
Isabelle C.
CELUI QUI CACHE
SON SECRET
EST MAÎTRE
DE SA ROUTE

Le vrai nom de Satoshi Nakamoto

- En fait, c’est aussi le mot de passe de son compte,
- Donc, celui qui découvre son vrai nom prend possession de ses bitcoins, …
- (Merci, Michaël).

bloc

Blockchains :

Des Incas au futur internet :
Les applications de demain.

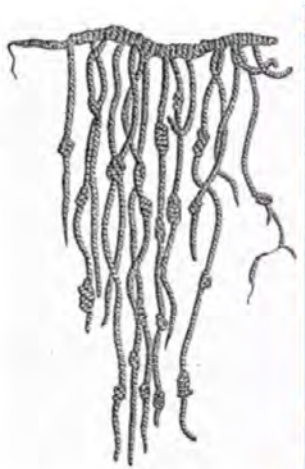
chaîne

?

22 mars
2021

Jean-Jacques Quisquater
UCL, Louvain-la-Neuve: professor em. jjq@uclouvain.be
MIT: research affiliate CSAIL, jjq@mit.edu
Math RiZK, director

MIT Khipu Research Group



The mystery:

The Inka Empire (1438–1533) had its own spoken language, Quechua, which is spoken today by about 10 million people including a third of the Peruvian population. It is believed that the only "written" language of the Inka Empire is a system of different knots tied in ropes that are attached to a longer cord. This system is called *khipu or quipu*. The ropes also have different colors, ply, and attachments, providing additional mechanics for encoding information. There is evidence from the Spanish crusades that khipus encoded census data as well as stories. However, no one knows how to decode either kind of information. There are several hundred khipus in the world today, waiting to be read.

The challenge:

Our research group is trying to break the khipu code: how did the Inkas record language with knots in rope? By combining computation, informatics, mathematics, linguistics, and anthropology, we hope to uncover the khipu mystery.

IAP class:

In January 2007, we ran an IAP class on Knot Language: Recreating Inca Quipu/Khipu, from which this research group was formed.

Videos of some of the lectures will be available here soon.

The group:

Our research group consists of students and faculty from a diverse range of fields and universities:

Faculty:

Samuel Blank	mathematics	Northeastern U.
Carrie Brezine	archaeology	Harvard
Erik Demaine *(cohead)*	computer science	MIT
Martin Demaine *(cohead)*	computer science	MIT
Stefan Langerman	computer science	Free U. Brussels, Belgium
Jean-Jacques Quisquater	electrical engineering	Catholic U. Louvain, Belgium
Gary Urton	archaeology	Harvard

Students and postdocs:

Kunal Agrawal	computer science	MIT
Scott Ananian	computer science	MIT
Nyls Braak	computer science	MIT
Edwin Chen	mathematics	MIT
Suzanne Dermine	computer science	Catholic U. Louvain, Belgium

Pourquoi ?

- 2007-2008 Séverine Gérard Essai de décryptage des cordelettes Quipus utilisées par les anciens Incas comme moyen de communication : Un exemple d'ethno-cryptographie

  Travail de fin d'études défendu pour l'obtention du titre d'ingénieur civil en mathématiques appliquées

- 2006-2007 Olaf Witowski Essai de décryptage des cordelettes Quipus utilisées par les anciens Incas comme moyen de communication : Un exemple d'ethno-cryptographie

  Travail de fin d'études défendu pour l'obtention du titre d'ingénieur civil en informatique

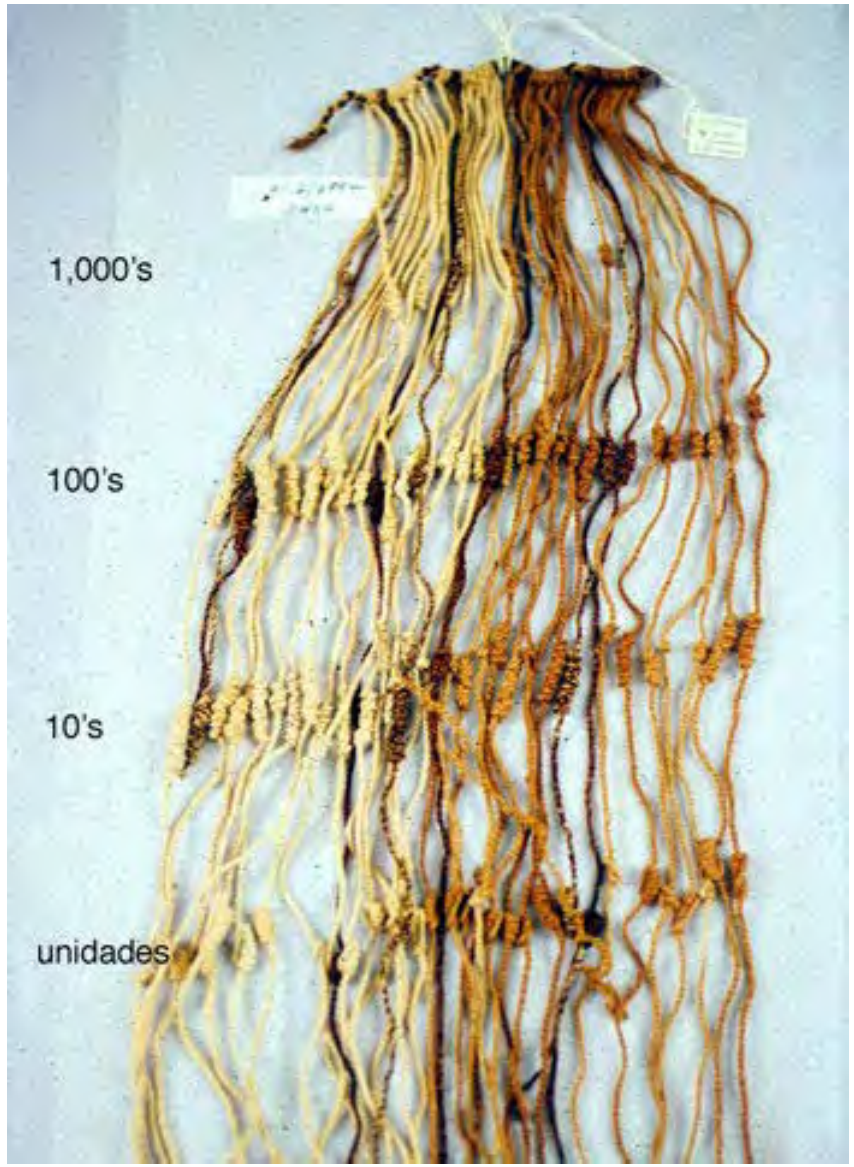
- 2006-2007 Suzanne Dermine Essai de décryptage des cordelettes Quipus utilisées par les anciens Incas comme moyen de communication : Un exemple d'ethno-cryptographie

  Travail de fin d'études défendu pour l'obtention du titre d'ingénieur civil en mathématiques appliquées

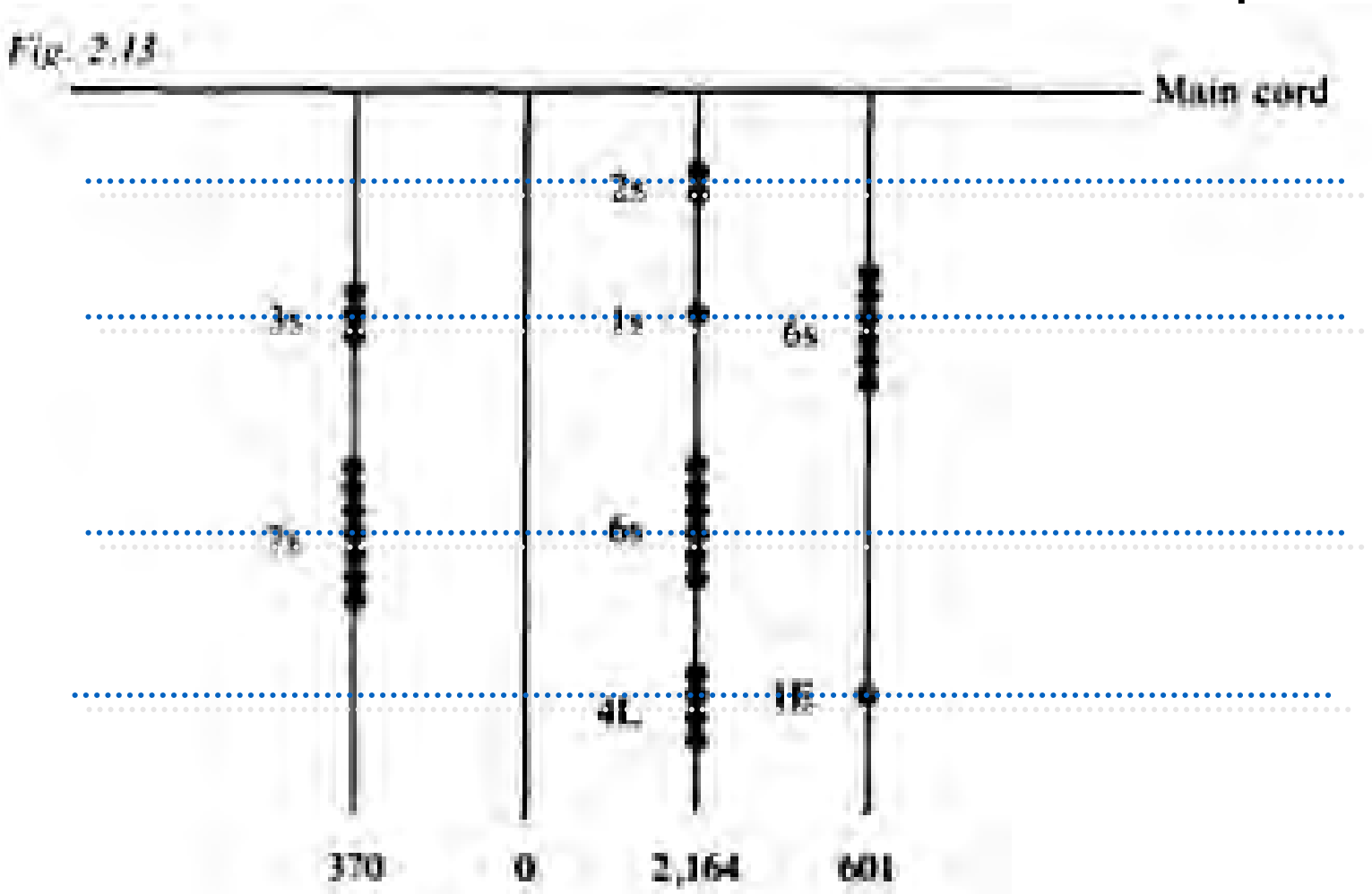
- 2006-2007 Vincent Castus Essai de décryptage des cordelettes Quipus utilisées par les anciens Incas comme moyen de communication : Un exemple d'ethno-cryptographie

  Travail de fin d'études défendu pour l'obtention du titre d'ingénieur civil en électricité

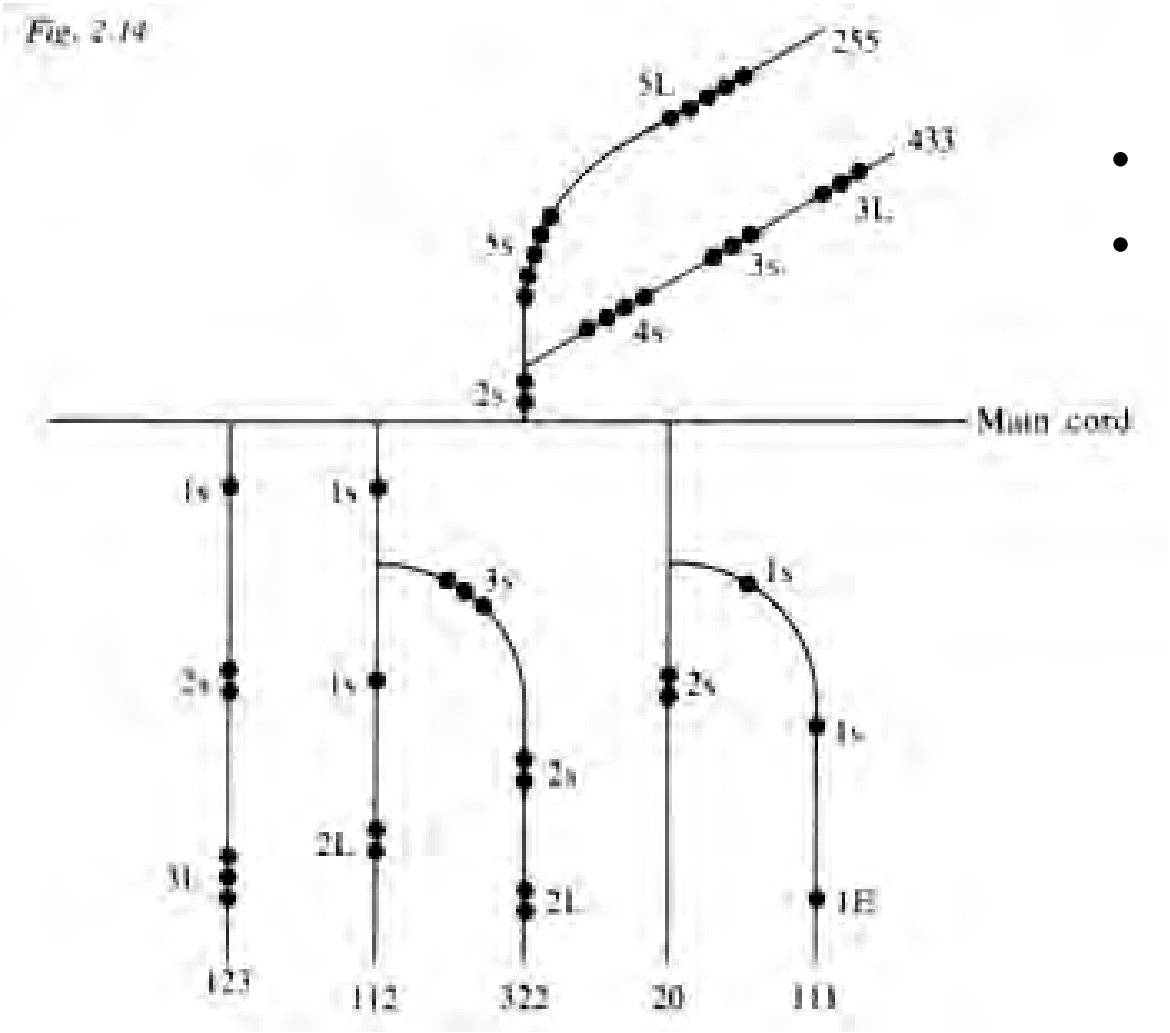

MUSEO NACIONAL
DE ARQUEOLOGIA, ANTROPOLOGIA
E HISTORIA DEL PERU
INC
Instituto
Nacional
de Cultura
Simposio
15·16·17
enero
2009
Quipu
y Tocapu
Programa
Qhapaq Ñan


1,000's
100's
10's
unidades

exemples



Pendants – cordes subsidiaires – cordes supérieures



- 123 + 112 + 20
- 322 + 111

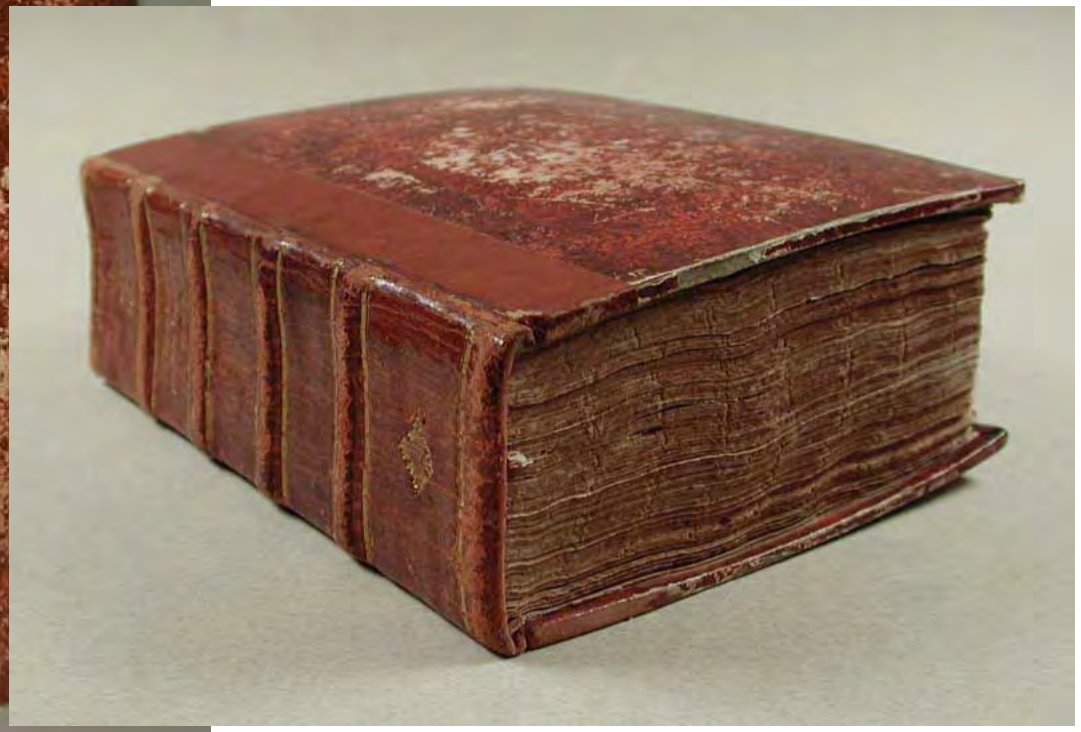
http://www.anthropology.wisc.edu/chaysimire/titulo2/galeria/foto26.htm
(from Tupicocha: ad hoc invented tradition?)

the house of the khipus, Kaha Wayi (‘Treasury House’ or ‘Counting House’).

- Rapaz’s unique patrimony consists of a walled precinct containing the structures that once made up a system of control of community resources using traditional Andean technology. This center consisted of a storage building called Pasa Qullqa in Quechua (‘Seasonal Storehouse’), and the house of the khipus, Kaha Wayi (‘Treasury House’ or ‘Counting House’).

http://www.khipurapaz.org/ingles.htm

12 pages mentionnent les quipus



Comment enregistrer le temps ?

- Cadran solaire, horloge,
- Synchronisation ?
- Enregistrement ?
- Ordre des arrivées ?
- À voir !

of grid, of management, …

… of grid, of management, …

Une mouche vole
…
ESSAYONS !

6 novembre 2015 :

la couverture qui a changé la perception du bitcoin
pour en découvrir la blockchain

6 novembre 2015 :

la couverture qui a changé la perception du bitcoin
pour en découvrir la blockchain

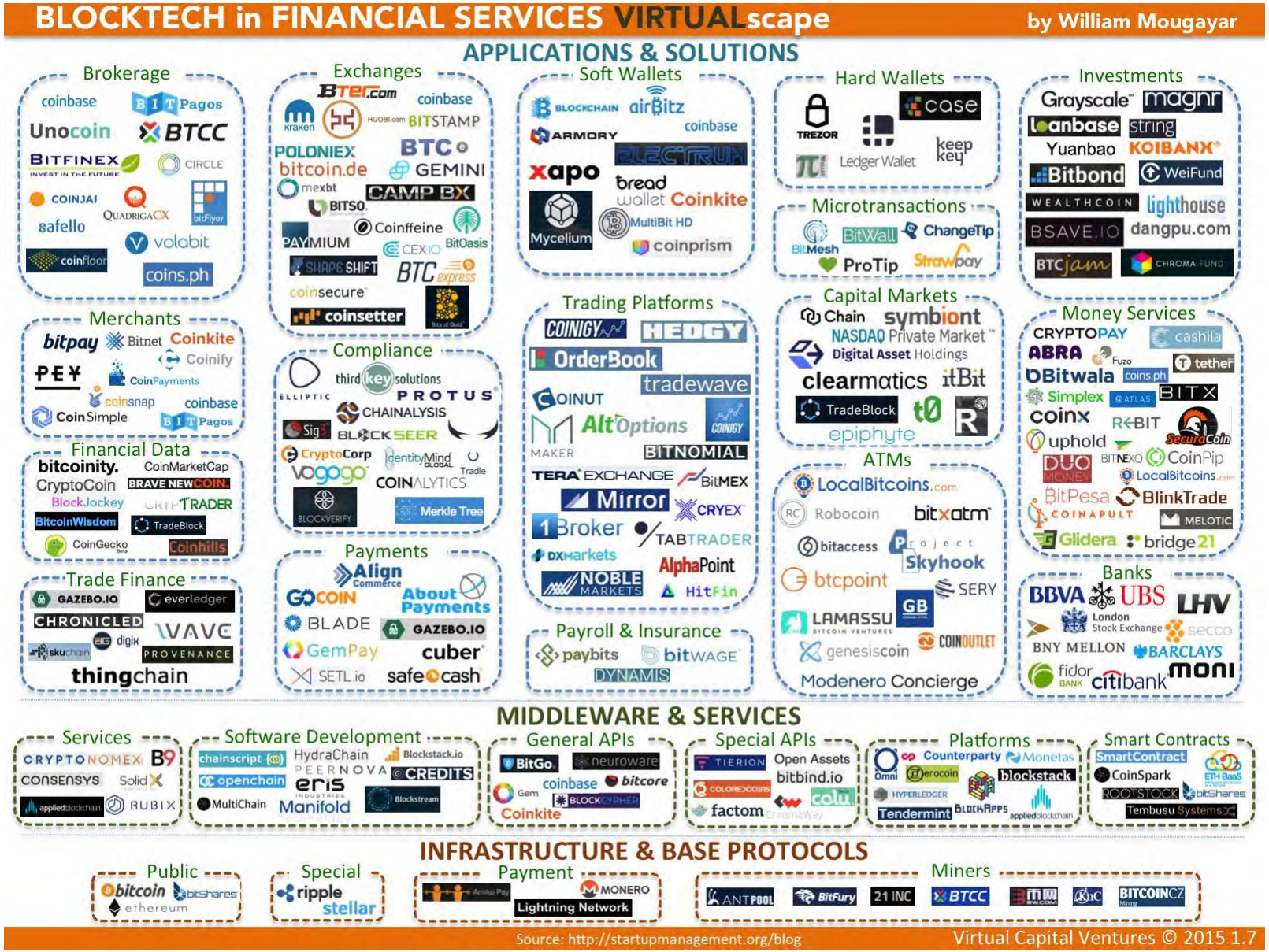
Introduction et contexte : comment s'y retrouver ?

Un écosystème florissant

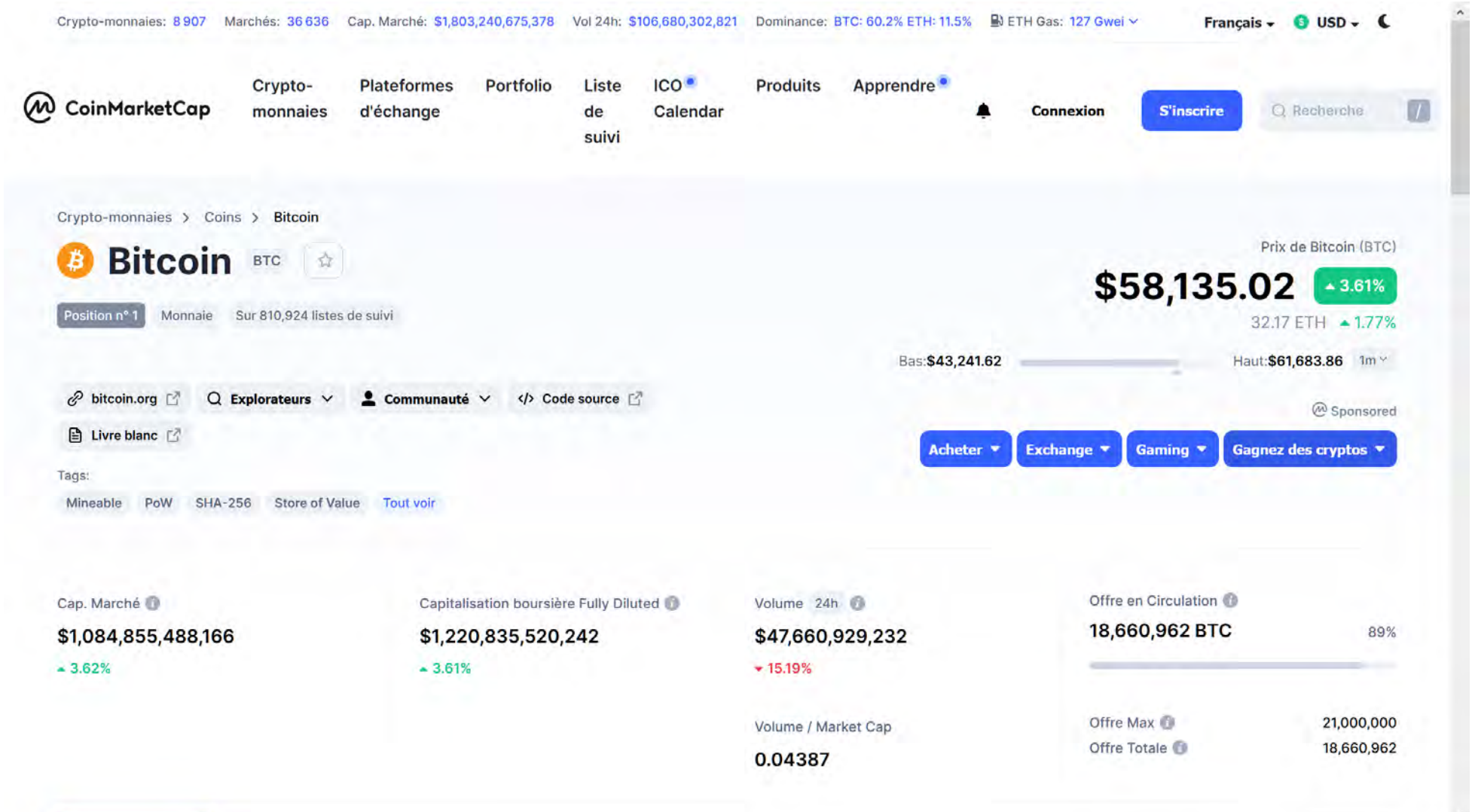
Des acteurs débutants et peu compétents mais avides

Un sujet valable

Évitons les catastrophes pour garder le meilleur



Un bitcoin valait 20.036 $ US … (17/12/2017) alors qu'il valait 1000 $ US au 1/1/2017 …
une monnaie sur internet, autonome,



Bitcoin BTC

Position n° 1 | Monnaie | Sur 810,924 listes de suivi

Prix de Bitcoin (BTC)

$58,135.02 ▲ 3.61%

32.17 ETH ▲ 1.77%

Bas:$43,241.62 — Haut:$61,683.86 1m

bitcoin.org | Explorateurs | Communauté | Code source | Livre blanc

Tags: Mineable | PoW | SHA-256 | Store of Value | Tout voir

Cap. Marché
$1,084,855,488,166
▲ 3.62%

Capitalisation boursière Fully Diluted
$1,220,835,520,242
▲ 3.61%

Volume 24h
$47,660,929,232
▼ 15.19%

Volume / Market Cap
0.04387

Offre en Circulation
18,660,962 BTC 89%

Offre Max 21,000,000
Offre Totale 18,660,962

Price | Market Cap | TradingView

1D 7D 1M 3M 1Y YTD ALL LOG

USD BTC

Want more data? Check out our API

Bitcoin

USD
United States Dollar

Historique des prix BTC

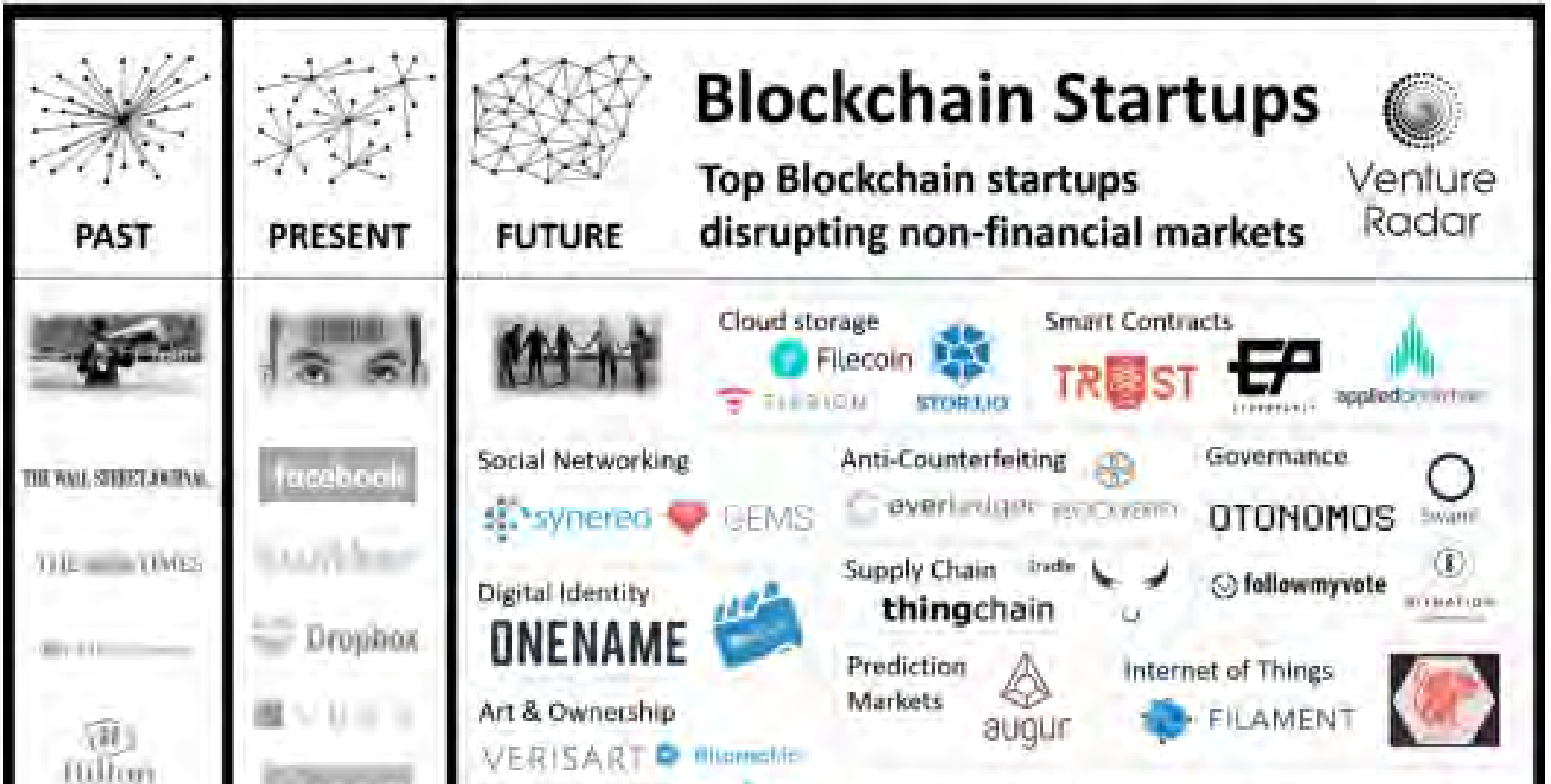
Bitcoin Prix aujourd'hui

Prix de Bitcoin	**$58,157.83**
Évolution du prix 24h	$1,912.81 3.40%
Étendue intrajour des prix	$56,066.93 / $58,471.48
Volume d'échange 24h	$47,690,606,893.93 15.42%
Volume / Market Cap	0.04391
Dominance du marché	60,22%
Rang sur le marché	#1

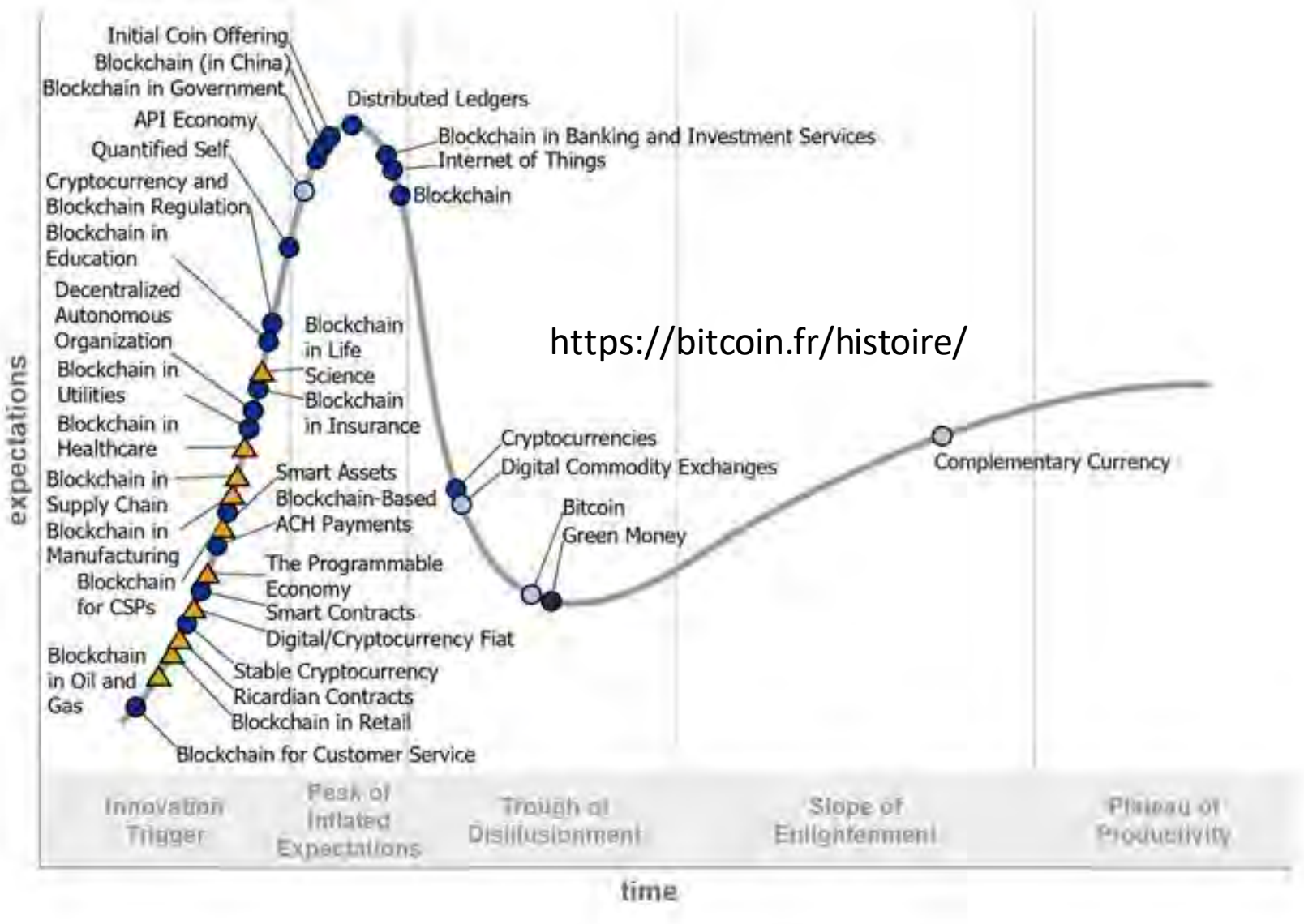
Global Cryptocurrency Charts

Capitalisation Totale Marché

De la centralisation à la décentralisation maîtrisée…



Gardner, inc. : cycle du hype blockchain ?
Comment gérer une bulle pour être productif ?



L’histoire de bitcoin : https://bitcoin.fr/histoire/

- **Avant Bitcoin**

- – 1977 : Première description du chiffrement RSA qui utilise une clé publique pour chiffrer et d’une clé privée pour déchiffrer des données confidentielles.
- – 1979 : Ralph Merkle invente le mécanisme de compression par l’arbre de Merkle, ou Merkle Tree compression mechanism. Il est utilisé pour stocker et vérifier un grand volume de données efficacement et de manière sécurisée, et employé par le protocole Bitcoin pour calculer la racine de Merkle de toutes les transactions contenues dans un bloc de données.
- – 1990 : Le mathématicien américain David Chaum invente DigiCash une monnaie électronique (centralisée et propriétaire) basée sur des protocoles cryptographiques.
- – 1991 : Dans un article intitulé How to Time-stamp a Digital Document, cité par Satoshi Nakamoto dans son livre blanc, Stuart Haber et W. Scott Stornetta énoncent les principes de ce qu’on nommera plus tard une chaine de blocs.
- – 1992 : Scott Vanstone (Certicom) propose l’algorithme ECDSA (Elliptic curve digital signature algorithm) qui utilise des clés plus courtes et permet des opérations de signature et de chiffrement plus rapides qu’RSA.
- – 1994 : Nick Szabo avance l’idée de smart contract, protocole de transaction informatique qui exécute les termes d’un contrat.
- – 18 juin 1996 : la NSA publie un rapport intitulé « Comment produire de la monnaie : la cryptographie du cash électronique anonyme ».
- – 1997 : Adam Back, qui deviendra 12 ans plus tard le premier interlocuteur de Satoshi Nakamoto, invente Hashcash, un système de preuve de travail. L’idée avait cependant déjà été explorée par Cynthia Dwork et Moni Naor dans un rapport intitulé Pricing via Processing or Combatting Junk Mail publié en 1993, mais Adam Back n’avait pas eu connaissance de ces travaux.
- – 1998 : Faillite de DigiCash. Wei Dai lance l’idée d’un cash numérique basée sur un registre distribué sur la liste de diffusion the cypherpunks.
- – 1999 : L’économiste Milton Friedman prévoit la création prochaine d’un e-cash fiable permettant de réaliser des transactions anonymes sur Internet.
- – Mai 1999 : Henri Massias, Xavier Serret-Avila, et Jean-Jacques Quisquater décrivent un service d’horodatage sécurisé sans tiers de confiance. Ce document sera mentionné plus tard dans le livre blanc de Bitcoin.
- – Juin 1999 : Shawn Fanning invente, avec Napster, la technologie pair-a-pair, ou peer-to-peer (P2P) technology. La plateforme de partage de fichiers audio Napster fonctionnait cependant avec un serveur central (appelé farm) qui jouait le rôle d’un registre centralisé de tous les fichiers appartenant à, ou demandés par les pairs. Ce système centralisé constituait le point unique de vulnérabilité (Single Point of Failure-SPOF) de Napster et le site a été fermé par le FBI en 2001 pour violation des droits de propriété intellectuelle.
- – 2000 : Tom Pepper et Justin Frankel développent Gnutella, première plateforme de transfert de fichiers P2P complètement distribuée.
- – 2001 : Publication de The Security Evaluation of Time Stamping Schemes: The Present Situation and Studies de Masashi Une qui parle de « chain of time stamp » et conceptualise un peu plus encore quelque chose qui ressemble à la blockchain (sans le mining).
- – De 1998 à 2005 : Nick Szabo développe le projet BitGold, une monnaie numérique décentralisée basée sur des chaînes infalsifiables de preuves de travail et utilisant beaucoup d’éléments qu’on retrouvera dans Bitcoin : horodatage, signatures numériques, clés publiques… Le système se révèle cependant trop vulnérable aux attaques.
- – 2004 : Développement de Ripplepay, une tentative de système monétaire décentralisé.

En bref, évolution rapide

- Du papier au numérique : internet, web, google, …
- Bitcoin, cryptomonnaie, **blockchain**.
- Un nouvel outil : un nouveau paradigme ? Un nouveau modèle !
- À considérer partout, ne s'applique pas à tout.
- Compétences utiles pour utiliser les blockchains :
  - Finance,
  - Réglementation (RGPD), juridique,
  - Informatique, système distribué, pair à pair,
  - Cryptographie,
  - Management, administration, gouvernement,
  - Risque (analyse de, gestion du), confiance,
  - …

Le vrai départ : bitcoin

- Une monnaie faite de calculs (= minage) comme on extrait de l'or : on parlera de cryptomonnaie car cela utilise la cryptographie. En bref, on dira que c'est de la **crypto**.

- Monnaie digitale, virtuelle, inventée par Satoshi Nakamoto (2008) : avec une solution très élégante pour éviter la double dépense, problème qui a bloqué longtemps l'idée de monnaie numérique,

- La production en est dominée par 4-5 consortia chinois,

- Échanges des bitcoins via une blockchain, l'élément essentiel,

- Un énorme marché, utilisé actuellement pour stocker des valeurs, …, risqué.

Top 100 Crypto-monnaies par capitalisation de marché

The global crypto market cap is $1.80T, a ▲ 3.51% increase over the last day. Lire plus

Alexandria Learning Corner

Take a dive into Elon Musk's fave crypto

New Feature

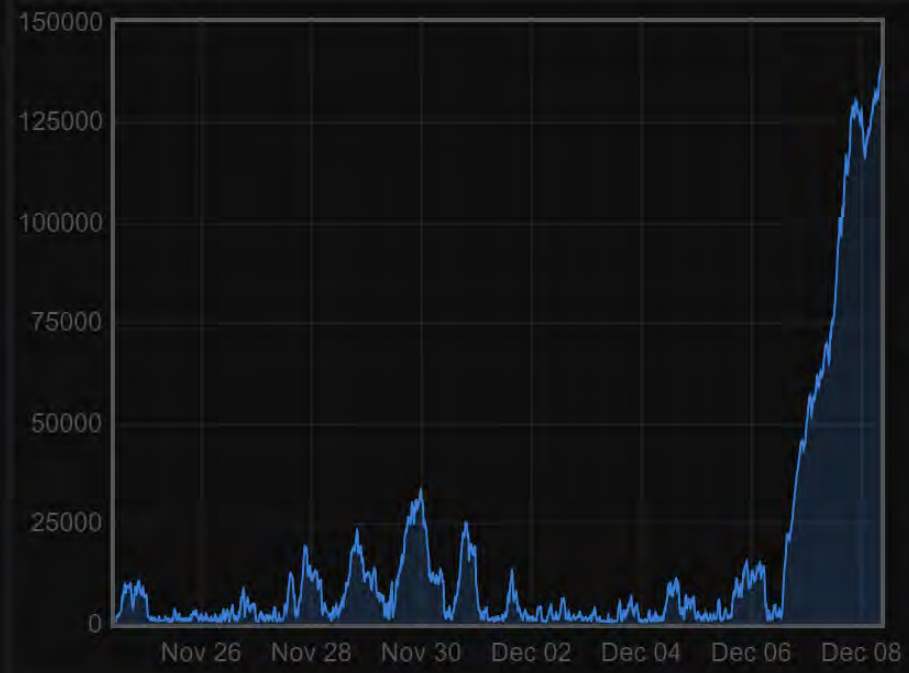
Make the CoinMarketCap homepage your own!

☆ Liste de suivi | Portfolio | Crypto-monnaies | Categories | DeFi | NFT | Polkadot Eco | BSC Eco | Yield Farming | Afficher les rangées 100 | Filtres

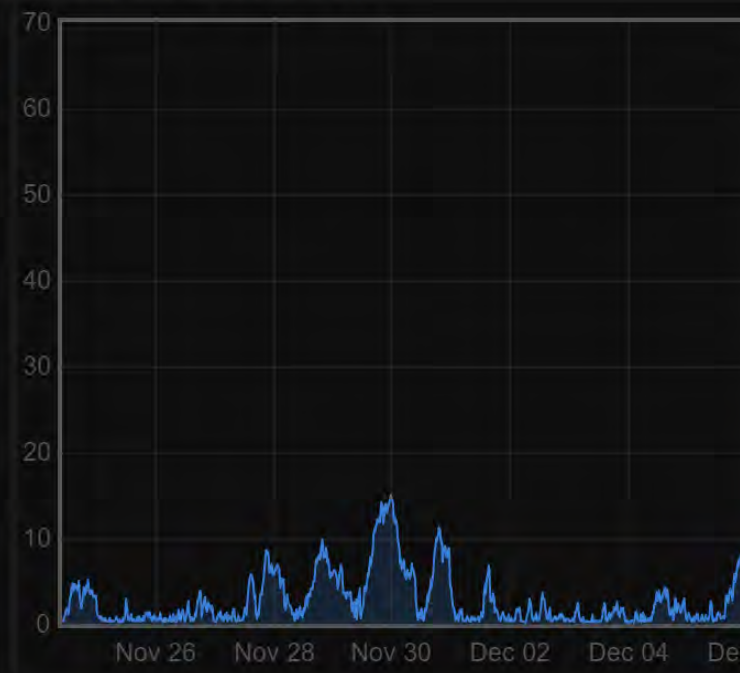
#	Nom	Prix	24h %	7d %	Cap. Marché	Volume (24 h)	Offre en Circulation	7 Derniers Jours
1	Bitcoin BTC	$58,167.17	▲ 3.18%	▲ 3.35%	$1,085,276,599,235	$47,737,043,095 820,822 BTC	18,660,962 BTC	
2	Ethereum ETH	$1,802.12	▲ 1.51%	▲ 1.54%	$207,698,913,570	$19,352,693,178 10,729,574 ETH	115,153,008 ETH	
3	Binance Coin BNB	$267.00	▲ 2.00%	▲ 4.15%	$41,290,872,987	$1,739,988,303 6,511,978 BNB	154,532,785 BNB	
4	Tether USDT	$1.00	▲ 0.08%	▲ 0.09%	$39,583,569,249	$70,986,888,784 70,935,776,066 USDT	39,555,067,876 USDT	
5	Cardano ADA	$1.20	▼ 0.44%	▲ 16.74%	$38,301,249,896	$3,331,833,166 2,779,189,642 ADA	31,948,309,441 ADA	
6	Polkadot DOT	$37.65	▲ 1.62%	▲ 7.28%	$34,703,385,970	$1,576,221,722 41,894,169 DOT	922,376,265 DOT	

Transactions/sec | Connections | Versions | Voting(Bloc

Mempool Transactions | Fee - btc/kB - within n blocks



Mempool Size (MB)



Recent Blocks | Mining Pools - 24h | Avg Block Size

Current Values

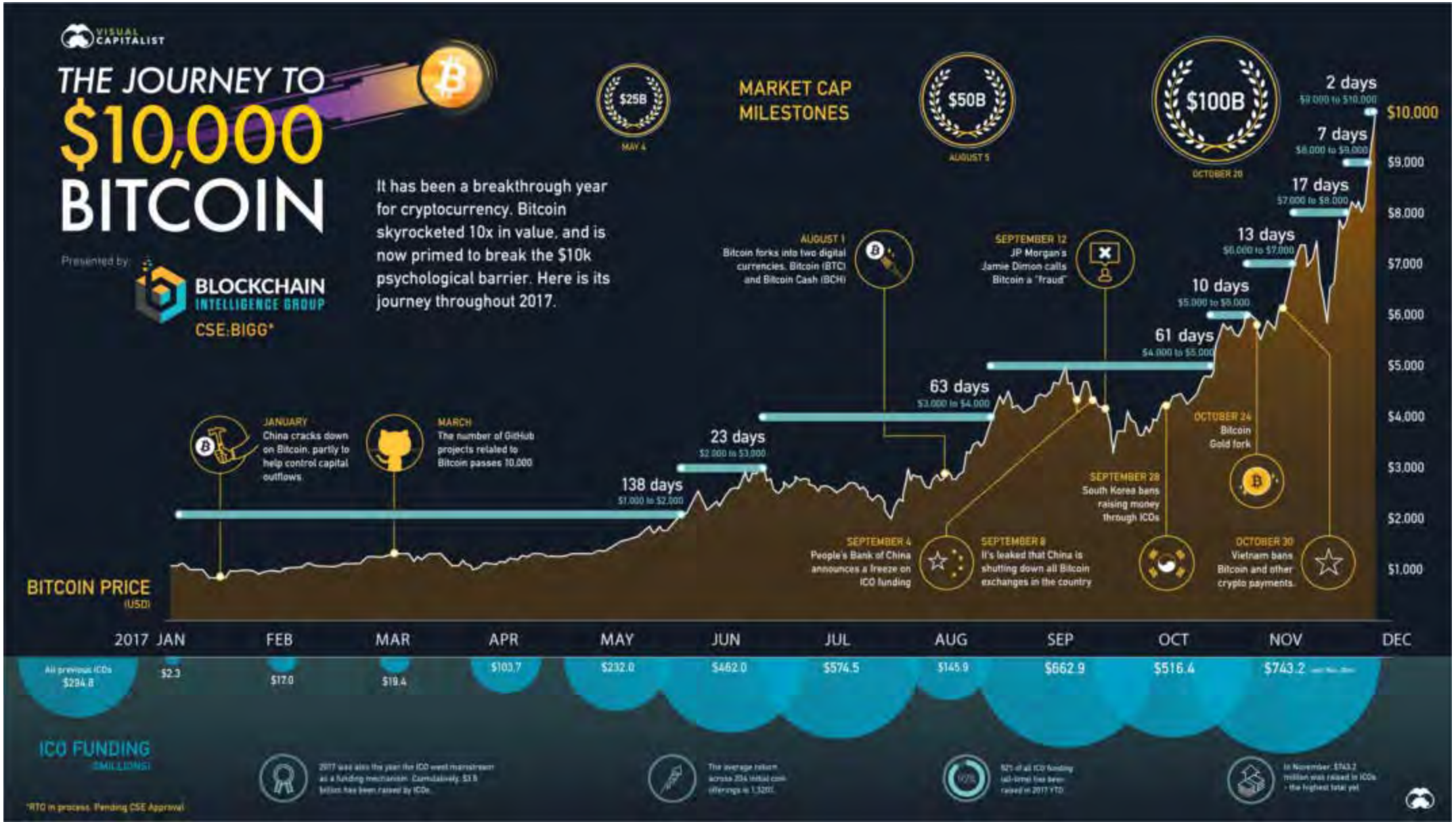
Node Connections:	33
Blocks:	498193
Time since last block:	00:06:08
Mempool Transactions:	137990
Mempool size(MB):	61.70
Transactions per second:	2.46
Next Reward Halving:	10/06/2020 17:34:46
Current Block Reward(btc):	12.5
Total number of Bitcoins:	16,727,412.5
Fee (btc/kB) 2 blocks:	0.00459107
Current Difficulty:	1590896927258
Est. Next Difficulty:	1619233151112
Est. Difficulty change:	1.78%

Highest | Lowest Priority | Latest | Oldest TX

mempool

Tx hash	Received	size(bytes)	fee(btc/kB
d9645a3c...	2:20	226	0.0032500
c8090415f...	6th Dec	815	0.0010940
ab943193...	7th Dec	370	0.0010000
92edf3abc...	5th Dec	192	0.0000100
a5357d27...	2:07	255	0.0019707
79739c35...	7th Dec	257	0.0014953
573aa22a...	7th Dec	1223	0.0008176
64ce3209...	7:53	223	0.0042767
c6ad788e...	7th Dec	36921	0.0012051
77989685...	8:10	928	0.0043719
2c4d5a67...	3:04	258	0.0033024

L’année 2017 pour le cours du bitcoin



Cryptography Mailing List

Bitcoin P2P e-cash paper

View Satoshi only

External link

From: Satoshi Nakamoto
#014810

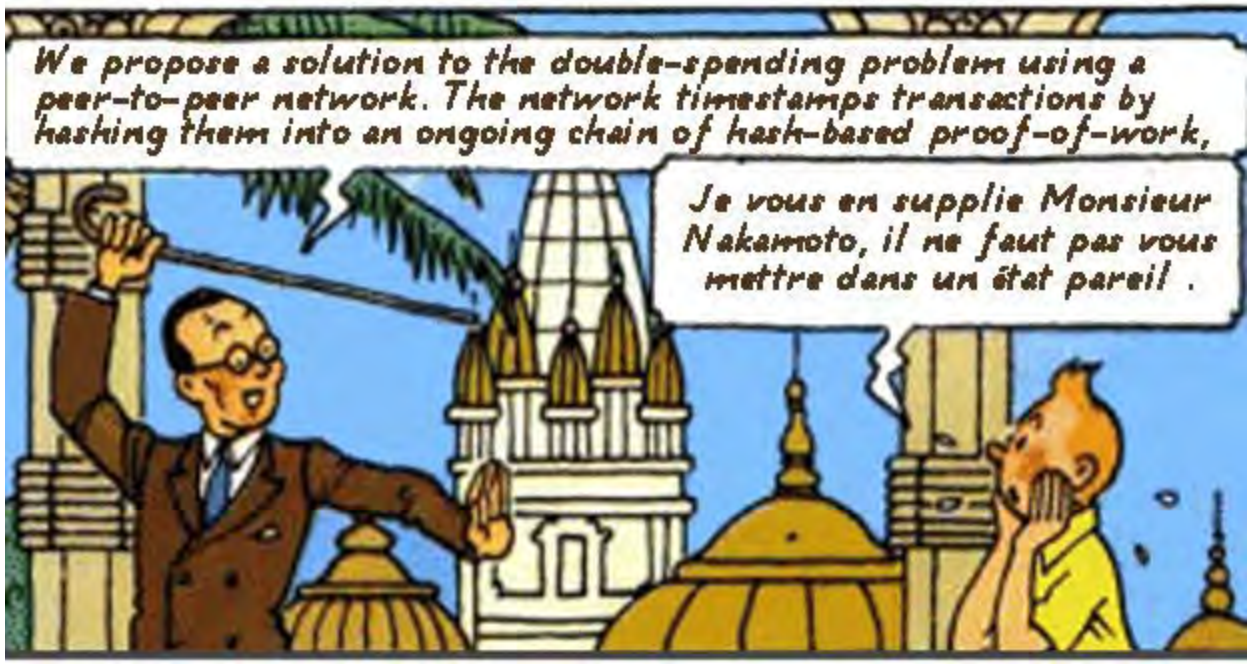
Bitcoin P2P e-cash paper

October 31, 2008, 06:10:00 PM

Replies: >>014814 >>014817 >>014827

```
I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the
network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would
allow online payments to be sent directly from one party to another
```

Manifesto of bitcoin (Satoshi Nakamoto – 2008)



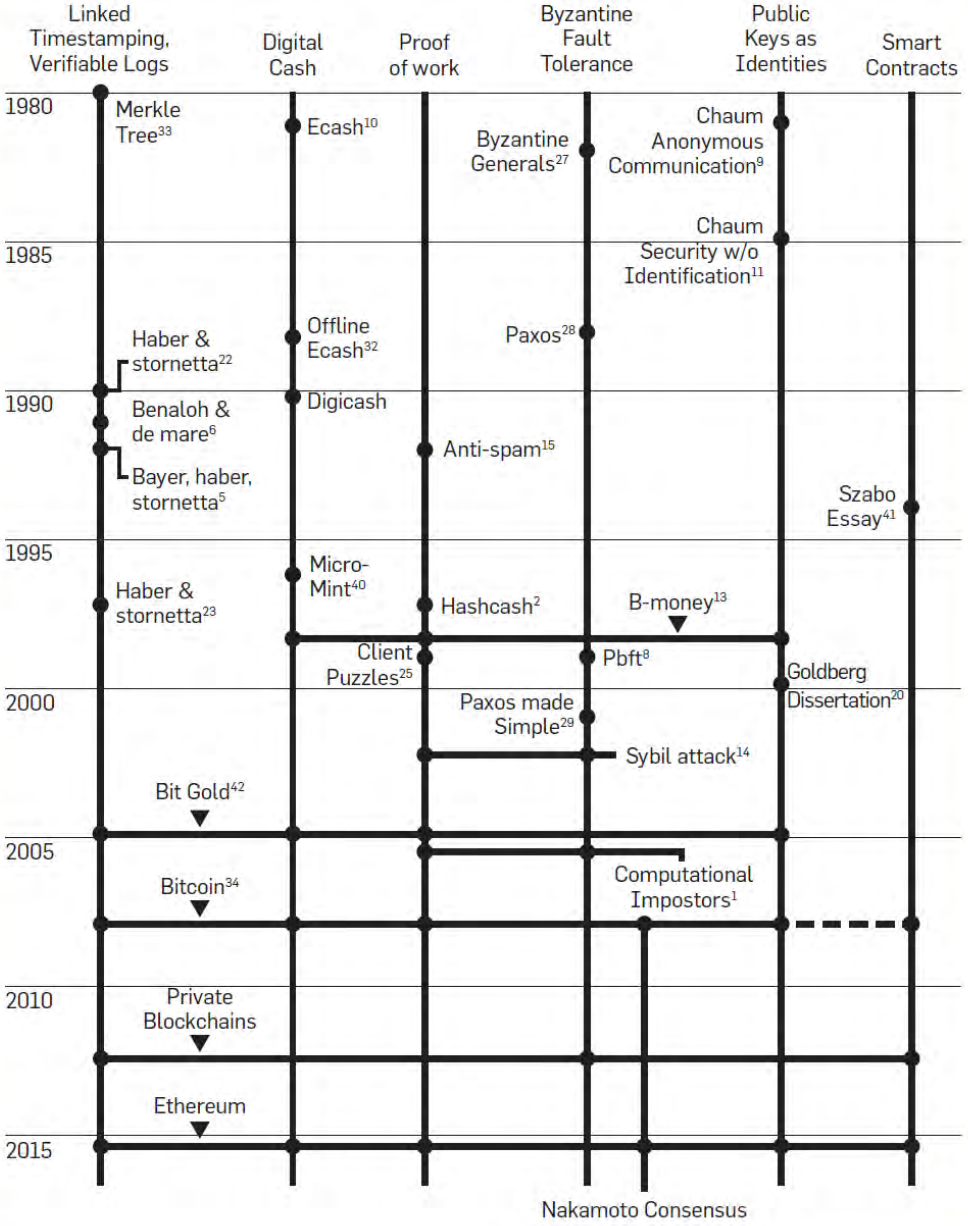
A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent 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 hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Mieux que TED (18 minutes)

- https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business?language=fr

- Satoshi Nakamoto nous a expliqué tout cela en une minute : voyons maintenant le détail.

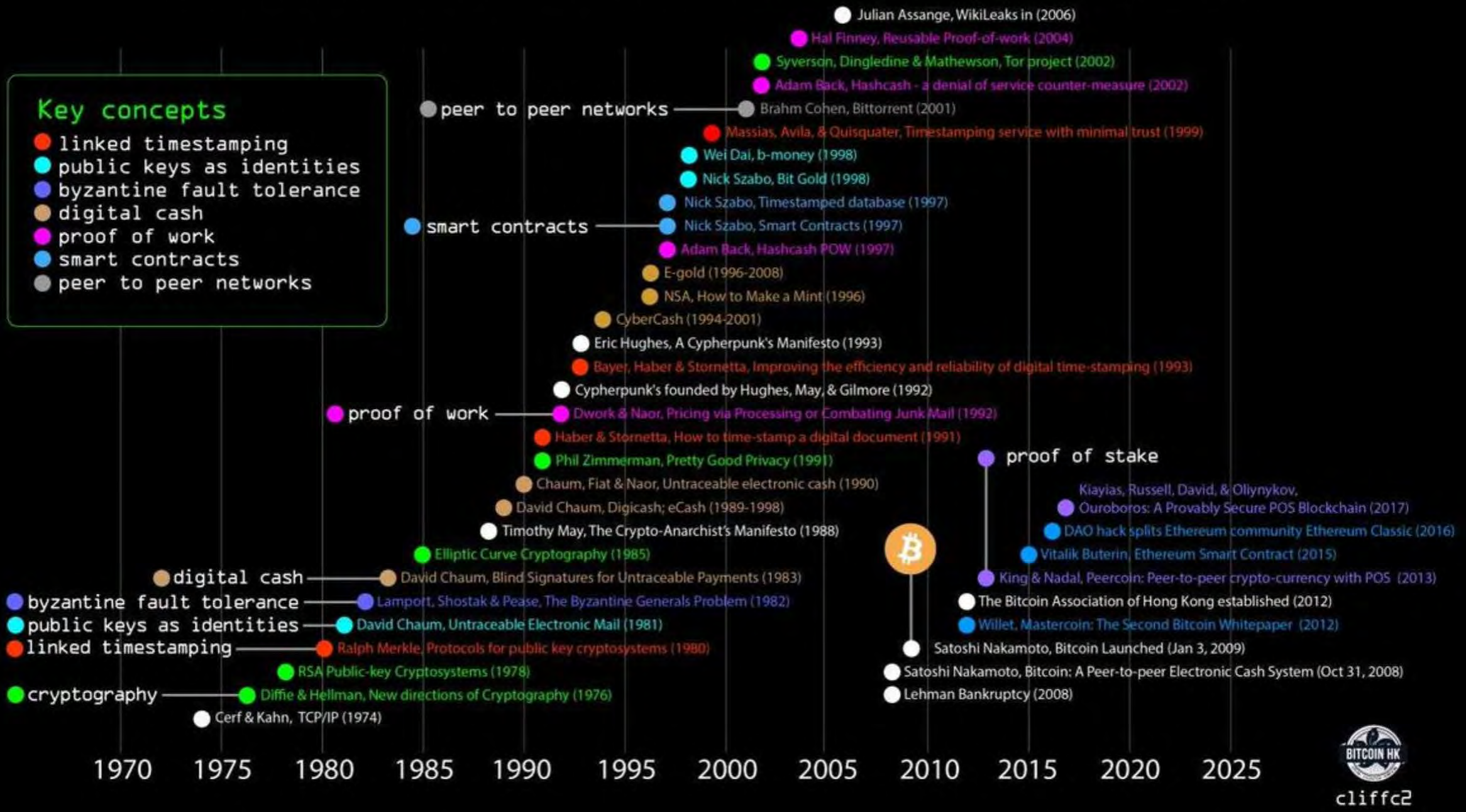
- A purely peer-to-peer version
- of electronic cash
- would allow online payments
- to be sent directly from one party to another without going through a financial institution.
- Digital signatures provide part of the solution,
- but the main benefits are lost if a trusted third party is still required 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 hash-based proof-of-work,
- forming a record that cannot be changed without redoing the proof-of-work.
- The longest chain not only serves as proof of the sequence of events witnessed,
- but proof that it came from the largest pool of CPU power.
- As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network,
- they'll generate the longest chain and outpace attackers.
- The network itself requires minimal structure.
- Messages are broadcast on a best effort basis,
- and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.



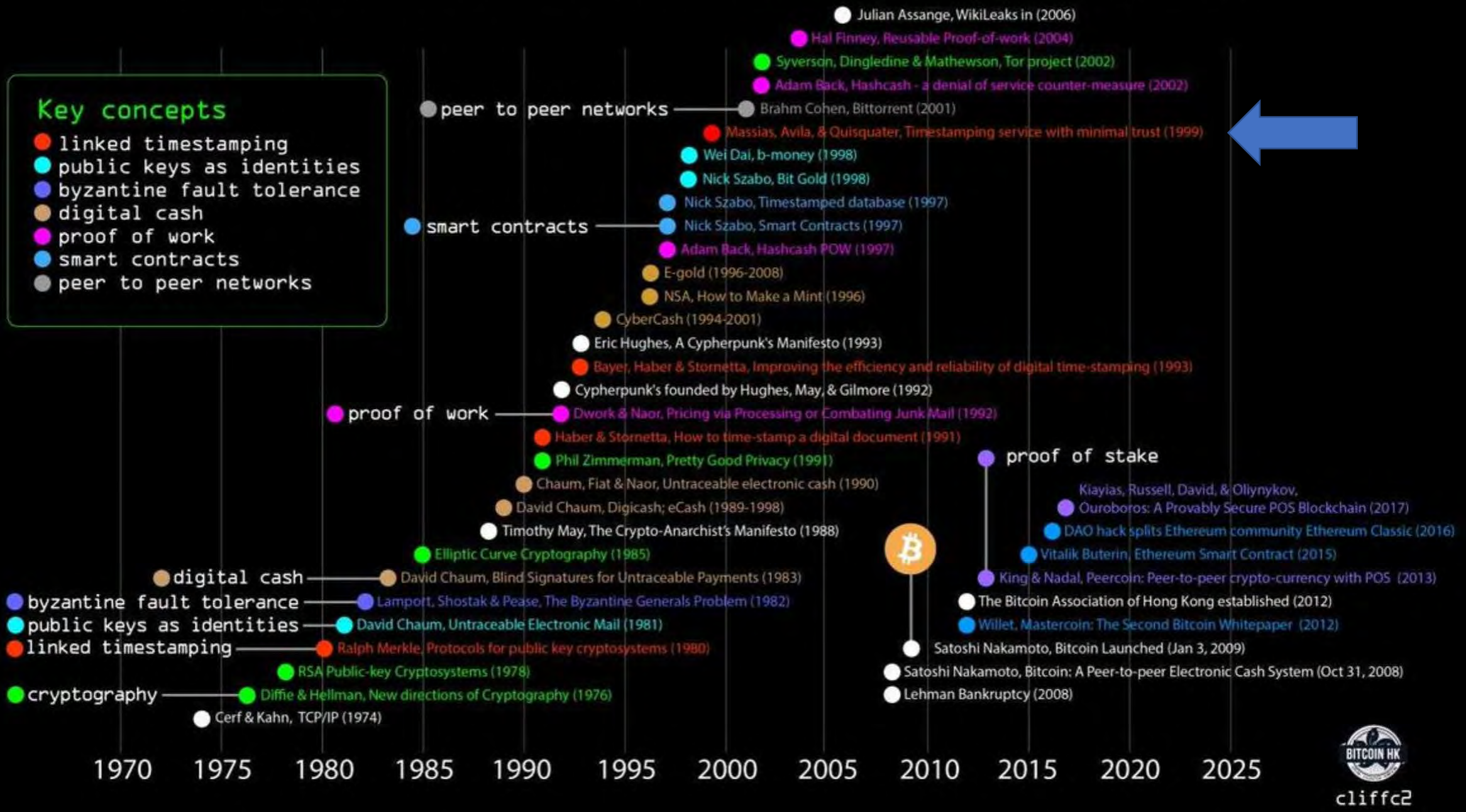
Histoire incomplète pour arriver là !


TIM C. MAY
CYPHERPUNK MAILING LIST
DAVID CHAUM
DIGICASH
SATOSHI NAKAMOTO
BITCOIN
HAL FINNEY
RPOW
JULIAN ASSANGE
WIKILEAKS
CYPHERPUNKS
PHIL ZIMMERMANN
PGP ENCRYPTION
ADAM BACK
HASHCASH
JOHN GILMORE
CYPHERPUNK MAILING LIST
NICK SZABO
BIT GOLD
WEI DAI
B MONEY

Bitcoin and the rise of Cypherpunks



Bitcoin and the rise of Cypherpunks



Bitcoin Prehistory

2 versions du papier de Satoshi … (2008)

moto-bitcoindraft.pdf - Adobe Acrobat Standard DC

Affichage Fenêtre Aide

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshi@vistomail.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 the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted 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 hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

bitcoin(18).pdf - Adobe Acrobat Standard DC

Fichier Edition Affichage Fenêtre Aide

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 hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

2 versions du papier de Satoshi …

moto-bitcoindraft.pdf - Adobe Acrobat Standard DC

Affichage Fenêtre Aide

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshi@vistomail.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 the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted 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 hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

bitcoin(18).pdf - Adobe Acrobat Standard DC

Fichier Edition Affichage Fenêtre Aide

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 hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Received October 31, 1996

HOW TO MAKE A MINT: THE CRYPTOGRAPHY OF ANONYMOUS ELECTRONIC CASH

Laurie Law, Susan Sabett, Jerry Solinas

National Security Agency Office of Information Security Research and Technology

Cryptology Division

18 June 1996

CONTENTS

1996

ESSAYS

HOW TO MAKE A MINT: THE CRYPTOGRAPHY OF ANONYMOUS ELECTRONIC CASH*

LAURIE LAW
SUSAN SABETT
JERRY SOLINAS

TABLE OF CONTENTS

---

* This research Essay was prepared by NSA employees in furtherance of the study of cryptography. The contents of the report do not necessarily represent the position or policies of the U.S. Government, the Department of Defense, or the National Security Agency.

The authors are mathematical cryptographers at the National Security Agency's Office of Information Security Research and Technology.

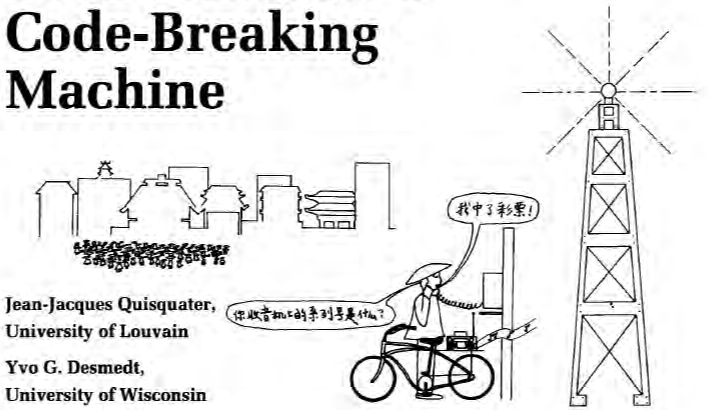
INTRODUCTION

With the onset of the Information Age, our nation is becoming increasingly dependent on network communications. Computer-based technology is impacting significantly our ability to access, store, and distribute information. Among the most important uses of this technology is *electronic commerce*: performing financial transactions via electronic information exchanged over telecommunications lines. A key requirement for electronic commerce is the development of secure and efficient electronic payment systems. The need for security is highlighted by the rise of the Internet, which promises to be a leading medium for future electronic commerce.

Electronic payment systems come in many forms including digital checks, debit cards, credit cards, and stored value cards ("SVC"). The usual security features for such systems are privacy (protection from eavesdropping), authenticity (identification and message integrity), and nonrepudiation (prevention of later denying having performed a transaction).

This Essay focuses on electronic cash. As the name implies, electronic cash is an attempt to construct an electronic payment system modelled after our paper money system. Paper money has such features as: portability (easily carried); recognizability (as legal tender), and thus readily acceptable; transferability (without involve-

Chinese Lotto as an Exhaustive Code-Breaking Machine



Jean-Jacques Quisquater,
University of Louvain

Yvo G. Desmedt,
University of Wisconsin

Why use a Cray-2 for problems that can be solved by less expensive distributed computers? Exploiting randomness can produce a simple fault-tolerant architecture.

Searching is one of the most frequently performed operations on modern computers. It is easy to search a database system that has been properly organized, but our focus is on cases where data organization is inherently bad. This occurs in the breaking of cryptosystems (cryptanalysis), in pattern recognition, and in searching a specific title (key) once in an unsorted and unorganized list. (If the list is searched frequently, it is better to sort the titles first.)

Our main goal is to demonstrate that some problems can be solved inexpensively using widely distributed computers instead of an expensive supercomputer. We illustrate this by discussing how to make a simple fault-tolerant exhaustive code-breaking machine. Our solution, which uses distributed processors, is based on some elementary concepts of probability theory (lotto). The need for communication between processors is almost nil — an important feature. We compare two approaches — deterministic and random — and then discuss how to hide such a machine and how to build larger versions.

Background

To illustrate the concept of searching in a disorganized file, let's consider a magician who mixes a deck of cards. He asks the audience to locate the ace of hearts in the deck. What is the best strategy for finding it when allowed to see only one card at a time? The most common solution is to use sequential search, exhaustively flipping each card, checking the face, and continuing until the right card turns up.

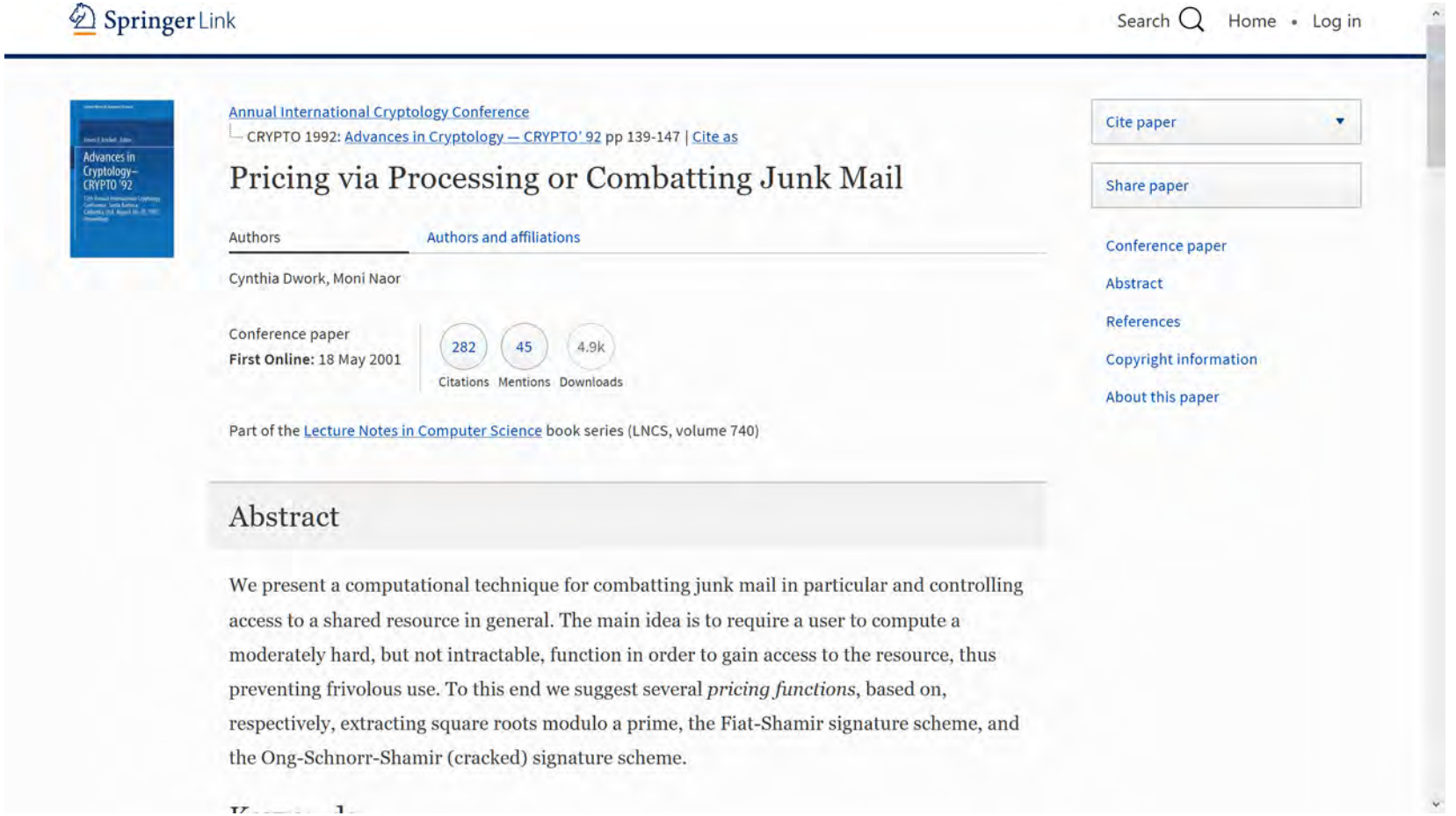
0018-9162/91/1100-0014$01.00 © 1991 IEEE

Preuve de travail.

hashcash

- Cynthia Dwork and Moni Naor,

  1992 paper "Pricing via Processing or Combatting Junk Mail".



Springer Link

Search Home • Log in

Annual International Cryptology Conference

CRYPTO 1992: Advances in Cryptology — CRYPTO' 92 pp 139-147 | Cite as

Pricing via Processing or Combatting Junk Mail

Authors Authors and affiliations

Cynthia Dwork, Moni Naor

Conference paper
First Online: 18 May 2001

282 Citations 45 Mentions 4.9k Downloads

Part of the Lecture Notes in Computer Science book series (LNCS, volume 740)

Cite paper

Share paper

Conference paper
Abstract
References
Copyright information
About this paper

Abstract

We present a computational technique for combatting junk mail in particular and controlling access to a shared resource in general. The main idea is to require a user to compute a moderately hard, but not intractable, function in order to gain access to the resource, thus preventing frivolous use. To this end we suggest several *pricing functions*, based on, respectively, extracting square roots modulo a prime, the Fiat-Shamir signature scheme, and the Ong-Schnorr-Shamir (cracked) signature scheme.

Len Assaman (KULeuven, Belgique)

This is an archive of Len Sassaman's homepage from July 2011. More info

Len Sassaman

Researcher
Computer Security and Industrial Cryptography
Katholieke Universiteit Leuven

Departement of Electrical Engineering
Kasteelpark Arenberg 10
B-3001 Leuven-Heverlee
Belgium
Tel: +32-16-321161
Fax: +32-16-321969

Email: len.sassaman-at-esat.kuleuven.be
Jabber: rabbi@jabber.ccc.de
Twitter: @lensassaman
Blog: http://rabbi.vox.com/

About me

I am a doctoral student in Electrical Engineering. My advisors are Bart Preneel and David Chaum.

Research Interests

My research is centered around the topic of privacy enhancing technologies. In particular, I am focused on both attacking and defending anonymous communication systems, exploring the applicability of information-theoretic secure systems for privacy solutions, and designing protocols which satisfy the specific needs of the use case for which they are applied. I have a very strong interest in the real-world applicability of my work; while some of what I do is pure theory, I have always held the believe that if a system cannot be implemented easily or be easily understood by the implementors, its utility is limited. Similarly, I believe that usability is a security concern; systems that do not pay close attention to the human interaction factors involved risk failing to provide security by failing to attract users. Thus, I follow closely the fields of HCI and Applied Programming as well as Information Theory, Cryptography, and Anonymity.

Professional Organizations

Researcher at COSIC; founding member of the Privacy Group and a member of the Software Protection and Trusted Computing Group.

Member, The Shmoo Group *(Inducted 2000)*
Affiliate Scholar, Institute for Ethics and Emerging Technologies *(Joined 2010)*
Member, International Association for Cryptologic Research *(Joined 2005)*
Member, Werkgemeenschap voor Informatie en Communicatietheorie *(Joined 2007)*
Member, The International Financial Cryptography Association *(Joined 2010)*
Member, Association for Computing Machinery *(Joined 2008)*
Member, IEEE Student Branch Leuven *(Joined 2008)*
Member, Society for Industrial and Applied Mathematics *(Joined 2009)*
Student Member, Society for Neuroscience *(Admitted 2010)*
Member, Electronic Frontier Foundation *(Joined 2001)*
Member, Foundation for a Free Information Infrastructure e.V. *(Joined 2011)*
Member, The Internet Society, Belgium Chapter *(Joined 2009)*
Member, ICANN's Noncommercial Users Constituency (NCUC) *(Joined June 2010)*
Member, The Internet Engineering Task Force (IETF) *(Joined 1998)*
Member, Liga voor Mensenrechten *(Joined 2011)*
Member, The Foresight Institute *(Joined 2010)*
Advisor, Scientific Advisory Board, The Lifeboat Foundation. *(Joined 2009)*

Other Projects

- Mixmaster is a mix-net implementation with widespread deployment and over ten years of development and use.
- The Pynchon Gate is an information-theoretic PIR-based pseudonymity system designed to obviate the need for reply-block based nym-servers.
- CodeCon is a conference I co-founded with Bram Cohen, aimed at attracting developers of active, highly practical projects with working code.
- HotPETS is a workshop I co-founded with Roger Dingledine and Thomas Heydt-Benjamin, to fill the void left as the PET Workshop matured into the PET Symposium. Influenced by PET and CodeCon, the goal of the workshop is to encourage discussion of "real-world" projects still in a formative state.
- Firekeeper is a browser-level intrusion detection system using Snort rules to detect and block browser-based attacks. This project was selected for the 2006 Google Summer of Code and sponsored by The Shmoo Group, and I served as mentor for its author, Jan Wrobel, for the duration of the Summer of Code program.
- Osogato, Inc. is a startup database software company, whose flagship product OBELisQ integrates fuzzy data mining into the standard relational database model. I am an advisor to the company.
- DIYBIO/Biohacking is a hobby I enjoy, with my wife Meredith.
- **High security ink** research is a side-interest of mine, which grew out of my passion for fountain pens.

Werkgemeenschap voor
Informatie- en
Communicatietheorie

WIC Homepage

The WIC is a professional organization that aims at coordinating and stimulating the work of professionals in the field of Information and Communication Theory in the Benelux (i.e. Belgium, The Netherlands, Luxembourg) and Germany.

The WIC organizes an annual two-day technical symposium where researchers from Industry and Universities from Belgium, The Netherlands, Luxembourg, and Germany meet and discuss their current research results and interests. The WIC also organizes MidWinter Meetings of a tutorial nature on current topics in its field.

News and upcoming events

Symposium 2021

Date: May 20 + 21
Organized by TU Eindhoven.
[Website]

Submission deadline: March 29

Van der Meulen seminar in honor of Frans Willems

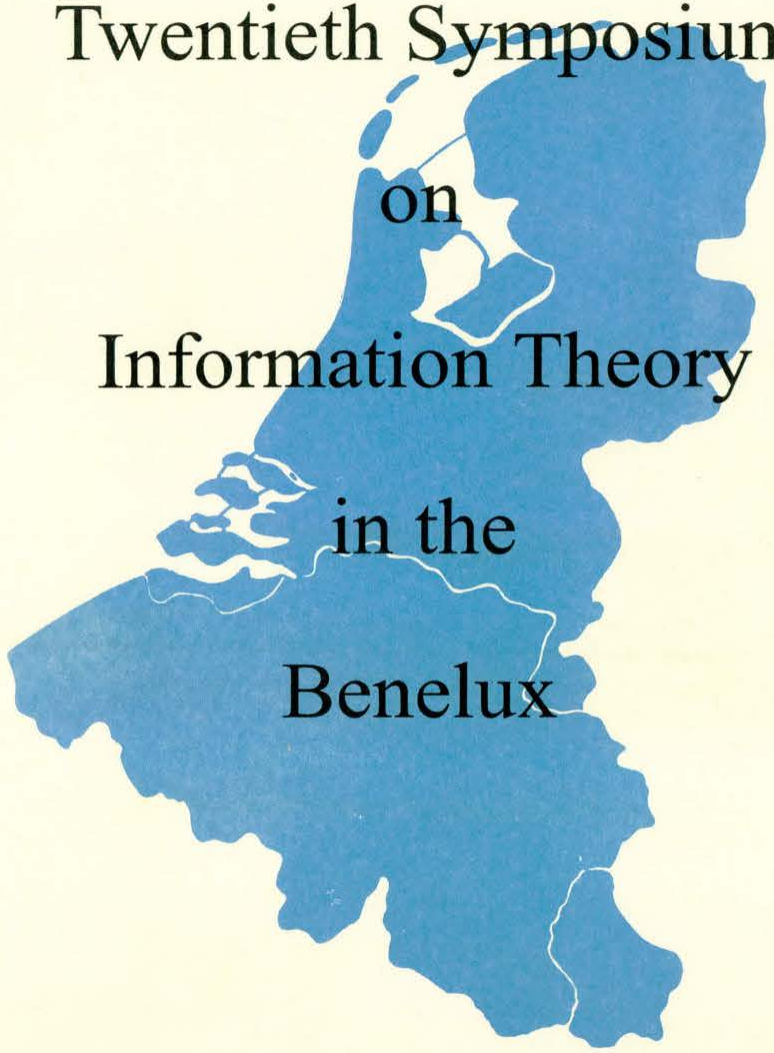
Venue: Corona Hall, TU/e, Eindhoven.
Date: Friday November 5, 2021.
Preliminary list of speakers:

- Pim Tuyls
- Gerhard Kramer
- Jean-Paul Linnartz
- Liesbet Van der Perre
- Ioannis Kontoyiannis
- Frans Willems

Index of /proceedings

Icon	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory		-	
[ ]	proceedings_SITB1985.pdf	2020-06-14 19:23	70M	
[ ]	proceedings_SITB1986.pdf	2020-06-14 19:26	74M	
[ ]	proceedings_SITB1987.pdf	2020-06-14 19:48	98M	
[ ]	proceedings_SITB1988.pdf	2020-06-14 19:51	72M	
[ ]	proceedings_SITB1989.pdf	2020-06-14 19:53	66M	
[ ]	proceedings_SITB1991.pdf	2020-06-14 19:55	56M	
[ ]	proceedings_SITB1992.pdf	2020-06-14 20:25	82M	
[ ]	proceedings_SITB1993.pdf	2020-06-14 20:29	108M	
[ ]	proceedings_SITB1994.pdf	2020-06-14 20:32	113M	
[ ]	proceedings_SITB1995.pdf	2020-06-14 20:44	74M	
[ ]	proceedings_SITB1996.pdf	2020-06-14 20:46	69M	
[ ]	proceedings_SITB1997.pdf	2020-06-14 20:49	75M	
[ ]	proceedings_SITB1998.pdf	2020-06-14 20:52	91M	
[ ]	proceedings_SITB1999.pdf	2020-06-14 20:55	99M	
[ ]	proceedings_SITB2000.pdf	2020-06-14 21:00	128M	
[ ]	proceedings_SITB2001.pdf	2020-06-14 21:03	104M	
[ ]	proceedings_SITB2002.pdf	2020-06-14 21:08	179M	
[ ]	proceedings_SITB2003.pdf	2020-06-14 21:11	109M	
[ ]	proceedings_SITB2004.pdf	2020-06-14 21:15	111M	
[ ]	proceedings_SITB2005.pdf	2020-06-14 21:18	128M	
[ ]	proceedings_SITB2006.pdf	2020-06-14 21:23	152M	
[ ]	proceedings_SITB2007.pdf	2020-06-14 21:27	160M	
[ ]	proceedings_SITB2008.pdf	2020-06-14 21:31	128M	
[ ]	proceedings_SITB2009.pdf	2020-06-14 21:34	123M	
[ ]	proceedings_SITB2010.pdf	2014-12-04 11:12	8.9M	
[ ]	proceedings_SITB2011.pdf	2014-12-10 15:28	19M	
[ ]	proceedings_SITB2012.pdf	2014-12-10 15:28	30M	
[ ]	proceedings_SITB2013.pdf	2014-12-10 15:28	15M	
[ ]	proceedings_SITB2014.pdf	2015-03-19 14:38	26M	
[ ]	proceedings_SITB2015.pdf	2015-06-11 08:10	68M	
[ ]	proceedings_SITB2016.pdf	2017-05-22 10:44	18M	
[ ]	proceedings_SITB2017.pdf	2017-05-16 09:25	21M	
[ ]	proceedings_SITB2018.pdf	2018-07-30 13:14	16M	
[ ]	proceedings_SITB2019.pdf	2019-06-24 14:40	30M	

Twentieth Symposium on Information Theory in the Benelux



Haasrode, Belgium
May 27 & 28, 1999

TIMING ATTACK: WHAT CAN BE ACHIEVED BY A POWERFUL ADVERSARY?

Gaël Hachez, François Koeune, Jean-Jacques Quisquater

UCL Crypto Group,
Place du Levant 3, B-1348 Louvain-la-Neuve, Belgium.
{hachez,fkoeune,jjq}@dice.ucl.ac.be
URL: http://www.dice.ucl.ac.be/crypto

INTRODUCTION

Implementations of cryptographic algorithms often perform computations in non-constant time, due to performance optimizations. If such operations involve secret parameters, these timing variations can leak some information and, provided enough knowledge of the implementation is at hand, a careful statistical analysis could even lead to the total recovery of these secret parameters. This idea, due to Kocher [Koc96], was developed in [DKL+98], were a timing attack

DESIGN OF A SECURE TIMESTAMPING SERVICE WITH MINIMAL TRUST REQUIREMENT

H. Massias, X. Serret Avila, J.-J. Quisquater
UCL Crypto group
Place du Levant, 3 , B-1348 Louvain-la-Neuve, Belgium
massias, serret, jjq@dice.ucl.ac.be

This paper presents our design of a timestamping system for the Belgian project TIMESEC. We first introduce the timestamping method used and we justify our choice for it. Then we present the design of our implementation as well as some of the important issues we found and the solutions we gave to them.

INTRODUCTION

The creation date of digital documents and the times expressed in them are becoming increasingly important as digital documents are being introduced into the legal domain.

We define "digital timestamp" as a digital certificate intended to assure the existence of a generic digital document at a certain time.

In order to produce fully trusted timestamps, very specific designs have been introduced. We give an overview of the most relevant methods and we introduce the one we used for the implementation of the Belgian project TIMESEC (see [PRQ+98]), justifying our choice for it. Then we present the design of the timestamping system we made for this project. We separate the different processes that are: document timestamping, timestamp verification, auditing, system start-up and system shutdown.

INTRODUCTION OF THE TIMESTAMPING TECHNIQUES

There are two families of timestamping techniques: those that work with a trusted third party and those that are based on the concept of distributed trust. Techniques based on a trusted third party rely on the impartiality of the entity that is in charge of issuing the timestamps. Techniques based on the distributed trust consist on making documents dated and signed by a large set of people in order to convince the verifiers that we could not have corrupted all of them. The trusted third party techniques can also be classified into two different kinds: those where the third party is completely trusted and those where it is partially

trusted. A detailed study of timestamping techniques can be found in [MQ97]. We believe that techniques based on distributed trust are not really workable in a professional environment, that is why we concentrate on the trusted third party approach. Nevertheless, we imposed to ourselves the requirement to lower the necessary trust on the third party to the maximum extend.

The "easy" solution, which consists on concatenating the document with the current time and sign the result, has been discarded because it has two main drawbacks

1. We must completely trust the third party, called Secure Timestamp Authority (STA), which can issue undetectable back-dated timestamps.
2. The limited lifetime of cryptographic signatures, which can be shorter than the document time-to-life.

The timestamping method that we have chosen uses a binary tree structure and has been described in [HS91] and [HS97]. This method works by rounds. For each round a binary tree is constructed with the requests filled during it. The rounds have a fixed duration, which is the result of a trade-off between the timestamps accuracy and the number of requests submitted. In Figure 1 we can see a graphical representation of a round constructed using this method.

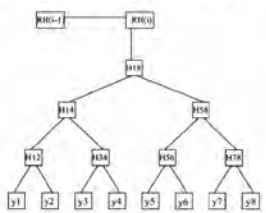


Figure 1: The binary tree structure

Each of the timestamp requests consists on a hash value of a given document. The leafs of the tree are each of those hash values. The leaf values are then

REFERENCES

[BHS92] D. Bayer, S. Haber, and W.-S. Stornetta. Improving the efficiency and reliability of digital timestamping. In Springer Verlag, editor, *Sequences'91: Methods in Communication, Security, and Computer Science*, pages 329–334, 1992.

[HS91] S. Haber and W.-S. Stornetta. How to timestamp a digital document. *Journal of Cryptology*, 3(2):99–112, 1991.

[HS97] S. Haber and W.S. Stornetta. Secure names for bit-strings. In *Proceedings of the 4th ACM Conference on Computer and Communication Security*, pages 28–35. ACM Press, April 1997.

[MQ97] H. Massias and J.-J. Quisquater. Time and cryptography. Technical report, TIMESEC Project (Federal Governement Project, Belgium), 1997. Available at `http://www.dice.ucl.ac.be/crypto/TIMESEC.html`.

[PRQ+98] B. Preneel, B. Van Rompay, J.-J. Quiquater, H. Massias, and X. Serret Avila. Design of a timestamping system. Technical report, TIMESEC Project (Federal Governement Project, Belgium), 1998. To be available at `http://www.dice.ucl.ac.be/crypto/TIMESEC.html`.

About len.sassaman.net

This is an archive of Len Sassaman's homepage from 2011. It is currently based on this archive.org mirror of the site.

Archive.org Resources

- Len Sassaman on archive.org

Links

- Twitter: @lensassaman
- Wikipedia: Len Sassaman
- freehaven.net anonymity bibliography
- langsec.org
- Zimmermann-Sassaman key-signing protocol

More

- dymaxion.org: Our Stories, Our Weapons
- The Monetary Future: Len Sassaman on Bitcoin
- The Lifeboat Foundation

Contact

Please send feedback to memorial at sassaman dot net

PGP: 0D27 66EA 193D 41AC 0A86 8679 F187 F666 4613 E63C

TUESDAY, JULY 5, 2011

Len Sassaman on Bitcoin

Len Sassaman was a brilliant cryptographer and a true champion for privacy rights and privacy enhancing technologies. He passed away on July 3rd, 2011 at the age of 31. He will be sorely missed.

I had several opportunities to discuss bitcoin and cryptocurrencies generally with Len, with the most recent exchange on June 25th below. In posting this, it is my hope that anonymity considerations with bitcoin are well understood by the individual user and appropriate for the type of bitcoin transaction that is undertaken, as all security is relative. I had asked him "if his concerns about bitcoin traceability were more of a non-cryptographic nature? i.e., real-world identity?" Len's reply, in his own words:

> "Well, it's hard to decouple cryptography from identity in a crypto-based currency, but, yes, my concerns are real-world identity issues. Bitcoin is less anonymous than physical cash. Compare to Digicash, which was 'more' anonymous. It's useful to speak about these things in more precise terms; using the Pfitzmann terminology, Bitcoin lacks unlinkability as a property. 'Throw Tor or Mixmaster at it' isn't a very satisfying answer, at least not to someone with an understanding of how those systems fail. My fear is people will associate 'bitcoin' and 'anonymous', get seriously burnt by the fact that it's 'not' anonymous, but rather a persistent ledger of all transactions ever, and then dismiss future e-cash that actually 'does' provide anonymity and unlinkability, etc., because they've 'heard that before.'

ABOUT ME

JON MATONIS

I am an e-Money researcher and a Founding Director of the Bitcoin Foundation. My career has included senior influential posts at Sumitomo Bank, VISA, VeriSign, and Hushmail.

"Free-market protagonists, such as Matonis, regard cybercash as better than traditional government-issued or -regulated money, because it is

Les différentes faces de len


DEF CON 9 - Len Sassaman - What is SSL a CA and FreeCert *
38:05 / 47:03
DEFCON


Len Sassaman & Meredith Patterson are CodeCon Valentines
0:40 / 4:08


DEF CON 12 Hacking Conference By Len Sassaman - Mixmaster vs Reliable - Video
Lots of Speculation
• Academic anonymity research is full of speculation about strength of anonymity systems
• We wanted "real world" evaluation of actually deployed systems with real traffic
• Joint work with Claudia Díaz and Evelyne Dewitte, at K.U. Leuven (ESAT-COSIC group)
• To be presented at ESORICS 2004 in September, France.
– Comparison between Two Practical Mix Designs
0:23 / 48:35


DEF CON 12 Hacking Conference By Len Sassaman - Mixmaster vs Reliable - Video
7:24 / 48:35


DEF CON 11 - Len Sassaman & Panel - Behind the Remailers
11:34 / 55:05
DEFCON

The Faithless Endpoint

How Tor puts certain users at greater risk

Len Sassaman[1]

Katholieke Universiteit Leuven
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
len.sassaman@esat.kuleuven.be

Abstract. We demonstrate that the decision to employ certain security solutions must be balanced against the additional risks that these security solutions introduce for a given user's situation, in the context of its specific threats. As an example case, we consider the anonymity network Tor and examine scenarios where the use of Tor decreases one's overall security. We then show that such trade-offs are reasonable for some, but not all, potential users of Tor. We then consider possible ways to mitigate these risks.

article-896.pdf - Adobe Acrobat Standard DC

Fichier Edition Affichage Fenêtre Aide

Acknowledgments

We would like to thank George Danezis, Roger Dingledine, and Nick Mathewson for insightful discussions on Tor security trade-offs. We also thank Meredith L. Patterson for her comments on this paper.

This work was supported in part by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government and by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy). Additional support was provided by the EU within the PRIME Project under contract IST-2002-507591.

References

1. Alessandro Acquisti, Roger Dingledine, and Paul Syverson. On the Economics of Anonymity. In Rebecca N. Wright, editor, *Proceedings of Financial Cryptography (FC '03)*. Springer-Verlag, LNCS 2742, January 2003.
2. Anonymizer. http://www.anonymizer.com.
3. David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 4(2), February 1981.
4. Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004.
5. Andreas Pfitzmann and Marit Hansen. Anonymity, unobservability, and pseudonymity: A consolidated proposal for terminology. Draft, July 2000.
6. Privoxy. http://www.privoxy.org/.

3. R. Lackey, P. Palfrader, and L. Sassaman, "Behind the Remailers: The Operators and Developers of Anonymity Services," *DEFCON 11*, Las Vegas, NV, USA, 2003.
4. R. Dingledine, and L. Sassaman, "Attacks on Anonymity Systems: Theory and Practice," *Black Hat Briefings*, Las Vegas, NV, USA, 2003.
5. L. Sassaman, "Designing Useful Privacy Applications," *Black Hat Europe Briefings 2003*, Amsterdam, NL, 2003.
6. L. Sassaman, "Anonymity in Practice," *COSIC Seminar*, Leuven, BE, 2003.
7. L. Sassaman, "Introduction to Anonymity Techniques," *University of Cambridge Security Seminar*, Cambridge, UK, 2003.
8. S. Kopsell, L. Sassaman, and A. Shostack, "Panel: Experiences Deploying Anonymous Communication Systems," *Workshop on Privacy Enhancing Technologies 2003*, Dresden, DE, 2003.

2002

1. L. Sassaman, "The Promise of Privacy," *16th Conference on Systems Administration (LISA 2002)*, Philadelphia, PA, USA, 2002.
2. L. Sassaman, "Anonymity Services and The Law," *DEFCON 10*, Las Vegas, NV, USA, 2002.
3. L. Sassaman, "Forensic Dead-Ends: Tracing Users Through Anonymous Remailers," *Black Hat Briefings*, Las Vegas, NV, USA, 2002.
4. L. Sassaman, "BOF: Future Directions for Anonymous Remailers," *Computers, Freedom, and Privacy*, San Francisco, CA, USA, 2002.

2001

1. L. Sassaman, "Fundamental Flaws in the SSL Certificate Authority Model," *DEFCON 9*, Las Vegas, NV, USA, 2001.

2000

1. L. Sassaman, "The State of the OpenPGP Keyserver Infrastructure," *North American Network Operators Group, 20th Conference*, Washington, DC, USA, 2000.

Benelux, Werkgemeenschap voor Informatie- en Communicatietheorie, 8 pages, 2007.

6. L. Sassaman, "The Faithless Endpoint: How Tor puts certain users at greater risk," Technical Report ESAT-COSIC 2007-003, pp. 1-4, 2007.
7. L. Sassaman, and B. Preneel, "The Byzantine Postman Problem: A Trivial Attack against PIR-based Nym Servers," Technical Report ESAT-COSIC 2007-001, pp. 1-7, 2007.

2005

1. L. Sassaman, B. Cohen, and N. Mathewson, "The Pynchon Gate: A Secure Method of Pseudonymous Mail Retrieval," In *Proceedings of the 4th ACM workshop on Privacy in the electronic society (WPES 2005)*, S. De Capitani di Vimercati, and R. Dingledine (eds.), ACM, pp. 1-9, 2005.
2. R. Dingledine, P. Palfrader, and L. Sassaman, "Panel: Future Anonymity Systems," *What The Hack*, Liempde, NL, 2005.

2004

1. L. Sassaman, "Privacy Issues in Identity Management," *13th CACR Information Security Workshop & 5th Annual Privacy and Security Workshop*, Toronto, ON, CA, 2004.
2. L. Sassaman, "Making Privacy Enhancing Technology a Reality," *TOORCON*, San Diego, CA, USA, 2004.
3. C. Diaz, L. Sassaman, and E. Dewitte, "Comparison between two practical mix designs," In *9th European Symposium on Research in Computer Security (ESORICS 2004)*, Lecture Notes in Computer Science 3193, D. Gollmann, P. Ryan, and P. Samarati (eds.), Springer-Verlag, pp. 141-159, 2004.
4. L. Sassaman, "The Anonymity Toolkit," *Black Hat Briefings*, Las Vegas, NV, USA, 2004.
5. L. Sassaman, "Ten Years of Practical Anonymity," *The Fifth HOPE Conference*, New York, NY, USA, 2004.

2003

1. L. Sassaman, and C. Wysopal, "Panel: How can Independent Researchers be adequately compensated for the valuable service they provide to vendors and customers while encouraging responsible reporting?," *CyberSecurity, Research & Disclosure*, Stanford, CA, USA, 2003.
2. G. Danezis, and L. Sassaman, "Heartbeat Traffic to Counter $(n-1)$ Attacks: Red-Green-Black Mixes," In *Proceedings of the 2nd ACM workshop on Privacy in the electronic society (WPES 2003)* ACM 101039, P. Samarati, and P. F. Syverson (eds.), ACM, pp. 89-93, 2003.

2. D. Kaminsky, and L. Sassaman, "Breaking Web Security: Practical Attacks on X.509," *Black Hat Briefings*, Las Vegas, NV, USA, 2009.

2008

1. G. Danezis, and L. Sassaman, "How to Bypass Two Anonymity Revocation Schemes," In *Privacy Enhancing Technologies - 8th International Symposium, PETS 2008*, Lecture Notes in Computer Science 5134, N. Borisov, and I. Goldberg (eds.), Springer-Verlag, pp. 187-201, 2008.
2. L. Sassaman, and B. Preneel, "The Byzantine Postman Problem," In *Proceedings of the 29th Symposium on Information Theory in the Benelux*, Werkgemeenschap voor Informatie- en Communicatietheorie, pp. 129-135, 2008.
3. L. Sassaman, "A Review of the OLPC XO Security Model," *Stanford University Security Seminar*, Stanford, CA, USA, 2008.
4. M. L. Patterson, L. Sassaman, and D. Chaum, "Freezing More Than Bits: Chilling Effects of the OLPC XO Security Model," In *Usability, Psychology, and Security 2008*, E. Churchill, and R. Dhamija (eds.), USENIX, pp. 5:1-5:5, 2008.
5. L. Sassaman, "Freezing More Than Bits: Chilling Effects of the OLPC XO Security Model," *University of California, Berkeley Security Reading Group*, Berkeley, CA, USA, 2008.
6. L. Sassaman, "Toward an Information-Theoretically Secure Anonymous Communication Service," Master thesis, *Katholieke Universiteit Leuven*, B. Preneel (promotor), 94 pages, 2008.

2007

1. L. Sassaman, "Anonymity for 2015," *24th Chaos Communication Congress*, Berlin, DE, 2007.
2. L. Sassaman, "Anonymity and its Discontents," *Black Hat Briefings*, Las Vegas, NV, USA, 2007.
3. L. Sassaman, and B. Preneel, "Solving the Byzantine Postman Problem," Technical Report ESAT-COSIC 2007-004, 15 pages, 2007.
4. K. Kursawe, P. Palfrader, and L. Sassaman, "Echolot and Leuchtfeuer: Measuring the Reliability of Unreliable Mixes," Technical Report ESAT-COSIC 2007-005, 15 pages, 2007.
5. M. L. Patterson, and L. Sassaman, "Subliminal Channels in the Private Information Retrieval Protocols," In *Proceedings of the 28th Symposium on Information Theory in the Benelux*, Werkgemeenschap voor Informatie- en Communicatietheorie, 8 pages, 2007.

2011

1. M. L. Patterson, and L. Sassaman, "Towards a Theory of Computer Insecurity: a Formal Language-Theoretic Approach," *Dartmouth College Institute for Security, Technology, and Society Speaker Series*, Hanover, NH, USA, 2011.

2010

1. L. Sassaman, "Minimizing Attack Surfaces with Language-Theoretic Security," *EIDMA/DIAMANT Cryptography Working Group*, Utrecht, NL, 2010.
2. J. C. Anderson, L. Sassaman, and E. You, "The rise of Distributed, Decentralized, Amateur/Citizen Science and Do It Yourself Biology: Safety and Security Concerns," *Open Science Summit 2010*, Berkeley, CA, USA, 2010.
3. M. L. Patterson, and L. Sassaman, "Exploiting the Forest with Trees," *Black Hat Briefings*, Las Vegas, NV, USA, 2010.
4. M. L. Patterson, and L. Sassaman, "Exploiting Computational Slack in Protocol Grammars," *PH-Neutral*, Berlin, DE, 2010.
5. L. Sassaman, "Language Theoretic Security Attacks: Exploiting Computational Slack in Protocol Grammars," *COSIC Seminar*, Leuven, BE, 2010.
6. L. Sassaman, "Ethical Guidelines for Computer Security Researchers: "Be Reasonable"," In *Workshop on Ethics in Computer Security Research 2010*, Lecture Notes in Computer Science, Springer-Verlag, 6 pages, 2010.
7. L. F. Cranor, E. Kenneally, and L. Sassaman, "Towards a Code of Ethics for Computer Security Research," *Workshop on Ethics in Computer Security Research (WECSR 2010)*, Tenerife, ES, 2010.
8. D. Kaminsky, M. L. Patterson, and L. Sassaman, "PKI Layer Cake: New Collision Attacks Against the Global X.509 Infrastructure," In *Financial Cryptography and Data Security - 14th International Conference, FC 2010*, Lecture Notes in Computer Science 6052, R. Sion (ed.), Springer-Verlag, 16 pages, 2010.

2009

1. L. Sassaman, "Lessons in Vulnerability Disclosure: So You Broke The Internet -- What Now?," *COSIC Seminar*, Leuven, BE, 2009.
2. D. Kaminsky, and L. Sassaman, "Breaking Web Security: Practical Attacks on X.509," *Black Hat Briefings*, Las Vegas, NV, USA, 2009.

2008

Improving the Efficiency and Reliability of Digital Time-Stamping

Dave Bayer*
Barnard College
Columbia University
New York, N.Y. 10027 U.S.A.
dab@math.columbia.edu

Stuart Haber
Bellcore
445 South Street
Morristown, N.J. 07960 U.S.A.
stuart@bellcore.com

W. Scott Stornetta
Bellcore
445 South Street
Morristown, N.J. 07960 U.S.A.
stornetta@bellcore.com

March 1992

Abstract

To establish that a document was created after a given moment in time, it is necessary to report events that could not have been predicted before they happened. To establish that a document was created before a given moment in time, it is necessary to cause an event based on the document, which can be observed by others. Cryptographic hash functions can be used both to report events succinctly, and to cause events based on documents without revealing their contents. Haber and Stornetta have proposed two schemes for digital time-stamping which rely on these principles [HaSt 91].

We reexamine one of those protocols, addressing the resource constraint required for storage and verification of time-stamp certificates. By using trees, we show how to achieve an exponential increase in the publicity obtained for each time-stamping event, while reducing the storage and the computation required in order to validate a given certificate.

We show how time-stamping can be used in certain circumstances to extend the useful lifetime of different kinds of cryptographic certifications of authenticity, in the event that the certifying protocol is compromised. This can be applied to digital signatures, or to time-stamping itself, making the digital time-stamping process renewable.

*Partially supported by NSF grant DMS-90-06116.

David Bayer

Professor of Mathematics

Department

Mathematics

Office

426 Mathematics Building on Columbia campus

Click website globe icon under Contact for office-hour calendar

Contact

212-854-2643 bayer@math.columbia.edu

Dave Bayer

Barnard College
Verified email at math.columbia.edu

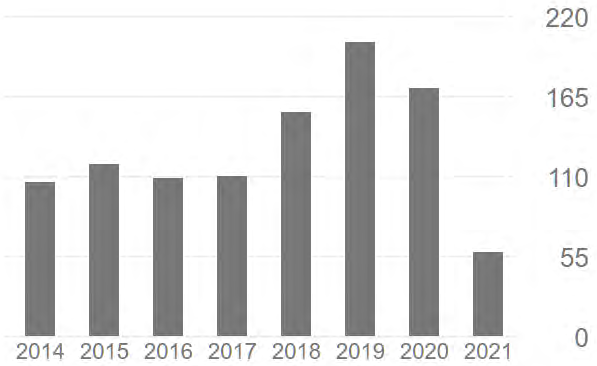
FOLLOW

TITLE	CITED BY	YEAR
Improving the efficiency and reliability of digital time-stamping D Bayer, S Haber, WS Stornetta Sequences Ii, 329-334	595	1993
Trailing the dovetail shuffle to its lair D Bayer, P Diaconis Annals of applied probability 2 (2), 294-313	452	1992
The nonlinear geometry of linear programming. I. Affine and projective scaling trajectories DA Bayer, JC Lagarias Transactions of the American Mathematical Society 314 (2), 499-526	365	1989
What can be computed in algebraic geometry? D Bayer, D Mumford arXiv preprint alg-geom/9304003	354	1993
Cellular resolutions of monomial modules D Bayer, B Sturmfels arXiv preprint alg-geom/9711023	241	1997
Monomial resolutions D Bayer, I Peeva, B Sturmfels arXiv preprint alg-geom/9610012	238	1996

Cited by

VIEW ALL

	All	Since 2016
Citations	3188	806
h-index	19	11
i10-index	20	12



Co-authors


Jeffrey C. Lagarias
Prof. of Mathematics, Univ. of Mi…


Bernd Sturmfels
Director of the Max Planck Institu…


Stuart Haber
Stuart Haber Crypto, LLC


David Eisenbud

How Do Digital Time-Stamps Support Digital Signatures?

Answered by **Stuart Haber, Burt Kaliski** *and* **Scott Stornetta**
as published in the Fall 1995 edition of *Cryptobytes*--The technical newsletter of RSA Laboratories

Consider two questions that may be asked by a computer user as he or she views a digital document or on-line record. (1) Who is the author of this record --who wrote it, approved it, or consented to it? (2) When was this record created or last modified?

In both cases, the question is one about exactly this record-exactly this sequence of bits--whether it was first stored on this computer or was created somewhere else and then copied and saved here. An answer to the first question tells **who & what**: who approved exactly what is in this record? An answer to the second question tells **when & what**: when exactly did the contents of this record first exist?

Both of the above questions have good solutions. A system for answering the first question is called a **digital signature scheme**. Such a system was first proposed in [2] and there is a wide variety of accepted designs for an implementation of this kind of system [4,5].

A system for answering the second question is called a **digital time-stamping scheme**. Such systems were described in [1,3], and an implementation is commercially available from Surety Technologies (http:// www.surety.com/).

Any system allowing users to answer these questions reliably for all their records must include two different sorts of procedures. First, there must be a **certification** procedure with which (1) the author of a record can "sign" the record, or (2) any user can fix a record in time. The result of this procedure is a small certifying file, a **certificate** if you will, that captures the result of this procedure. Second, there must be a **verification** procedure by which any user can check a record and its accompanying certificate to make sure it correctly answers (1) who and what? or (2) when and what? about the record in question.

The "certificate" returned by the certification procedure of a digital signature system is usually called a **signature**; it is a signature for a particular signer (specifying whom) and for a particular record (specifying what). In order to be able to "sign" documents, a user registers with the system by using special software to compute a pair of numbers called keys, a **public key** and a corresponding **private key**. The private key should only be available to the user to whom it belongs, and is used (by the certification or "signing" procedure) in order to sign documents; it is by employing the user's private key that the signature and the record are tied to that particular user. The public key may be available to many users of the system, and is used by the verification procedure. That is, the verification procedure takes a particular record, a particular user's public key, and a putative signature for that record and that user, and uses this information to check whether the would-be signature was correctly computed using that record and the corresponding private key.

Special computational methods are employed for signing documents and for verifying documents and signatures; when these methods are carefully implemented, they have the remarkable property that the knowledge of a user's public key does not enable an attacker or hacker to figure out the user's corresponding private key. Of course, if, either through carelessness or deliberate

Information-
technology Promotion
Agency
Bunkyo Green Court
Center Office
2-28-8,
Honkomagome.
Bunkyo-KU
Tokyo 113-6591.
Japan


BITCOIN • DECENTRALIZED • PEER TO PEER
1 TROY OZ .999 FINE COPPER

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

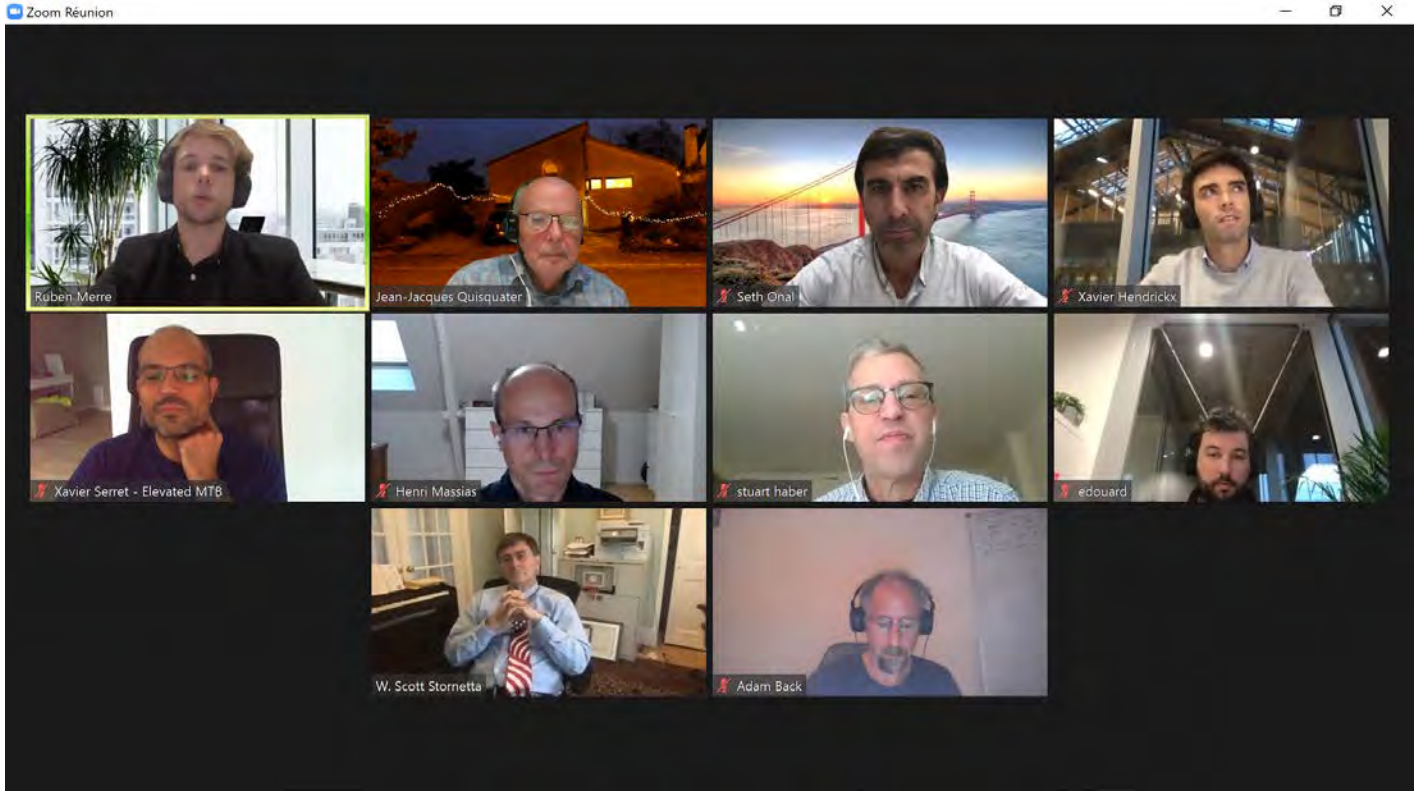
[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

1er octobre 2020



This complimentary WebSite Sampler is a service of TABNet.

Math RiZK

A creative company devoted to cryptographic and smartcard research

Everything you want and need about secure timing:

- research in cryptography in due time,

- timing attacks and countermeasures,

- SPA and DPA studies for yesterday hardware, (not only power problems!)

- secure timestamping for today,

- smartcard research for the future,

- managed by Prof. Jean-Jacques Quisquater,

- contact: jjq@cryptographic.com.

Verte Voie 20; Boite 5 , Louvain-la-Neuve, Belgium, B-1348
Phone: 32.2.358.19.07 - Fax: 32.2.358.55.83

My view: timestamping

- In 1989, my boss at Philips Research asked us to think about digital everywhere using cryptography. Signatures and encryption were already done but a lot of applications to be designed and discovered.

- So we did: watermarking, timestamping, …

- Timestamping with notaries using hash functions and they wanted to sign (their job ☺. But there was a scheme only with hash functions and chains. Never implemented and published.
- problem: lack of good hash functions (MD4 and MD5 will come later and ISO more later).

The inventor: Haber and Stornetta

[1] S. Haber, W. S. Stornetta: “How to time-stamp a digital document”, Journal of Cryptology, January 1991, Vol. 3, Issue 2, pp 99–111 (first presented at CRYPTO ’90). (see also patent US 5136647 A).

Two solutions: one with TTP, the other one decentralized.

[2] J. Benaloh, M. de Mare: “Efficient Broadcast Time-Stamping”, TR from Clarkson University, 1991/1992.

How to Time-Stamp a Digital Document*

Stuart Haber
stuart@bellcore.com

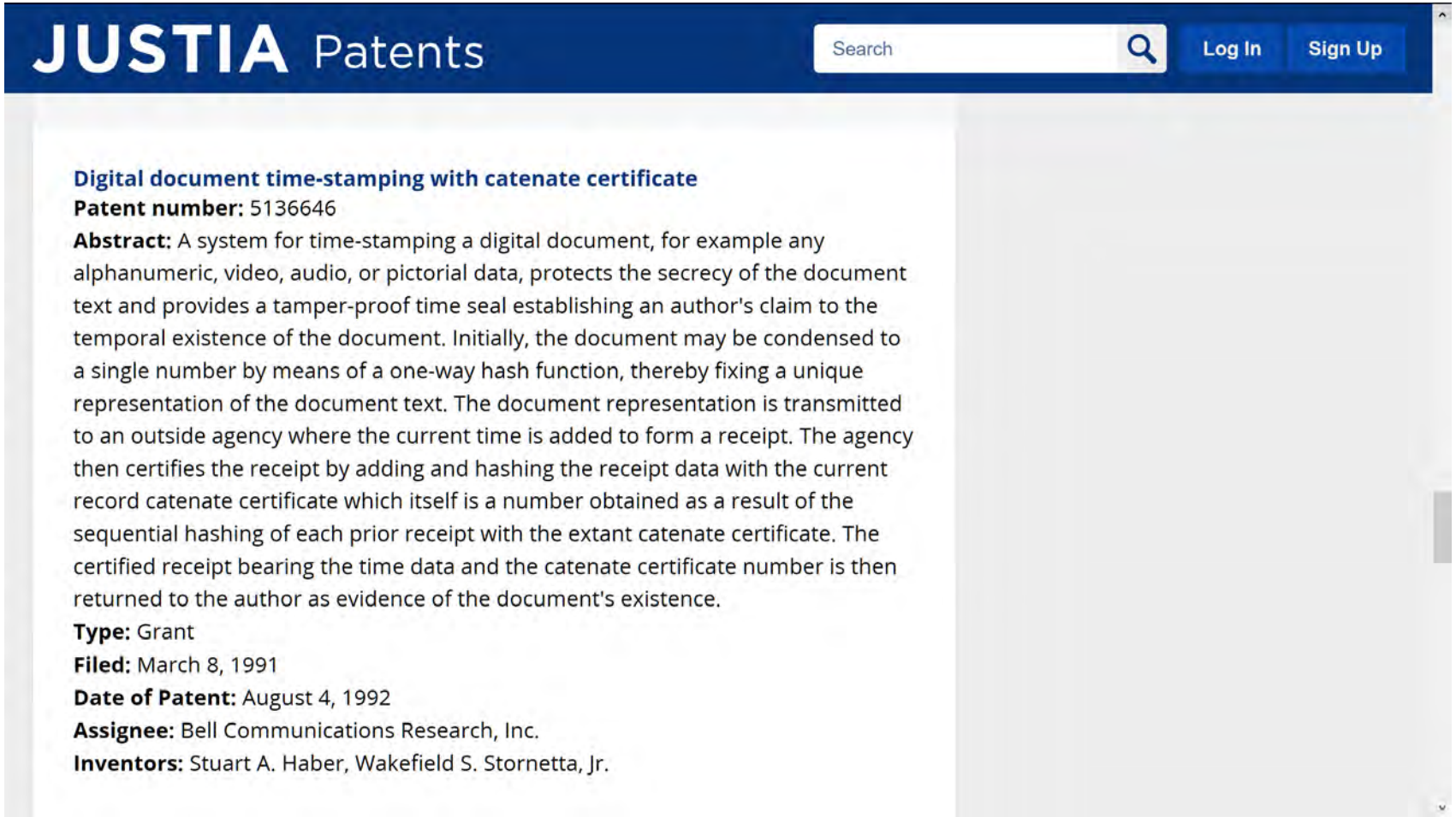
W. Scott Stornetta
stornetta@bellcore.com

Bellcore
445 South Street
Morristown, N.J. 07960-1910

Abstract

The prospect of a world in which all text, audio, picture, and video documents are in digital form on easily modifiable media raises the issue of how to certify when a document was created or last changed. The problem is to time-stamp the data, not the medium. We propose computationally practical procedures for digital time-stamping of such documents so that it is infeasible for a user either to back-date or to forward-date his document, even with the collusion of a time-stamping service. Our procedures maintain complete privacy of the documents themselves, and require no record-keeping by the time-stamping service.

*Appeared, with minor editorial changes, in *Journal of Cryptology*, Vol. 3, No. 2, pp. 99–111, 1991.


JUSTIA Patents
Search
Log In
Sign Up
Digital document time-stamping with catenate certificate
Patent number: 5136646
Abstract: A system for time-stamping a digital document, for example any alphanumeric, video, audio, or pictorial data, protects the secrecy of the document text and provides a tamper-proof time seal establishing an author's claim to the temporal existence of the document. Initially, the document may be condensed to a single number by means of a one-way hash function, thereby fixing a unique representation of the document text. The document representation is transmitted to an outside agency where the current time is added to form a receipt. The agency then certifies the receipt by adding and hashing the receipt data with the current record catenate certificate which itself is a number obtained as a result of the sequential hashing of each prior receipt with the extant catenate certificate. The certified receipt bearing the time data and the catenate certificate number is then returned to the author as evidence of the document's existence.
Type: Grant
Filed: March 8, 1991
Date of Patent: August 4, 1992
Assignee: Bell Communications Research, Inc.
Inventors: Stuart A. Haber, Wakefield S. Stornetta, Jr.

Then voting: 1991: Josh Benaloh-de Mare

- With reference to the work of Stuart Haber

- Then there was « The Chinese Lotto » (also 1991: an early proof of work, by Q and Yvo Desmedt),

- Then the TIMESEC project …

Banque de données projets FEDRA

- Presentation
- Actions de recherche
- Personnes
- Chercher

TIMESEC - Time-Stamping Digital et l'évaluation des primitifs de protection

Projet de recherche NO/B/007 (Action de recherche NO)

- Description
- Documentation

Personnes :

- Prof. dr. PRENEEL Bart - Katholieke Universiteit Leuven (K.U.Leuven)
  Partenaire financé belge
  Durée: 1/8/1996-31/7/1998
- Prof. dr. QUISQUATER Jean-Jacques - Université Catholique de Louvain (UCL)
  Partenaire financé belge
  Durée: 1/8/1996-31/7/1998

Description :

Contexte

Les services de Time-stamping sont un composant important pour la protection des services de télécommunication modernes, par exemple pour la conclusion de contrats électroniques, EDI (Electronic Data Interchange), la protection de IPR (Intellectual Property Rights), les services multimédia interactifs, etc. Les instances pour la standardisation travaillent actuellement à des solutions à cette problématique.

Belgian project TIMESEC: 1996-1998

- With the support of Stuart Haber,
- Implementing his ideas and improving it also by implementations and tests,
- Two servers, but in theory many ones,
- Also using 2 hash functions in parallel, Merkle trees, accumulators, aso,
- ISO: ISO-IEC WD 18104 (SC27)
- IETF: yes we proposed there the use of blockchains in 1997!

Some references

[MAQ99a] H. Massias, X. Serret Avila, and J.-J. Quisquater. Design of a secure timestamping service with minimal trust requirements. In A. Barbé, E.C. van der Meulen, and P. Vanroose, editors, *Twentieth Symposium on Information Theory in the Benelux*, pages 79–86, May 1999.

[MAQ99b] H. Massias, X. Serret Avila, and J.-J. Quisquater. Timestamps: Main issues on their use and implementation. Accepted at Wet Ice '99, Stanford CA, June, 1999.

[Mas98] H. Massias. A survey of accumulators. Technical report, UCL Crypto Group Technical Report, February 1998.

[MQ97] H. Massias and J.-J. Quisquater. Time and cryptography. Technical report, TIMESEC Project (Federal Governement Project, Belgium), 1997. Available at `http://www.dice.ucl.ac.be/crypto/TIMESEC.html`.

[PRQ+98] B. Preneel, B. Van Rompay, J.-J. Quiquater, H. Massias, and X. Serret Avila. Design of a timestamping system. Technical report, TIMESEC Project (Federal Governement Project, Belgium), 1998. To be available at `http://www.dice.ucl.ac.be/crypto/TIMESEC.html`.

Nothing really new! Scalability, granularity … Conclusion of TIMESEC

7 Conclusion

As we explained, the problem of securely timestamping documents is not as easy as it seems. The lifetime of the crypto-algorithms used to define a timestamping system must be carefully studied. A value associated with a time must be published somewhere in an unmodifiable media in order to be trusted by all the possible verifiers. The place and frequency of this published round value influences directly the trust and granularity provided by the timestamps. The dependency on this published value is the major brake for the scalability of the timestamping system, which must be further investigated.

IMES DISCUSSION PAPER SERIES

The Security Evaluation of Time Stamping Schemes: The Present Situation and Studies

Masashi UNE

Discussion Paper No. 2001-E-18

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

C.P.O BOX 203 TOKYO
100-8630 JAPAN

Blockchain here …

completely and therefore find it hard to manipulate a time stamp. However, just as in the case of the linking scheme, a distributed scheme system is more complicated than a simple scheme. For example, the time signature distributed system (Takura et al. [1998]) belongs to this category, and Ansper et al. [2001] proposed a scheme possessing the characteristics of both the linking and distributed schemes. The main strengths and limitations of these schemes are summarized in Table 1.

Table 1 Main Strengths and Limitations of Three Schemes

Schemes	Strengths	Limitations
simple scheme	The system is relatively simple.	It is necessary to assume that the issuer is the trusted third party.
linking scheme	The assumption that the issuer is the trusted third party is rendered unnecessary, for example, by the periodical publication of a part of a chain of time stamps.	The system is relatively complicated because additional operations for linking all time stamps are needed.
distributed scheme	The assumption that the issuers are the trusted third parties is rendered unnecessary by sharing the secret data among multiple issuers.	The system is relatively complicated because multiple issuers generate a time stamp cooperatively.

The classification described above is also adopted in standardization activities relating to a time stamping service. A working draft of ISO/IEC 18014 (Time stamping services, ISO/IEC [2001]) includes the following two types of scheme: "mechanisms producing independent tokens" and "mechanisms producing linked tokens." These correspond to the simple and linking schemes, respectively. On the other hand, ISO/IEC 13888 (Non-repudiation, ISO/IEC [1997]) and IETF PKIX

Who are these authors?

- Une, Masa**shi**, and Tsutomu Matsu**moto**,
- The author of bitcoin is:
  - Sato**shi** Naka**moto**,
- Curious coincidence!
- Better, **Satoshi** is a reference:
  - Takura, Akira, Satoshi Ono and Shozo Naito

Who is Masashi Une?

- Majored in experimental economy!
- research subjects: cryptography linked to financial services,
- Related to cryptographic systems of distributed chaining and trusted!

coin: paper

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 hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

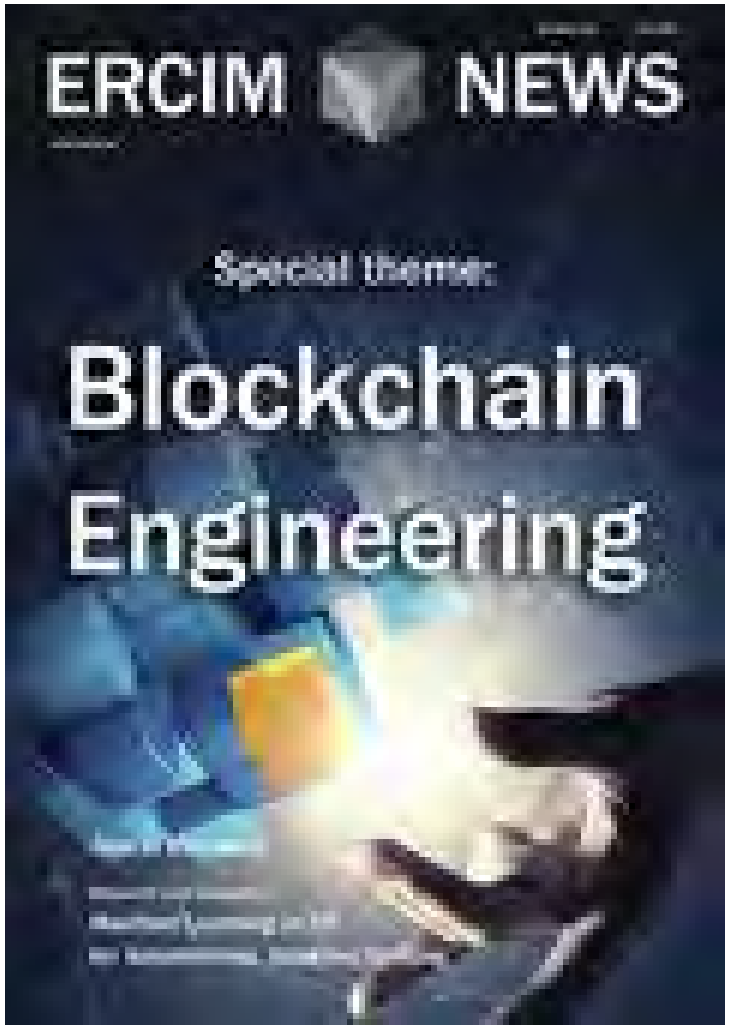
- The inventor of bitcoin knows very well this story.
- Out of 8 references 5 references are Haber, Merkle, and … me.
- Thanks to him. Curiously Satoshi cites the less known paper from an unknown conference in Benelux …

Question: why invented so early without use?

- People didn’t think it was important,
- People didn’t understand very well the concept of distributed computation (that is, peer-to-peer) and thn wait for bittorrent, gnutella and napster, …
- Then bitcoin was coming! And people saw the blockchain inside.

This story in

- https://ercim-news.ercim.eu/



COMPRENDRE LES BLOCKCHAINS

- introduction aux blockchains : tableau d'affichage et horodatage, dématérialisation, l'arrivée du peer to peer,

    - la désintermédiation,

- histoire des blockchains :

    - exemples anciens,

    - monnaie électronique : le problème difficile de la gestion de la double dépense (fraude),

- un retour sur le bitcoin : les blocs, à quoi sert le minage (loterie pour désigner un gagnant, gestion de la participation sans identification, clones et attaque sybile), les délais, les forks, scalabilité.

Définitions

- La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle ... (une base de données avec des propriétés spéciales).

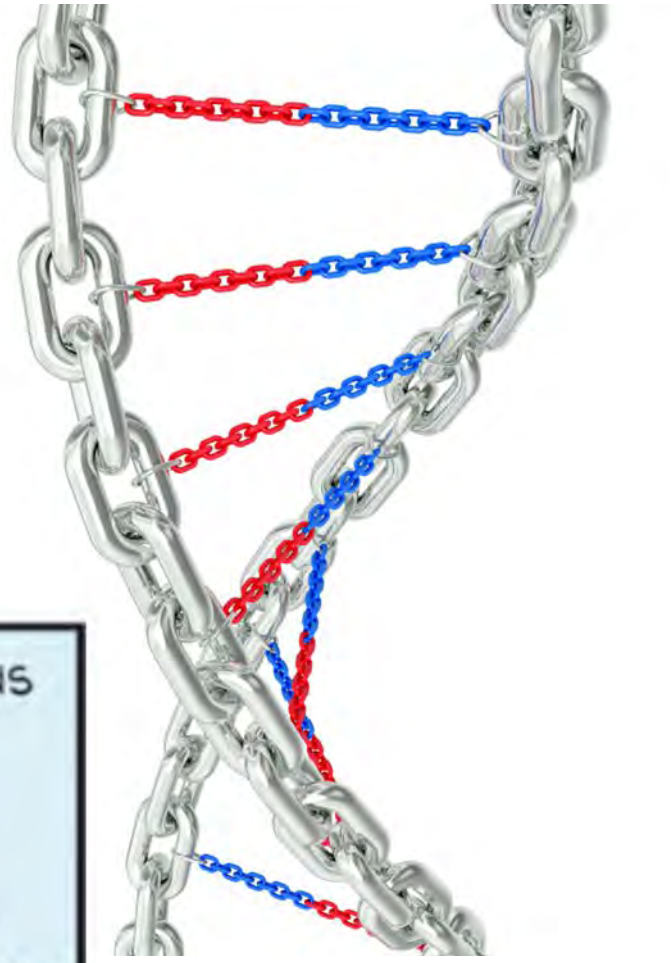
- Une blockchain publique peut donc être assimilée à un **grand livre comptable public, anonyme et infalsifiable sur internet,**

un grand registre où toutes les nouvelles opérations sont écrites dans l'ordre avec un horodatage.

- **C'est aussi un immense tableau d'affichage où toutes les nouvelles opérations doivent être approuvées par tous et ajoutées de façon inaltérables.**

- Grâce à des horodatages, copies multiples, ordre inaltérable des opérations passées, le peer-to-peer, la cryptographie, le consensus.

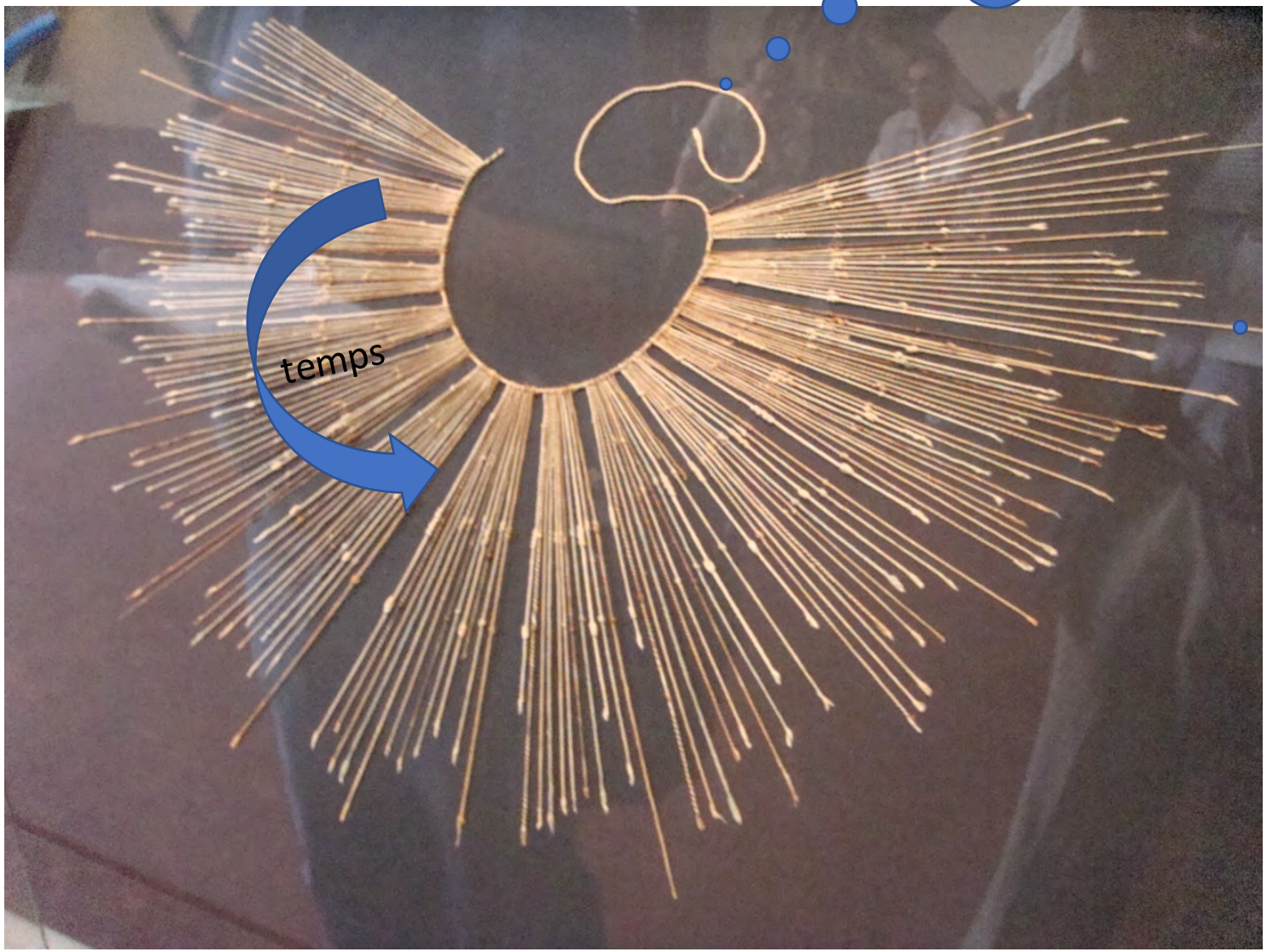
L’histoire ancienne des blockchains



Anciennes blockchains (tablettes crétoises)

Preuve de travail

Khipus incas (1500 AC) : cordes et nœuds



chaîne

Enregistrement (bloc)

Disque de Phaistos (Crète) ?

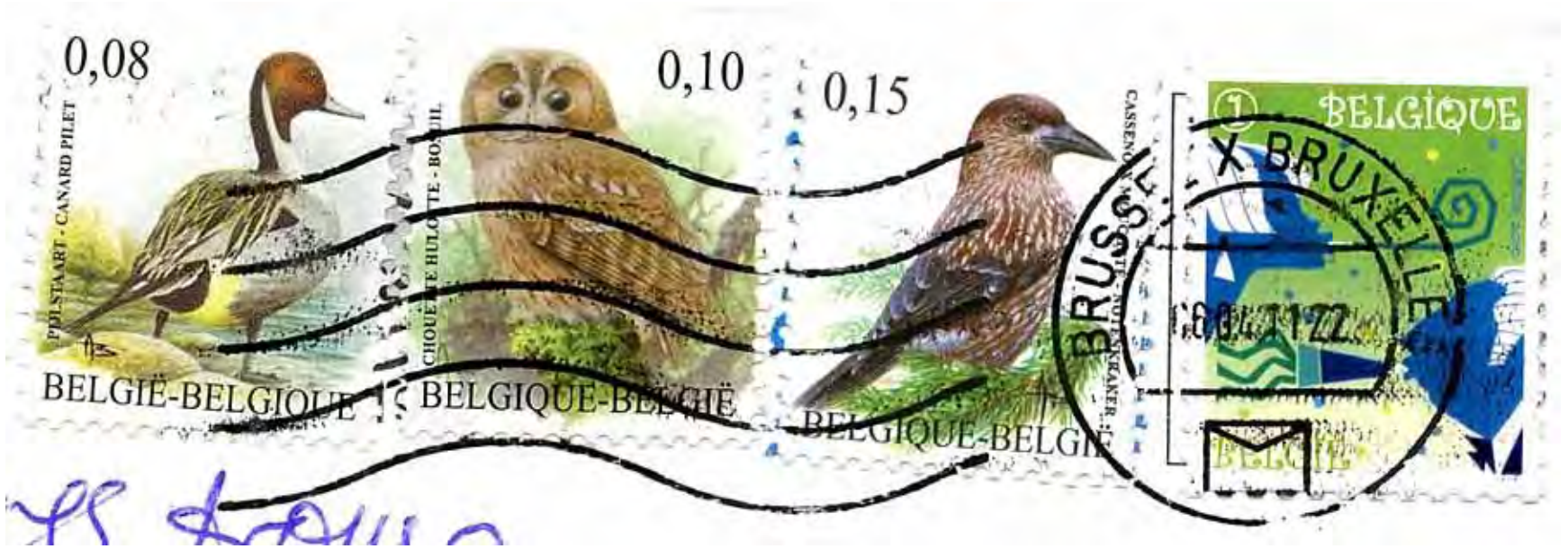
Timestamping (horodatage, estampillage)

- anciens problèmes

- « le cachet de la poste faisant foi » !!!
  - Voir https://www.arcep.fr/index.php?id=12335 et cette citation …
  - « en France, aucune disposition juridique n'impose aux prestataires de services postaux l'obligation d'apposer un cachet postal sur les plis qu'ils acheminent. De même, aucun texte ne définit la notion de « cachet de la poste », ni ne précise les mentions qu'il doit comporter pour apporter une sécurité juridique suffisante. »
    - Le saviez-vous ? Et idem en Belgique, et, sans doute, partout !
    - Le concept d'heure et de date n'est pas simple ☺ voir https://fr.wikipedia.org/wiki/ISO_8601

- Synchronisation des horaires de train (gares = heure locale) : Einstein, relativité restreinte, GPS !

« Cachet de la poste faisant foi »



Mais donne-t-il foi ?

Tableau d’affichage (public) :
« ledger » : ordre des opérations, date crédible ?

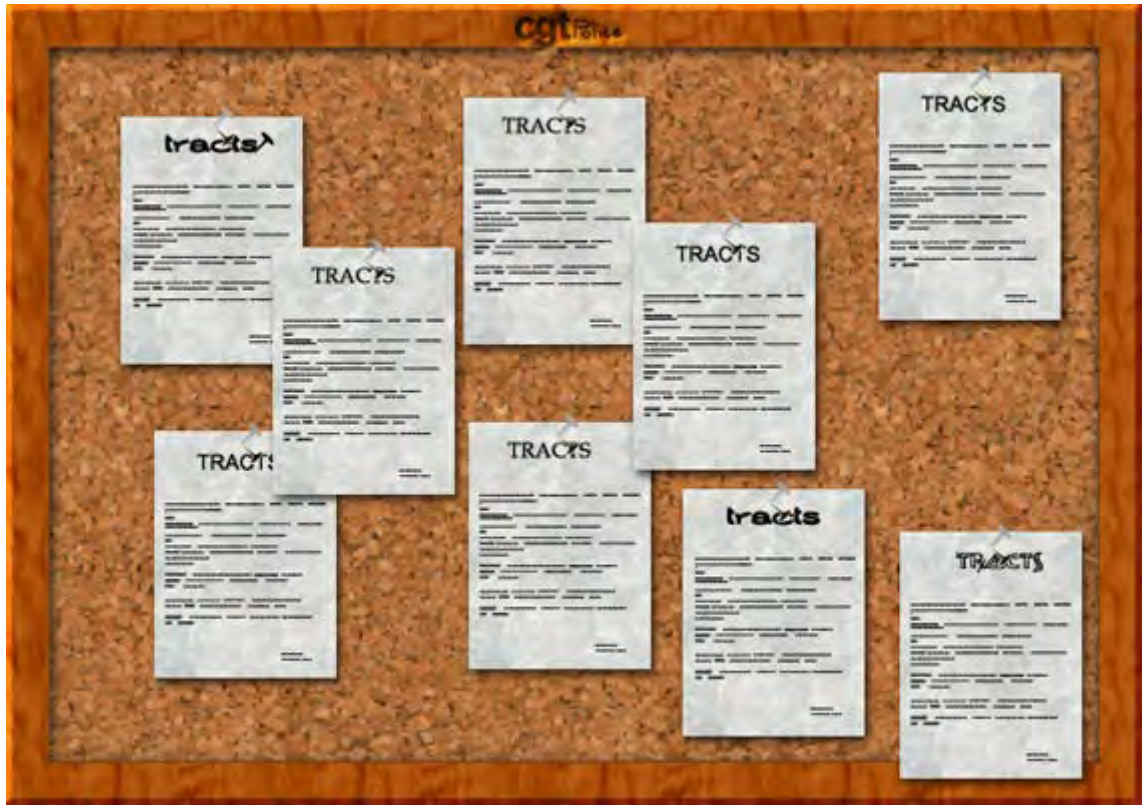
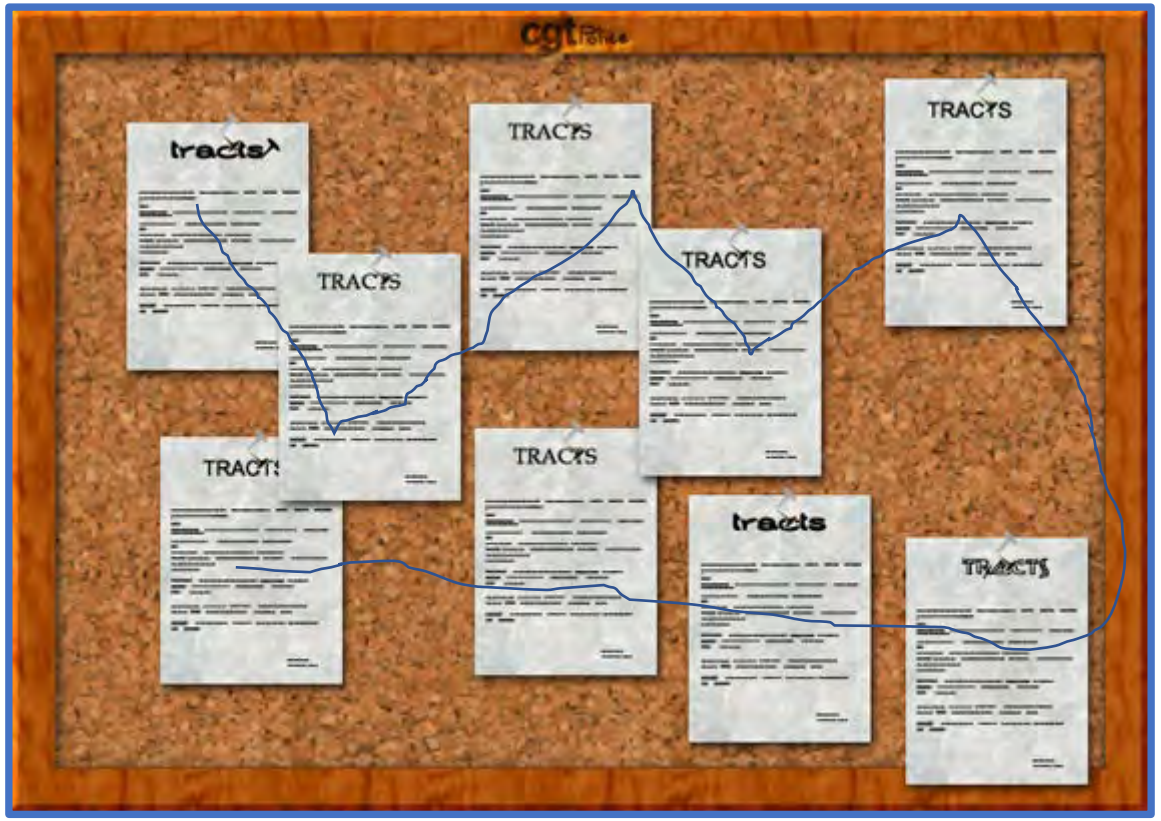
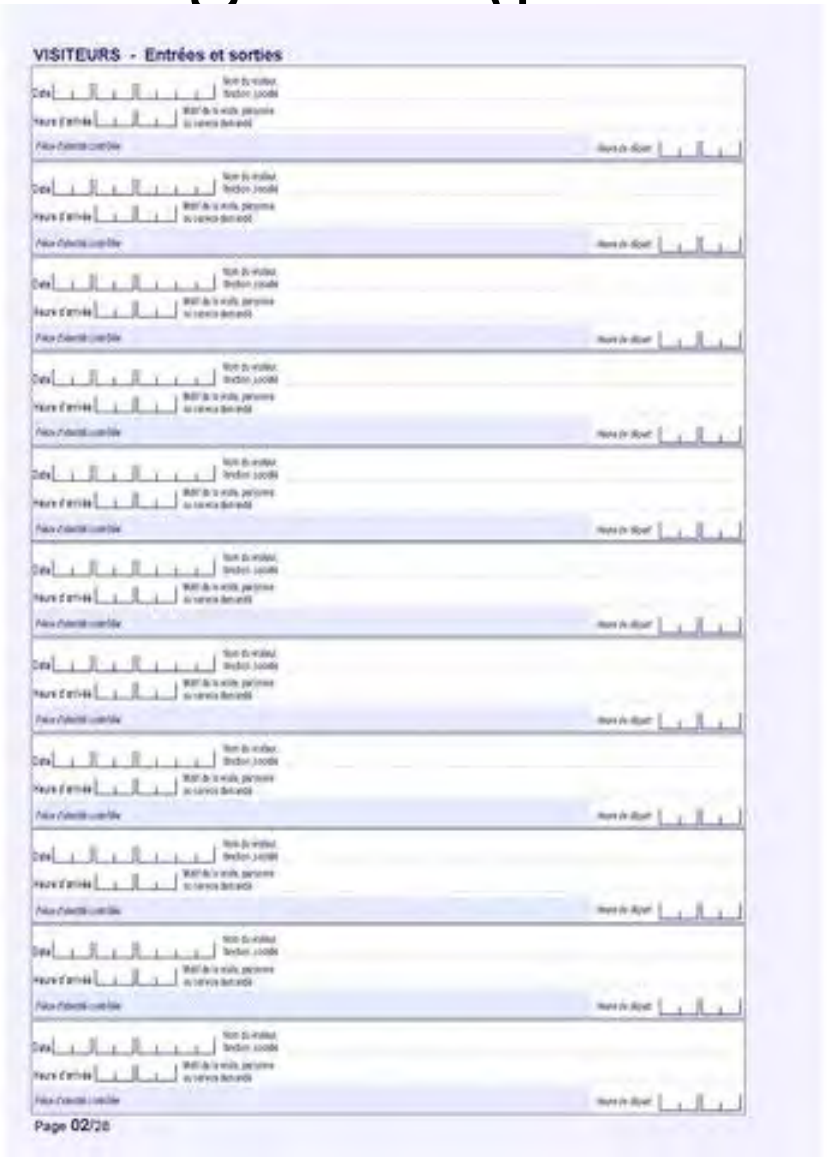


Tableau d’affichage (public): ledger : ordre des opérations ?



Secure Public Board to avoid adding dangerous noise or removing cards: the delicate part of it.

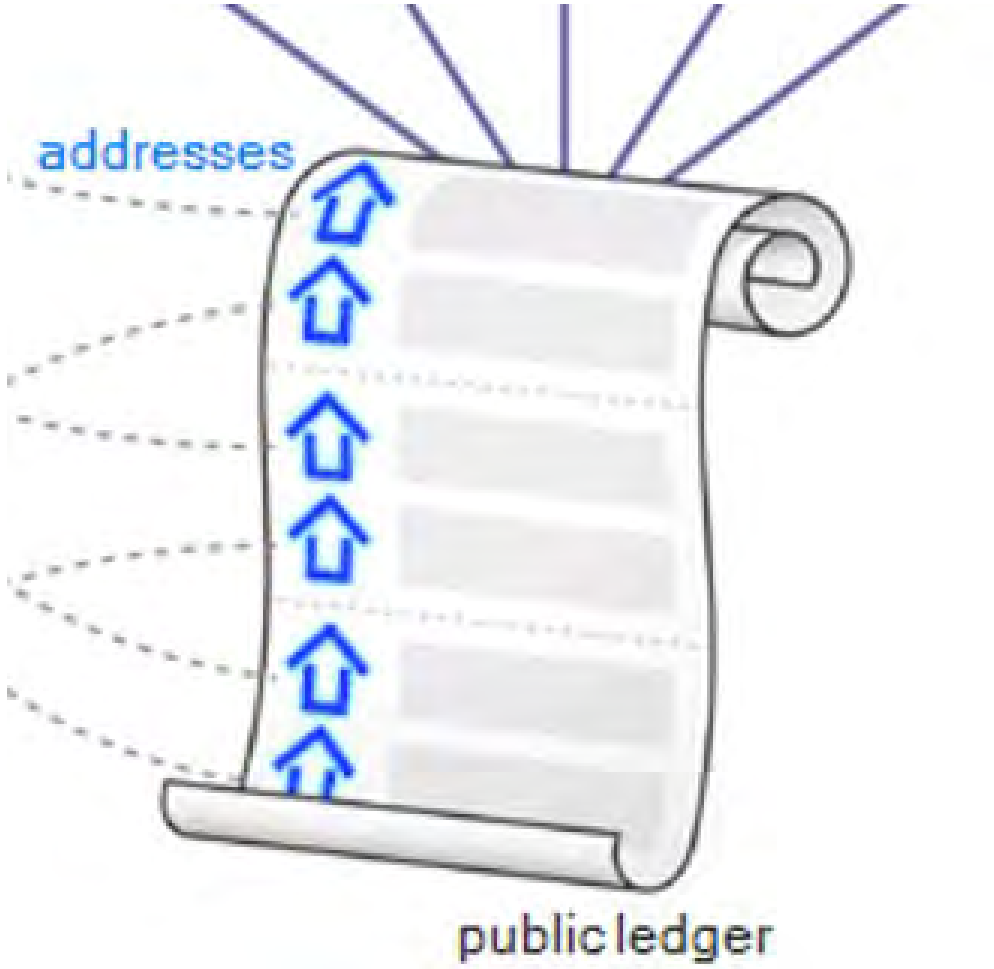
Registre (présences dans l'ordre temporel)



temps

Difficile à modifier,
ajouter,
ratures interdites, …

Affichage public, ordonné dans le temps



Plus sûr (vitre blindée. serrure)

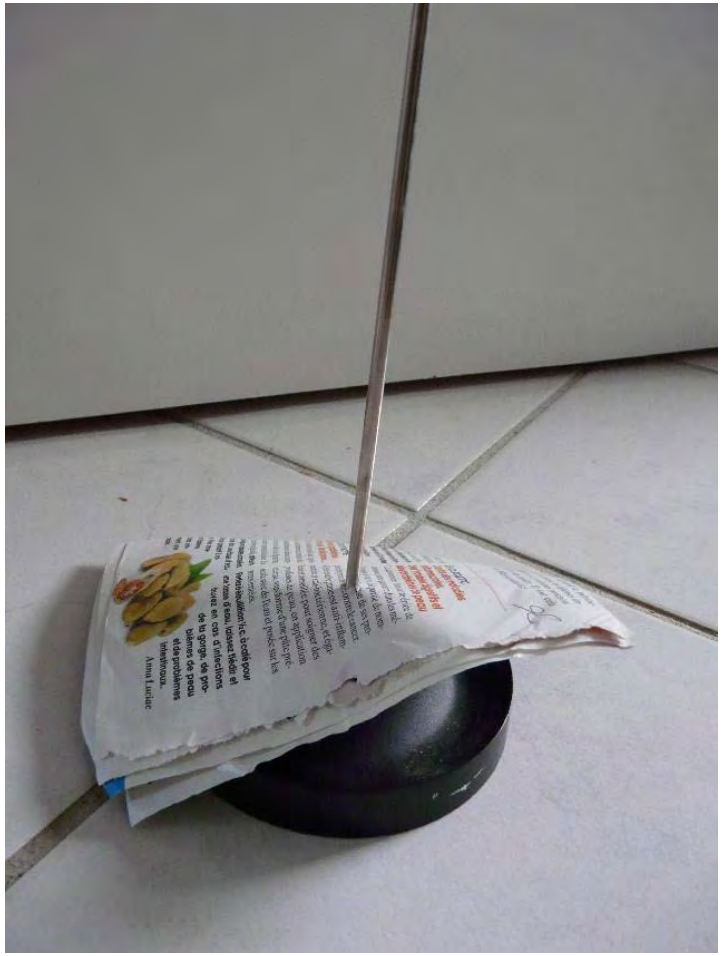
Qui a la clé ?

« Autres exemples »

- Arbres généalogiques royaux (c'est public),
- Titres de propriétés (maison, terrain, …) : cela donne la succession des propriétaires et des événements survenus liés aux différents actes,
- *Un notaire peut faire cela mais c'est un **tiers**-partie de confiance,*
- *Authentifier des événements, leur ordre, éviter la double vente d'une propriété, c'est un rôle rempli par un notaire mais peut être réalisé autrement (blockchain).*

Pique-notes et blockchain

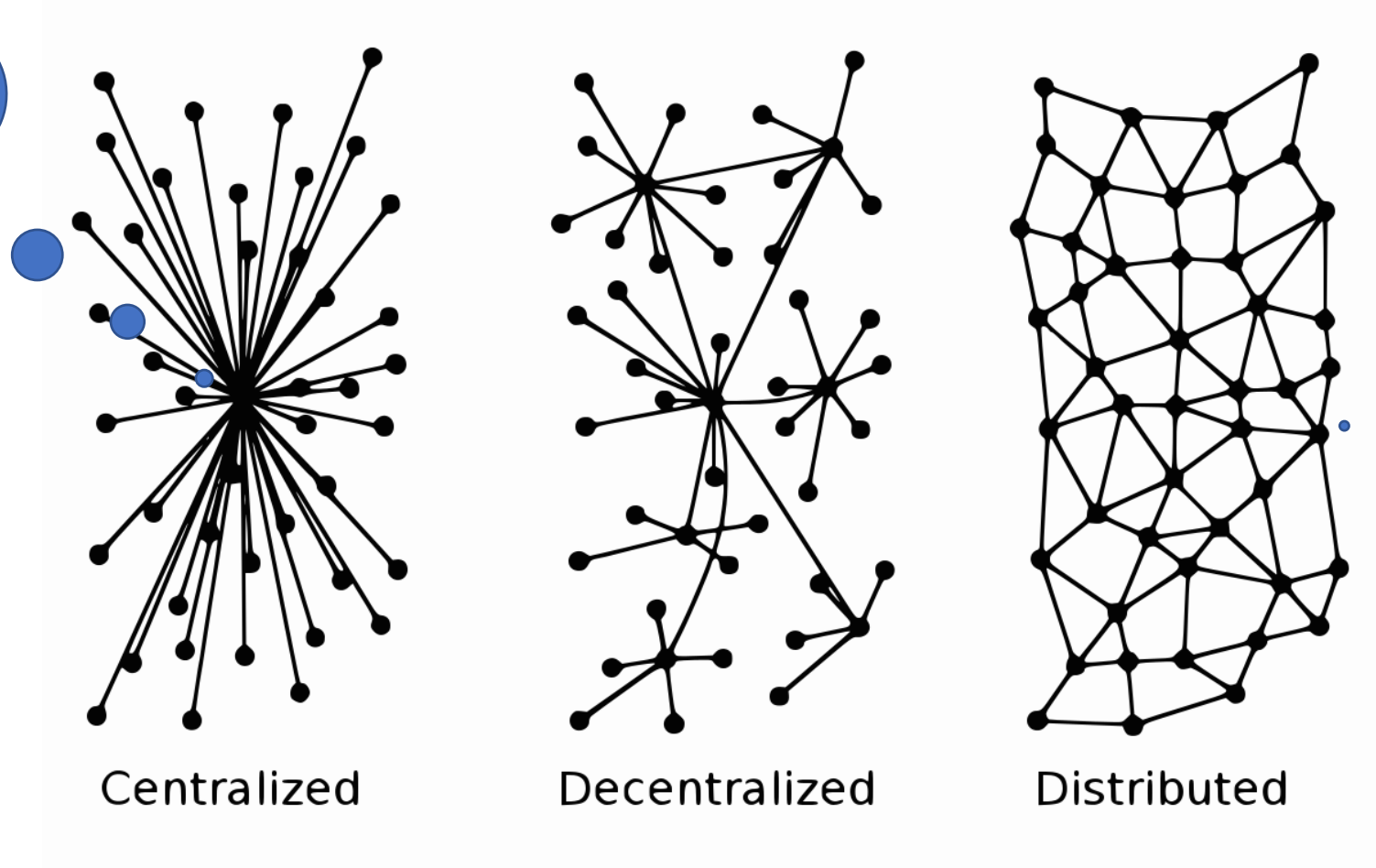
Pique-notes pour tickets de caisse (message spike)



Modèle plus sûr

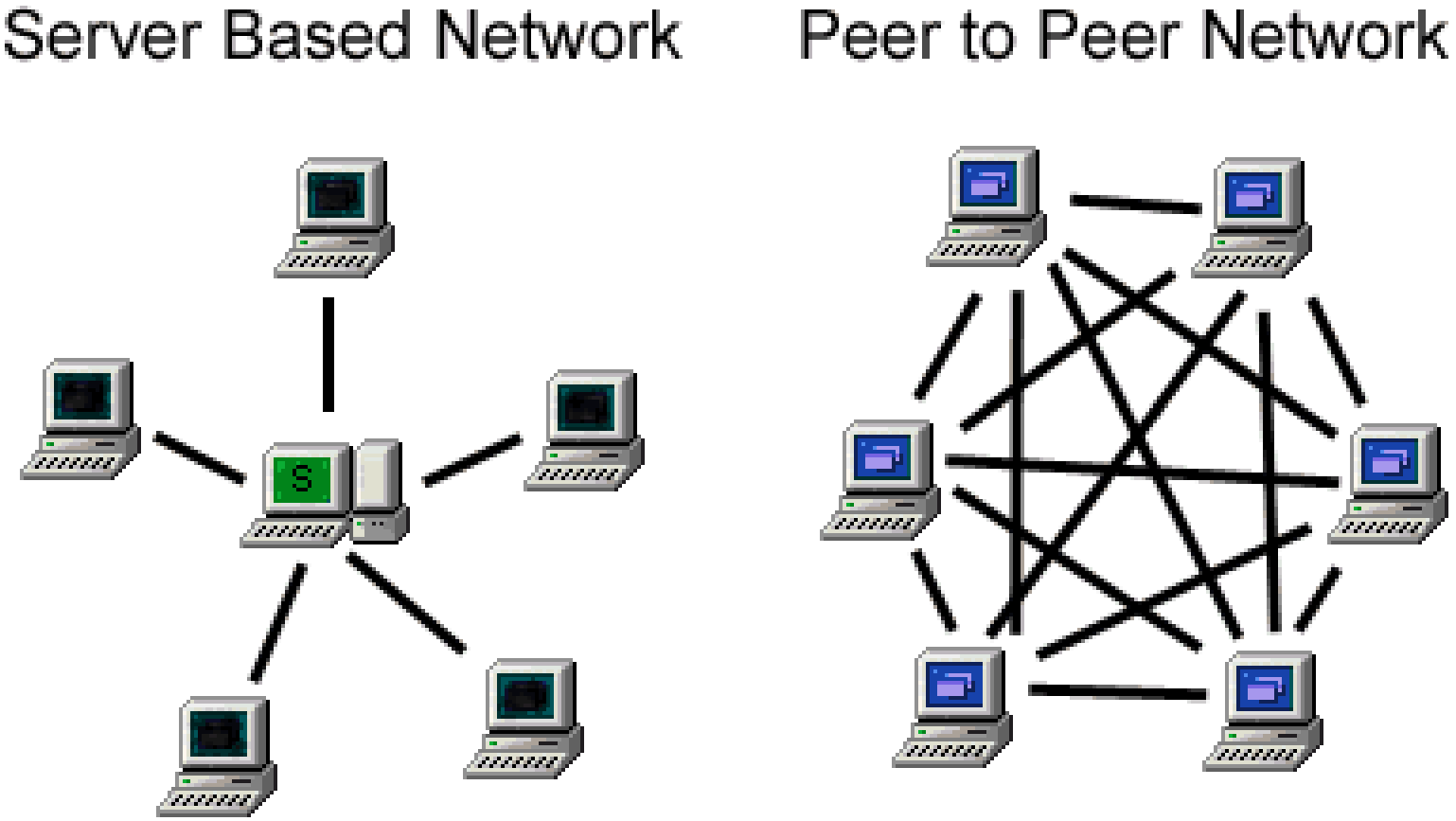
Réseau de communication : Internet (distribué)
Paul Baran (1963)

fragile



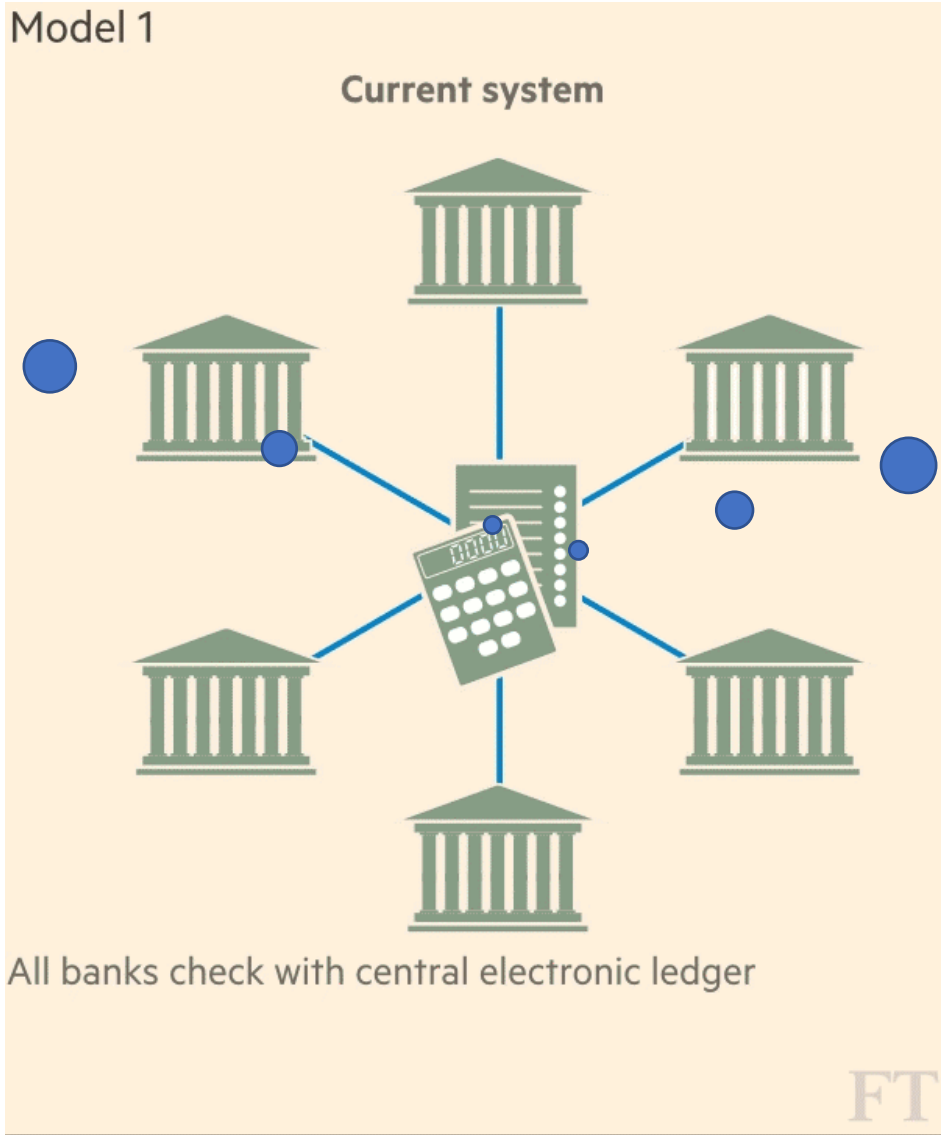
robuste

Peer to peer (« virtuel »)
pair à pair



Modèle courant pour les banques (avec intermédiaire)

Clearing (compensation)



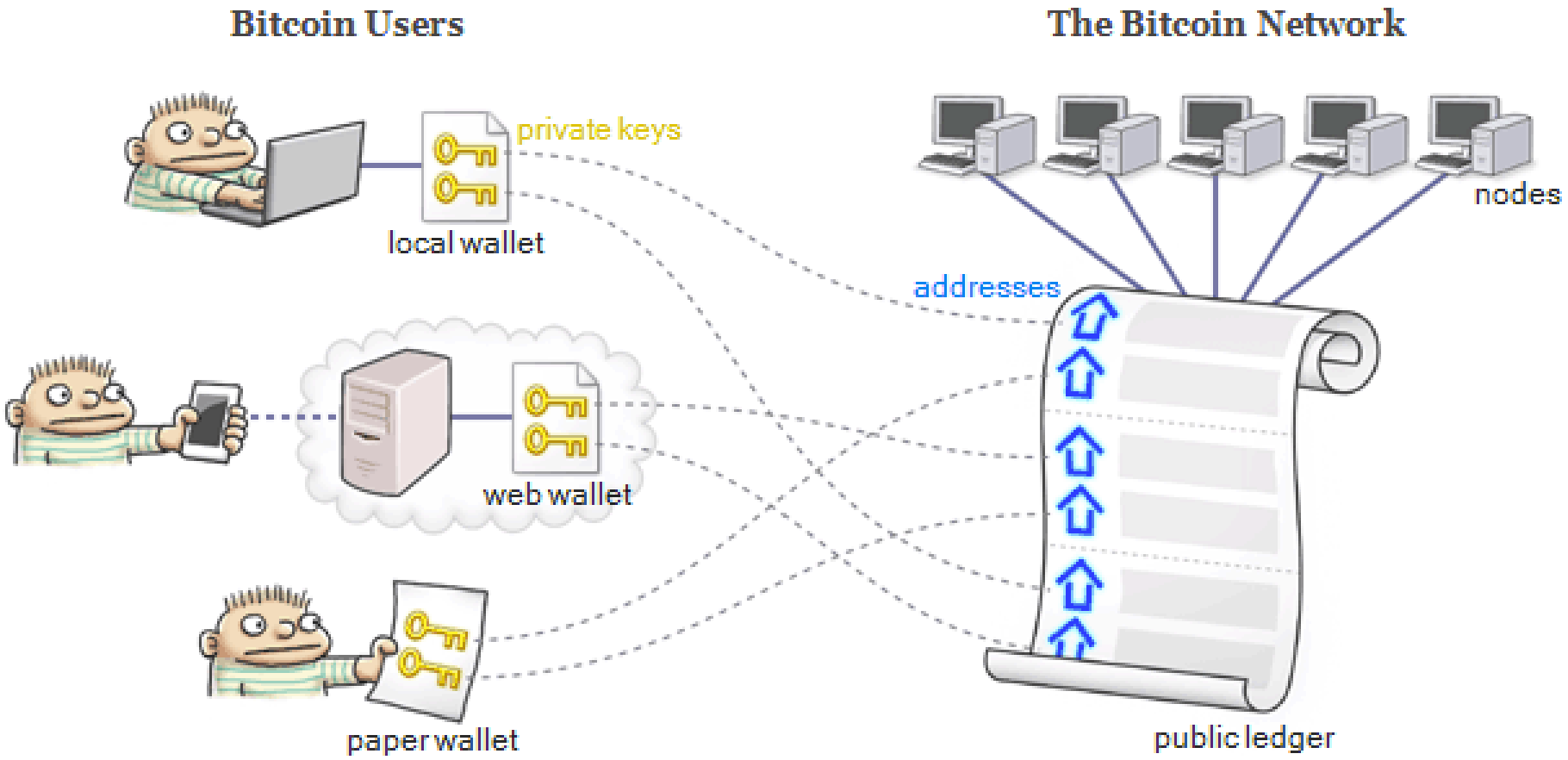
Les blockchains pourraient supprimer cet intermédiaire

Les outils cryptographiques

- Cryptographie à clé publique
- Signature
- fonction de hash
- Merkle: signature, arbre (tree)

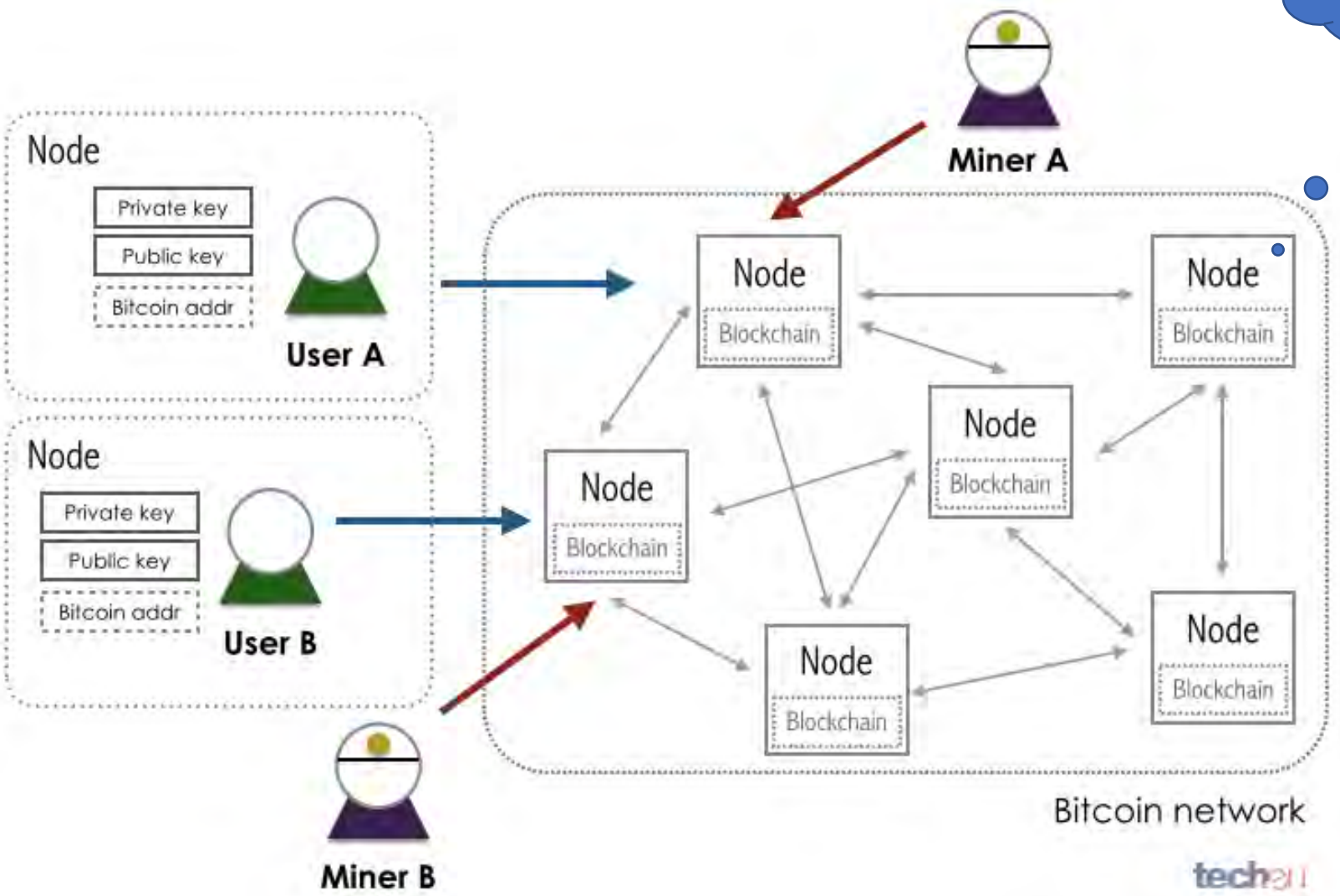
- Les fonctions de hash vont permettre de lier entre eux de façon solidaire et non modifiable les informations publiées dans le tableau d’affichage

Public ledger, bitcoin et blockchain



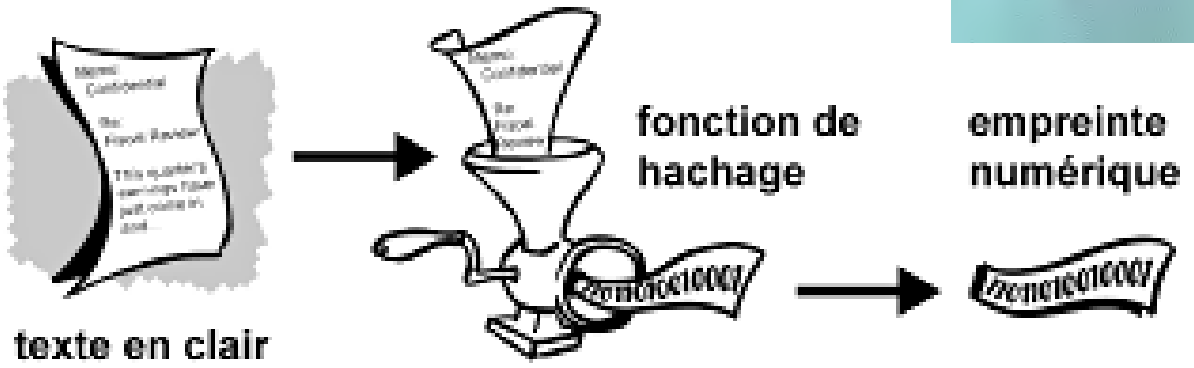
Blockchain dans bitcoin

Copies multiples



Cryptographic hash function

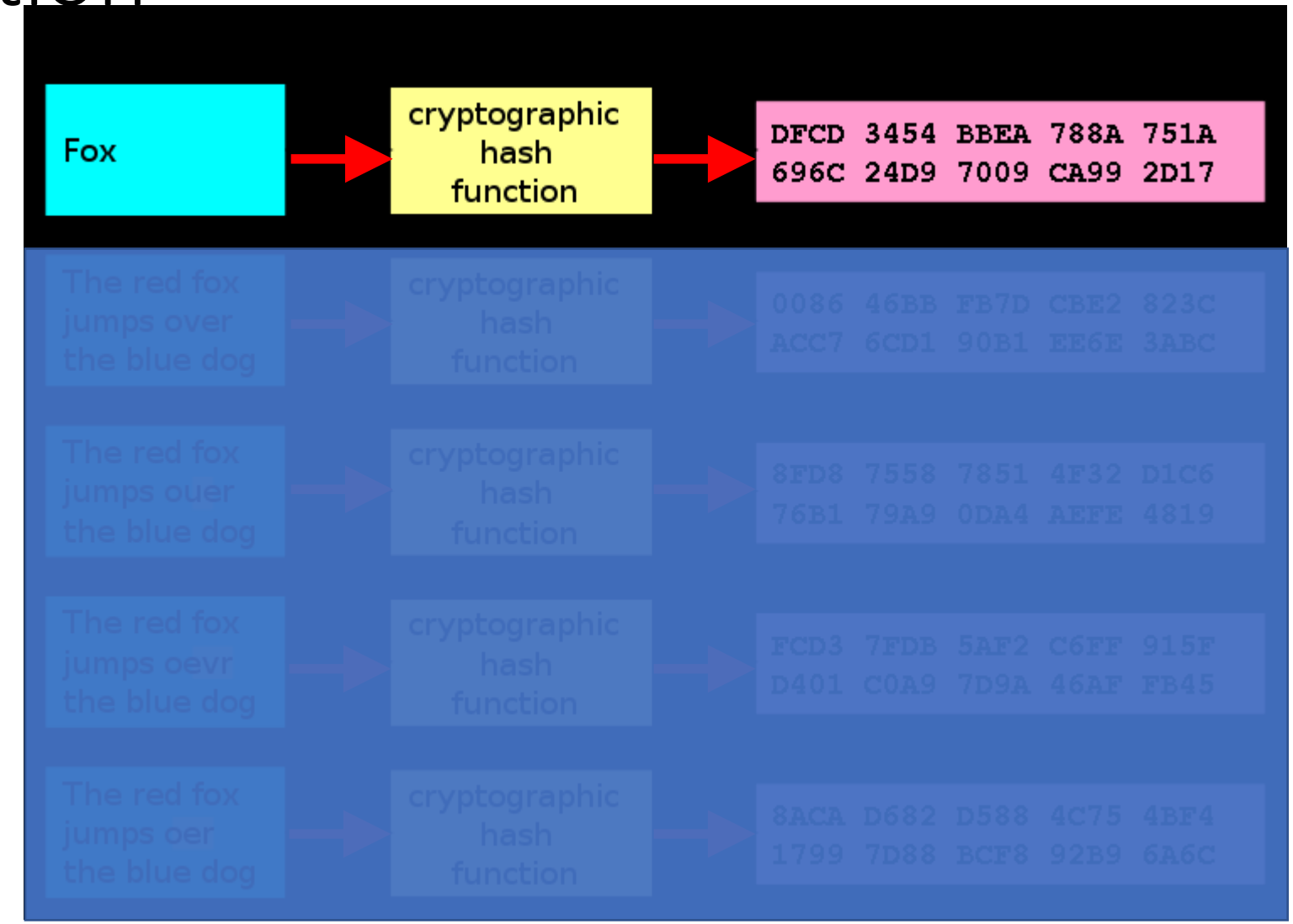
- Facile à calculer,
- Difficile à inverser (trouver un texte clair qui correspond à une empreinte),
- Facile à vérifier avec le texte clair et l'empreinte,



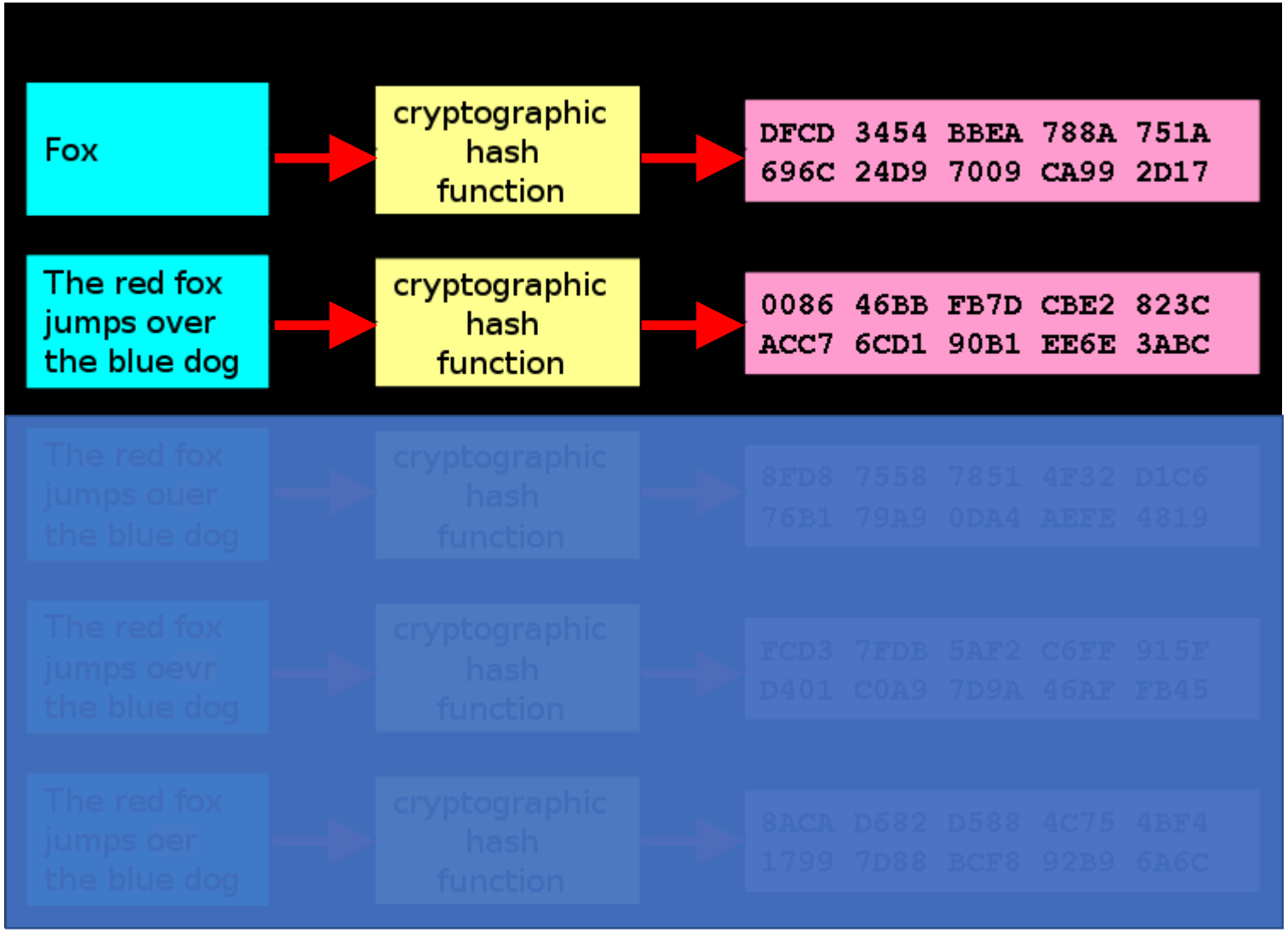
- Difficile de trouver des collisions (deux personnes qui ont la même empreinte),
  - En général,
  - Etant donnée une empreinte comme cible,

- Fonction mathématique avec donc des propriétés spéciales, rares.

Cryptographic hash function : utilisation

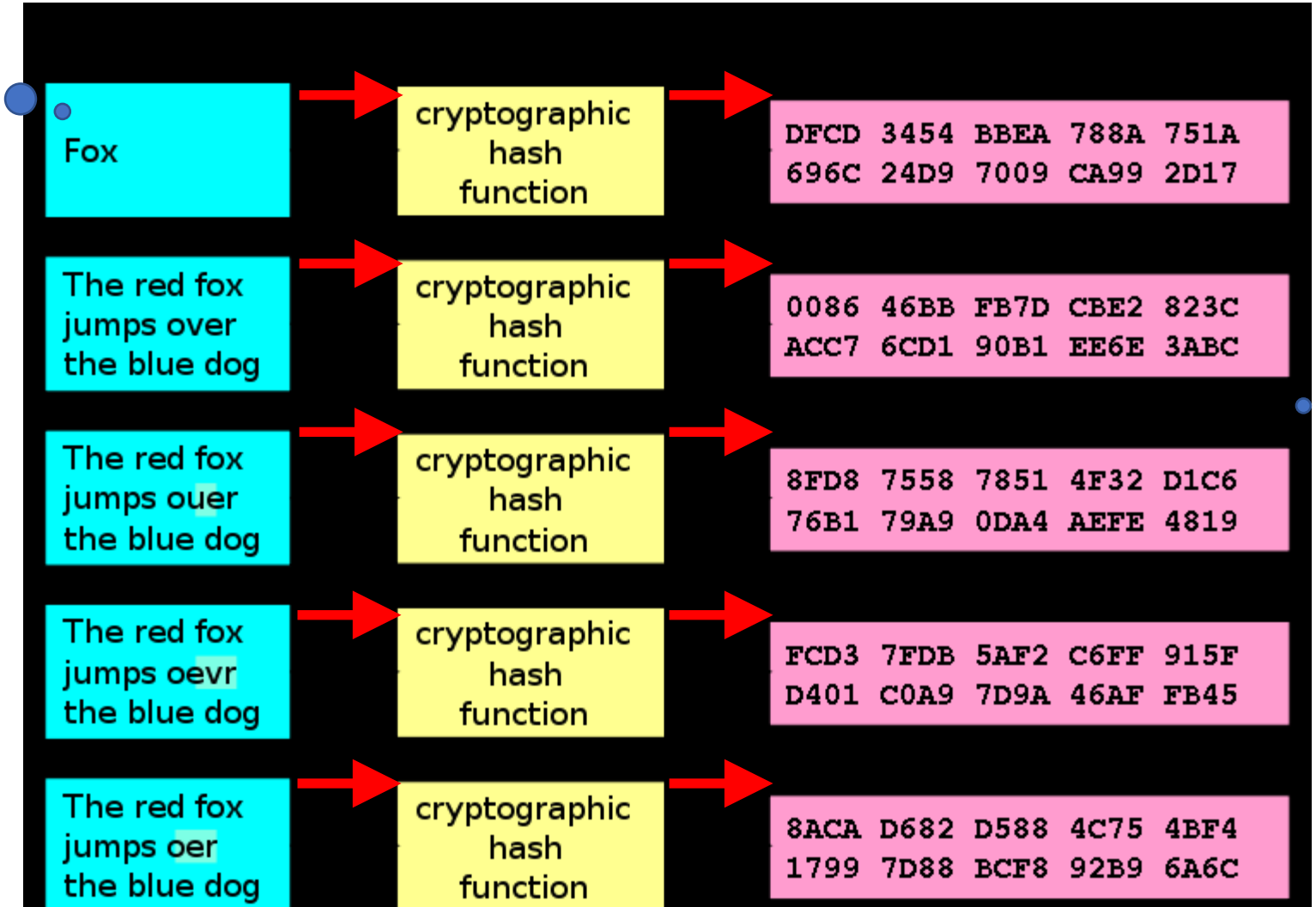


Cryptographic hash function



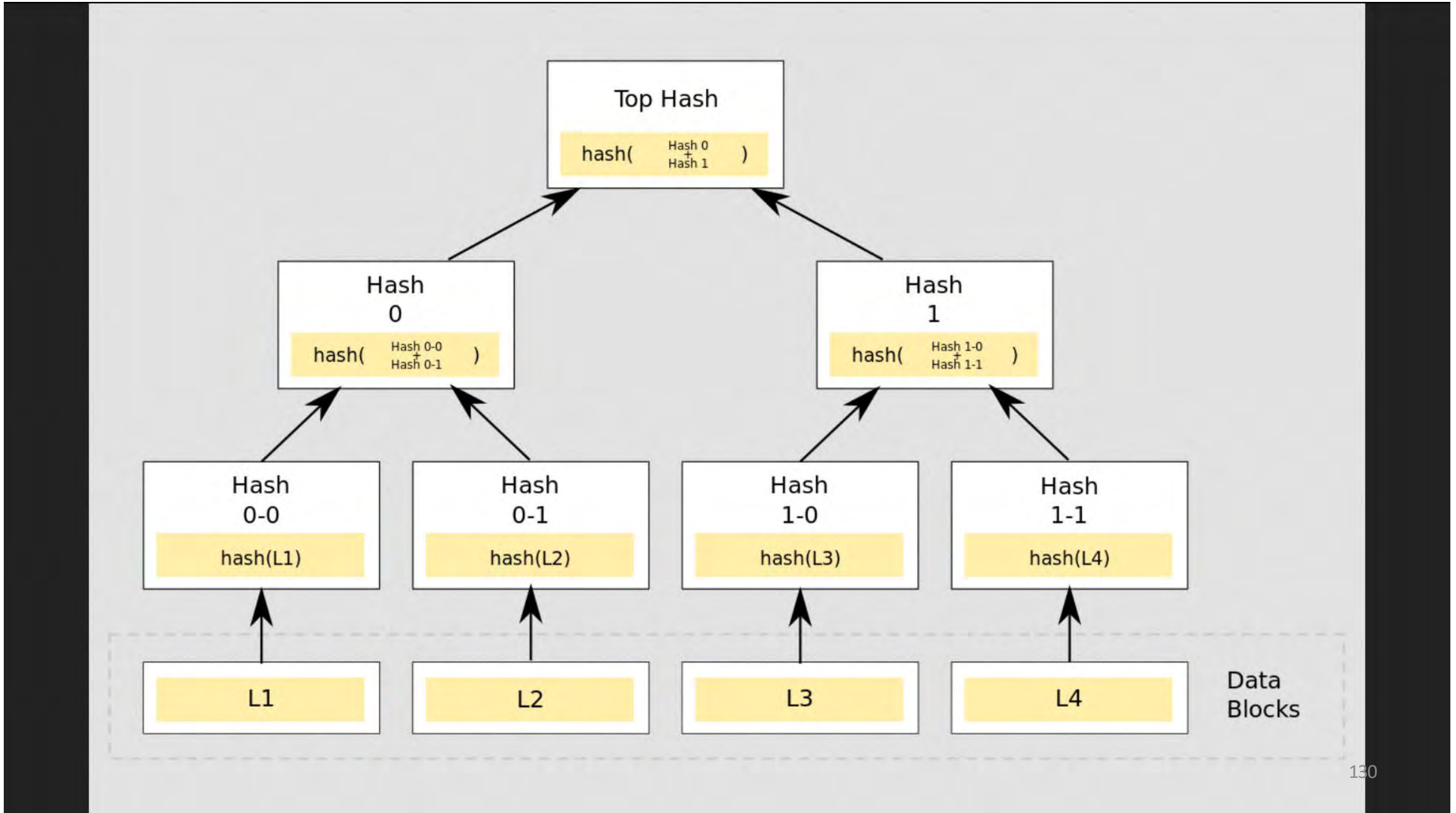
fonction de hash cryptographique = calcul d'une fonction spéciale (très sensible à une petite modification)

Texte d'entrée

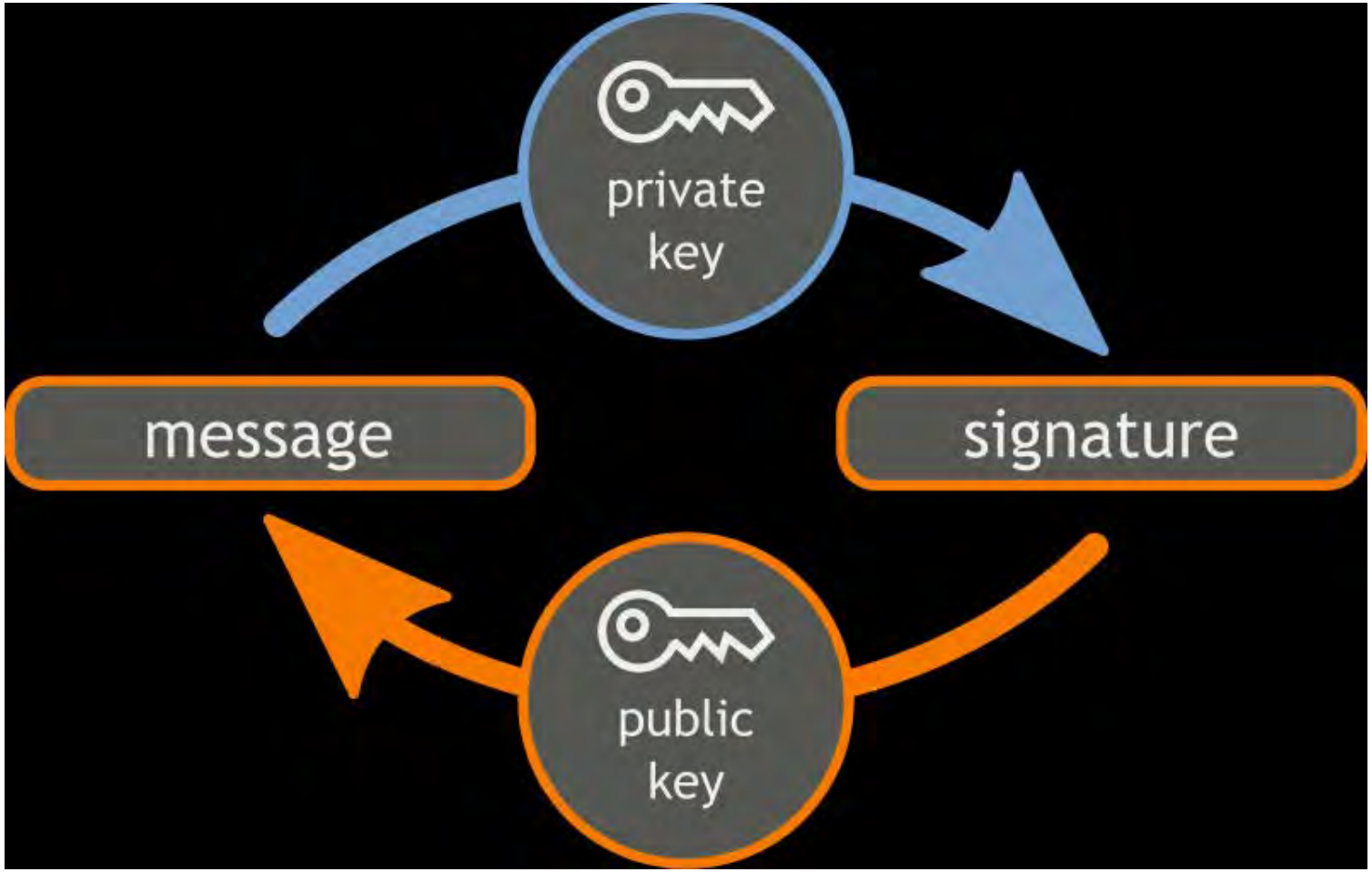


Le hash est une suite de caractères

Merkle tree (arbre) : hash de hash

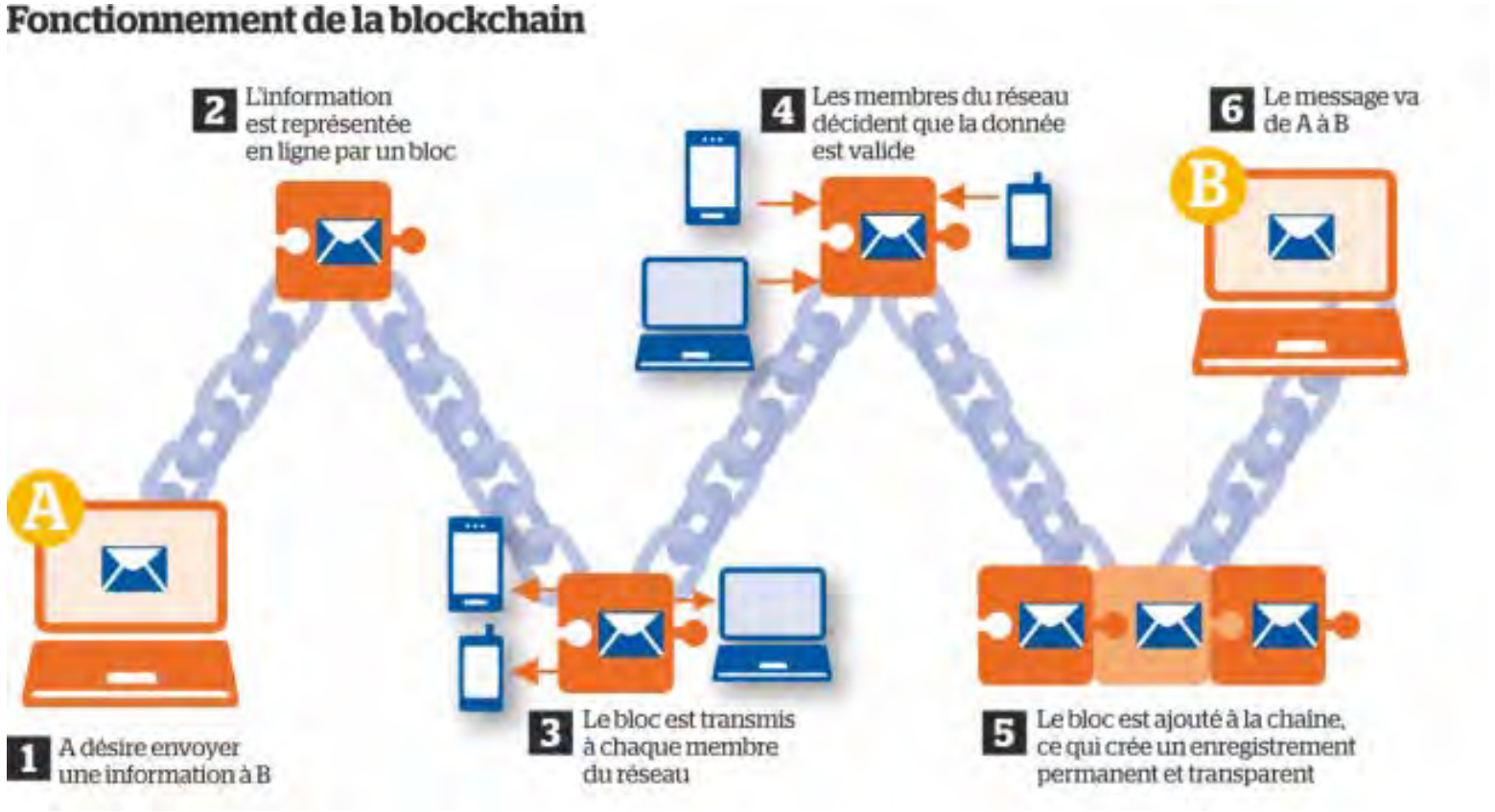


Digital signature (concept) : 2 clés par utilisateur



Chaîne en construction

- usage séquentiel,
- Merkle tree pour les blocs (1978) …

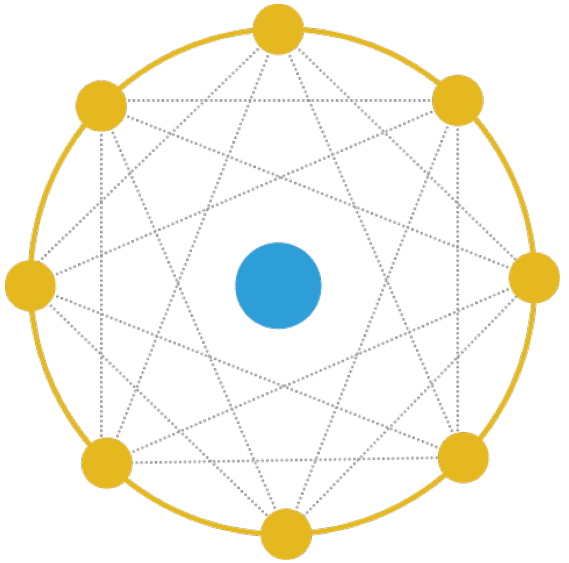


Distributed trusted third-party

- The concept!
- The really new idea inside bitcoin,

- Everybody get a copy, able to verify everything,
- No more monopole of confidence-trust!

Qu’est ce que la confiance décentralisée ?



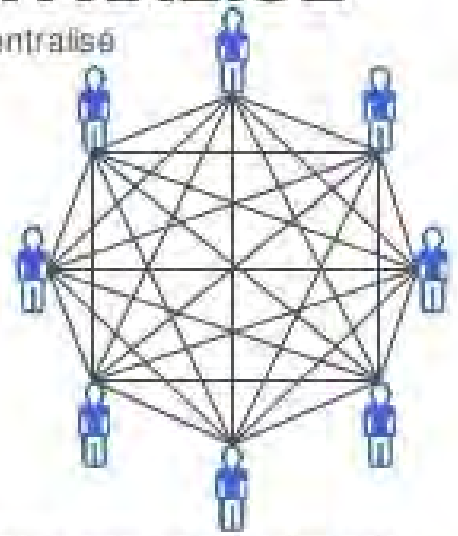
- Accorder une confiance forte à des informations non gérées de façon centralisée par un tiers de confiance.
- Faire confiance aux informations sans faire confiance aux participants au réseau.
- Pas de Single Point Of Failure dans la chaine de confiance.
- Tous les participants au réseau peuvent valider des informations et communiquent entre eux.

MODÈLE CENTRALISÉ VS. DÉCENTRALISÉ

Modèle centralisé

- Pas de confiance requise entre les pairs
- Contrôle de l'information et des échanges
- Point de défaillance
- Confiance en le tiers requise
- Pairs dépendant du tiers de confiance

Modèle décentralisé



- Pas de confiance requise entre les pairs
- Pas de point de défaillance
- Pas de dépendance à un tiers de confiance ou à un pair
- Processus supplémentaires requis pour créer le consensus, assurer la sécurité et la transmission de l'information)
- Difficulté d'accès à l'information
- Difficulté à faire évoluer le protocole

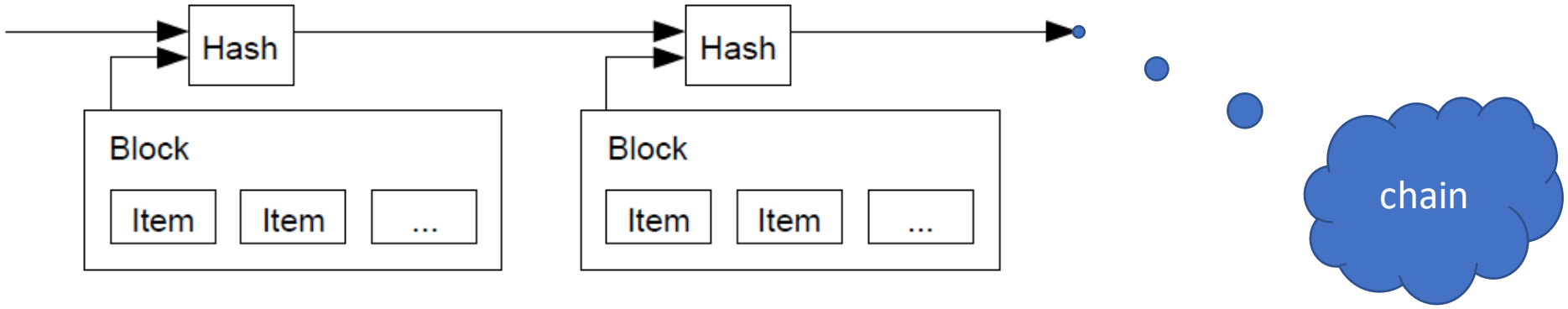
Anonymity -tracability

- By default there is no name, address, URL in the block,
- If wanted it is also possible to hidden the content of the message using the hash function,

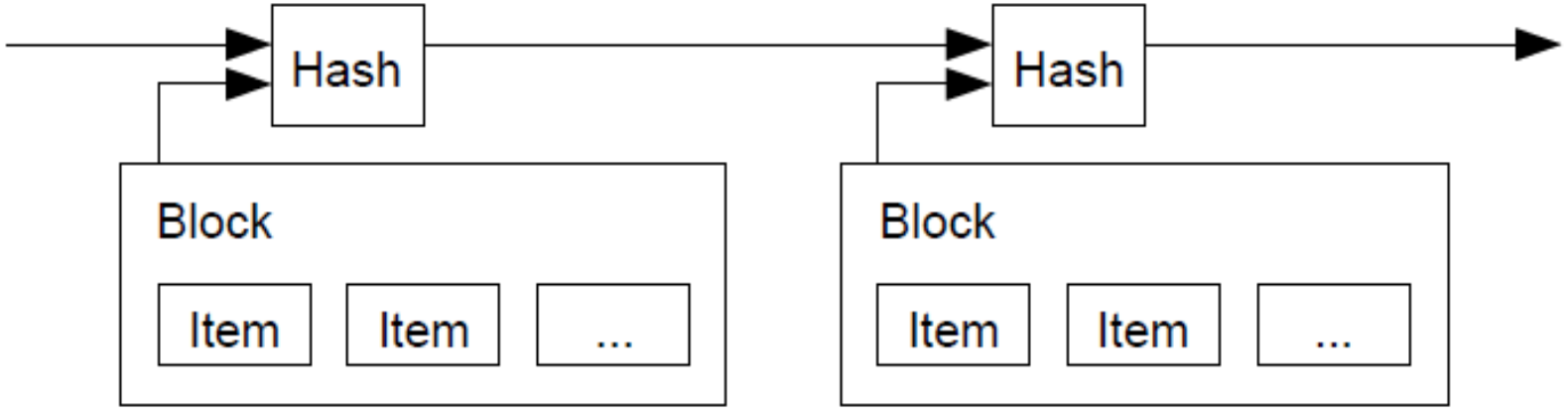
Satoshi Nakamoto : p. 2 du papier original : block et chain

3. Timestamp Server

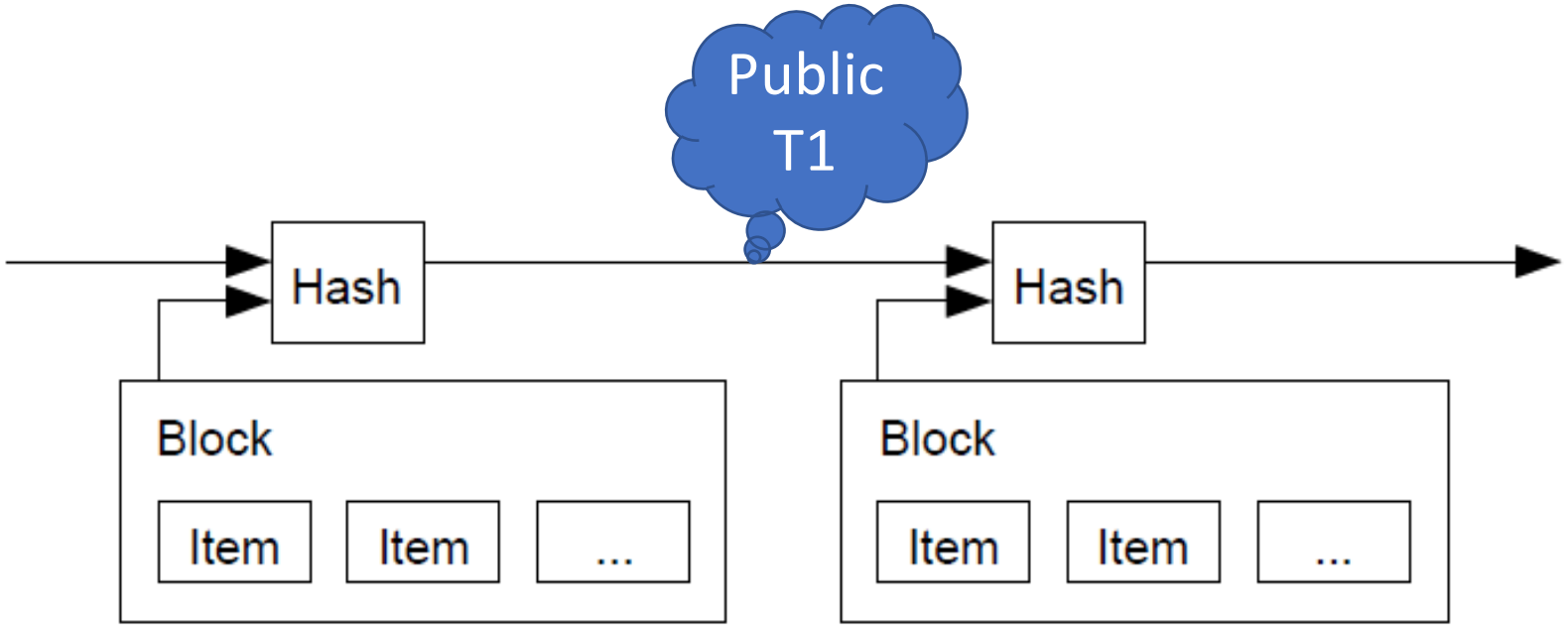
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



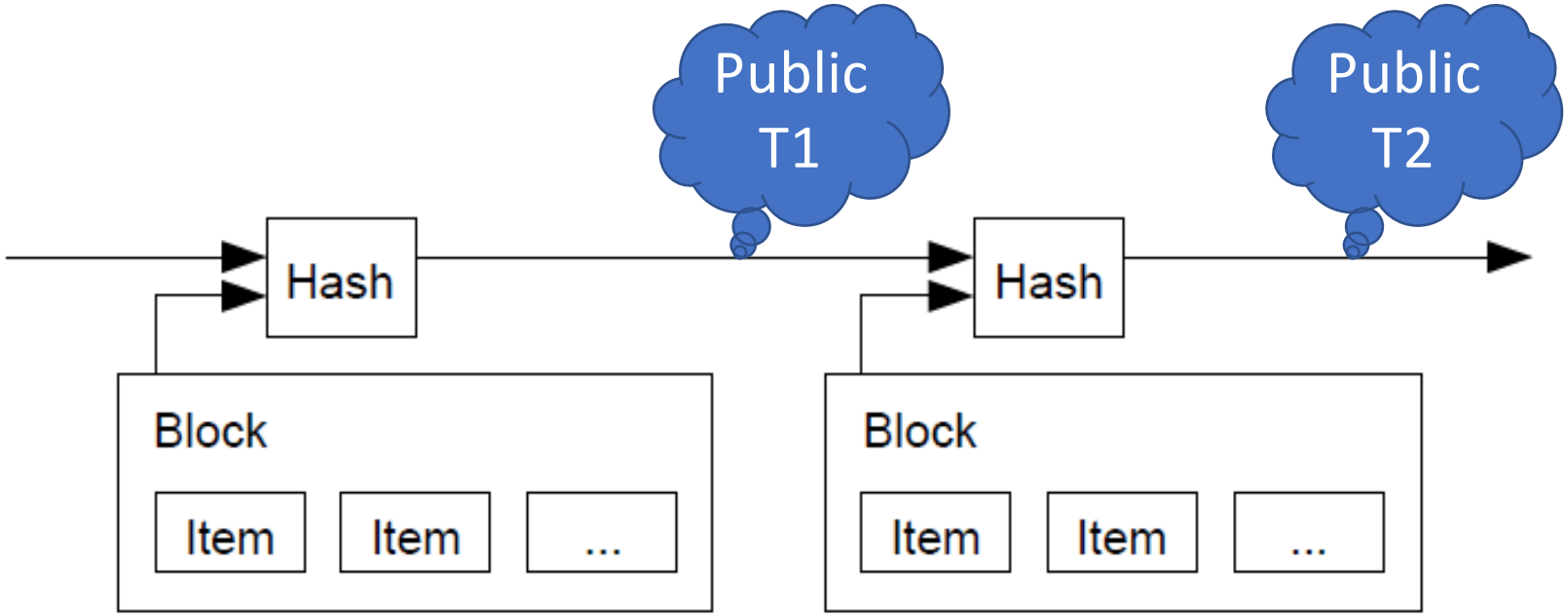
Chain(ing) – publication du hash



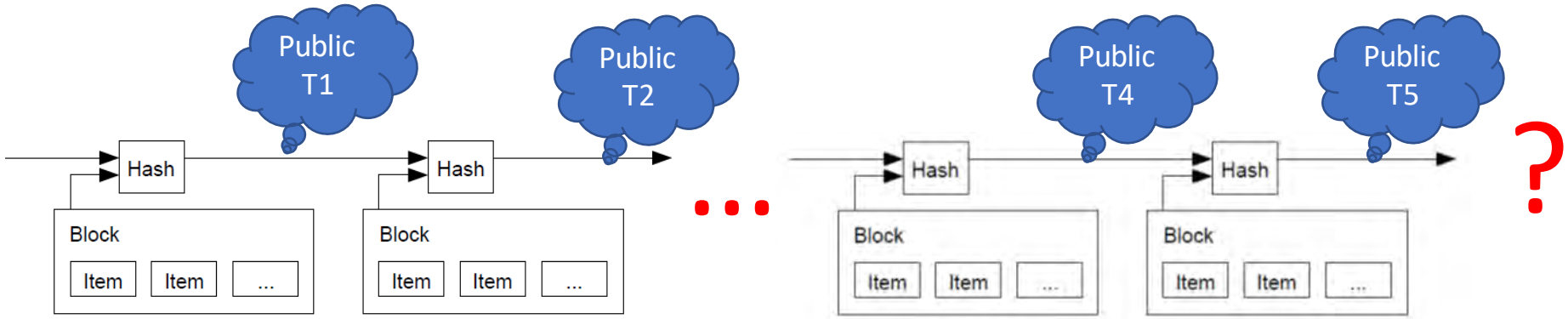
Chain(ing) – publication du hash

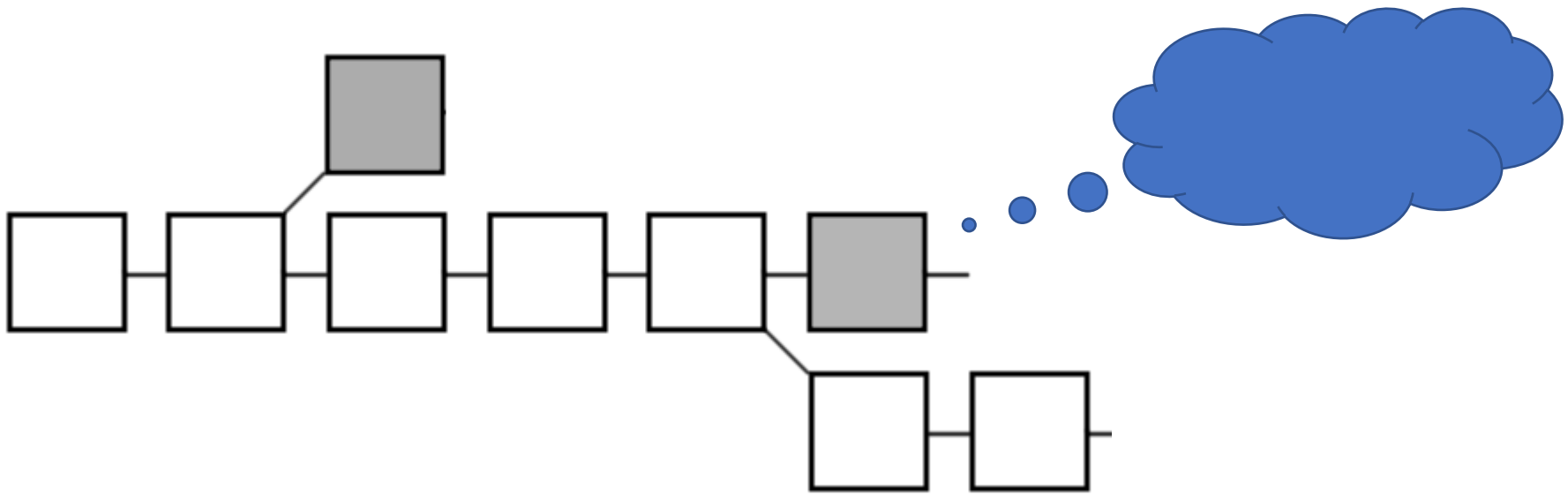


Chain(ing) – publishing the hash



Chain(ing) – hash suivant … ? - fork





Adding the next hash? Who?

- Trusted third-party,

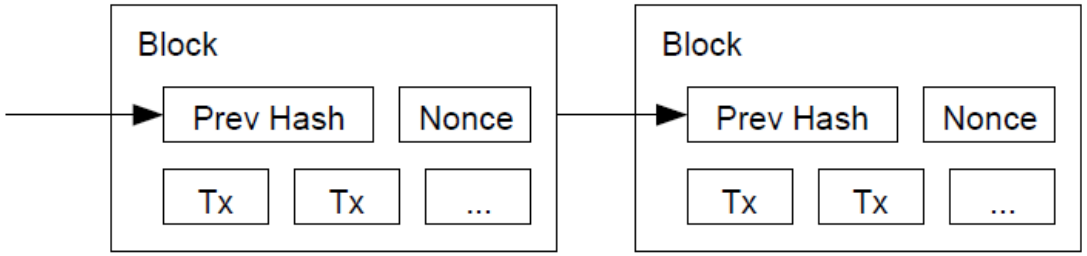
- Distributed and public network?
  - Fair and random choice of the node,
  - problems of delay between nodes!

Preuve de travail (Satoshi Nakamoto, p. 3)

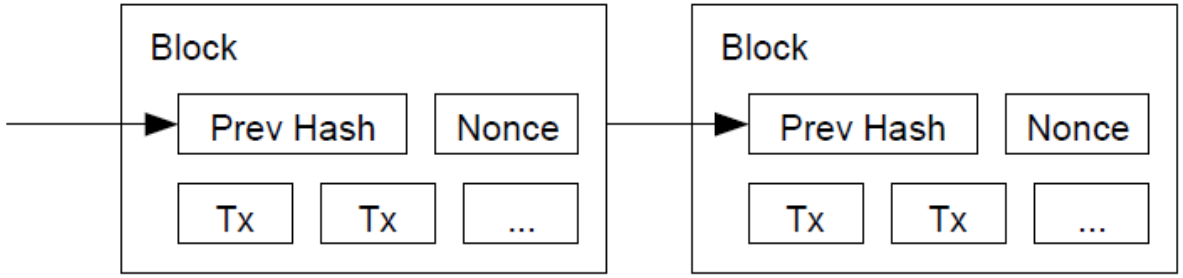
4. Proof-of-Work

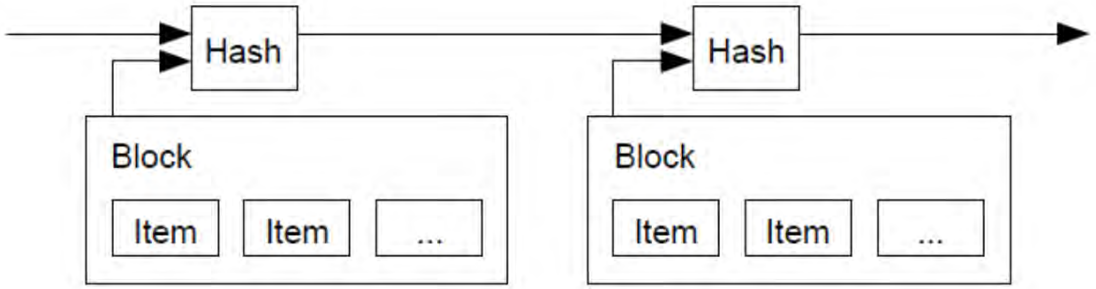
To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



Adding a nonce
(« random » number used one time)



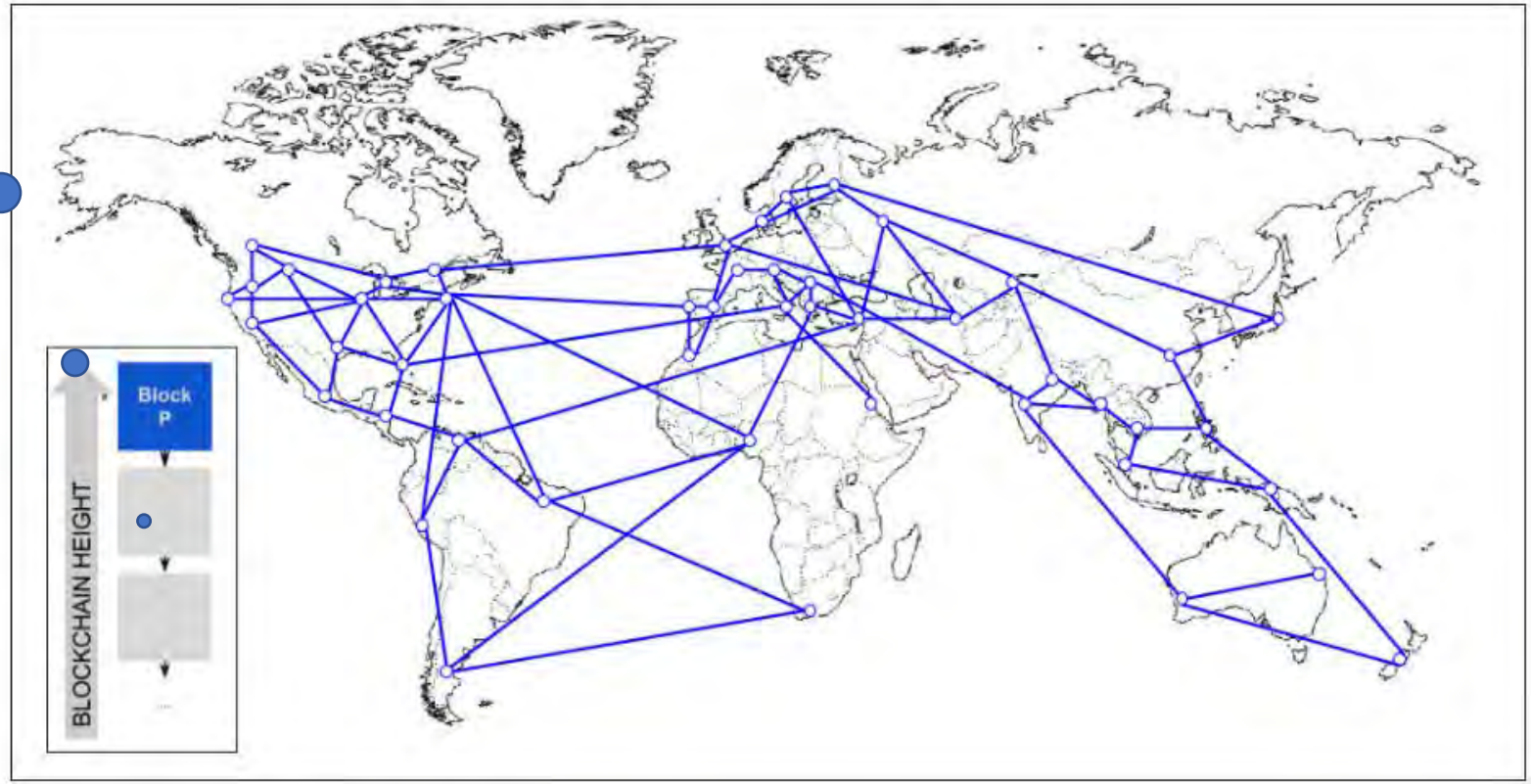


Nonce: special property for bitcoin

- Mining is the process to find an hash with a very specific property (00..0s) thanks to the nonce (to be found)
- Each miner begins with this same problem,
- The winner miner is chosen at « random »,
- And receives 12.5 bitcoins, today (
- Finding the hash is difficult (set at 10 minutes) but the verification of the result is very easy.

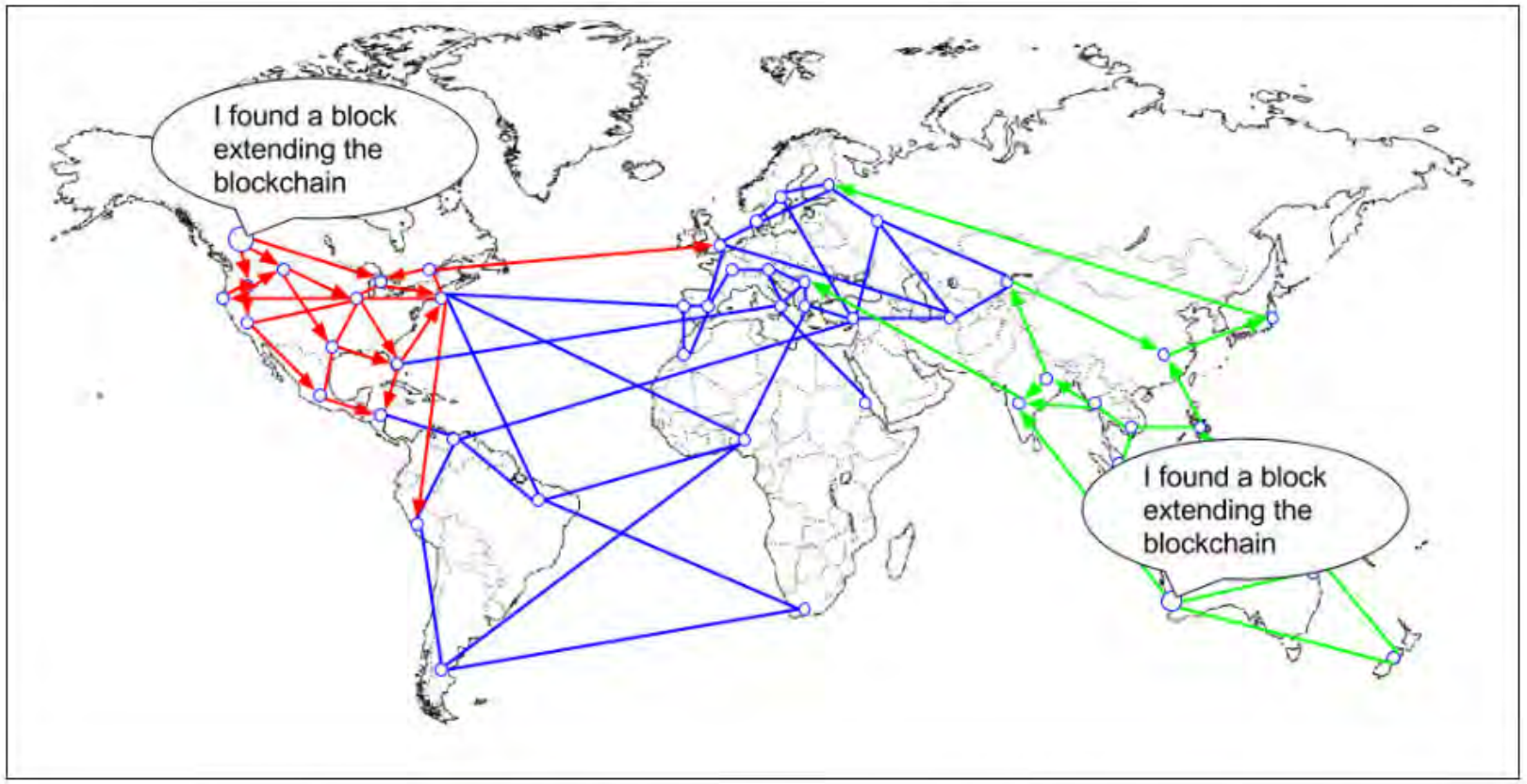
Des nœuds (ordinateurs) calculent ce qui constitue le minage

bloc



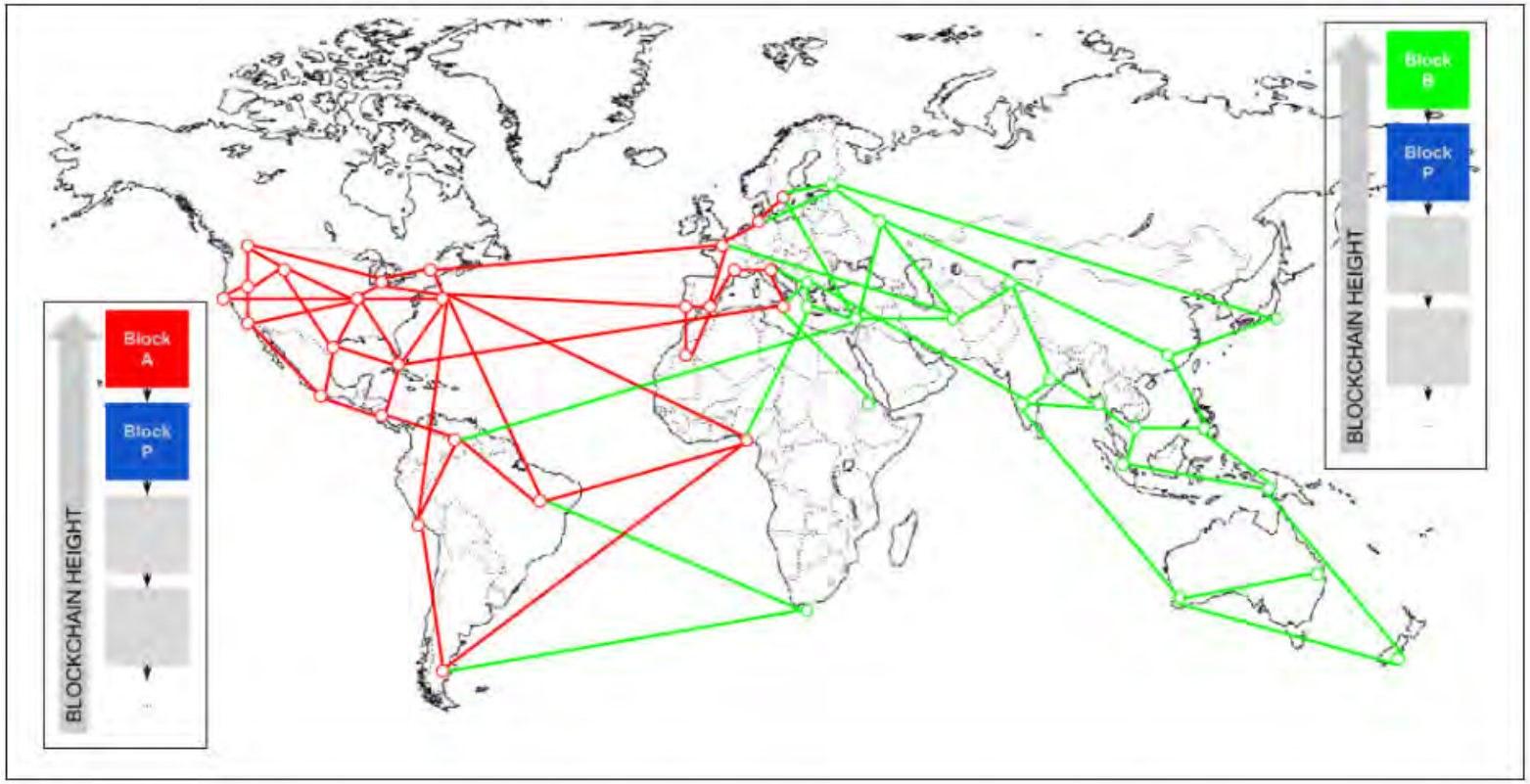
Visualization of a blockchain fork event - Before the Fork

Deux blocs sont trouvés en même temps !



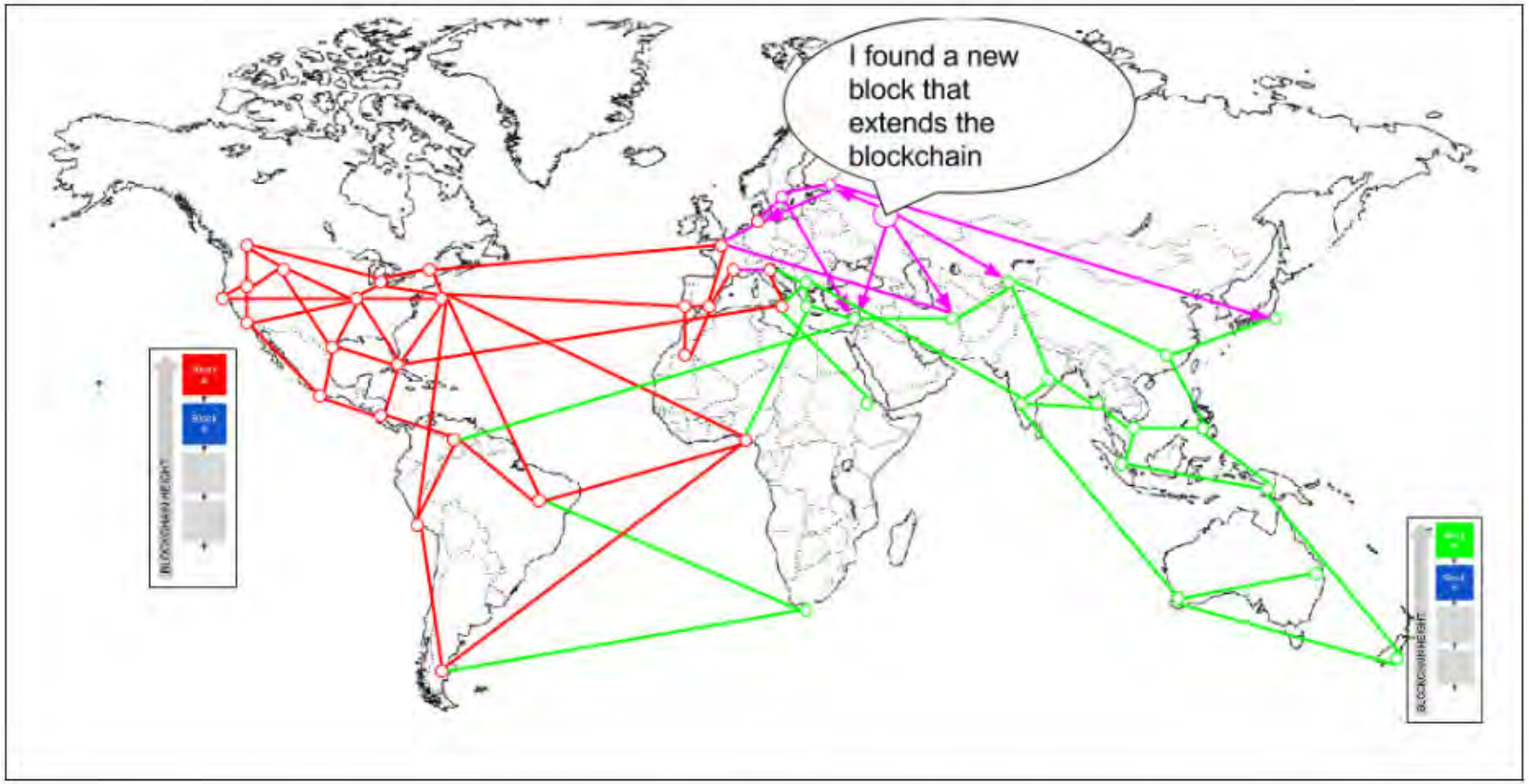
Visualization of a blockchain fork event - Two blocks found simultaneously

Que faire pour rendre la chaîne unique ?



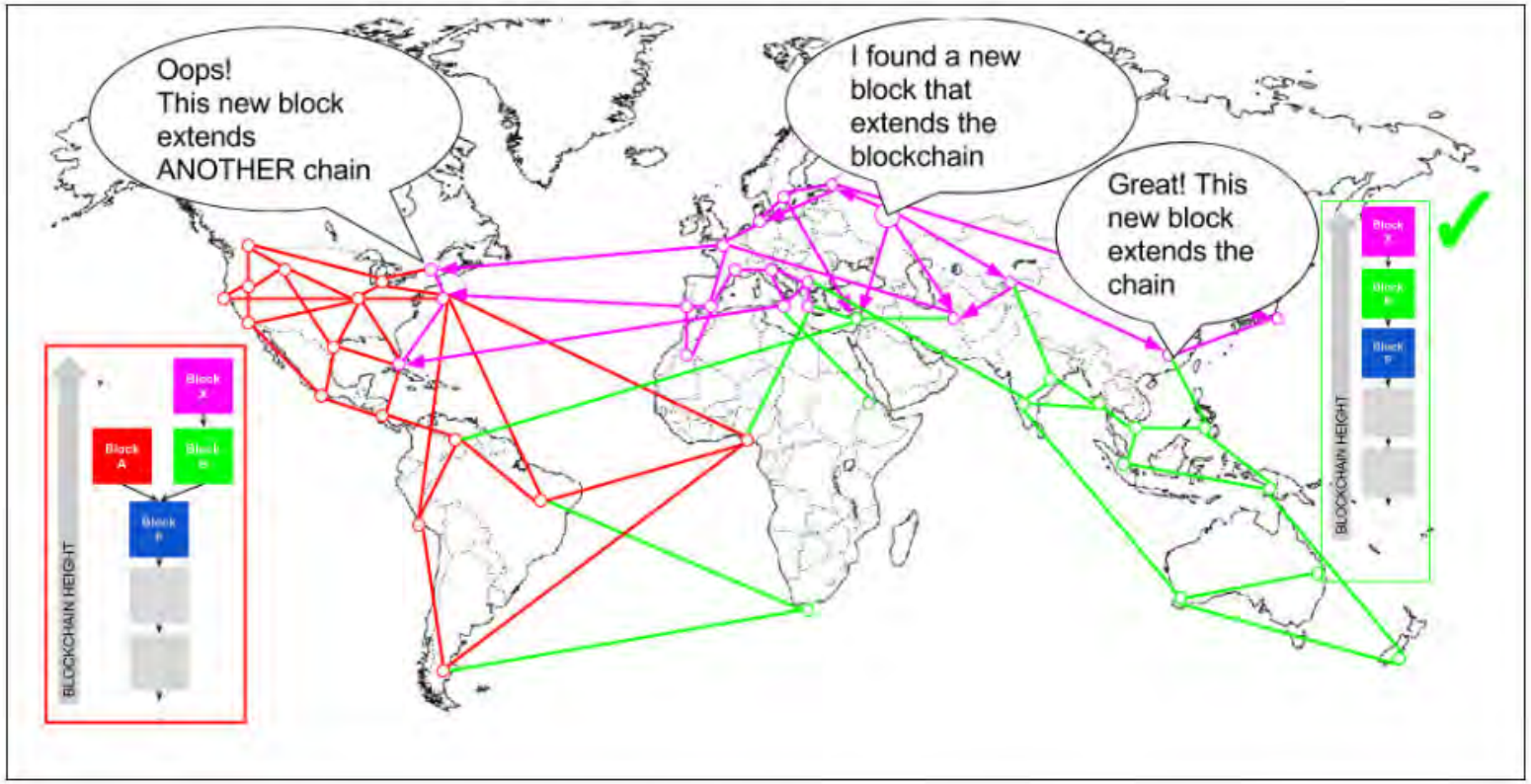
Visualization of a blockchain fork event - Two blocks propagate, splitting the network

Un bloc de plus …



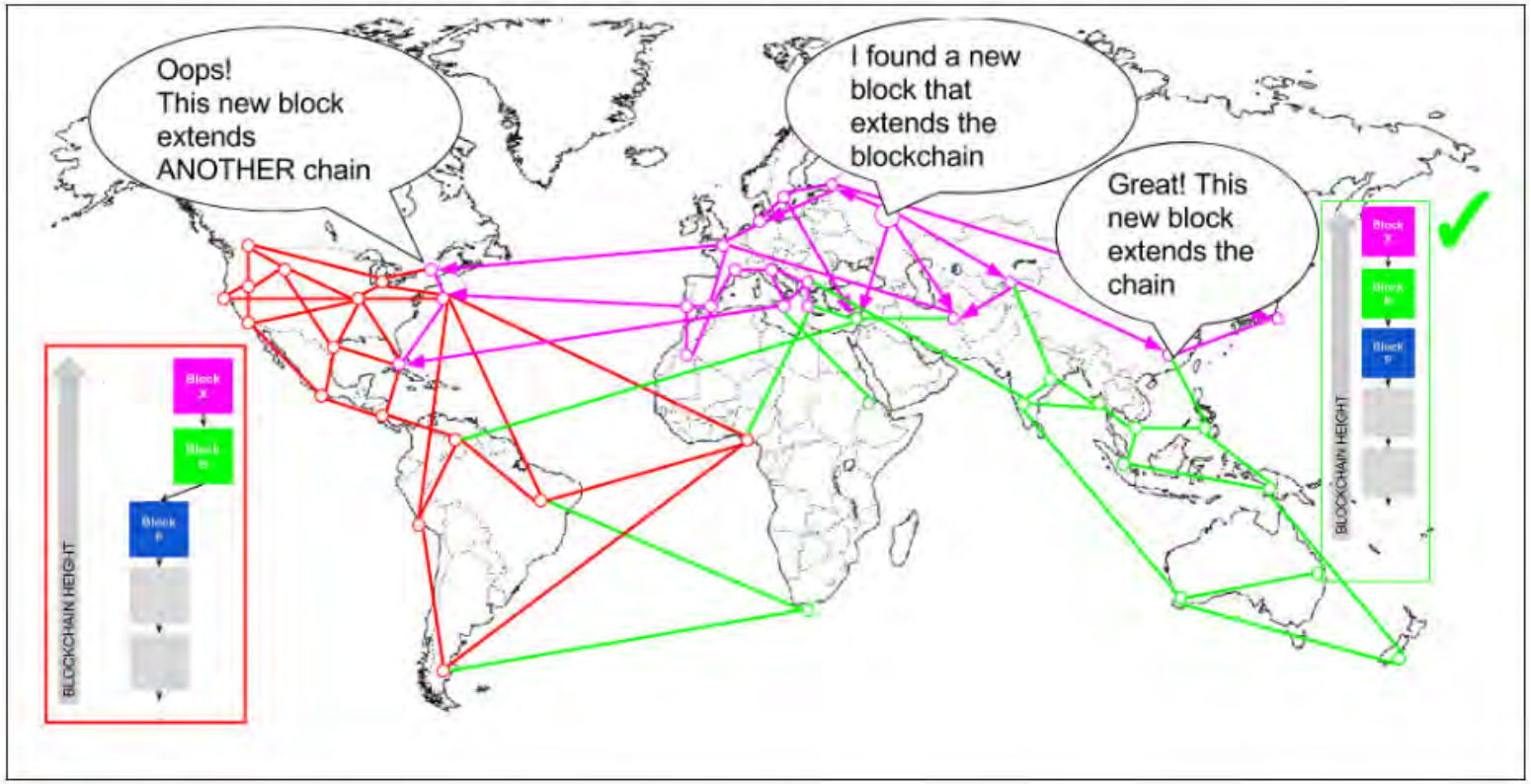
Visualization of a blockchain fork event - A new block extends one fork

Cela fourche (fork) !



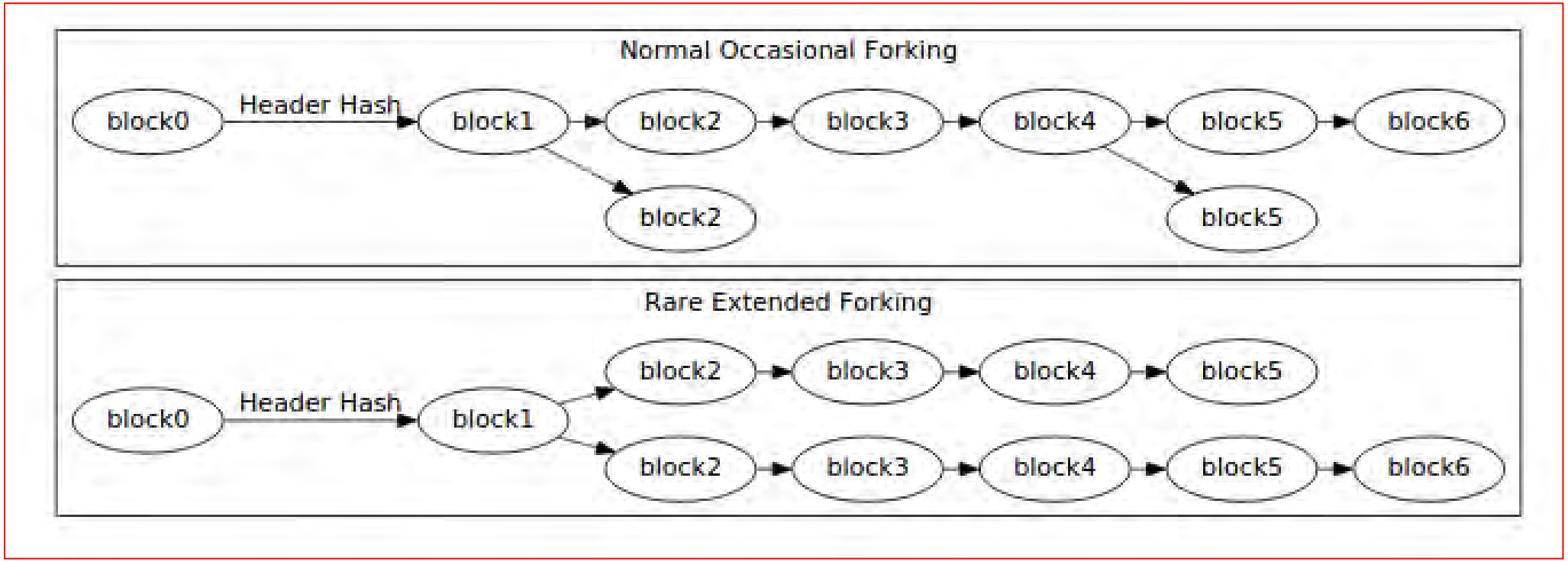
Visualization of a blockchain fork event - The network re-converges on a new longest chain

Le réseau ne conserve que la chaîne la plus longue



Visualization of a blockchain fork event - The network re-converges on a new longest chain

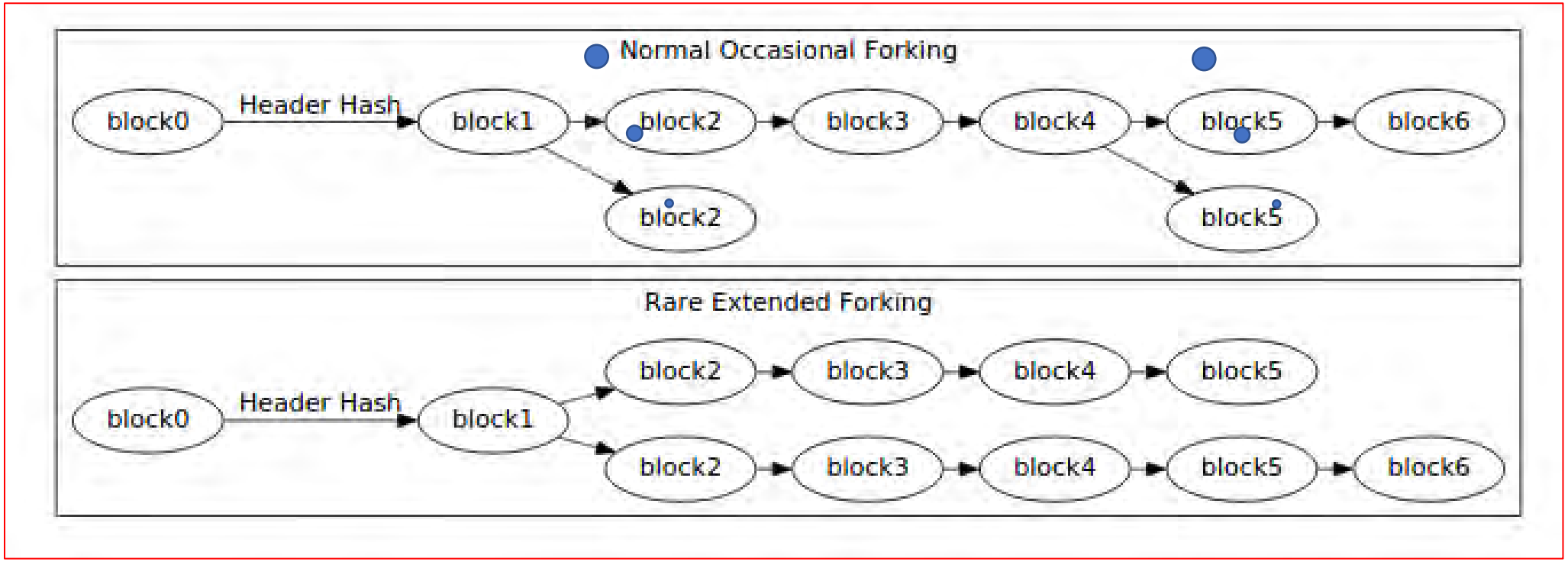
Plus généralement :



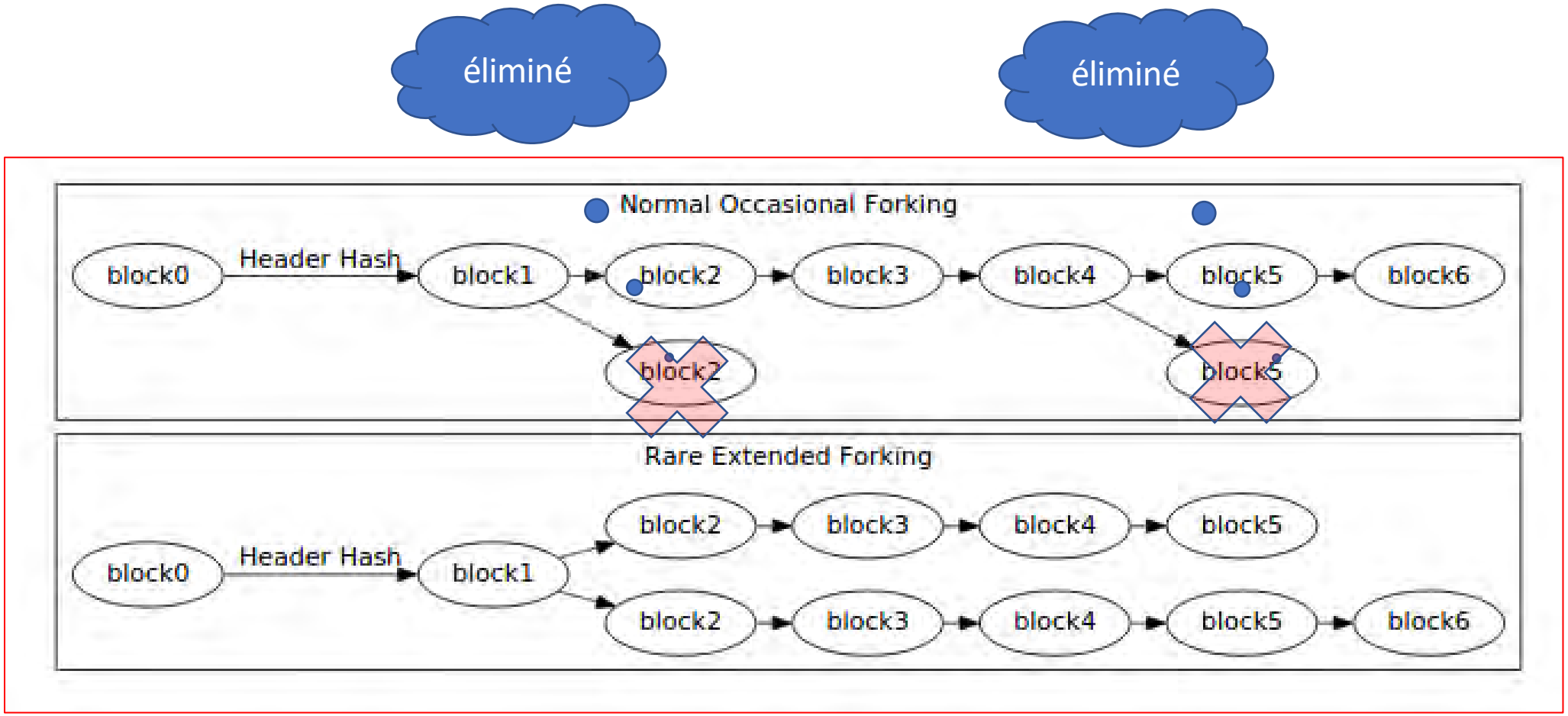
Cas d’un bloc hors chaîne

éliminé

éliminé

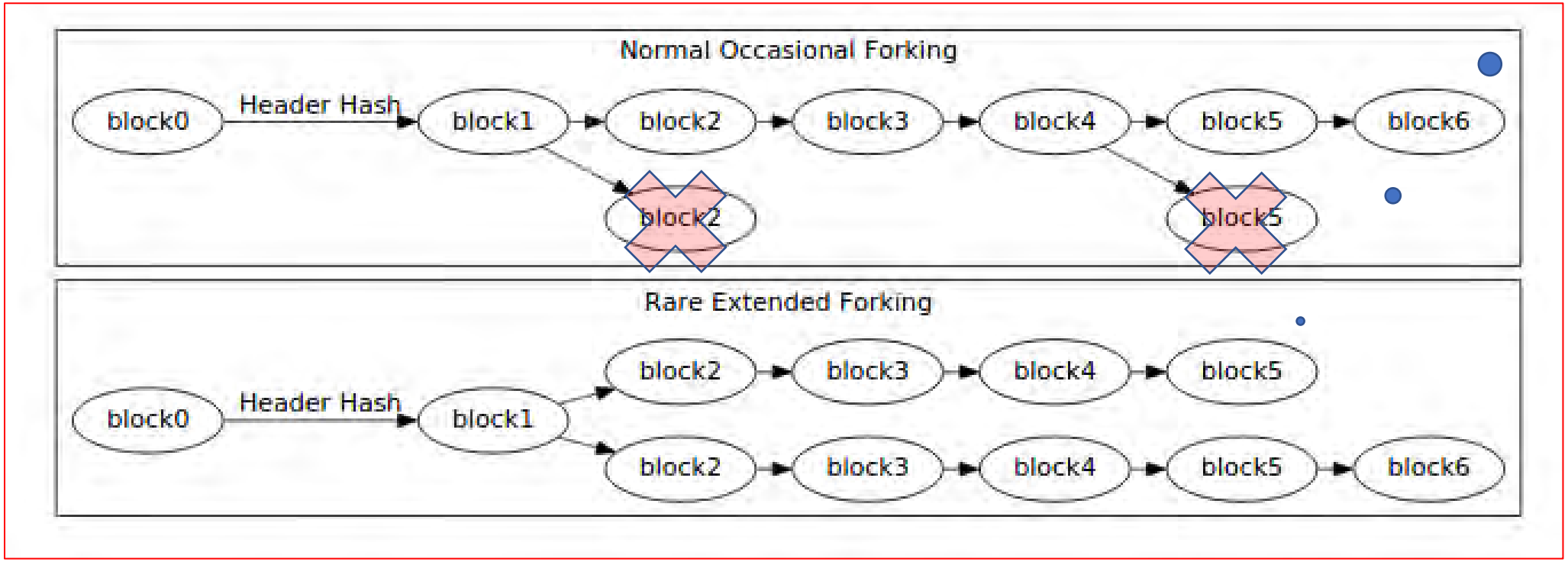


Cas d’un bloc hors chaîne



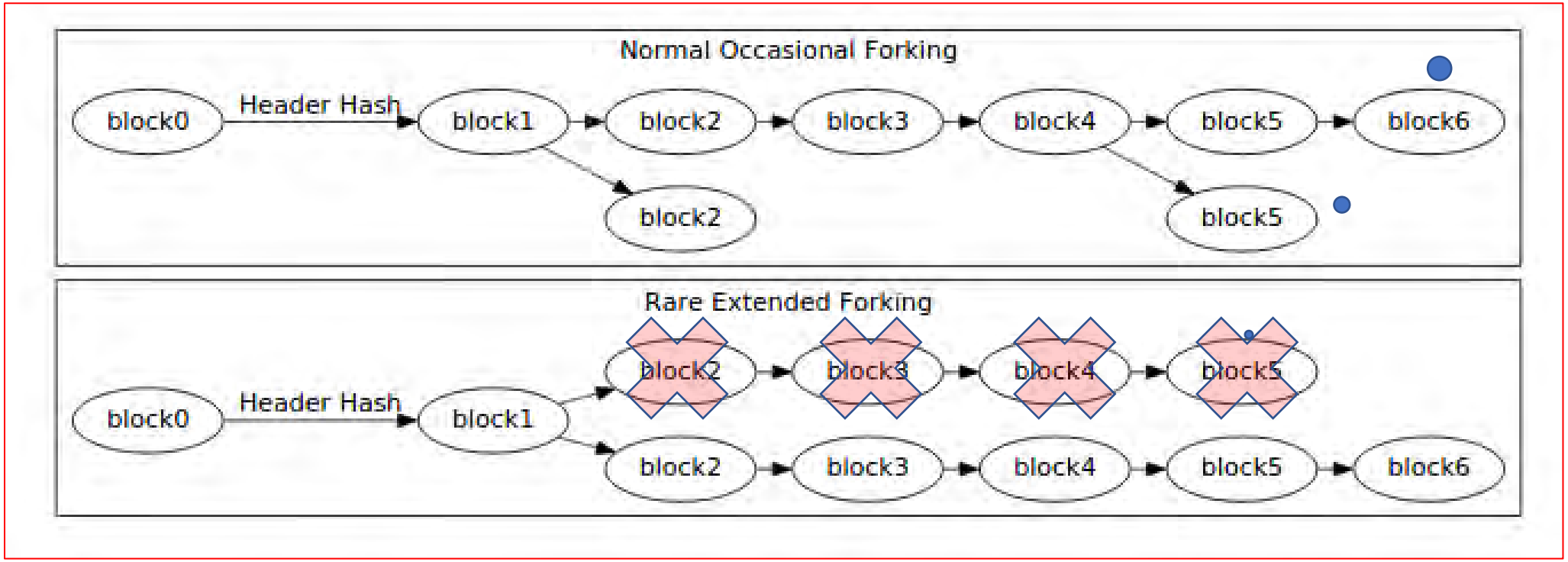
Cas de deux extensions de chaîne :

Chaîne éliminée



finalement : retour à la normale

Chaîne éliminée



How to generate this nonce?

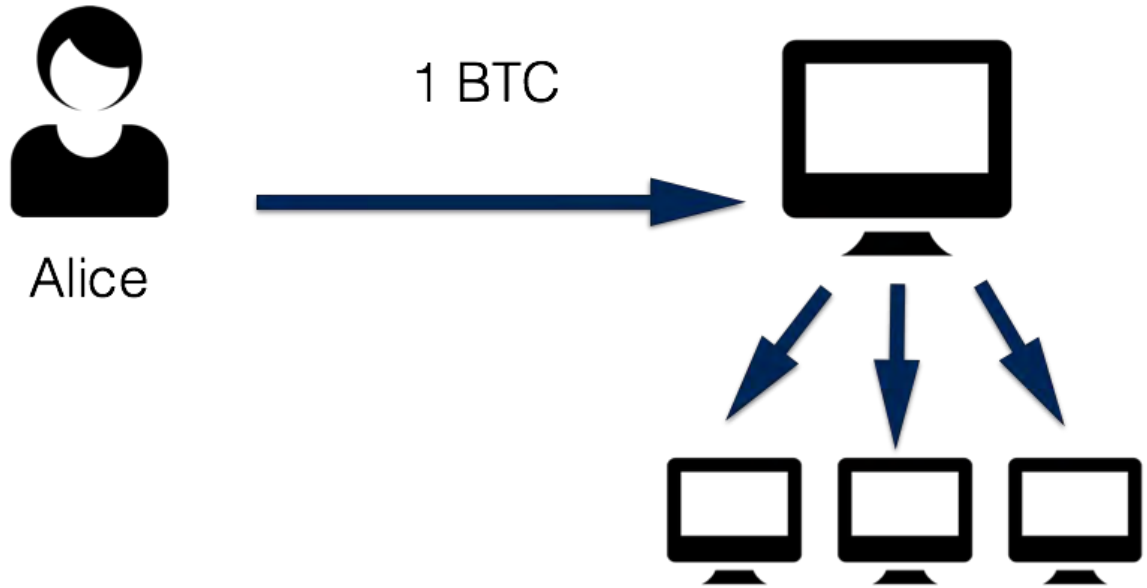
- Cryptographic protocols exist!

- To be implemented …

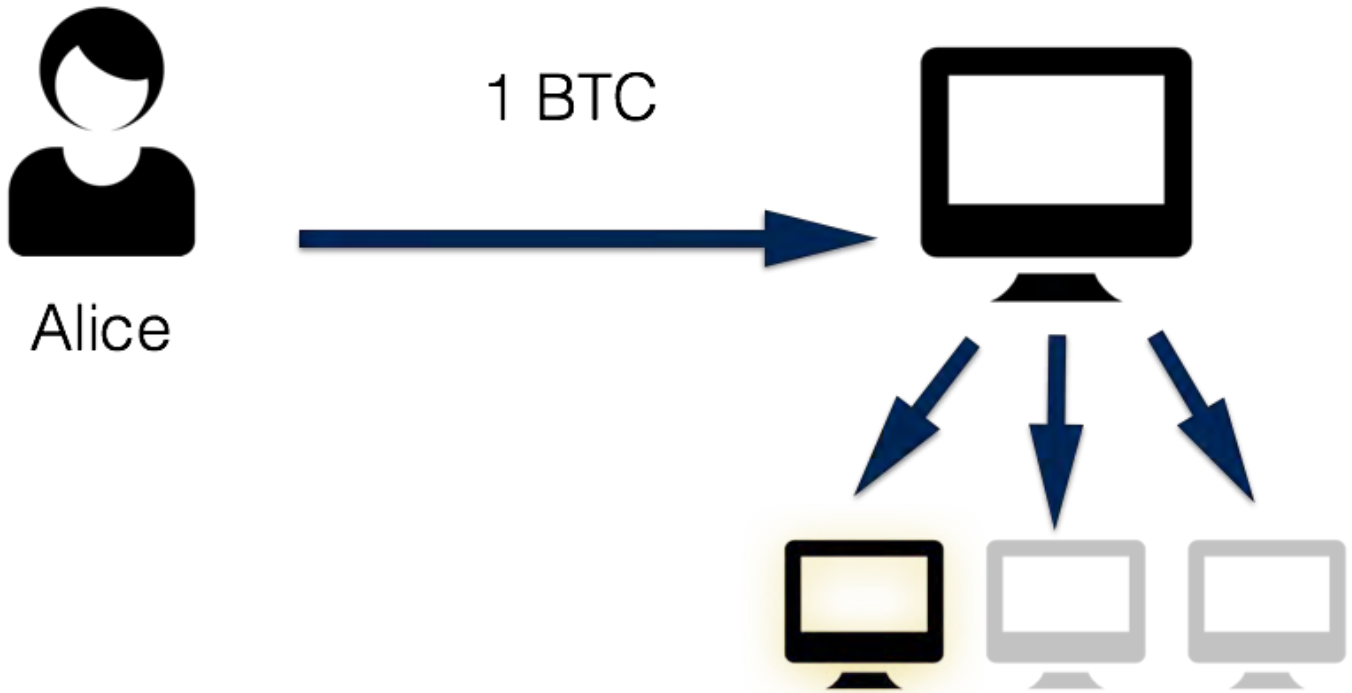
Exemple d’un transfert (paiement en bitcoin)

- Alice veut envoyer un bitcoin à Bob,
- Comment cela se passe ? Voir les 4 slides suivantes.
- Comment faire en pratique ? Voir encore un peu plus loin.

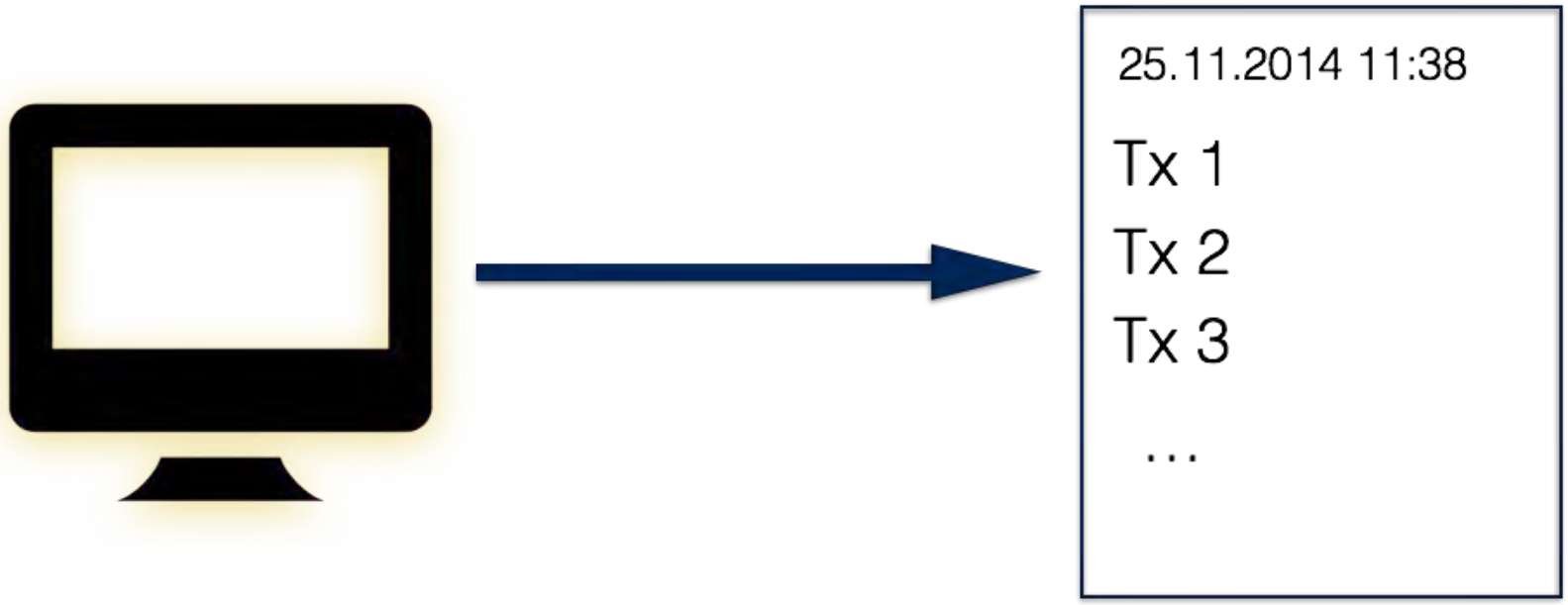
La transaction est envoyée à tout le réseau pour validation



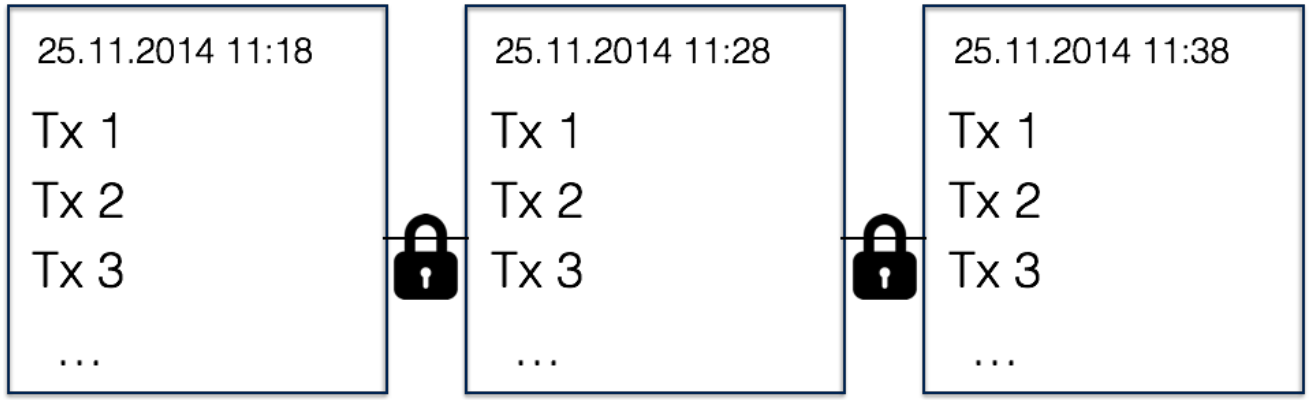
Un participant est tiré au sort pour mettre ensemble toutes les transactions en cours (créer un bloc)



Le “gagnant” reçoit la récompense

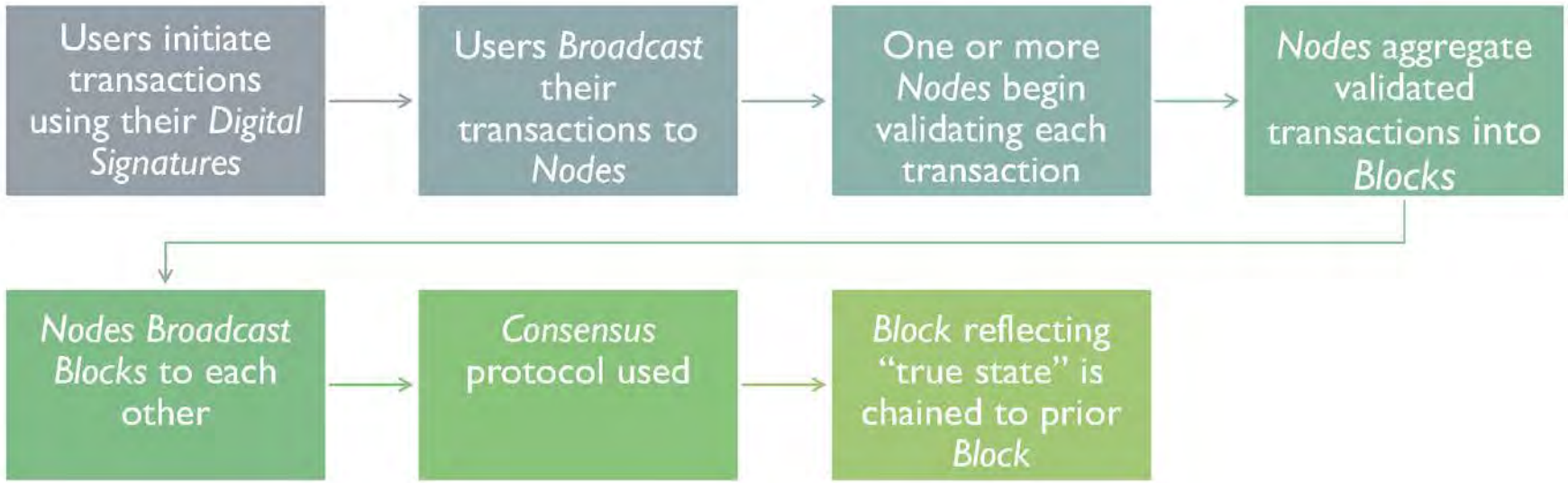


Le bloc créé est sécurisé de manière cryptographique et ajouté à la suite des blocs existants



Une fois dans un bloc, la transaction est “confirmée” et Bob a reçu son Bitcoin
Blockchain= « public ledger » registre publique

HOW MIGHT A DISTRIBUTED LEDGER WORK?



WHERE MIGHT A DISTRIBUTED LEDGER USE CRYPTOGRAPHY?

Initiation and Broadcasting of Transaction	• *Digital Signatures* • *Private/Public Keys*
Validation of Transaction	• *Proof of Work and certain alternatives*
Chaining Blocks	• *Hash Function*

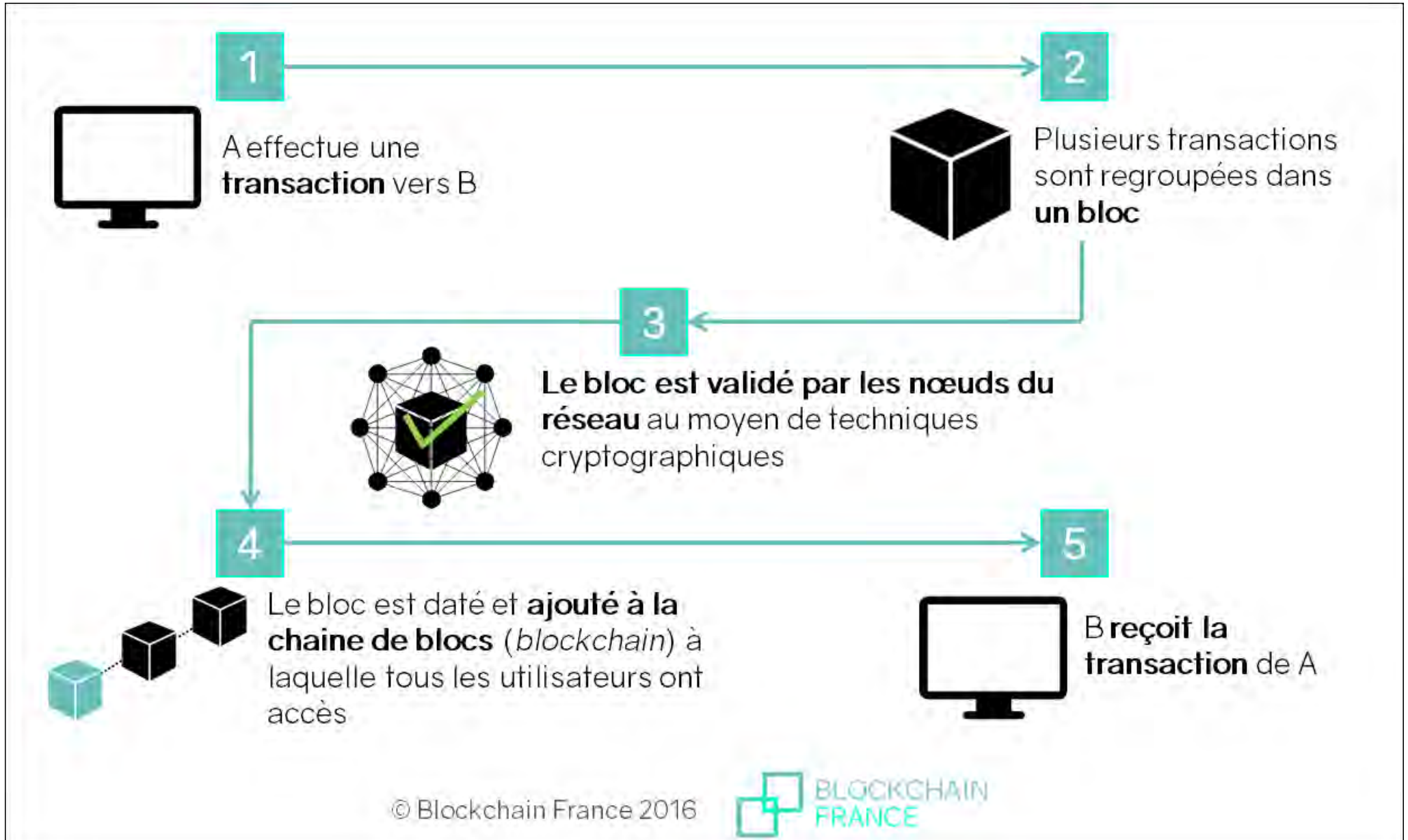
Nice properties of a blockchain

- Decentralisation,
- Consensus,
- Validity,
- Unicity,
- Authenticity,
- Immuable past,
- Sure (security),
- Trust,
- Non-repudiation.

COMMENT ?

- - blockchain, un maillon sans faille, de confiance, inaltérable : droit à l'oubli ou à l'erreur ? anonymat, traçabilité, ...
- - usage incontournable de la cryptographie (nécessité d'être à jour et de respecter les normes),
- - types de blockchains : publique, semi-publique, privée,
- - au sujet du consensus : variantes, un sujet de recherches depuis 50 ans,
- - au sujet du minage : est-il nécessaire ?
- - smart contracts et ethereum, le langage solidity, puissance et danger !
- (autres langages : Serpent, Mutan, LLL, Viper, Bamboo), tests de contrats (zeppelin, wafr)
- - les cryptomonnaies, les cryptomonnaies d'Etat : volabilité versus stabilité, circulation ou placement ?,
- - les ICO (initial coin offering) :
- - retour rapide sur la cryptographie : les normes, les ordinateurs quantiques, etc (les enjeux de la sécurité pratique),
- - attention aux fausses nouveautés, aux compétences autoproclamées,
- - les services rendus par de nouvelles sociétés pour démarrer de tels projets,
- - projets de normes autour des blockchains.

blockchain


1
A effectue une **transaction** vers B
2
Plusieurs transactions sont regroupées dans **un bloc**
3
Le bloc est validé par les nœuds du réseau au moyen de techniques cryptographiques
4
Le bloc est daté et **ajouté à la chaine de blocs** (*blockchain*) à laquelle tous les utilisateurs ont accès
5
B **reçoit la transaction** de A
© Blockchain France 2016
BLOCKCHAIN FRANCE

How a ₿itcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

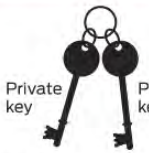
An address is a string of letters and numbers, such as 1HULMwZEPkjEPeCh43BeKJL1ybLCWrfDpN.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

Each address has its own balance of bitcoins.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.



Public Key Cryptography 101
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

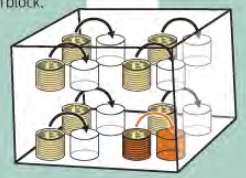
Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

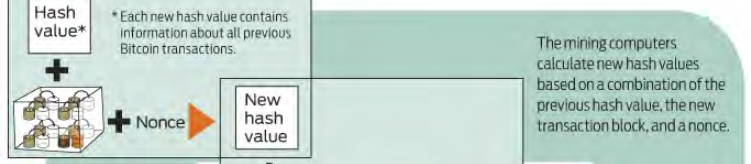
VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."



The miners' computers are set up to calculate cryptographic hash functions.



The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

Cryptographic Hashes
Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil	6d0a 1899 086a... (56 more characters)
The root of all evil	486c 6be4 6dde...
The root of all veil	b8db 7ee9 8392...

Nonces
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

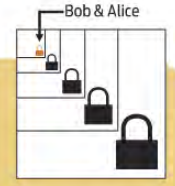
The root of all evil ???	0000 0000 0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

TRANSACTION VERIFIED



As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

JOSHUA J. ROMERO, BRANDON PALACIO & KARLSSONWILKER INC.

minage

- An exahash solves 10^18 hashes (problem-solving with algorithms) per second

- On en est à environ 185 exahash par seconde !

Statistiques de la monnaie

Summary of bitcoin statistics for the previous 24 hour period.

BLOCK SUMMARY

Blocs minés	154
Temps écoulé entre chaque bloc	8.79 minutes
Bitcoins minés	962.50000000 BTC

RÉCAPITULATIF DU MARCHÉ

Prix du marché	$57,009.96	Voir le graphique
Volume de transactions	$433,340,531.23	
Volume de transactions	7,583.09000000 BTC	

TRANSACTION SUMMARY

Somme des frais des transactions (BTC)	71.83198298 BTC	Voir le graphique
Nombre de transactions	267,260	Voir le graphique
Volume total des outputs (BTC)	1,202,123.93920467 BTC	Voir le graphique

Volume estimé des transactions (BTC)	80,644.46566418 BTC	Voir le graphique
Volume estimé des transactions (USD)	$4,608,479,602.84	Voir le graphique

COÛT DU MINAGE

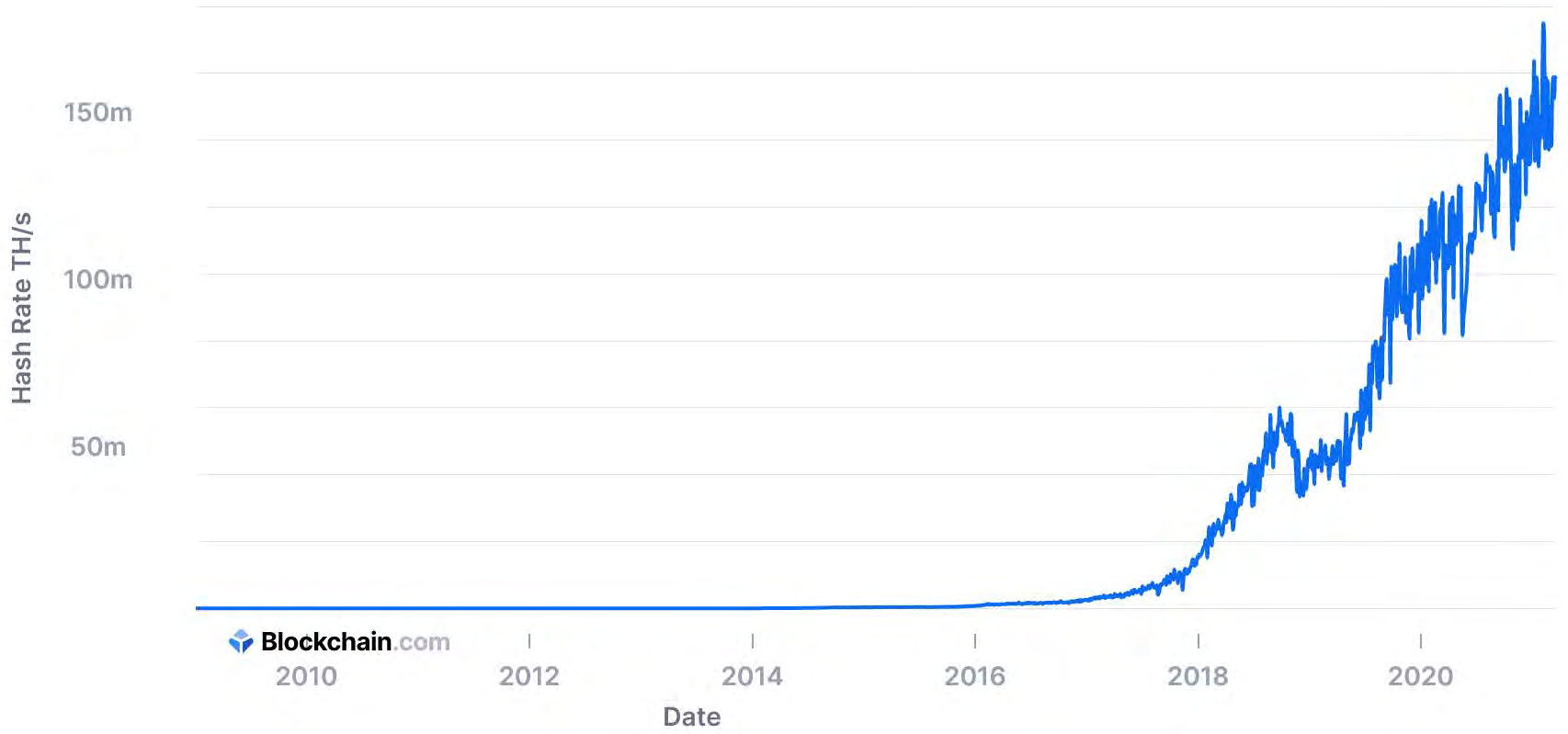
Revenu total des mineurs (USD)	$59,107,563.14	Voir le graphique
% De Gains Grâce Aux Frais De Transaction	6.93%	
% Du Volume Des Transactions	1.28%	Voir le graphique
Coût par transaction (USD)	$220.64	Voir le graphique

TAUX DE HASH ET CONSOMMATION D'ÉLECTRICITÉ

Difficulté	21,865,558,044,610	Voir le graphique
Taux de hash	167,389,189,044 GH/s	Voir le graphique

Total Hash Rate (TH/s)

The estimated number of terahashes per second the bitcoin network is performing in the last 24 hours.

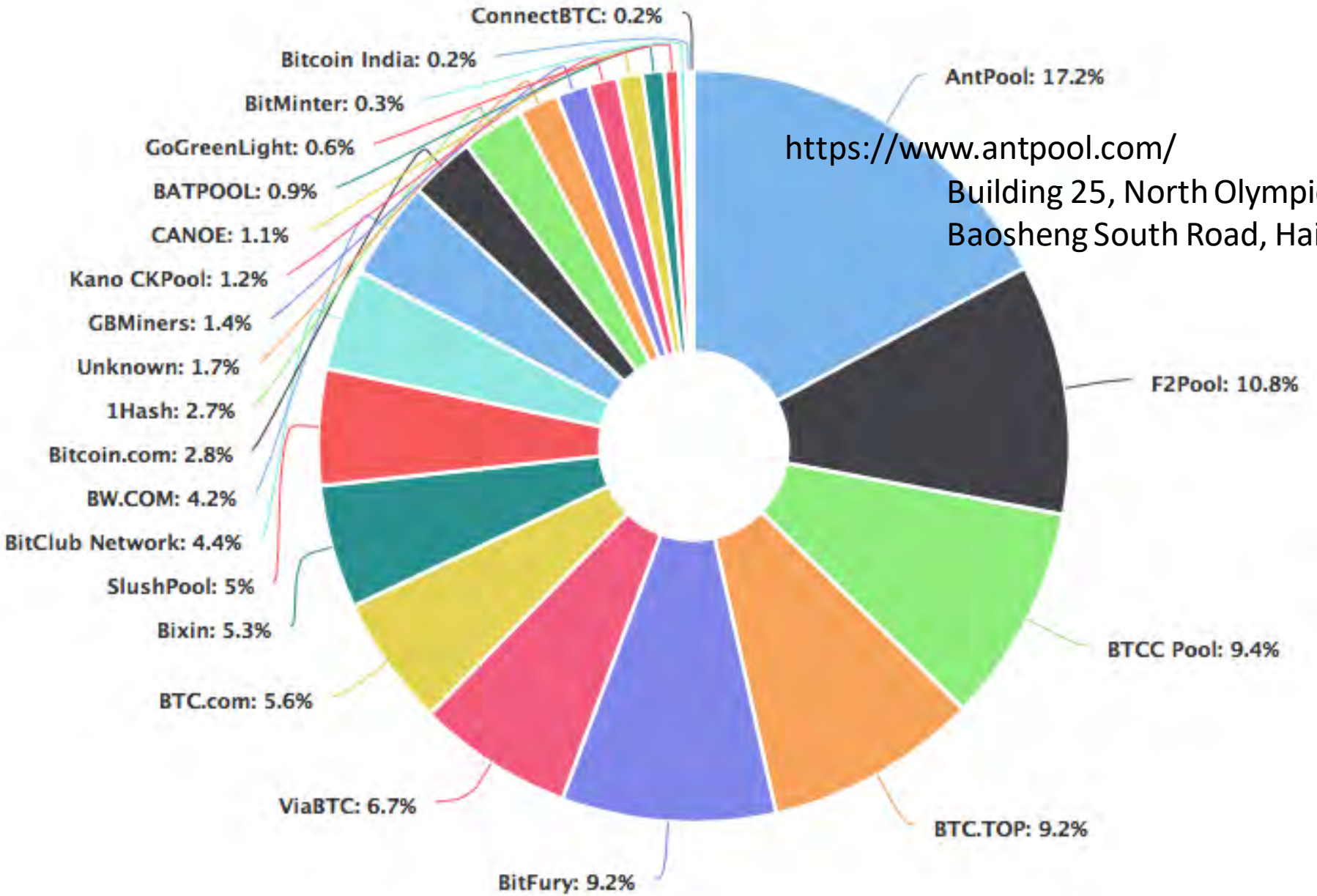


30 Days | 60 Days | 180 Days | 1 Year | 3 Years | All Time

Raw Values | 7 Day Average | 30 Day Average

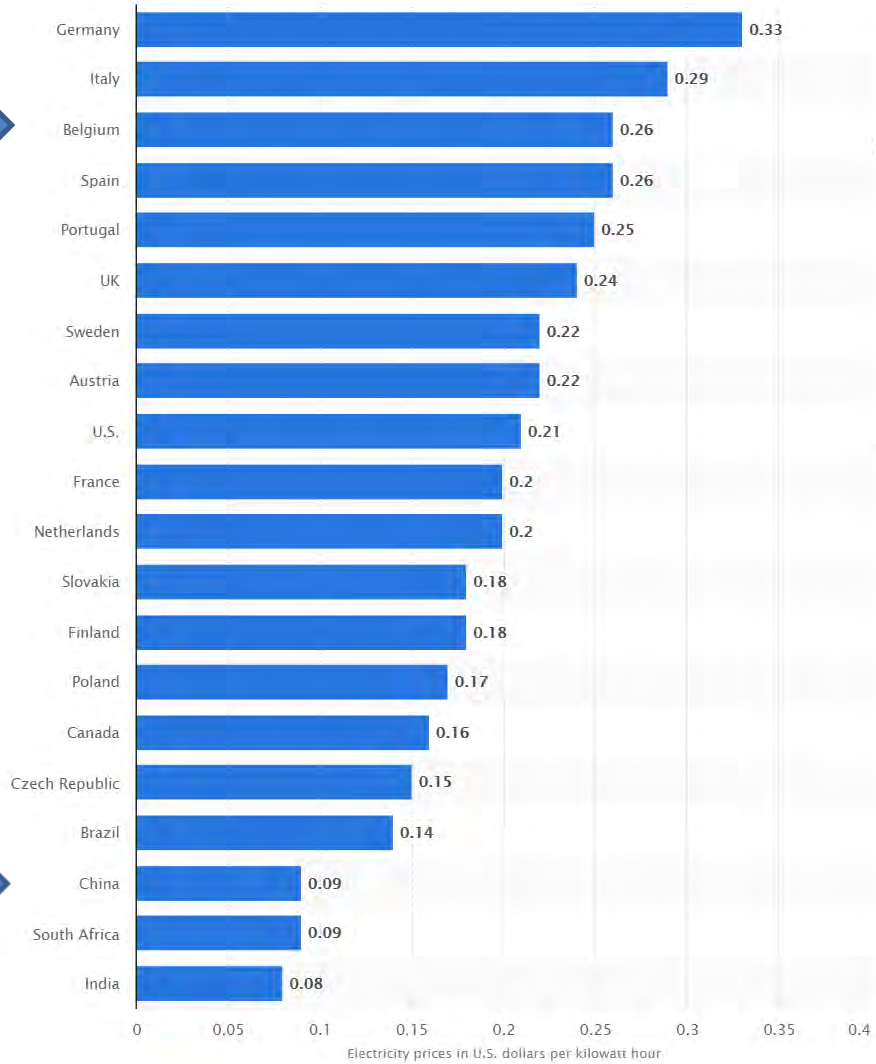
Linear Scale | Logarithmic Scale

Export Data



https://www.antpool.com/
Building 25, North Olympic Science & Technology Park,
Baosheng South Road, Haidian District, Beijing, China 100029

Global electricity prices by select countries in 2017 (in U.S. dollars per kilowatt hour)



DESCRIPTION SOURCE MORE INFORMATION

This statistic shows electricity prices in selected countries worldwide in 2017. In the United States, electricity prices stood at 0.21 U.S. dollars per kilowatt hour. In the United Kingdom, electricity users paid 0.24 U.S. dollars per kilowatt hour.

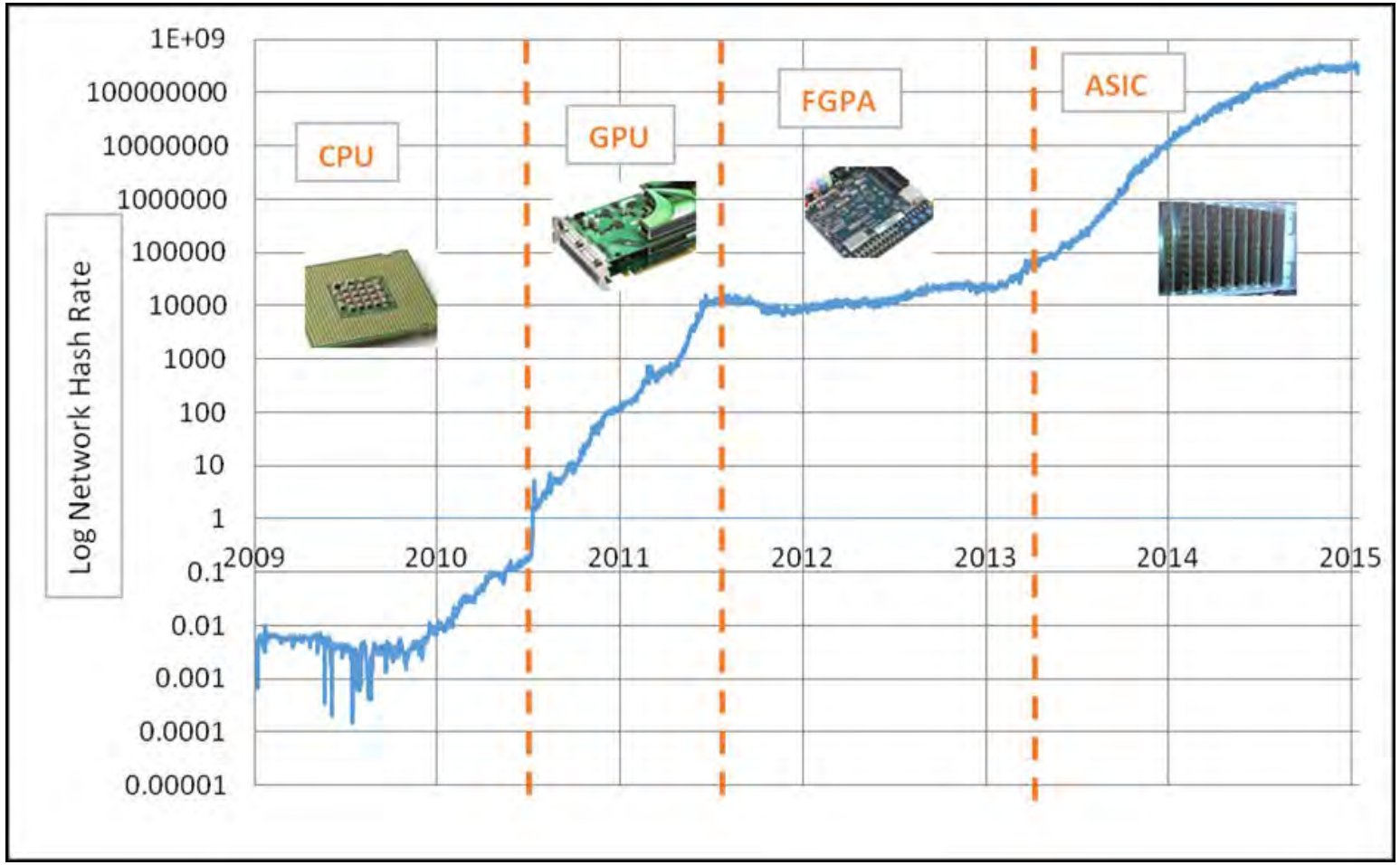
Electricity prices in selected countries in 2015

Electricity prices by country can vary widely and even within a country itself, depending on factors like infrastructure and geography. Among developed countries, Sweden enjoys some of the cheapest electricity prices in the world. For global electricity prices, Italy topped the list of countries with the highest electricity prices worldwide in 2015. Italian customers were charged around 15.7 U.S. dollar cents per kilowatt hour plus value added tax.

The selection of fuels used to generate electricity remains a main driver behind Italy's high electricity prices. There are no nuclear power plants in the country. Due to the fact that Italy is located in a seismically active area, all nuclear power plants were closed following a popular referendum in the late 1980s, when an explosion in Chernobyl reminded Europeans of the dangers of nuclear power. As a result, the country's electricity generation mix consists mainly of natural gas, renewable energy, petroleum products and coal. Although Italy has one of the largest proved natural gas reserves in Europe, the

Minage : https://www.crypto-news.net/bitcoin-mining-hardware-2017/

Mining hardware-software



perspectives

- Be careful with smart contracts (language solidity too powerful!)
  - Models for contracts (limited)
  - Analyzers: not mature …
  - Trust about a contract (notary again? Human people!)?
- Proof of work (aso): also proof of speed (ammbr.com)
- Avoid strong or fast standardization
  - Everybody is doing it: ENISA, IETF, NIST, …
- Evolution of security: we don’t know all the attacks
- Evolution of cryptography:
  - Strong enough primitives?
  - Quantum computers
  - NSA and NIST
- Research continues: Cryptology ePrint Archive: Report 2017/775 Proofs of Work for Blockchain Protocols

  Juan A. Garay and Aggelos Kiayias and Giorgos Panagiotakos
- Well-known solutions for blockchains exist, see …
- Snake oil

Blockchain Consensus Protocols
Snake Oil Warning

Christian Cachin
IBM Research - Zurich

Models?

Proofs?

Analysis?

Public peer review?

Hyperledger

- A Linux Foundation project – www.hyperledger.org
  - Open-source collaboration, developing blockchain technologies for business
  - Started in 2016, 135 members in Apr. '17

- Blockchain technologies for business
- Today 4 frameworks and 4 tools, hundreds of contributors

- Hyperledger Fabric was initially contributed by IBM – github.com/hyperledger/fabric/
  - Architecture and consensus protocols originally contributed by IBM Research - Zurich

Workshop on Blockchain Technology and Theory

16 October 2017, Vienna

In connection with DISC 2017

www.blockchain-workshop.net

standards

- ISO-NBN: TC307: https://www.iso.org/committee/6266604.html
- IEEE: https://blockchain.ieee.org/
- IETF: https://trac.ietf.org/trac/irtf/wiki/blockchain-federation (DINRG)
- ENISA: https://www.enisa.europa.eu/news/enisa-news/enisa-report-on-blockchain-technology-and-security
- W3C: https://www.w3.org/community/blockchain/
- NIST: https://github.com/usnistgov/Blockchain
- BSI-RAND: https://www.rand.org/pubs/research_reports/RR2223.html
- NB: https://www.internationalairportreview.com/news/33288/7-principles-blockchain-wave/

ISO/TC 307

Blockchain and distributed ledger technologies

About

Secretariat: SA

Secretary: Ms Rachel Frank

Chairperson (until end 2019): Mr Craig Dunn

ISO Technical Programme Manager : Mr Henry Cuschieri

ISO Editorial Programme Manager : Mme Mercè Ferrés Hernández

Creation date: 2016

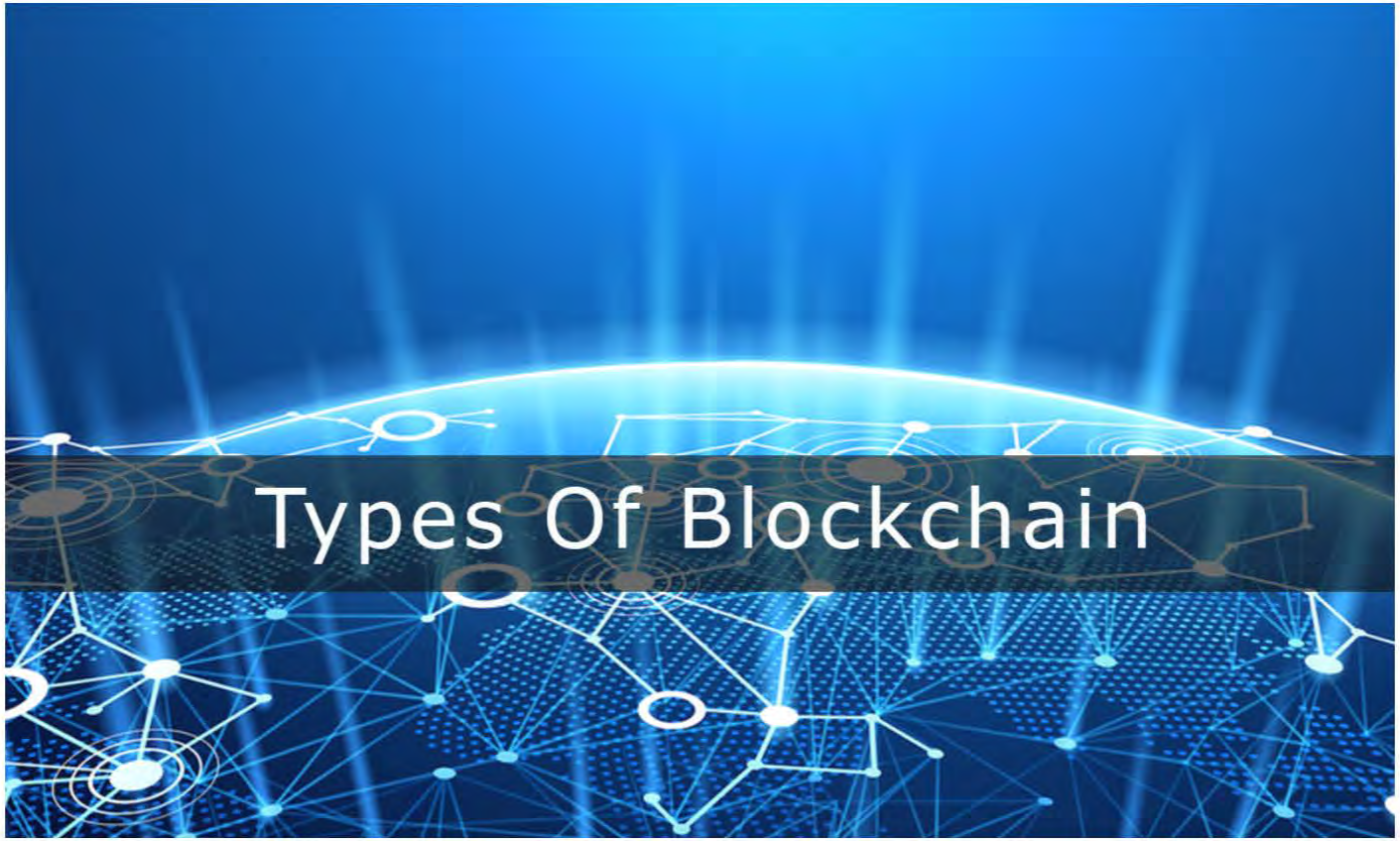
Quick links

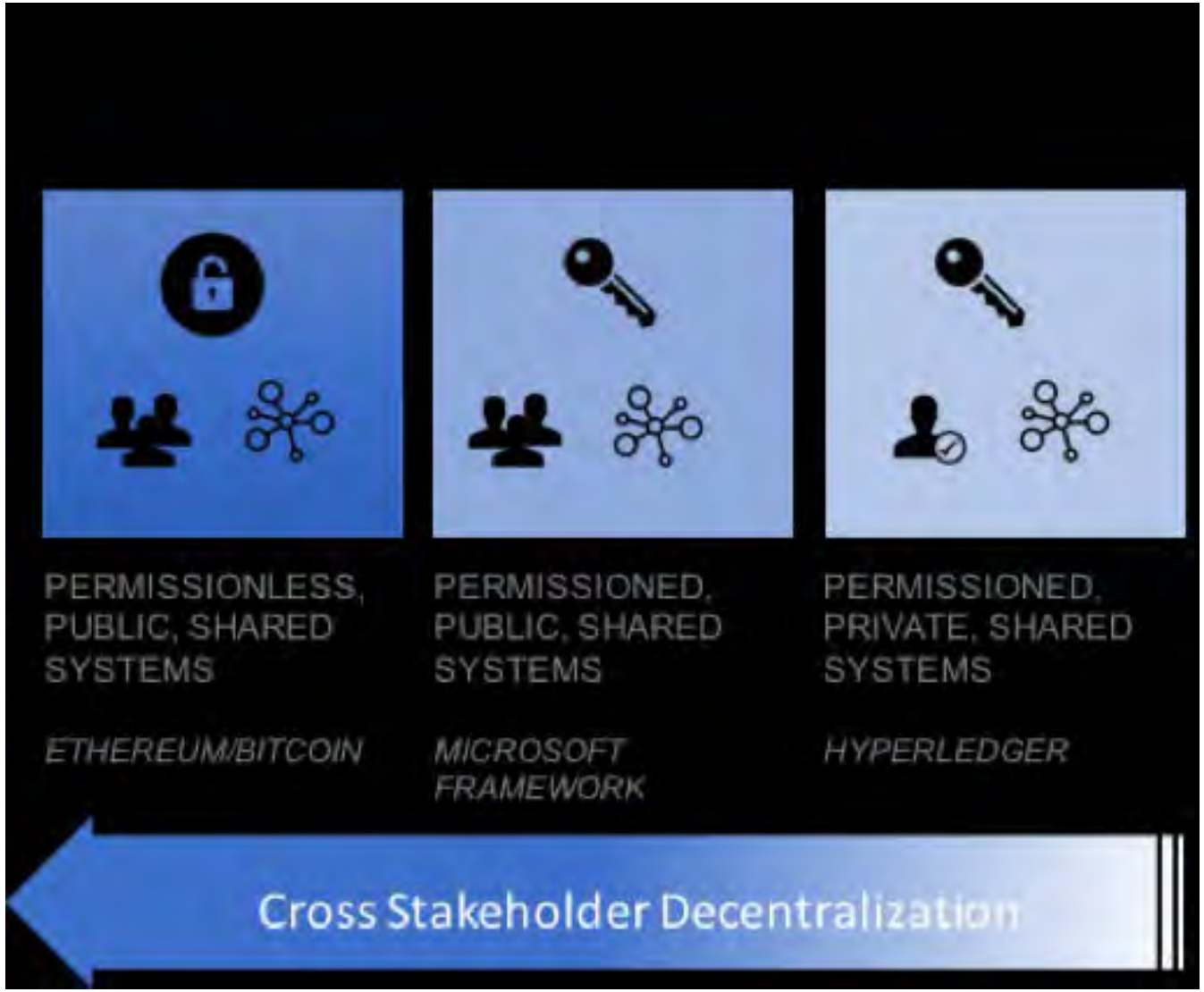
Work programme
Drafts and new work items

Business plans
TC Business plans for public review

Working area
on ISOTC and Public information folder

Types of Blockchain—Public, Private and Permissioned




PERMISSIONLESS, PUBLIC, SHARED SYSTEMS
ETHEREUM/BITCOIN
PERMISSIONED, PUBLIC, SHARED SYSTEMS
MICROSOFT FRAMEWORK
PERMISSIONED, PRIVATE, SHARED SYSTEMS
HYPERLEDGER
Cross Stakeholder Decentralization

Alt Coins

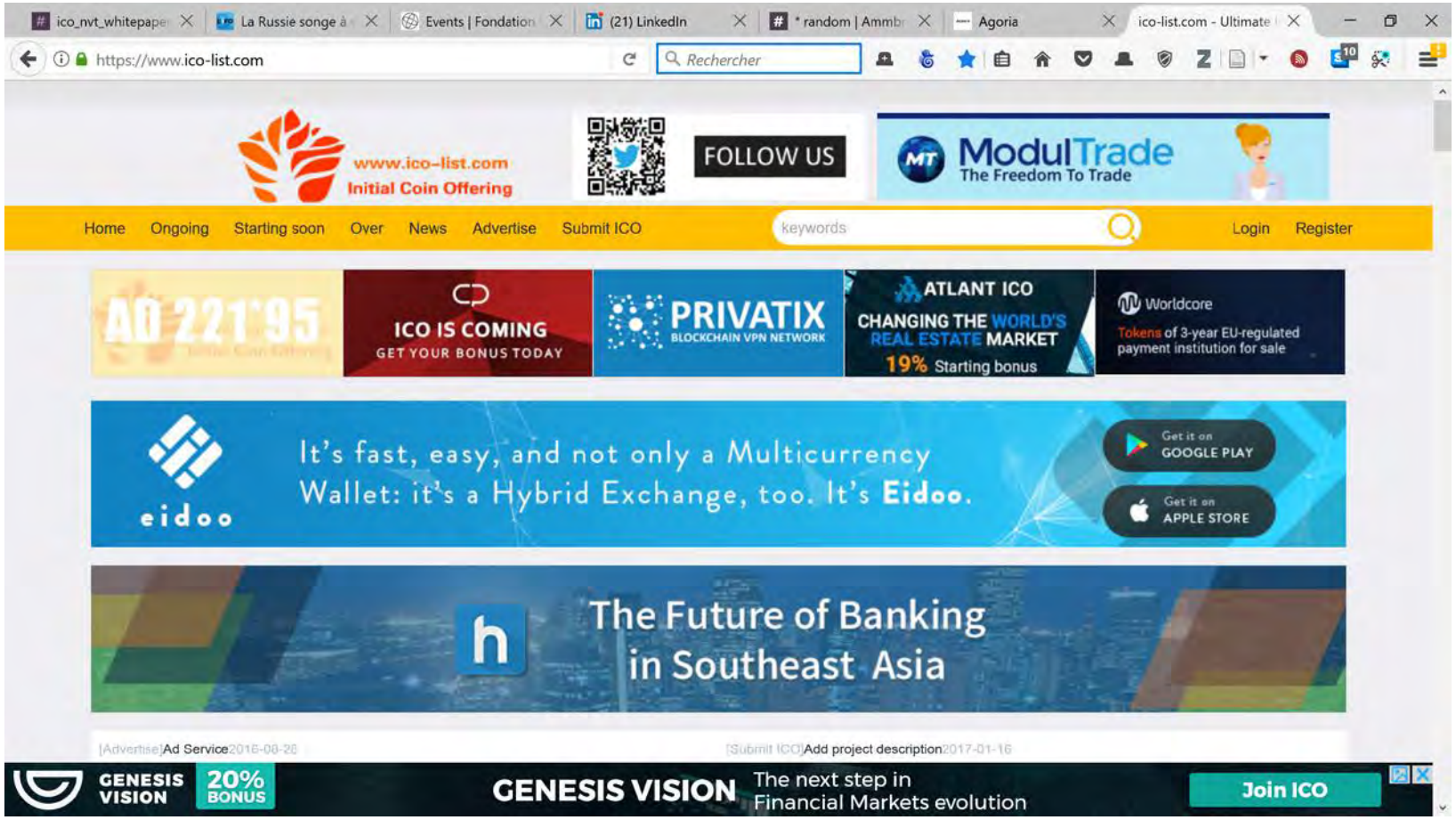
REX Ends ICO Amidst $1.6 Million Lost Due to Coding Error

August 28, 2017 108

Sharding :

- https://github.com/ethereum/wiki/wiki/Sharding-FAQ

Cryptocurrencies and ICO (initial coin offering)



OPPORTUNITES

- - usages des blockchains : rapide tour d'horizon mondial, pour mieux comprendre pourquoi, quand, comment, qui sont les acteurs,

- - RGPD (nouveau règlement européen sur la protection des données) et blockchains,

Blockchain Use Cases: Comprehensive Analysis & Startups Involved

Growing number of blockchain initiatives around the word

CANADA - Toronto Stock Exchange hires bitcoin guru as Chief Digital Officer to study blockchain potential.

CANADA - The federal government is considering the use of blockchain technology when advantageous to deliver government services and to enhance the security of private information.

USA - The Federal Reserve discusses the creation of a blockchain based digital currency with IBM and expresses optimism over the technology.

USA - Linux Foundation leads 28 leading technology and financial firms to create open source Hyperledger blockchain standard.

MEXICO - Bank of Mexico is considering blockchain to create a digital version of peso.

HONDURAS - Government is working with Factom to develop a blockchain land title record system.

UKRAINE - Government plans to trial Ethereum blockchain-based election platform.

EU - European Central Bank intends to assess blockchain for banking services like payments, securities settlement as well as collateral.

UK - PWC partners Blockstream and Eris Industries to create a solution portfolio for FIs.

UK - UK government exploring use of blockchain recordkeeping.

FRANCE - Allianz explores real world use case of blockchain in its Fintech Accelerator Programme.

NIGERIA - Government proposes to regulate bitcoin and monitor exchanges and gateways to fight money laundering.

KENYA - Government appoints bitcoin remittance startup BitPesa board member as Kenyan Ministry of Information, Communications and Technology.

RUSSIA - Central Bank establishes Blockchain Working Group to "analyse and evaluate" potential applications of blockchain technology within finance.

JAPAN - Financial Services Agency considers amendments to legislation to include virtual currencies such as bitcoin as "fulfilling the functions of currency."

CHINA - Alibaba explores blockchain for cloud service and to fight counterfeit products.

CHINA - People's Bank of China weighs blockchain for digital currency.

JAPAN - Fujitsu and Mizuho completed a blockchain trial to streamline cross-border securities transaction settlements.

SOUTH KOREA - Korea Stock Exchange has begun preliminary steps to develop a blockchain trading platform for off-board dealers.

DUBAI - Government establishes Blockchain Council to promote the technology.

HONG KONG - Hong Kong Monetary Authority is funding research into how the ledger system underpinning the controversial cryptocurrency could make its financial services sector safer and cheaper.

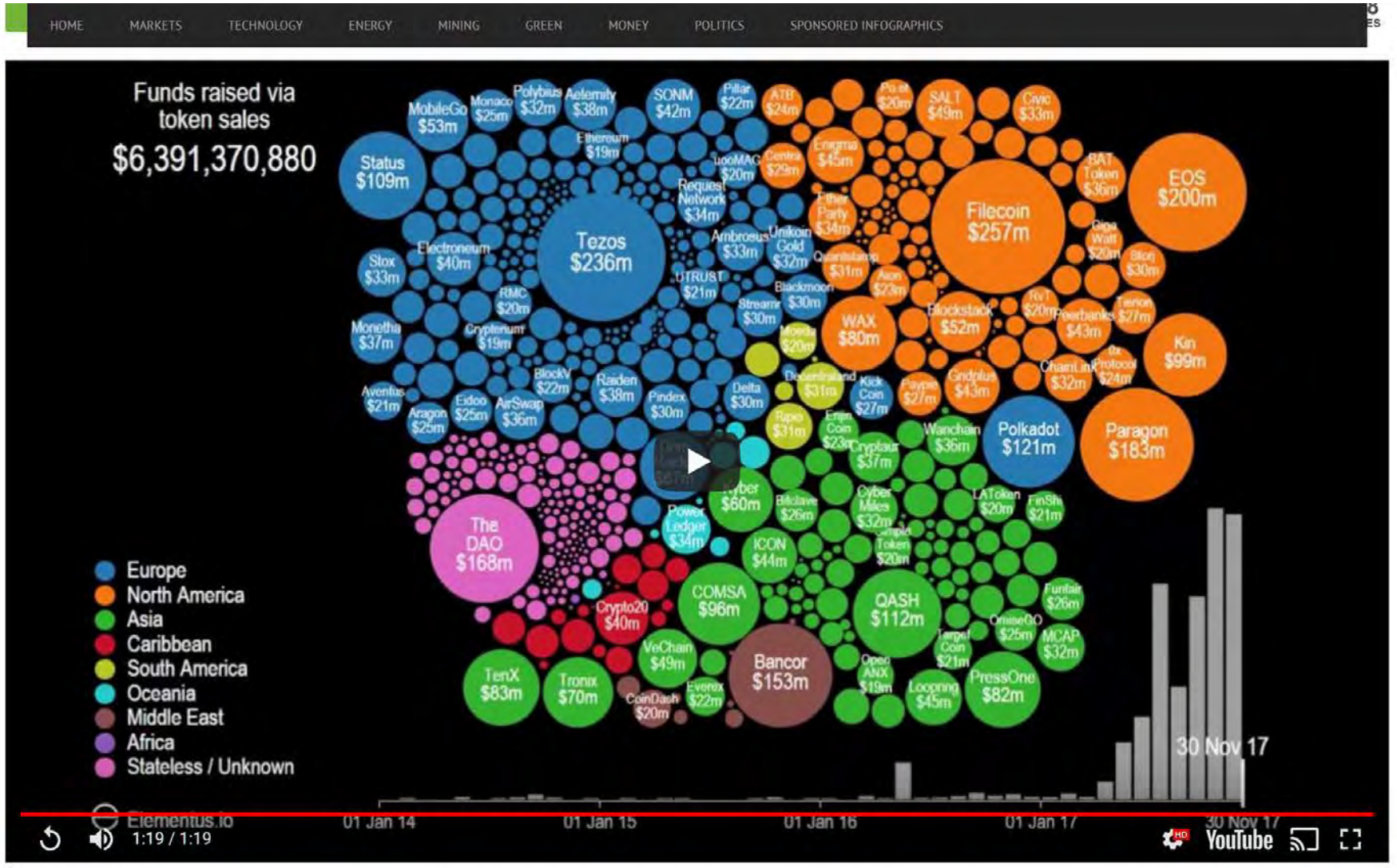
SINGAPORE - Monetary Authority of Singapore launches Smart Nation Initiative and commits over $167 million to support fintech and blockchain innovations.

SINGAPORE - DBS and SCB launch trade finance proof of concept using Ripple technology.

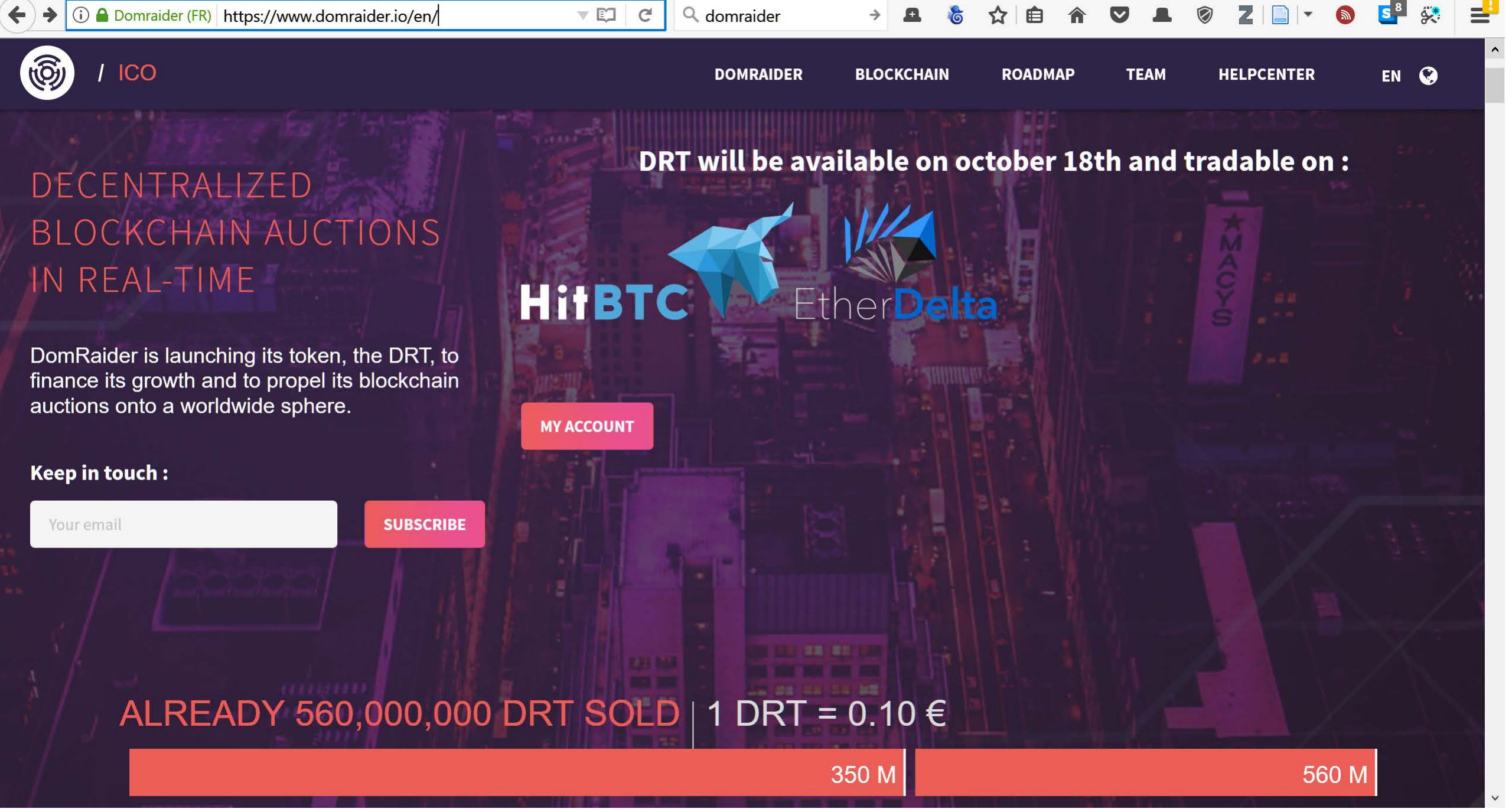
AUSTRALIA - Government seeks to end double taxation on bitcoin and is seeking new rules to govern the use of distributed ledgers in financial services.

AUSTRALIA - Australian Stock Exchange is actively working on a technology transformation programme that will employ blockchain technology to potentially replace its equities settlement systems.

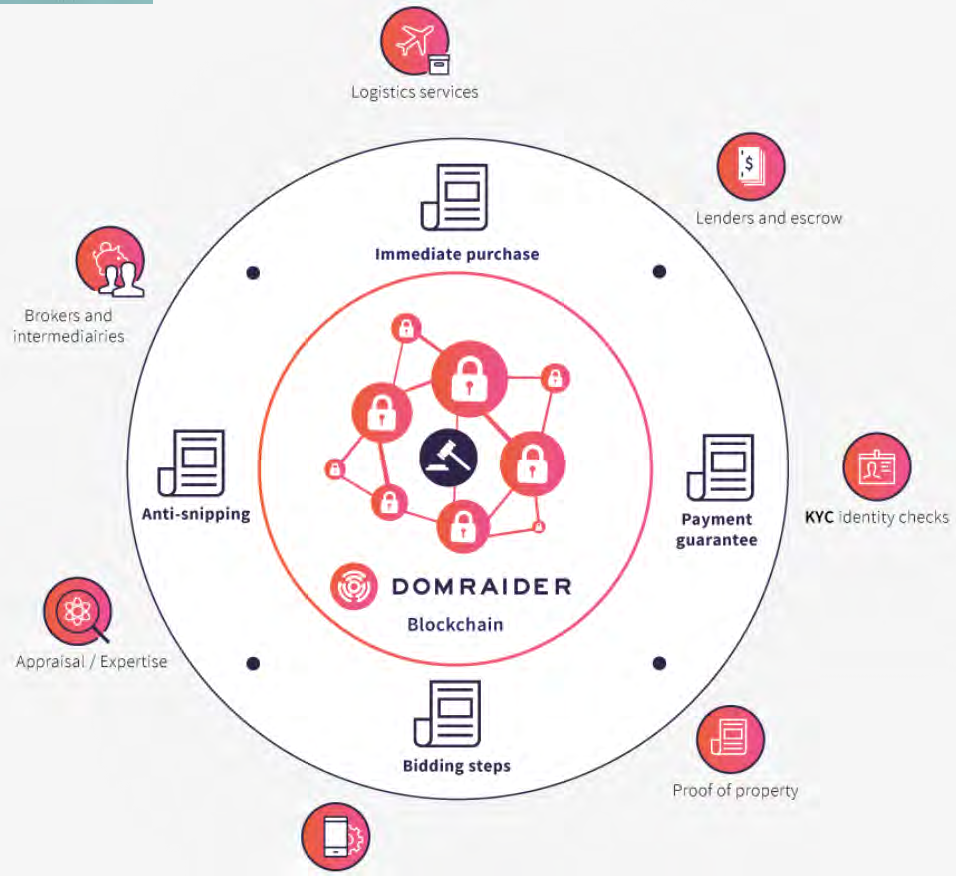
ICO explosion



Animation: Visualizing the ICO Explosion


Domraider (FR) https://www.domraider.io/en/
domraider
/ ICO
DOMRAIDER
BLOCKCHAIN
ROADMAP
TEAM
HELPCENTER
EN
DECENTRALIZED BLOCKCHAIN AUCTIONS IN REAL-TIME
DomRaider is launching its token, the DRT, to finance its growth and to propel its blockchain auctions onto a worldwide sphere.
Keep in touch :
Your email
SUBSCRIBE
DRT will be available on october 18th and tradable on :
HitBTC
EtherDelta
MACYS
MY ACCOUNT
ALREADY 560,000,000 DRT SOLD | 1 DRT = 0.10 €
350 M
560 M

THE CREATION OF A NEW ECOSYSTEM DEDICATED TO AUCTIONS



This is an open-source blockchain dedicated to the decentralization of auctions in real time. It will be transparent, reliable, adaptable and interoperable, without compromising on speed.

The DomRaider network is not only aimed to register auctions and bids. It is the core of a complete new auctioning ecosystem aimed to provide an innovative solution for all worldwide auctioning players.

Live auctioneers, escrow, appraisal experts, delivery services and online auctions providers will all be able to join the network, provide their services and add value to the blockchain.

The core of the network

Logging of bids and registration of transactions

Application of common rules

Advanced features

Addition of advanced rules specific to organizers in order to adapt to different types of sales

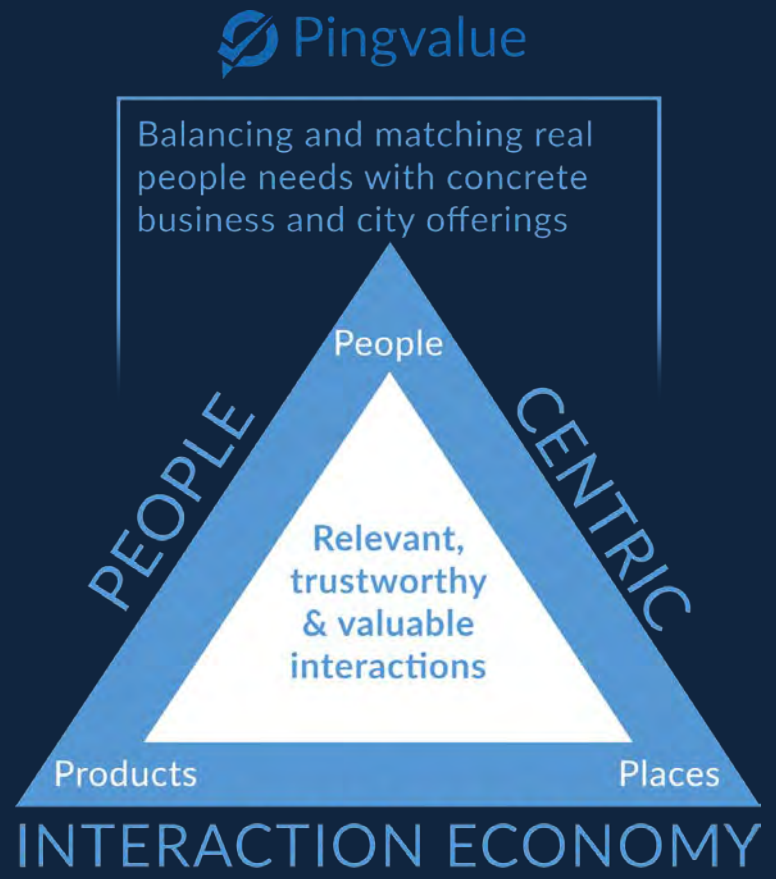
Additional services

Advanced service providers enhancing the functionning of the network

Pingvalue: Trustworthy Interactions/Transactions

There is a **unique opportunity** within the digital world to help individuals and businesses/institutions shape their experiences in the physical world.

At Pingvalue, we are putting the individual centre-stage where they can create **relevant interactions/transactions** with businesses and cities.



Pingcoin as Hybrid Token

Utility & Reward for Stakeholders in the Pingvalue Platform

- Truly bridge the digital and physical by earning currency on Pingvalue
- Platform interactions earning system linked to Social and Trust Factors
- Loyalty card earning model
- One-step goods and services payment with zero transactional costs
- Purchase a proportion of high value assets: Pingspots (Pingvalue hotspots), …
- Pingcoins can be exported to other platforms

Share WiFi with neighbours and the community. Earn tokens.

WiFi mining with a higher purpose

4.1 Billion people do not have an Internet connection, or it is of a poor quality. Ammbr is designed to extend the Internet, and its benefits, to these people using viral profit motives.

Token Sale

26 : 04 : 46 : 55

DAYS HOURS MIN SEC

November 14

Enter Your Email

Subscribe for updates

Read The Whitepaper

What is Ammbr?

Ammbr is a wireless mesh network built on blockchain.
Bandwidth is traded 24/7 in an autonomous market.

Cryptorouble, cryptoeuro, banks?

Derniers articles | Archives | Recherche

La Russie songe à créer un «cryptorouble»

par Emilien Ercolani, le 11 octobre 2017 14:24

La Banque centrale de la Fédération de Russie voit plutôt d'un bon œil la création d'une cybermonnaie nationale, capable de stimuler la croissance des paiements électroniques et non-cash.

« *Il devient de plus en plus pratique pour tout le monde de payer des biens et des services grâce à un portefeuille électronique, et une cybermonnaie pourrait jouer un rôle de catalyseur à un niveau plus global* ». C'est ce qu'a expliqué Olga Skorobogatova, gouverneure de la Banque centrale de la Fédération de Russie lors du forum Finopolis qui se déroule à Sotchi, en Russie.

Cette nouvelle déclaration va dans le sens qu'a indiqué cette semaine le ministre russe des Finances, Igor Shuvalov. Il évoquait lui aussi la création d'une cybermonnaie nationale. Le ministre et la banque centrale travailleraient d'ailleurs déjà conjointement sur ce sujet. Ils s'accordent pour dire que ce serait une bonne manière de stimuler et de renforcer l'économie Russe. « *Je pense qu'un cryptorouble devrait exister* », a d'ailleurs affirmé Igor Shuvalov, ce qui ne laisse guère de place à l'interprétation.

see La Tribune (17 October 2017):

LA TRIBUNE

ECONOMIE BOURSE ENTREPRISES & FINANCE HI-TECH VOS FINANCES IDÉES MÉTROPOLES CARRIÈRES

Opinions > Tribunes

Bitcoin, fintech, intelligence artificielle ne font pas peur au FMI

Par **Charles Cuvelliez et Jean-Jacques Quisquater** | 17/10/2017, 10:04 | 895 mots

(Crédits : Reuters / Yuri Gripas)

LA TRIBUNE BOURSE

5 365,37 Pts **-0,34 %**

Palmarès

Valeurs	Cours	Variation
Pernod ricard	125,70	+2,86 %
Carrefour	17,45	+1,90 %
Engie	14,27	+0,25 %
Publicis groupe	58,43	-6,05 %

Bank of England: September 29, 2017: end of the banks?

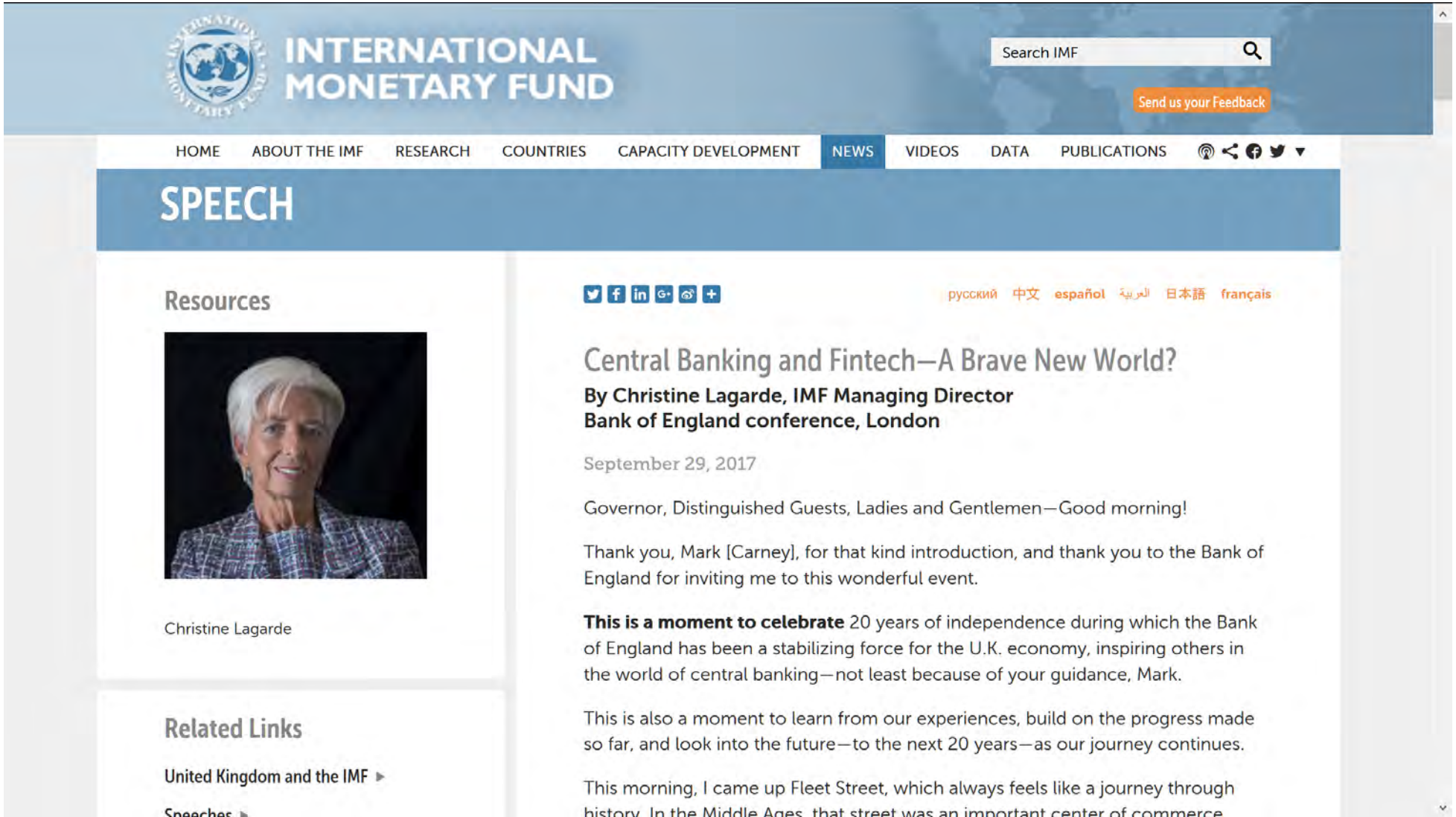
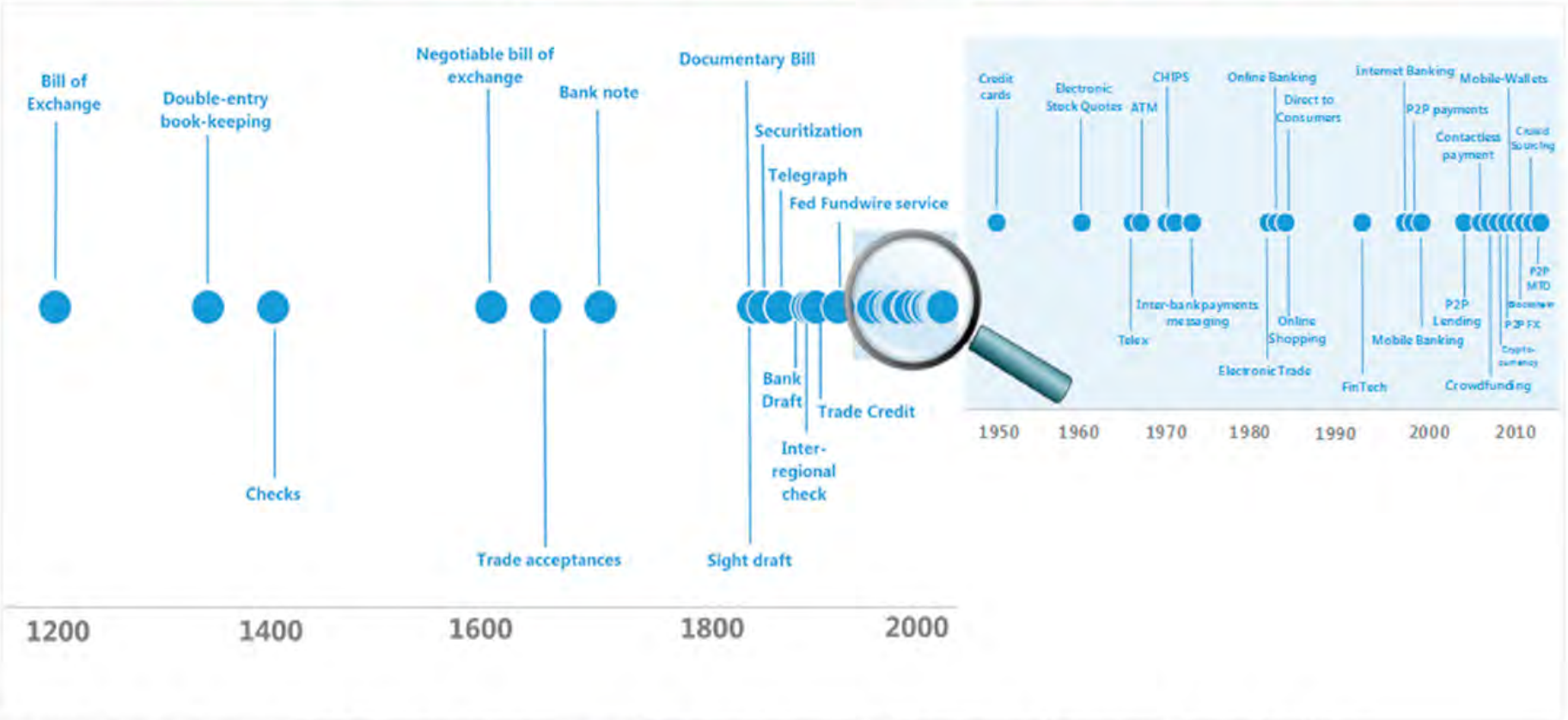
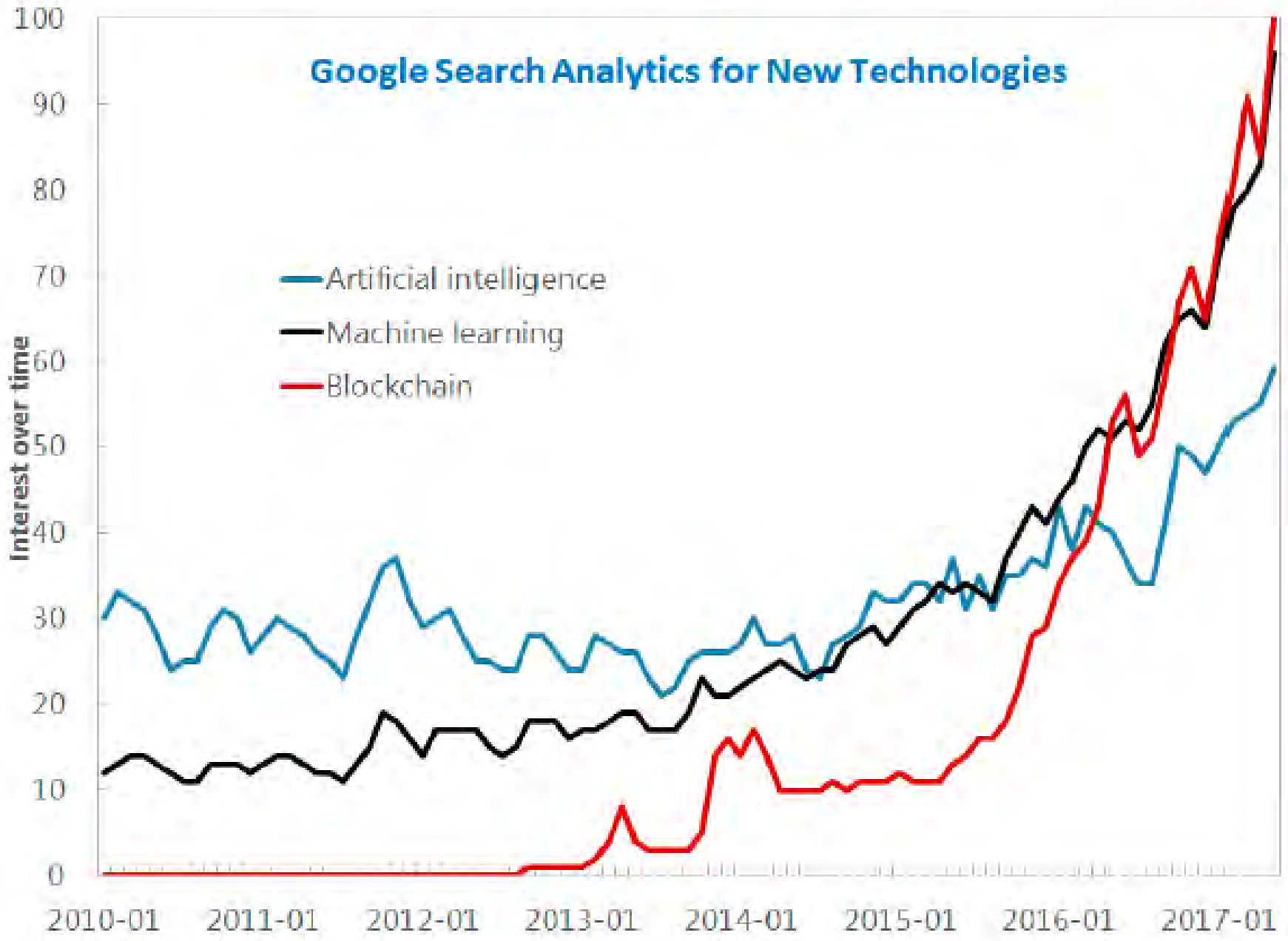


Figure 1. Accelerating Pace of Technological Progress in Financial Services



Sources: Arner, Barberis, and Buckley (forthcoming); Quinn and Roberds (2008); World Economic Forum (2015).



Source: Google Trend Analytics.

Google Trends | Comparer

Connexion

- cryptocurrency — Terme de recherche
- bitcoin — Terme de recherche
- blockchain — Terme de recherche
- euro — Terme de recherche
- macron — Terme de recherche

Dans tous les pays | 2017 , Cinq dernières années | Toutes les catégories | Recherche sur le Web

Évolution de l'intérêt pour cette recherche

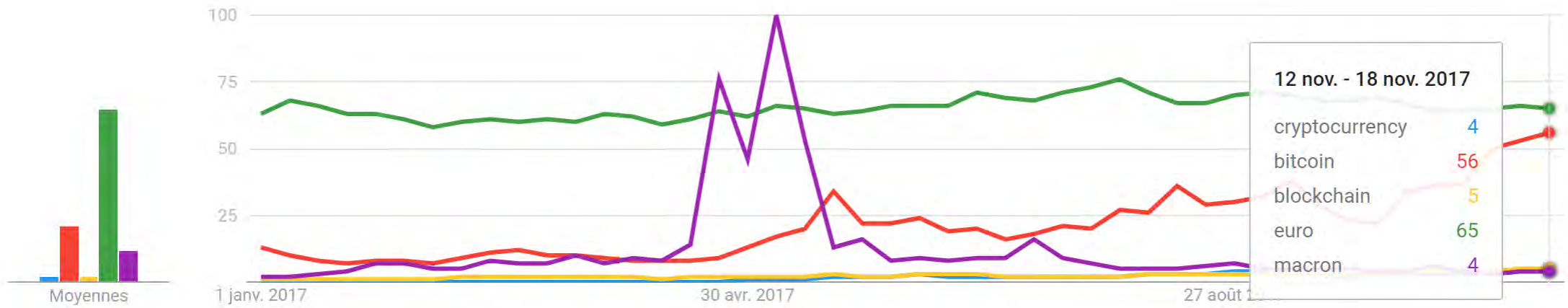
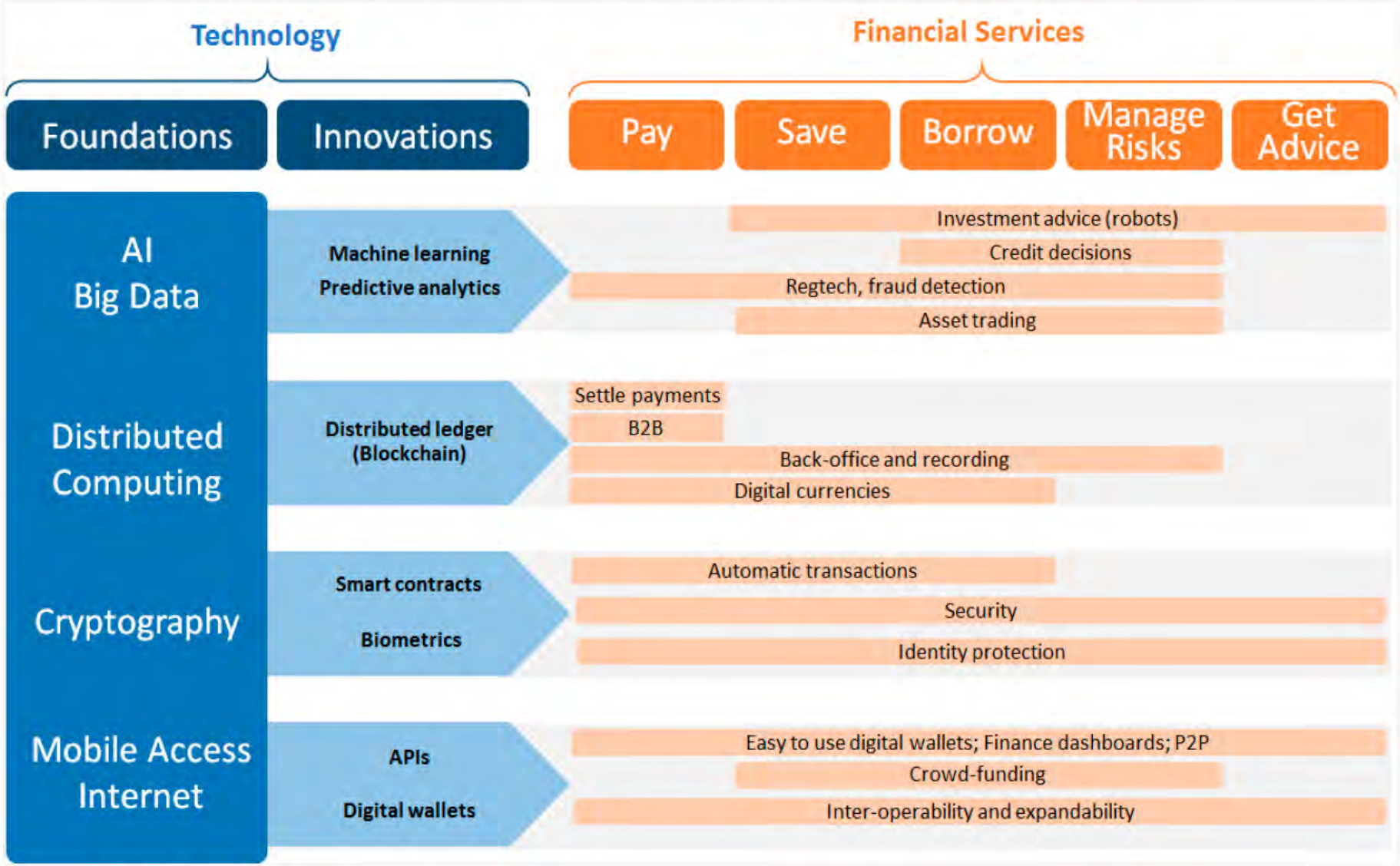


Figure 4. Major Technologies Transforming Financial Services



Source: IMF staff.

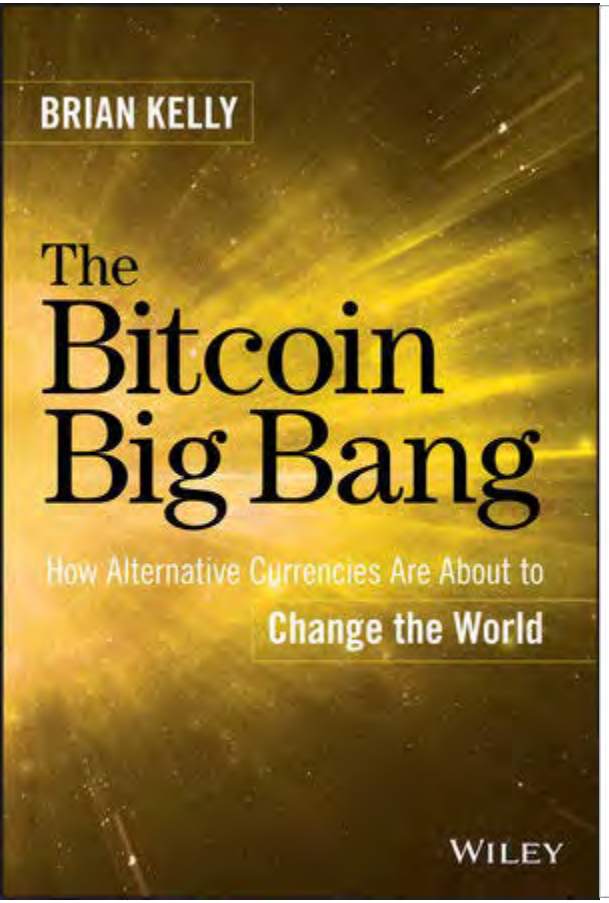
Analyse par Deloitte : vers une monnaie d'Etat

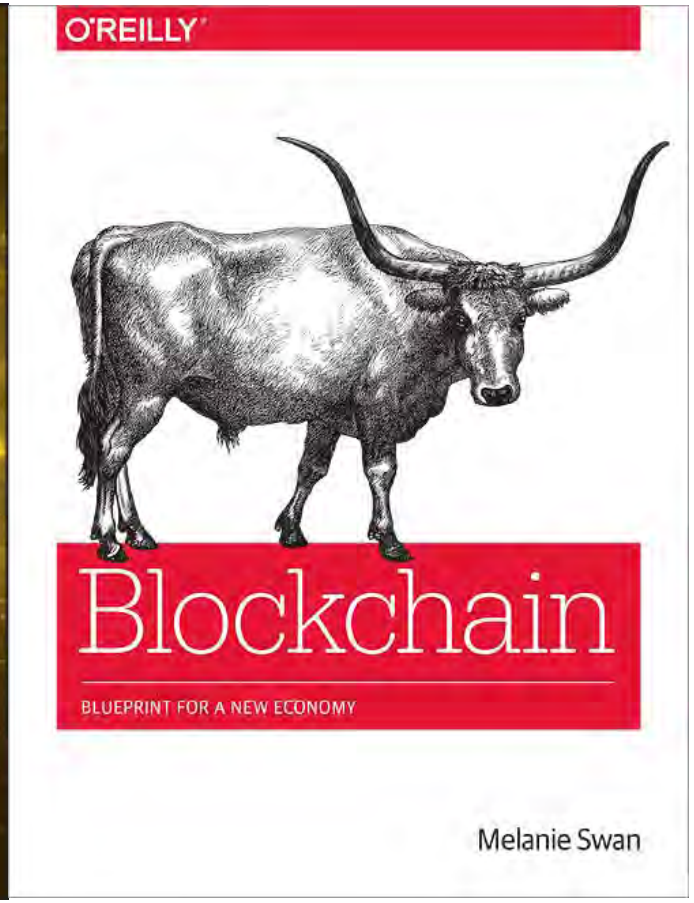
Altcoin News Blockchain News FinTech News

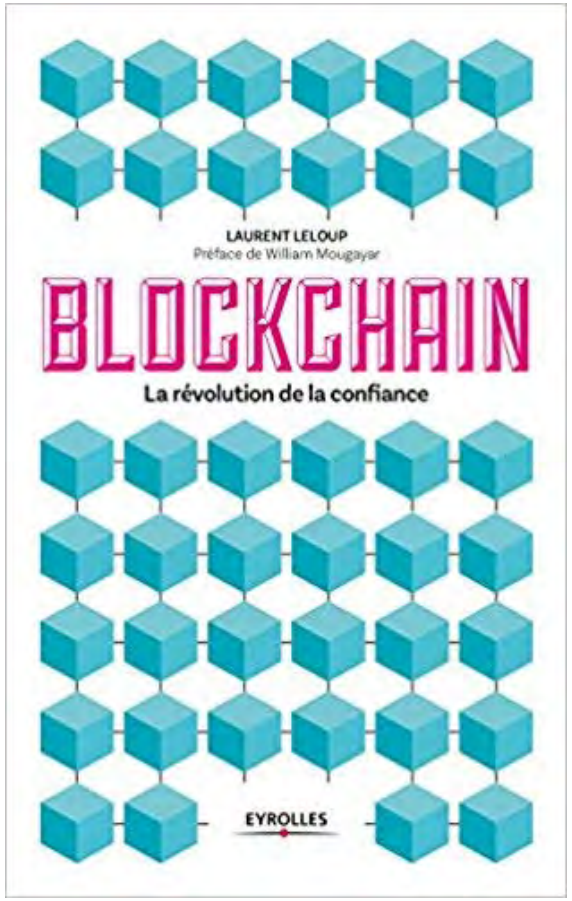
emCash is Dubai's First Official State Cryptocurrency

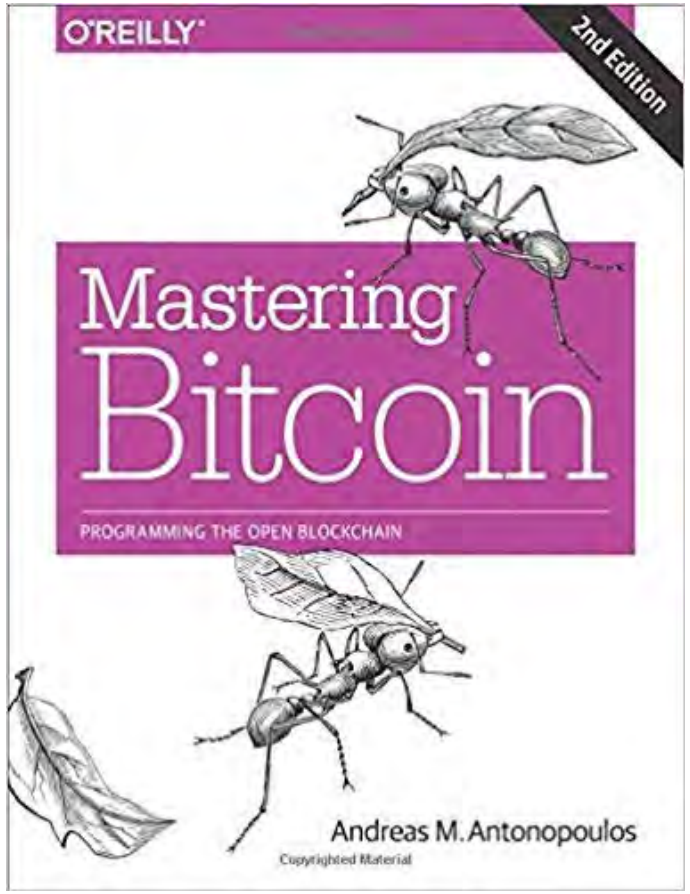
Samburaj Das on 03/10/2017

Livres : blockchain et bitcoin

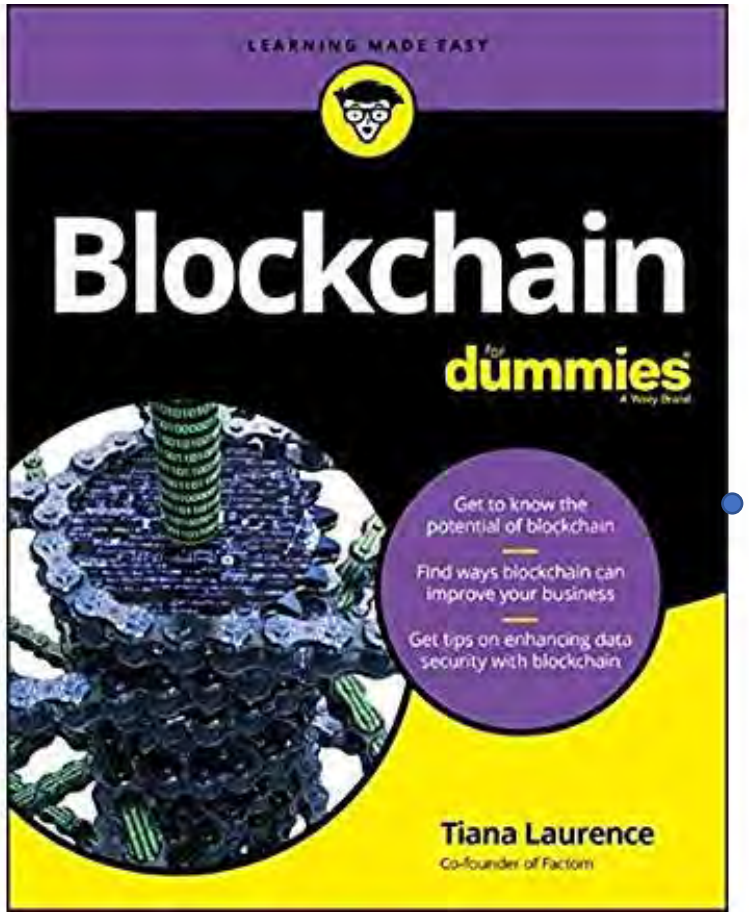








Livres de base



Version française disponible fin janvier 2018

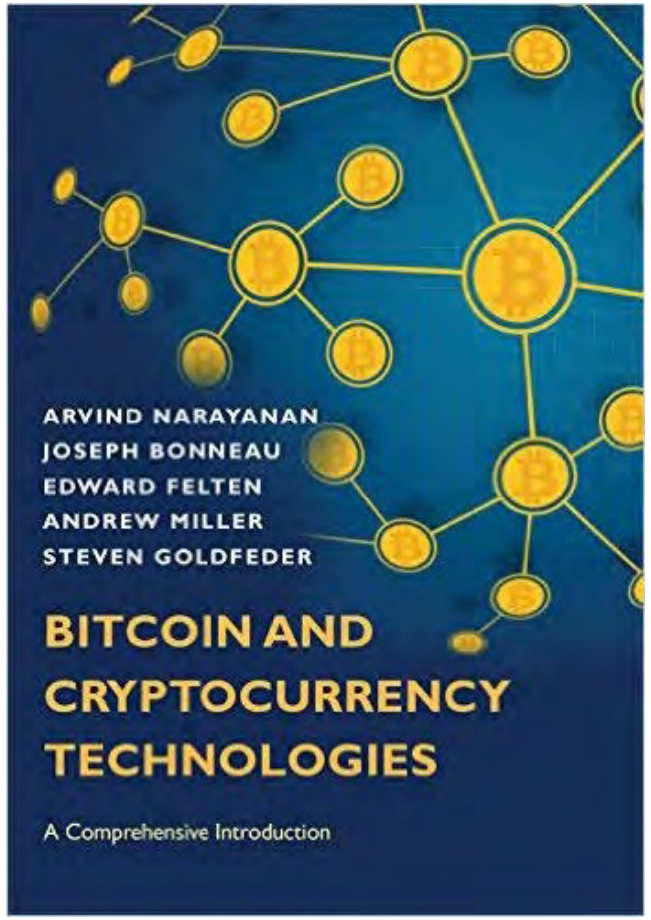
MOOC (cours en ligne)

- https://fr.coursera.org/learn/cryptocurrency
- https://online.princeton.edu/course/bitcoin-and-cryptocurrency-technologies

- https://www.edx.org/course/blockchain-business-introduction-linuxfoundationx-lfs171x

- https://online.stanford.edu/course/bitcoin-and-crypto-currencies

http://bitcoinbook.cs.princeton.edu
(préversion est libre)



Pour suivre le bitcoin et le top

- https://bitcoin.org/fr/ressources
- https://bitcoin.org/fr/innovation

- http://blockchain.mit.edu/
- http://blockchain.cs.ucl.ac.uk (un groupe important !)

- https://news.coinify.com/10-universities-blockchain-courses/

- https://coinmarketcap.com/coins/

Pour suivre les cryptomonnaies

- https://journalducoin.com
- https://cryptoactu.com

L’actualité des blockchains

- https://blockchainfrance.net

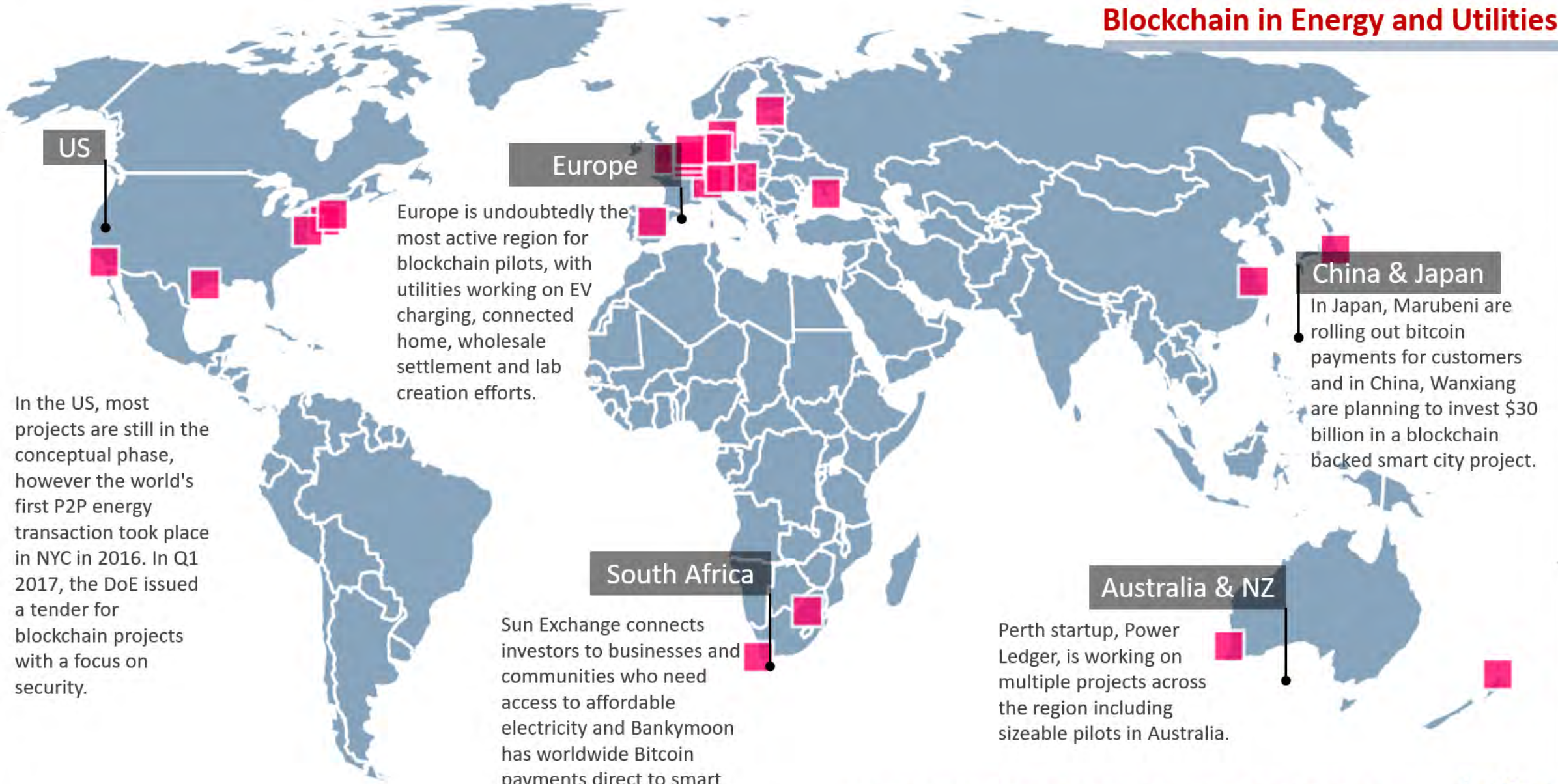
- ICO compétence : http://www.chaineum.com
- http://www.zdnet.fr/actualites/blockchain-4000237562q.htm

- https://www.blockchainresearchinstitute.org/members/


9B22FBC10002C4EF
183695F24A01DE11
82AF3C4156C2109D
EA59EE93346BC3CC
SHA256
Corned Beef
Hash
Internet Style

Indigo Interactive Map

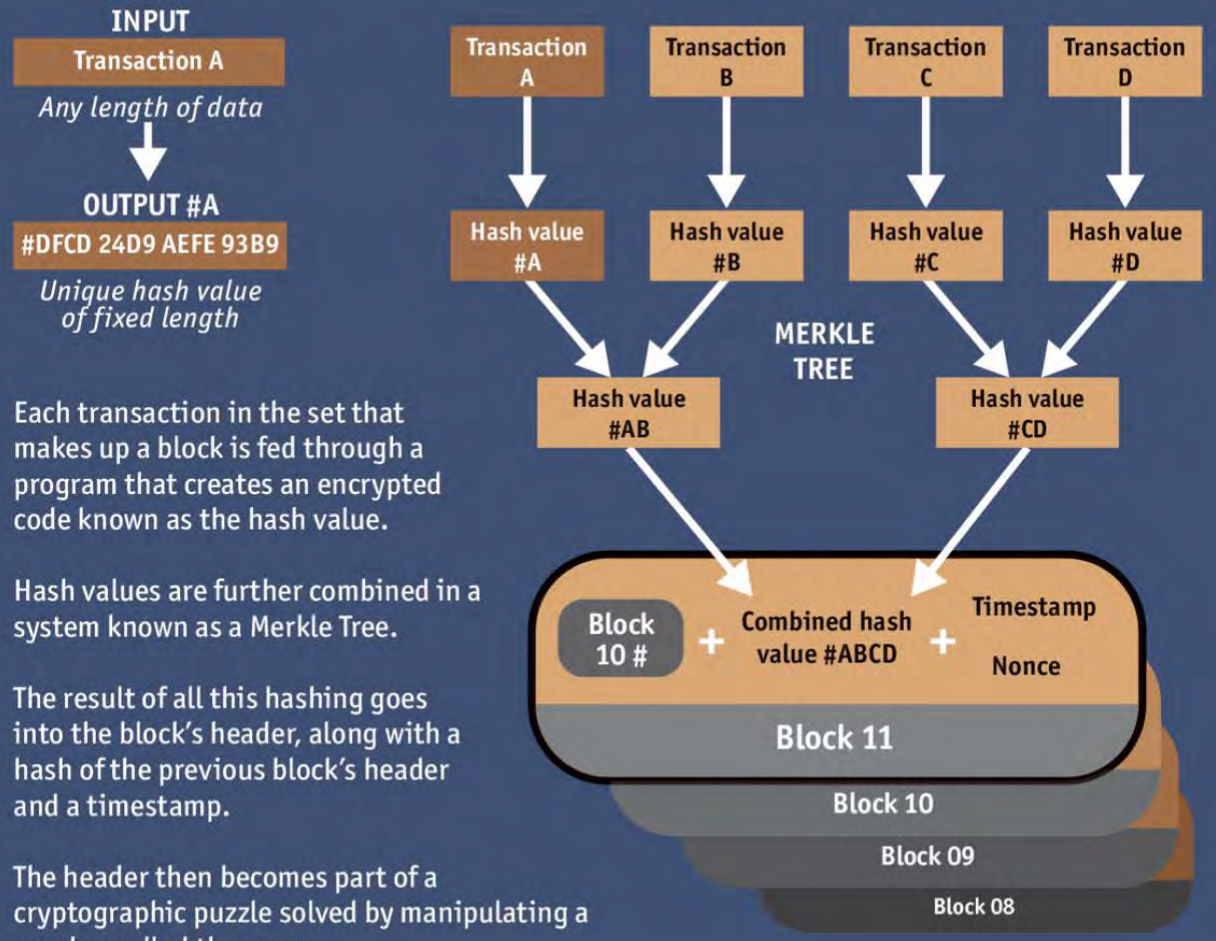
Blockchain in Energy and Utilities



See the map at indigoadvisorygroup.com/blockchain

Indigo ADVISORY

Making a hash of it



Each transaction in the set that makes up a block is fed through a program that creates an encrypted code known as the hash value.

Hash values are further combined in a system known as a Merkle Tree.

The result of all this hashing goes into the block's header, along with a hash of the previous block's header and a timestamp.

The header then becomes part of a cryptographic puzzle solved by manipulating a number called the nonce.

Once a solution is found the new block is added to the blockchain.

Economist.com

Wallet – portefeuille digital

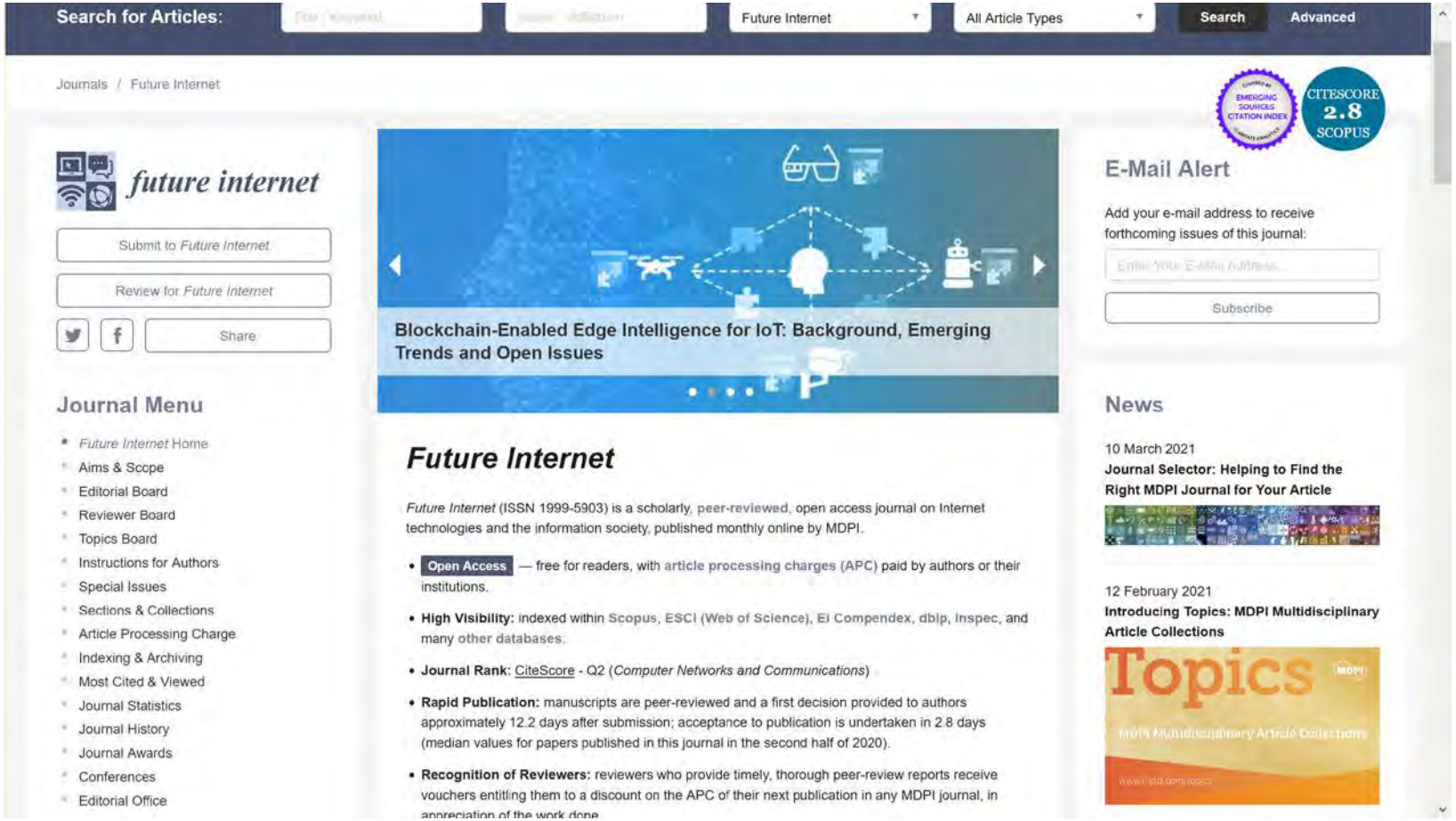
Blockchains : entre mystères et fantasmes (cycle 2020-2021)

- Blockchain et preuve
- Blockchain et droit des sociétés
- Conférence en *streaming* : Blockchain et intelligence artificielle
- Blockchain et santé
- Foisonnement des expressions de la Blockchain

Partager cette page

- Agenda et programme des colloques passés
- **Appels à communication**
- **Colloques ouverts à inscription**
- **Agenda des colloques à venir**
- **Colloques en vidéos**

Appel à article sur les blockchains



- Journal: Future Internet (ISSN 1999-5903,
- https://www.mdpi.com/journal/futureinternet)

    - Section: Cybersecurity

- Special Issue Title: Cryptography in Blockchain

- Special Issue deadline: 20 August 2021 (this is tentative deadline, you
- can adjust it according to your schedule)

- Guest Editor 1: Quisquater Jean-Jacques