# Basic Principles of Security and Blockchain

Spring 2021,

Instructor: Fabrizio Baiardi, Laura Ricci
f.baiardi@unipi.it
laura.ricci@unipi.it

## Lesson 1: Introduction

23/2/2021

# COURSE STRUCTURE

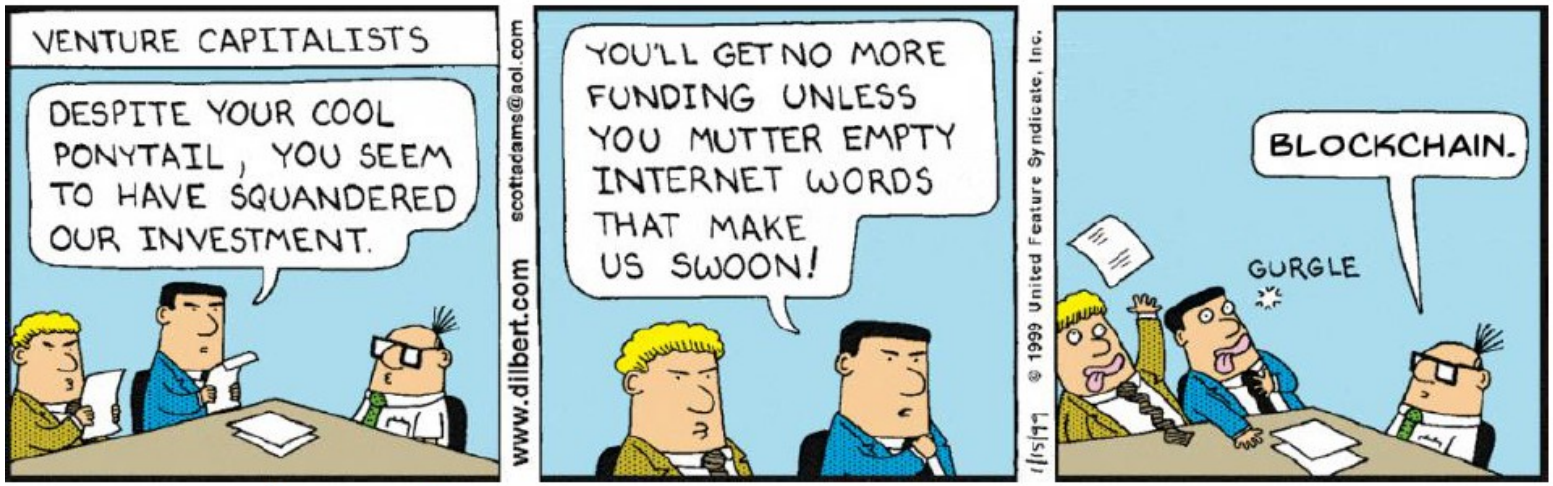
- security
  - introduction and glossary
  - adversary modelling
  - adversary simulation
- blockchains:
  - introduction: basic concepts
  - consensus mechanisms: different flavours
  - applications
- exams:
  - seminar on one of the topics of the course OR development of a simple project
  - proposals coming from the students and suggestions by the teachers

# BLOCKCHAINS: WHY TO STUDY THEM?

- to avoid this...

# BLOCKCHAINS: WHY TO STUDY THEM?

- and maybe take advantage of this....



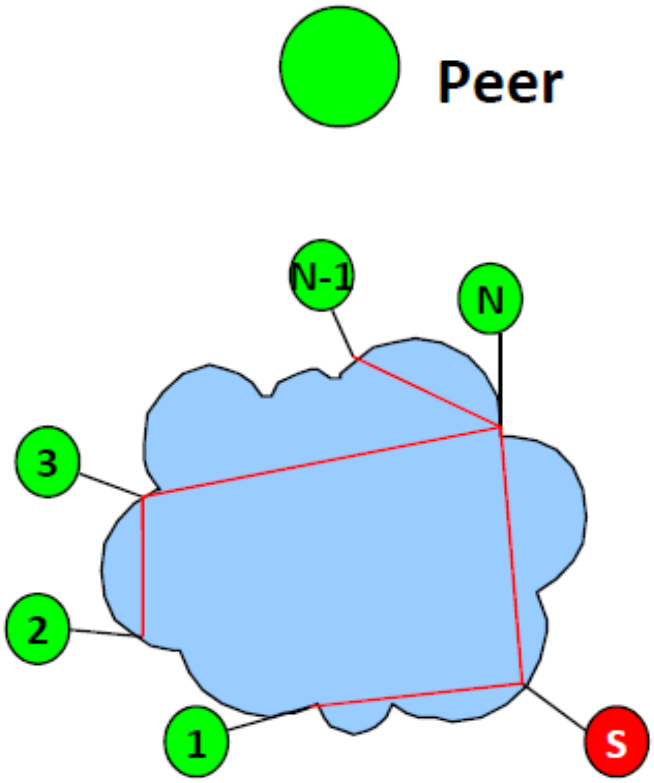

MENU CNBC MARKETS BUSINESS NEWS INVESTING TECH

## Salaries for blockchain engineers are skyrocketing, now on par with AI experts

- Blockchain engineers are making between $150,000 and $175,000 in annual salaries on average.
- Blockchain engineers are the top paid roles in software development, on par with specialists focused on artificial intelligence.
- Demand for blockchain engineers has increased by 400 percent since late 2017 on Hired, a firm that helps clients recruit tech candidates.

# THE PEER TO PEER PARADIGM

- symmetric paradigm, different with respect to client server
- run on end-hosts
- on/off behavior, handle churn
- need to join and discover other peers
- nodes are service providers an consumers
- communicate directly among them
- need to define communication rules
  - prevent free riding
  - incentivate participation ... and reciprocation



# THE PEER TO PEER PARADIGM: A GENERAL DEFINITION

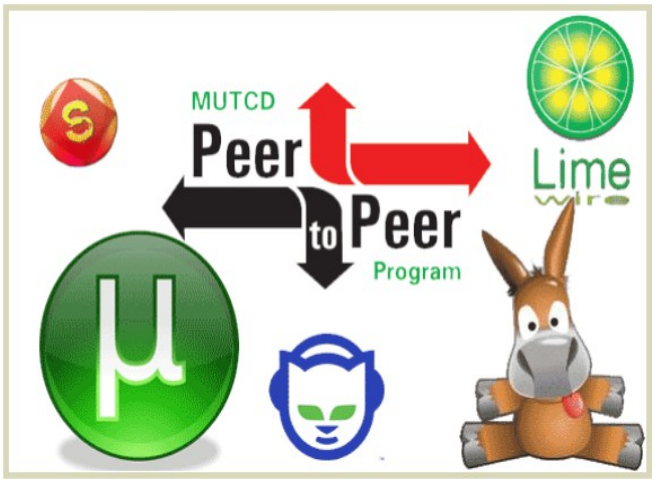
- A peer to peer system is a set of autonomous entities (peers) able to auto-organize and sharing a set of distributed resources in a computer network. The system exploits such resources to give a service in a complete or partial decentralized way. The system is able to adapt to a continuos churn of the nodes maintaining connectivity and reasonable performances without a centralized entity (like a server)

- Shared Resources:
  - Ledgers/Blockchains
  - Read/Write storage space (Distributed File System)
  - Computing power
  - Bandwidth

# P2P KILLER APPLICATIONS

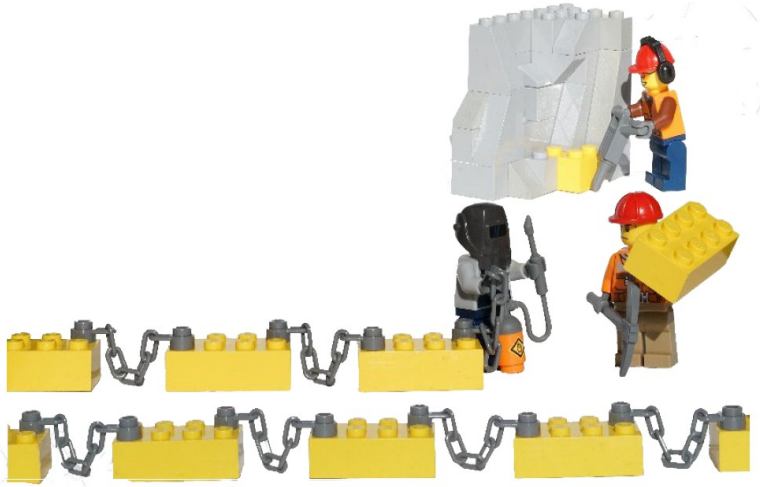
## First generation applications: file sharing

- read only, no writers
- light weight/ best effort
- persistence and security are not  the main goal
- anonymity  is important
- examples:
  - Napster
  - Gnutella, KaZaa
  - eMule
  - BitTorrent

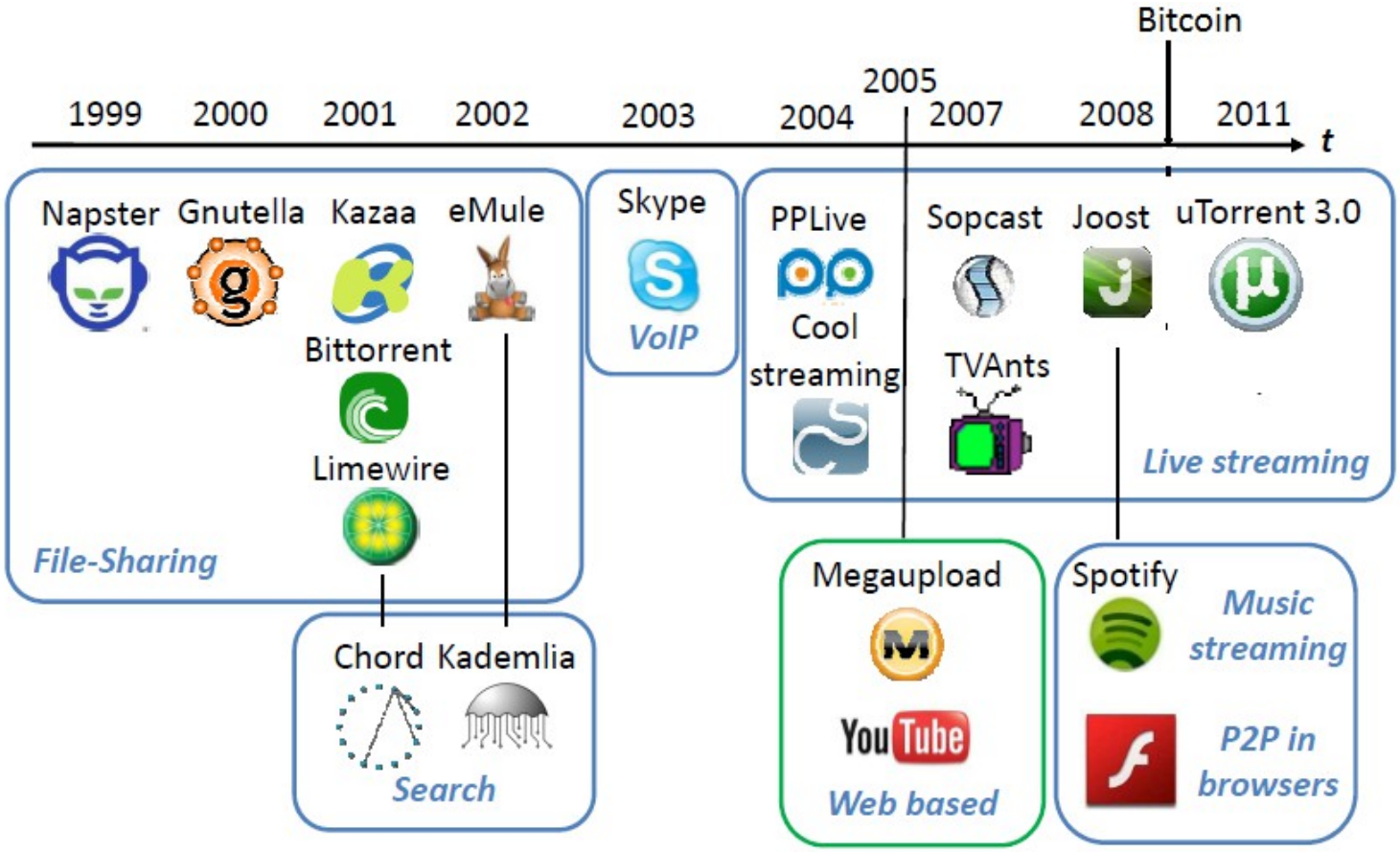



## Second generation applications

- cyptocurrencies and blockchain



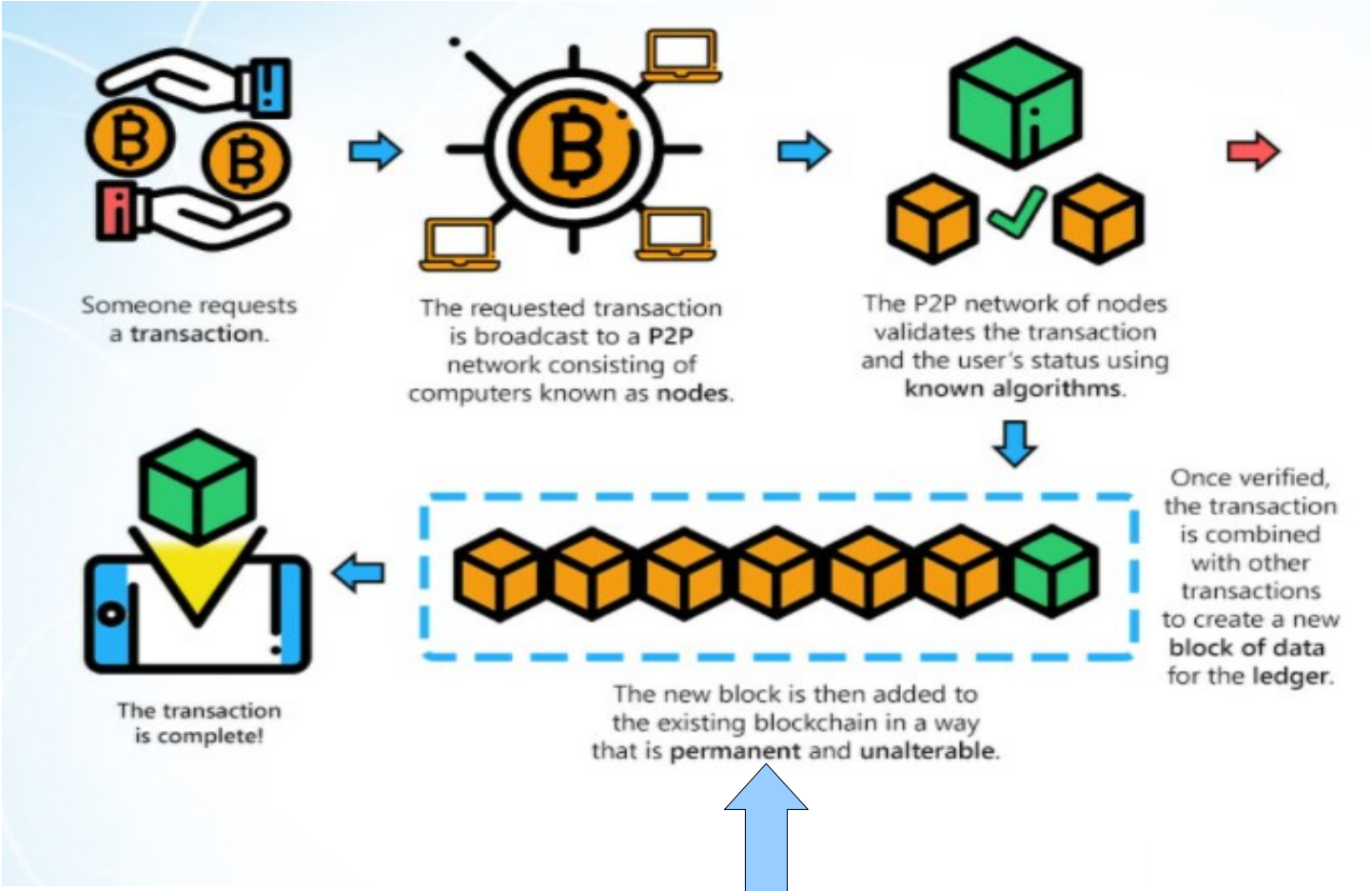
# P2P BEFORE THE BLOCKCHAINS



# BLOCKCHAIN: WHAT IS IT?

- Definition #1
  - a shared database stored in multiple copies on computers throughout the world
  - maintained without the need for a trusted central authority (e.g. a bank, a government, Google, etc.)
- Definition #2
  - replicated and consistent, immutable, append-only data storage system resistant to tampering
- Definition #3
  - a decentralized, state machine that is maintained by untrusted actors, secured by economic incentive
  - cannot delete data
  - cannot be shut down or censored
  - supports defined operations agreed upon by participants
  - participants may not know each other (public)
  - in actors best interest is to play by the rules

# A BLOCKCHAIN IN A NUTSHELL




consensus

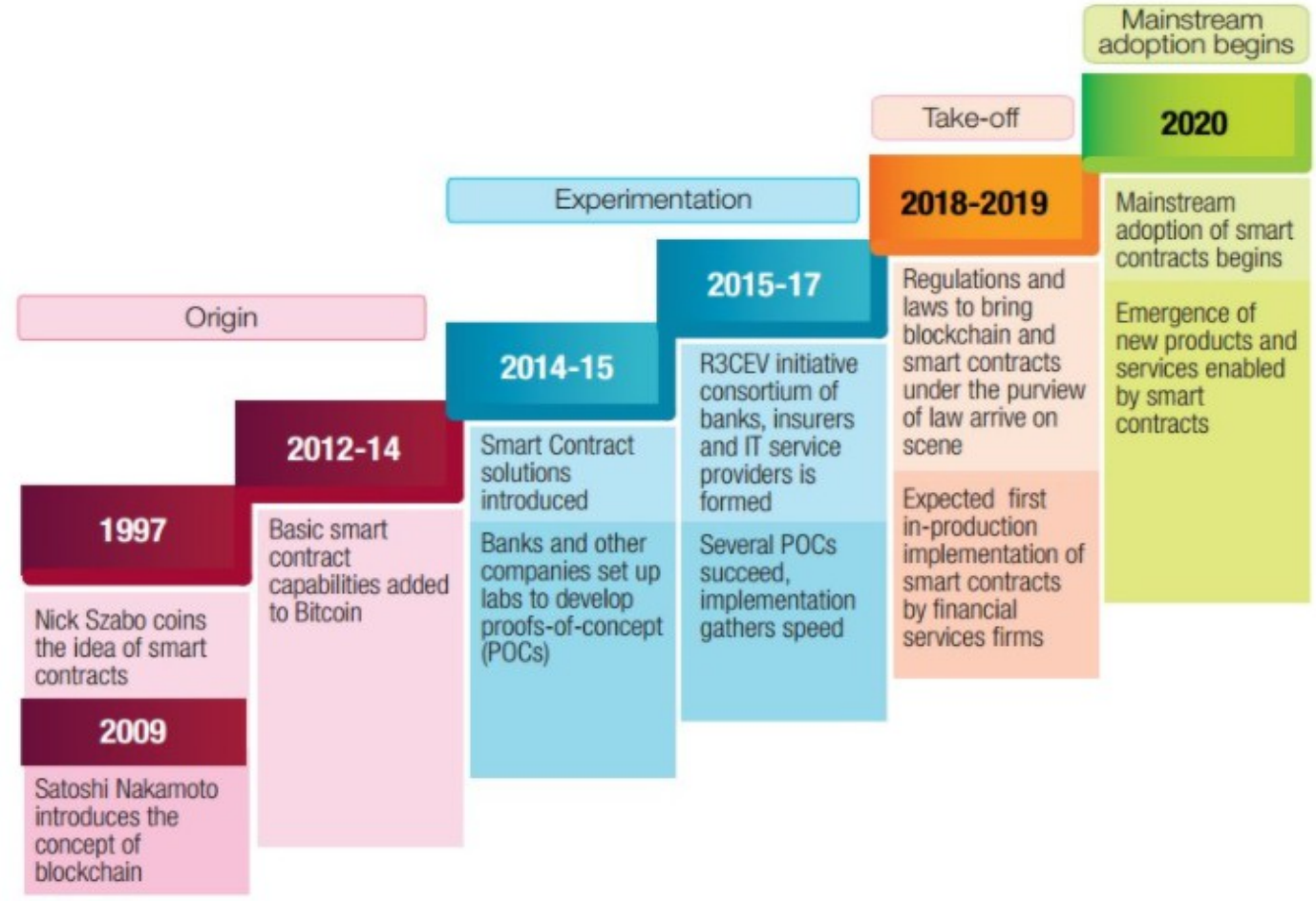
# WHICH TECNOLOGIES ARE INVOLVED?

- Cryptography
  - Digital signatures (e.g. public-key cryptography) to provide authentication
  - Cryptographic hash functions (e.g. hash chains of data transactions) to provide tamper-resistant immutability
- Distributed consensus amongst mutually distrusting replica
  - decentralized control
  - provides consistency among the replicas
- Formal Methods: to prove properties of
  - consensus algorithms
  - smart contracts
- Data analysis and Machine Learning Techniques
  - a lot of public data is avaliable from permissionless blockchains
  - calls for complex network analysis tools, also exploiting AI

# AND MANY CHALLANGES.....

- applied cryptography: novel efficient implementation of cryptographic techniques
  - Zero-knowledge, Diffie-Helmann, Multiparty Computation,....
- techniques to increment the scalability
  - off-chain channels,...
- interledger techniques: techniques to exchange transaction between different ledgers.

# BLOCKCHAIN EVOLUTION



# "THE MOTHER OF ALL BLOCKCHAIN": BITCOIN


**Bitcoin: A Peer-to-Peer Electronic Cash System**

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of

```
bitcoin-0.1.0.rar
bitcoin-0.1.0.tgz
```

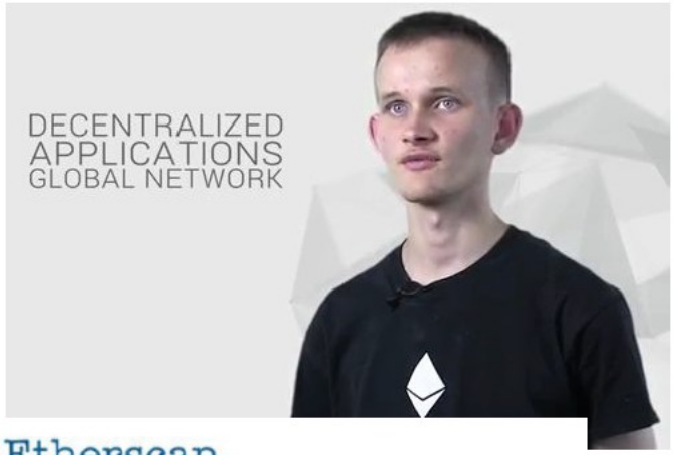
**Paper published in October 2008: working from 2009**

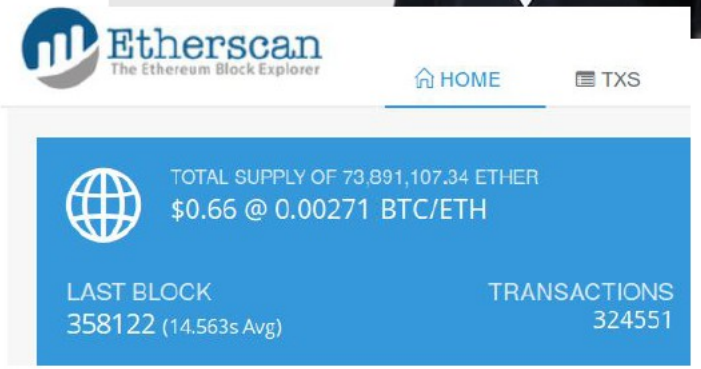
# BITCOIN: P2P CRYPTOCURRENCIES

- payments directly done between the users, no centralized financial entity which guarantees the electronic payment, lower costs
- the cypherpunk vision: "we can revolutionize our world by building secure protocols"
- new motivation and tools for learning traditional concepts in computer security
- after Bitcoin....."Blockchain technology," a related and more general concept
  - a new technology for developing secure applications in an untrusted environment
  - Ethereum and many others
  - As such, it affects many processes, companies and societies

# ETHEREUM

- Crowdfunded ~$20M in ~ a month
- Popularized a grand vision of "generalized" cryptocurrency
- smart contracts:
  - implement a protocol that uses a block-chain
  - programmable through Turing complete language
    - Solidity
    - Serpent,...
  - executed by all nodes: consensus as agreement on the results of computation



# THE ETHEREUM BLOCKCHAIN

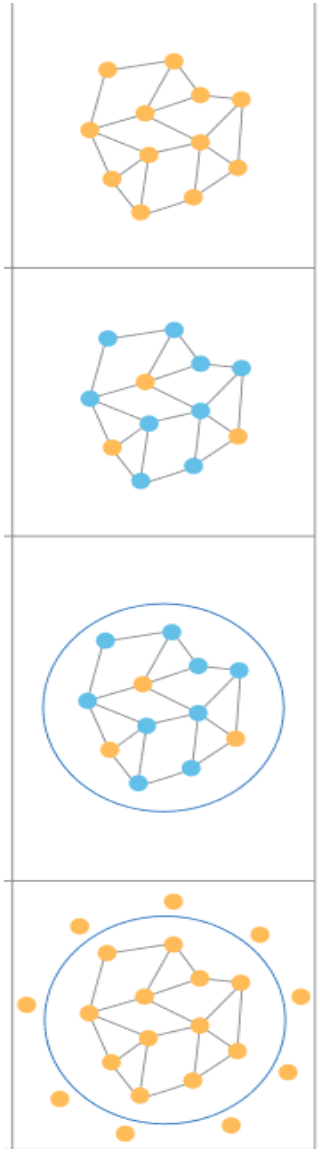
- introduces smart contracts to be executed by blockchain nodes
  - Turing-complete : can solve any computational problem
    - in Bitcoin scripts have only limited computational power
  - gas to avoid denial of service
- treats blockchain and its nodes as a single, global, replicated, consistent computer
- entire state machine, its code, and its input/output replicated and executed in a consistent manner

# ONE CONCEPT, DIFFERENT FLAVOURS

- classification on the basis of who can read, generate and validate transactions and blocks
- public vs. private
  - public: anyone can access the blockchain and read its content
  - private: only authorized parties can read the blockchain
- permissionless vs. permissioned
  - permissionless: anyone can send and validate transactions
  - permissioned: entities are authorized to execute and validate transactions

# ONE CONCEPT, DIFFERENT FLAVOURS

- yellow dots
  - validators nodes can also transact
- lightblue dots nodes that
  - can transact
  - but cannot validate transactions and partecipate to the consensus
- blue circle
  - only nodes within the circle can see the transaction history
- no circle
  - everyone can see the transaction history



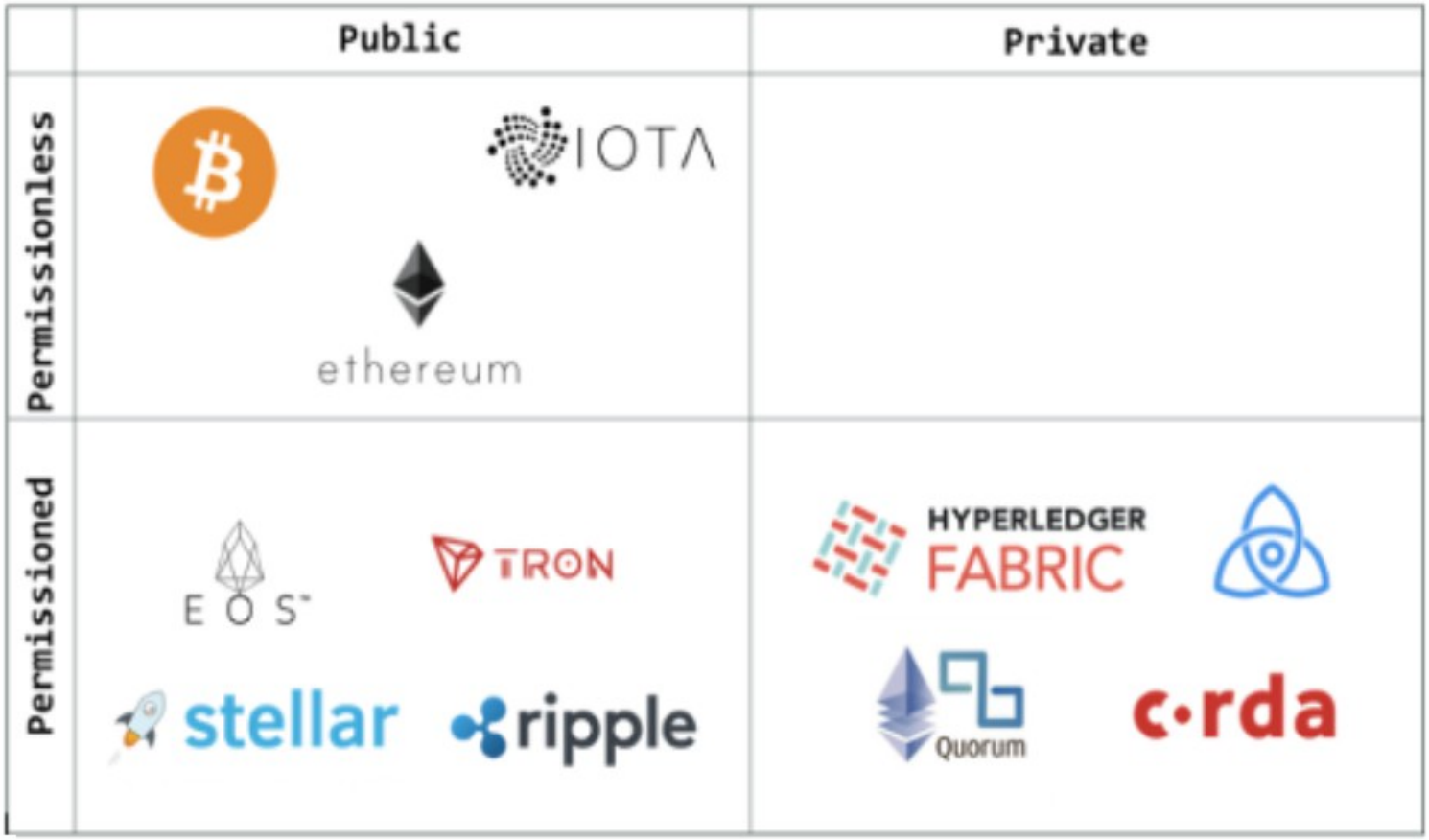
public permissionless

public permissioned

private permissioned

private permissionless

# ONE CONCEPT, DIFFERENT FLAVOURS



# BLOCKCHAIN: GOING DEEPER

- what is a ledger?
- consensus in a distributed environment
- tamper freeness
- proof of ownership
- permissioned and permissionless blockchains

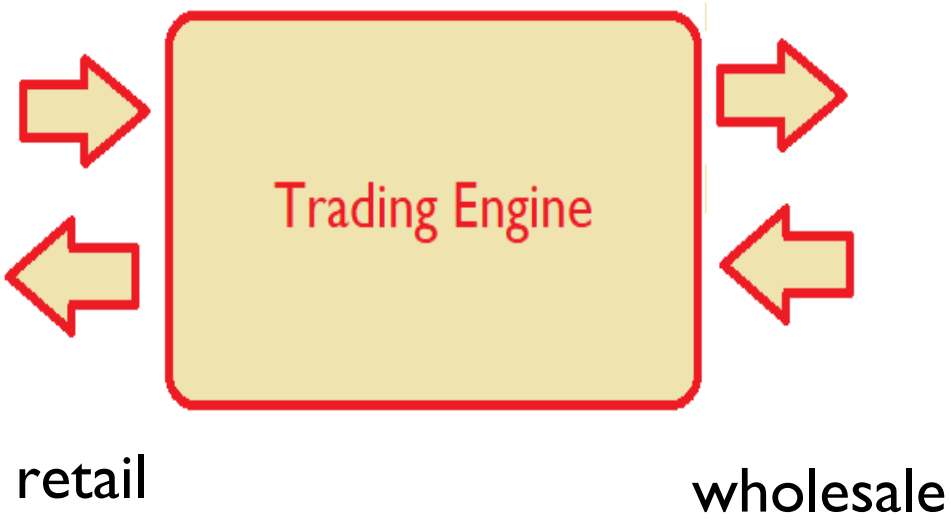
# FIRST ABSTRACTION: THE LEDGER

- a ledger
  - like a bullettin storing operations
  - maintains the order of operations
- which properties needed for a ledger?
  - append-only list of events
  - tamper-proof
    - auditability
  - everyone agrees on content
    - consensus
- not just finantial!
  - any application which needs a log of events

| Cash | | | | |
|---|---|---|---|---|
| Date | Description | Increase | Decrease | Balance |
| Jan. 1, 20X3 | Balance forward | | | $ 50,000 |
| Jan. 2, 20X3 | Collected receivable | $ 10,000 | | 60,000 |
| Jan. 3, 20X3 | Cash sale | 5,000 | | 65,000 |
| Jan. 5, 20X3 | Paid rent | | $ 7,000 | 58,000 |
| Jan. 7, 20X3 | Paid salary | | 3,000 | 55,000 |
| Jan. 8, 20X3 | Cash sale | 4,000 | | 59,000 |
| Jan. 8, 20X3 | Paid bills | | 2,000 | 57,000 |
| Jan. 10, 20X3 | Paid tax | | 1,000 | 56,000 |
| Jan. 12, 20X3 | Collected receivable | 7,000 | | 63,000 |

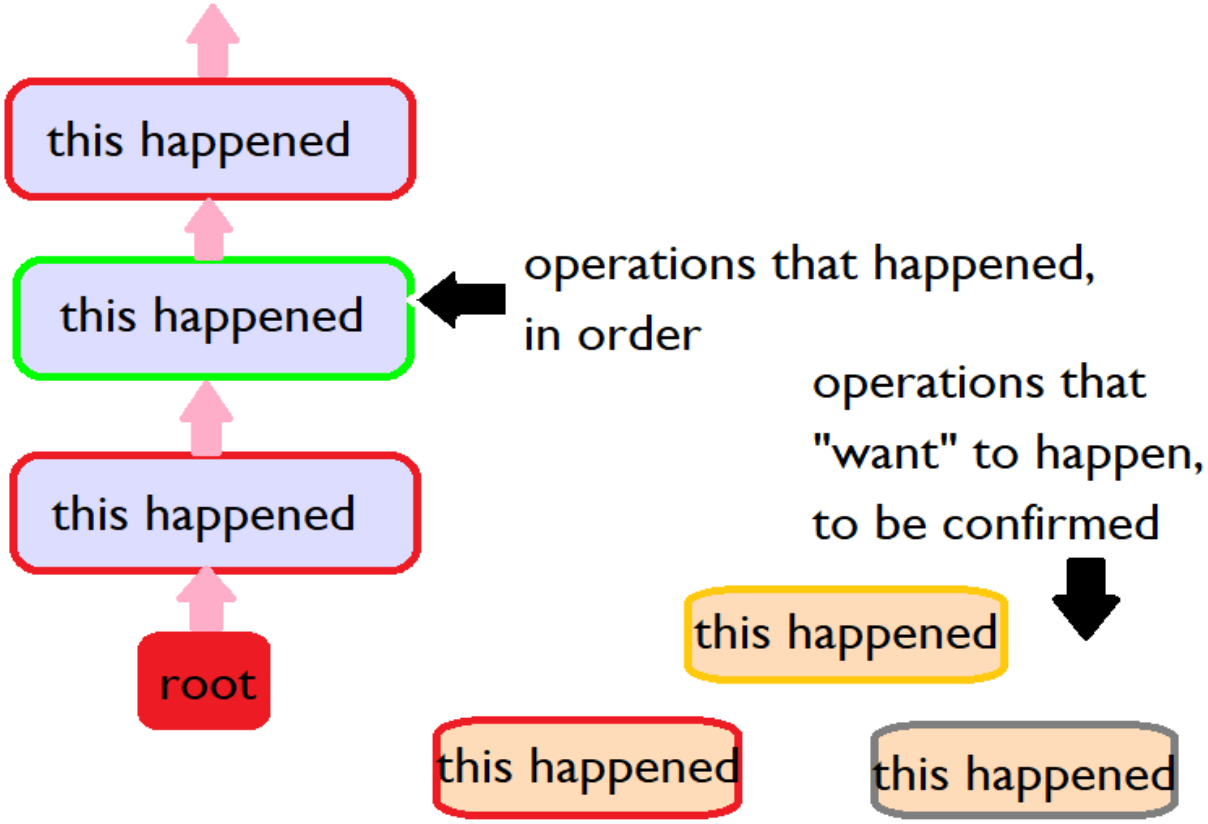
# FIRST ABSTRACTION: THE LEDGER

- Alice has a company
  - works as an intermediary between ratail and wholesale. Retail, wholesale and Alice do not trust each other and does not agree on a trusted third party
- needs a ledger to log the asset/values transfers
- several entities will access the ledger
  - wholesales sends good to Alice
  - Alice transfers good to ratails
  - the ledger registers all these operations

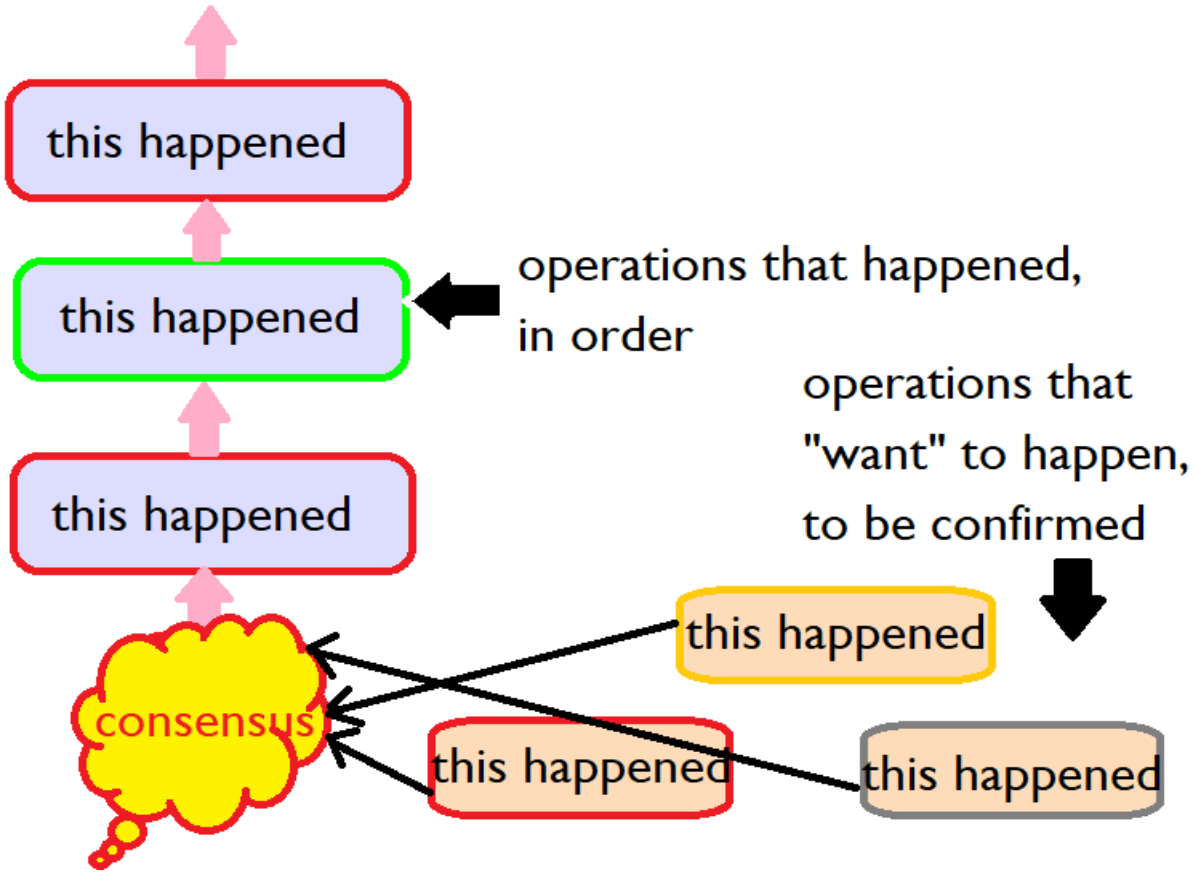


# LEDGER AS A BLOCKCHAIN

- if the ledger is organized as a list of blocks
  - call it a blockchain
  - but other structures are possibles! for instance, graphs
- we represent the ledger through a simplification: one operation for each block



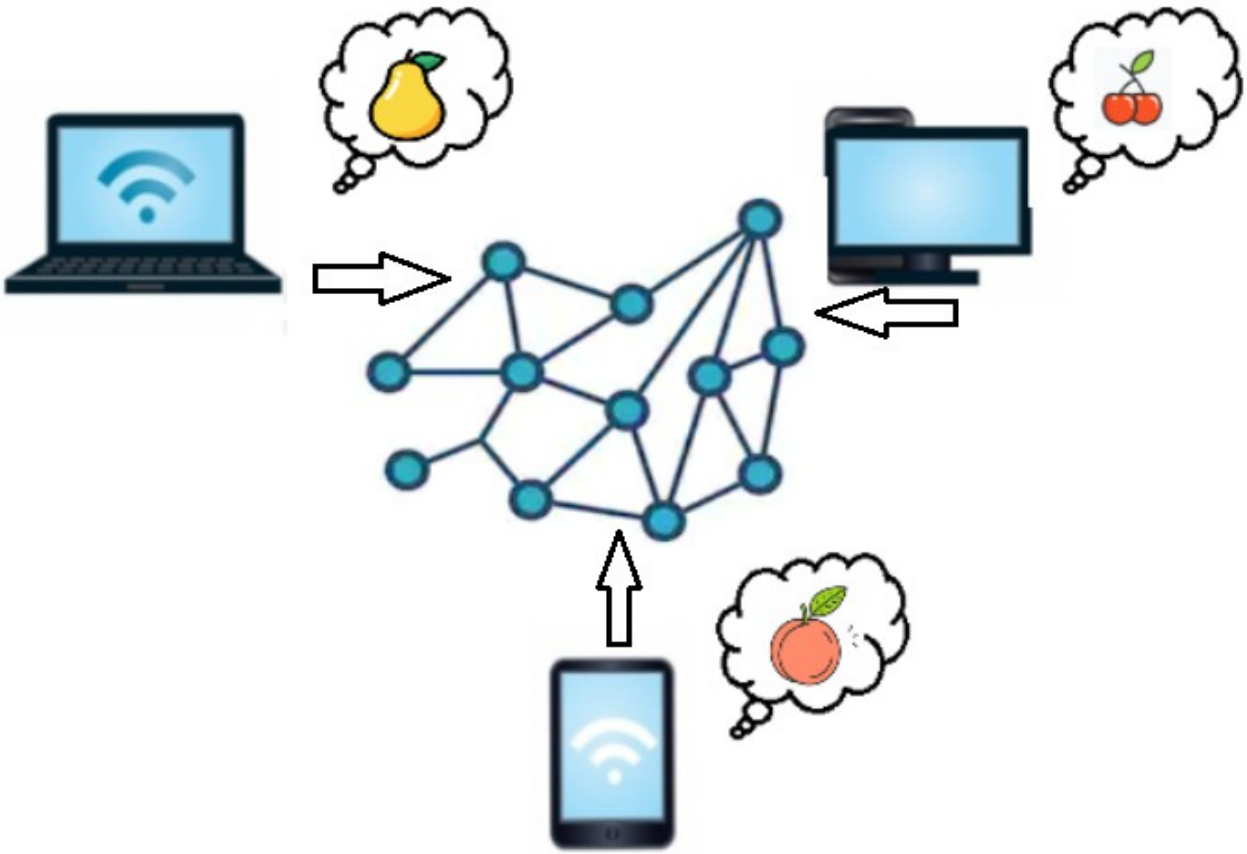
# ADDING ENTRIES TO THE LEDGER




consensus is the mechanism which defines

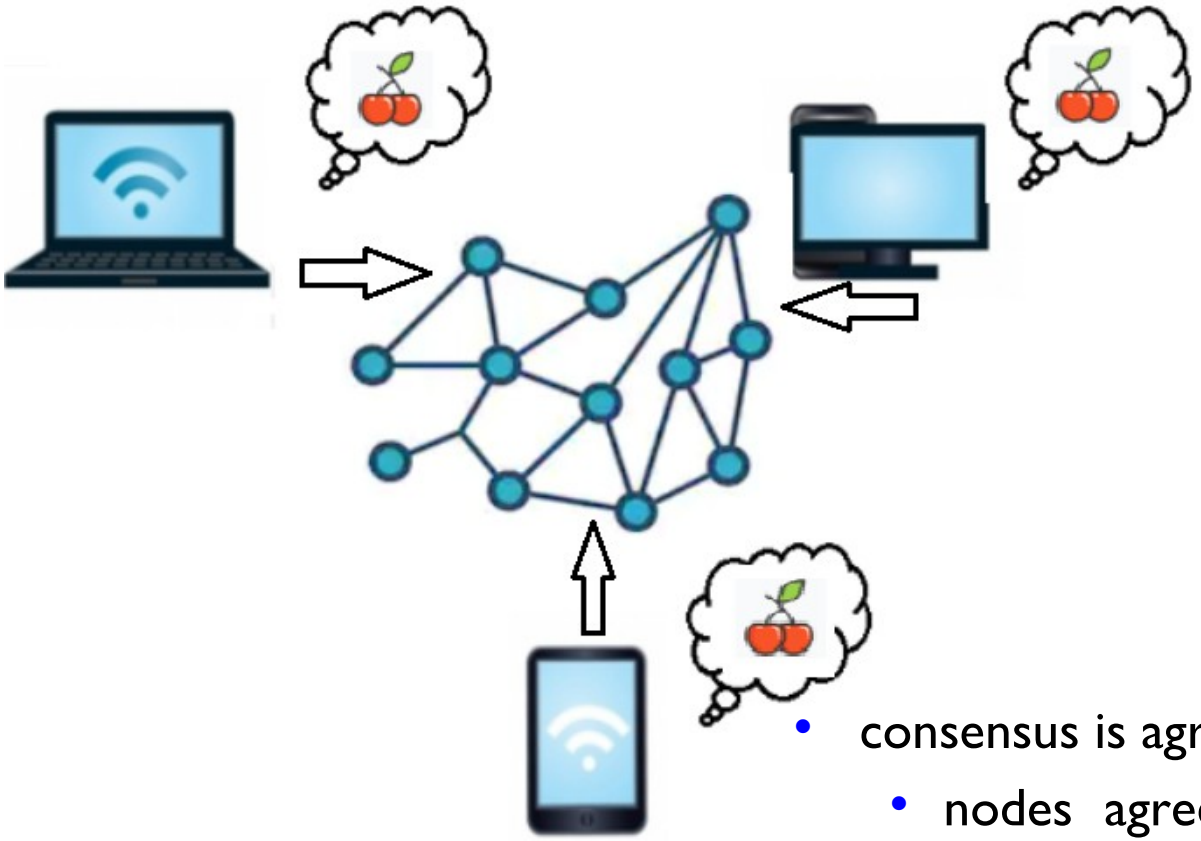
- who decides which operation will be added to the blockchain
- which operation among those to be confirmed, will be added

# WHAT IS CONSENSUS?



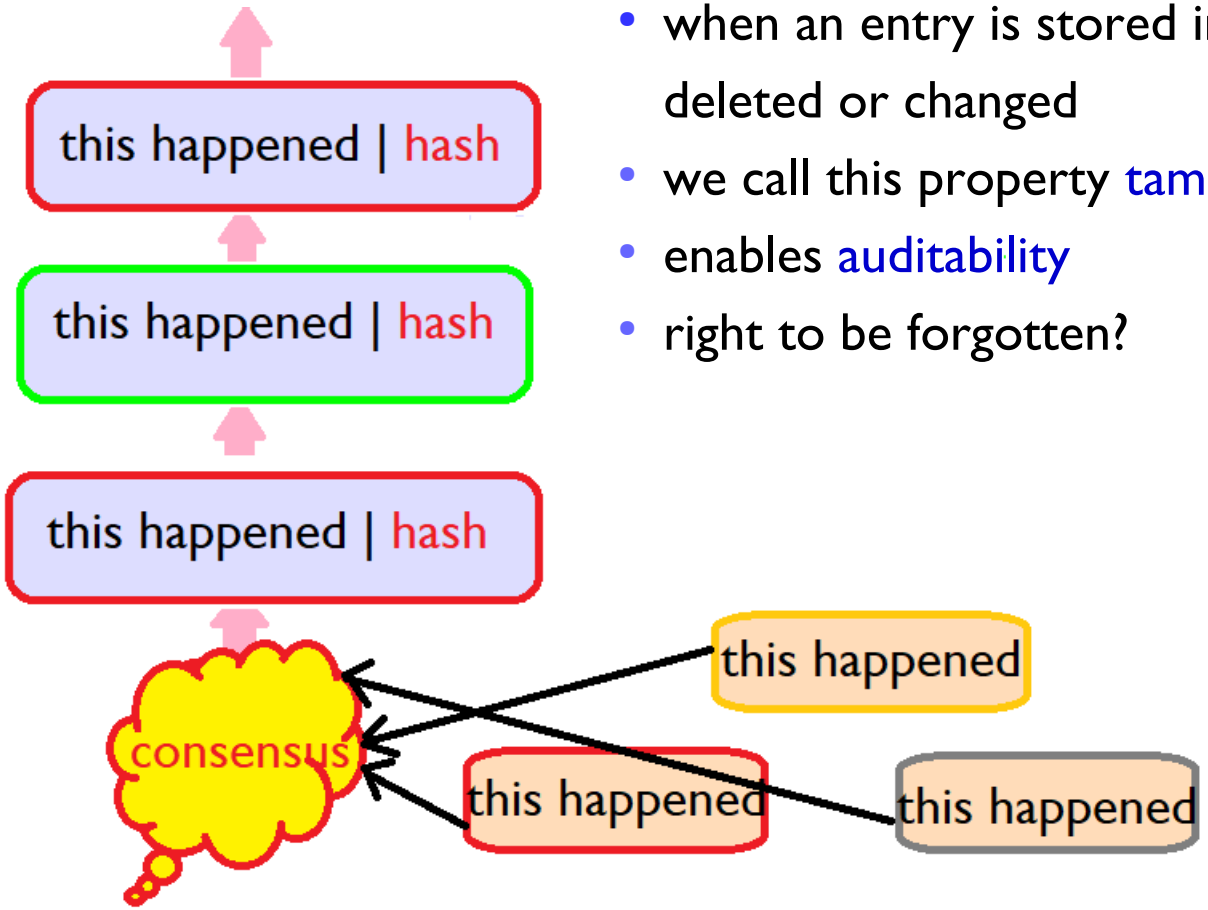
each node presents an item to add to the ledger

# WHAT IS CONSENSUS?



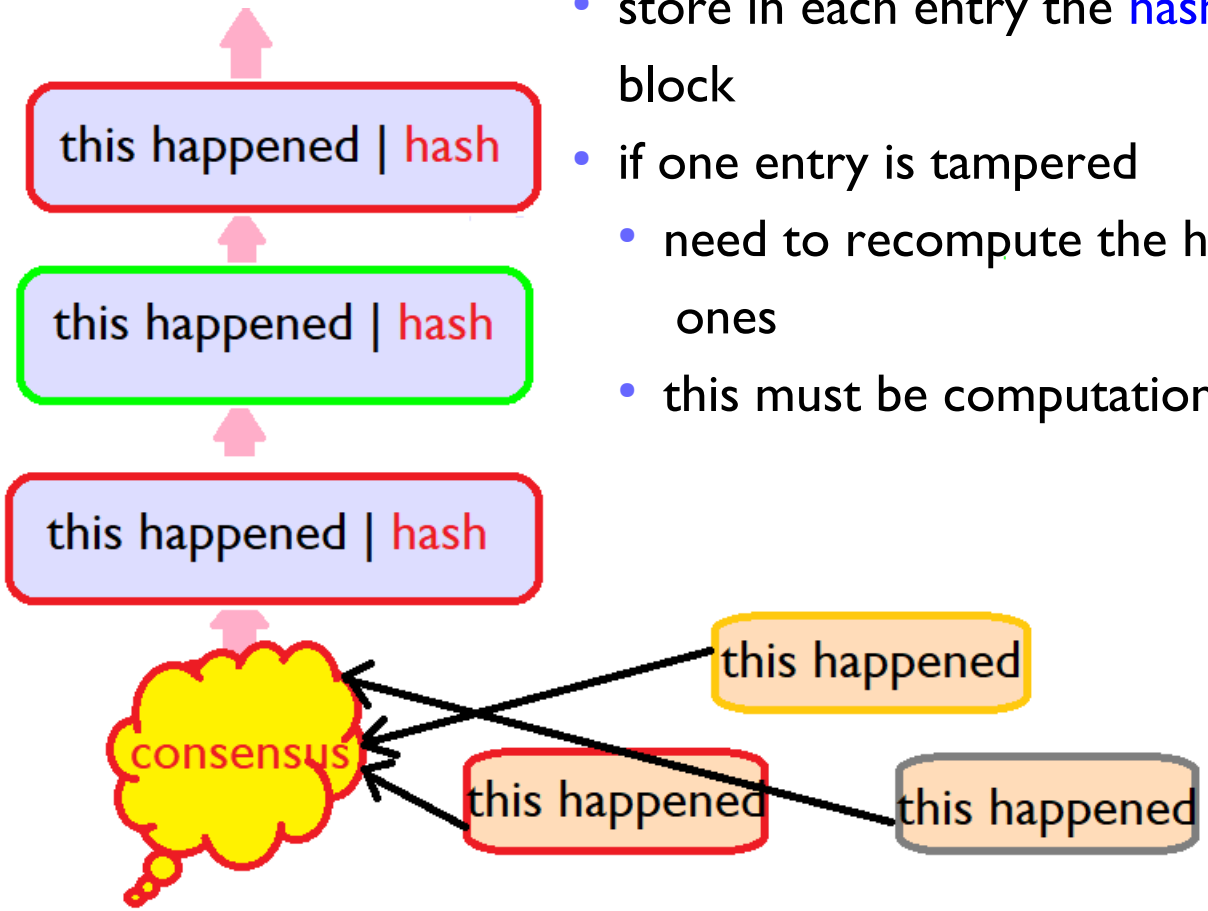
- consensus is agreement on the same value
  - nodes agree on one of the nodes's input
- validity: agree on someone's proposal
- hard because of faulty or malicious byzantine nodes

# TAMPER FREENESS



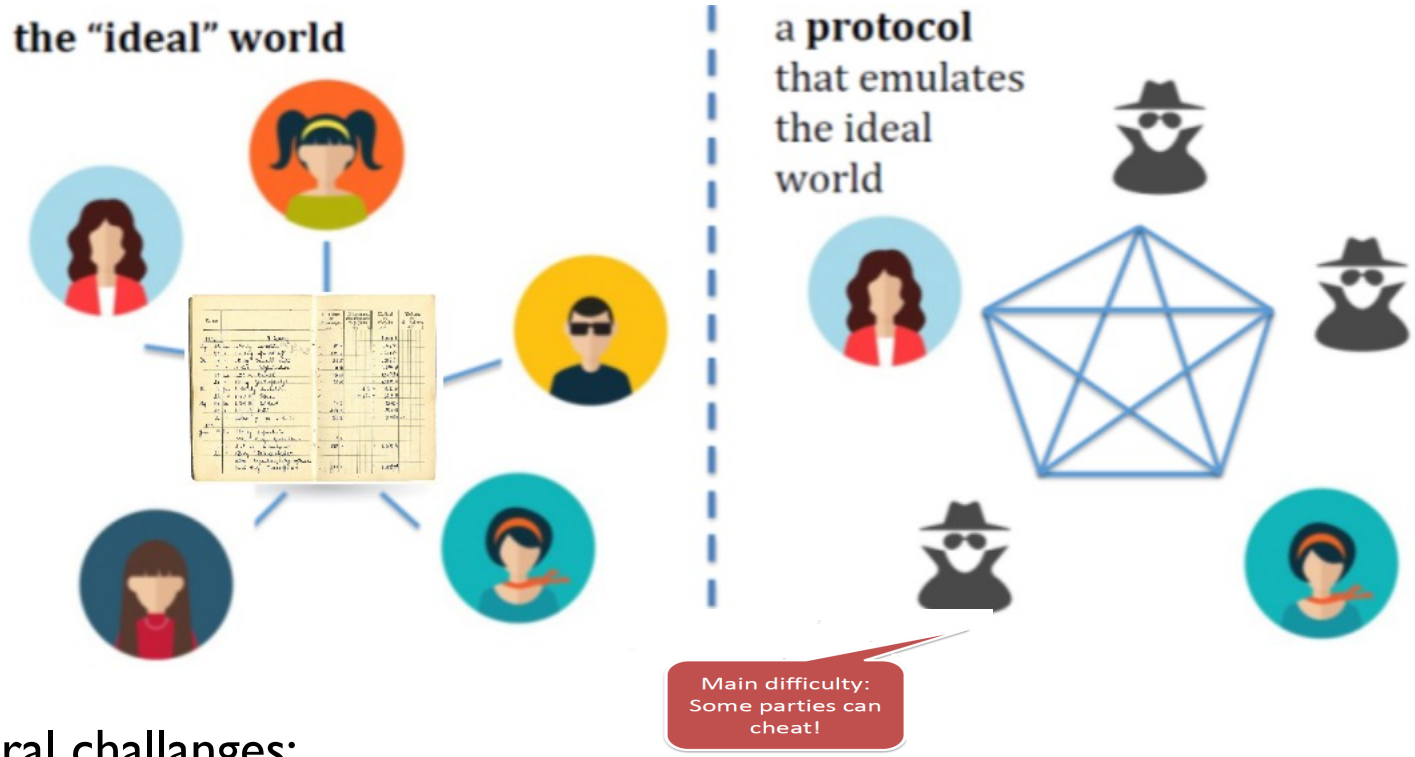

- ledger should be immutable
  - when an entry is stored in the ledger, it cannot deleted or changed
  - we call this property tamper freeness
  - enables auditability
  - right to be forgotten?

# TAMPER FREENESS: HOW TO




- compute the hash of each block
- store in each entry the hash of the predecessor block
- if one entry is tampered
  - need to recompute the hash of all the following ones
  - this must be computationally hard

# CONSENSUS IN A DISTRIBUTED NETWORK




- several challanges:
  - maintain consistency in presence of different network jitter, delay,...
  - the main challange is that some parties can cheat: byzantine parties
- classical results: if the honest nodes are over a threashold the system works well:
  - majority, 2/3 of the nodes,....

# CONSENSUS IN A DISTRIBUTED NETWORK

- assume honest majority: nodes which follow correctly the protocol
- but...which notion of majority?
- first possibility: implement majority by voting
  - broadcast every operation on the network and then collect votes


| Transaction id | Value |
|---|---|
| ddbs21239864k... | 0.084 BTC |
| edd98763hn3nr... | 1.2 BTC |
| mkk8765g4g2j3... | 0.036 BTC |

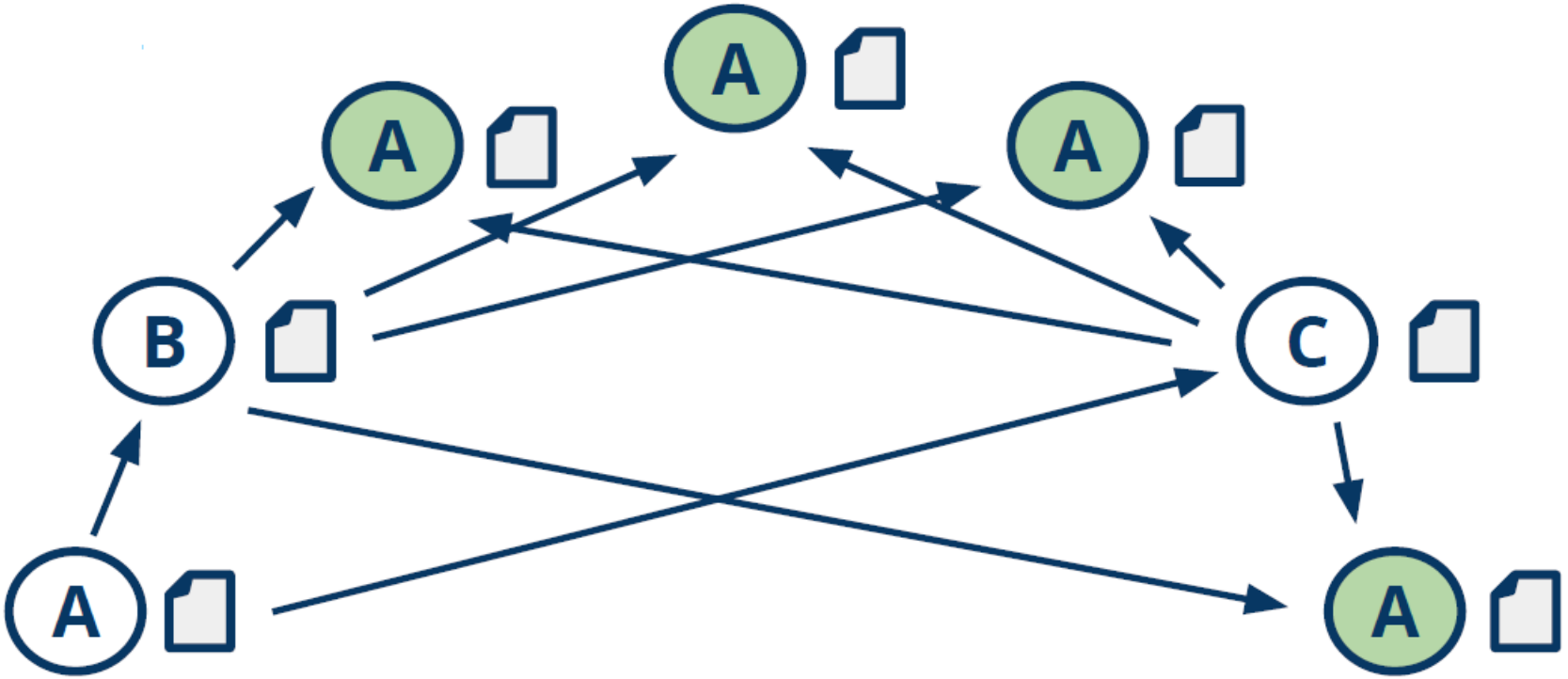
- how to implement voting?
- different assumptions if we consider permissionless versus permissioned vlockchains

# MAJORITY AND SYBILS

- in a permissionless blockchain an attacker can easily control the network by assuming a lot of identities and voting more times

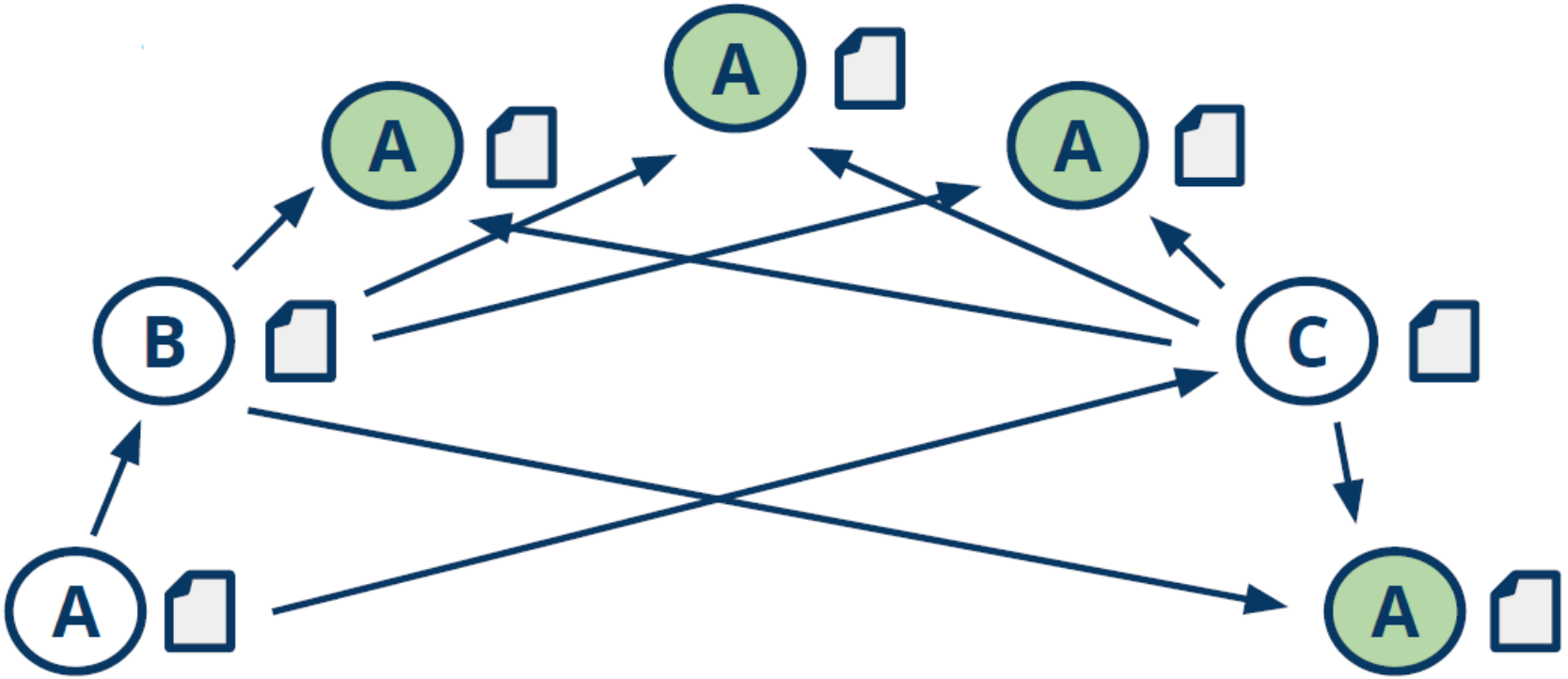
- I am the Delphic Sybil !
- I like voting a lot!

# DOUBLE SPENDING AND SYBILS




- Alice
  - double spends the same bitcoin with B and C: easy bitcoin is just a sequence of bits....
  - performs a Sybil attack
    - assume more identities: easy in permissionless blockchain

# DOUBLE SPENDING AND SYBILS

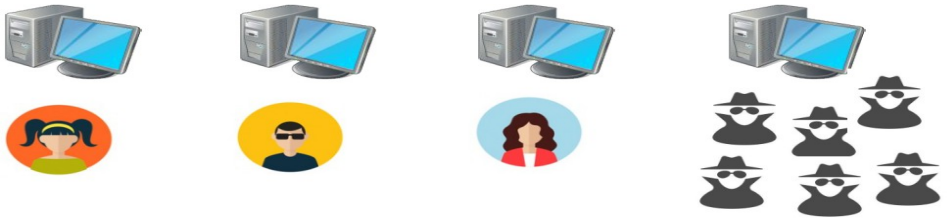



- store transaction in a ledger: each operation approved through consensus
- Alice will approve with her multiple identities the double spending of herself with Bob and Charlie
- the attack is succesfull

# HOW TO AVOID A SYBIL ATTACK?

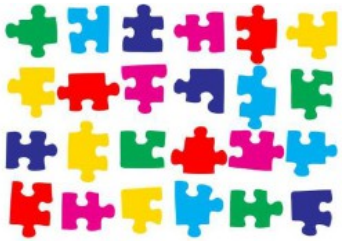
- how to define majority in a context where everybody can easily join the network and assume multiple identities?
  - easy to control the majority of the network by creating multiple accounts
  - cannot simply count the number of votes....

- Bitcoin change the perspective with the Proof of Work
  - a distributed lottery
  - you can control the newtork only if you control the majority of the computational power (difficult and pricey)

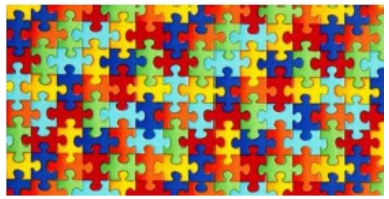


# PROOF OF WORK

- a voting scheme that is hard to fake!
- proof of Work
  - Solution of a cryptographic puzzle
  - requires a lot of computation to fake



Hard to find solution



Easy to verify

- like a lottery
  - winner of the lottery decides which is the next node of the blockchain
  - tickets of the lottery are very expensive
    - need to solve the cryptographic puzzle
  - winner of the lottery is paied when later winners endorses validity
- give incentives for well behaviour
- Sybil attacks expensive and pointless

# IS IT ALL? NEED ALSO PROOF OF OWNERSHIP

Alice now decides to change work and opens a restaurant

- rental is high, venture capitalists are greedy
- Alice uses an ICO (Initial Coin Offering)
  - proposes a project that will be implemented on a blockchain
  - get fundings from people proposing to partecipate to the project
  - create tokens to be given to the funders, as a compensation
  - cryptocopupons
    - discount meals when the restaurant opens

# PROOF OF OWNERSHIP

- Alice  register token transfers on a ledger
- needs  a solution to guarantee ownership of coupons
  - how Alice can prove that she owns a coupon?
  - how a funder that is going to spend a coupon can prove that he/she has received it from Alice and he/she ows it?
- no certification authority, i.e. no centralized entity certifying the identities
- a completely decentralized solution using asymmetric key cryptography

# PROOF OF OWNERSHIP

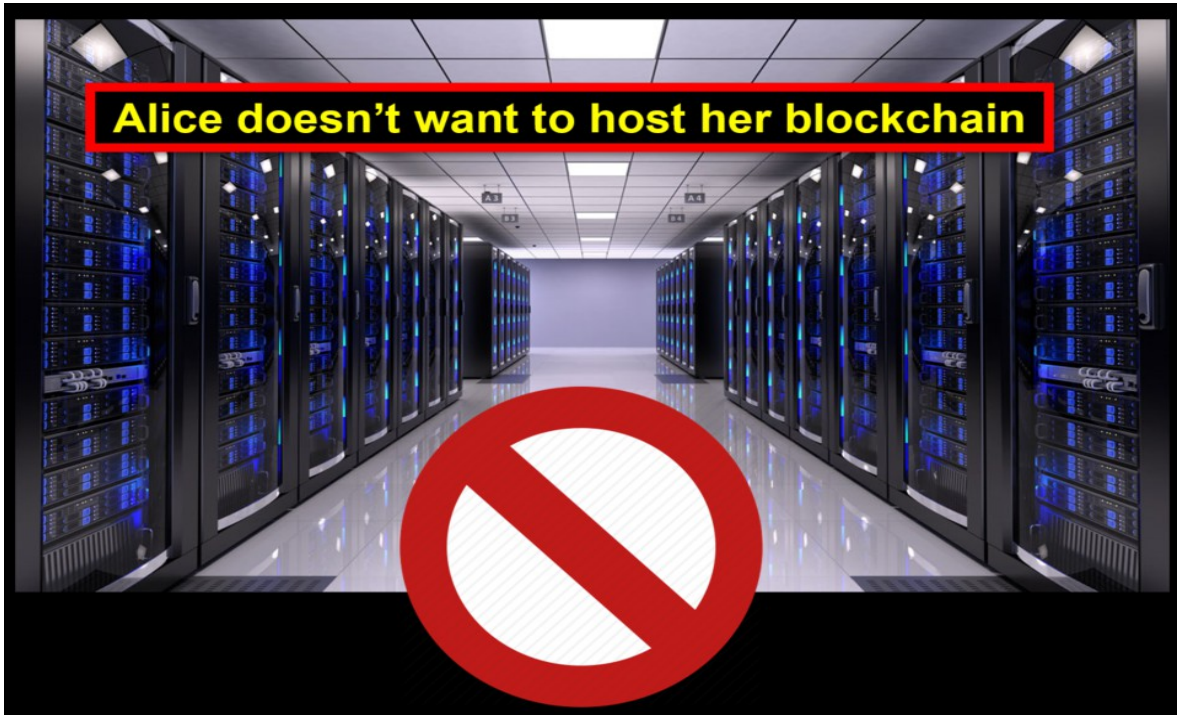
- Alice generates a pair (public key, private key)
- anyone who knows the private key matching the public key of Alice, for instance af876f536....., owns the Alice cryptocoupons
  - Alice themself
  - everyone Alice gives the private key to
  - everyone who steal Alice's private key
- private key gives ownership
  - possibility to sign the transfer operation
- public key gives the proof of ownership
  - prove that the emitter of the transfer is really the owner of the coupon
- register on the ledger the signed transactions
  - can be verified by the receiver

# SPENDING COUPONS

- Alice decides to transfer 50% ownership of coupon to each one of two different founders
- has a private key matching the public key af876f536.....
  - identifies the public key of the users she wants to transfer the coupon to
    - 1FE1W2EEJE....
    - A5d65ab38.....
  - signs the transfer to prove she knows the private key and is therefore authorized to do the transfer
  - transfer the 50% ownership
    - to each one of two owners of the private key
    - which corresponds to the previous public keys
- the two founder exploit their private key to collect and use half of the coupon

# WHO STORES THE BLOCKCHAIN?

- Alice does not want to host her blockchain
  - expensive
  - customer may not trust her



# CROWDSOURCE BLOCKCHAIN MANAGEMENT

- use a peer to peer network between all the users and Alice
- the blockchain is replicated by each node
- someone has to enforce operations validity, voting for the next operations to add to the blockchain: these are the miners
  - partecipate to the lottery
  - solve the proof of work
- but why I should be a miner, since a need computing power and this costs a lot?
  - a rewarding system to reward miners
  - may be Alice offer extra coupons to the miners to maintain the network
  - the system itself may reward the miners, like Bitcoin

# A PERMISSIONED BLOCKCHAIN

- Alice sells her restaurant and opens a frozen yogurt business
- but her business is in trouble
  - shipments arrive melted
  - where is the problem?

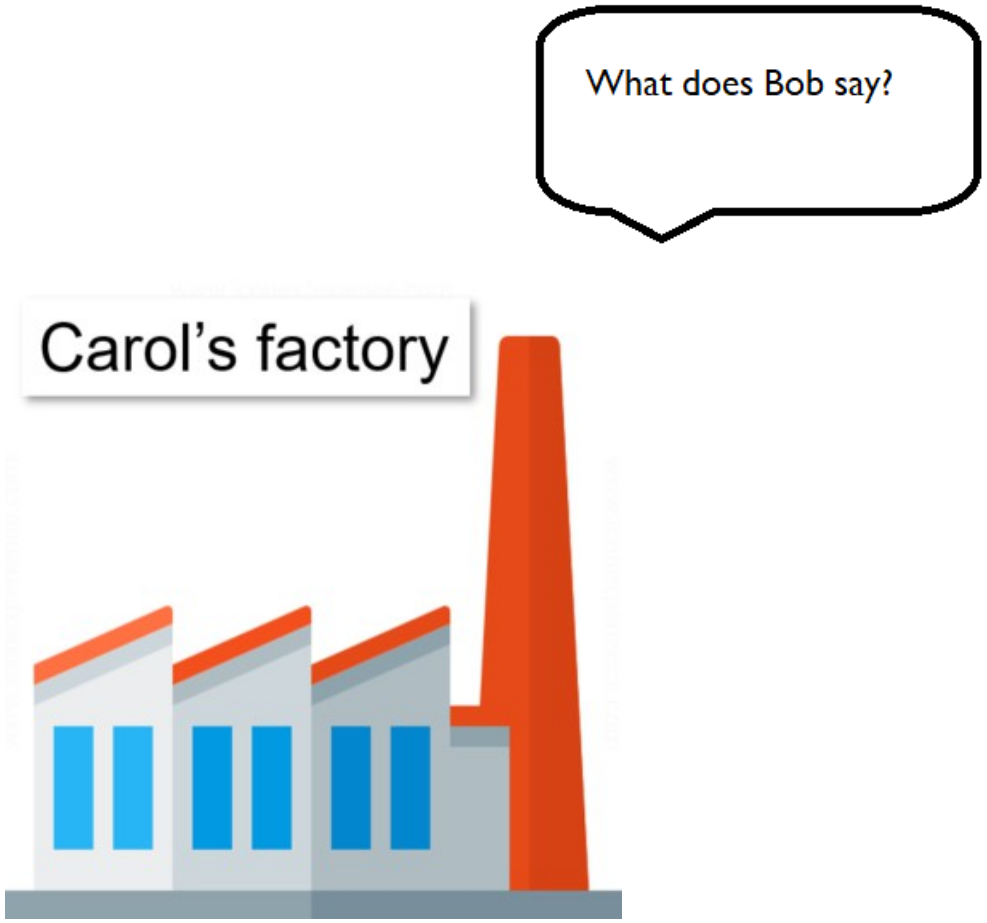
# ALICE SUPPLY CHAIN


# ALICE SUPPLY CHAIN

1. I never trasported that yougurt
2. It was meletd when I got it from Carol
3. It was OK when I delivered it to Alice


Bob's truck

# ALICE SUPPLY CHAIN



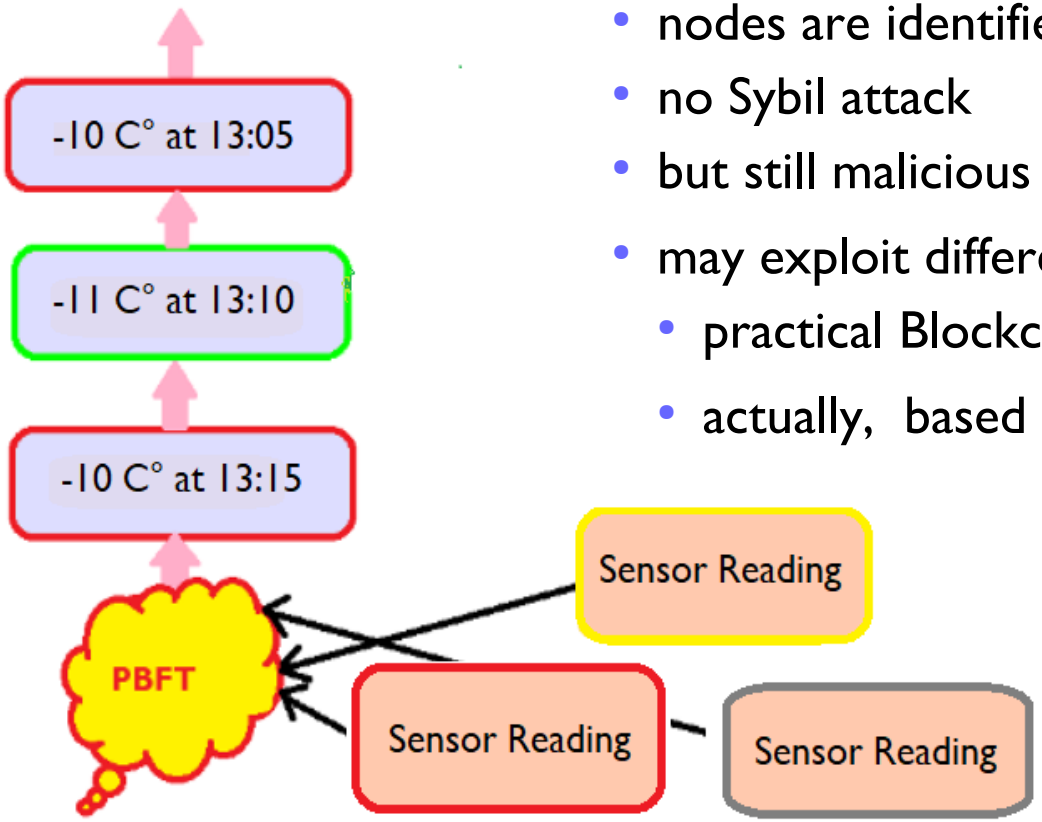
# USE A PERMISSIONED BLOCKCHAIN!

- a distributed ledger to record the events
- put the ledger in the cloud

Bob and Carol

Sensors

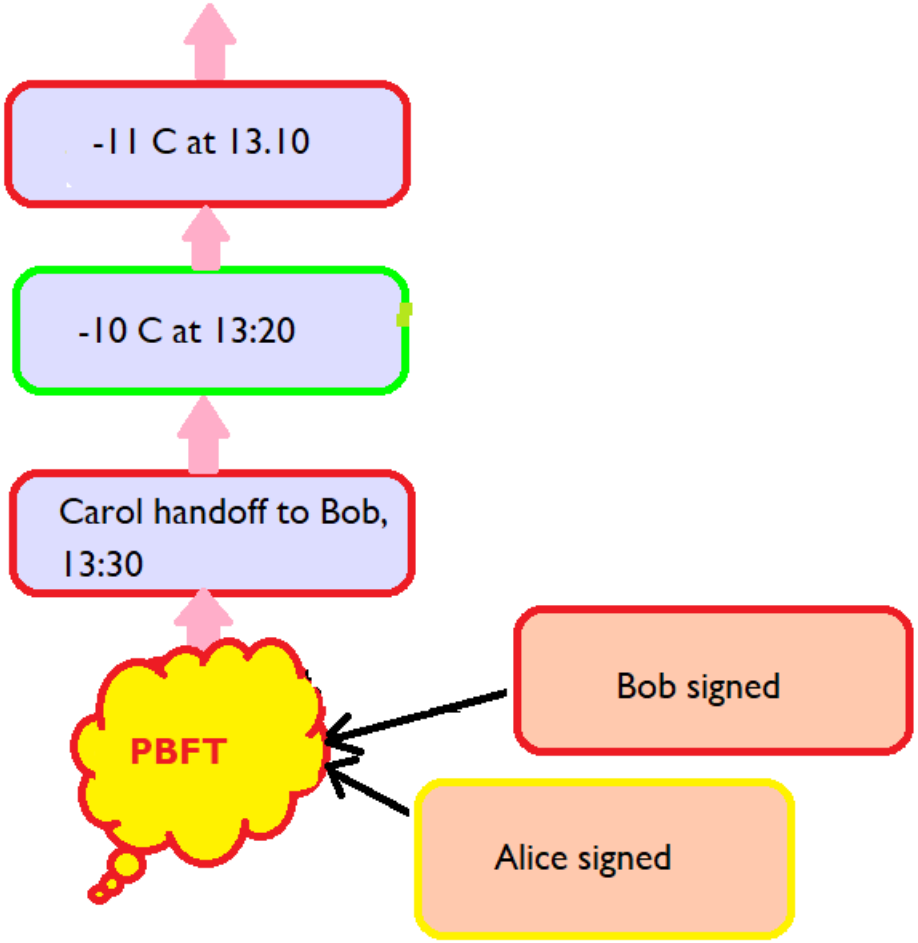
# PERMISSIONED BLOCKCHAIN FOR SUPPLY CHAIN




The scenario is different

- nodes are identified (Alice, Carol, Bob...)
- no Sybil attack
- but still malicious nodes (sw error, ...)
- may exploit different consensus algoritms
  - practical Blockchain Fault Tolerance (PBFT)
  - actually, based on voting

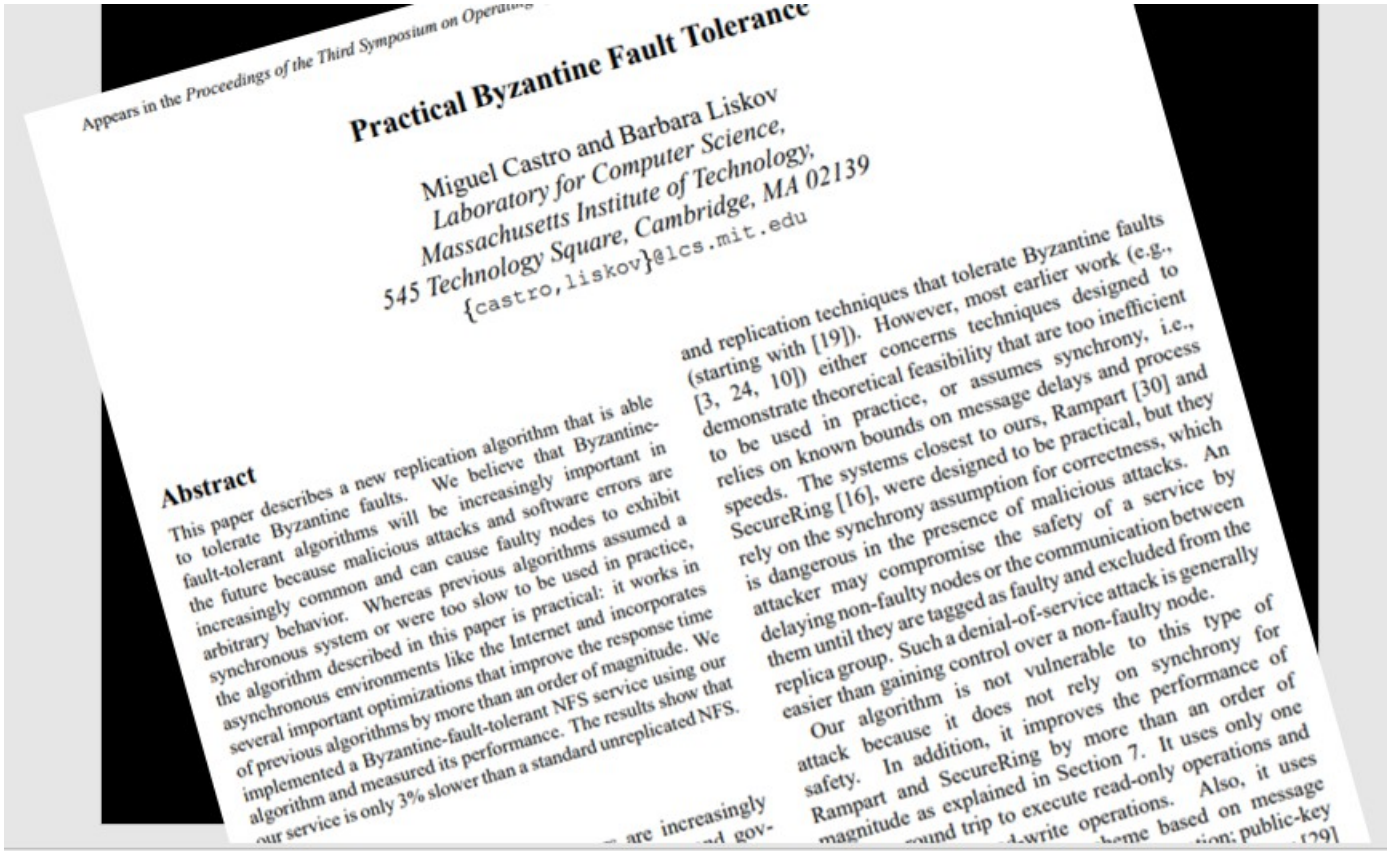
# PERMISSIONED BLOCKCHAIN FOR SUPPLY CHAIN



# PERMISSIONED BLOCKCHAIN: WHAT IS DIFFERENT?

- parties have identities
- humans have passwords, keys
- sensors have keys
  - both humans and sensors are authenticated
- no Sybil attack
- different consensus mechanisms
- accountability if caught cheating

# BYZANTINE FAULT TOLERANCE



Appears in the *Proceedings of the Third Symposium on Operating*

**Practical Byzantine Fault Tolerance**

Miguel Castro and Barbara Liskov
*Laboratory for Computer Science,*
*Massachusetts Institute of Technology,*
*545 Technology Square, Cambridge, MA 02139*
{castro,liskov}@lcs.mit.edu

**Abstract**

This paper describes a new replication algorithm that is able to tolerate Byzantine faults. We believe that Byzantine-fault-tolerant algorithms will be increasingly important in the future because malicious attacks and software errors are increasingly common and can cause faulty nodes to exhibit arbitrary behavior. Whereas previous algorithms assumed a synchronous system or were too slow to be used in practice, the algorithm described in this paper is practical: it works in asynchronous environments like the Internet and incorporates several important optimizations that improve the response time of previous algorithms by more than an order of magnitude. We implemented a Byzantine-fault-tolerant NFS service using our algorithm and measured its performance. The results show that our service is only 3% slower than a standard unreplicated NFS.

and replication techniques that tolerate Byzantine faults (starting with [19]). However, most earlier work (e.g., [3, 24, 10]) either concerns techniques designed to demonstrate theoretical feasibility that are too inefficient to be used in practice, or assumes synchrony, i.e., relies on known bounds on message delays and process speeds. The systems closest to ours, Rampart [30] and SecureRing [16], were designed to be practical, but they rely on the synchrony assumption for correctness, which is dangerous in the presence of malicious attacks. An attacker may compromise the safety of a service by delaying non-faulty nodes or the communication between them until they are tagged as faulty and excluded from the replica group. Such a denial-of-service attack is generally easier than gaining control over a non-faulty node.

Our algorithm is not vulnerable to this type of attack because it does not rely on synchrony for safety. In addition, it improves the performance of Rampart and SecureRing by more than an order of magnitude as explained in Section 7. It uses only one round trip to execute read-only operations and


50+ BLOCKCHAIN
REAL WORLD USES CASES
GOVERNMENT
Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government
essentia.one
IDENTIFICATION
Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by Uport.
uport
MOBILE PAYMENTS
The blockchain ledger that Ripple uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.
ripple
INSURANCE
A smart contract-based blockchain is being used by Insurer American International Group Inc as a means of saving costs and increasing transparency.
AIG
ENDANGERED SPECIES PROTECTION
The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.
CARBON OFFSETS
IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.
IBM
HYPERLEDGER
ENTERPRISE
Ethereum's blockchain can be accessed as a cloud-based service courtesy of Microsoft Azure.
Microsoft Azure
BORDER CONTROL
Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.
essentia.one
SUPPLY CHAINS
IBM and Walmart have partnered in China to create a blockchain project that will monitor food safety.
IBM
Walmart
HEALTHCARE
A number of healthcare systems that store data on the blockchain have been pioneered including MedRec.
MEDREC
SHIPPING
Shipping is a natural fit for blockchain, and Maersk have been trialling a blockchainbased project within the maritime logistics industry.
MÆRSK
REAL ESTATE
Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by Propy.
PROPY
ENERGY
Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.
essentia.one
LAND REGISTRY
Land registry titles are now being stored on the blockchain in Georgia in a project developed by the National Agency of Public Registry.
NATIONAL AGENCY OF PUBLIC REGISTRY
COMPUTATION
Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.
DIGITAL CURRENCY GROUP
ADVERTISING
New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.
NYIAX
BORDER CONTROL
Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.
essentia.one
JOURNALISM
Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as Civil has shown.
CIVIL
WASTE MANAGEMENT
Waltonchain is using RFID technology to store waste management data on the blockchain in China.
ENERGY
Food importation is another industry where blockchain is proving its worth, with Louis Dreyfus Co trialling a soybean importation operation using this technology.
LDC.
DIAMONDS
The De Beers Group is using blockchain to track the importation and sale of diamonds.
DE BEERS
FINE ART
By storing certificates of authenticity on the blockchain, it's possible to dramatically reduce art forgeries, as one blockchain project is proving.
NATIONAL SECURITY
For the past two years, the US Department of Homeland Security has been using blockchain to record and safely store data captured from its security cameras.
TOURISM
In a bid to boost its tourism economy, Hawaii is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.
TAXATION
In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by Miaocai Network.
ENERGY
Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.
CNE
COMISIÓN NACIONAL DE ENERGÍA
RAILWAYS
Russian rail operator Novotrans is storing inventory data on a blockchain pertaining to repair requests and rolling stock
HOBOTPAHC
ENTERPRISE
Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by Alphabet Inc
Google
Alphabet
MUSIC
Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.
arbit
FISHING
Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.

# BLOCKCHAIN APPLICATIONS: CURRENCY

Alternative to fiat currencies:

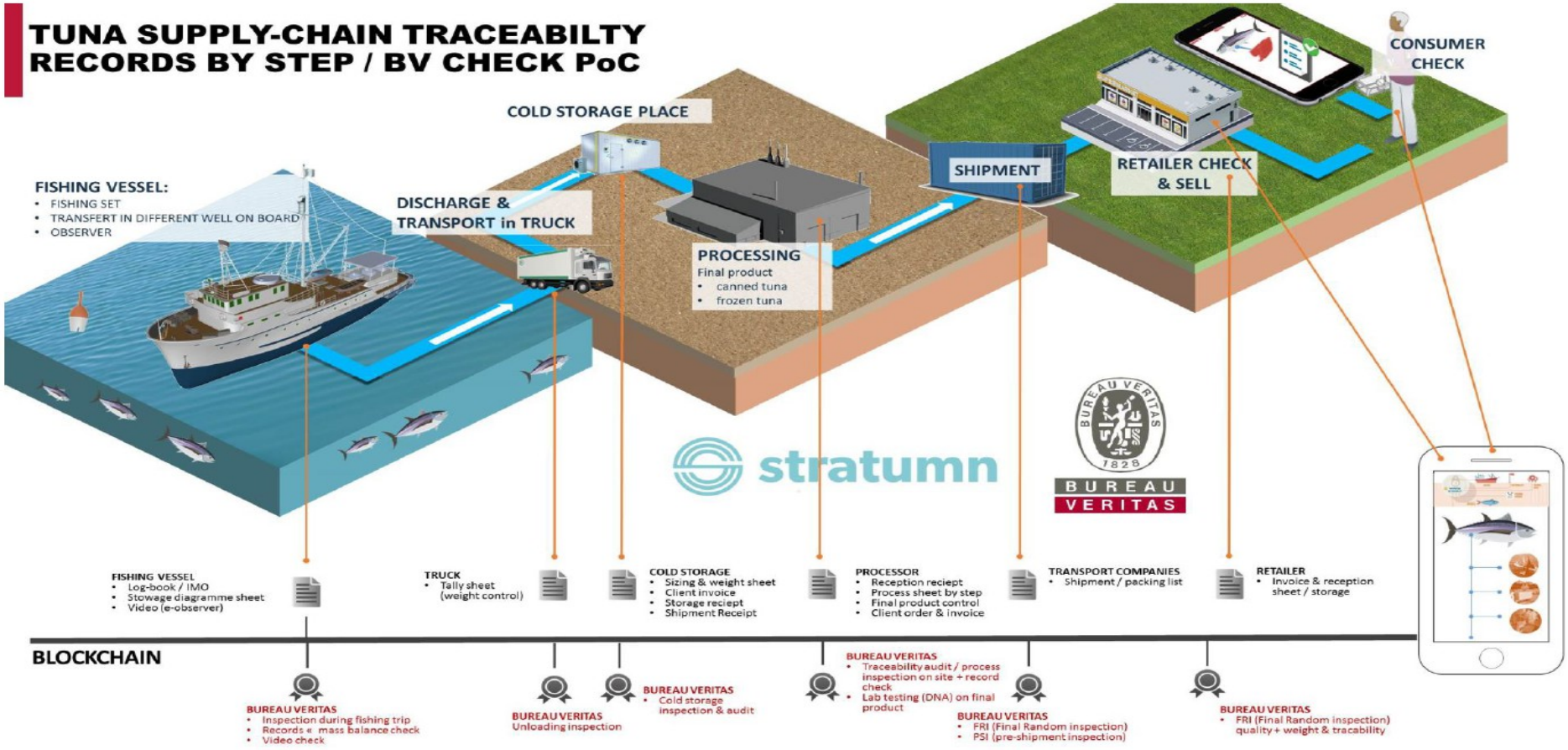
- breaks status-quo where:
  - only government issues money, defines issuing procedures
  - central authorities (banks) decide which transactions are valid and which are not
- fiat currencies decouple supply from a physical good (i.e. gold)
- block-chain typically ties supply to a bounded, virtual good
  - cryptographic bounded
- blockchain records and verifies transfers
- blockchain solves the problem of double spending

# PROVENANCE AND SUPPLY CHAIN: WALLMART

- devoped using Hyperledger technology
- a collaboration between Walmart and IBM
- track farm origin, expiration dates, storage temperature shipping details, parameters taken from sensors,....

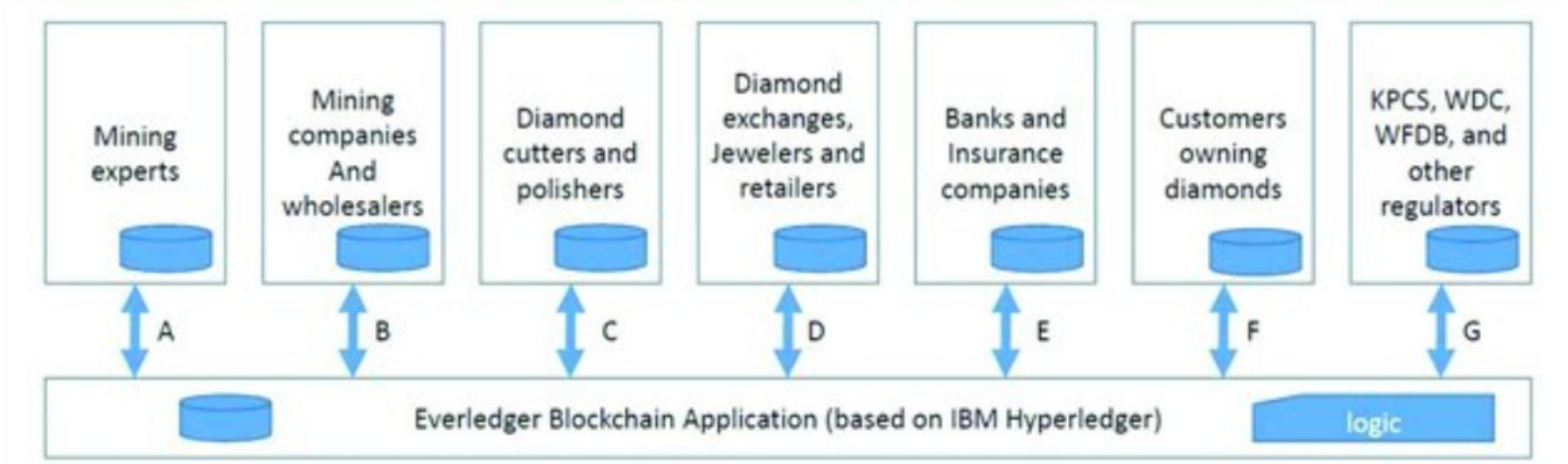
# PROVENANCE AND SUPPLY CHAIN: FISHING

- restaurants can view and verify chain of custody for fish
- sensors attached to fish can log location/temperature/humidity
  https://youtu.be/Buw3g8oNG74



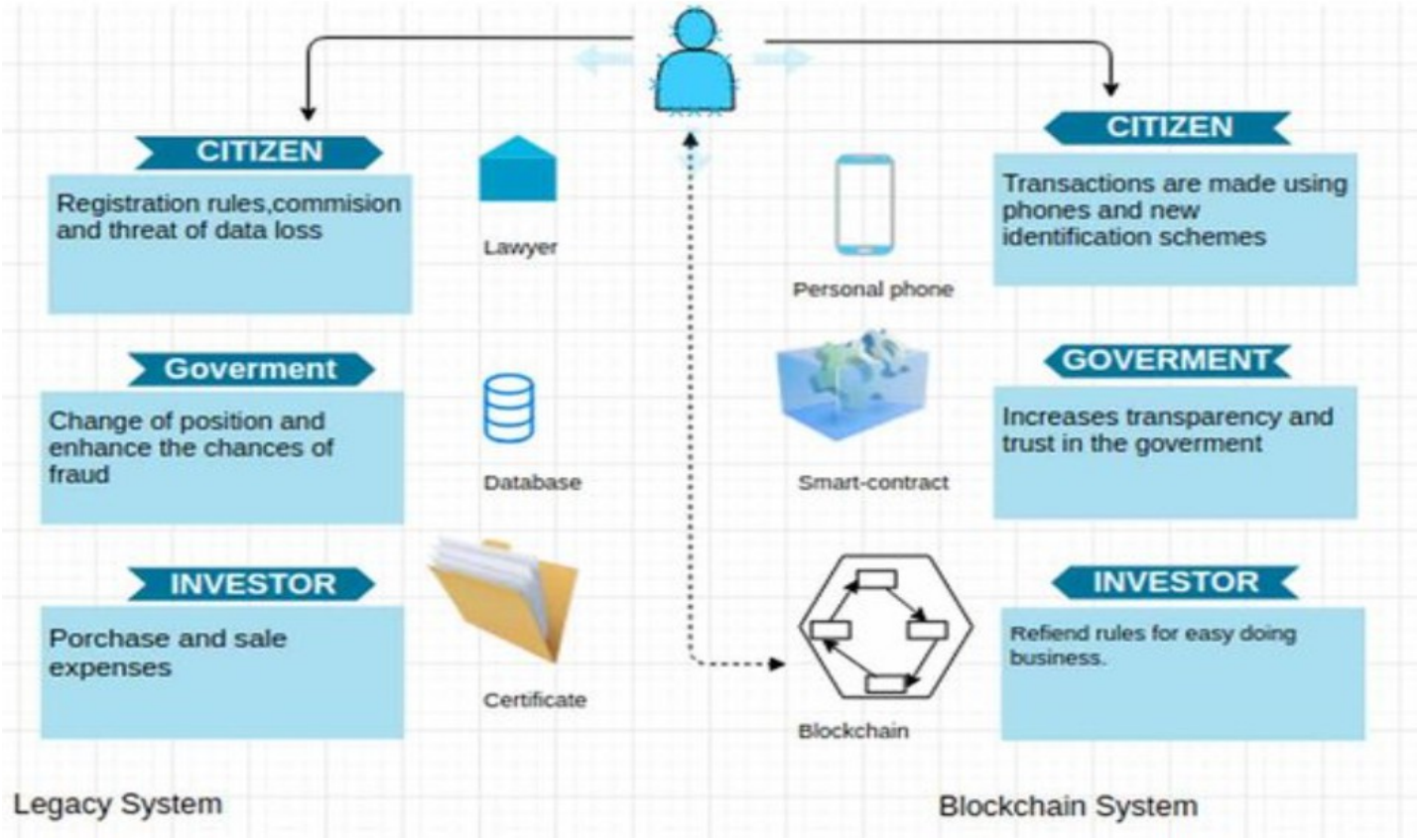
# PROVENANCE AND SUPPLY CHAIN: DIAMONDS

- auditing to track provenance and chain of custody for materials and products
- conflict diamonds (e.g. blood diamonds)
- a distributed ledger where all the transaction refarding a dimond are recorded.



# BLOCK CHAIN FOR LAND REGISTRY

- Land registry titles registered on the blockchain
- A project in Georgia by National Agency of Public Registry

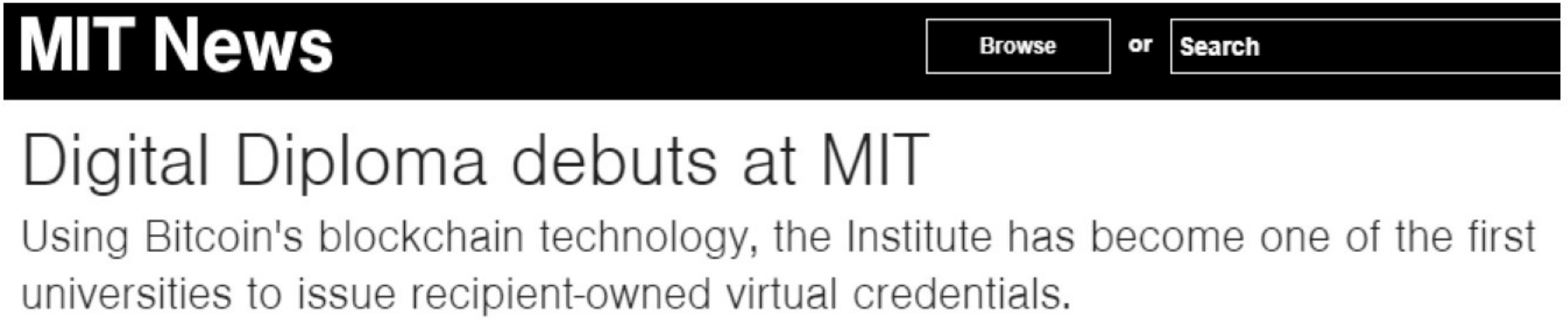


# INTELLECTUAL PROPERTY

- Digital content owner hashes content together with their identity and commits to the blockchain.
  - if nobody else can prove they published it prior to that commitment, this is evidence that they own it.
  - more convenient than a patent office and allows for you to not have to disclose details of the digital object.

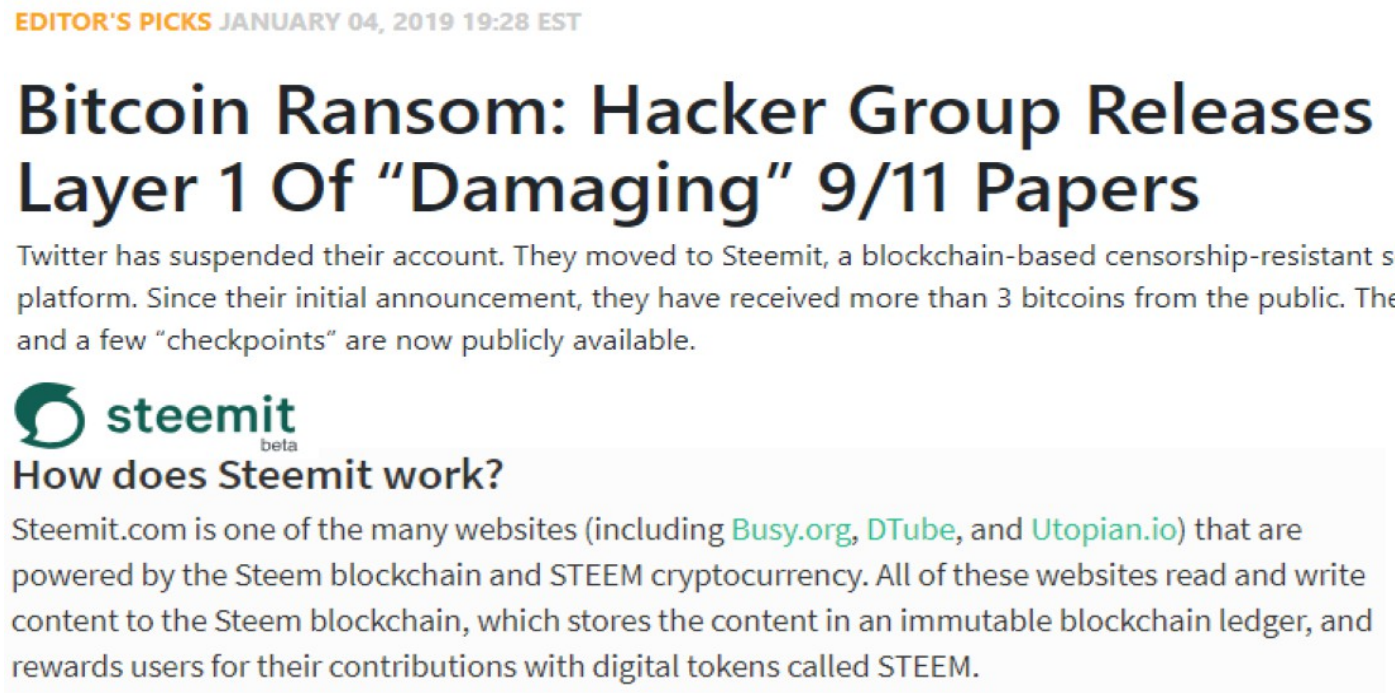
# CERTIFICATES

- Recording certifications, licenses, degrees (e.g. AWS certs)
  - University of Pisa joined a blockchain project with other EU Universities for recording certificates on a blockchain



# CENSORSHIP RESISTANCE

- Bitcoin ransom (2019)
  - group attempting to get paid to release damaging papers on 9/11 attacks
  - payment mileposts in BTC determine which documents are released
  - banned from mainstream social media platforms
  - messaging via Steemit to prevent censorship. Bunned by Steemit, but track remains on Steem blockchain



EDITOR'S PICKS JANUARY 04, 2019 19:28 EST

## Bitcoin Ransom: Hacker Group Releases Layer 1 Of "Damaging" 9/11 Papers

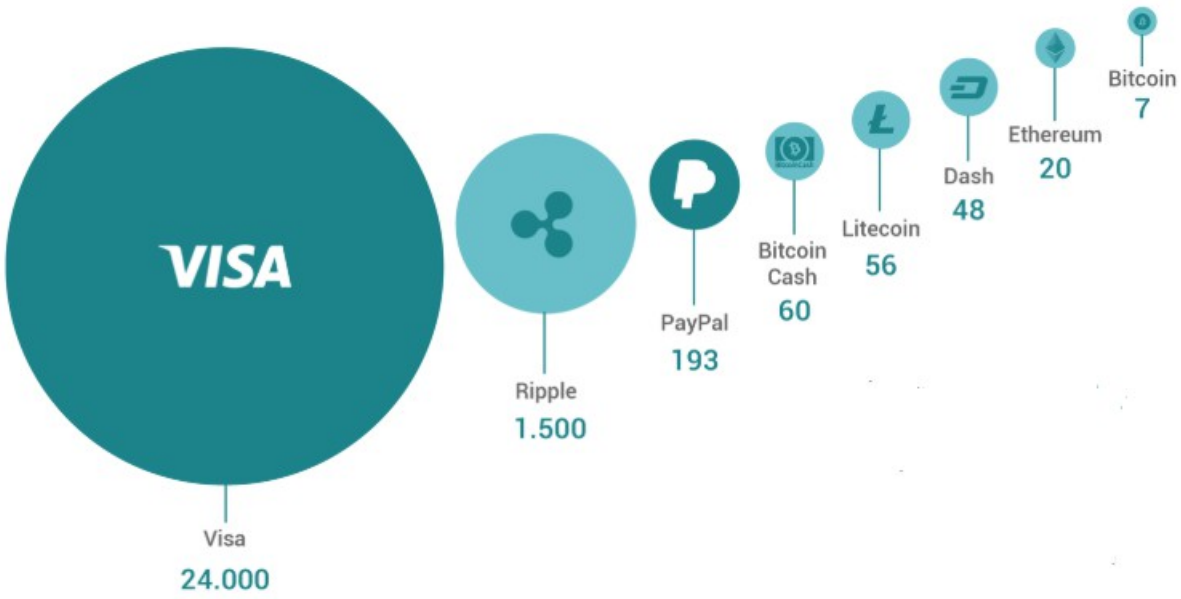
Twitter has suspended their account. They moved to Steemit, a blockchain-based censorship-resistant social media platform. Since their initial announcement, they have received more than 3 bitcoins from the public. The first "level" and a few "checkpoints" are now publicly available.

steemit beta

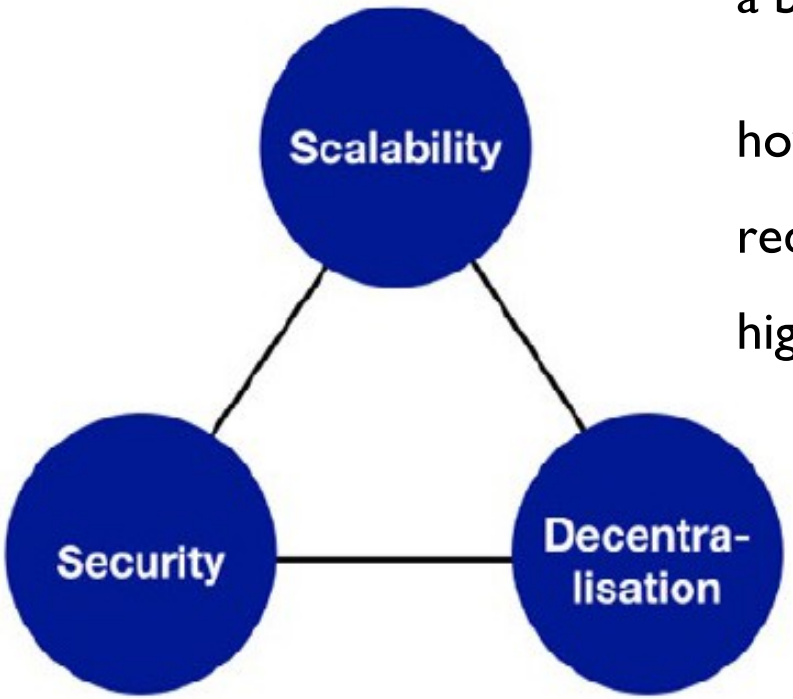
### How does Steemit work?

Steemit.com is one of the many websites (including Busy.org, DTube, and Utopian.io) that are powered by the Steem blockchain and STEEM cryptocurrency. All of these websites read and write content to the Steem blockchain, which stores the content in an immutable blockchain ledger, and rewards users for their contributions with digital tokens called STEEM.

# BLOCKCHAIN CHALLANGES



# THE BLOCKCHAIN TRILEMMA

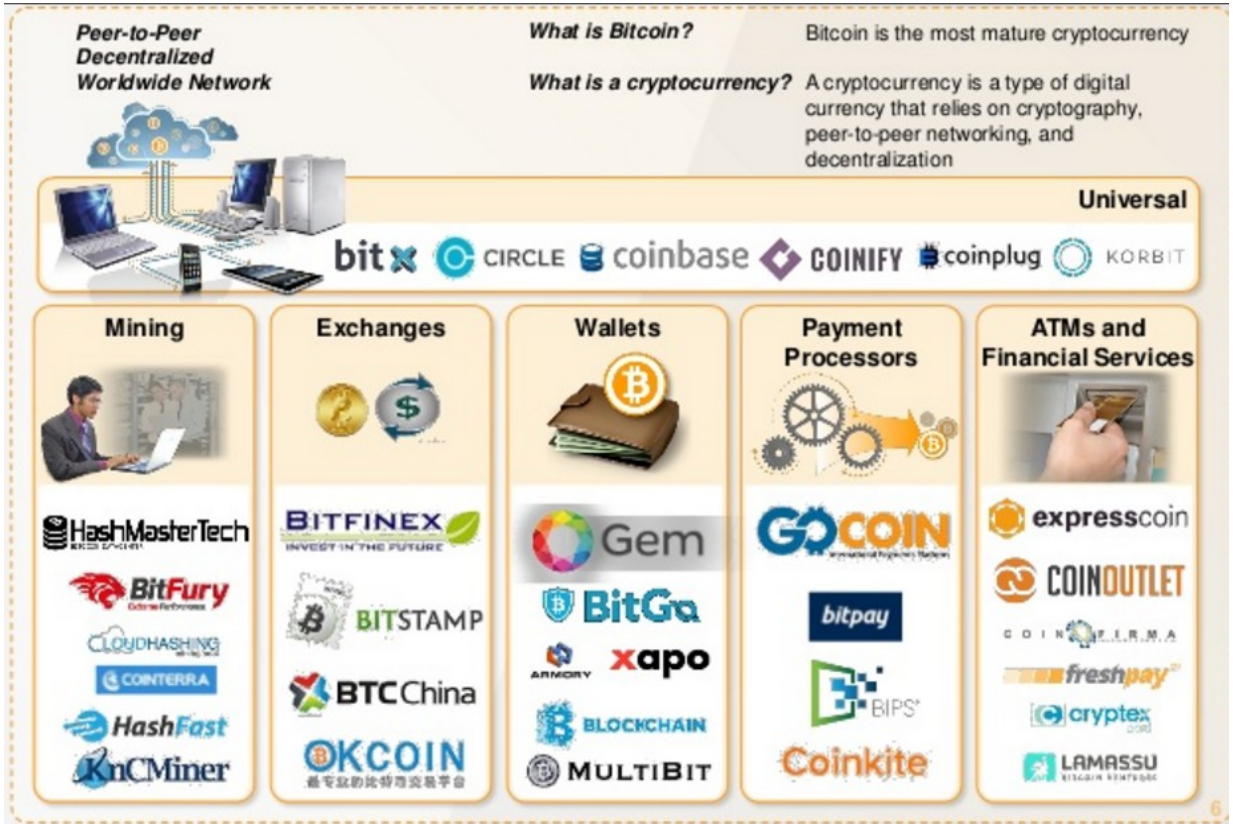



a big scientific challange:

how can we improve scalability without reducing the security level and maintaining a high level of decentralization?

# BLOCKCHAIN: A COMPLEX ECOSYSTEM

- different actors involved
- in the Bitcoin blockchain: Miners, Exchangers, Wallets, Mixer,.....
- a lot of data available: data analysis, artificial intelligence techniques



# REFERENCES

Materials published by the teachers

- lesson slides
- tutorials and material published on the course page

Fine books:


- Hao Zhang, Yong gang Wen, Haiyong Xie, Nenghai Yu, Distributed Hash Table Theory, Platforms and Applications, Springer
- Andreas M. Antonopoulos and Gavin Wood, Mastering Ethereum, Implementing Digital Contracts, O'Really
- Andreas M. Antonopoulos, Mastering Bitcoin, Unlocking Digital Cryptocurrencies, O'Really
- Kalle Rosenbaum, Grokking Bitcoin, April 2019, Manning
- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Bitcoin and Cryptocurrency Technologies, Princeton University Press
- Saravanan Vijayakumaran, An Introduction to Bitcoin, Course Notes