The blockchain and its applications to energy, videosurveillance and e-commerce

Pierluigi Gallo
pierluigi.gallo@unipa.it

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

Outline

- Motivation
- Blockchain applications
- blockchain technical intro
  - Hash functions
  - Hash cash
  - Blockchain structure
- Comparison between finance transactions and energy transactions
- Application in videosurveillance
- An exemplary application in e-commerce

Pierluigi
Gallo

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

Motivations

- Why we talk about blockchains during a Linux Day?
  - It’s an hot topic and everyone talks about it
  - Several platforms are designed to run everywhere, most of them run on Linux
  - For the Kerckhoffs's principle the code has to be open source

Pierluigi
Gallo

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

Applications

- **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
- **Notary and Real Estate**
  - Ubitquity
- **Testament and crypto-will**
  - Smart will
- **Stock trading**
- **Trading**
  - OpenBazaar
- **Energy management**
  - **EWF (Energy Web Foundation)**
  - Transactive Grid, LO3, SolarCoin, AutoGrid
- **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
- **Videosurveillance**

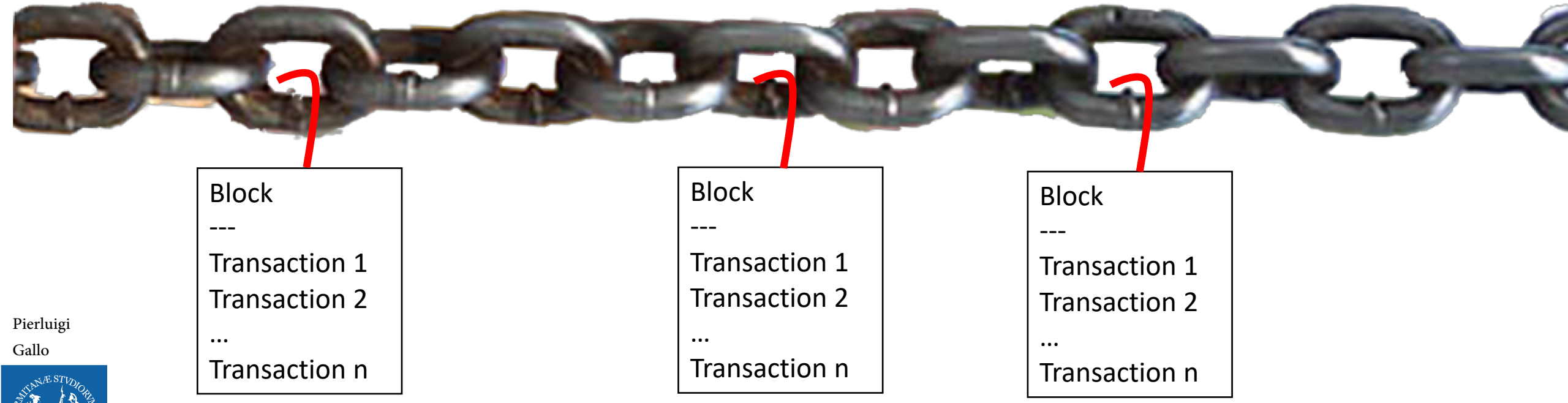
Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

What is a blockchain?

*Blockchain is a **data structure** containing **authoritative** log of **validated** transactions without a **trusted** intermediary*

The blockchain as a chain of ownership



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

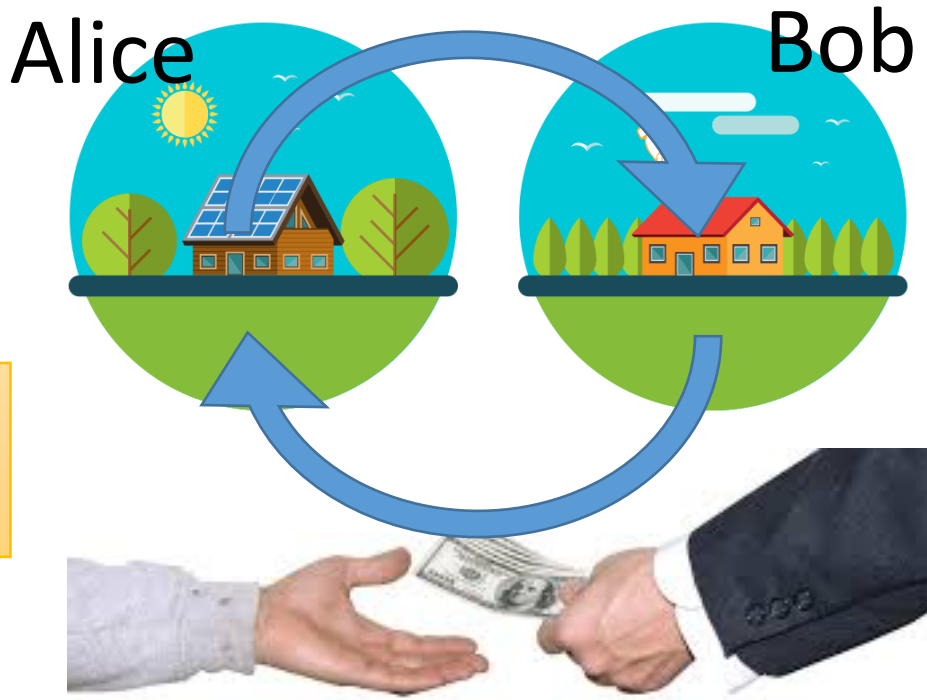
Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

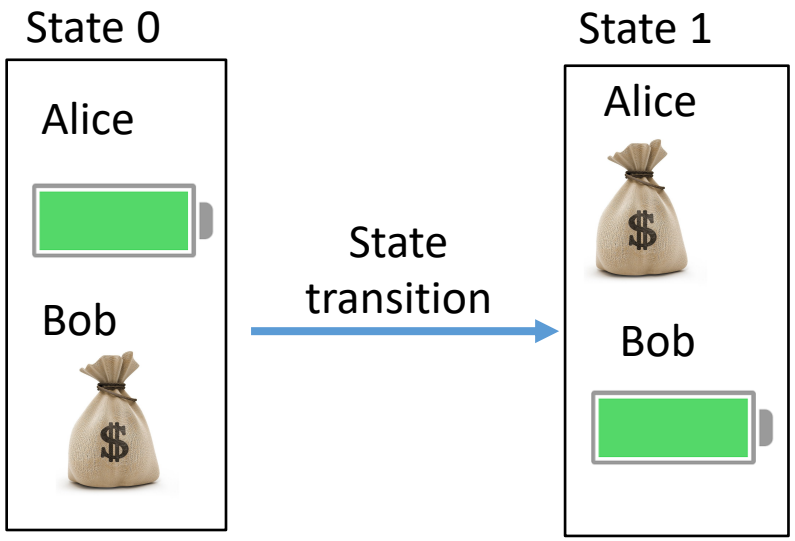
From financial transactions to energy transactions

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

Transition - from Latin Transitionem, *pass, passage*



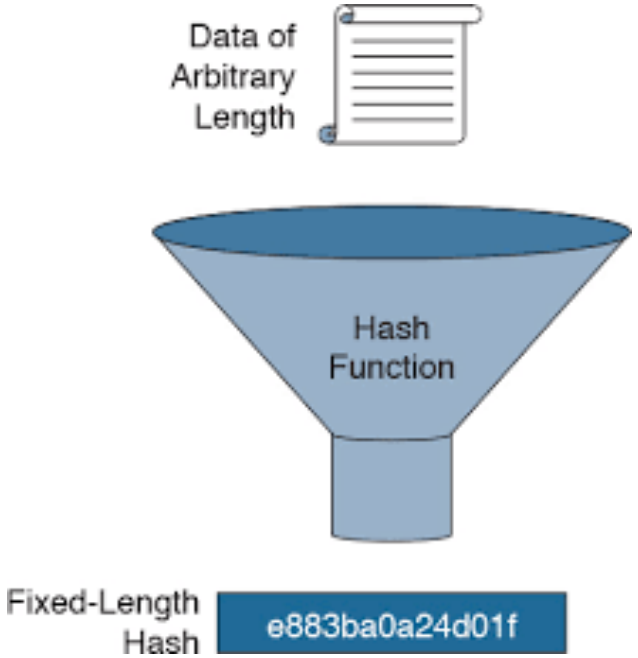
- Mapping the physical (and digital) world in the digital world
- Transactions are movements of anything with a value between two parties
  - **In Bitcoin** transactions keep track of **transfer of bitcoins**,
  - in the energy sector, transactions involve the transfer of **energy between a generator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

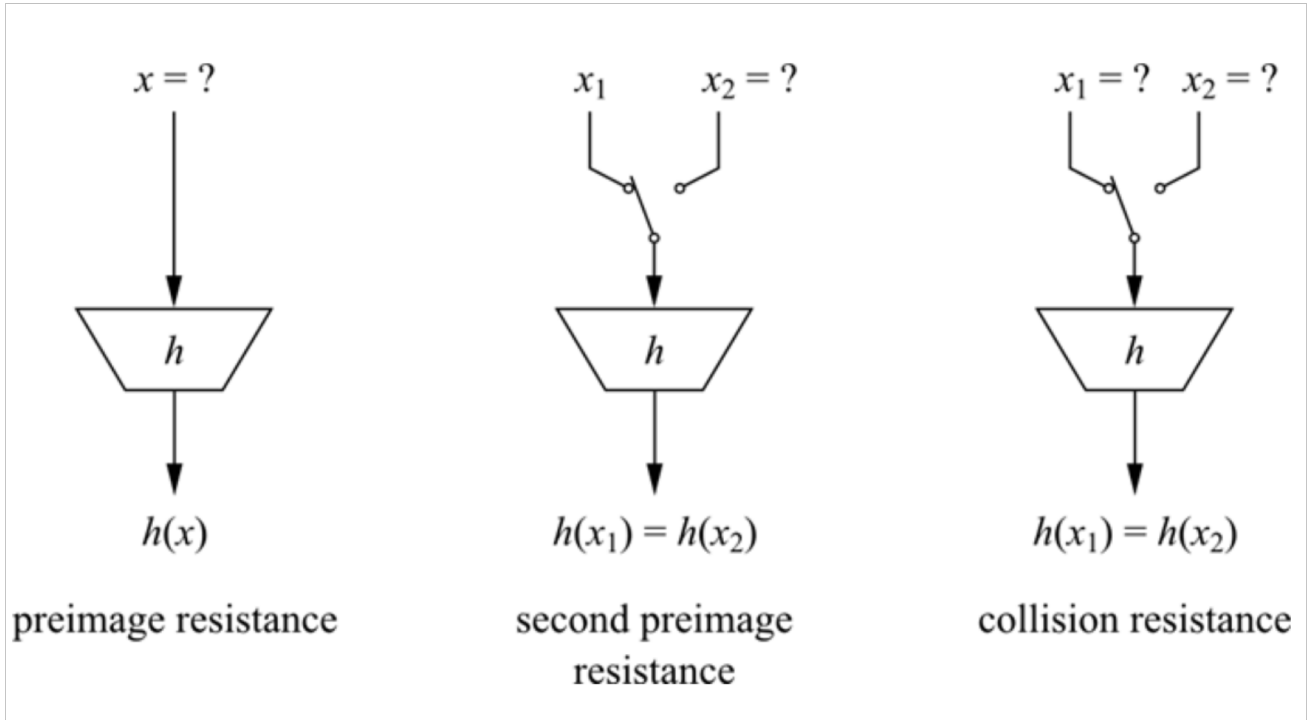


Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

Hash functions





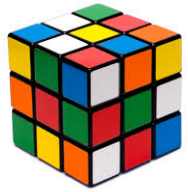
Understanding Cryptography – Christof Paar and Jan Pelzl

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

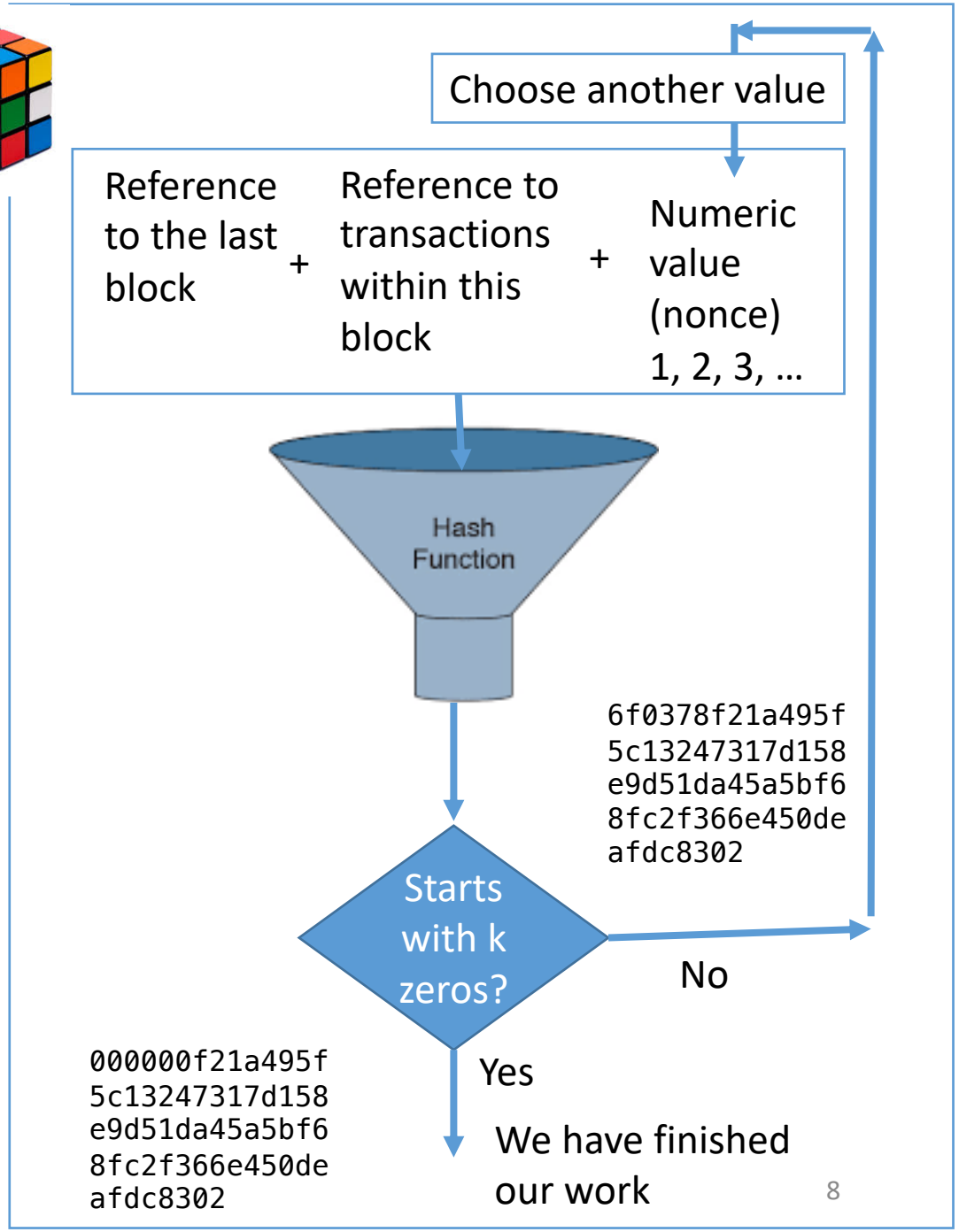
Pierluigi
Gallo

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

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
- This work is 'provable' (it only needs to compute one hash to prove it)
- dynamically adjusted target
- Hashcah makes block creation computationally "hard"
- SHA256 is designed to be a completely unpredictable pseudorandom function, the only way to create a valid block is simply trial and error, repeatedly incrementing the nonce and seeing if the new hash matches
- The winner of this puzzle will be able to write his block in the blockchain
  - It is rewarded with some 'transaction fee'
  - The other ones will stop their quest for the solution

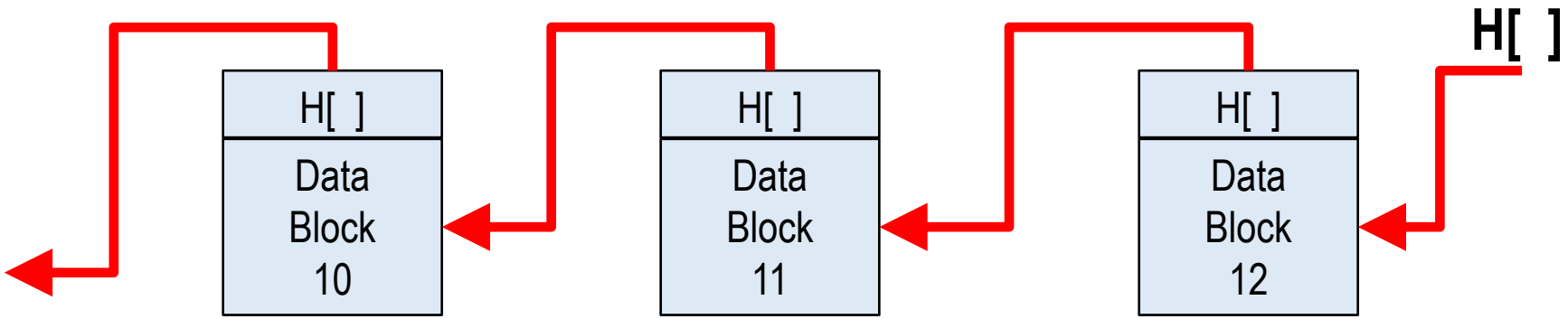


Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

Blockchain internals: Hash pointers

Blockchain are append-only, they maintain the whole history



Hash Pointer data structures, since the 70ies

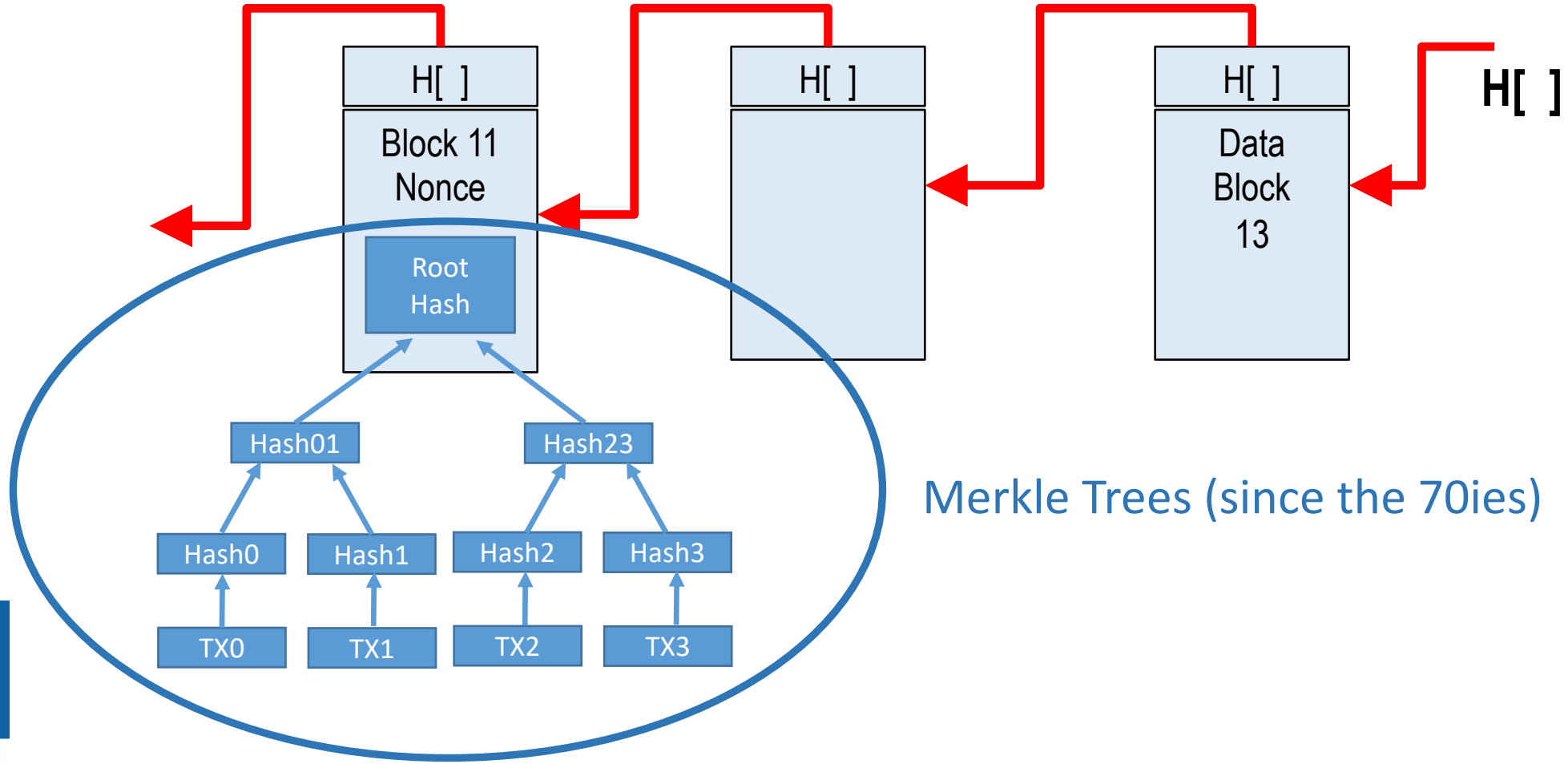
Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

Data Integrity guaranteed even on unsecure storage

Blockchain internals: Merkle Trees

Blockchain are append-only, they maintain the whole history



Merkle Trees (since the 70ies)

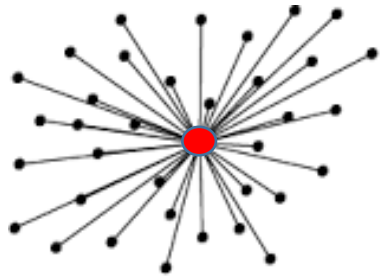
Data Integrity guaranteed even on unsecure storage

Pierluigi
Gallo

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

Blockchain features

Shareability across boundaries of trust
(no need for single trust anchor)



centralised

distributed

- Distributed ledger
  - Fully distributed, no need for middleman
  - Immutable
  - Byzantine fault tolerant system with decentralized consensus
  - Cryptographically secure
  - Works well in trustless environments
  - A fertile soil for smart contracts

3T

- **Traceability**
- **Transparency**
- **Trust**

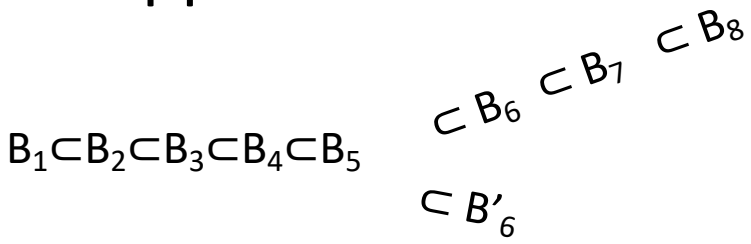
(no need for single trust anchor)

Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

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.

Pierluigi
Gallo

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

Orazi and Curiazi
(my personal view on proof of work)

A B C Z

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)

Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

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 bee 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?

Pierluigi
Gallo

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

How transactions are added and chained (consensus protocol)

- 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.

Pierluigi
Gallo

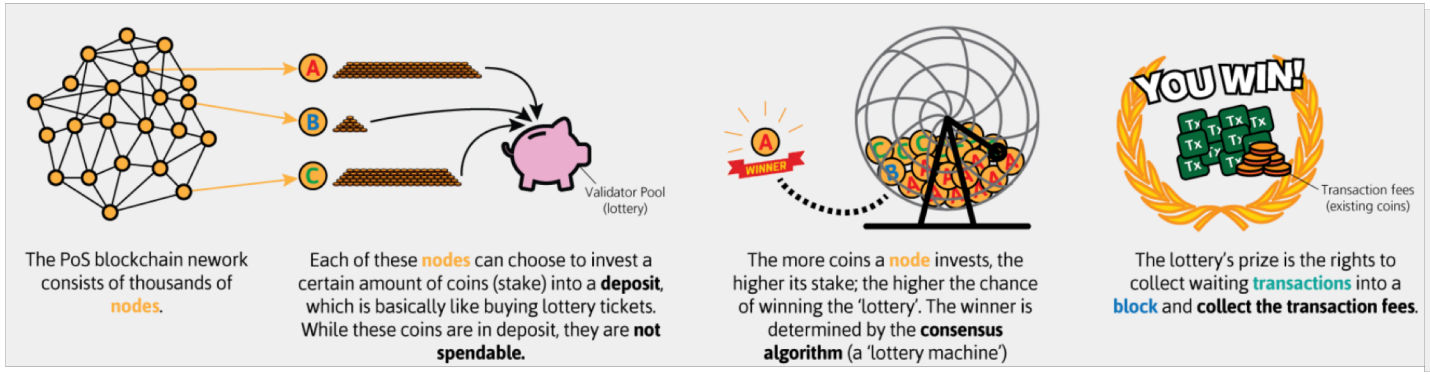
UNIVERSITÀ
DEGLI STUDI
DI PALERMO

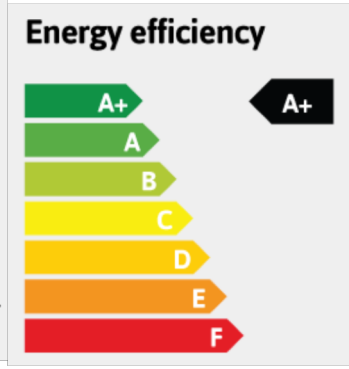
Lightweight proving before writing a block

- ~~proof of work~~,
- PBFT,
- proof of stake,
- proof of activity,
- proof of burn,
- proof of Elapsed Time (PoET),
- proof of location.

Pierluigi
Gallo

UNIVERSITÀ
DEGLI STUDI
DI PALERMO





Blockchain taxonomy by permission to write blocks

- Public or permissionless
  - Typical application: cryptocurrencies
  - Proof of work – requires a lot of energy

- Permissioned
  - Most of the rest of the applications, except cryptocurrencies
  - Proof of X (including proof of work)
  - Does not require much energy

- Private
  - Not of big interest

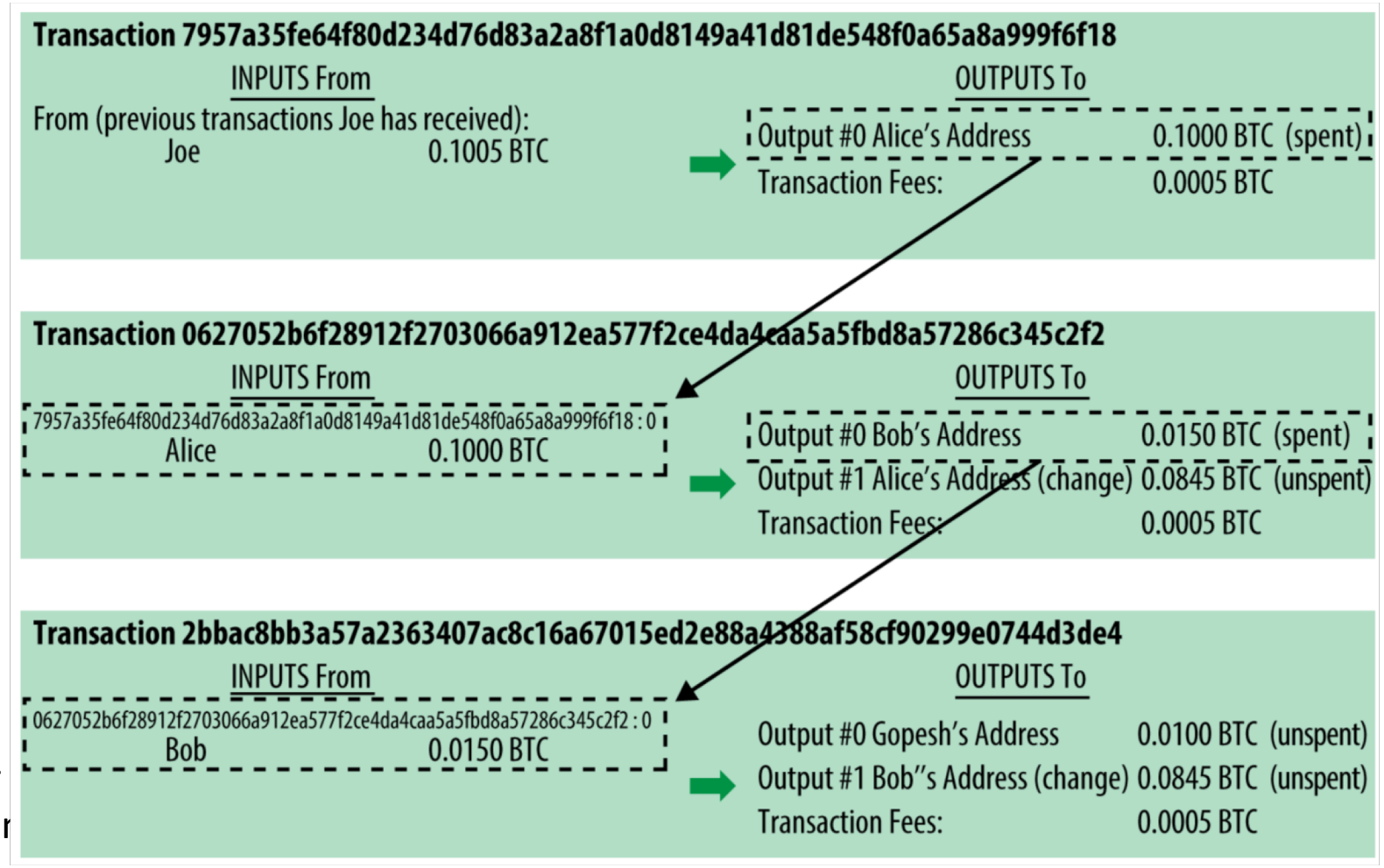
Pierluigi
Gallo

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

Financial transactions

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

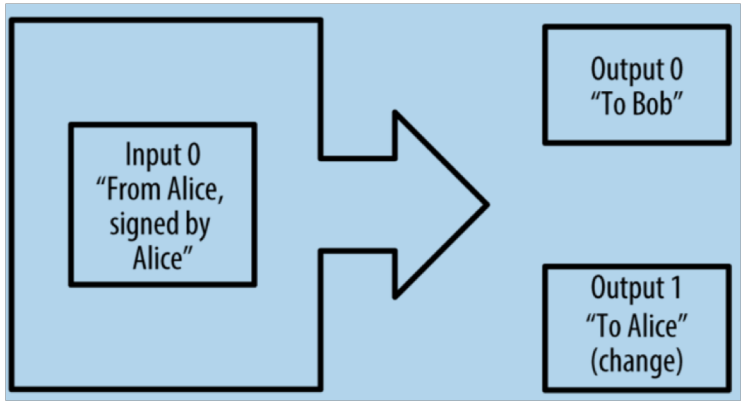
- Transactions are like lines in a double-entry bookkeeping ledger.
- one transaction contains:
  - one or more “inputs,” which are debits against a bitcoin account.
  - one or more “outputs,” which are credits added to a bitcoin account.
- The inputs and outputs (debits and credits) do not necessarily 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



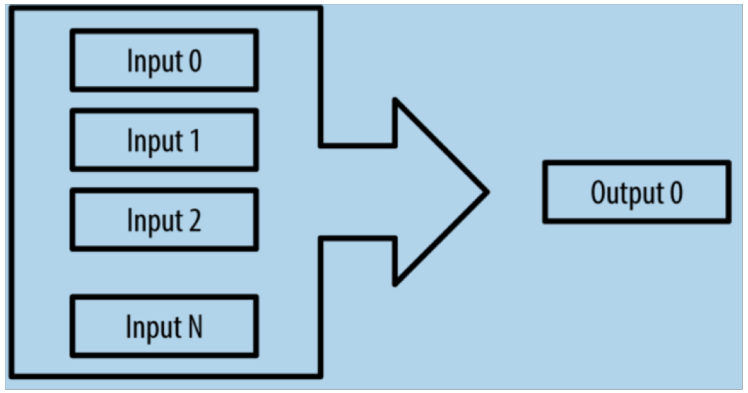
Transactions move value from *transaction inputs* to *transaction outputs*

Pierluigi Gallo
UNIVERSITÀ DEGLI STUDI DI PALERMO

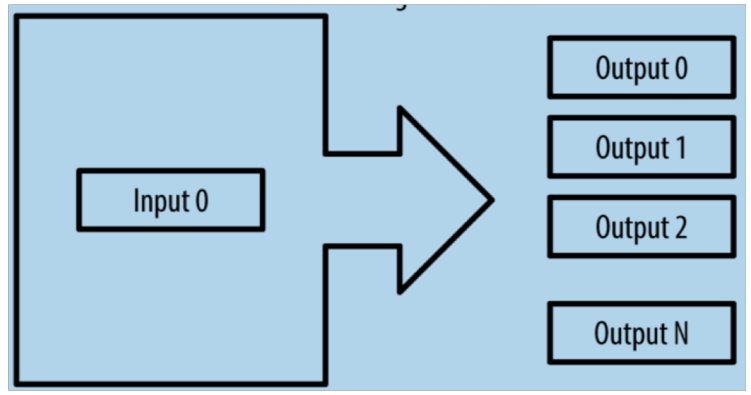
Typical financial transactions



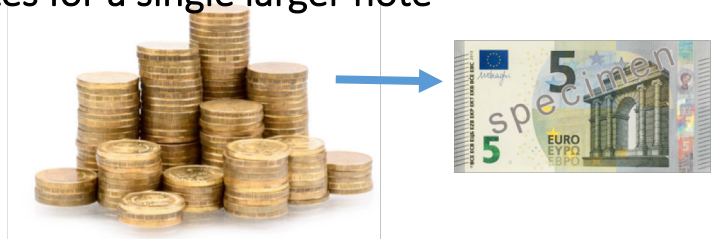
simple payment from one address to another, which often includes some "change" returned to the original owner.



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)



20 = 100-80

Pierluig
Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

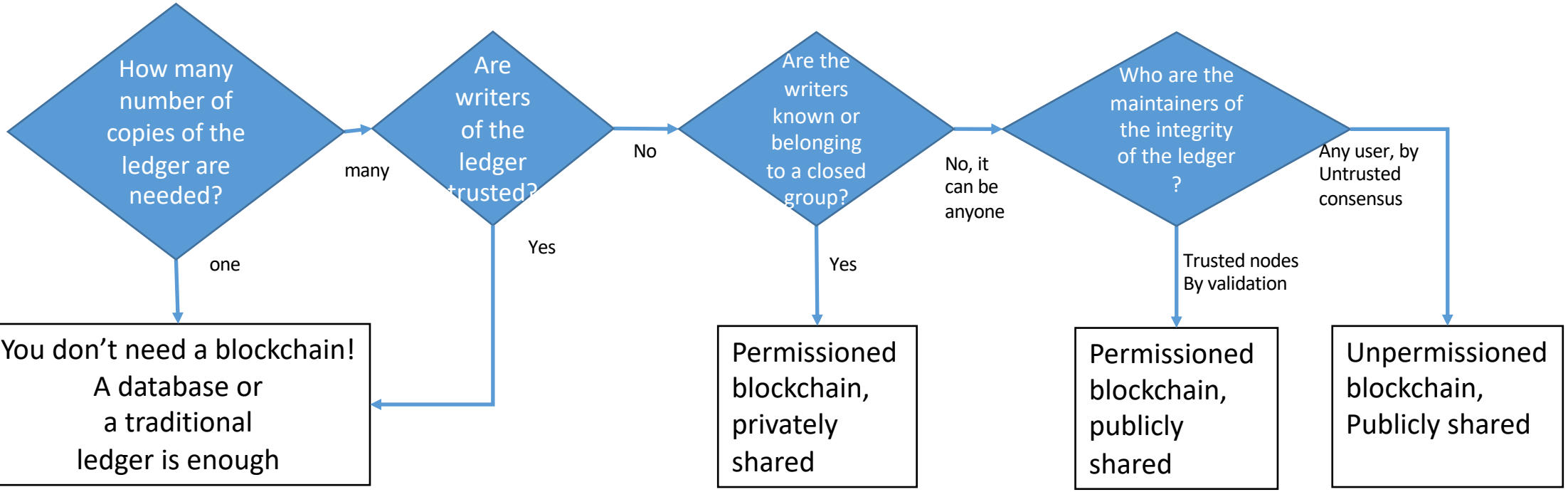
Blockchains taxonomy

- 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+Λ if the message is long, t+λ 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

Pierluigi
Gallo

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

How to choose the right blockchain



Pierluigi Gallo

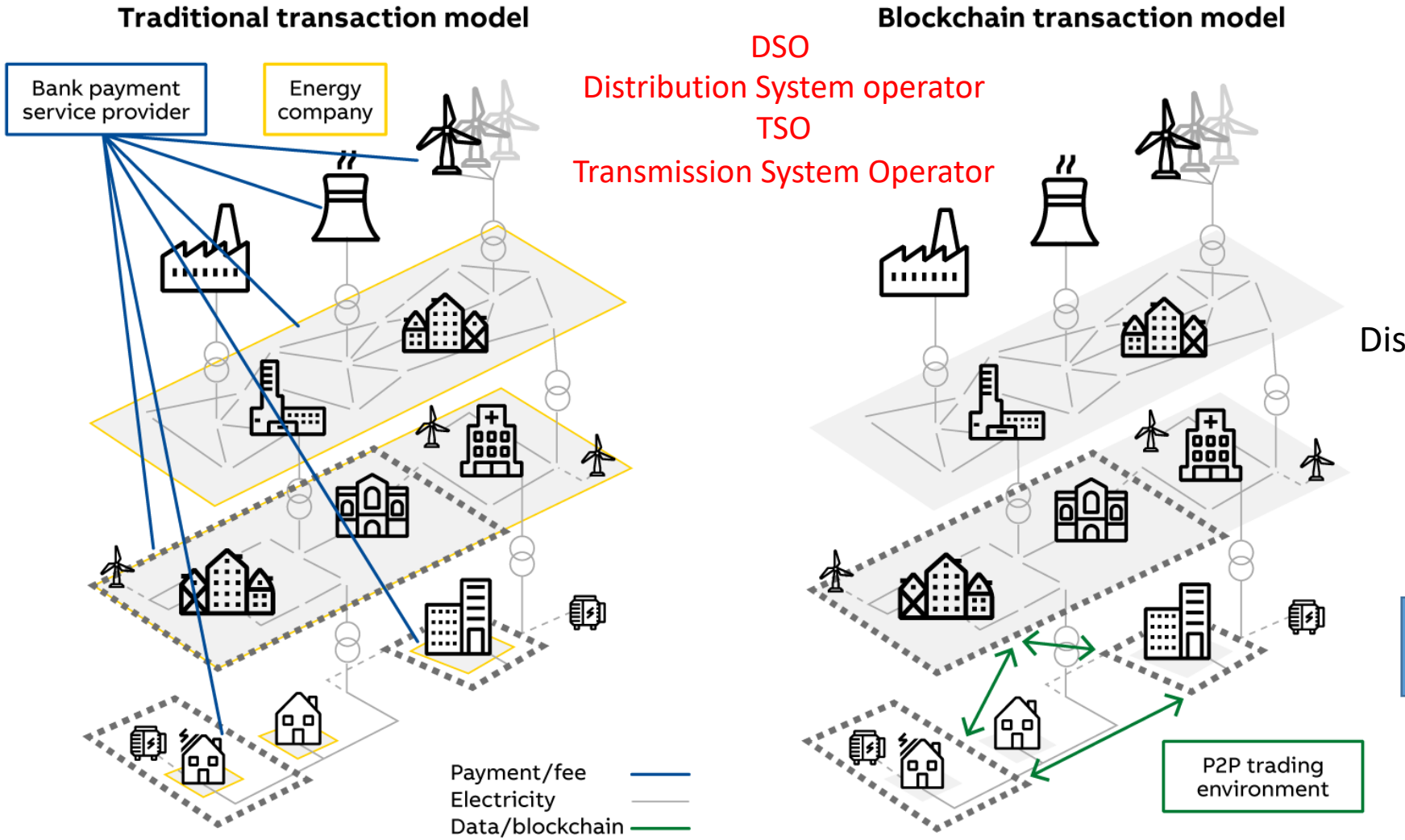
UNIVERSITÀ DEGLI STUDI DI PALERMO

Blockchain for energy transactions

Pierluigi
Gallo

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

Modelling energy transactions
(monetizing energy exchanges)

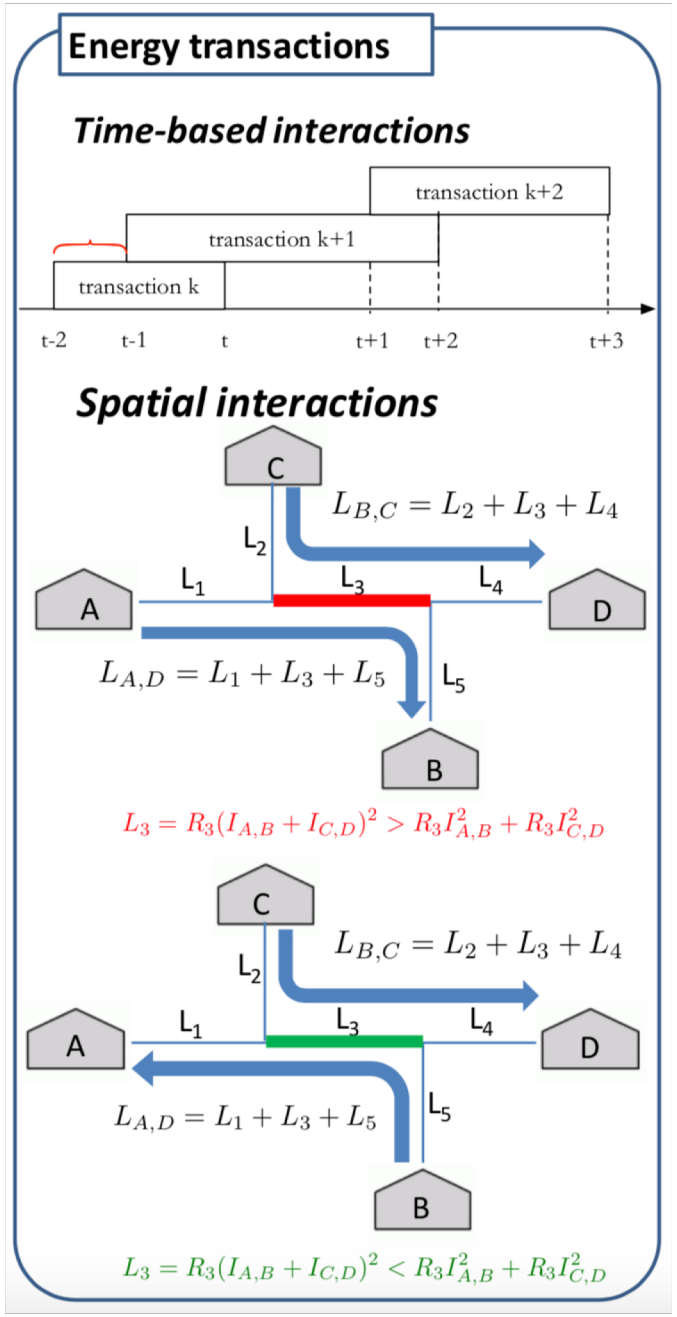


Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

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



Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

Regulatory challenges for energy transactions

Energy

- **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**

Pierluigi
Gallo

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

Law and blockchain

- balancing consumer protection interests with the interests of energy suppliers
- The current energy market in Europe is not yet ready for blockchain adoption
- 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) has recently entered into force (May 2018)** (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

Pierluigi
Gallo

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

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***

Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

BlockSee: Blockchain and videosurveillance

Motivation

- Video-surveillance systems are an important part of smart cities
- Video flows and camera settings can be tampered
- Scene reconstruction from multiple cameras of different owners

Court of Cassation, Italy's supreme court, states that to modify the field of view of the camera or change its optical properties are simple operations that can be done out of control from the appellants and can lead to potential privacy issues

Goals

- Tracing camera settings over time
- Making video sequences available in case of events

Methodology

- Computer vision + Blockchain

Results

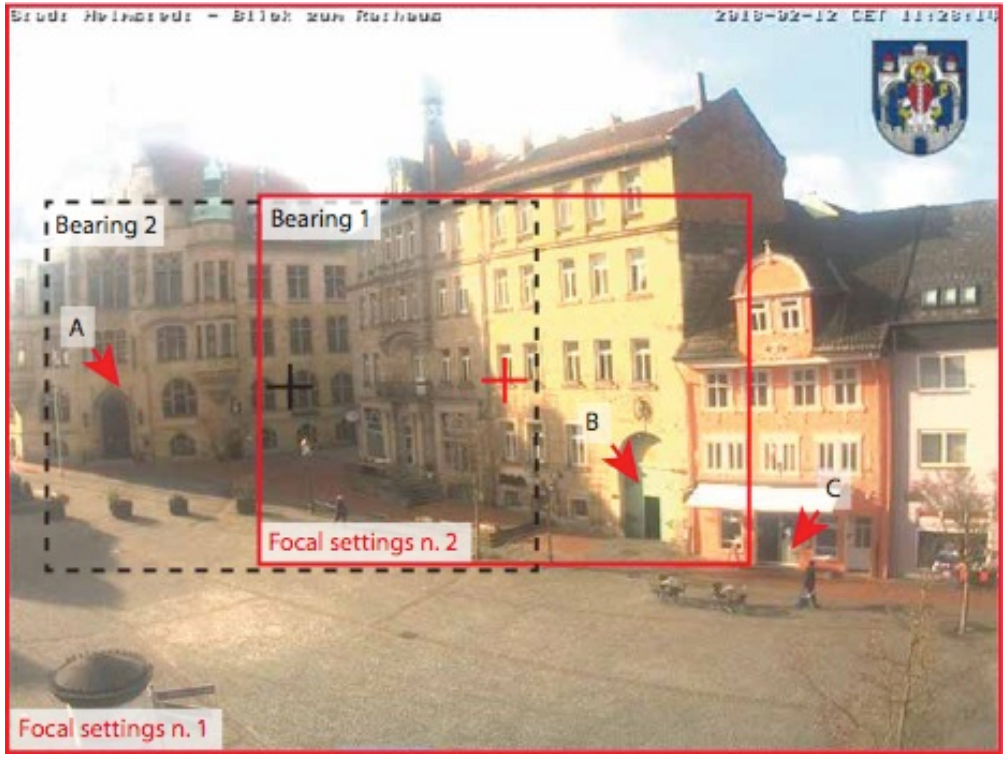
- Performance of the proposed tool

Pierluigi Gallo, Suporn Pongnumkul, Uy Quoc Nguyen, "BLOCKSEE: BLOCKCHAIN FOR IOT SURVEILLANCE IN SMART CITIES", to appear in Proceedings of EEEIC 2018, Environment and Electrical Engineering , June 2018,

Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

Camera settings and privacy



Camera settings

- Position of the camera
- Direction of view
- Zoom level
  - Focal length (varifocal cameras)

- Video surveillance is an important security element of modern cities
- CCTVs pointed to inappropriate directions could violate the privacy of others
- Can modifications of camera settings be prevented? Can them be detected?

Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

Image analysis for tracking camera settings

February 2018

April 2018

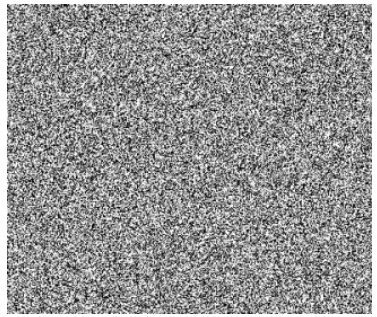
- Removal of watermarks and time indications
- Segmentation
  - distinguish background and foreground
  - Usually background substraction, BlockSee has different interests
- Background usually does not contain information while for BlockSee it is crucial

- Estract features from background
  We used **BRISK**, Binary Robust Invariant Scalable Keypoints but other choices are possible
- Position features to the borders – features as fingerpring of camera settings

Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

Accountability, proof of immutability, confidentiality



encryption
M-of-N transactions

Three types of frames (and camera configurations):

- Normal (signed only by the camera)
- Accountable (signed by the camera and by a technician)
- Certified (signed by the camera, the technician and a court official)

M out of N can decrypt
And watch the video.
No need to search for video
In case of events

- proof of immutability, as provided by BlockSee. Any modification of camera settings is permanently recorded on the blockchain and can be timely faced.

Pierluigi
Gallo

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

Trading evolution

Have / request

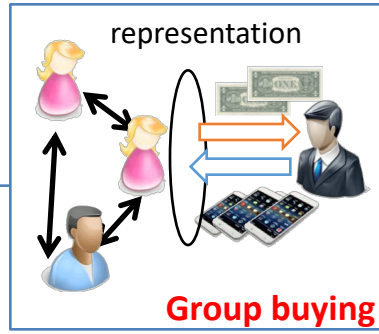
Want / receive

Local interaction

in the past

Large-scale interaction buyer /seller - Static pricing

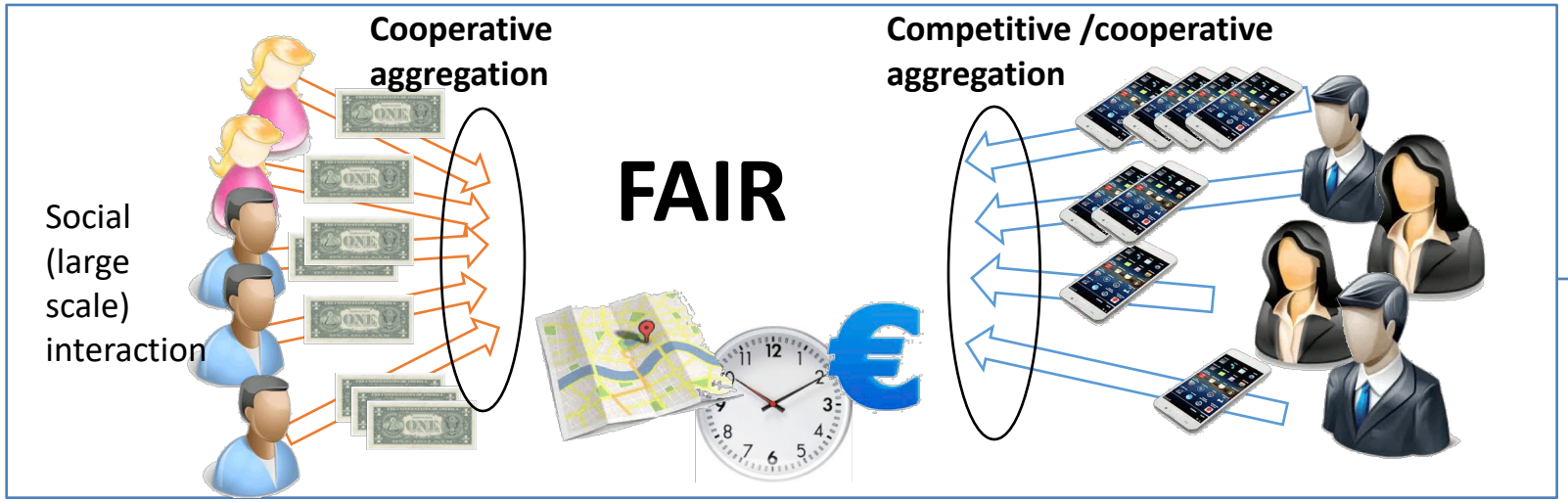
Large scale interaction, increasing prices



Small scale interaction among buyers - Static pricing

Large scale interaction buyer /seller – No cash

today



Dynamic pricing – control on pricing

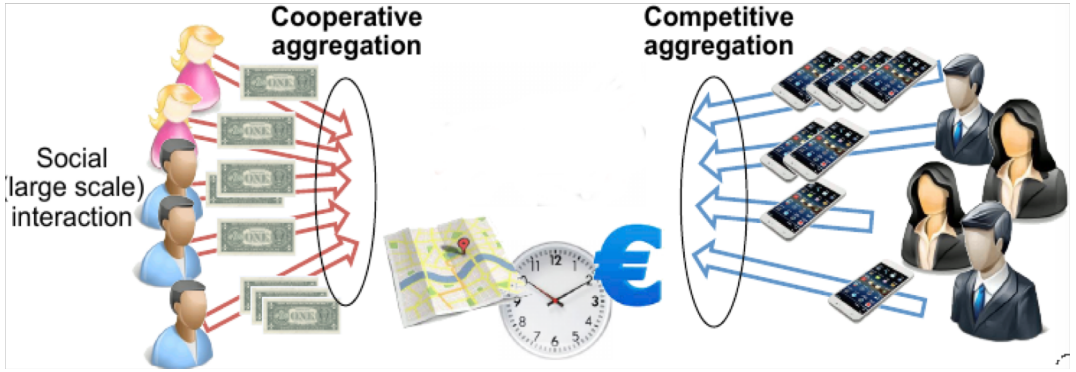
tomorrow

Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

e-Fairs in brief

e-Fairs: new business model based on **aggregation.**



Aggregation

Buyers aggregation

- Fairs aggregate purchase orders from buyers;
- **Cooperative**: the more buyers aggregate, the more they save.

Sellers aggregation

- e-Fairs aggregate supplies from sellers;
- **Cooperative**: e-Fairs aggregate demand may be fulfilled by several sellers;
- **Competitive**: sellers compete to

Shipment aggregation

Reduces shipment costs because of a single delivery instead of multiple ones;

Reduces pick-up points revenues for parcel withdrawal;

Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

e-fair components and challenges

- Price model
- Cost optimization
- e-Fair participation
  - Distributed approach to aggregate buyers/sellers (no central platform)
  - Notification
  - Commitment of the participating buyers/sellers
  - Traceability of people that join the e-fair
  - Distributed approach
  - Transparency for buyers and sellers
  - Trust
  - Actors have competing objectives
- e-Fair evolution
  - Handle users that join the e-fair
  - Start and end of the e-fair
  - Run the optimization algorithm (when? centralized/distributed?)

Background

May we use a blockchain?

May we use smart contracts?

Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

Smart contracts

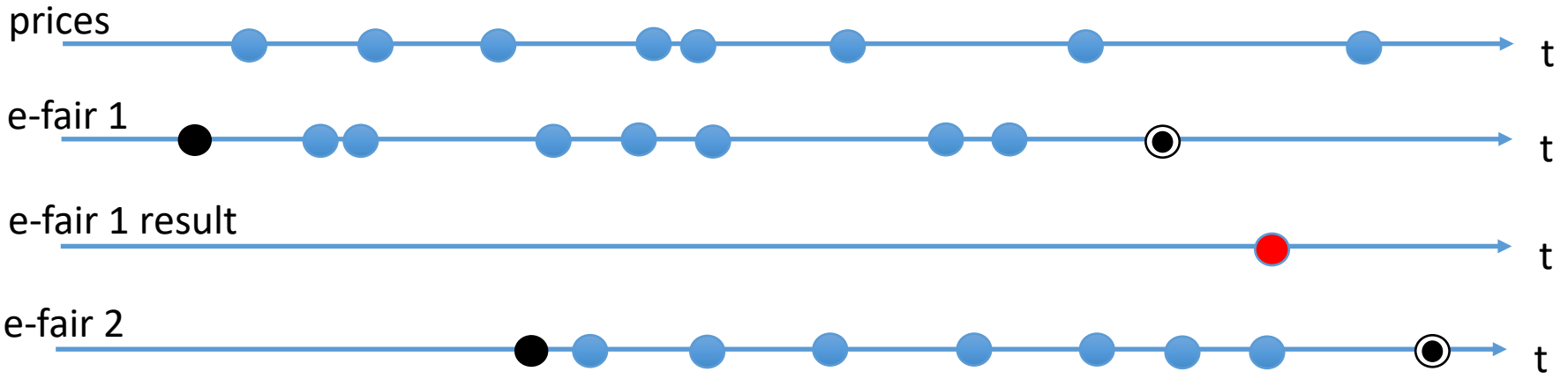
- ***Smart contracts*** *are self-executing* ***contracts*** *with the terms of the* ***agreement*** *between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network.*

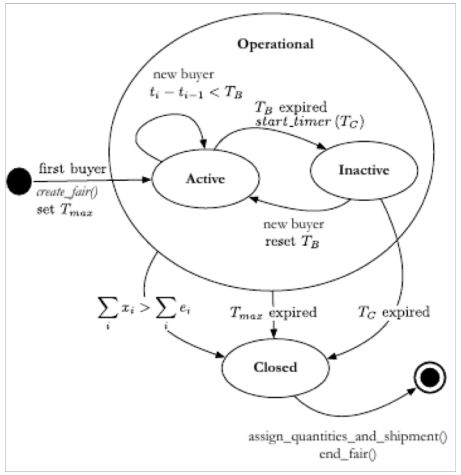
- *I'm a blockchain, it is raining, therefore let me execute a smart contract!*
  - *Who verifies it is raining?*
  - *Is him trusted?*
  - *How to verify the occurrence of a condition in the real world?*

Pierluigi
Gallo

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

Handling the e-fairs





- Identity of the buyers are known
- Transactions contain the requests to join the e-fair
  - The request to join is signed by the buyer
  - The request to join is added on the Multichain stream
  - The buyer is committed to buy the product, all other participants to the e-fair know about it (transparency)
  - The chronological order is fundamental, as buyers are rewarded depending on the time they arrive in the e-fair
- Buyers have contrasting goals, but they all want to maximize the number of participants to the e-fair
- Buyers (and sellers) are not trusted

The smart contract relies only on data that are already on the blockchain (the requests to join the e-fair)

Pierluigi Gallo

UNIVERSITÀ DEGLI STUDI DI PALERMO

Happy blockchaining!

Q&A

Pierluigi Gallo

pierluigi.gallo@unipa.it