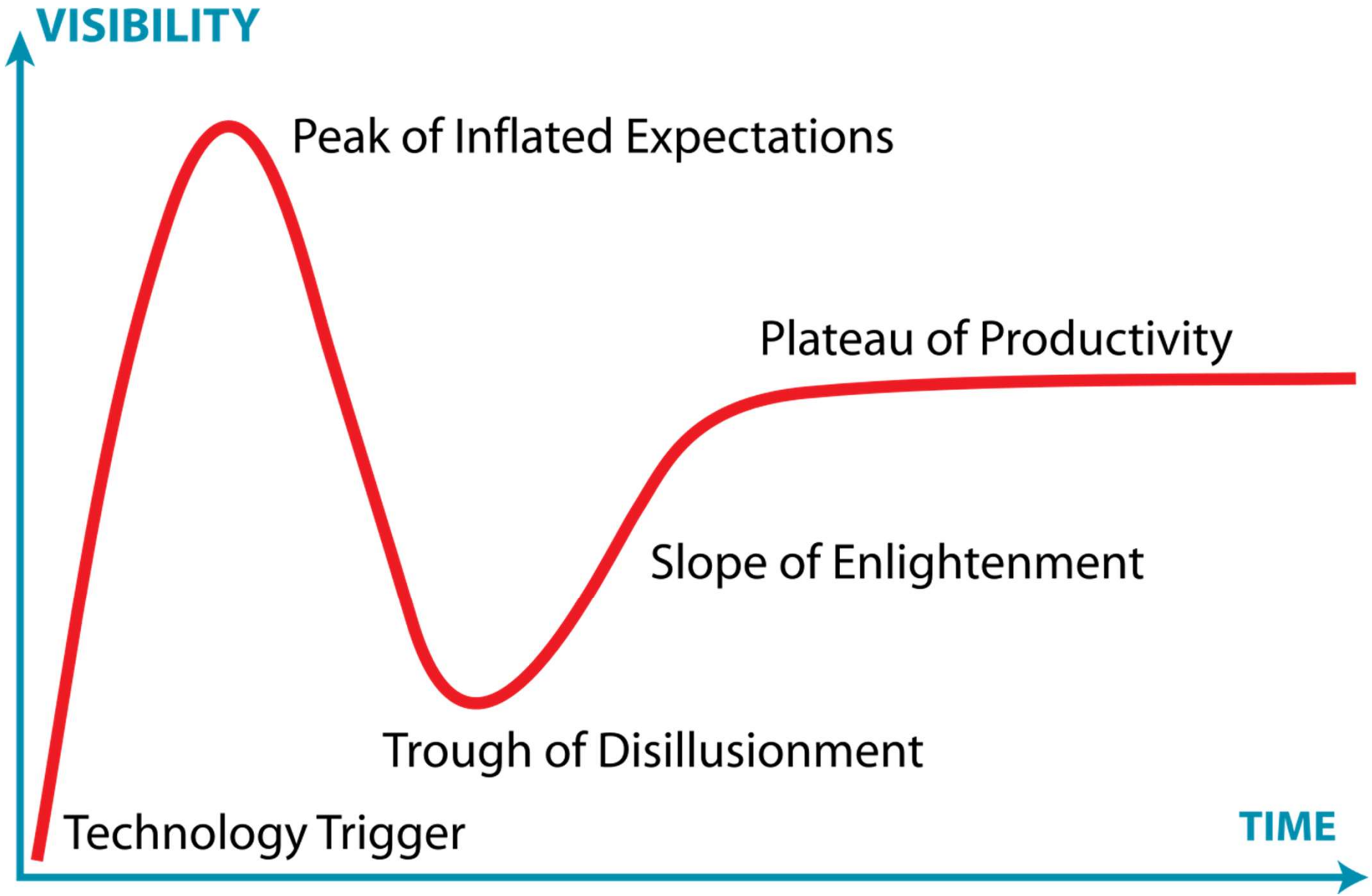
Introduction à la blockchain

Yorick de Mombynes

CNES, 15/10/20


VISIBILITY
Peak of Inflated Expectations
Plateau of Productivity
Slope of Enlightenment
Trough of Disillusionment
Technology Trigger
TIME

Plan

1. **Ancêtre**
2. **Promesses**
3. **Illusions**
4. **Perspectives**

Plan

1. **Ancêtre**
2. **Promesses**
3. **Désillusions**
4. **Perspectives**

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.

Tiers de confiance

- Micropaiements
- Vie privée
- Monnaie

Enjeux

- Cash numérique
- Double dépense
- Numérique & non duplicable

Innovation

- Réseau de paiements
  - Sans tiers de confiance
  - Résistant à la censure
- Système monétaire
  - Sans régulation centrale
  - Résistant à l’inflation
  - Programmable

Enjeu

- Consensus distribué
- Sécurité maximale

Concepts

- Open source
- Transactions publiques
- Registre distribué
- Décentralisation

Technologies

- Cryptographie asymétrique
- P2P
- Registre distribué (blockchain)
- Minage par la preuve de travail

J. Cryptology (1991) 3: 99–111

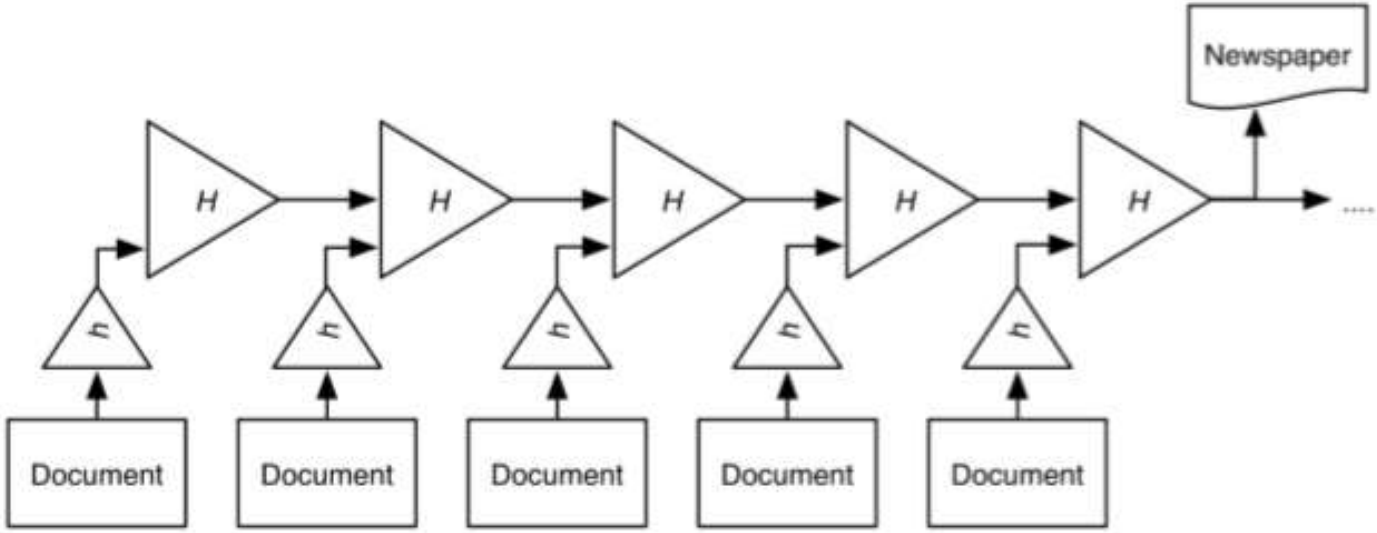
Journal of Cryptology

How To Time-Stamp a Digital Document[1]

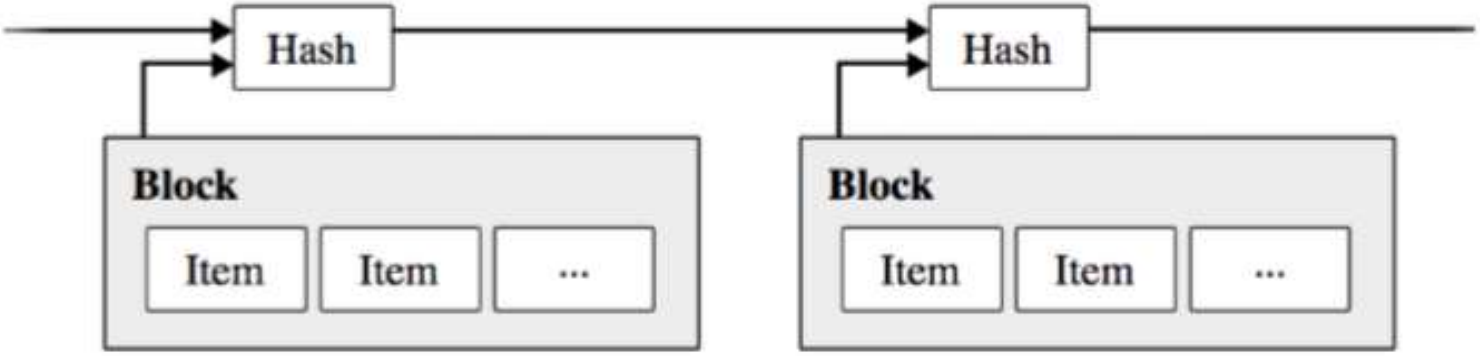
Stuart Haber and W. Scott Stornetta

Bellcore, 445 South Street,
Morristown, NJ 07960-1910, U.S.A.
stuart@bellcore.com stornetta@bellcore.com

Chaîne d'horodatage inventée dans les années 1990

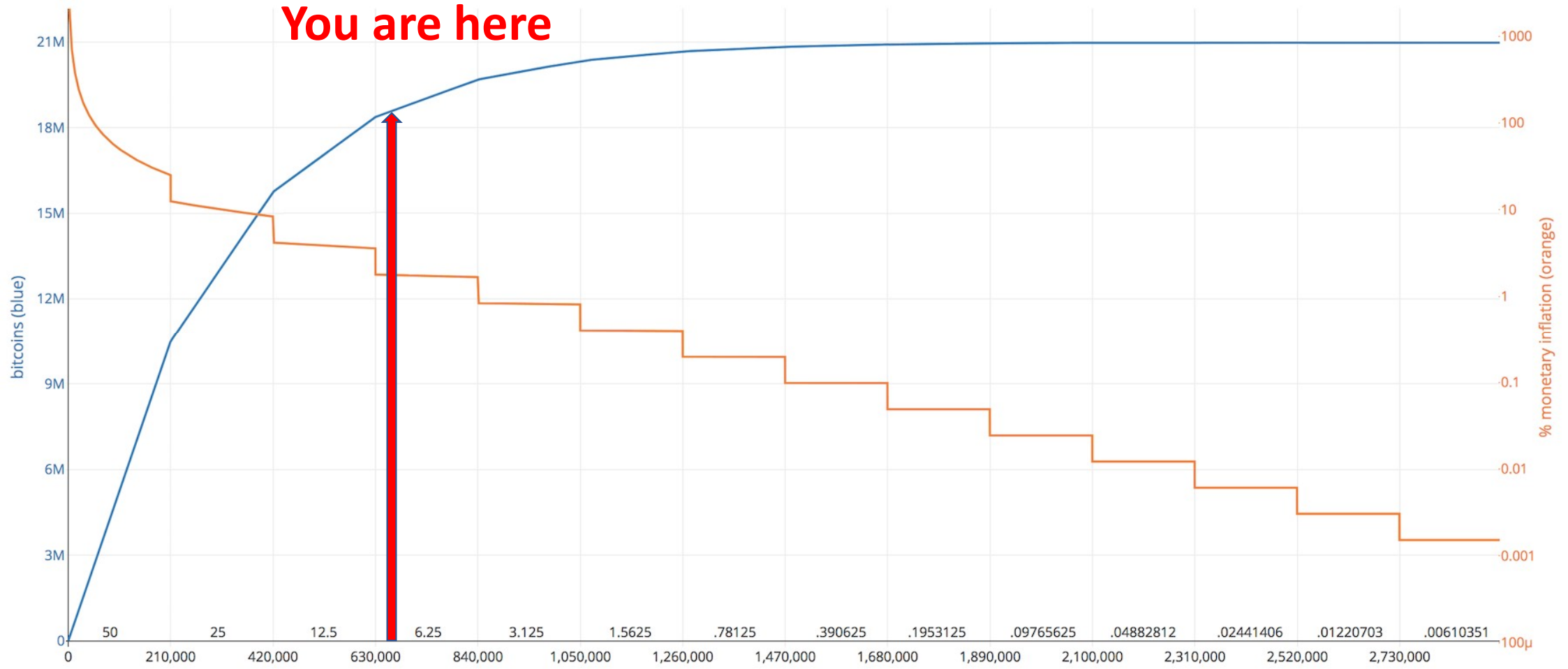


Chaîne d'horodatage du white paper Bitcoin



Minage par la preuve de travail

- Compétition
- Equation cryptographique
- Jeton natif
- Dépense énergétique
- Ajustement de la difficulté


You are here
21M
18M
15M
12M
9M
6M
3M
0
bitcoins (blue)
1000
100
10
1
0.1
0.01
0.001
100µ
% monetary inflation (orange)
50
25
12.5
6.25
3.125
1.5625
.78125
.390625
.1953125
.09765625
.04882812
.02441406
.01220703
.00610351
0
210,000
420,000
630,000
840,000
1,050,000
1,260,000
1,470,000
1,680,000
1,890,000
2,100,000
2,310,000
2,520,000
2,730,000

« Révolution blockchain » ?

- Deux fonctionnalités :
  - Ancrage, horodatage
  - Programmabilité

→ Usages non monétaires ?

Plan

1. Ancêtre
2. **Promesses**
3. Désillusions
4. Perspectives


SCEGLIERE LA BEVANDA
Zucchero
- zucchero
+ zucchero
espresso
caffè d'orzo
caffè lungo
caffè d'orzo macchiato
caffè macchiato
cioccolato
cappuccino
tè al limone
Solista
NECTA
ART OF THE BREAK

Smart contracts

- Concept
  - Automatique, incensurable
  - Oracles
- Exemple : assurance
- Decentralized Autonomous Organizations (DAO)

Secteurs

- Assurance
- Finance
- Audit
- Logistique
- Industrie
- Objets connectés
- Notariat
- Propriété intellectuelle
- Identité
- Vote

Blockchains

- Ethereum, Tezos, etc.
- Paramètres :
  - Langage de programmation
  - Auditabilité
  - Algorithme de consensus
    - Preuve de travail
    - Preuve d’enjeu
  - Régime d’émission

Boom

- POC : proof of concept
- DAO : decentralized autonomous organization
- ICO : initial coin offerings
- STO : security token offering

Plan

1. Ancêtre
2. Promesses
3. **Désillusions**
4. Perspectives

Enjeux techniques

- Blockchain publique / privée
- Complexité, lourdeur, bugs
- Oracles
- Besoin ?

Enjeux économiques et juridiques

- ICO : démobilisation, arnaques
- Vulnérabilité à la régulation
- Incentives économiques :
  - Algorithme de consensus
  - Régime d'émission
- (Crypto)monnaies ? Cryptoactifs ?

Plan

1. Ancêtre
2. Promesses
3. désillusions
4. **Perspectives**

Perspectives

- Cadre réglementaire et fiscal
- Compétition
  - Entre blockchains
  - Entre Etats
- Nouveaux services
- DeFi

Conclusion

- Espoir…déceptions
- « Technologie blockchain »
- « Autoroutes de l’information »
- Enjeu monétaire
- Maturité ?