

Cardano

Blockchain de 3ème Génération

Malik Koné

Mardi 1 juin 2020

Outline

1. Introduction
2. Blockchain de 1^{re} et 2^e Génération
3. Cardano : blockchain de 3^e génération
4. Perspectives

1. Introduction

2. Blockchain de 1^{re} et 2^e Génération

3. Cardano : blockchain de 3^e génération

4. Perspectives

Définitions

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus
- ▶ Cryptographie
- ▶ Application distribuée (dApp)

Token-économie

- ▶ Tokens ou jeton
- ▶ Porte-feuilles électroniques
- ▶ Les marchés de crypto-monnaies

Définitions

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus
- ▶ Cryptographie
- ▶ Application distribuée (dApp)

Token-économie

- ▶ Tokens ou jeton
- ▶ Porte-feuilles électroniques
- ▶ Les marchés de crypto-monnaies

Définitions

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus
- ▶ Cryptographie
- ▶ Application distribuée (dApp)

Token-économie

- ▶ Tokens ou jeton
- ▶ Porte-feuilles électroniques
- ▶ Les marchés de crypto-monnaies

Définitions

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus
- ▶ Cryptographie
- ▶ Application distribuée (dApp)

Token-économie

- ▶ Tokens ou jeton
- ▶ Porte-feuilles électroniques
- ▶ Les marchés de crypto-monnaies

Définitions

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus
- ▶ Cryptographie
- ▶ Application distribuée (dApp)

Token-économie

- ▶ Tokens ou jeton
- ▶ Porte-feuilles électroniques
- ▶ Les marchés de crypto-monnaies

Définitions

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus
- ▶ Cryptographie
- ▶ Application distribuée (dApp)

Token-économie

- ▶ Tokens ou jeton
- ▶ Porte-feuilles électroniques
- ▶ Les marchés de crypto-monnaies

Définitions

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus
- ▶ Cryptographie
- ▶ Application distribuée (dApp)

Token-économie

- ▶ Tokens ou jeton
- ▶ Porte-feuilles électroniques
- ▶ Les marchés de crypto-monnaies

Quel problème résoud la 1^{re} blockchain : Bitcoin-core ?

Comment créer une *espèce digitale*, ou *l'argent de l'Internet* ?

HTTP - 1990



1995

TCP/IP - 1974



1984

Ethernet - 1974



1979

Quel problème résoud la 1^{re} blockchain : Bitcoin-core ?

Comment créer une *espèce digitale*, ou *l'argent de l'Internet* ?

SSL/TLS - 1996



HTTP - 1990



TCP/IP - 1974



Ethernet - 1974



Quel problème résoud la 1^{re} blockchain : Bitcoin-core ?

Comment créer une *espèce digitale*, ou *l'argent de l'Internet* ?



2009

???

SSL/TLS - 1996



HTTP - 1990



TCP/IP - 1974



1984

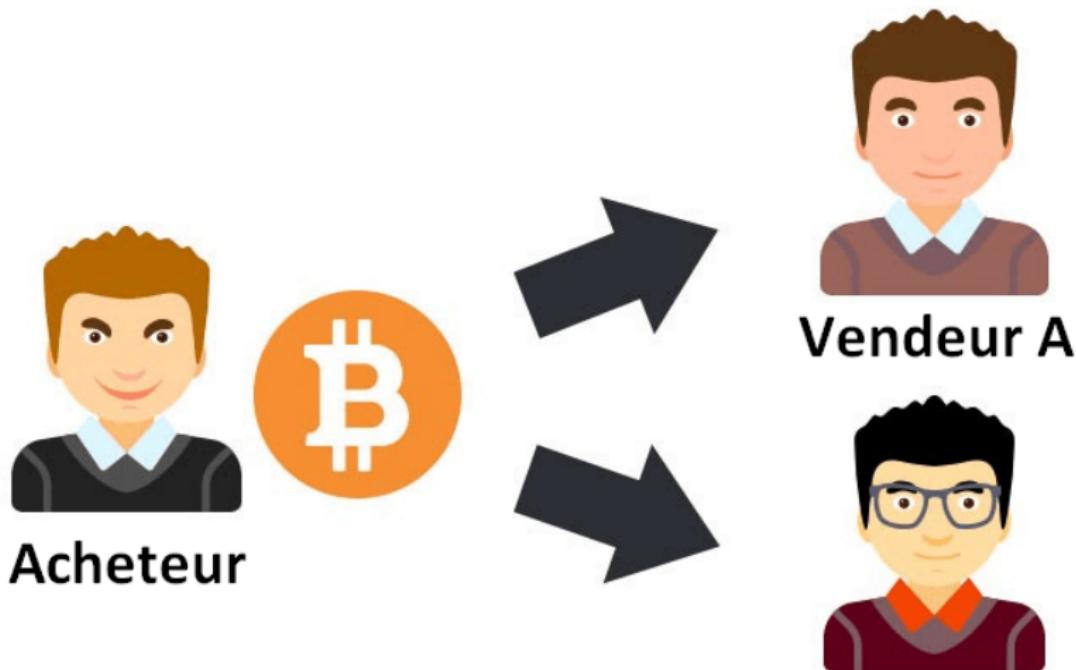
Ethernet - 1974



1979

Les obstacles

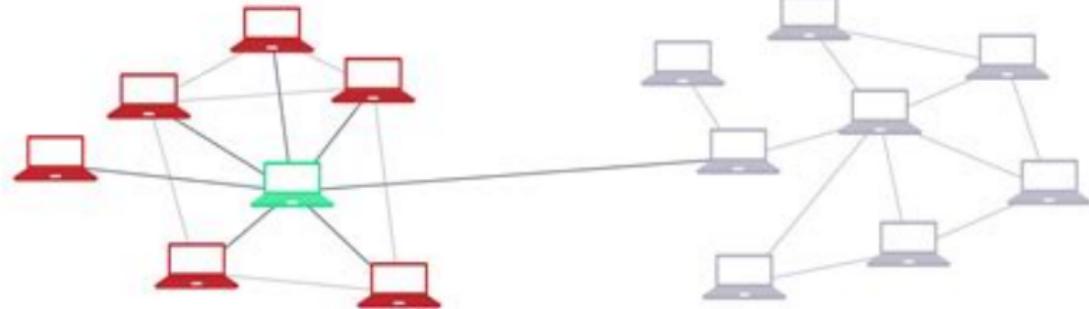
La double dépense



Les obstacles

La double dépense

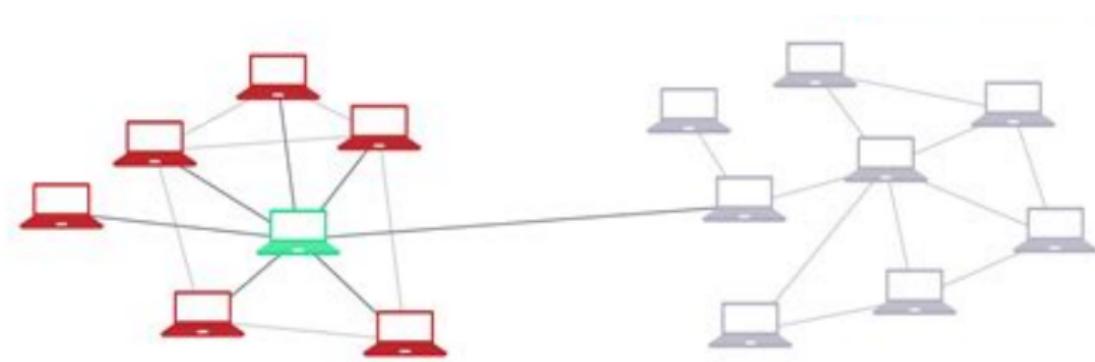
L'attaque de Sybil



Les obstacles

La double dépense

L'attaque de Sybil



L'attaque de Goldfinger (ou attaque des 51%)

Comment le problème est-il résolu ?

Bitcoin-core : une 1^{er} solution

From Satoshi Nakamoto <satoshi<at>vistomail.com>

Subject : Bitcoin P2P e-cashe paper

Newsgroups : gmane.comp.encryption.general

Date : Friday 31st October 2008 18 :10 :00 UTC

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

Comment le problème est-il résolu ?

Bitcoin-core : une 1^{er} solution

Un journal comptable d'enregistrements, organisés en blocks infalsifiables qui s'enchainent de façon unique les uns aux autres dans un réseau public et décentralisé.

Comment le problème est-il résolu ?

Bitcoin-core : une 1^{er} solution

Les 4 rôles des blockchain* (Chaum)



- ▶ Utilisateur (noeud simple)
- ▶ Participant (noeud validateur / mineur)
- ▶ Décideur (gagnant du bon nonce dans POW)
- ▶ Empereur (bitcoin core developpers)

Comment le problème est-il résolu ?

Bitcoin-core : une 1^{er} solution

Les 4 rôles des blockchain* (Chaum)



- ▶ Utilisateur (noeud simple)
- ▶ Participant (noeud validateur / mineur)
- ▶ Décideur (gagnant du bon nonce dans POW)
- ▶ Empereur (bitcoin core developpers)

Comment le problème est-il résolu ?

Bitcoin-core : une 1^{er} solution

Les 4 rôles des blockchain* (Chaum)



- ▶ Utilisateur (noeud simple)
- ▶ Participant (noeud validateur / mineur)
- ▶ Décideur (gagnant du bon nonce dans POW)
- ▶ Empereur (bitcoin core developpers)

Comment le problème est-il résolu ?

Bitcoin-core : une 1^{er} solution

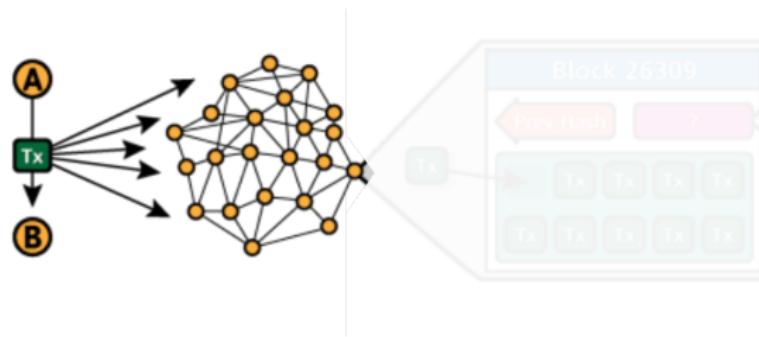
Les 4 rôles des blockchain* (Chaum)



- ▶ Utilisateur (noeud simple)
- ▶ Participant (noeud validateur / mineur)
- ▶ Décideur (gagnant du bon nonce dans POW)
- ▶ Empereur (bitcoin core developpers)

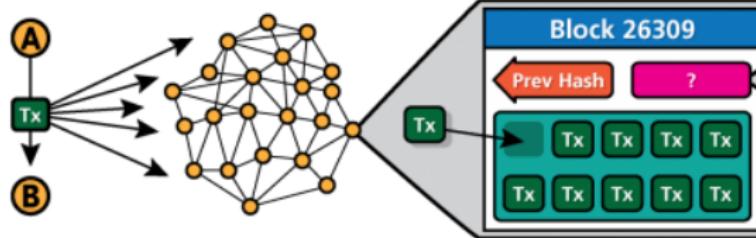
Pour faire une transaction

1. une transaction : .0000231 BTC pour Halima, signé Koffi
2. Les mineurs l'inclue dans un bloc et cherchent le *nonce* validateur
3. Le 1^{er} mineur à trouver le *nonce* publie le block
 - ▶ ce dernier contient une auto (avec une auto-récompense)
4. Les autres mineurs :
 - ▶ abandonne leur quête
 - ▶ ajoute le nouveau block à la chaîne
 - ▶ Recommence une nouvelle quête



Pour faire une transaction

1. une transaction : .0000231 BTC pour Halima, signé Koffi
2. Les mineurs l'inclue dans un bloc et cherchent le *nonce* validateur
3. Le 1^{er} mineur à trouver le *nonce* publie le block
 - ▶ ce dernier contient une auto (avec une auto-récompense)
4. Les autres mineurs :
 - ▶ abandonne leur quête
 - ▶ ajoute le nouveau block à la chaîne
 - ▶ Recommence une nouvelle quête



Pour faire une transaction

1. une transaction : .0000231 BTC pour Halima, signé Koffi
2. Les mineurs l'inclue dans un bloc et cherchent le *nonce* validateur
3. Le 1^{er} mineur à trouver le *nonce* publie le block
 - ▶ ce dernier contient une auto (avec une auto-récompense)
4. Les autres mineurs :
 - ▶ abondonne leur quête
 - ▶ ajoute le nouveau block à la chaîne
 - ▶ Recommence une nouvelle quête

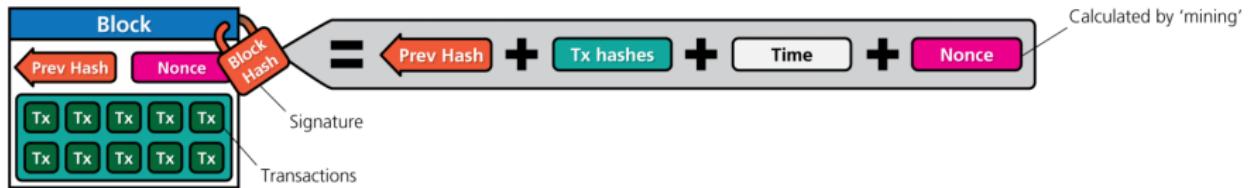


Illustration by CryptoGraphics.info

Pour faire une transaction

1. une transaction : .0000231 BTC pour Halima, signé Koffi
2. Les mineurs l'inclue dans un bloc et cherchent le *nonce* validateur
3. Le 1^{er} mineur à trouver le *nonce* publie le block
 - ▶ ce dernier contient une auto (avec une auto-récompense)
4. Les autres mineurs :
 - ▶ abandonne leur quête
 - ▶ ajoute le nouveau block à la chaîne
 - ▶ Recommence une nouvelle quête

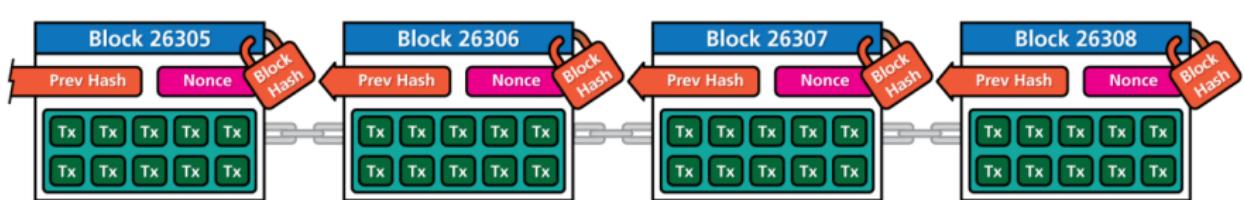


Illustration by CryptoGraphics.info

A quand son garba payé avec son téléphone ?

Pizza for bitcoins ? Le 18 mai 2010, laslo sur bitcointalk.org



Les limites de la blockchain bitcoin

- ▶ Vitesse de traitement des transactions
- ▶ Politique : forks
- ▶ jeux d'instructions limités
- ▶ Coût énergétique
- ▶ Concentration des pouvoirs (hashrate)

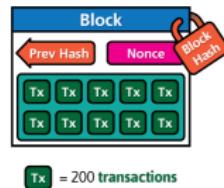
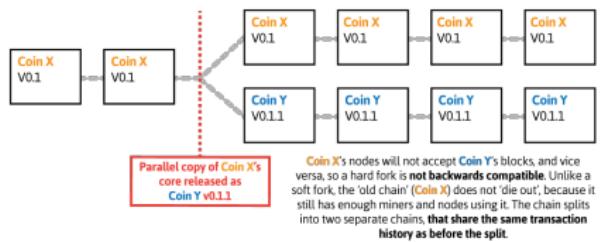


Illustration by Cryptogaphica.info

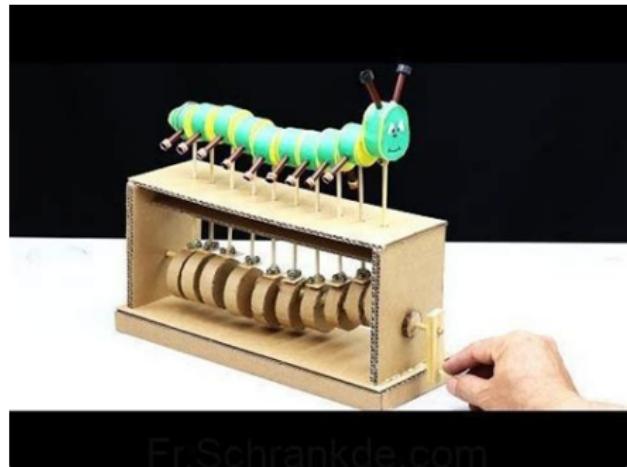
Les limites de la blockchain bitcoin

- ▶ Vitesse de traitement des transactions
- ▶ Politique : forks
- ▶ jeux d'instructions limités
- ▶ Coût énergétique
- ▶ Concentration des pouvoirs (hashrate)

Illustration by Cryptographica.info

Les limites de la blockchain bitcoin

- ▶ Vitesse de traitement des transactions
- ▶ Politique : forks
- ▶ jeux d'instructions limités
- ▶ Coût énergétique
- ▶ Concentration des pouvoirs (hashrate)



Fr.Schrankde.com

Les limites de la blockchain bitcoin

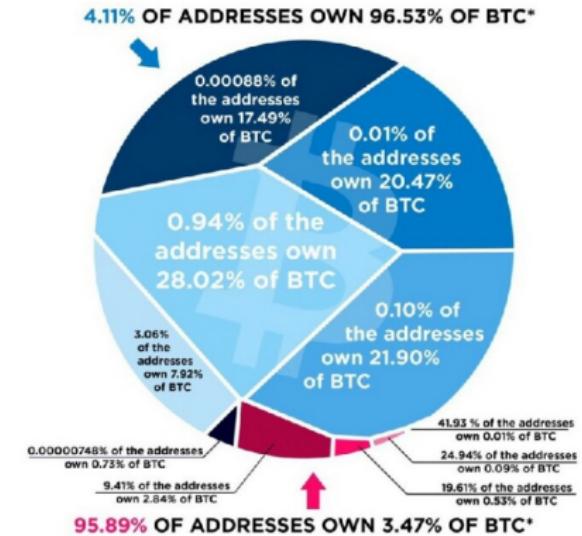
- ▶ Vitesse de traitement des transactions
- ▶ Politique : forks
- ▶ jeux d'instructions limités
- ▶ **Coût énergétique**
- ▶ Concentration des pouvoirs (hashrate)



Les limites de la blockchain bitcoin

- ▶ Vitesse de traitement des transactions
- ▶ Politique : forks
- ▶ jeux d'instructions limités
- ▶ Coût énergétique
- ▶ Concentration des pouvoirs (hashrate)

The Bitcoin Wealth Distribution



* Data as of September 12th, 2017

Article and Sources:

<https://howmuch.net/articles/Bitcoin-wealth-distribution>

<https://bitcoincapital.net/>

Blockchain de 2^e génération : Etherum

Etherum



- ▶ Système comptable classique
- ▶ Turing complet
- ▶ dApps et smart-contrats (solidity)
- ▶ ETH et gaz

Blockchain de 2^e génération : Etherum

Etherum



- ▶ Système comptable classique
- ▶ Turing complet
- ▶ dApps et smart-contrats (solidity)
- ▶ ETH et gaz

Blockchain de 2^e génération : Etherum

Etherum



- ▶ Système comptable classique
- ▶ Turing complet
- ▶ dApps et smart-contrats (solidity)
- ▶ ETH et gaz

Blockchain de 2^e génération : Etherum

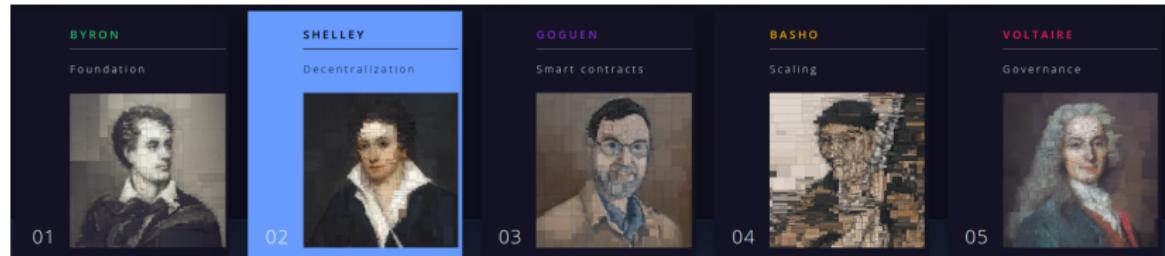
Etherum



- ▶ Système comptable classique
- ▶ Turing complet
- ▶ dApps et smart-contrats (solidity)
- ▶ ETH et gaz

Originalité du projet

1^{er} déploiement scientifique d'une blockchain



Fonctionnement

- ▶ Utilisateurs (*vous et moi*)
 - ▶ Utilisation des ADA
 - ▶ Smart-contract
- ▶ Participants (*vous et moi*)
 - ▶ Délégation dans des pools (*staking*)
 - ▶ Système Décentralisé, rapide et efficient
- ▶ Décideurs (*vous et moi*)
 - ▶ Consensus par preuve d'engagement, Proof of stake (Ouroboros)
- ▶ Empereurs (*nous*) :
 - ▶ Votes & Trésor



Fonctionnement

- ▶ Utilisateurs (*vous et moi*)
 - ▶ Utilisation des ADA
 - ▶ Smart-contract
- ▶ Participants (*vous et moi*)
 - ▶ Délégation dans des pools (*staking*)
 - ▶ Système Décentralisé, rapide et efficient
- ▶ Décideurs (*vous et moi*)
 - ▶ Consensus par preuve d'engagement, Proof of stake (*Ouroboros*)
- ▶ Empereurs (*nous*) :
 - ▶ Votes & Trésor



Fonctionnement

- ▶ Utilisateurs (*vous et moi*)
 - ▶ Utilisation des ADA
 - ▶ Smart-contract
- ▶ Participants (*vous et moi*)
 - ▶ Délégation dans des pools (*staking*)
 - ▶ Système Décentralisé, rapide et efficient
- ▶ Décideurs (*vous et moi*)
 - ▶ Consencus par preuve d'engagement, Proof of stake (*Ouroboros*)
- ▶ Empereurs (*nous*) :
 - ▶ Votes & Trésor



Fonctionnement

- ▶ Utilisateurs (*vous et moi*)
 - ▶ Utilisation des ADA
 - ▶ Smart-contract
- ▶ Participants (*vous et moi*)
 - ▶ Délégation dans des pools (*staking*)
 - ▶ Système Décentralisé, rapide et efficient
- ▶ Décideurs (*vous et moi*)
 - ▶ Consencus par preuve d'engagement, Proof of stake (*Ouroboros*)
- ▶ Empereurs (*nous*) :
 - ▶ Votes & Trésor



Exemple d'applications

Token-économique

Qu'est ce que la monnaie

- ▶ à l'origine
- ▶ aujourd'hui

Les Tokens

- ▶ Utilitaires ou d'applications
- ▶ de protocole
- ▶ Stable coins
- ▶ NTFs

Commencer avec Cardano

Ouvrir un porte-feuille électronique

par exemple <https://yoroi-wallet.com>

- ▶ noter les mots de sauvegarde
- ▶ partager votre adresse publique
- ▶ Recevez des ADA ou lovelace
- ▶ Déléguer à une pool POA ou STKH

