Blockchain: les aspects organisationnels pour l'eSanté

Alevtina Dubovitskaya

Assistante, Institute Informatique de Gestion
HES-SO Valais-Wallis

Doctorante, EPFL, Lausanne
Laboratoire des systèmes informatiques distribuées,
✉ alevtina.dubovitskaya@epfl.ch

22 Mai 2017, 17e Séminar d'Informatique Juridique de Macolin

Le Plan de la Presentation

- **La blockchain, qu'est-ce que c'est ?**
  - La technologie
  - La blockchain publique
  - La blockchain privée
- Utilisation de la technologie blockchain
- Les aspects organisationnels et les questions ouvertes

Blockchain

- Technologie presentée par Satochi Nacamoto sur laquelle la « monnaie numérique » **Bitcoin** est basée

Bitcoin: A Peer-to-Peer Electronic Cash System

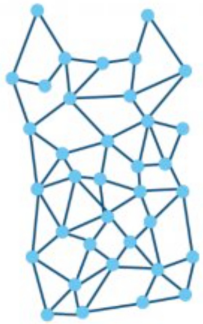
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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.

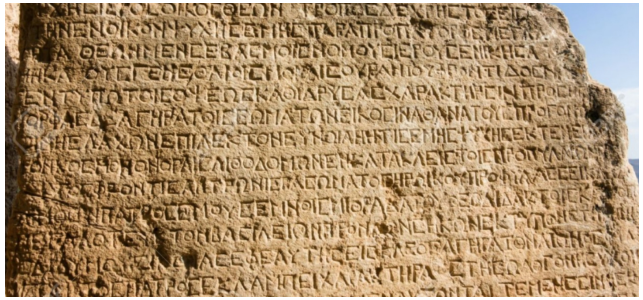
La Blockchain est …

- un Ledger
  (livre de compte)

- Distribuée (non centralisée)



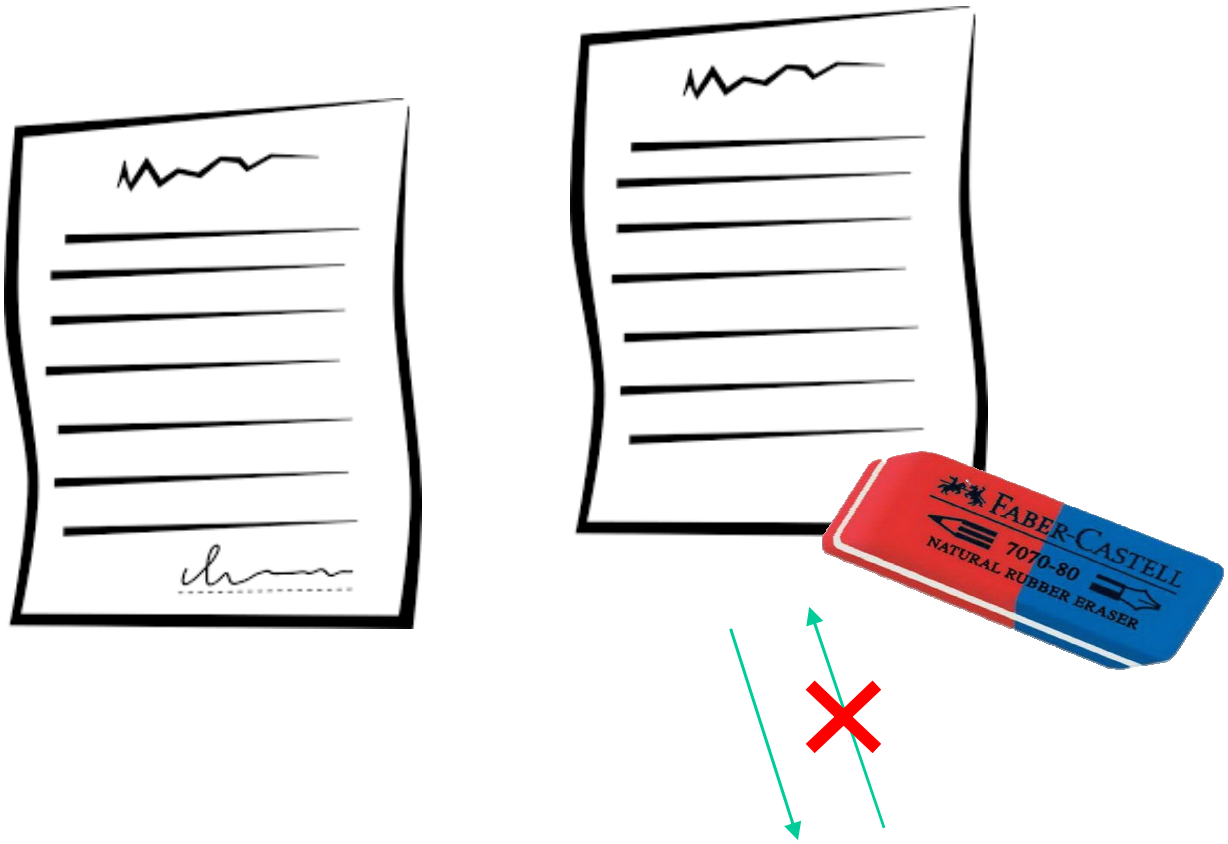
- Sécurisée (avec cryptographie)
- Immutable



Hash code (algorithme SHA-256)

cdd31151f5635f923bd640383149666d772921f594b8200054ba0bc08aefbe0d

Hash code (algorithme SHA-256)

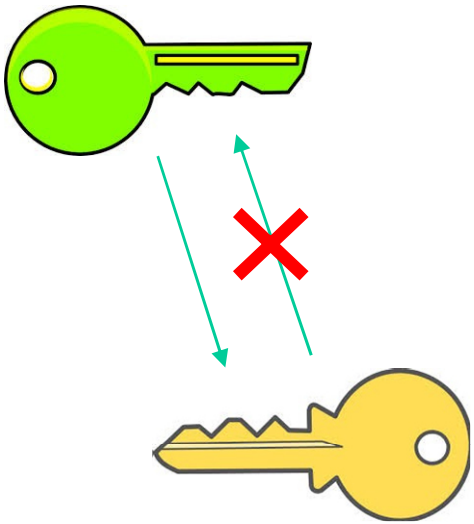


~~cdd31151f5635f923bd6403831496666d772921f594b8200054ba0bc08aefbe0d~~

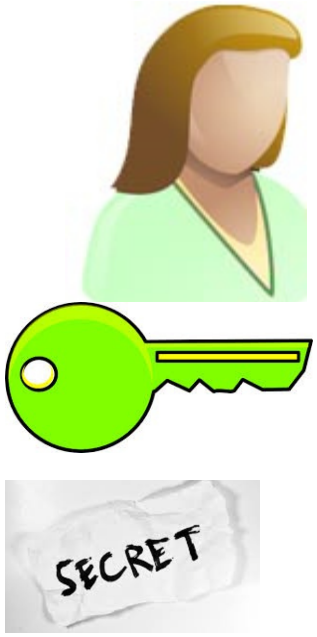
903790784f694f00534736a8dc808ed43f4659f0298e9332bf41bcae18a633f2

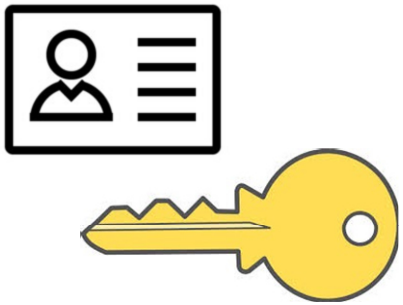
PKI (Infrastructure à clés publiques)

Clé privé

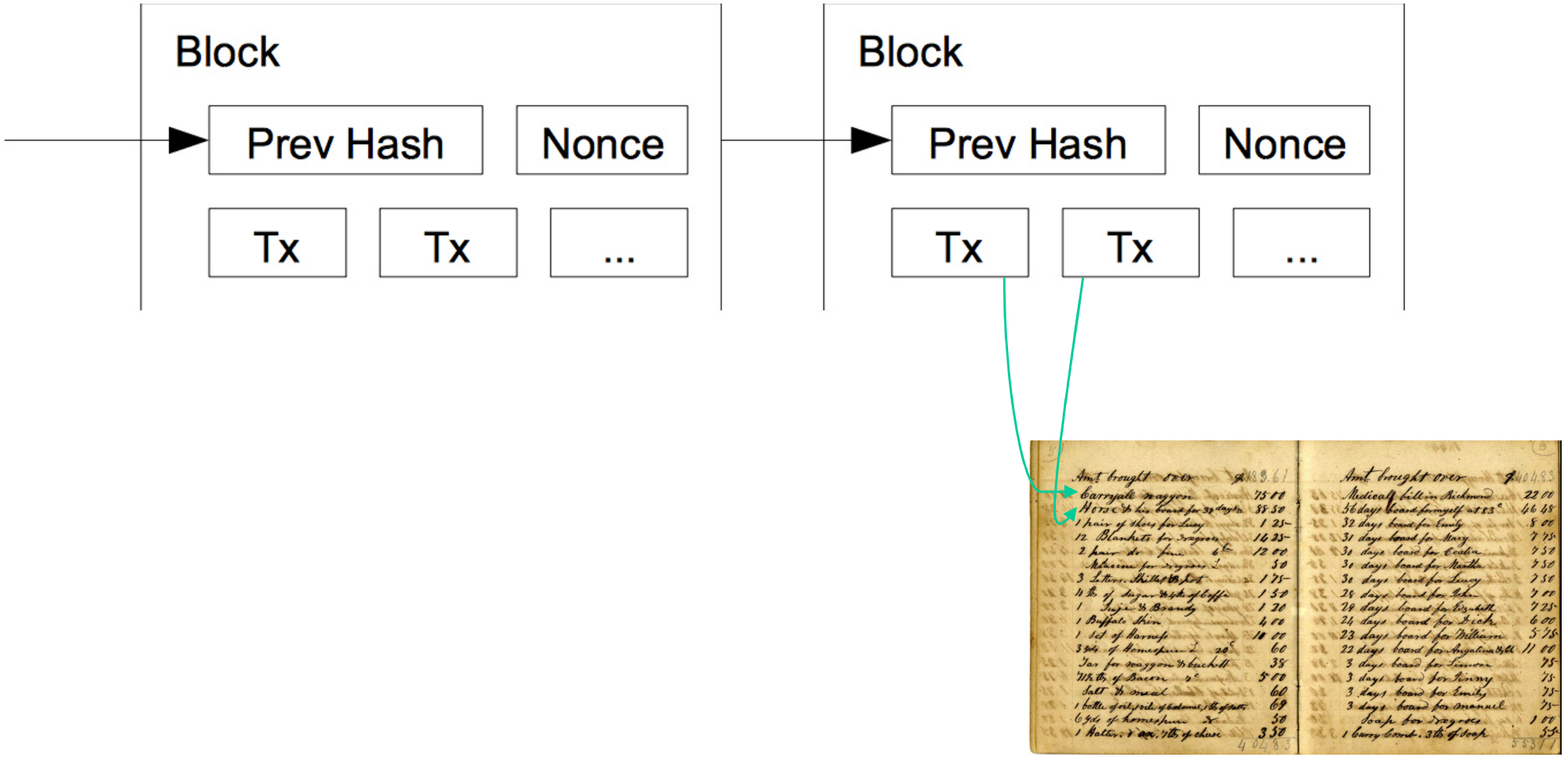


Clé public

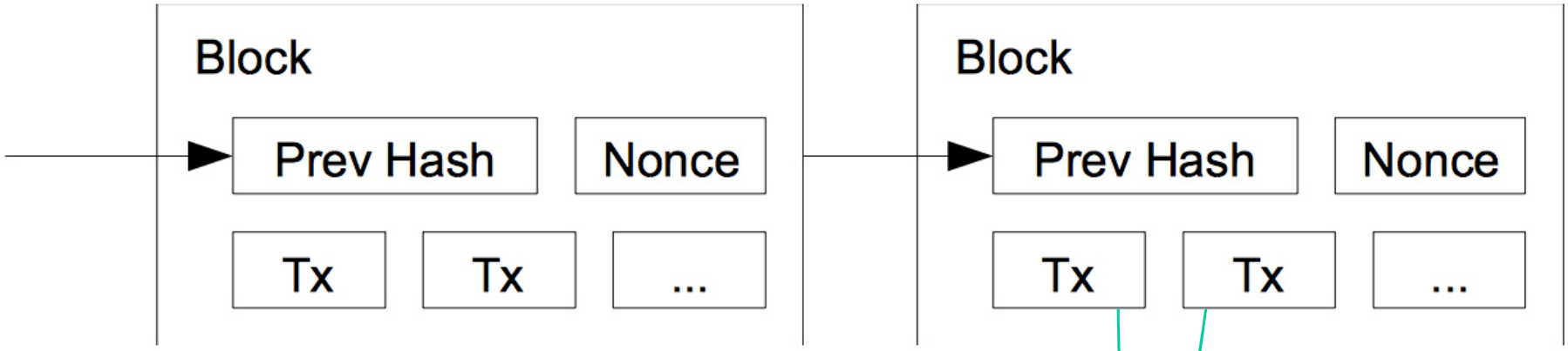


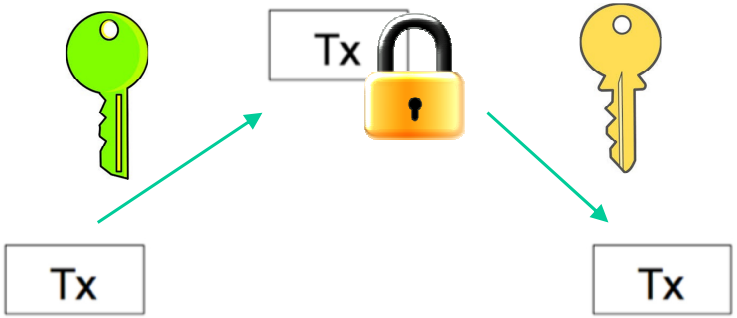


Blockchain: *Transaction* (Tx)

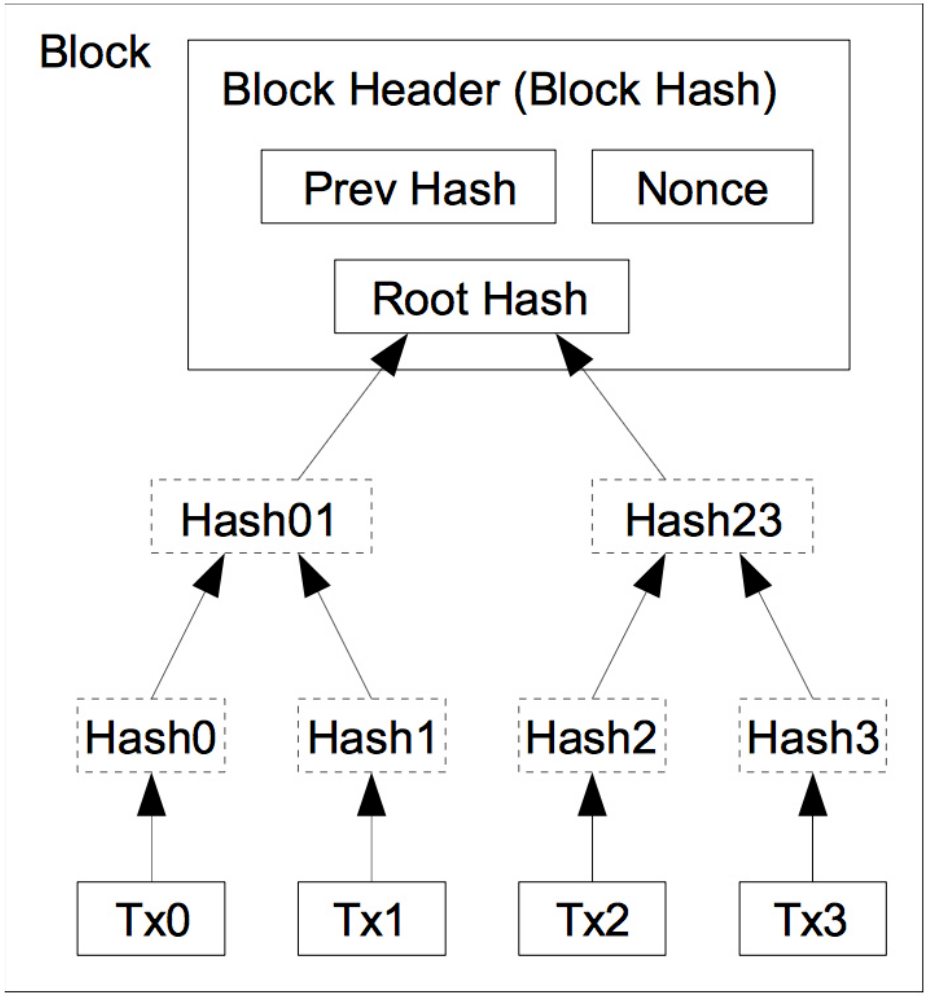


Blockchain: *Transaction* (Tx)

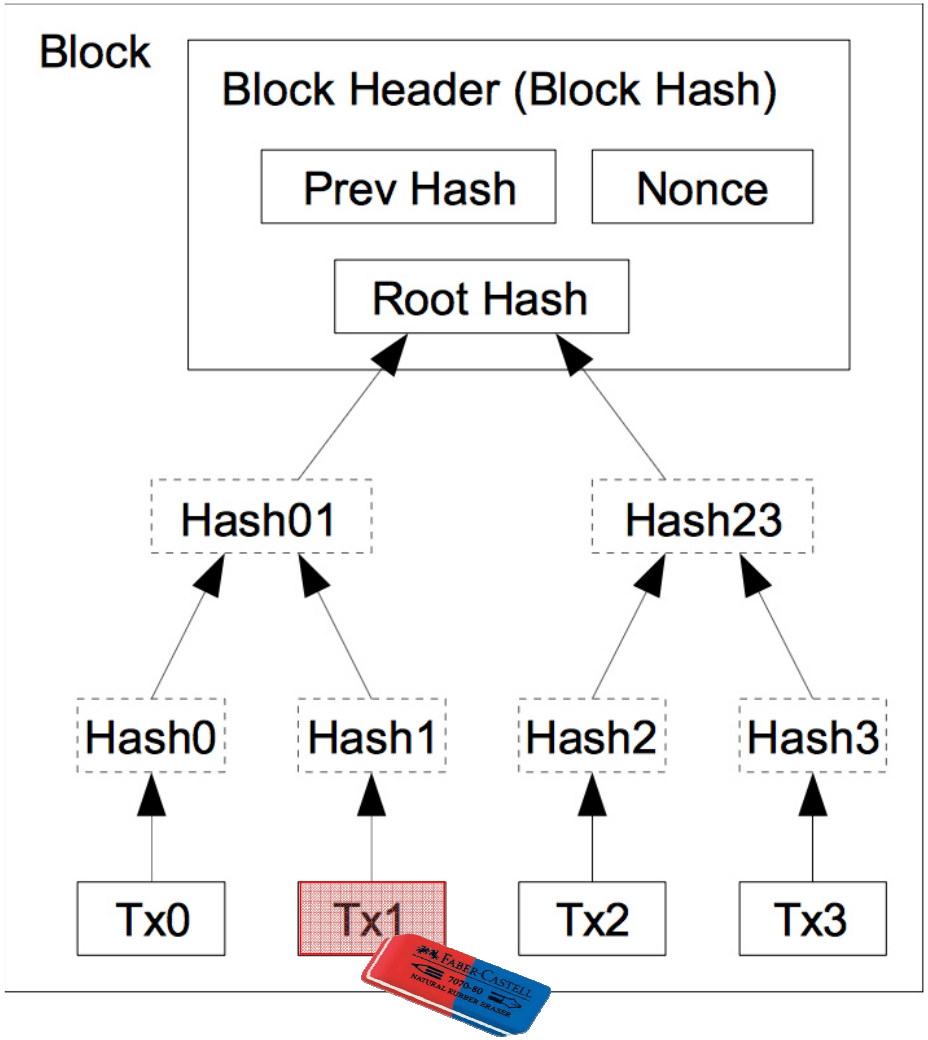




Comment organiser les Txs?



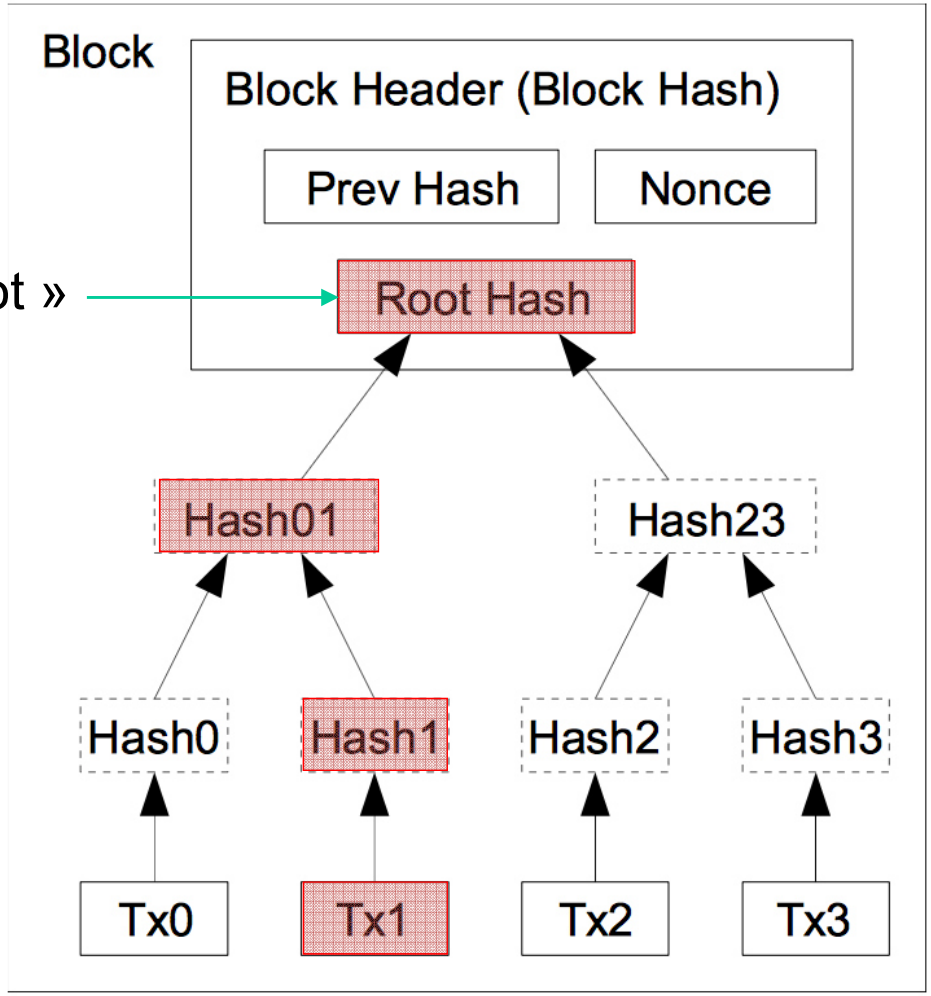
Comment organiser Txs?



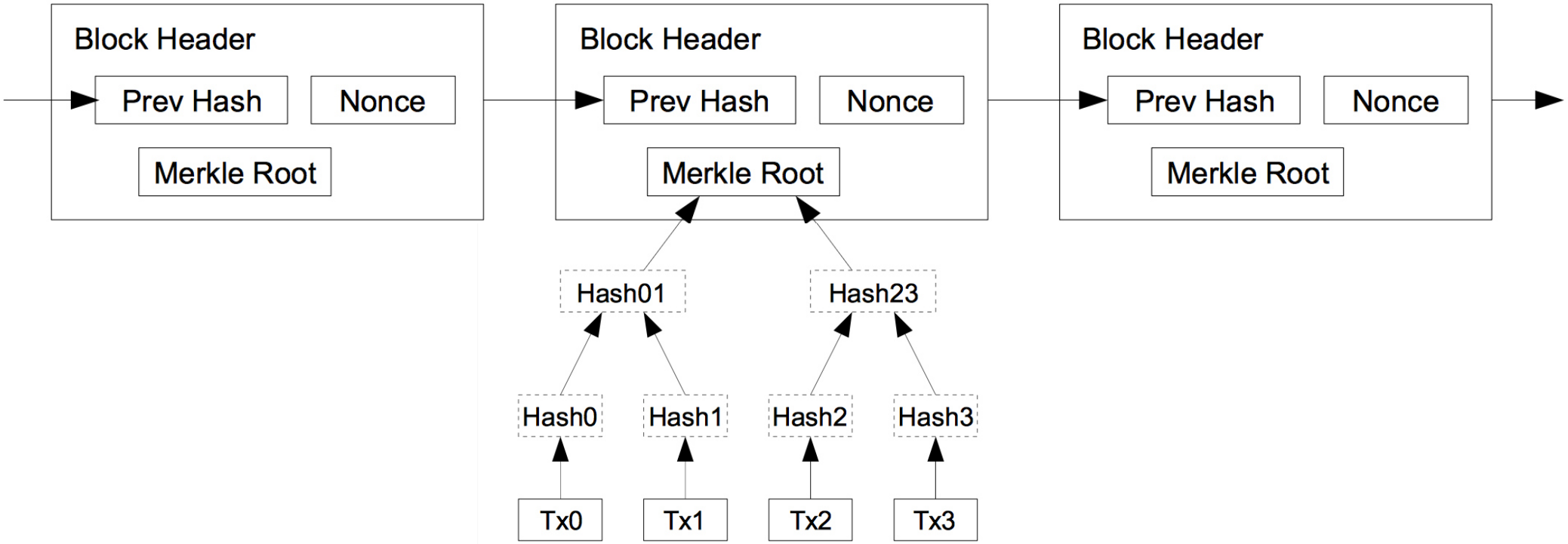
Comment organiser Txs?

Merkle tree:

« Merkle root »



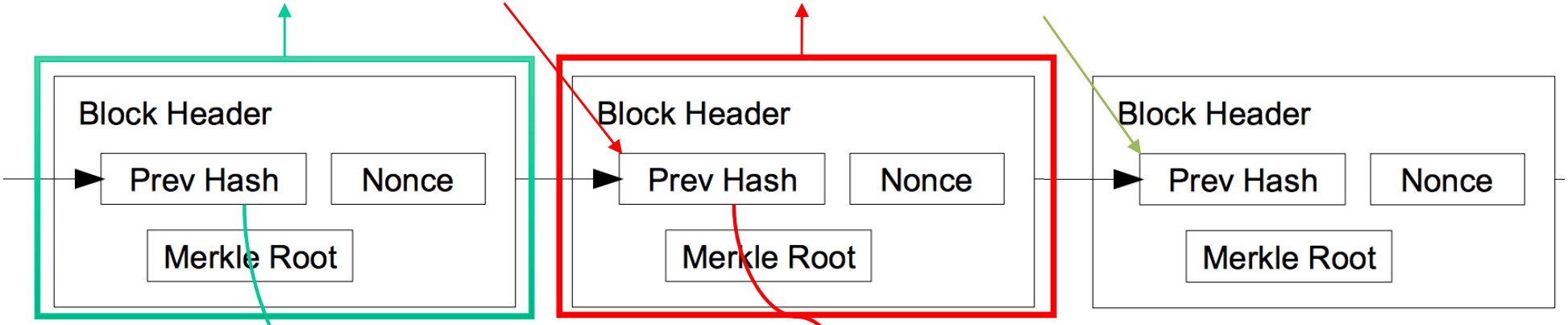
Blockchain: *Transaction* (Tx)

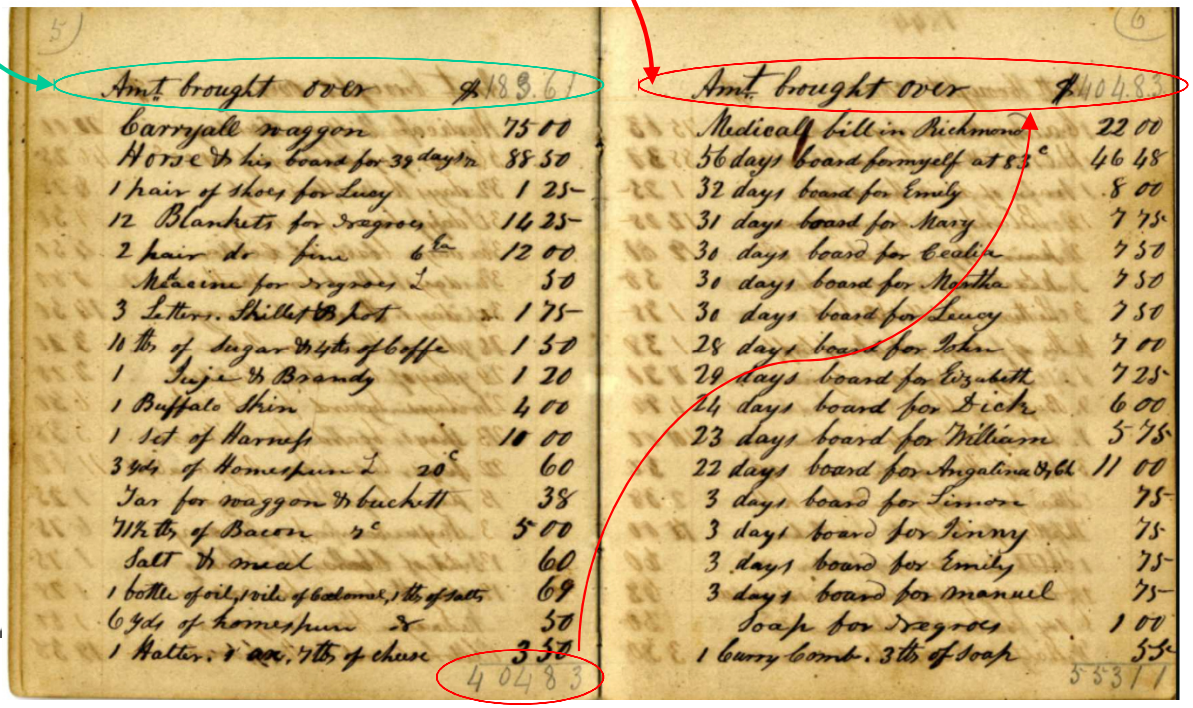


Blockchain: *Prev Hash*

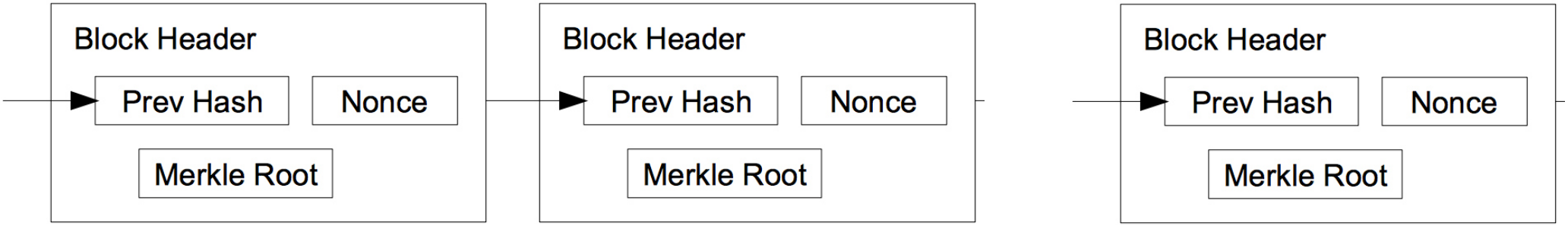
000000000000000d09d04db816e84
af4e3616db1d0694b13ab86f49fd251bf

000000000000000000510934345a8d2
af724565862bcb4ee512023ecce27fa61



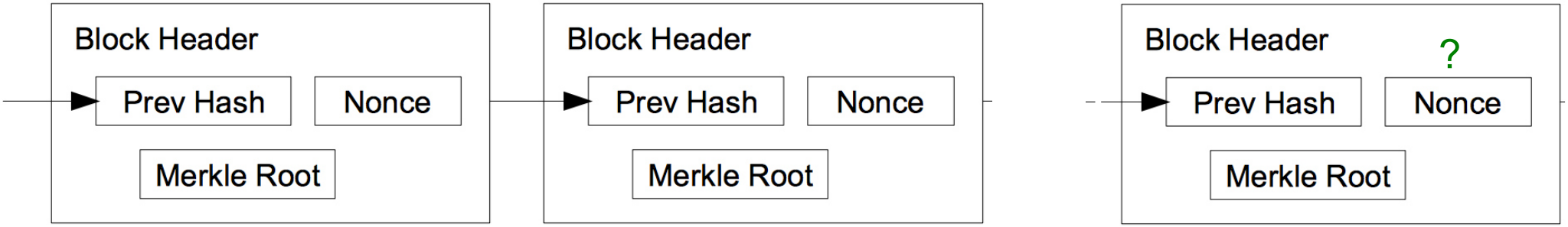


Blockchain: *Nonce*



- Qui décide quand ajouter un nouveau block?
- Consensus: *Proof of Work (Mining)*

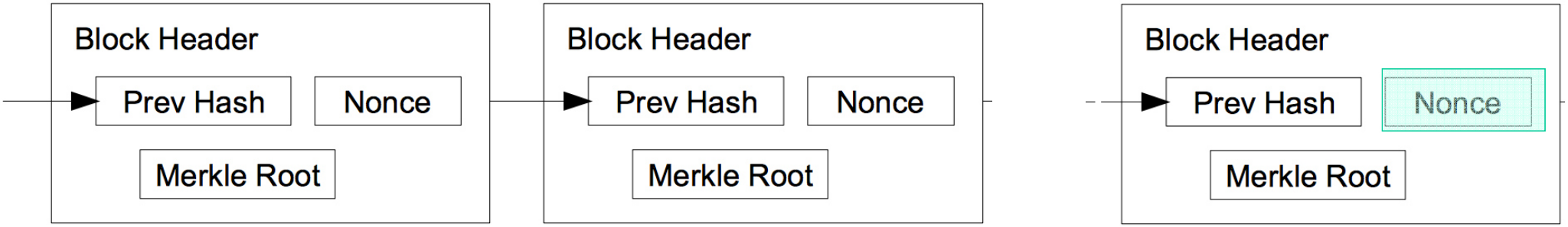
Blockchain: *Nonce*



000000000000000000…

- Qui décide quand ajouter un nouveau block?
- Consensus: *Proof of Work (Mining)*

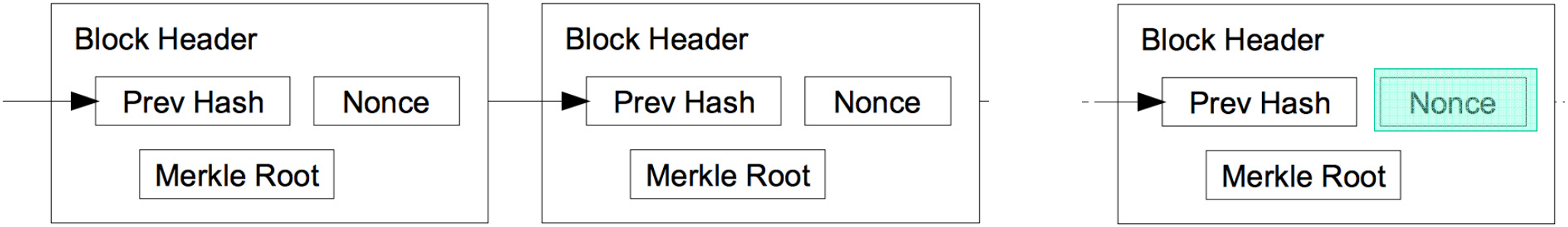
Blockchain: *Nonce*



Nonce= 1

44c8216c1c32ce64ee115aa5715f21f2280
68ccc2e717978874c463ba0f1447

Blockchain: *Nonce*



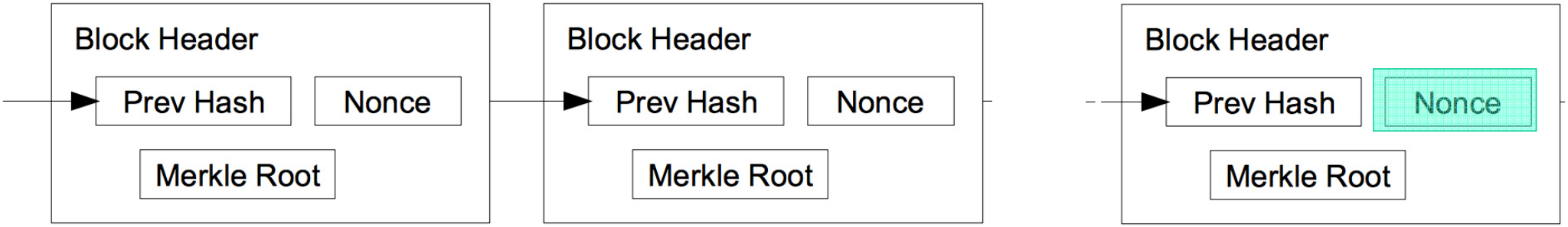
Nonce= 1

44c8216c1c32ce64ee115aa5715f21f2280
68ccc2e717978874c463ba0f1447

Nonce= 2

d61d04d716dcfb0c37e2cd499a026025b2
51cb43690e6a9e216c055aca7b90d3

Blockchain: *Nonce*



Nonce= 1

44c8216c1c32ce64ee115aa5715f21f2280
68ccc2e717978874c463ba0f1447

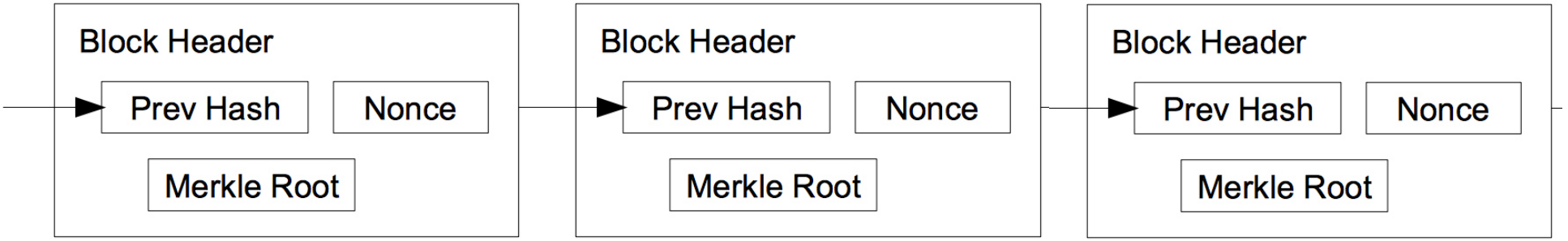
Nonce= 2

d61d04d716dcfb0c37e2cd499a026025b2
51cb43690e6a9e216c055aca7b90d3

Nonce= 80

082522dcfd3dc03eef67cae85dfaeaa09e8
c4c33d6a1ff14b3679ab28d2c09ea

Blockchain: *Nonce*



Nonce= 1

44c8216c1c32ce64ee115aa5715f21f2280
68ccc2e717978874c463ba0f1447

Nonce= 2

d61d04d716dcfb0c37e2cd499a026025b2
51cb43690e6a9e216c055aca7b90d3

Nonce= 80

082522dcfd3dc03eef67cae85dfaeaa09e8
c4c33d6a1ff14b3679ab28d2c09ea

Nonce= 2'164'485'429

0000000000000001358e5dd3135e48a
3f74139bad5d09cb26583eac5fbe09c

Bitcoin blockchain

LATEST BLOCKS

SEE MORE →

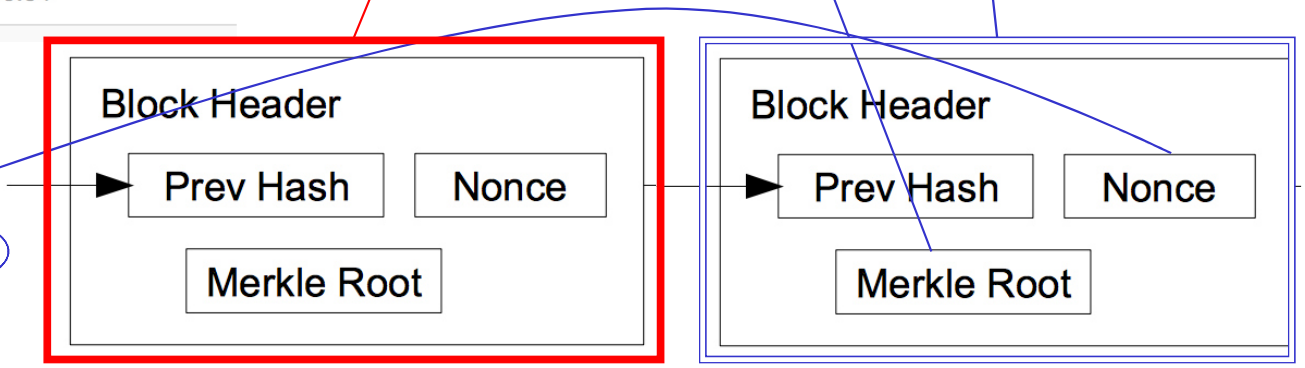
Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
466539	2 minutes	2275	25,480.52 BTC	AntPool	998.09
466538	14 minutes	2229	5,206.52 BTC	BW.COM	998.05
466537	14 minutes	2160	45,184.11 BTC	AntPool	998.19
466536	18 minutes	2105	29,219.12 BTC	AntPool	998.18

Bitcoin blockchain

Block #466523

Summary	
Number Of Transactions	1530
Output Total	11,604.71011584 BTC
Estimated Transaction Volume	1,307.03484249 BTC
Transaction Fees	1.48656223 BTC
Height	466523 (Main Chain)
Timestamp	2017-05-15 10:58:28
Received Time	2017-05-15 10:58:28
Relayed By	BitClub Network
Difficulty	559,970,892,890.84
Bits	402781863
Size	998.147 KB
Version	4
Nonce	2164485429
Block Reward	12.5 BTC

Hashes	
Hash	00000000000000001358e5dd3135e48a3f74139bad5d09cb26583eac5fbe09c
Previous Block	000000000000000000510934345a8d2af724565862bcb4ee512023ecce27fa61
Next Block(s)	000000000000000009fca0980074ddab428b353dfe56f074f10df93f9bf6bc8
Merkle Root	cd95446b4c43845f865d48b760e82cd398bb3b5e4b06c3623d04e4ca03fe9e79



Service Notarial

Bitcoin.com Start here | News | Forum | Games Blockchain Cruise

Home › Announcements › Bitcoin.com Launches Blockchain-Based Notary Page

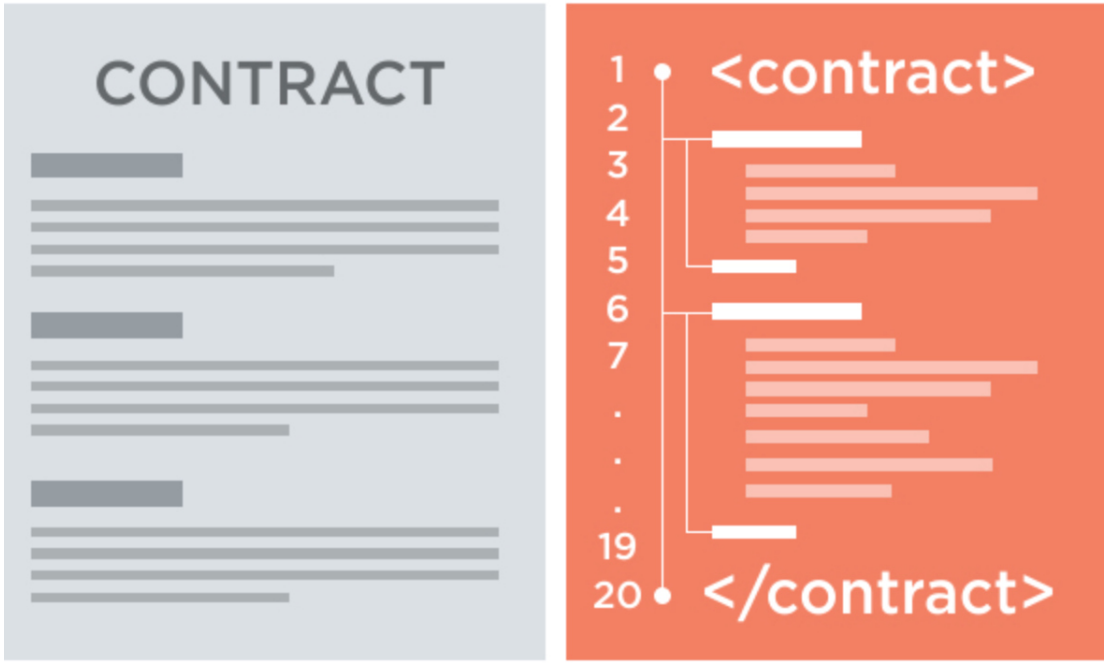
ANNOUNCEMENTS ENCRYPTION PROMOTED POST

Bitcoin.com Launches Blockchain-Based Notary Page

By ***Sterlin Lujan*** - April 15, 2017 13459 8

SHARE Facebook Twitter G+

Smart Contract



« un programme qui contrôle directement des actifs numériques » (V. Buterin)

Blockchain Publique

- n'importe qui peut lire et ajouter les transactions dans le registre, peut participer au consensus

  - Consensus: Proof of Work (PoW) (PoStake, PoBurn)
  - Crypto-monnaie
  - Les nodes anonymes
  - «Smart contracts» (contracts intelligents)

bitcoin

ethereum

Blockchain Privé

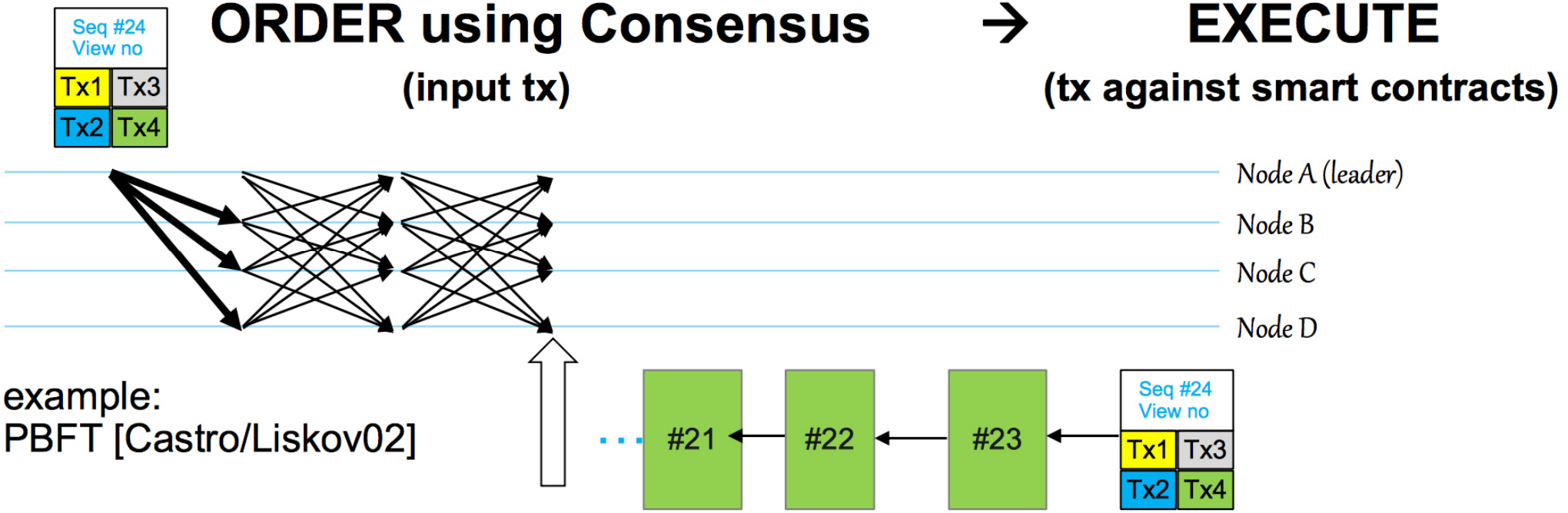
THE LINUX FOUNDATION

HYPERLEDGER PROJECT

- le consensus est contrôlé par un groupe d'utilisateurs pré-sélectionné.

PBFT

- Consensus utilisé dans la blockchain privée (Hyperledger v0.6)



Avantages

- Pas de point unique de défaillance
- Pas besoin de notion de confiance entre les acteurs
- Transparence et immutabilité à chaque étape

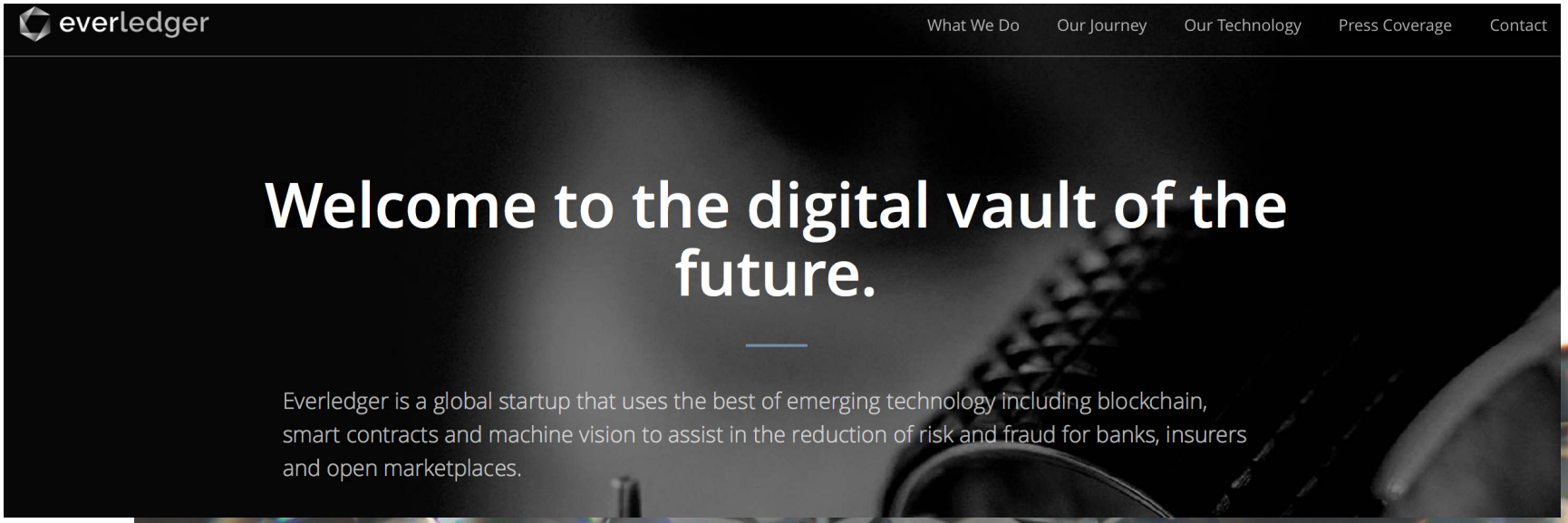
Le Plan de la Presentation

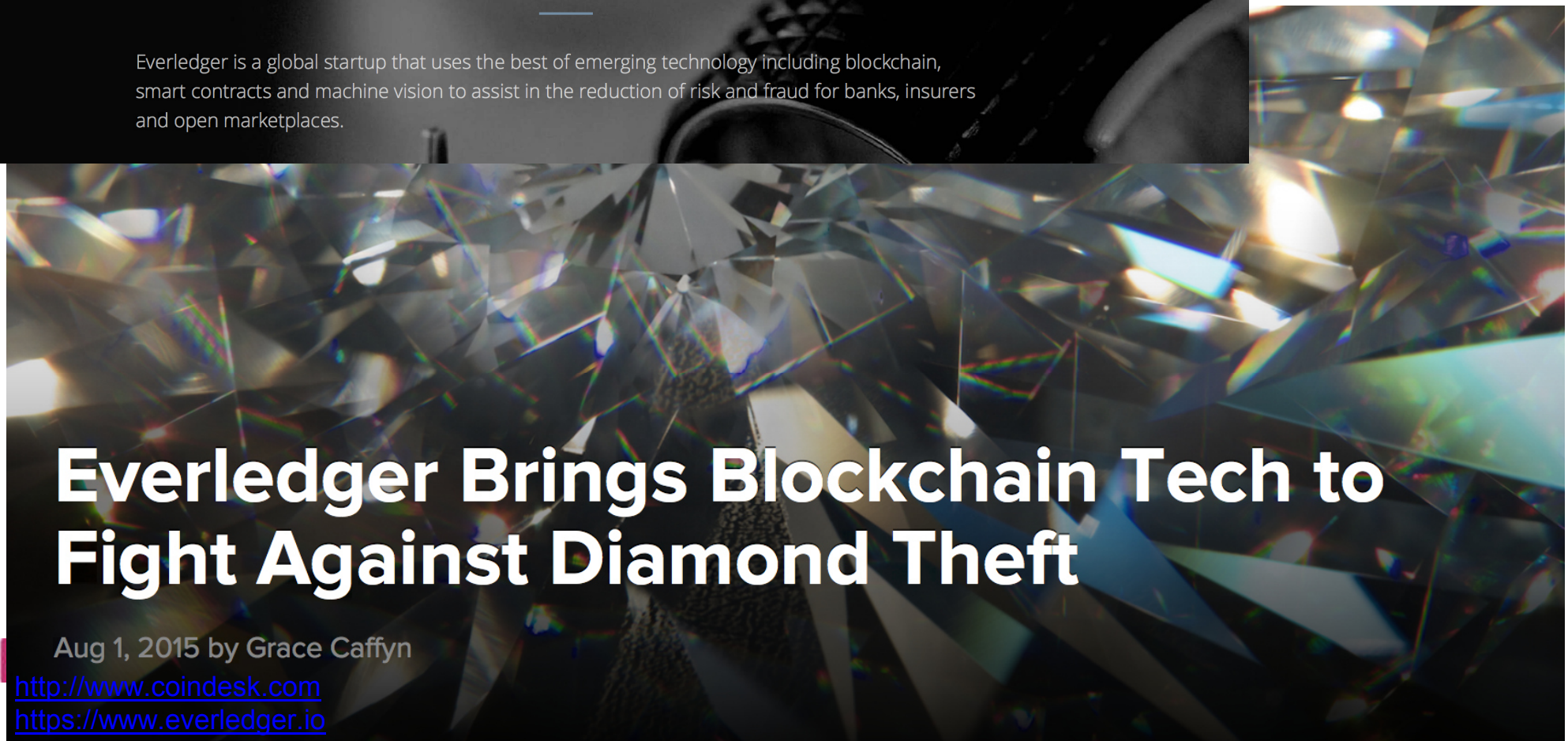
- La blockchain, qu'est-ce que c'est ?
- **Utilisation de la technologie blockchain**
- Les aspects organisationnels et les questions ouvertes

eGouvernement

http://www.coindesk.com
http://www.bitland.world/about/

Everledger



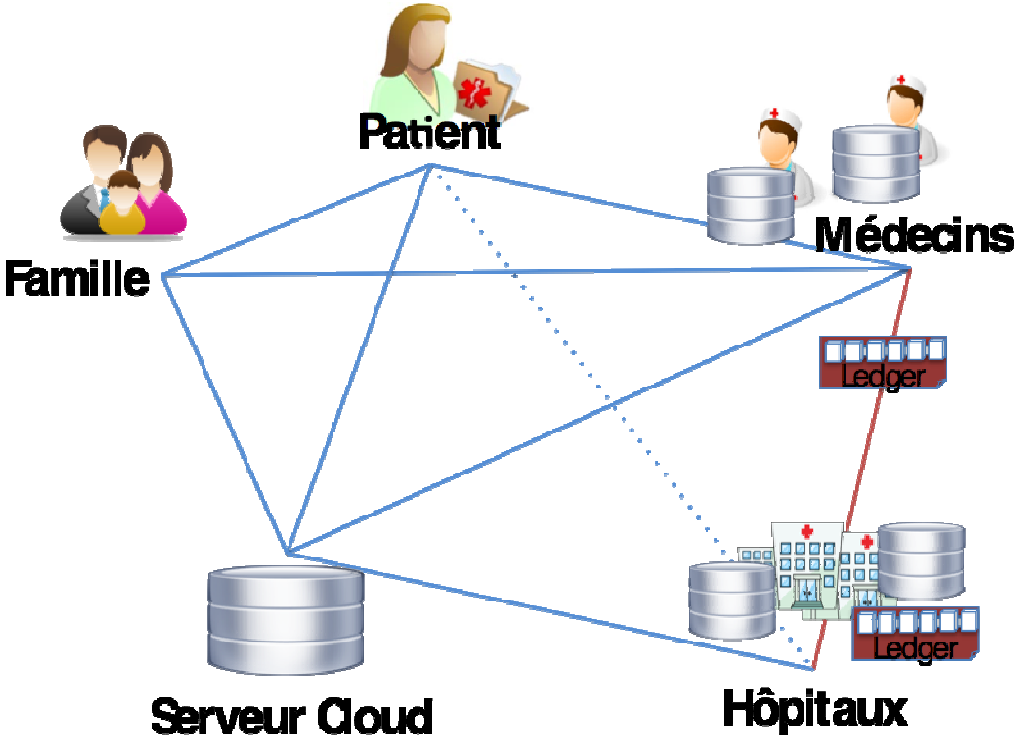


http://www.coindesk.com
https://www.everledger.io

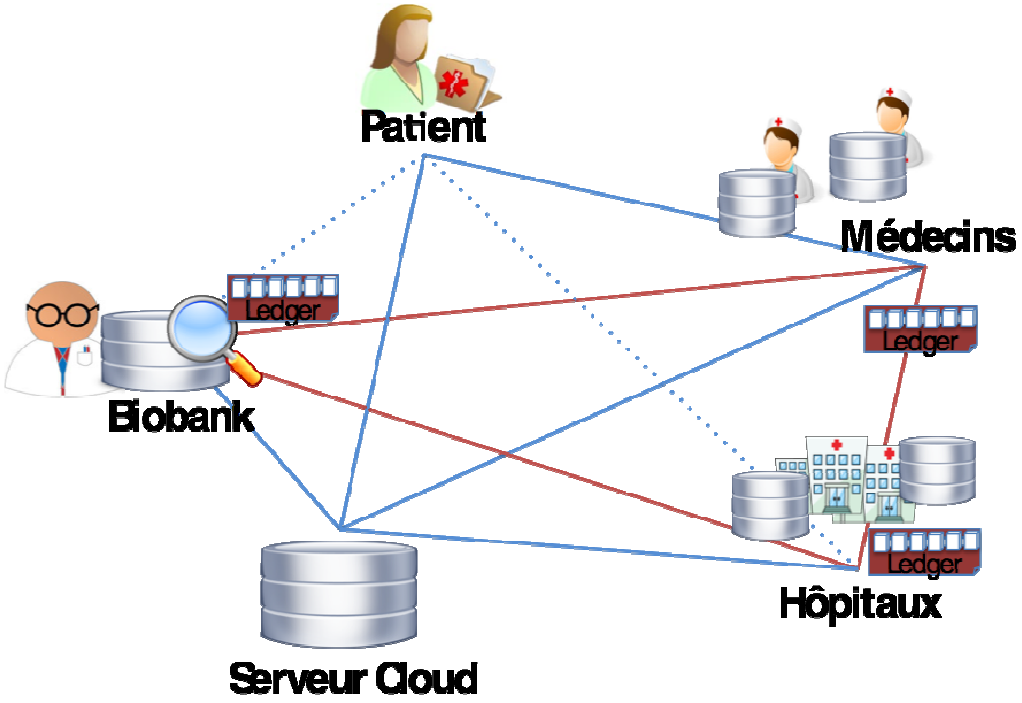
Pourquoi l'eSanté a Besoin de la Blockchain ?

- Données médicales:
  - de grandes valeurs et très sensibles,
  - dispersées entre les acteurs du système de santé.
- Partage des données:
  - autorisation du patient (consentement),
  - anonymisation.
- Gestion des maladies chroniques et conditions graves.

Applications dans l'eSanté

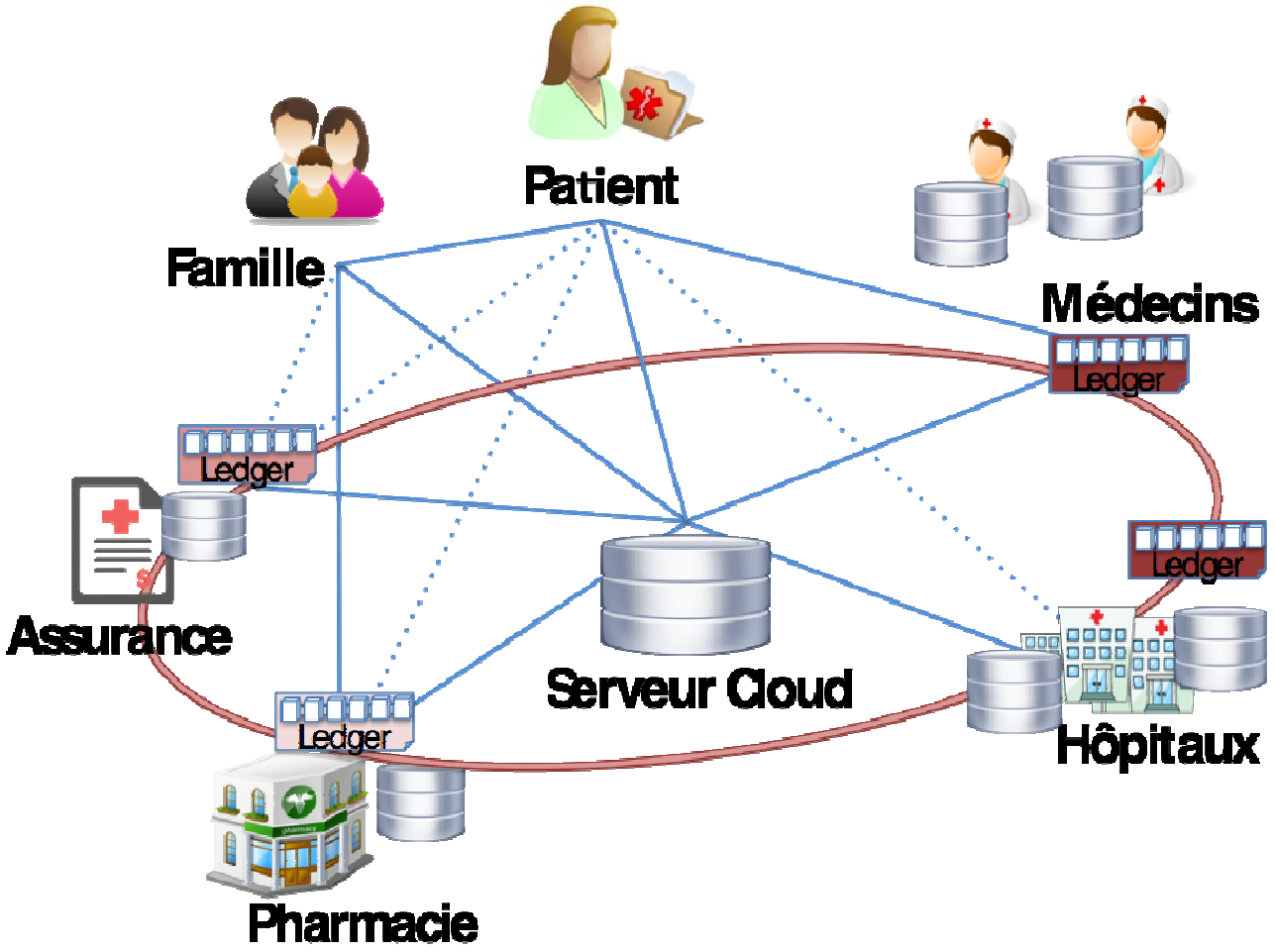


Traitement quotidien



Collecte de données
pour la recherche scientifique

eSanté connectée



eSanté

- **GemOS:** une *platforme «générale»* pour créer des applications *basées sur la blockchain*
- **Guardtime:** technologie basée sur *KSI (Infrastructure de signatures sans clé)*

guardtime

- **MedREC***:* système decentralisé pour la gestion des dossiers médicaux basé sur la *blockchain public*

Gem

The blockchain company for healthcare and supply chain.

Le Plan de la Presentation

- La blockchain, qu'est-ce que c'est ?
- Utilisation de la technologie blockchain
- **Les aspects organisationnels et les questions ouvertes**

Les aspects organisationnels pour l'eSanté

- Qui contrôle le Service des membres?
- Comment gérer les clés privées
- Adoption de la blockchain

Les aspects organisationnels pour l'eSanté

- Qui contrôle le Service des membres?
- Comment gérer les clés privées
- Adoption de la blockchain
- Audit
- Affaires juridiques dans le domaine médical

Questions ouvertes

- Qui est propriétaire de la blockchain?
- Aucune base juridique
- Besoin d'un traité international (aspects transfrontaliers)

Questions ouvertes

- Qui est propriétaire de la blockchain?
- Aucune base juridique
- Besoin d'un traité international (aspects transfrontaliers)
- Vérification des smart contracts
- Nouveaux risques à anticiper

Conclusion

- La blockchain est une **nouvelle technologie** basée sur des primitives cryptographiques et les principes d'un réseau distribué
- Des projets pilotes existent, plusieurs pays commencent l'intégration de la blockchain **pour gérer des registres**
- **Besoin d'une base juridique** pour utiliser la technologie, plusieurs questions sont encore ouvertes