



The energy blockchain and other applications of e-commerce.

Pierluigi Gallo
pierluigi.gallo@unipa.it

Outline

- Blockchain applications
- blockchain technical recap
- Comparison between finance transactions and energy transactions
- Comparison between proof of work and proof of X



- **Finance and money transfer**
 - **R3** (Intel, Microsoft, Oracle, +60)
 - WSBA Wall Street Blockchain Alliance

- **Education and University**
 - Certificates stored on the blockchain

- **Human resources**
- **Voting systems**



- **Leasing and selling cars**
 - Visa + DocuSign

- **Networking and IoT**
 - Adept, ChainOfThings
 - IBM+Samsung, cognitive IoT applications with smart contracts. Filament

- **Data analysis, bets, forecasting**
 - Augur
 - The Wisdom of the Crowd

- **Crowdsourced knowledge**
 - Lunyr

- **Online music**
 - Voise, Mycelia

- **Car sharing**

- **Insurance**
 - **B3I**, The Blockchain Insurance Industry Initiative
 - Aeternity, LenderBot from Stratumn, InsurETH



- **Healthcare**
 - Tierion, Gem, Philips, Microsoft

- **Decentralized File Storage**
 - IPFS, Swarm, StoreJ

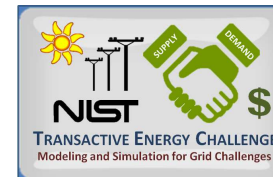
- **Energy management**
 - **EWf** (Energy Web Foundation)
 - Transactive Grid, LO3, SolarCoin, AutoGrid

- **Notary and Real Estate**
 - Ubitquity

- **Testament and crypto-will**
 - Smart will

- **Stock trading**

- **Trading**
 - OpenBazaar



- **Government**
 - Circles, GovCoin
 - Dubai is aiming to put all its government documents on the blockchain by 2020.

- **Crowdfunding**

- **Charity and ONG**
 - BitGive

- **Supply Chain Management**
 - Provenance, Fluent, SKUChain, and Blockverify

- **Transport**
 - **BiTA** – Blockchain in Transport Alliance



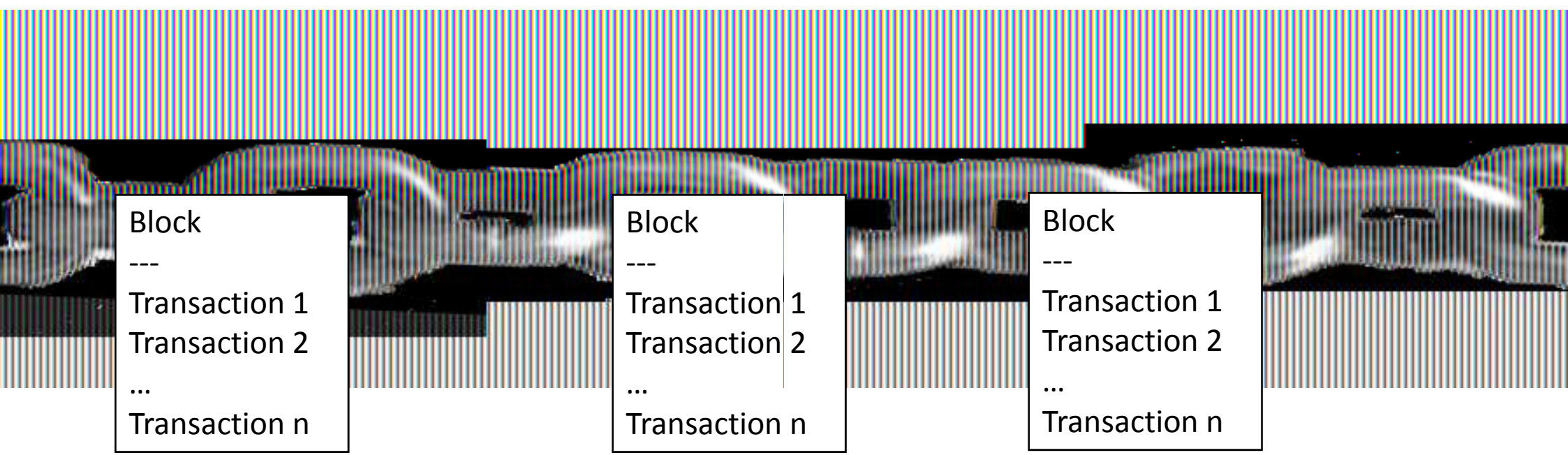
- **Blockchain as a service**
 - IBM Hyperledger

- **Internet of loyalty**
 - loyyal

- **Cybersecurity**
 - Guardtime



The blockchain as a chain of ownership



Block

Transaction 1
Transaction 2
...
Transaction n

Block

Transaction 1
Transaction 2
...
Transaction n

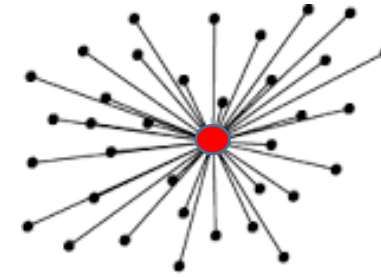
Block

Transaction 1
Transaction 2
...
Transaction n

It's a chain because changes can be made only by adding new information to the end and because blocks are linked each other

What is the blockchain (recap from previous presentation)

- Distributed ledger with interesting properties:
 - Fully distributed, no need for middleman
 - Immutability
 - Byzantine fault tolerant system with decentralized consensus
 - Cryptographically secure
 - Works well in trustless environments
 - A fertile soil for smart contracts
 - Can be designed and deployed in different forms: public, permissioned, private



centralised



distributed

Beyond energy transactions

- Can we use the blockchain only for transacting energy?
 - Green certificates
 - Certify that some electricity is generated using renewable energy sources
 - Verification of Kyoto goals
 - Certified energy production



Financial transactions

Transactions are chained (not only blocks the inputs from the latest transaction correspond to outputs from previous transactions).

Transactions are like lines in a double-entry bookkeeping ledger.

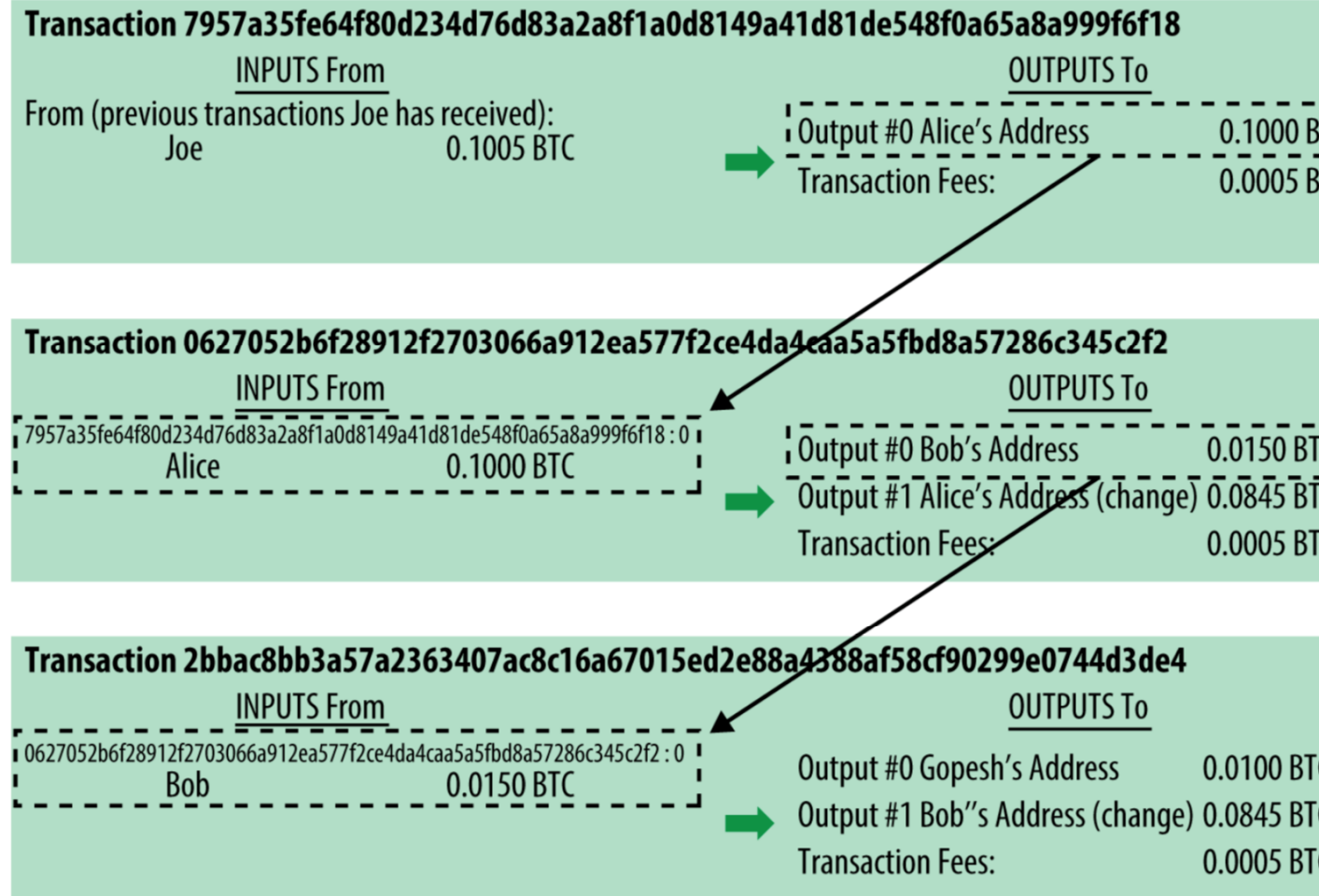
one transaction contains:

- one or more “inputs,” which are debits against a bitcoin account.
- one or more “outputs,” which are credits added to a bitcoin account.

The inputs and outputs (debits and credits) do not necessarily add up to the same amount

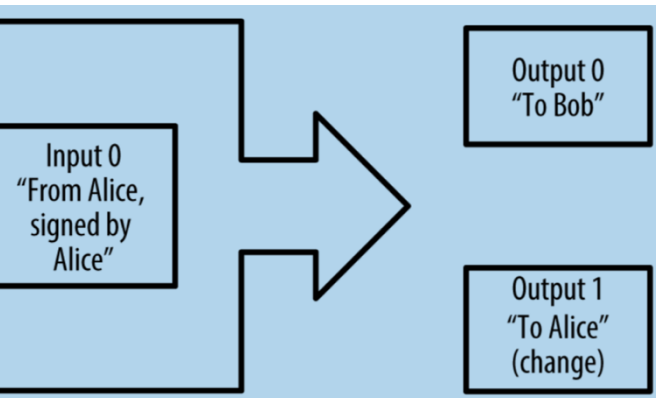
Generally, outputs add up to slightly less than inputs, the difference is the “transaction fee”

The transaction fee is used as reward for the miner who includes the transaction in the ledger for his work

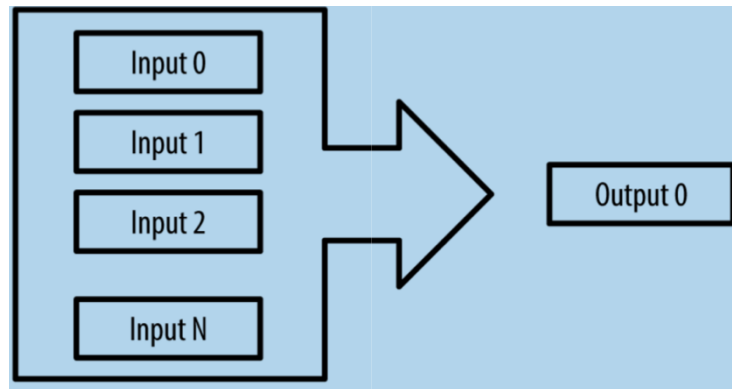


Transactions move value from transaction inputs to transaction outputs.

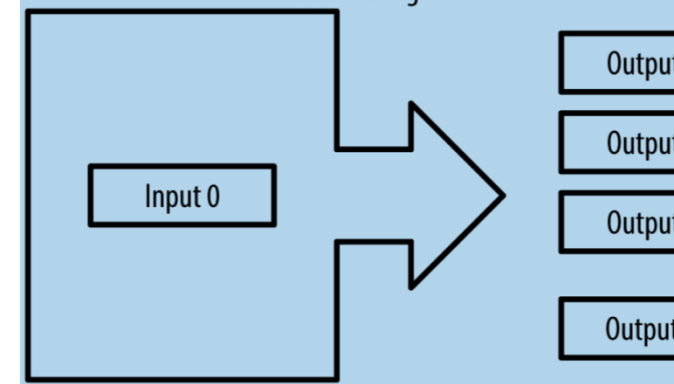
Typical financial transactions



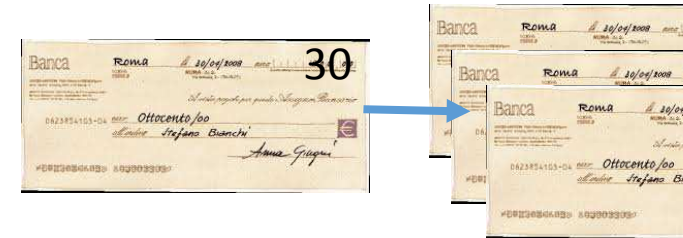
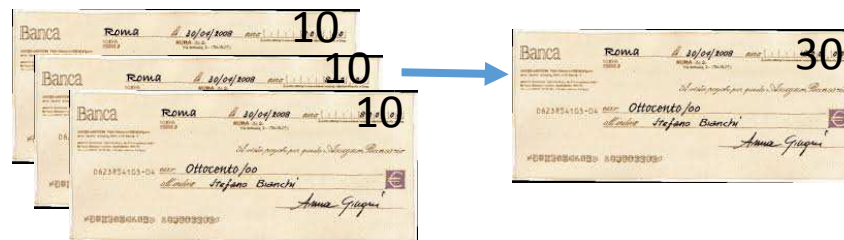
The payment from one address to another, which often includes some "change" returned to the original owner.



A transaction is one that aggregates several inputs into a single output. This represents the real-world equivalent of exchanging a pile of coins and currency notes for a single larger note.



This transaction distributes one input to multiple outputs representing multiple recipients (e.g. a company pays multiple employees)

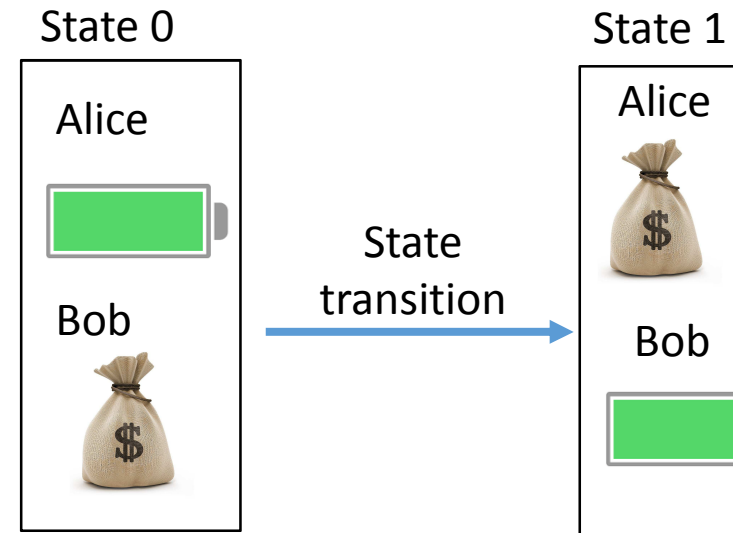


From financial transactions to energy transactions

Transaction - from Latin Transactus, p.p. of Transigere, to negotiate

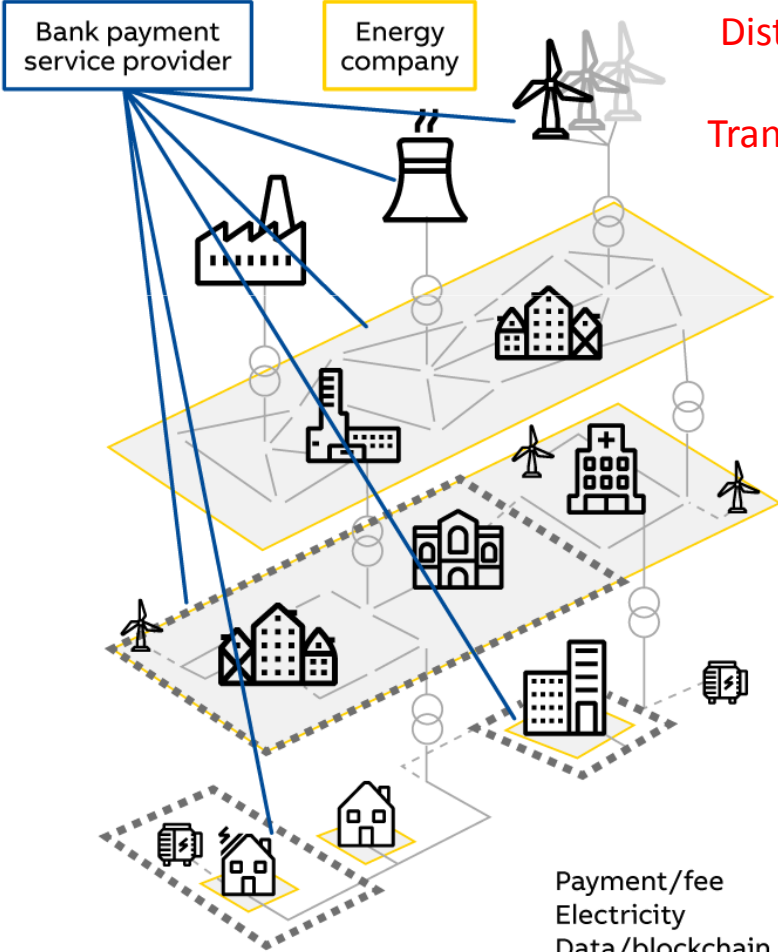
Transition - from Latin Transitionem, pass, passage

- Mapping the physical (and digital) world in the digital world
- Transactions are movements of **anything with a value** between two parties
 - In **Bitcoin** transactions keep track of **transfer of bitcoins**,
 - in the **energy sector**, transactions involve the transfer of **energy between a generator and a load**
- Transactions record events in the physical world
 - Energy transactions



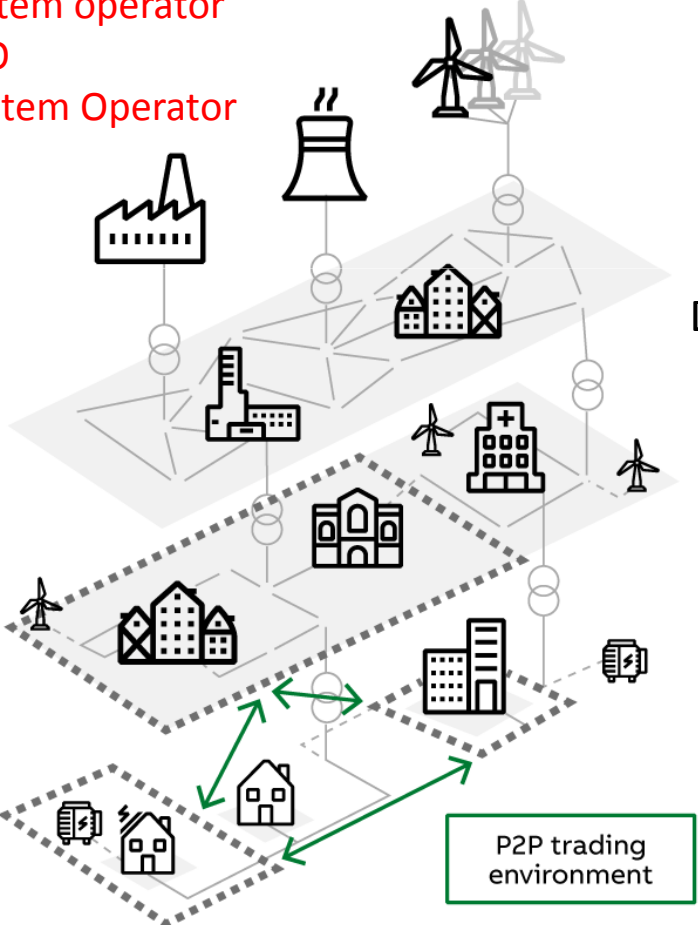
Modelling energy transactions (monetizing energy exchanges)

Traditional transaction model



Blockchain transaction model

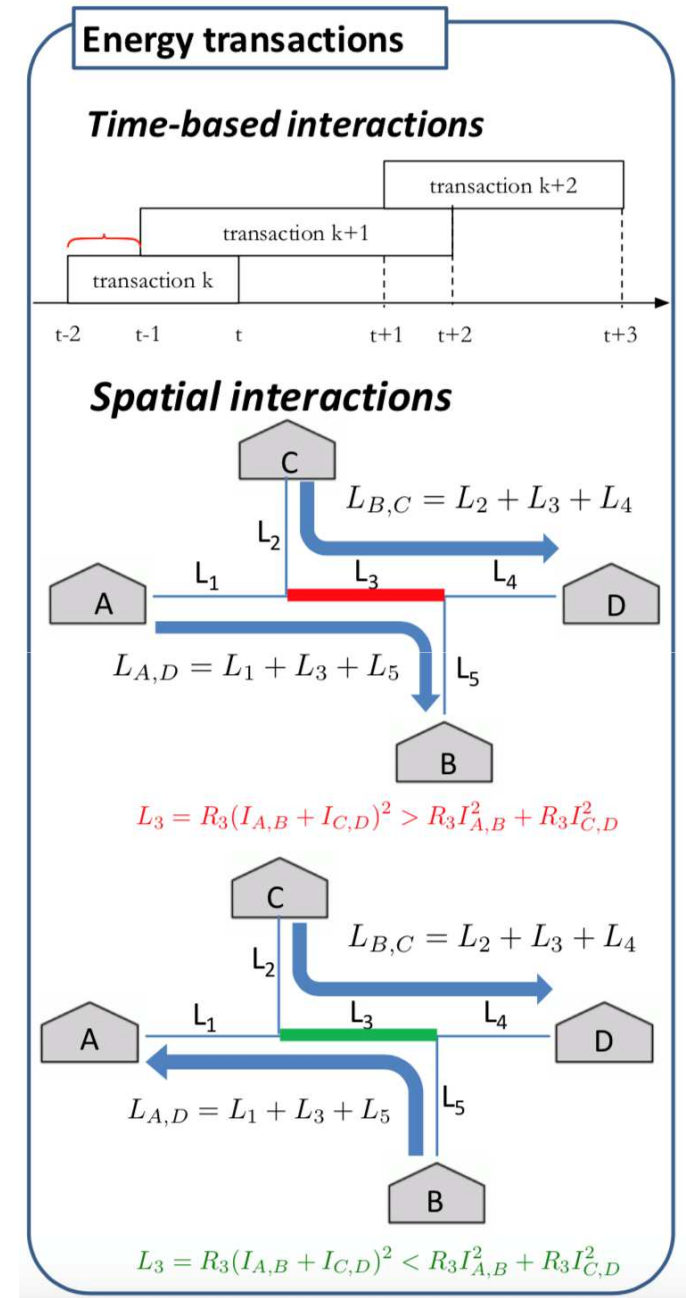
DSO
Distribution System operator
TSO
Transmission System Operator



Hash functions

Energy transactions

- Are energy transactions yet another 'value' to be transacted?
 - Which energy?
 - **Active energy** (the one that is intended)
 - **Reactive energy**
 - **Energy losses** on the distribution network
 - The transactions and the blockchain requirements depend on the physics of the (energy) sector
 - **What** to add on the blockchain
 - **When** to add it
 - **Where** it is meaningful to analyze the distributed interactions
 - A blockchain for energy transaction has to be energy-preserving

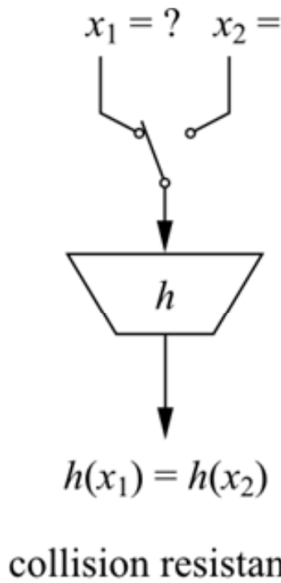
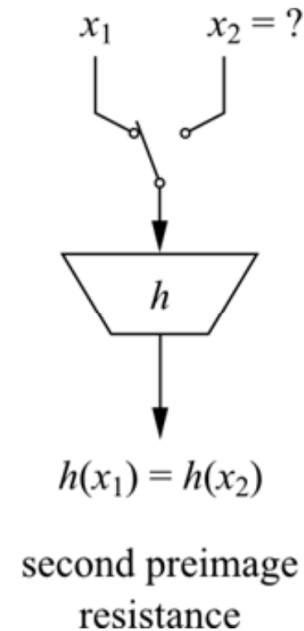
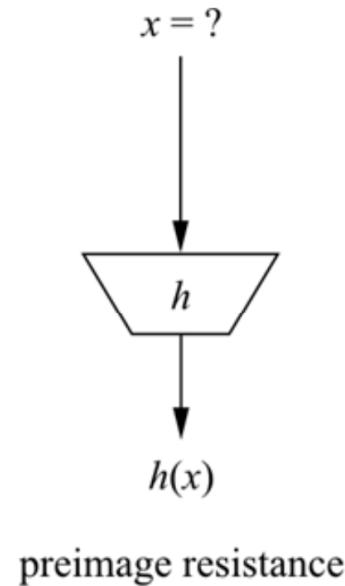
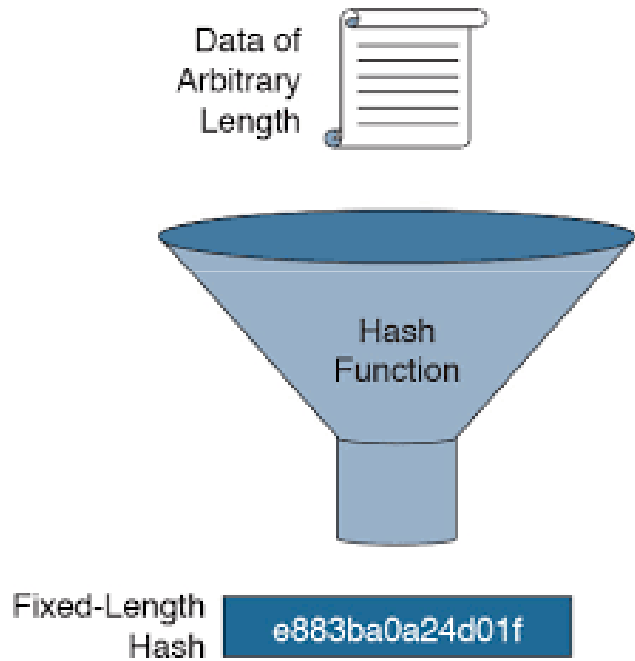


How transactions are added and chained

- It depends on the blockchain, but we need some 'rules' to avoid clashes and inconsistencies
 - In a fully-distributed system rules are needed to select who can write next block
- Nodes that receive a valid transaction that has not seen before will immediately forward it to other connected nodes
- the transaction rapidly propagates out across the peer-to-peer network, reaching a large percentage of the nodes within a few seconds.



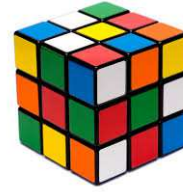
Hash functions



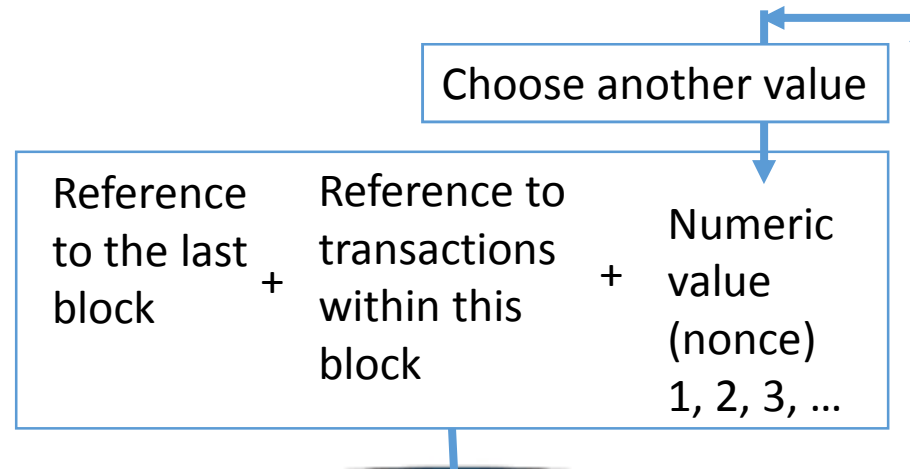
Understanding Cryptography – Christof Paar and Jan Pelzl

The Hash rate indicates how many hash functions can be computed by a computer per second

Hashcash (PoW)



- The puzzle depends on the last block in the blockchain
 - when the puzzle is solved, automatically there is a new puzzle to solve



What happens if two nodes solve the puzzle at the same time?
They both have write permissions to the blockchain ...

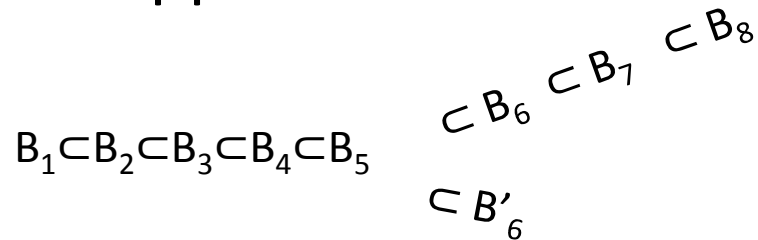
- It is rewarded with some 'transaction fee'
- The other ones will stop their quest for the solution

51da45a5bf68fc2f3
66e450deafdc8302

↓ We have finished our work

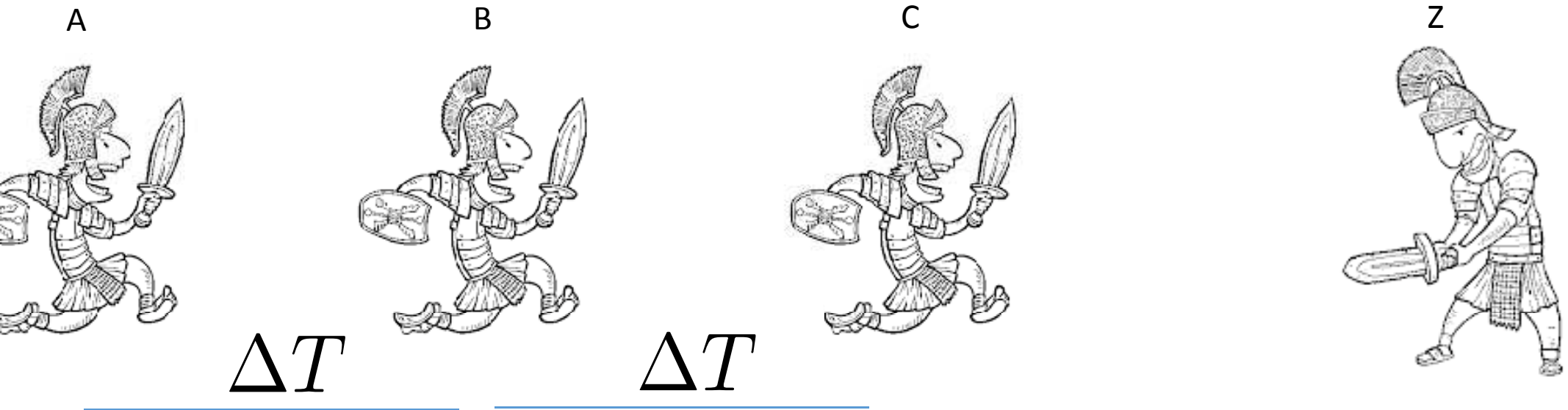
Forks

It happens a fork!



- How to resolve forks?
 - Choose the longest branch (more work is behind the longest branch)
 - Remove the shortest branch
- To be sure that my block is not involved in a fork I need to wait for other successive 6 blocks. This protects from forks but introduces latency
- The more blocks are added after a block, the more such block is trusted
- As the blocks pile on top of each other, it becomes exponentially harder to reverse the transaction, thereby making it more and more trusted by the network.

Orazi and Curiazi



The legend

3 soldiers (A,B,C) against 1 (Z) would easily win but ...

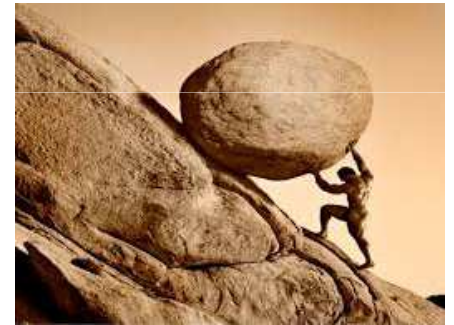
- All soldiers that want to kill Z have to run after him
- A,B,C run after Z
- Running is a time- and energy-consuming process
- After the run, A,B,C arrive at different time

The mining procedure

- All nodes that want to add a block have to mine
- Mining is a time- and energy-consuming process
- Miners arrive at different times (the difficulty of mining can be tuned)

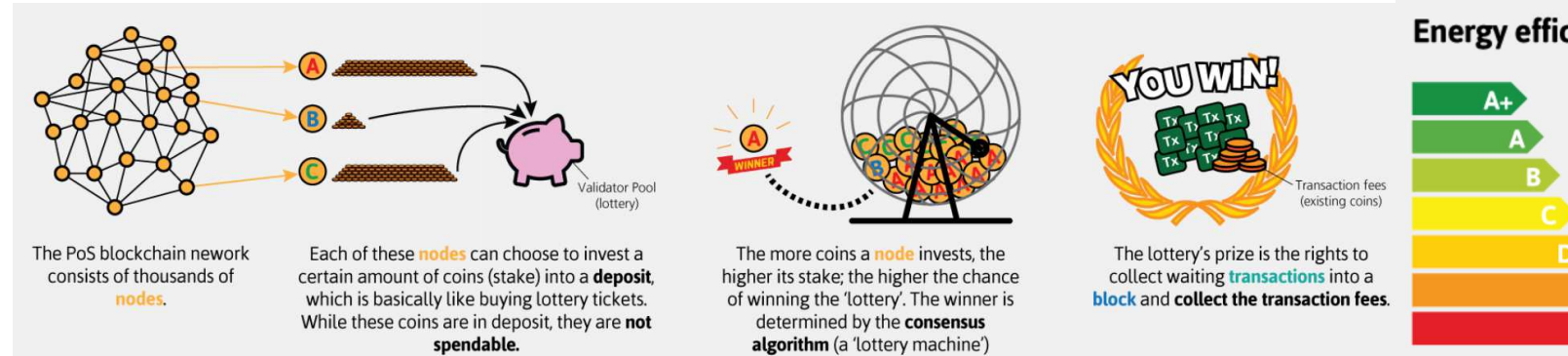
Tuning the difficulty of mining new blocks

- d is tuned so that we have a winner every 10 minutes (average)
- This time has not to be too short to avoid too many forks
- This time should be the shortest possible in order to reduce latencies
- We tune d to have a constant difficulty as computation capabilities increase over time
- The work has to be hard, in order to provide consensus while preventing Sybil attacks
- Our goal is to have energy-efficient transactions
 - Does it make sense to have a such huge waste of energy to maintain the blockchain?



Lightweight proving before writing a block

- ~~proof of work,~~
- proof of stake,
- proof of activity,
- proof of burn,
- proof of Elapsed Time (PoET),
- PBFT,
- proof of location
 - **build a consensus-driven map of the world that can be trusted for all applications.**
 - To do this, we are developing a *protocol for proof-of-location*, an *API for geospatial interactions on the blockchain*, and the *Spatial Index* (a visual explorer)



Actors of energy blockchain

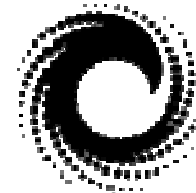
- Conjoule (Germany)

- *"We all get more value when energy is local, connected, and shared"*.
- peer-to-peer trading of energy among rooftop PV owners



- Grid+ (by ConsenSys, formerly CO-TRICITY)

- Based on Ethereum + proof of stake + Casper
- Creates economic incentives through market-based energy pricing encouraging the adoption of distributed generation (solar panels), and distributed energy storage (batteries).
- Not yet operational
- Not deployable in Italy because of our rules (you cannot store energy and resell it at later time)



39,236,491

GRID tokens sold

0.0037 E

Price per GRID

Actors of energy blockchain

- TEPCO, the largest utility in Japan, invests in ElectrON
- On October 4th 2017, E.On and Enel traded electricity using the blockchain, the two firms completed a day-ahead contract of 1 MW power delivered in Hungary,
 - Enerchain by PONTON – the code is not available :(
 - The transaction is not publicly available (it seems only a PoC)



Storage co-optimization



C&I DR



Virtual power plant (VPP)



DER ancillary services



Distribution flexibility



Smart inverter management



EV & EVSE management



Customer engagement portal



Residential BYOT (Bring-Your-Own-Things) DR



Residential behavioral/pricing programs



Residential direct load control (DLC) DR



Community DR

Law and blockchain



The current energy market in Europe is not yet ready for blockchain adoption

- balancing consumer protection interests with the interests of energy suppliers
- establishing a competitive internal market in electricity and gas
- current legal framework for the application of blockchain technology in dealings with consumers and prosumers and future legal challenges presented by blockchain
 - *Direct customer-to-customer transactions & financial settlement*
 - *Verification & certification*
 - *Clearing & settlement*
- **European General Data Protection Regulation (GDPR)** is going to apply soon (EU Regulation 2016/679)
 - It harmonizes the rules for the processing of personal data by private-sector businesses and public-sector entities across the EU. The interaction with blockchain uses cases is still under review

Regulatory challenges

- **transform current market roles (especially the role of DSO and TSO)**
- **meter operators (all transactions are recorded in the blockchain)**
- **electricity suppliers**
- **clearing process**, which is run to reconcile planned consumption against customers' actual consumption as recorded by their meters
- **providers of ancillary services**

The user's point of view

Opportunities +

- **Lower transaction costs** due to the cutting out of intermediaries
- **Falling prices** as a result of greater **market transparency**
- Simple **option for customers to become a service/electricity provider**
- **Transactions are generally made more simple** (documentation, contracts, payment)
- **Greater transparency** thanks to decentralised data storage
- **Flexible** products (tariffs) and supplier switching
- **Strengthening of prosumers** thanks to independence from central authority (direct purchases/sales of energy)

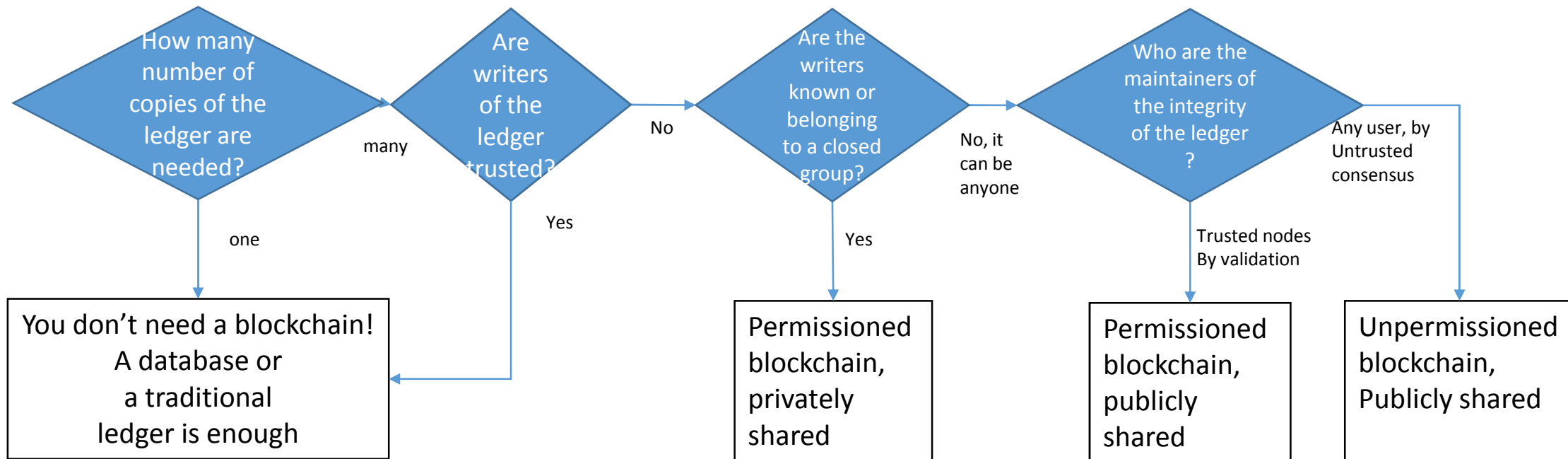
Risks -

- **Complete loss of data** on loss of ID
- Currently **high transaction costs for public blockchain systems**
- Possibly **lack of acceptance** on the part of consumers
- No **authority in the case of disputes**, no direct possibility of escalating conflicts
- Risk of **fraudulent activities** at the interface between the real world and the digital blockchain world (e.g. the smart meter/blockchain interface)
- **Lack of long-term experience**
- **Technical problems with initial applications** possible to start with
- Insufficient or inadequate functionality and security risks due to **lack of standardisation**
- Networks must cope with **greater flexibility**

Blockchains can be distinguished by models

- Adversarial model
 - Any (chosen) honest user can immediately be corrupted by the adversary
 - Perfect coordination of all corrupted users
- Communication model
 - Message gossiping
 - E.g. a message honestly gossiped m at time t reaches 90% of users nodes by time $t+\Lambda$ if the message is long, $t+\lambda$ if the message is short
- Honesty assumption
 - The majority of users is honest (but users are public keys, therefore an adversary can create 'malicious' users creating several couples of (pk, sk))
 - The majority of money is honest

How to choose the right blockchain



Happy blockchaining!

Q&A

Pierluigi Gallo

pierluigi.gallo@unipa.it

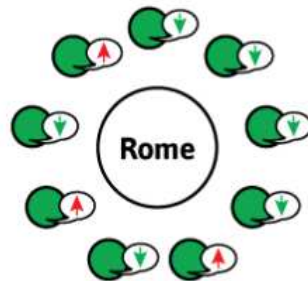
The Byzantine Generals' Problem



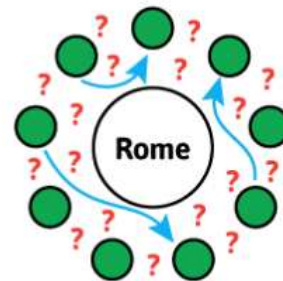
Rome being
by **nine armies**,
commanded by a
(nine) general.



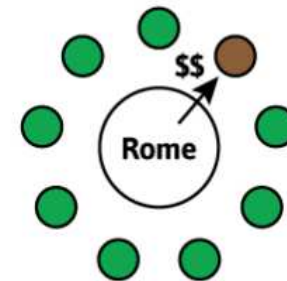
In order to launch a
successful **attack** or retreat,
all armies have to **do the
same**, otherwise they will
be decimated by Rome's
armies.



The decision to either
attack or retreat is put up
to a **vote**. Whichever option
receives **more than 50%** of
the votes, that's what the
Generals will do (**retreat** in
the example above).



Problem 1
The generals communicate
by using **couriers**, who
have to cross unknown
areas controlled by the
Romans, risking capture or
their message becoming
corrupt.



Problem 2
Each of the generals could
be bribed by the Romans:
Traitorous Generals.



Problem 3
Any of the Generals
could make the wrong
decision, regardless of the
bribe, resulting in a
**Improperly Funded
General.**

<https://cryptographics.info/cryptographics/blockchain/consensus-mechanisms/delegated-byzantine-fault-tolerance-dbft/>

