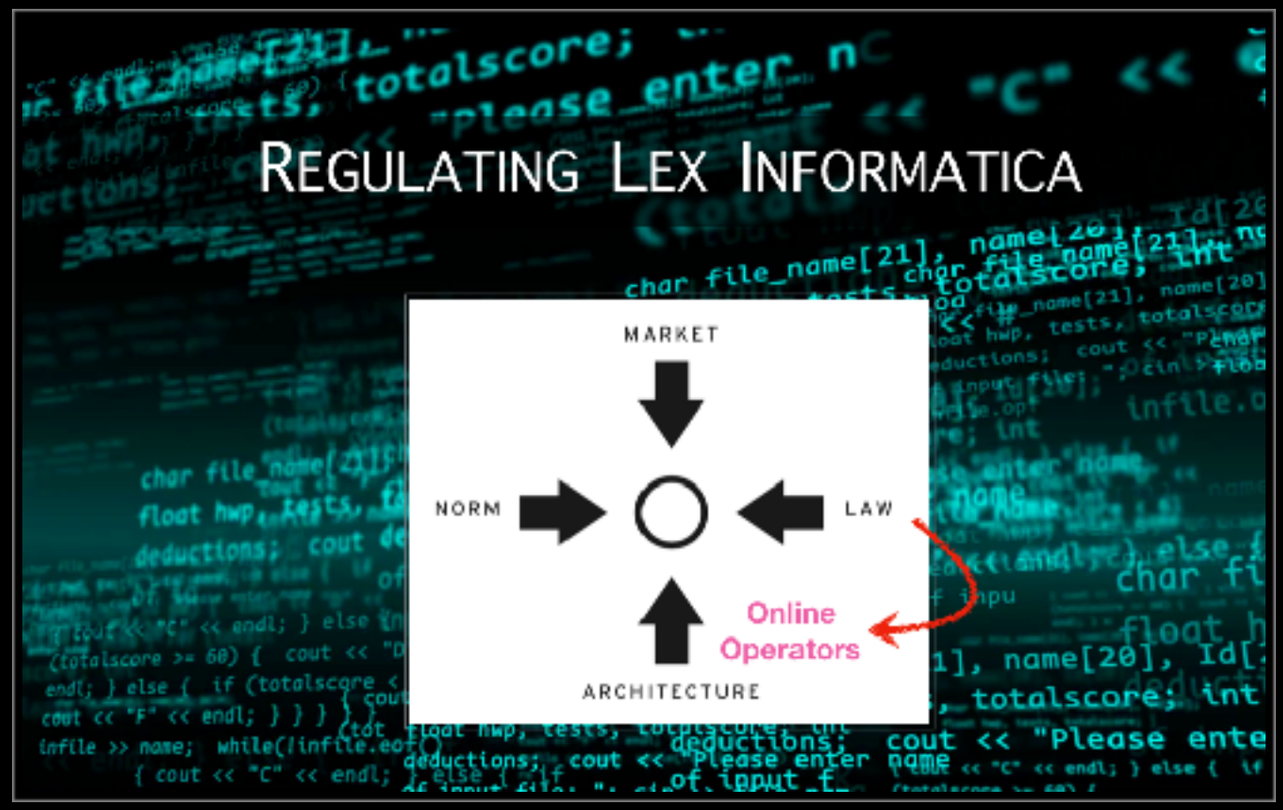
Outside the purview of the law

Code Is Law

(Lawrence Lessig —2000)

Code Is Law

(Lawrence Lessig —2000)



Code Is Law

(Lawrence Lessig —2000)

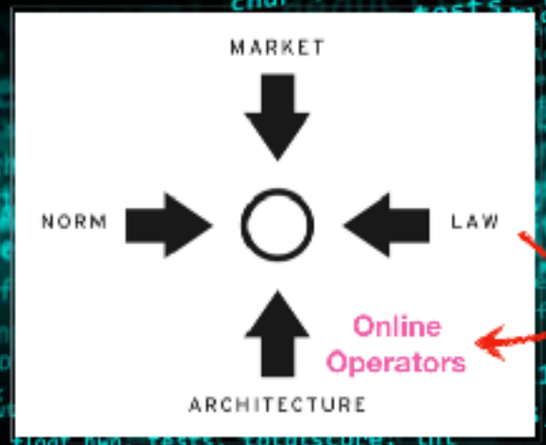
Lex Informatica

Rule by Code

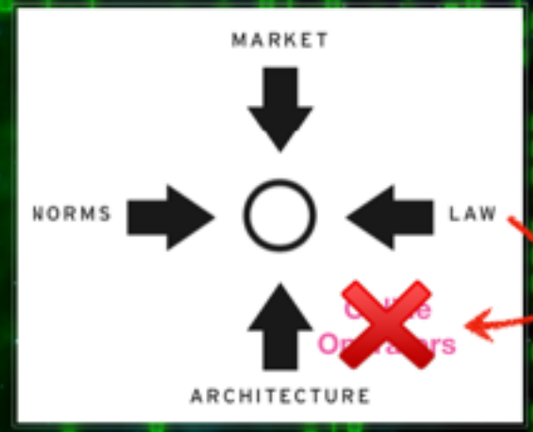
Lex Cryptographica

Rule of Code

Regulating Lex Informatica



Regulating Lex Cryptographica



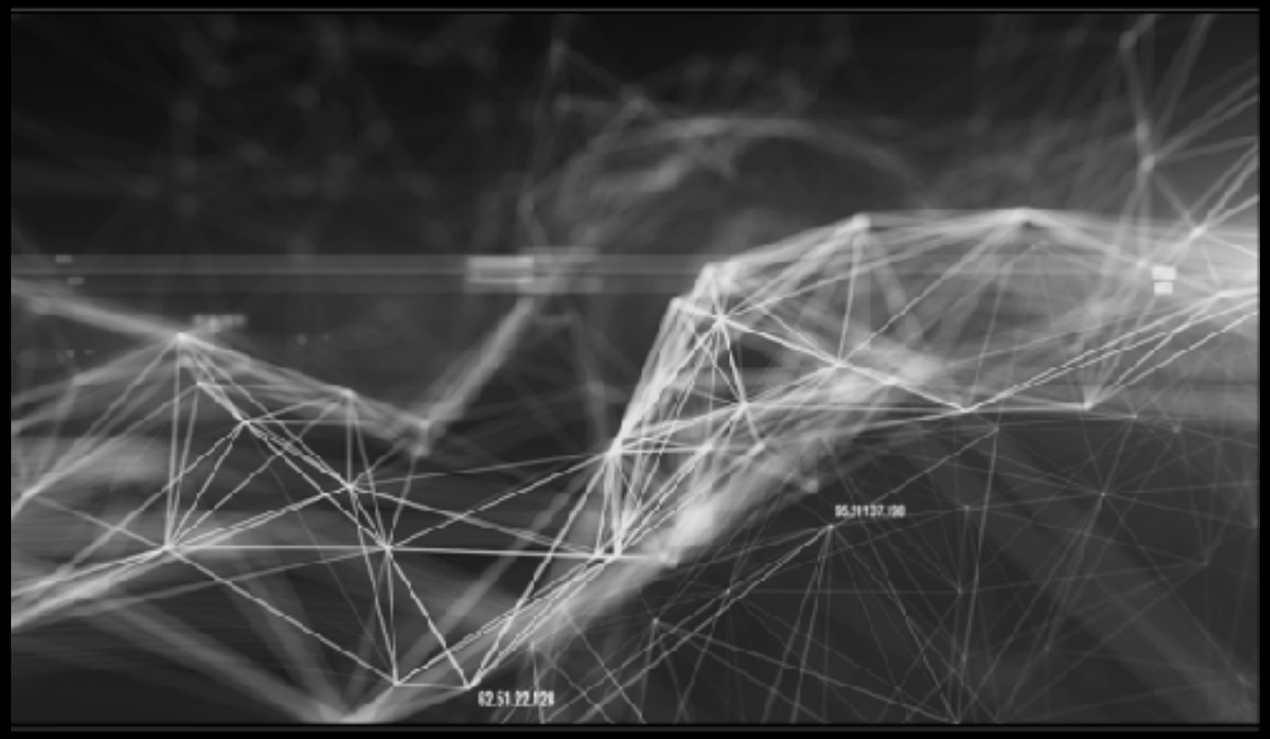
Rule of Code

Technological Guarantees as Constitutional Constraints

(1) Decentralized Database

(2) Global & Transnational

(3) Resilient

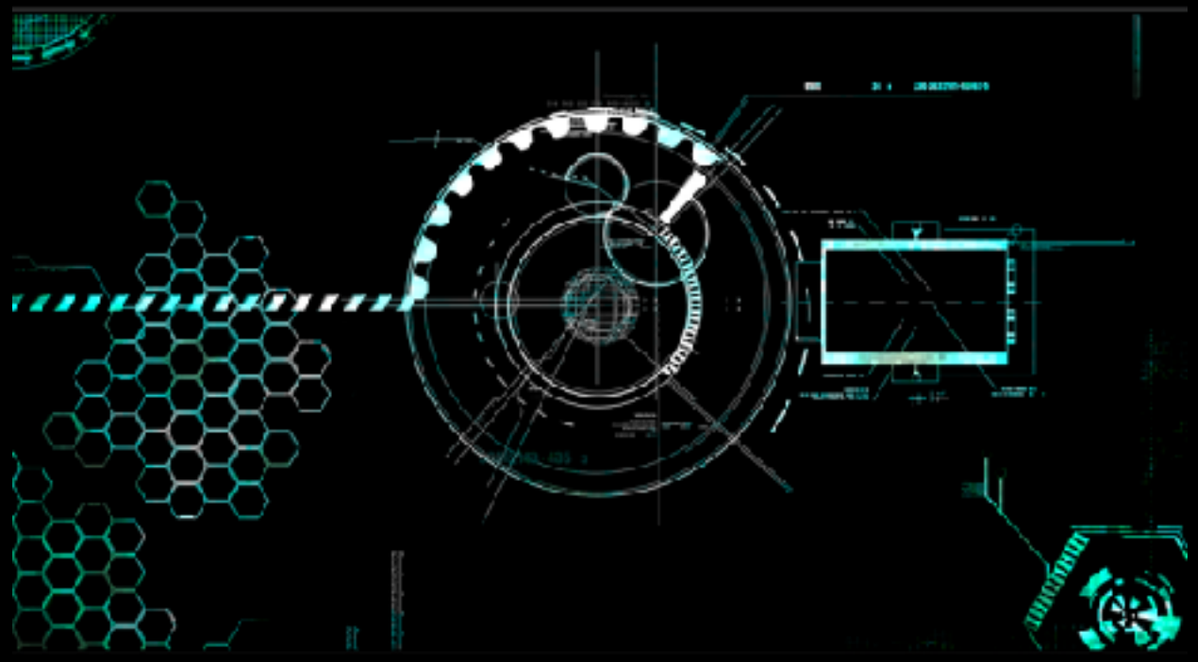


(4) Non-Coercive

(5) Tamper-Resistant

(6) Transparent

(7) Non-Repudiable



(9) Guarantee of Execution

TheDAO HACK

Wording of the Code

The attacker simply “used” TheDAO
Restoring the balance would be a theft

Intent of the Code

The attacker has “exploited” TheDAO
Restoring the balance is fully legitimate

Ethereum

Ethereum Classic

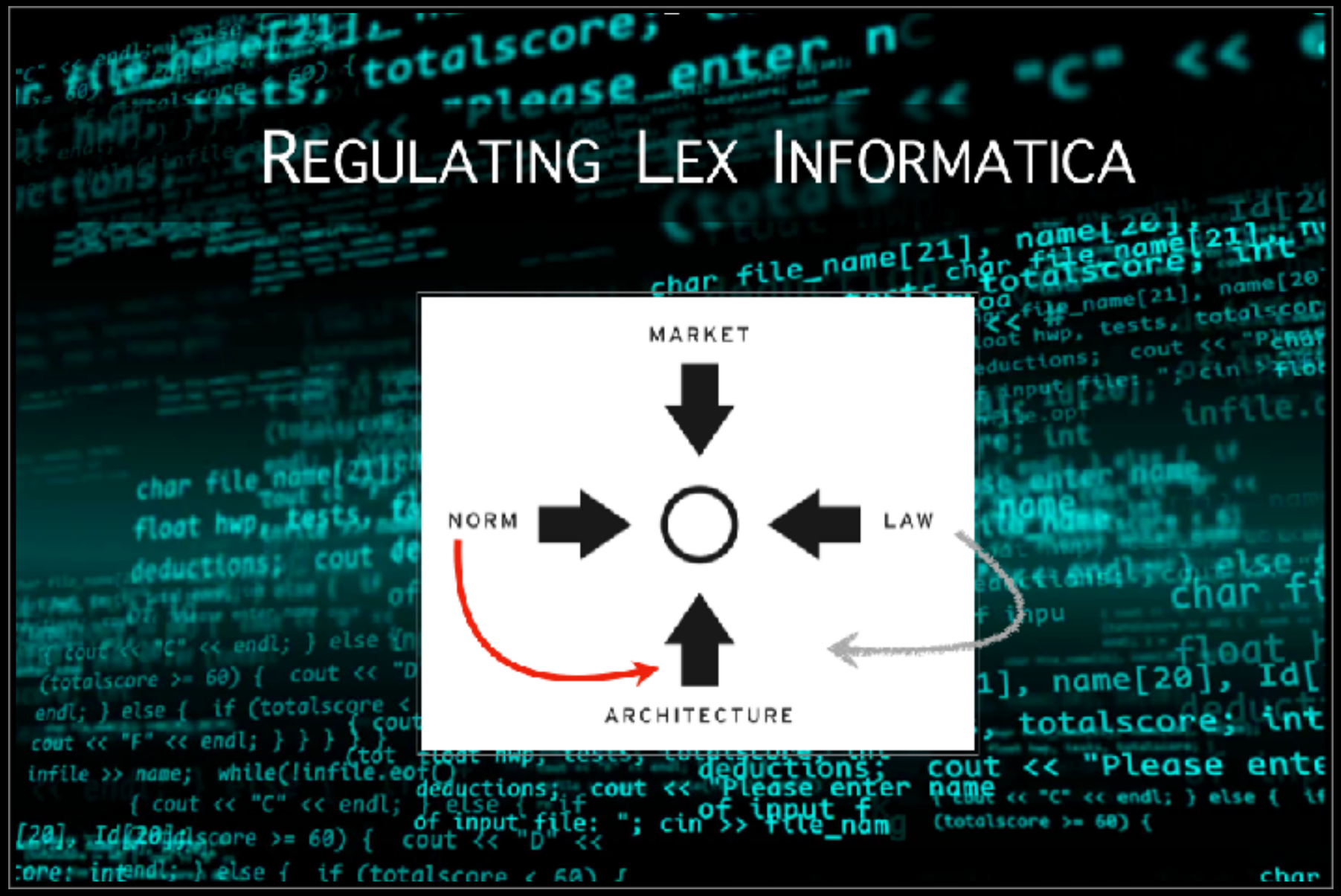
No Coercion

STATE OF EXCEPTION

Departure from the Protocol Rules

Rule of Code can be displaced by the **State of Exception**

But who's the **Sovereign**?

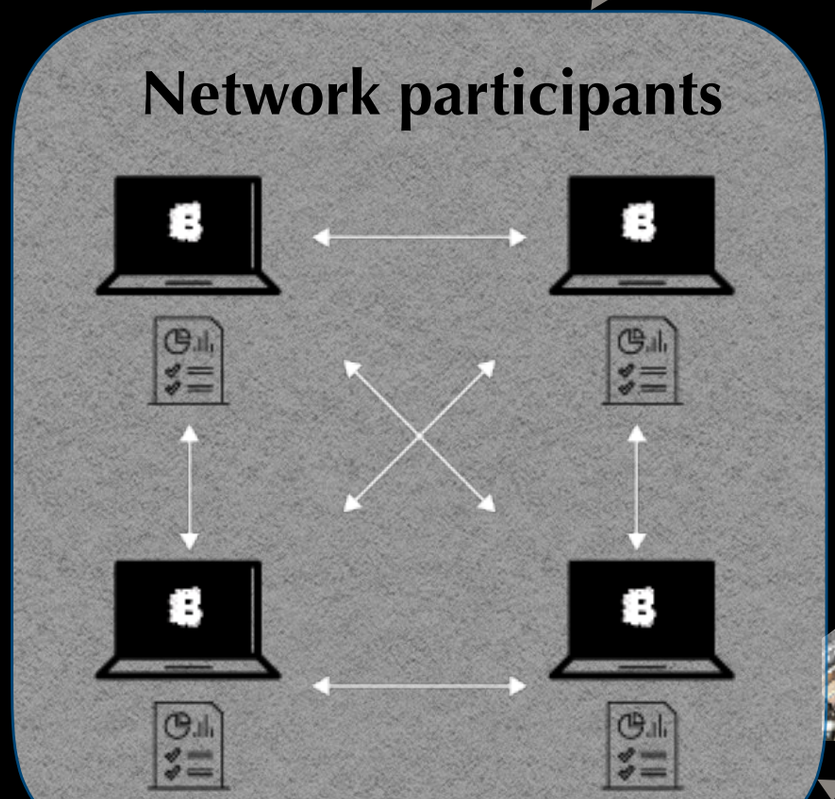


REGULATION VIA GOVERNANCE

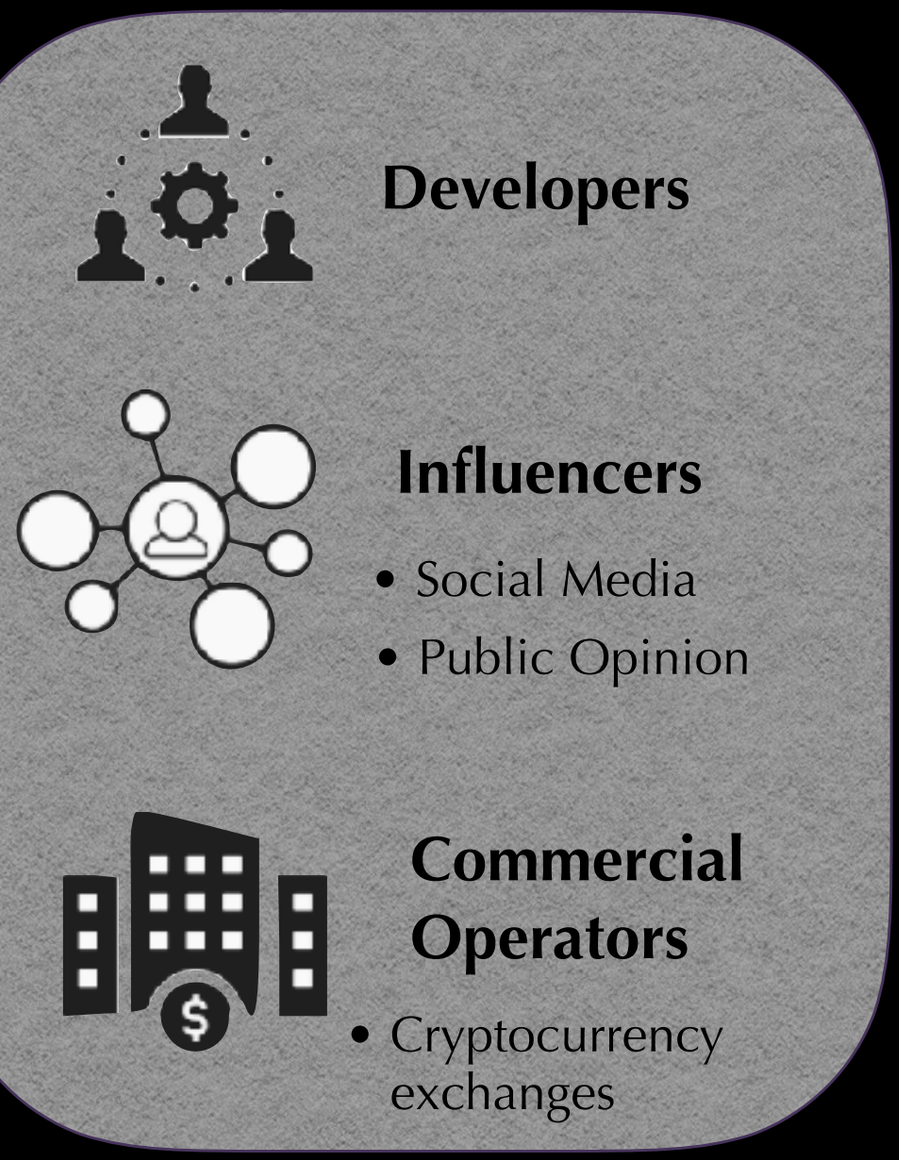
Polycentric Governance System

Governments

Users



"Shelling point"



Technical Layer

Social Layer

POLYCENTRIC GOVERNANCE

…emerges from the fact that, although all clusters remain relatively independent from each other, when it comes to making decisions, they necessarily account for what the others are doing

…as a result of the interdependence between this web of actors, *a common set of rules, norms and strategies* emerges to guide the behaviour of a large majority of actors within the system

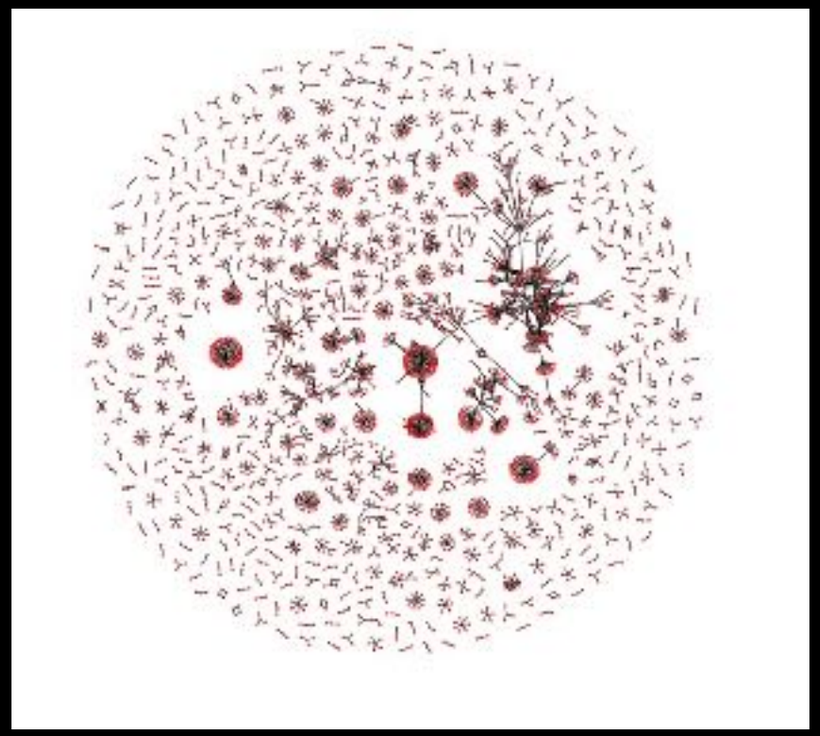
Polycentric Constitution

- ★ ***General rules***
  - *Counteract tendencies towards mono centricity*
  - *Separation of powers, conflict resolutions, etc.*
- ★ ***Domain specific rules***
  - *Strategies and rules of actors*

New York City Watersheds Memorandum of Agreement

Establishes general rules for multi-stakeholder governance over common resource

Constitutional Constraints



On Chain

Off Chain

Procedural: separation of powers, transparency, etc.

Substantive: protection of vulnerable actors, positive rights, etc.

Concluding Remarks