



# Les blockchains, des panoptiques ?

Par Adli TAKKAL BATAILLE

Présentation du 28 Juin 2017 au Centre Pompidou

# UNE ROUTE SINUEUSE

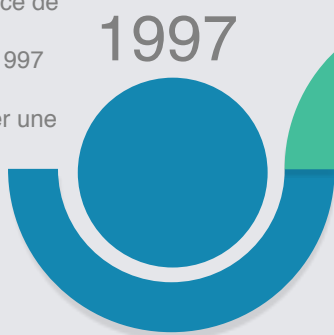
AVANT D'ARRIVER À BITCOIN ET AUX BLOCKCHAINS

## L'idée germe

La conscience d'un Hacker de Blankenship en 1986  
Manifeste Crypto-anarchiste de May en 1988  
Déclaration d'indépendance du Cyberspace de Barlow en 1996  
Un manifeste Cyberpunk de Kirtchev en 1997  
Internet vient de naître, comment lui donner une monnaie ?

90'

1997



Hashcash par Back

Hashcash et principe de preuve de travail (proof-of work)

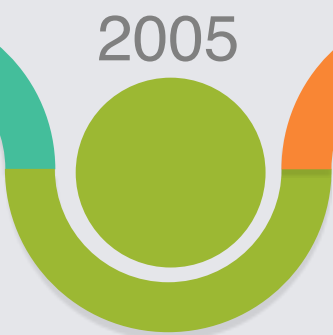
1998



B-Money par Wei Dai

Utilisation du principe de hashcash et de l'horodatage. Système P2P.

2005



BitGold de Szabo

Principe similaire à B-Money. Les puzzles mathématiques sont toujours l'unité monétaire.

Bitcoin

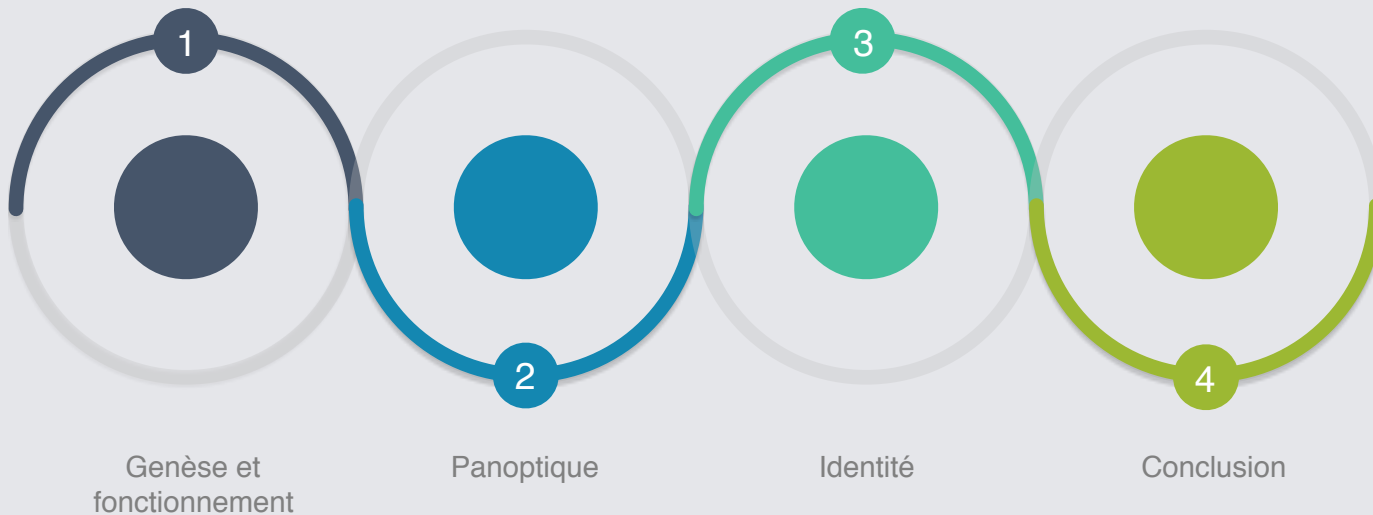
La publication du papier fondateur de Bitcoin : *Bitcoin, a peer-to-peer electronic cash system* par Satoshi Nakamoto

2008



# RENTRONS DANS BITCOIN

QU'ALLONS NOUS ABORDER ?



1

# BITCOIN ?

## INNOVATION PROTOCOLAIRE

Bitcoin est un système de jetons infalsifiables et transférables, conservables en toute sécurité.

Bitcoin peut-être considéré comme une monnaie numérique si ses utilisateurs donnent de la valeur à ces jetons.

Mais Bitcoin est avant tout un protocole informatique comme l'est TCP/IP pour internet. (un système transactionnel) Dans le logiciel Bitcoin, ce sont des jetons nommé bitcoins.

Bitcoin peut en plus permettre d'autres choses: considérons la monnaie Bitcoin comme une méta-monnaie.

Le consensus de Bitcoin est exprimé dans sa blockchain

**Protocole  
Logiciel  
Réseau  
Monnaie**



# 1 LES BLOCKCHAINS

Zoom sur les particularités de ces bases de données structurantes

## POINTS COMMUNS

- Chainage unidirectionnel immuable avec timestamp
- *Trustless* (sans confiance)
- Écritures transactionnelles avec des tokens
- Contrats auto-exécutables
- Encadrées par un protocole
- Distribuées

## VARIANTES

- Ouverte (Bitcoin) /Semi-Ouverte (HyperLedger) / Fermée
- Avec blocs (Bitcoin) ou sans bloc (IOTA)
- Turing Complete (Ethereum) ou non (Bitcoin)
- Transparente (Bitcoin) ou non (Monero)
- Sans-token-et-avec token
- Différence de langage (Formel / Non formel)

## ENVIRONNEMENT

- *Incentive* (motivation) pour faire tourner le réseau
- Cryptographie asymétrique
- Algorithme de consensus
- Communauté importante ou non

Un sacré fourre-tout non ?

# MOT FOURRE TOUT







LA BLOCKCHAIN N'EXISTE PAS

IL Y A DES **BLOCKCHAINS** PRODUITES PAR LE  
**CONSENSUS** DE DIFFÉRENTS **PROTOCOLES**

# 1 NOUVELLE NORME

Un alphabet des échanges

Les protocoles avec blockchains sont une nouvelle norme de communication internationale.

L'aspect normatif du protocole est capital.

C'est un nouvel alphabet sur lequel il est possible de construire énormément de choses diverses et variées.





The background of the image is a deep space photograph showing a dense field of stars and a prominent nebula with purple and blue hues. The text is overlaid on this cosmic scene.

UNE NOUVELLE COSMOLOGIE

**DES RÉSEAUX HORIZONTAUX ET AUTONOMES  
AU CONSENSUS DÉCENTRALISÉ**



2

# UN PANOPTIQUE

Les blockchains sont-elles des panoptiques ?

Foucault nous dit : « le *Panopticon* ne doit pas être compris comme un édifice onirique : c'est le diagramme d'un mécanisme de pouvoir ramené à sa forme idéale ; son fonctionnement, abstrait de tout obstacle, résistance ou frottement, peut bien être représenté comme un pur système architectural et optique : c'est en fait une figure de technologie politique qu'on peut et qu'on doit détacher de tout usage spécifique. »

Les blockchains sont également transparentes.

Linguistiquement on retrouve des chaînes.

Mais ces chaînes sont libératrices et les vitres peuvent être opaques. Panoptique sans autorité !

Une libération par des jetons idéaux ?



3

# IDENTITÉ

Traditionnellement

Délégation à des grandes entreprises.

Prédation de l'identité pour le pistage.

Des systèmes non inter-opérables.

Fiabilité discutable



3

# IDENTITÉ

Nouveau Paradigme

Déterritorialisation de l'identité

Réseau Rhizomatique d'identité

Jeu de certification entre pairs et autorités

Segmentation de l'identité

Identité normalisée

Confidentialité accrue





3

# IDENTITÉ

De nouveaux usages

Apparition d'une méta-identité

Possibilité hardware

Possibilité d'authentification unique et sécurisée

Possibilité d'organisation de communautés locales

Possibilité de voter en ligne

Et d'autres encore à imaginer





4

# Conclusion

Un système cohérent pour de tels buts

Les blockchains semblent être des panoptiques où il serait possible d'accueillir nos identités.

Cela peut-être un atout pour de nombreux acteurs différents et surtout pour le citoyen.

Cependant il faudra tout de même faire attention à conserver la vie privée et la décentralisation pour ne pas que cela deviennent un vrai panoptique.



# MERCI !

## DES QUESTIONS ?

### S'informer



### S'impliquer

