THE POLITICS OF BLOCKCHAIN

From *Primus Inter Pares* to *Peer-to-Peer*

HOW BLOCKCHAIN WORKS

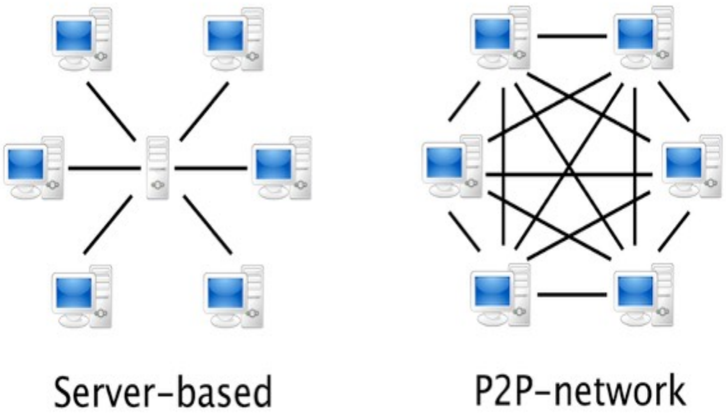
- In *peer-to-peer* networks, all the operations equally rely on each node in the system.
- Registry + *leech/seed.*

- Computational power α n° connected nodes.
- No *Single Point of Failure.*

- Danger! *Dishonest* nodes:
  - Reintroducing a central server

    or
  - Cryptography

***Peer-to-peer* networks**
Proof-of-work
Digital signature
Public ledger



HOW BLOCKCHAIN WORKS

- In order for every transaction to be performed, the system requires the resolution of some algorithms.

- Any unlocked transaction gets written on the software's registry.

- The necessary computational power is collected but active nodes, willfully investing their CPU power to fuel the system (with economic incentives… *Mining*).

Peer-to-peer networks

Proof-of-work

Digital signature

Public ledger

HOW BLOCKCHAIN WORKS

- A digital signature is assigned to each transaction:
  - Time stamp
  - Sender's address
  - Receiver's address
  - Transaction identifier (txid)

- The txid is encrypted.
- The *proof-of-work* of a transaction is completed when its txid has been decrypted.

Peer-to-peer networks
Proof-of-work
Digital signature
Public ledger

HOW BLOCKCHAIN WORKS

- In more traditional organizations, the transactions’ registry is written by a central privileged institution.

- Blockchain software *authomatically* writes the list of all unlocked transfers, without any third-party control, using their digital signatures.

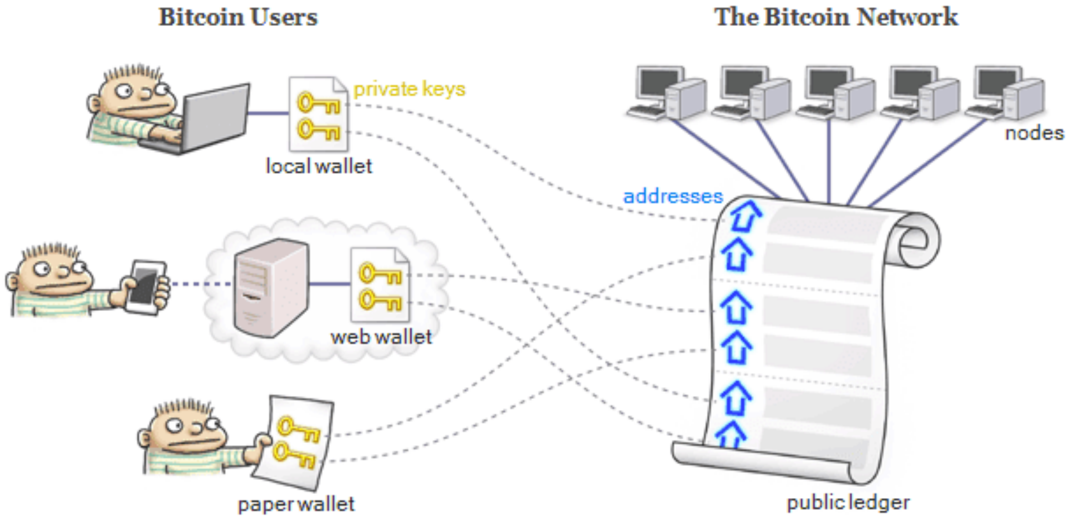
- The public ledger is locally downloaded by all nodes and updated in real time.

Peer-to-peer networks

Proof-of-work

Digital signature

Public ledger



WHY HAD NOBODY THOUGHT OF THAT?

- *Double spending problem*.

No one being in charge of the public ledger, the system can’t distinguish between two simultaneous transactions.

It is sufficient for a hypothetical thief 1) to require my data to his own address and 2) to put in the system the necessary computational power before I do, and his (malicious) transfer will be performed.

- *Hashcash* is the solution.

WHY HAD NOBODY THOUGHT OF THAT?

- *Each* transaction is assigned a digital signature, not the user (vs credit cards…).

- Txids are encrypted through the *hash function*.

- Each *hash* contains some bits of the preceding *hashes*.
- Our hypothetical thief would have to decrypt the *hash* associated with the transaction n, the one with transaction n-1, n-2,… back to the very beginning of the block-chain. This would have to be done in the same time that *every other nodes* in the net work *collectively* to unlock *one single hash*.

OVERCOMING TRUST

- *Trust-based* → *Trust-free*.
- The Code gives, the Code takes back.
- *Blockchain* vs *sharing economy*.

UBER airbnb tripadvisor

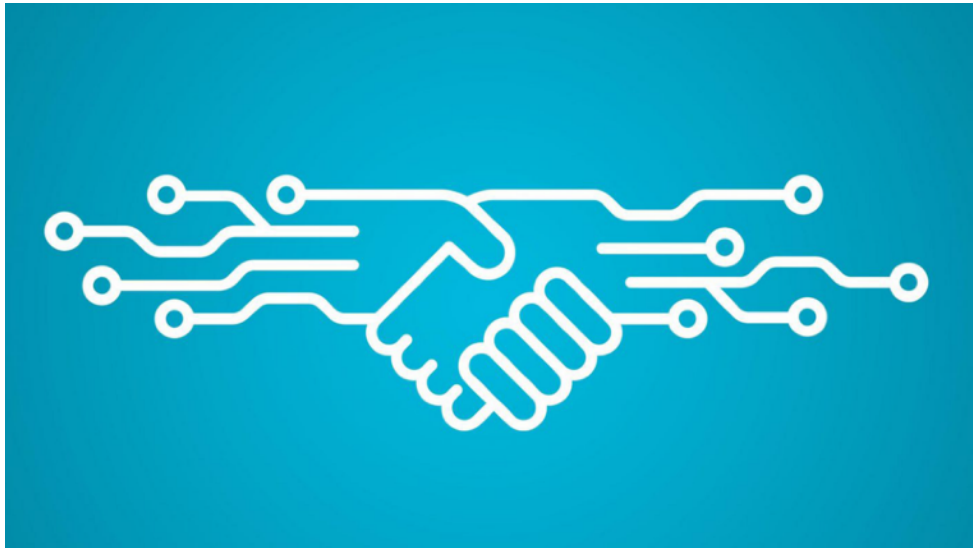
OVERCOMING TRUST

- So… is this a world without social relations?
  - The goal isn't to prevent human interactions, but to heal their weaknesses, requiring all relevant information to be trasparently displayed *ex ante*
  - Man is a social animal

«Go into the London Stock Exchange – a more respectable place than many a court – and you will see representatives from all nations gathered together for the utility of men. Here Jew, Mohammedan and Christian deal with each other as though they were all of the same faith, and only apply the word infidel to people who go bankrupt. Here the Presbyterian trusts the Anabaptist and the Anglican accepts a promise from the Quaker. On leaving these peaceful and free assemblies some go to the Synagogue and others for a drink, this one goes to be baptized in a great bath in the name of Father, Son and Holy Ghost, that one has his son's foreskin cut and has some Hebrew words he doesn't understand mumbled over the child, others go to heir church and await the inspiration of God with their hats on, and everybody is happy.»

(VOLTAIRE, *Letters on England*., Penguin Books, 1980.)

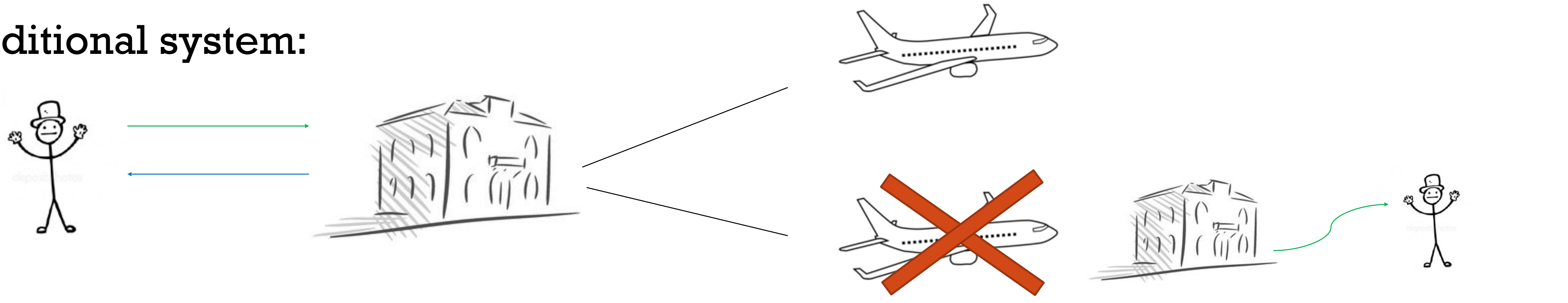
SMART CONTRACTS



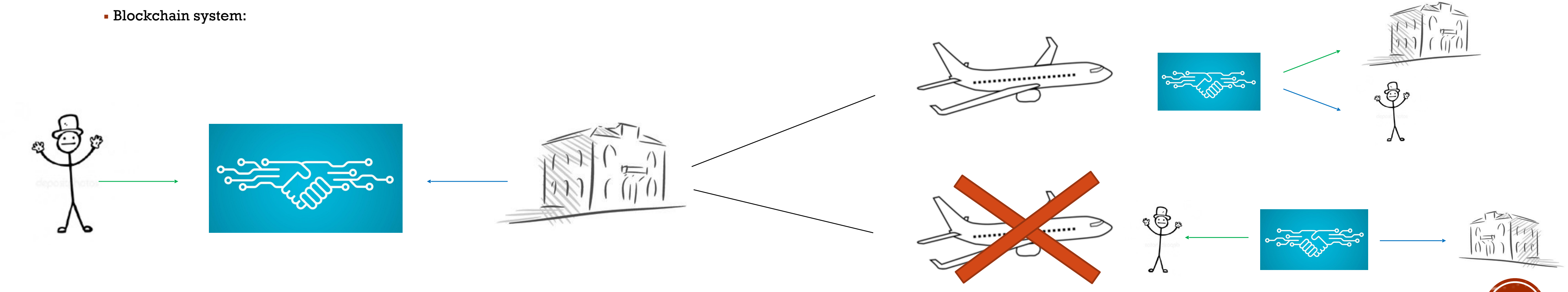
- *Smart contracts* are protocols that can unlock specific transactions when some pre-set conditions are met.
- A safe, immediate, authomatic, necessary form of contract.
- The software locks the relevant data, detects the parties' operations, and unlocks the objective-state only the conditions are fulfilled.

AN EXAMPLE

- Traditional system:



- Blockchain system:



INTERNET OF THINGS

- *Internet of Things* (*IoT*) is to remotely use devices connected to the net through software and sensors that confront external conditions and pre-set instructions.

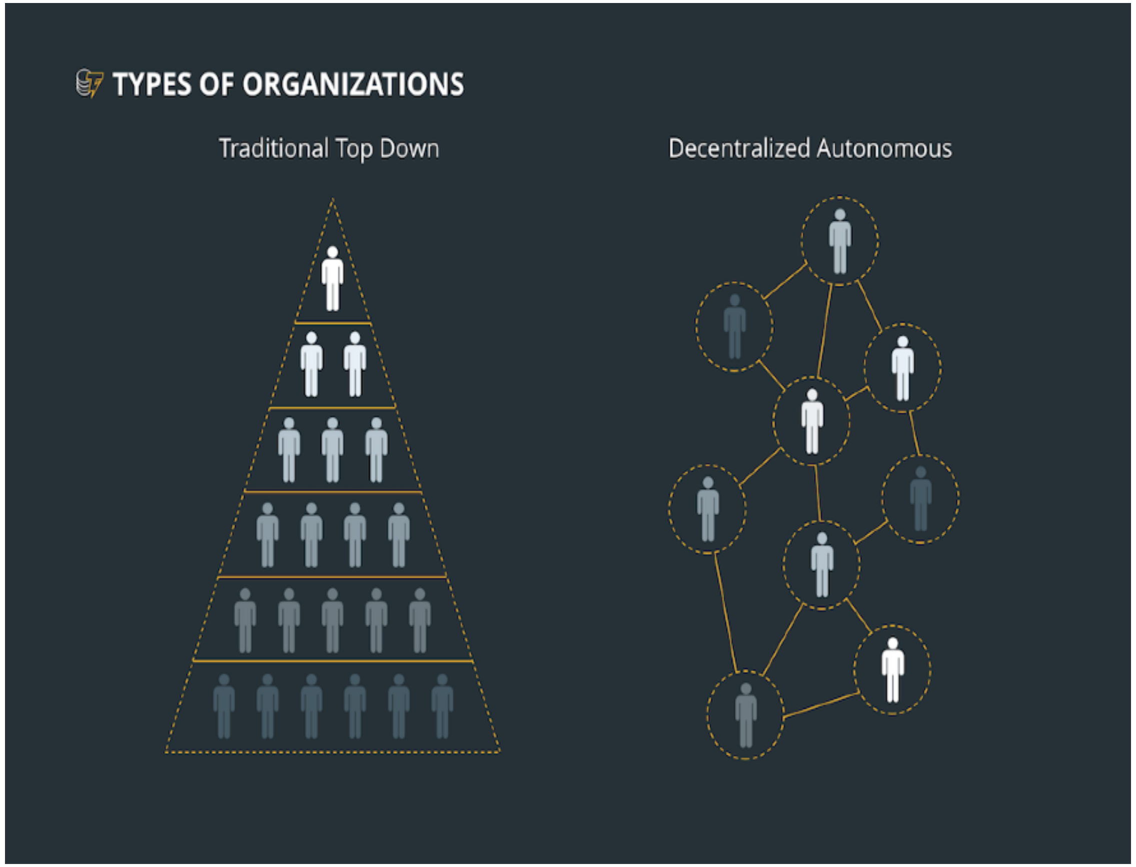
- *Smart contract* + *IoT* = Decentralized management of the real world.

DIGITAL COMMUNITIES

- DAO = *Decentralized Autonomous Organization*

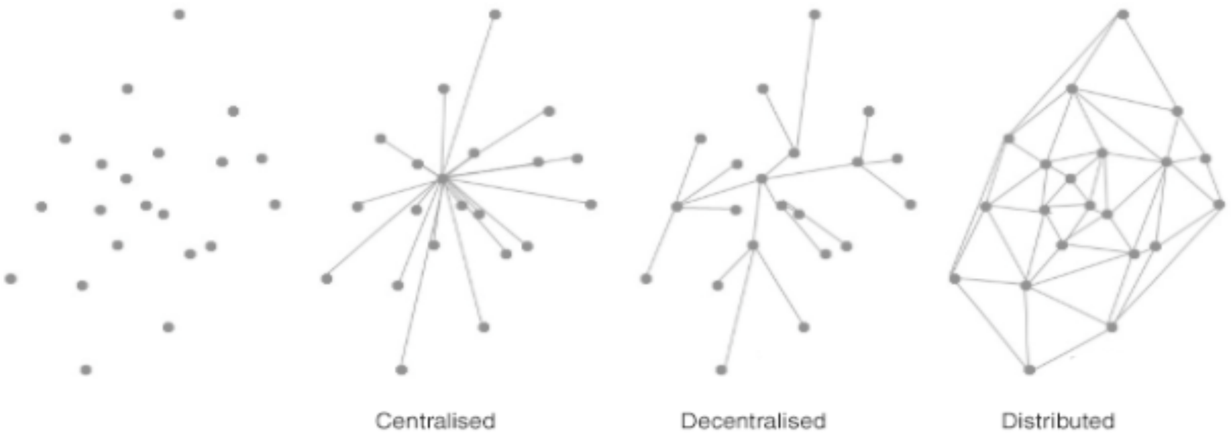
- Fluid participation
- No coercion
- No goverment, no power
- Transparency
- Public decisions = Public actions

- Decisions can be uttered by modifying the source code of the underlying smart contracts.



DIGITAL COMMUNITIES

- *Distributed* management of society.



- «*Likes* and *retweets* are a *voting* system, though not optimized.»

- Democracy.earth, Flux, Aragon, Bitnation…

Democracy.Earth

flux.

ARAGON

BITNATION
GOVERNANCE 2.0

THE CYPHERPUNK MOVEMENT

- The *cypherpunk* movement was born in 1992 by the occasional meeting of some friends. Their *mailing list* brought to life many innovations for the online world.
- People: Eric Hughes, Timothy May, John Gilmore, Wei Dai, Adam Back, Nick Szabo, Julian Assange, Satoshi Nakamoto.

  Vitalik Buterin and Cody Wilson are close to the movement.
- Inventions: *B-Money*, *hashcash*, *smart contract*, *smart property*, WikiLeaks, *blockchain*, Bitcoin.
- Mission: applying globalization in a complete and safe manner for individuals in the digital age.
- Enemies: states, banks, all traditional and centralistic sources of power (responsible of the 2008 crisis).

THE CYPHERPUNK IDEALS

- Blockchain technology has characteristics that are close to «distributed capitalism»:
  - Coercion is never acceptable
  - →Natural rights
  - Resilience to regulation,
    Political decentralization
  - →*Laissez-faire*, individual contracts
  - →Subjective theory of value (digital scarcity…)
  - →Economical analysis only for real contexts
  - Property as a bundle of right (*smart contract*)

- *Ideals*: how come?
- How to (re)build a digital state.

WHERE HAS AUTHORITY GONE?

Non est potestas Super Terram quae Comparetur ei Iob. 41. 24
CRYPTOGRAPHY
IN MATH WE TRUST
TECHNO-LEVIATHAN

- Is there no more authority… or is the software itself the authority?

- Two conflicting views:
  - Techno-statalism

    Marcella Atzori, Anton Antonopoulos, Melanie Swan, Democracy.earth, Flux
  - Crypto-anarchism

    Cody Wilson, Timothy May, Julian Assange, Bitnation

WHERE HAS AUTHORITY GONE?

TECHNO-STATALISM

- Blockchain is the natural evolution of the state.
- There is (depersonalized) power.
- There is human influence on DAOs, although the *élites* in power are changing:
  - Influent *mining pool*
  - Software developers
  - External aggressions are possible
- → DAOs need control.

CRYPTO-ANARCHISM

- Blockchain is the natural evolution of law: from *lex mercatoria* to *lex cryptographia.*
- The software isn't the ruler; it is the rules.
- Assumptions:
  - Any juridical relation can be translated into algorithms (*if x, then y*)
  - Individuals+properties+rules+time
  - *Homo Oeconomicus*
- → We could and should get rid of coercion.