

La Blockchain: révolution dans le monde de la confiance

Jacques PANTIN
7 Septembre 2016

JPA: Une rapide présentation

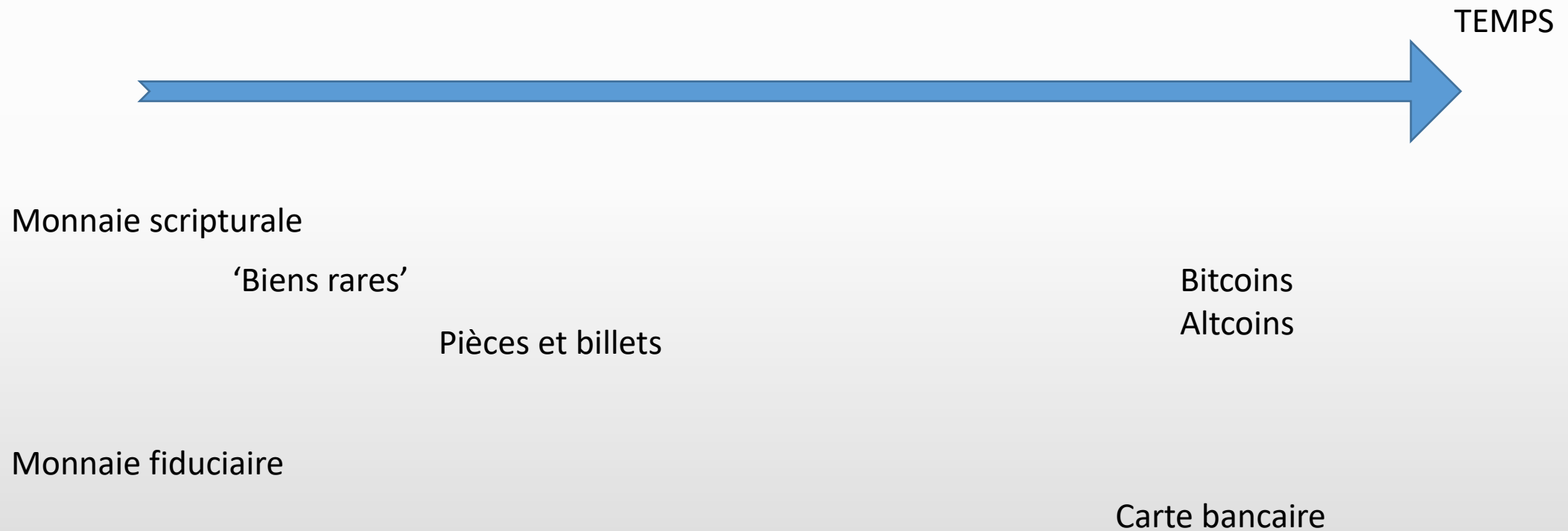
- Manager et créateur d'entreprises
- Engagement fort dans les problématiques de sécurité et de confiance
- Dictis: architectures techniques
- Certplus: l'Autorité de Confiance française
- Dictao: éditeur de solutions d'authentification, de signature et d'archivage

A stylized, handwritten signature in black ink, consisting of a series of loops and curves.

- Le contexte
- Le Bitcoin comme monnaie
- La Blockchain comme plate-forme technique
- Les défis
- Les cas d'usage

What, Why, How?

Les monnaies



Le rôle d'une monnaie

Une monnaie a 3 fonctions

- Une unité de compte
- Une réserve de valeur (une fonction 'coffre-fort')
- Un intermédiaire pour des échanges

Le rôle du tiers de confiance

- Pour une monnaie fiduciaire, l'AC (Autorité de Confiance) a la charge de:
 - Créer la monnaie
 - En garantir la stabilité
- Pour une monnaie scripturale, l'AC garantira en outre:
 - La qualité de la transaction et, en particulier le non 'double spending'
 - La conservation de la monnaie dans des 'comptes bancaires'
- Dans le monde bancaire, la confiance s'est organisée autour de:
 - Un modèle à 4 coins (les grands schemes comme Visa, Mastercard, GIE CB)
 - Un modèle 3 coins (AMEX, PayPal)

Le bitcoin: Les principes

Le besoin d'une cryptomonnaie:

- Anonyme
 - L'utilisateur ne dévoile pas son identité 'réelle', mais s'appuie sur des jeux de clés cryptographiques
- Sans AC

La transaction (et donc le non 'double spending') sera garantie:

- Non pas par un intermédiaire tel qu'une banque
 - Mais par un pool d'acteurs anonymes (les 'mineurs') qui par leurs travaux permettront de définir un consensus
- Décentralisée
 - Pour éviter d'abord les pannes, mais surtout la censure

Bitcoin: Une première définition



Un réseau pair à pair permettant de transférer de l'argent sans l'intervention d'une entité centrale et, en particulier, d'une banque

Une monnaie



Une plateforme de confiance

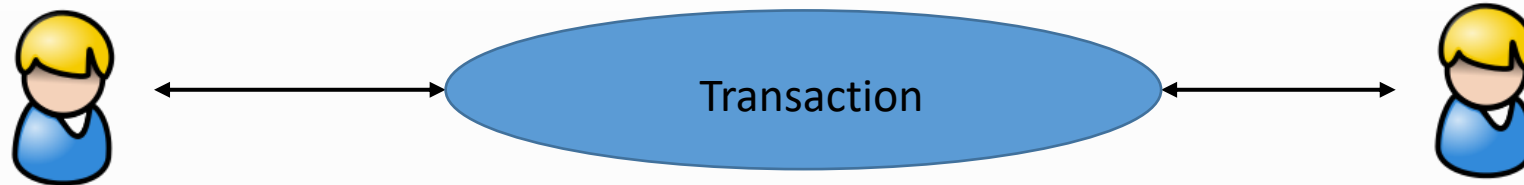
La Blockchain

Un assemblage très innovant de solutions cryptographiques existantes (hash et signature) dans une approche décentralisée et anonyme

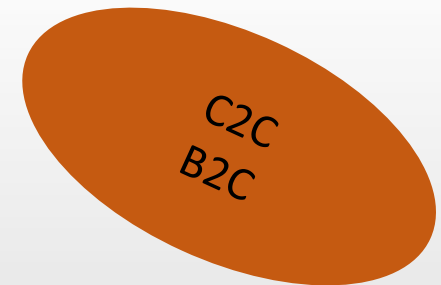
Un réseau PtoP / P2P

'Bitcoin is an implementation of Wei Dai's b-money proposal on Cypherpunks in 1998 and Nick Szabo's Bitgold proposal'
Satoshi Nakamoto

Intérêt du bitcoin



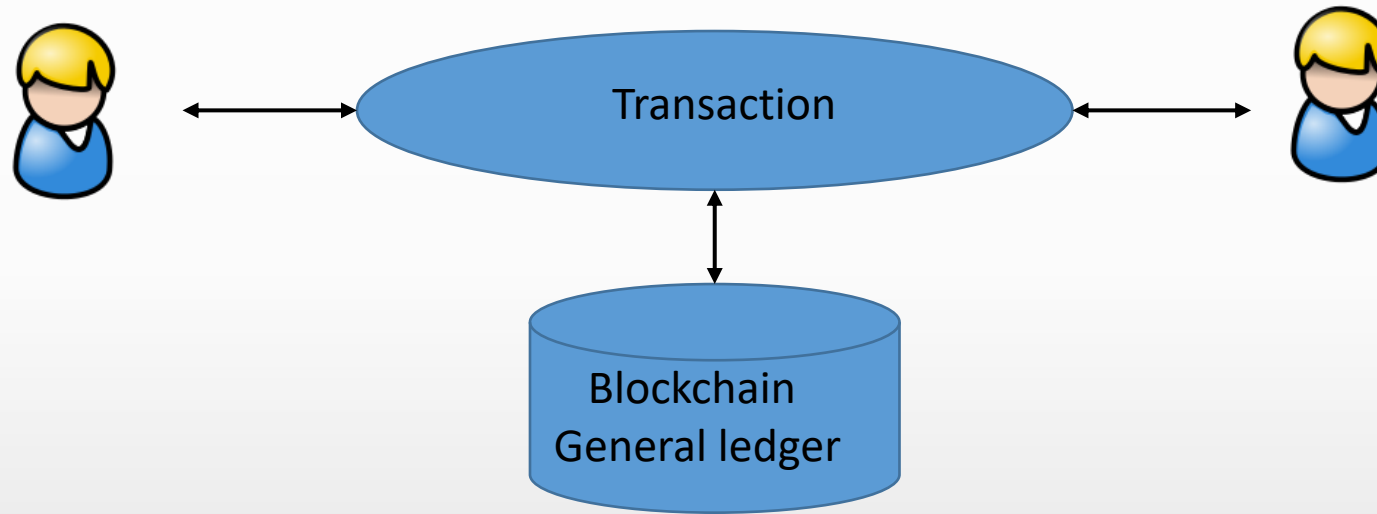
- Une monnaie mondiale
 - Pas d'intermédiaire, pas de frais multiples
- Un réel anonyme
 - Blanchiment, achat de produits et substances illicites!!
- Une instantanéité
 - Délais de l'ordre de la dizaine de minutes, quelle que soit la position des acteurs
- Un potentiel spéculatif
 - Stock de monnaie encore faible
- Quelques incidents
 - Problématiques de 'gestion des bugs' et de la gouvernance



Le bitcoin comme unité de compte

- Un stock de monnaie encore limité (une dizaine de milliards d'€)
 - Pas de banque centrale pouvant intervenir sur le cours
 - Et donc, une valeur très spéculative
- Un stock qui sera limité à terme (2140) à 21 millions de BtC
 - Donc une 'monnaie déflationniste'
- Un processus de création associé aux travaux des mineurs (25 BtC pour le mineur gagnant)
- La possibilité de convertir de la 'vraie monnaie' (€, \$...) en BtC et réciproquement
 - Initialement, de la 'main à la main'
 - Aujourd'hui:
 - En ligne avec des agences de change
 - Avec des 'DAB/GAB'

Blockchain: 3 grandes fonctions



- Système transactionnel (quasi-instantanéité, décentralisation, approche universelle)
- 2 usages principaux:
 - Échange d'argent (en multi devises)
 - Enregistrement de titres
- Minage: Inscription dans le 'General Ledger'
- Coffre-fort et outil de traçabilité



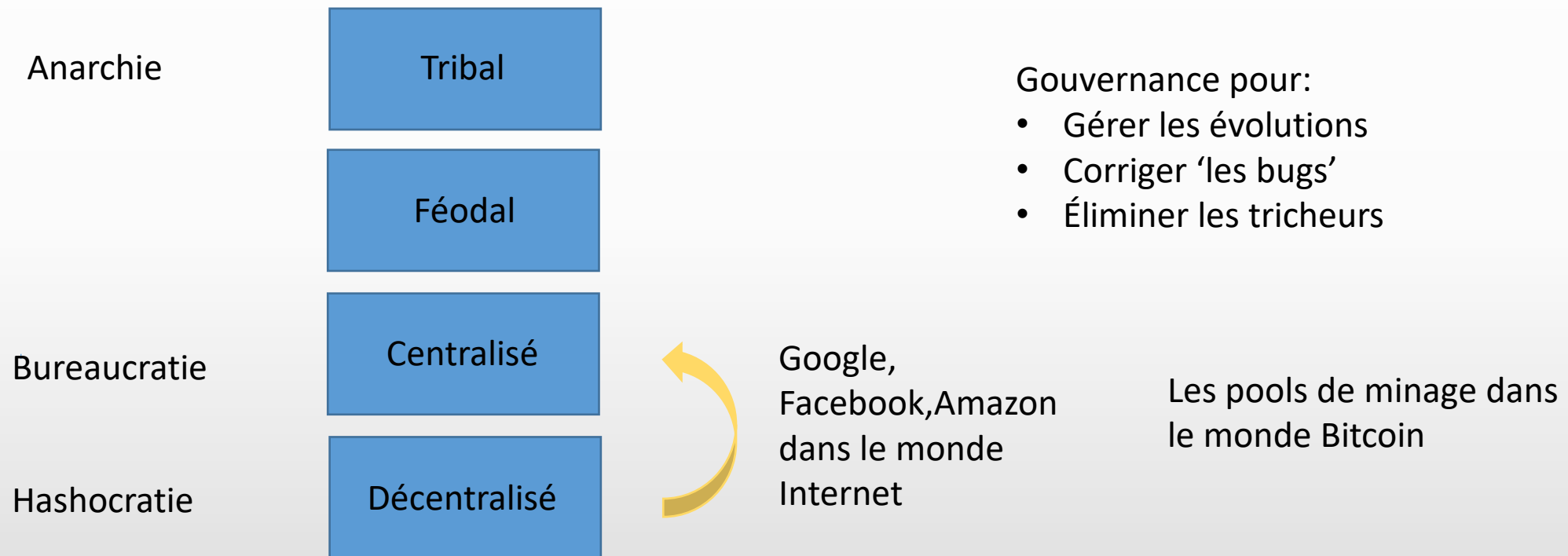
Quelques axes de travail

- La performance et les délais
- La gouvernance
- (La confiance)

Les performances et les délais

- Fondamentalement liées:
 - Au principes d'un fonctionnement P2P
 - Aux techniques de minage retenues:
 - Un nombre maximale de mineurs
 - 'Proof of work' (la résolution d'un puzzle)
- La puissance nécessaire pour être le premier à sceller un bloc:
 - D'une CPU aux GPU et, maintenant, des chips spécialisés
- L'équipement nécessaire: coût supérieur à 100 000€
 - D'où l'apparition de 'fermes de minage'
- L'énergie consommée:
 - Celle d'une ville de 300.000 habitants
 - Supérieure à celle de Google
- Ethereum (dont les performances sont supérieures à celles de Bitcoin) est comparé à un 'smartphone des années 90'
- Les temps de réponse sont longs (6 fois environ 10 mn pour être certain de la validité de la transaction)

La gouvernance



La confiance

- Qualité de l'infrastructure
- Stockage des clés privées (multi-sig)
- Identité des mineurs
- Identité des acteurs

La blockchain: Un système qui s'enrichit rapidement - 1

(environ 700 altcoins...)

GFU- Groupe Fermé d'Utilisateurs



BLC – Blakecoin
GLD – GoldCoin
....

Systèmes
transactionnels

Archivage
Traçabilité

Bitcoin

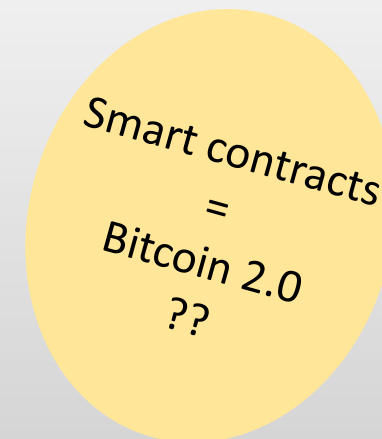
Blockchains publiques

Blockchains privées
Blockchains fédérées

La blockchain: Un système qui s'enrichit rapidement - 2

Avec Ethereum (et ses concurrents)...

- Du 'smart contract' au 'World Computer'
- Le bloc contient des transactions (à la Bitcoin), mais aussi des programmes, eux-mêmes déclenchés par des transactions
- L'approche 'smart contracts' concentre, aujourd'hui, la majorité des investissements

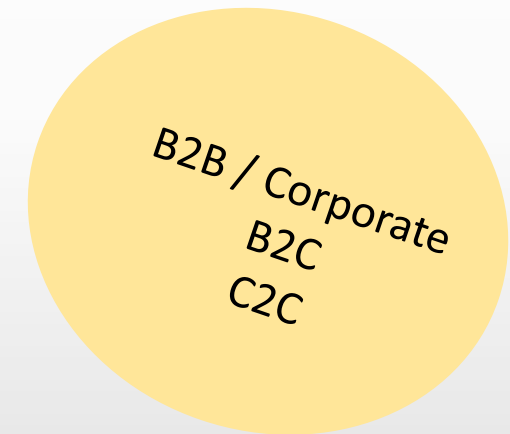


Les enjeux en sécurité

- Stabilité à long terme (fonctions cryptographiques)
- Risque d'un 'breakdown' majeur (malgré l'approche décentralisée)
- Gestion des 'bugs'
- Gouvernance du système et cadre légal
- 'Garbage in /Garbage out' ou la confiance à l'entrée:
 - Connaitre les utilisateurs (gestion d'identité)
 - Identifier la qualité des inputs

Quelques pistes d'utilisation

- Crypto-monnaies
- Gestion de titres
 - Finances
 - Cadastre
- Bourses d'échange/Places de marché
- Tracabilité
- IOT
- Applications sociétales (DAO)
- ...



En conclusion

???

Code is Law

- What, Why, How
 - On sait répondre précisément à la question 'How'
 - Les cas d'usage (qui sont aujourd'hui, d'abord, à l'état de POC's) nous permettront de définir à la question du Why
 - La question du What reste encore en discussion
- Si l'on avait mis des fonctions de paiement dans les browsers, Ethereum n'existerait probablement pas