CNRS - INP - UT3 - UT1 - UT2J
Institut de Recherche en Informatique de Toulouse

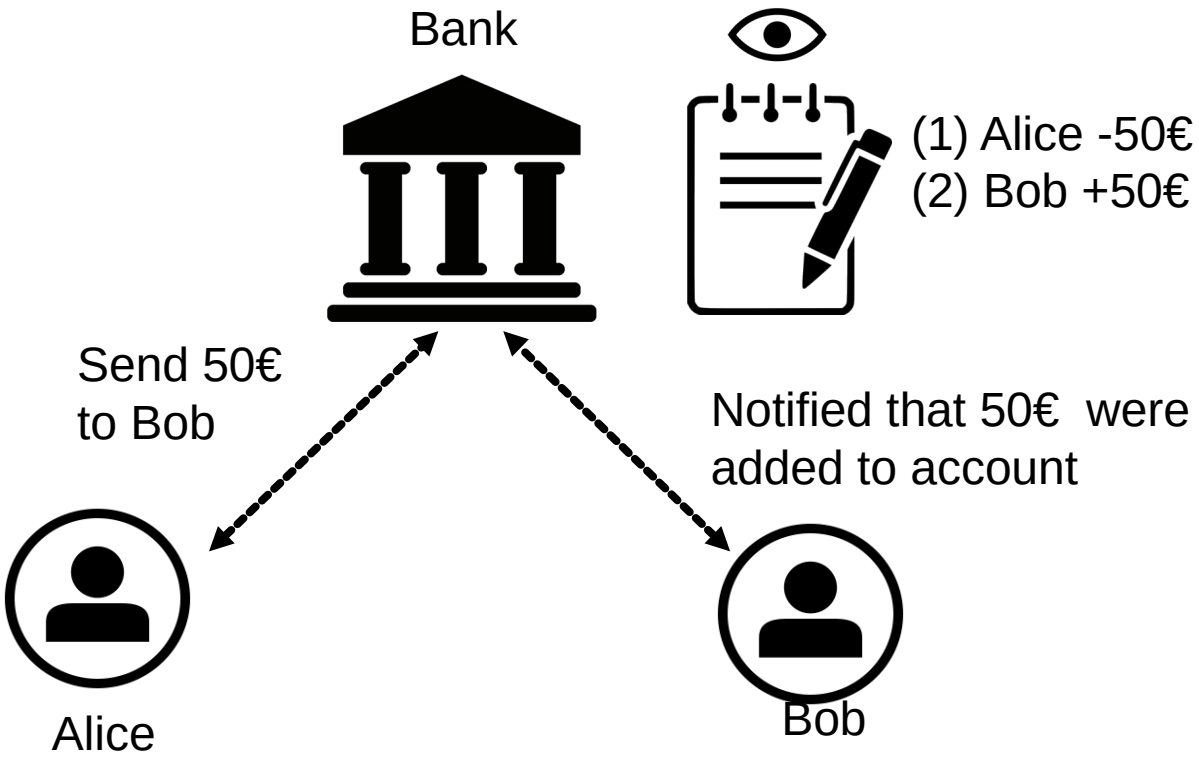
Introduction to the Blockchain

Author: Omar El Rifai
Project Team Members:
Dr. Imen Megdiche, Pr. Franck Ravat, Pr. Olivier Teste, Dr. Maëlle Biotteau (INSERM, CHU), Pr. Xavier Deboissezon (INSERM, CHU)

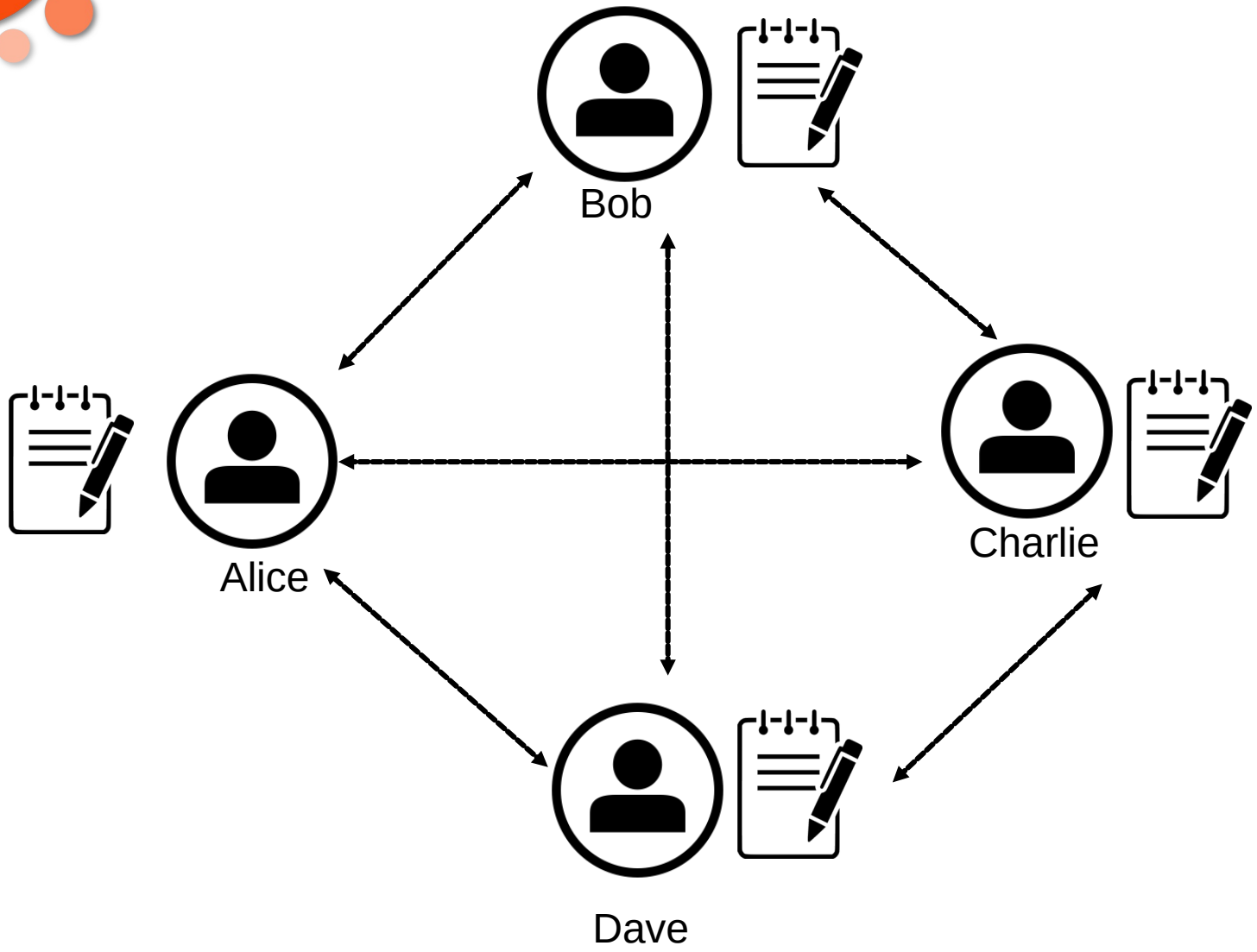
Hôpitaux de Toulouse
UNIVERSITÉ TOULOUSE III PAUL SABATIER

An Illustrative Example

Centralized Currency: the Banking System



Decentralized (digital) Currency



What the blockchain *is not*:

A way to make quick money

A way to privately send data over a network

The solution to our worlds' economic (or global) crisis

What the blockchain is:

A way for peers to reach consensus

An authority free network

An open source, mathematically based solution

Technical Presentation Overview

Part I: Background concepts

- Digital Currencies
- Cryptographic Primitives

Part II: Blockchain Implementations:

- Bitcoin Implementation
- Ethereum Implementation (Smart Contracts)
- Consensus Protocols

Part III: Use Cases

- General cases
- Health care

Background Concepts

Digital Currencies

- The idea of a trust-less decentralized currency has been around for decades [Chaum 1989]

- **Motivation**:
  - Free of administrative and government control
  - Value based on supply and demand *only*

- **Challenges**:
  - Digital Fingerprint
  - Digital Signatures
  - Consensus

Secure Communication with Cryptography

- **Classical (Symmetric) cryptography**

- There exists a secret key that we use for encrypting a message
- The secret key is the same for encrypting and deciphering a message
- Analogy: we put a message in a safe
- *Problem: how to share the password safely?*

- **Modern (Asymmetric) cryptography 1976**

- No need for initial password exchange
- Every user has one private key sk and one public key pk
- Analogy: public mailbox where the address is the public key

Secure communication: example RSA algorithm

- The RSA (Rivest-Shamir-Adleman) cryptosystem is based on the fact that it is:

Easy to find three very large positive integers e, d and n such that:

$$(m^e)^d \equiv m \pmod{n}$$

Message to encrypt

Public key

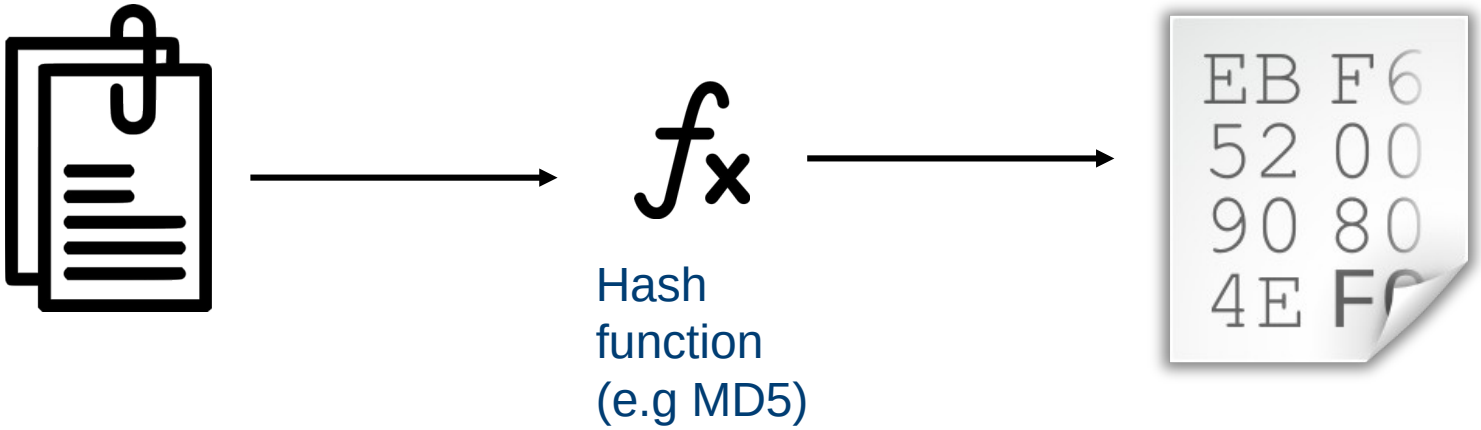
Private key

1) Difficult to find the factorization of the product of two large prime numbers

Hash Functions

How to Manipulate Large Files: Cryptographic Hash Functions

- Algorithm that maps an arbitrary size input to a fixed size output.
- Used to uniquely identify data (fingerprint) and ensure integrity.



Hash function (e.g MD5)

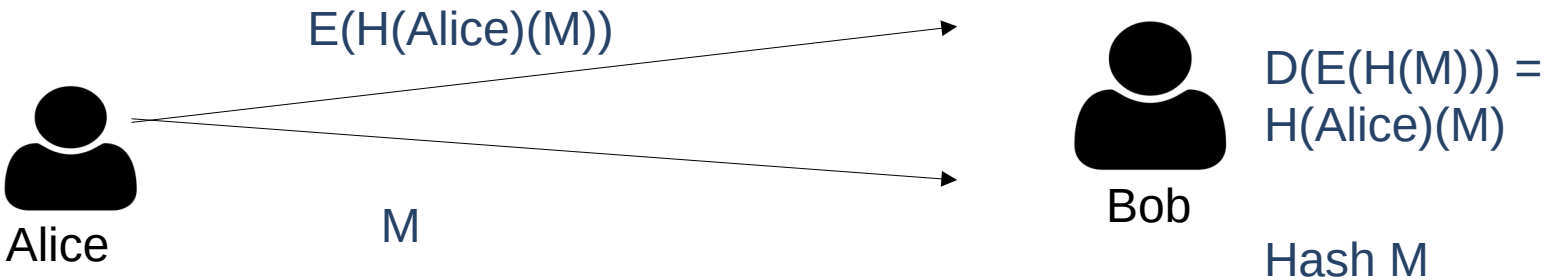
Deterministic Distributed Efficient Pre-image resistant Collision-resistant

Digital Signatures

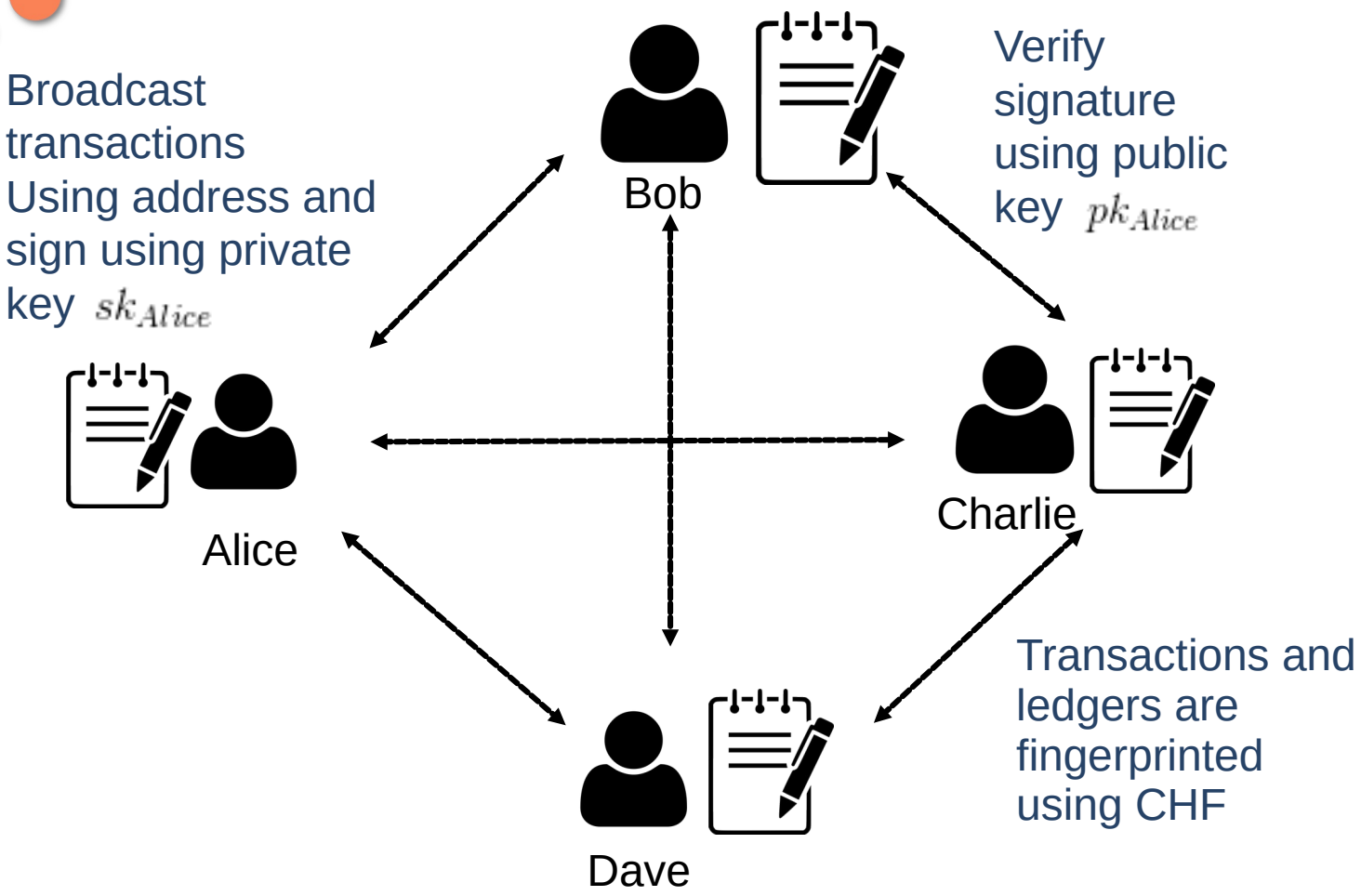
- A digital signature *needs* to have the following properties :
  - Unduplicable: no other document can be signed by it
  - Sender binding: associated with one sender only
  - Document binding: the original document can not be changed

Digital Signatures

- Let M be the message Alice wants to send
- H() be a hash function
- E() be a asymmetric encryption function
- D() be the associated decryption function



Recap of a Blockchain Architecture



...What about consensus?

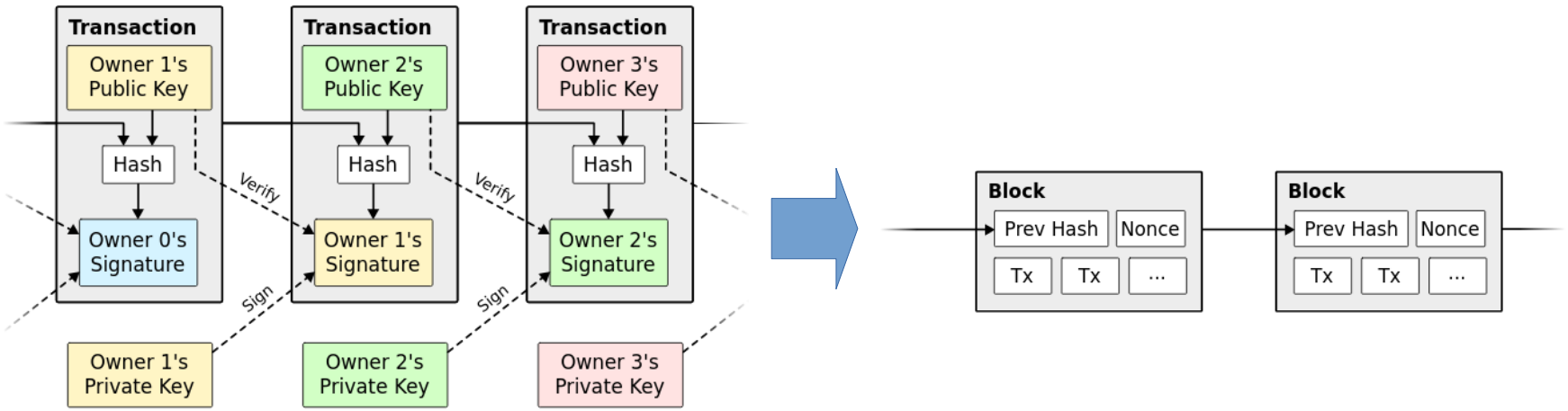
Blockchain Implementations

Bitcoin : A first working example

- Based on established work in cryptography Satoshi Nakamoto published a paper in 2008 [Nakamoto2008] that contributed with the following :
  - A fully functional *trustless* digital currency system
  - An algorithm which prevents the “double spend” problem. The intuition is that transactions have to be timestamps and trust based on the entire network.
  - Security is guaranteed is the number of honest nodes is larger than the number of malicious nodes

Bitcoin: A chain of blocks

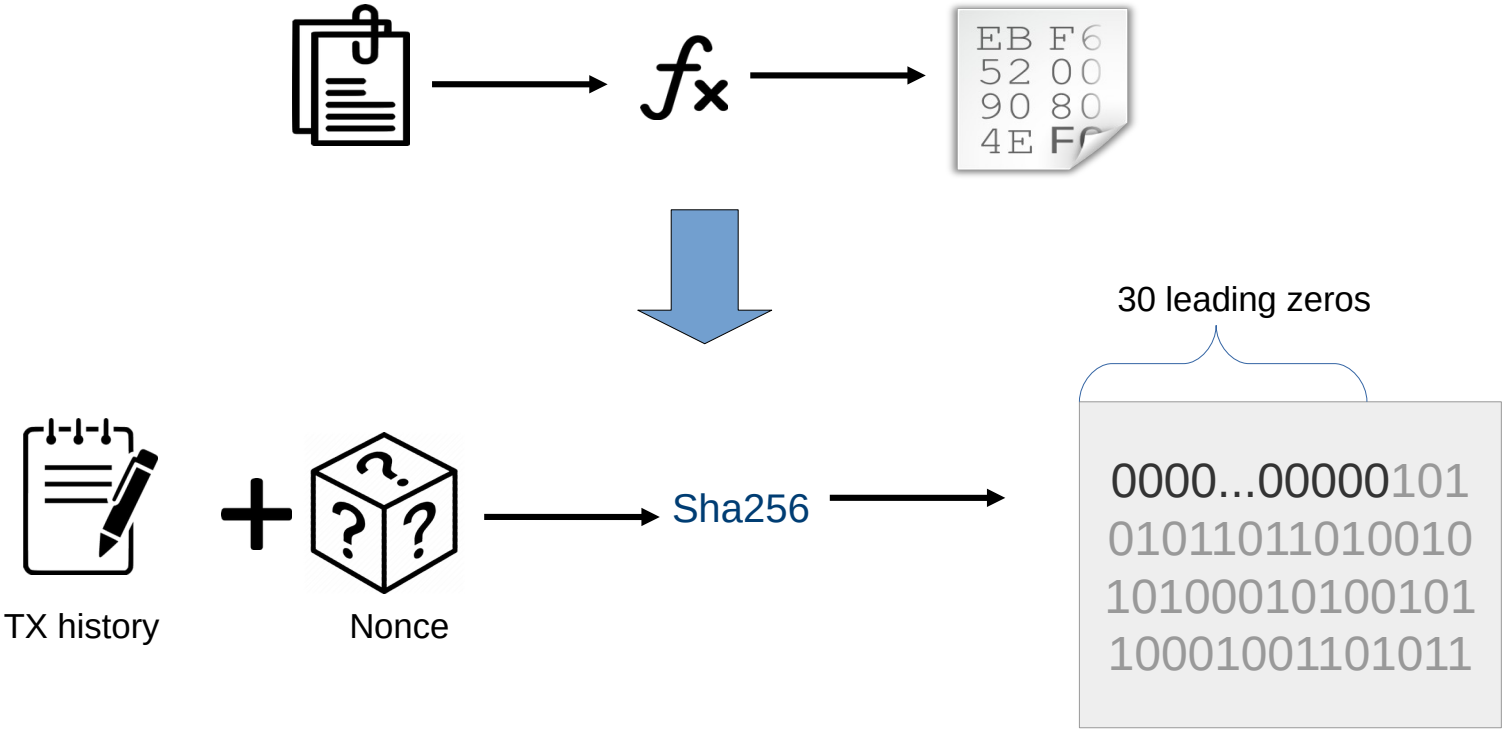
1. List of TXs
2. A hash of previous TX
3. POW (consensus)



Bitcoin: Proof of Work (POW)

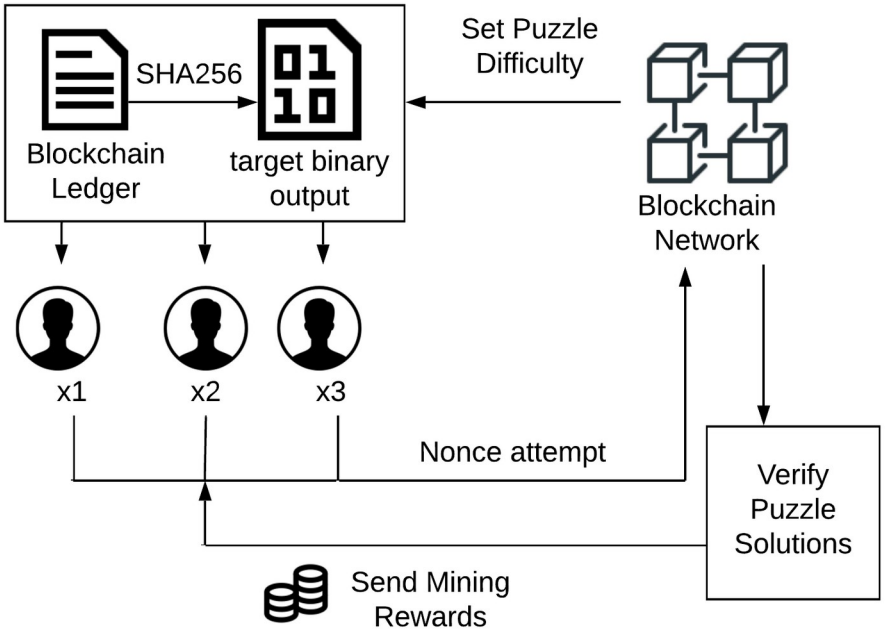
High level idea:

- Proof of CPU effort (solving a puzzle) is attached to the block
- The block cannot be changed without redoing the work
- After chaining other blocks, it becomes even more difficult
  - o



Bitcoin: Proof of Work (POW) ctd.

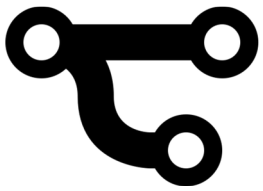
- So what incentivize the network to perform these computations (expending computational power)?
- One answer is simple to be able to use a secure network of value exchange
- Another (less idealistic) reason is that nodes that verify transactions (i.e miners) are rewarded with bitcoins when validating a block



Bitcoins : The Network

Transactions are broadcast to the entire netwok in the following way:

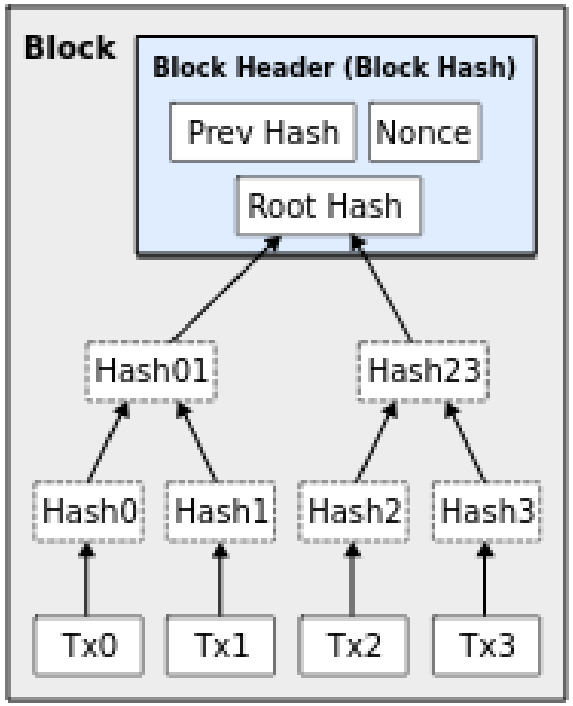
1) Every node (participant) gather new transactions in “blocks”
2) Every node tries to find the POW for its block
3) When a node finds the solution to the POW, it transmits its block to other nodes
4) Nodes accept a bloc if all the TX are valid and not already spent
5) Nodes express their approval of the bloc by using its hash as part of the later TX they process



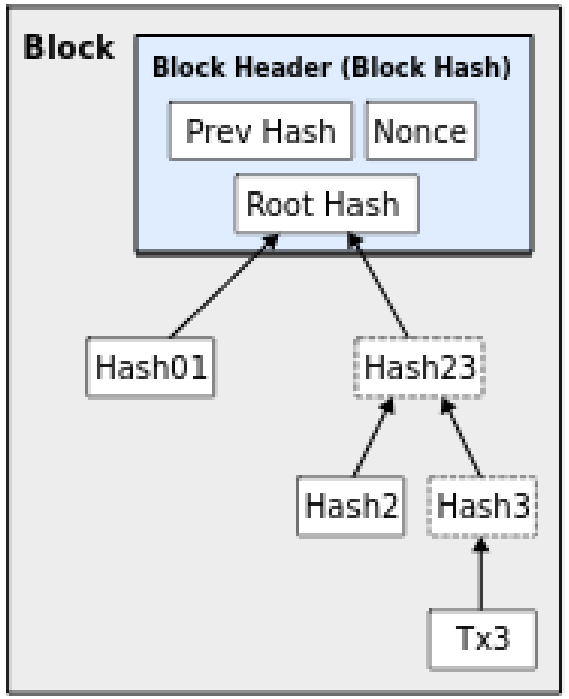
In case of conflict, temporary branches can be created locally

Bitcoins : Reclaiming disk Space

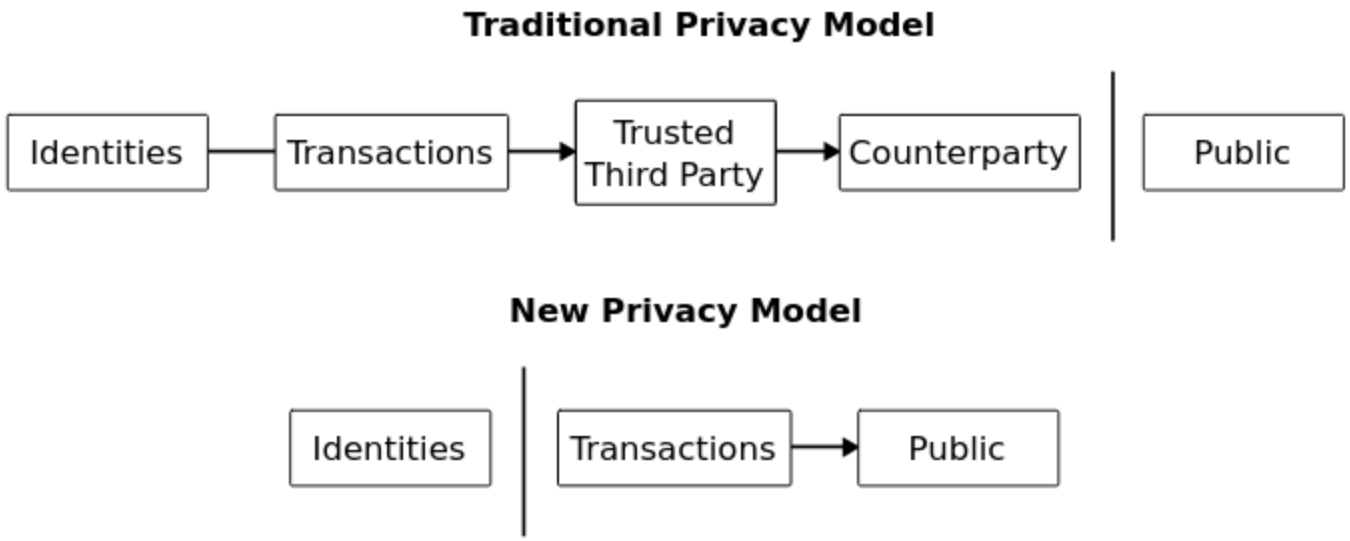
- To save up disk space, old transaction can be discarded.
- A Merkle Tree structure is used so that the hash of the history is not changed



Pruning old transactions

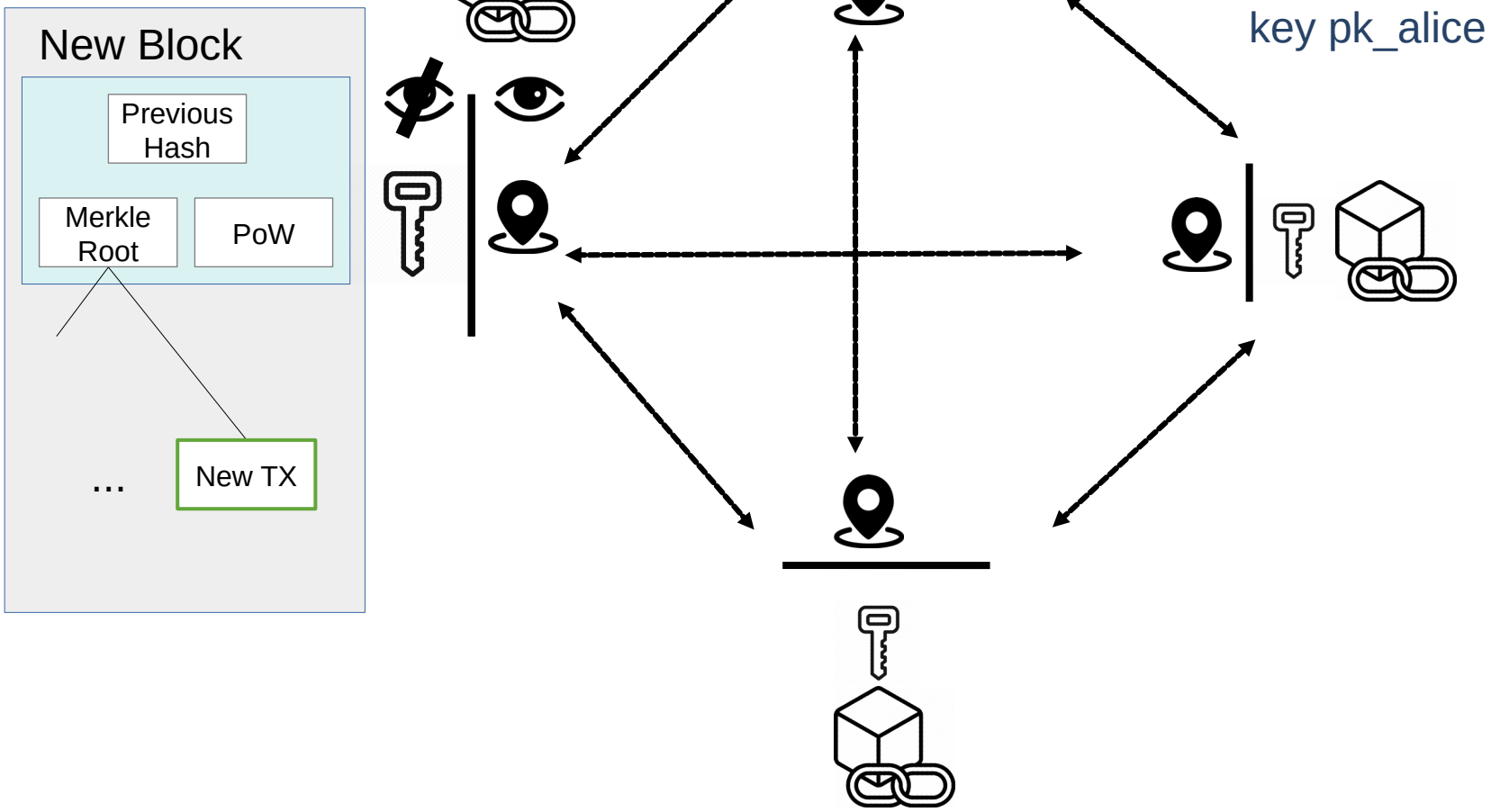


Bitcoins : Privacy in the blockchain

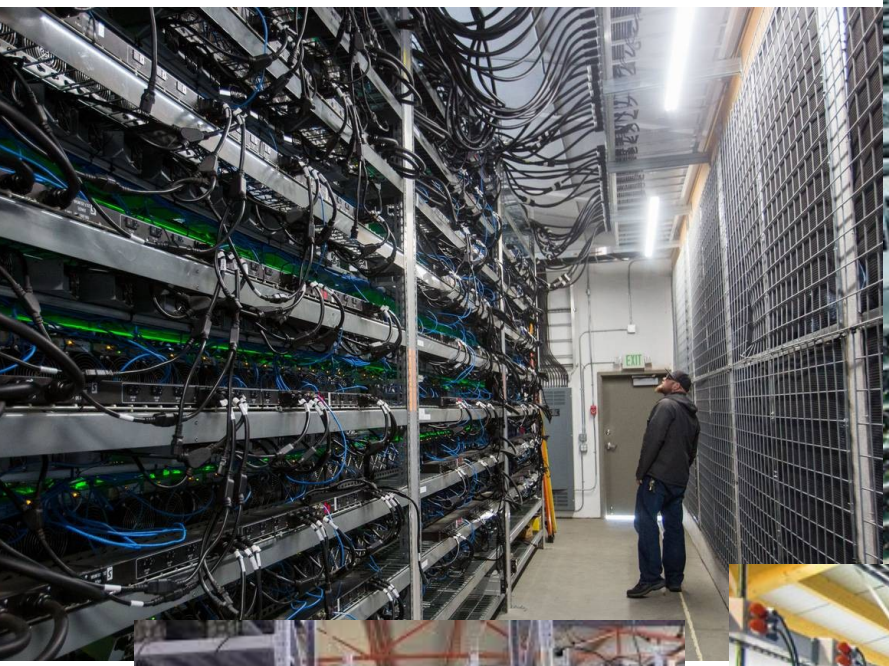


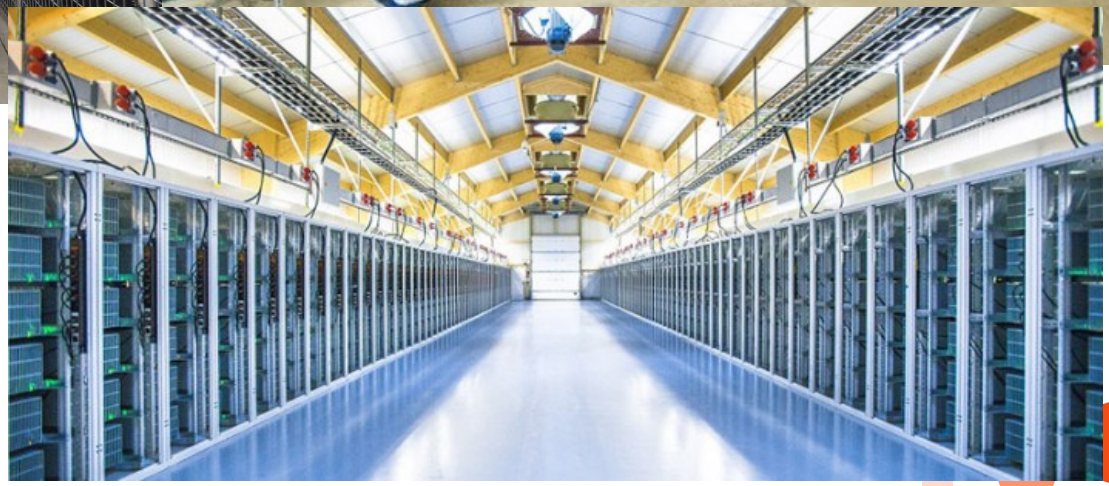
- Because of consensus requirements, all transactions should be made public
- Asymmetric encryption protocols (along with a firewall) can protect the identity of users

Recap of a Blockchain Architecture with Bitcoin




107
SAMSUNG





Ethereum Implementation

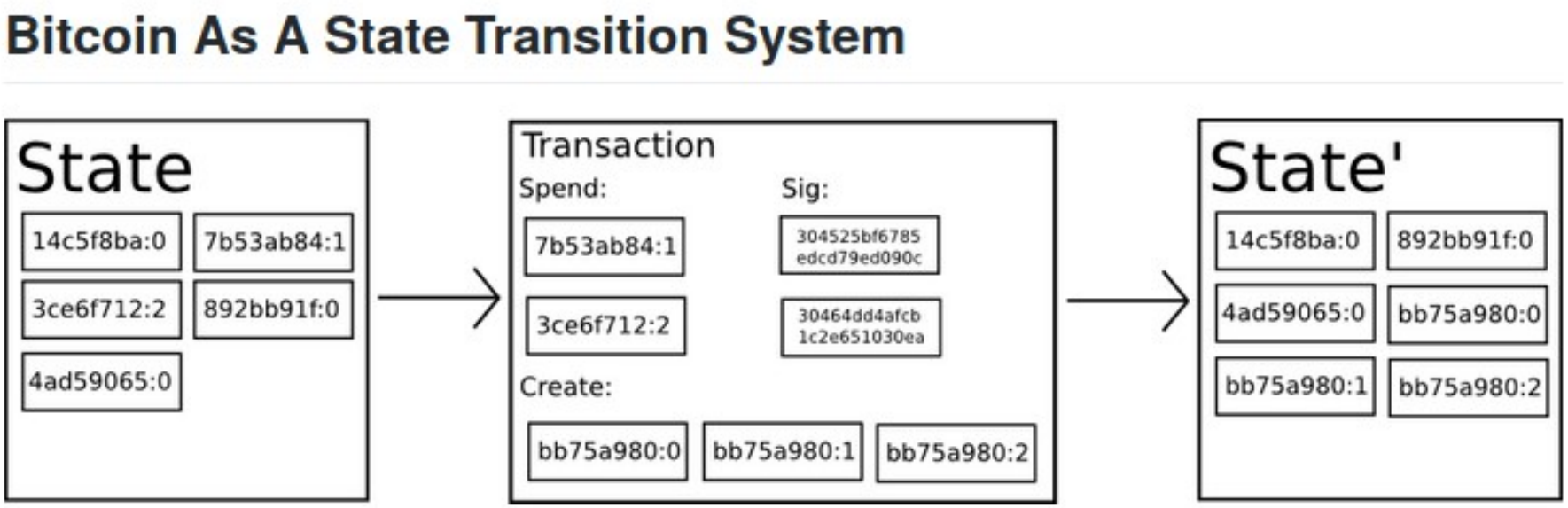
Ethereum: Smart Contracts

- Bitcoin: Consensus in a network *without the need for a trusted third party*
- But consensus is limited to simple transactions
- More complicated rules such as *conditional money transfers* or *online voting* can not be implemented
- Ethereum: develop the idea further to allow consensus on code [Buterin2014]

Bitcoin	Ethereum
Private keys own simple values (UTXO)	Private keys own Accounts
All values are owned by a private key	There are externally owned accounts and internal accounts (can not be called directly)

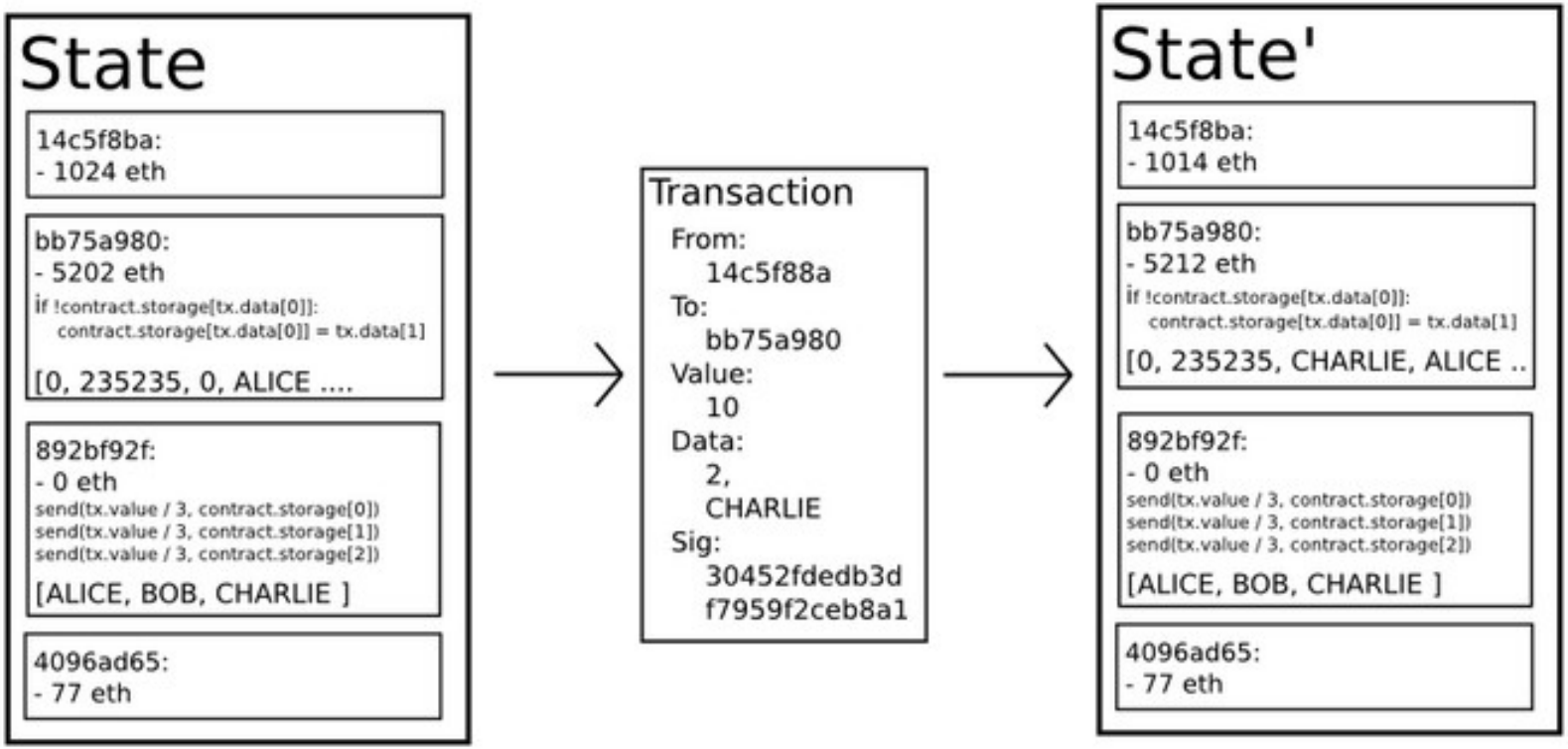
Ethereum: Smart Contracts (ctd.)

- Let’s think of the bitcoin as a state transition system



Ethereum Smart Contracts

Ethereum State Transition Function



Consensus Protocols

What is wrong with PoW

- In PoW, the algorithm rewards participants who solve puzzles to validate transactions and create new blocks → mining
- There are only 21 million bitcoins that can be mined in total.
- Miners will still be incentivized to validate the bitcoin blockchain because they will collect transaction fees from users
- The fact that bitcoin is capped means it was thought as a deflationary economy
- PoW consumes large quantities of electricity

Proof of stake: the future?

Instead of relying on computational work, POS chooses the validator randomly but with probability associated to with wealth or age (i.e., the stake) → the more you own the more incentive you have of keeping the blockchain active

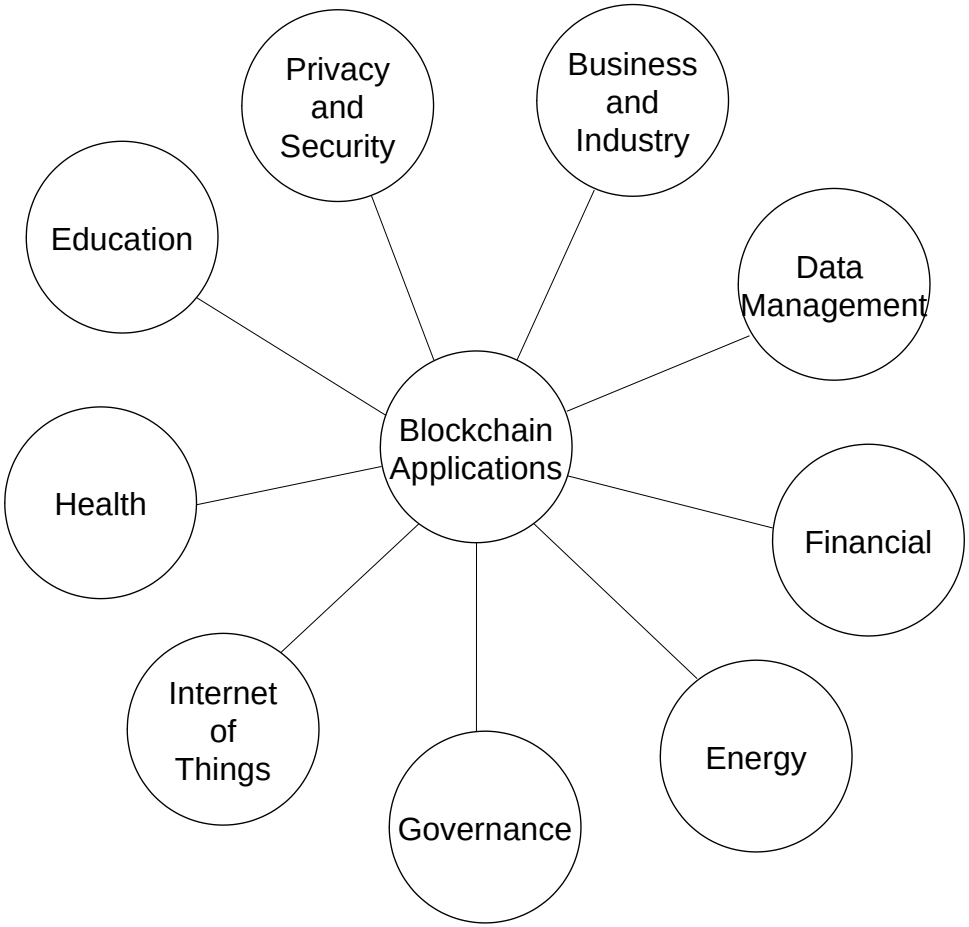
Proof of Work	Proof of Stake
Participating nodes are called miners.	Participating nodes are called validators
Mining capacity depends on computational power	Validating capacity depends on the stake in the network
Mining produces new coins	No new coins are formed
Miners receive block rewards	Validators receive transaction fees
Massive energy consumption	Low to moderate energy consumption.
Significantly prone to 51% attacks	51% attacks are virtually impossible

Use Cases

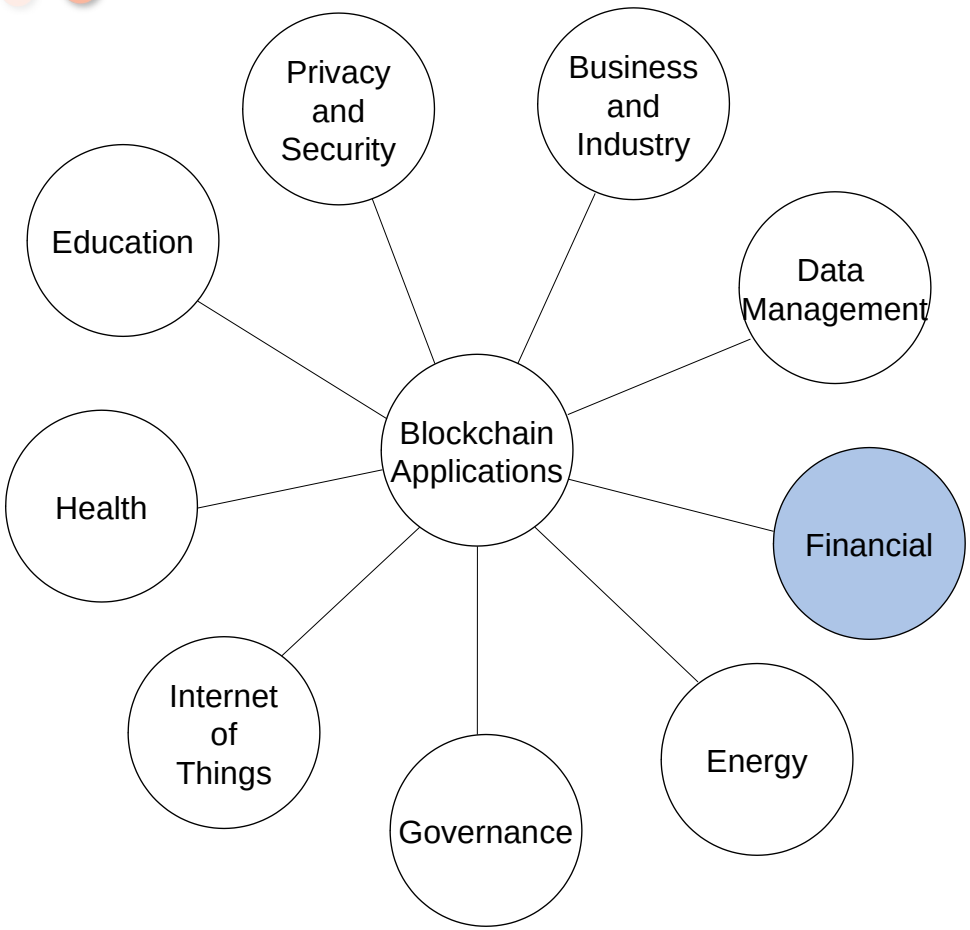
Properties of the Blockchain that make it desirable for different use cases

Decentralization	Distributed stakeholders require a decentralized management system. Decentralization means no central authority can unilaterally take decisions
Improved data security and privacy	Data, once saved on the blockchain, can not be corrupted, alterated or erarased. All the data are timestamped and saved in chronological order. Cryptographic keys help protect the identities of users
Data Ownership	Proof of ownership and access control mechanisms through Scs
Availability/ Robustness	Replication of records on all nodes removes the single point of failure problems
Transparency and Trust	All the records and transactions are visible by everyone. This makes audit operations simple and efficient

Different areas of Application



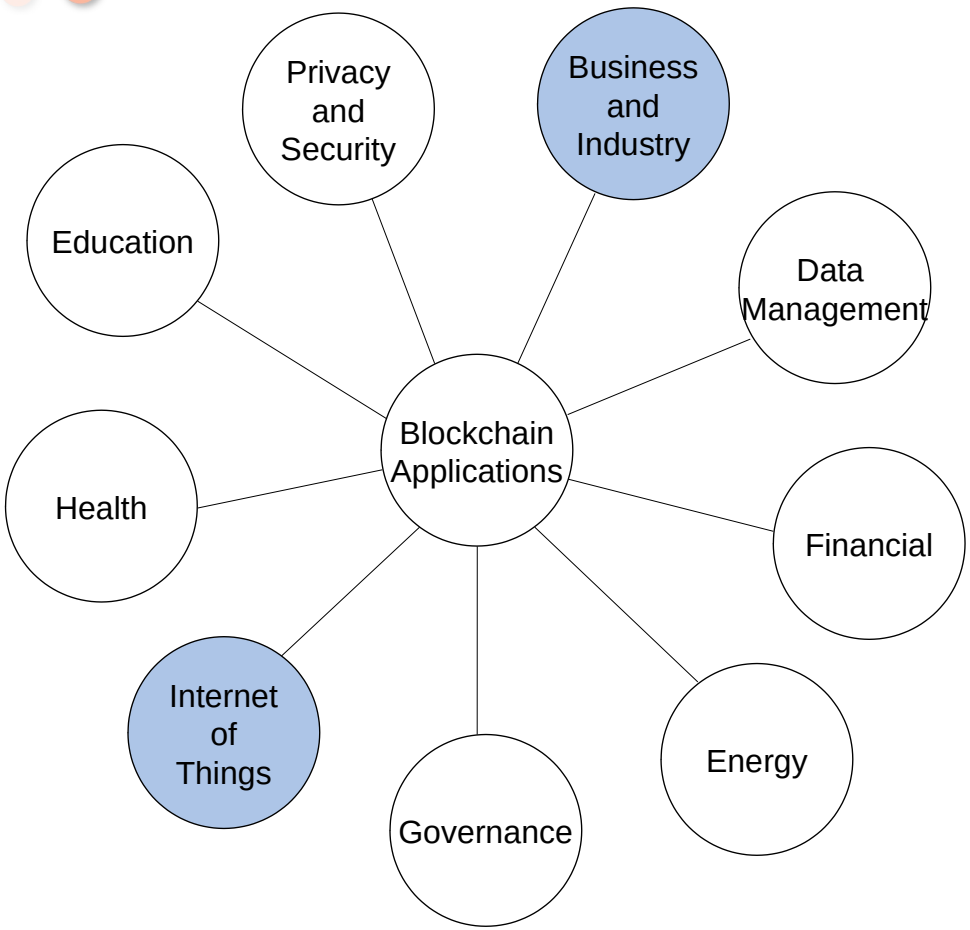
Financial Applications



- Besides crypto-currencies, a host of financial applications have been developed Example applications include:
- Loan management
- Financial auditing
- Commercial property registration
- Prediction Market Place Systems
- ….

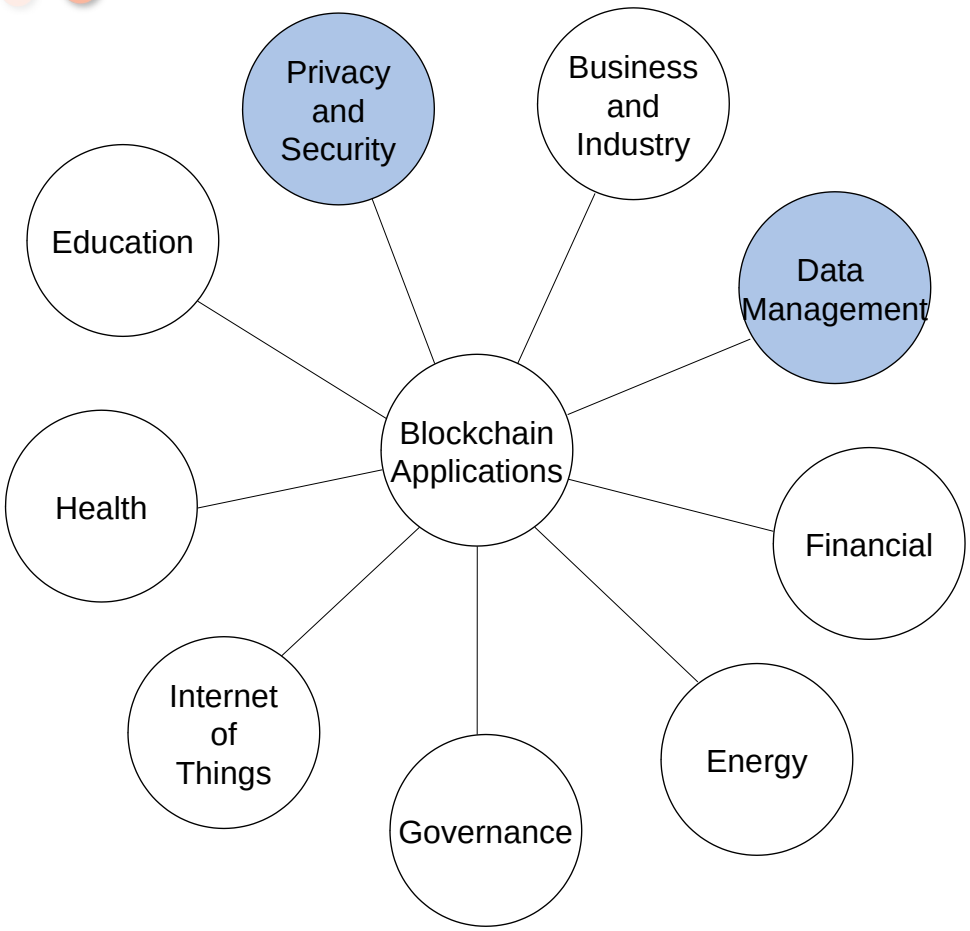
BARCLAYS Goldman Sachs r3

Business and Industry Applications



- Supply chain auditing using the inherent transparency and immutability properties of the blockchain
- Intellectual property management (musicians can store a hash of their creations on the blockchain and be remunerated accordingly)
- Decentralized Insurance Policies with smart contracts automatically reimbursing if an accident were to happen

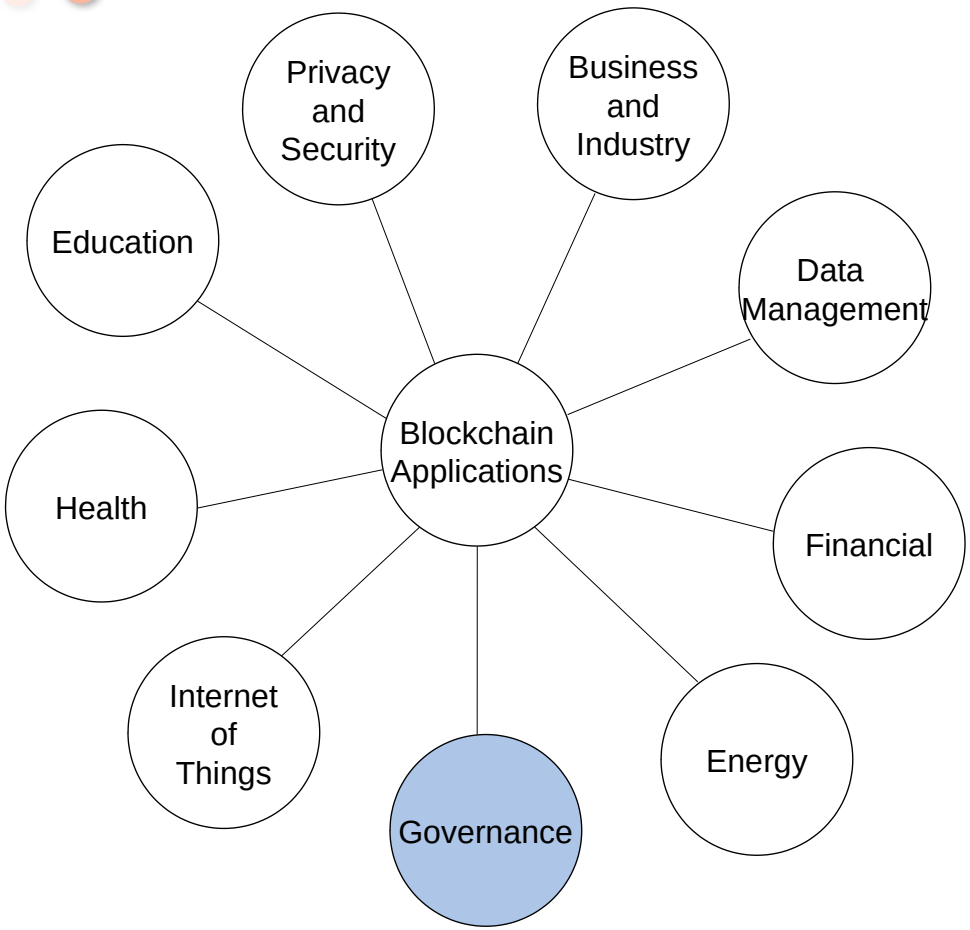
Data Management Applications



- Data can not be stored directly because of privacy issues and scalability issues.
- An encryption method called “zero knowledge Proof” (ZKP) is being studied for increasing the privacy (Zcash)
- Some efforts in the direction of homomorphic encryption are also being done

Zcash

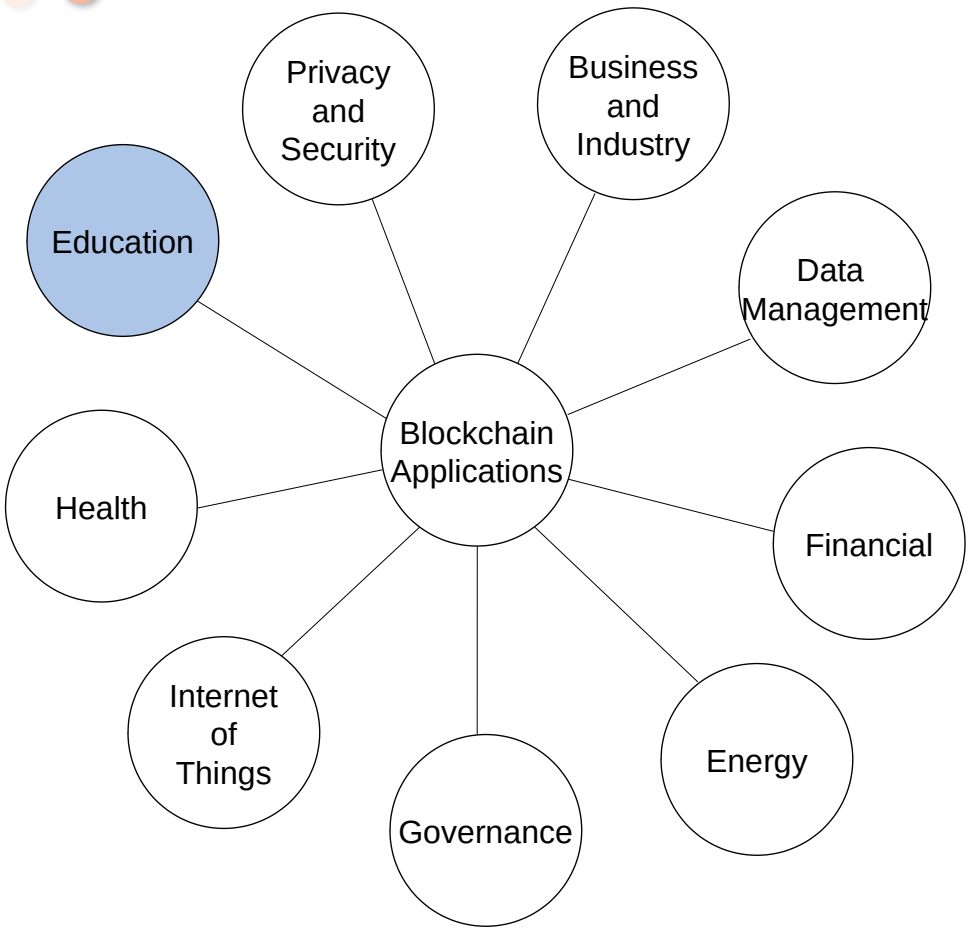
Governance Applications



- Citizenship / legal documents
- Marriage, divorce, taxes
- Voting
- Namecoin for DNS service

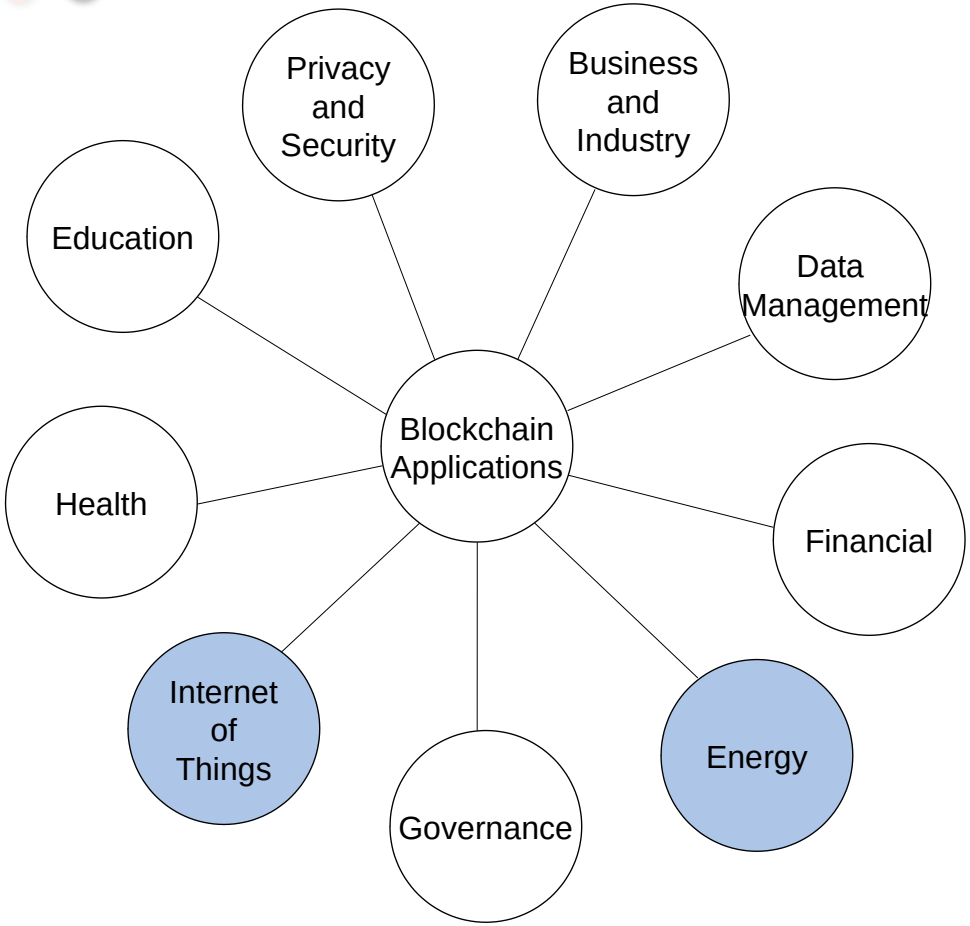
namecoin

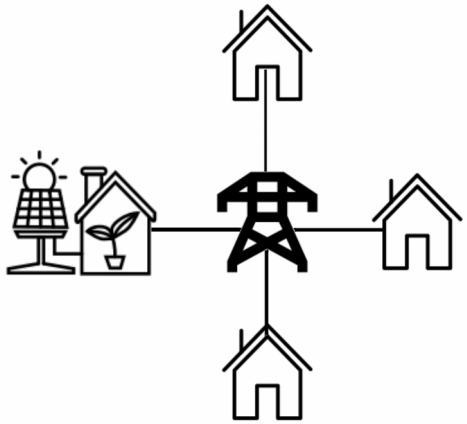
Education Applications

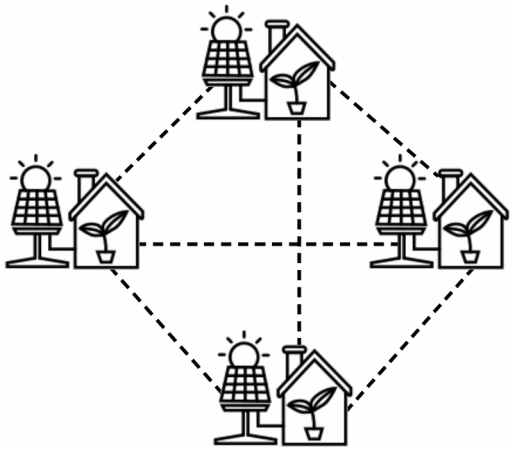


- Education certificates
- Credit management
- Securely Timestamped Manuscript Submission and Peer Review Feedback using the Blockchain

Energy Sector Application

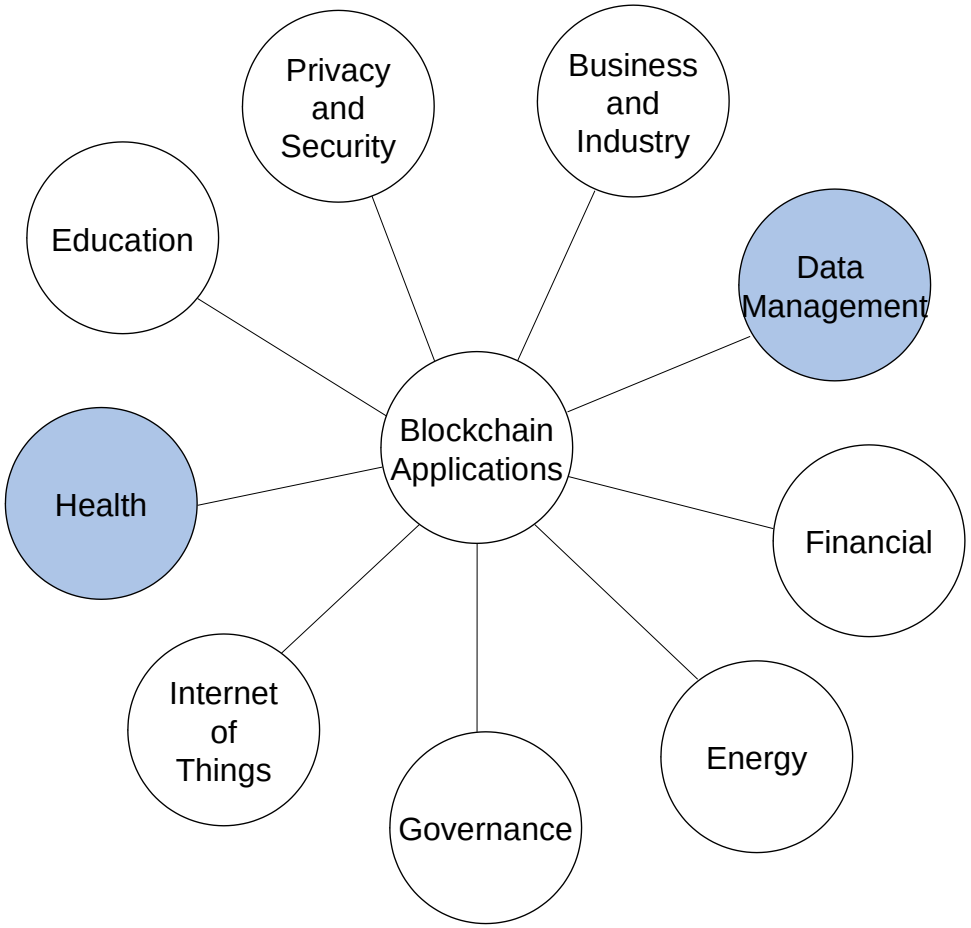






SUNCHAIN

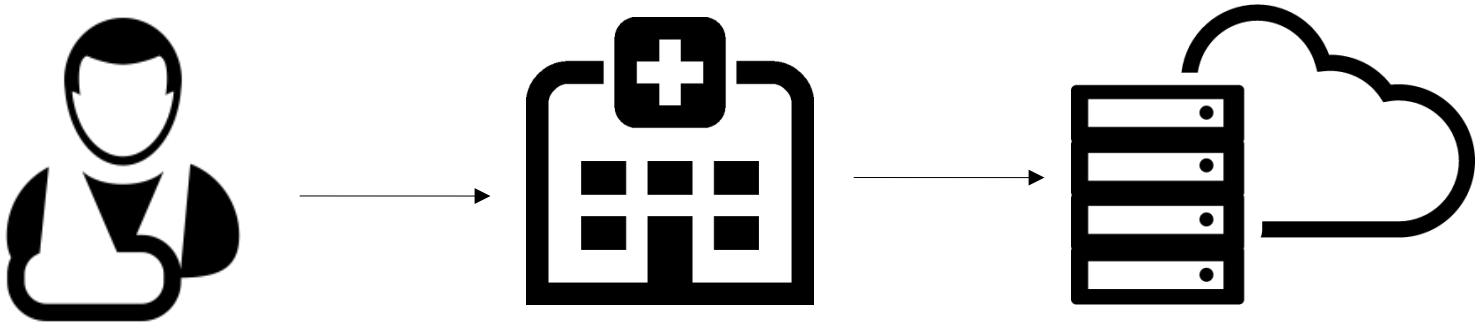
Health Care Applications



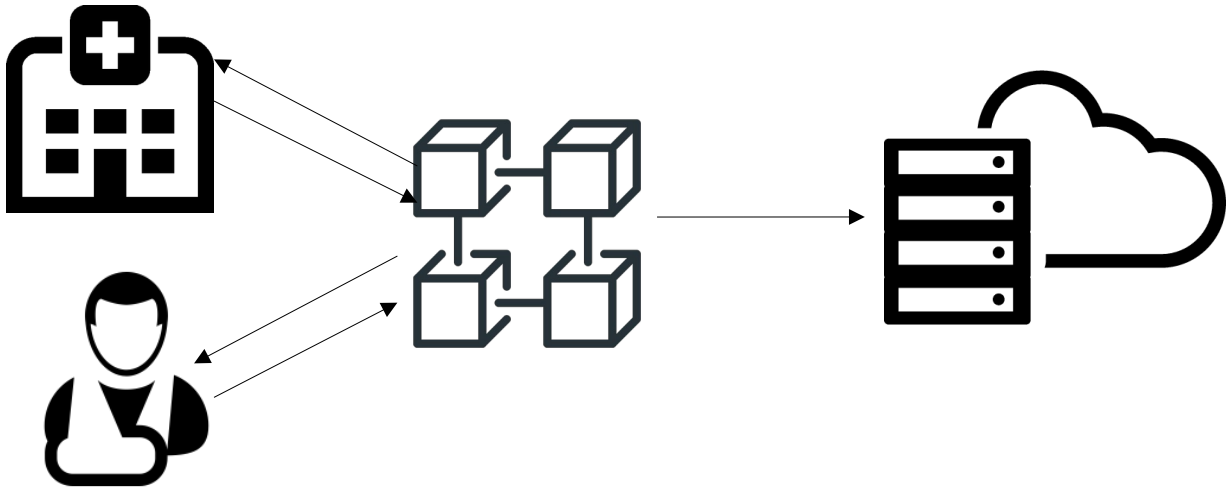
- Many applications (medical insurance, medical supply, iot related etc…)
- The most prominent use case in health-care applications are Electronic Health Records (EHR)
- As the data are sensitive and patient specific some ownership and control issues arise
- The blockchain has been used in several studies to guarantee data ownership and access control mechanisms for patients

Health Care Applications

Traditional architecture for EHR



Blockchain-based architecture



Hashes of data are stored on-chain:

- Ownership can be proved
- Access control can be managed
- Data modification can be detected

Blockchain-based EHR literature

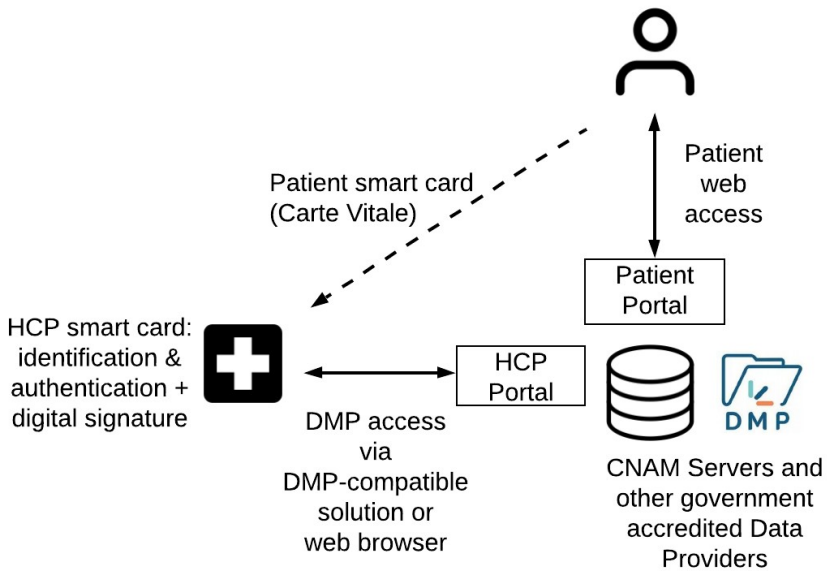
Table 1. Properties of related blockchain-based EHR/PHR framework in the literature

Article	Blockchain Use	External Storage	Blockchain Technology	Cryptographic Protocols
[Zyskind et al., 2015]	Data access policies	Distributed Hash Table NoSQL	Bitcoin	Symmetric and asymmetric key encryption
[Ariel Ekblaw, 2016]	Identity management Access policies Reference pointers Summary logs	Providers DB storage	Ethereum	Digital signatures Encryption (no details)
[Xia et al., 2017]	DB actions log for auditing	Existing DB infrastructure Authenticator Server	Proprietary	Digital signature Asymmetric encryption
[Fan et al., 2018]	Reference pointers Hash of EMRs Summary logs	Providers DB (unspecified)	Proprietary	Digital signature Symmetric and asymmetric key encryption
[Dagher et al., 2018]	Identity management Hashes of reference pointers History summary Access policies Proxy re-encryption	Providers' DB storage	Ethereum	Symmetric and asymmetric key encryption Proxy re-encryption signature
[Liu et al., 2018]	Access policies Reference pointers Access logs	Cloud storage	Smart Contract based - unspecified	Symmetric and asymmetric key encryption Content Extraction Signature
[Zhang et al., 2018]	Identity Verification Access policies Reference pointer	Providers' DB storage	Ethereum	Digital Signature Symmetric and asymmetric key encryption

The French Use Case

"Blockchain-Based Personal Health Records for Patients' Empowerment" EL RIFAI O., Bioteau M., MEGDICHE I., RAVAT F, TESTE O. (Submitted RCIS2020)

Without blockchain



- Access and control mechanisms unilateral
- All identities hosted on server
- Records security and immutability can be compromised just attacking the CNAM server

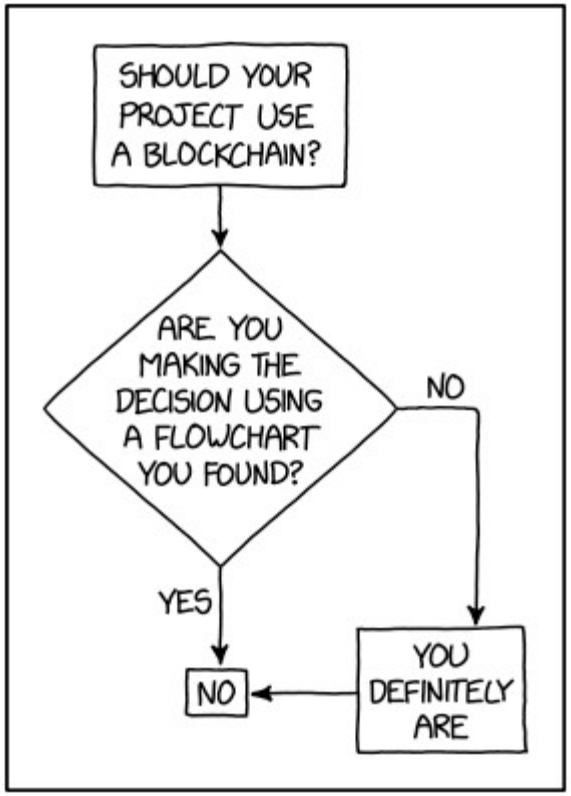
With blockchain

Identity Management:
CNAM registerand maintain a list of registered patients.

1) Democratize the governance of the registration process
2) Automatize the rules for registration clear and transparent.

Access Management:
The blockchain can host data hashes and user-defined access control policies. Data hashes fingerprint their medical records guaranteeing that the original copy is never tampered with.
Access control policies stored on the blockchain would serve as immutable reference for the access rights

Data Audit:
Transactions are natively immutable on the bockchain, patients are guaranteed that the logs are not tampered with.



https://xkcd.com/2267/

References

[Chaum1988] Chaum, David, Amos Fiat, and Moni Naor. "Untraceable electronic cash." Conference on the Theory and Application of Cryptography. Springer, New York, NY, 1988.

[Nakamoto2008] Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019.

[Buterin2014] Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." white paper 3.37 (2014).

[Casino2019] Casino, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. "A systematic literature review of blockchain-based applications: current status, classification and open issues." Telematics and Informatics 36 (2019): 55-81

[Fan et al., 2018] Fan, K., Wang, S., Ren, Y., Li, H., and Yang, Y. (2018). MedBlock:Efficient and Secure Medical Data Sharing Via Blockchain. Journal of Medical Systems, 42(8):1–11.

References (ctd.)

[Liu et al., 2018] Liu, J., Li, X., Ye, L., Zhang, H., Du, X., and Guizani, M. (2018).BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records. 2018 IEEE Global Communications Conference, GLOBECOM 2018 Proceedings

[Xia et al., 2017] Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., and Guizani, M. (2017). MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain. IEEE Access, 5:14757–14767.

[Zhang et al., 2018] Zhang, P., White, J., Schmidt, D. C., Lenz, G., and Rosenbloom,S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data.Computational and Structural Biotechnology Journal, 16:267–278.

[Zyskind et al., 2015] Zyskind, G., Nathan, O., and Pentland, A. S. (2015). Decentralizing privacy: Using blockchain to protect personal data. In Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015, pages 180–184