

Proof of Africa



CARDANO

Blockchain de 3ème génération

Samedi 5 juin 2021



Outline

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

Définitions

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus
- ▶ Cryptographie
- ▶ Applications distribuées (dApp)

Token-économie

- ▶ Tokens ou jetons
- ▶ Portefeuilles électroniques (Yoroi-wallet)
- ▶ Marché de crypto-monnaies

Définitions

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus
- ▶ Cryptographie
- ▶ Applications distribuées (dApp)

Token-économie

- ▶ Tokens ou jetons
- ▶ Portefeuilles électroniques (Yoroi-wallet)
- ▶ Marché de crypto-monnaies

Définitions

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus
- ▶ Cryptographie
- ▶ Applications distribuées (dApp)

Token-économie

- ▶ Tokens ou jetons
- ▶ Portefeuilles électroniques (Yoroi-wallet)
- ▶ Marché de crypto-monnaies

Définitions

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus
- ▶ Cryptographie
- ▶ Applications distribuées (dApp)

Token-économie

- ▶ Tokens ou jetons
- ▶ Portefeuilles électroniques (Yoroi-wallet)
- ▶ Marché de crypto-monnaies

Définitions

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus
- ▶ Cryptographie
- ▶ Applications distribuées (dApp)

Token-économie

- ▶ Tokens ou jetons
- ▶ Portefeuilles électroniques (Yoroi-wallet)
- ▶ Marché de crypto-monnaies

Définitions

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus
- ▶ Cryptographie
- ▶ Applications distribuées (dApp)

Token-économie

- ▶ Tokens ou jetons
- ▶ Portefeuilles électroniques ([Yoroi-wallet](#))
- ▶ Marché de crypto-monnaies

Définitions

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus
- ▶ Cryptographie
- ▶ Applications distribuées (dApp)

Token-économie

- ▶ Tokens ou jetons
- ▶ Portefeuilles électroniques ([Yoroi-wallet](#))
- ▶ Marché de crypto-monnaies

Pourquoi des Blockchain ?

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

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

Comment créer *l'argent de l'Internet* (une espèce digitale) ?

HTTP - 1990



1995

TCP/IP - 1974



1984

Ethernet - 1974



1979

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

Comment créer *l'argent de l'Internet* (une espèce digitale) ?

SSL/TLS - 1996



HTTP - 1990



TCP/IP - 1974



Ethernet - 1974



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

Comment créer *l'argent de l'Internet* (une espèce digitale) ?



2009

???

SSL/TLS - 1996



HTTP - 1990



TCP/IP - 1974



1984

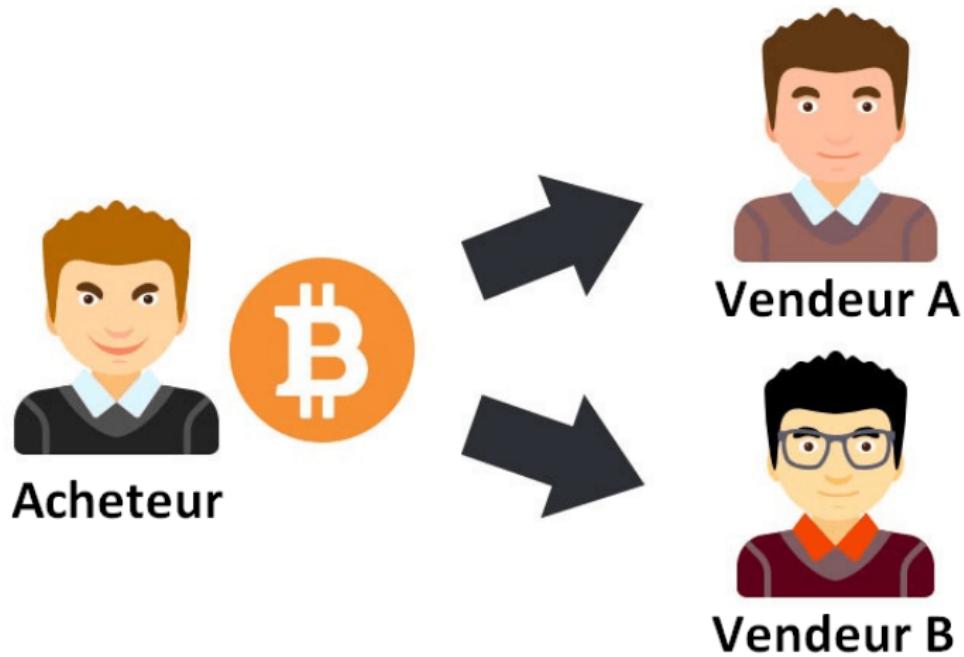
Ethernet - 1974



1979

Les obstacles

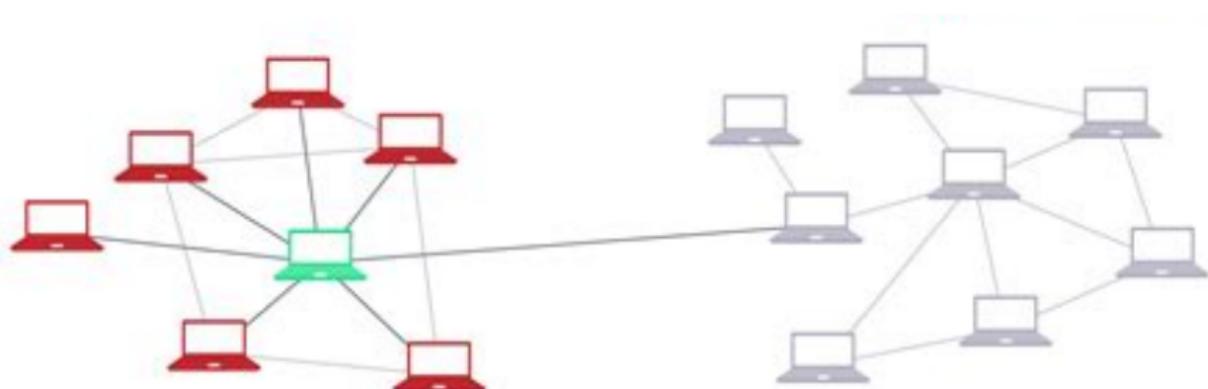
La double dépense



Les obstacles

La double dépense

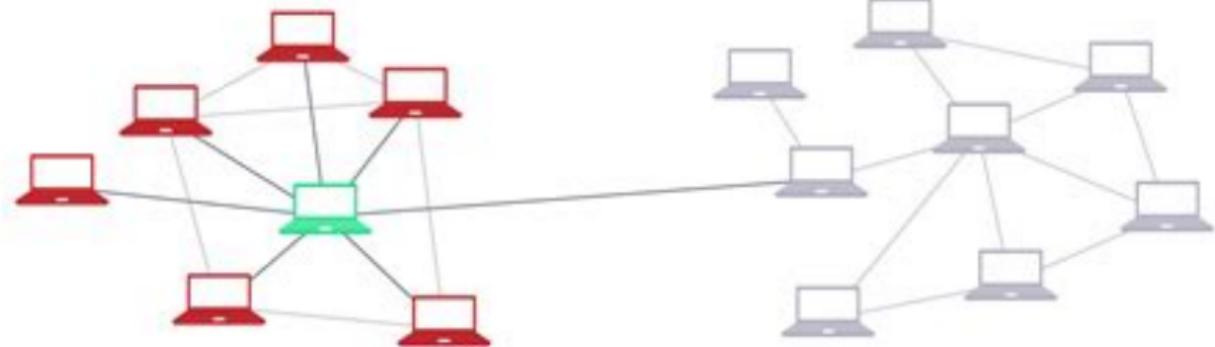
L'attaque de Sybil



Les obstacles

La double dépense

L'attaque de Sybil



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

Comment le problème est-il résolu ?

Blockchain du Bitcoin : jour J

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

Subject : Bitcoin P2P e-cashe paper

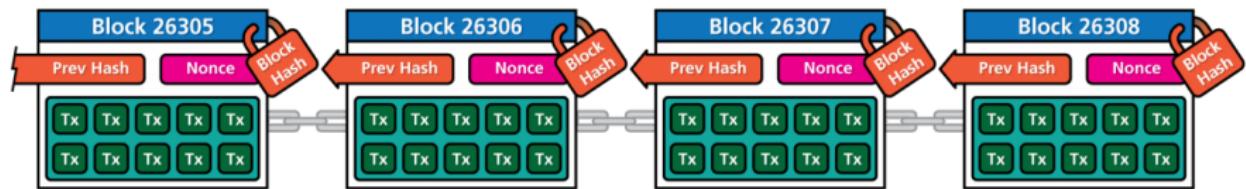
Newsgroups : gmane.comp.encryption.general

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 ?

Blockchain du Bitcoin : C'est quoi ?



Comment le problème est-il résolu ?

Blockchain du Bitcoin : C'est quoi ?

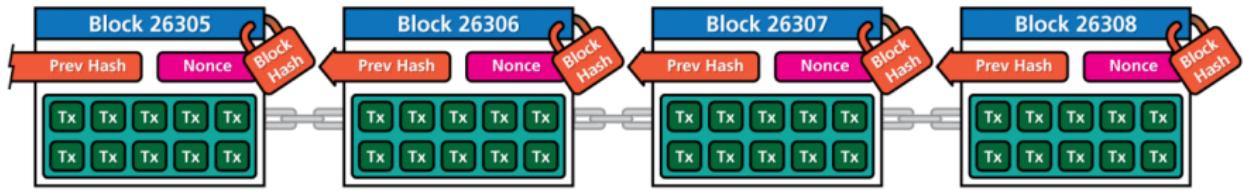


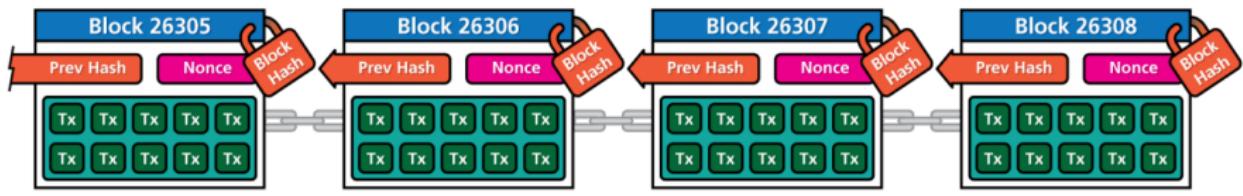
Illustration by CryptoGraphics.info

Un journal comptable d'enregistrements,

- ▶ organisés en blocks infalsifiables
- ▶ qui s'enchainent les uns aux autres,
- ▶ de façon unique,
- ▶ dans un réseau public et décentralisé.

Comment le problème est-il résolu ?

Blockchain du Bitcoin : C'est quoi ?



Un journal comptable d'enregistrements,

- ▶ organisés en blocks infalsifiables
- ▶ qui s'enchainent les uns aux autres,
- ▶ de façon unique,
- ▶ dans un réseau public et décentralisé.

Comment le problème est-il résolu ?

Blockchain du Bitcoin : C'est quoi ?

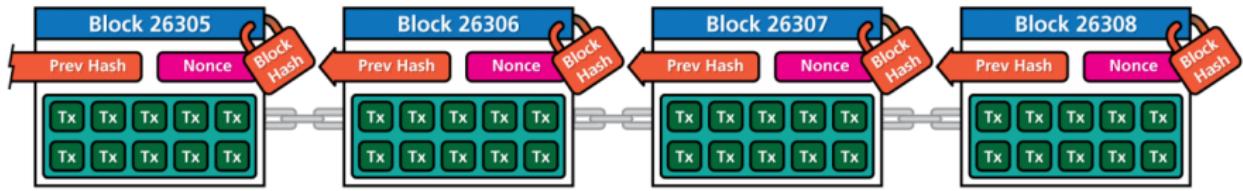


Illustration by CryptoGraphics.info

Un journal comptable d'enregistrements,

- ▶ organisés en blocks infalsifiables
- ▶ qui s'enchainent les uns aux autres,
- ▶ de façon unique,
- ▶ dans un réseau public et décentralisé.

Comment le problème est-il résolu ?

Blockchain du Bitcoin : C'est quoi ?

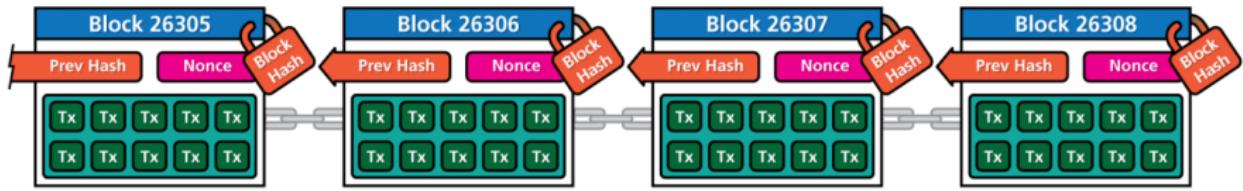


Illustration by CryptoGraphics.info

Un journal comptable d'enregistrements,

- ▶ organisés en blocks infalsifiables
- ▶ qui s'enchainent les uns aux autres,
- ▶ de façon unique,
- ▶ dans un réseau public et décentralisé.

Comment le problème est-il résolu ?

Blockchain du Bitcoin : C'est quoi ?

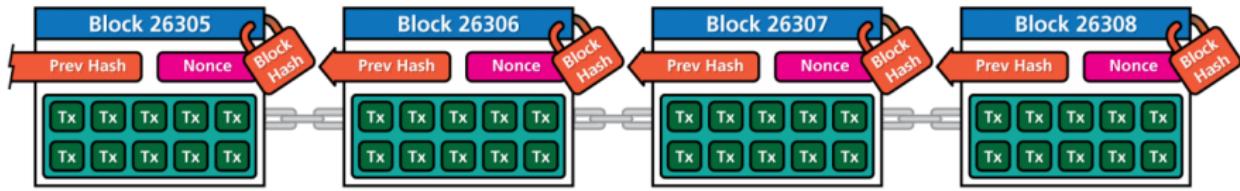


Illustration by CryptoGraphics.info

Un journal comptable d'enregistrements,

- ▶ organisés en blocks infalsifiables
- ▶ qui s'enchainent les uns aux autres,
- ▶ de façon unique,
- ▶ dans un réseau public et décentralisé.

Comment le problème est-il résolu ?

Block 0

General info		Technical details									
	-		-								
Hash	000000000019d6689c085e165831e934f763ae46a2a6c172b3f1b60a8ce26f	Difficulty	1								
Mined on	2009-01-03 18:15 (12 years ago)	Miner	Unknown								
Coinbase data		Size	285								
Transaction count	1	Fee per kB	0.00000000 BTC								
Witness tx count	0	Fee per kWU	0.00000000 BTC								
Input count	1	Output count	1								
Input total	0.00000000 BTC	Output total	50.00000000 BTC								
Fee total	0.00000000 BTC	Coindays destroyed	0.00								
Generation	50.00000000 BTC	Reward	50.00000000 BTC								
Click to see more ↴											
Transactions included in this block											
Block #	T	Hash	Inputs #	Outputs #	Coindays destroyed	Output (BTC)	Output (USD)	Transaction fee (BTC)	Transaction fee (USD)	Fee/kB (BTC)	Size (kB)
0			1	1	0.00	50.00000000	0.50	0.00000000	0.00	0.00000000	0.204

Le block 123 456

Comment le problème est-il résolu ?

4 rôles



- ▶ Utilisateurs (noeud simple)
- ▶ Acteurs (noeud validateur / mineur)
- ▶ Décideurs (le 1^{er} à avoir un nonce dans POW)
- ▶ Empereurs (MIT bitcoin-core développeurs et d'autres...)

Comment le problème est-il résolu ?



4 rôles

- ▶ Utilisateurs (noeud simple)
- ▶ Acteurs (noeud validateur / mineur)
- ▶ Décideurs (le 1^{er} à avoir un nonce dans POW)
- ▶ Empereurs (MIT bitcoin-core développeurs et d'autres...)

Comment le problème est-il résolu ?

4 rôles



- ▶ Utilisateurs (noeud simple)
- ▶ Acteurs (noeud validateur / mineur)
- ▶ Décideurs (le 1^{er} à avoir un nonce dans POW)
- ▶ Empereurs (MIT bitcoin-core développeurs et d'autres...)

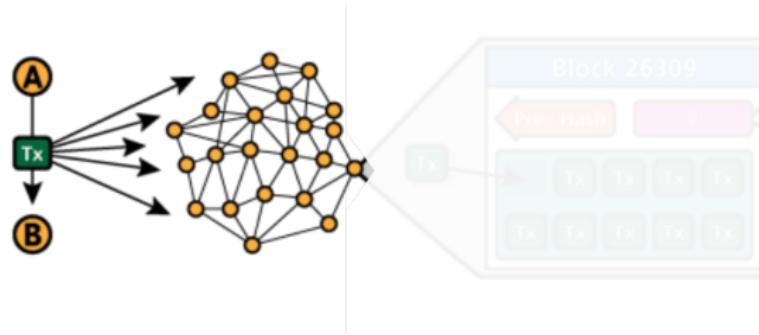
Comment le problème est-il résolu ?

4 rôles



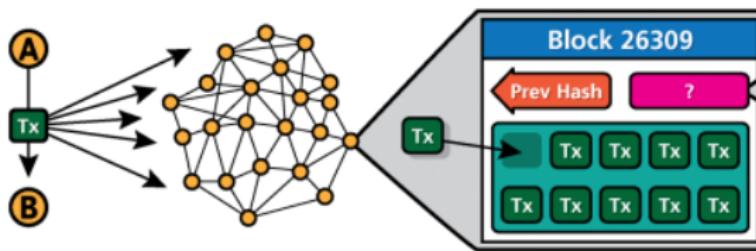
- ▶ Utilisateurs (noeud simple)
- ▶ Acteurs (noeud validateur / mineur)
- ▶ Décideurs (le 1^{er} à avoir un nonce dans POW)
- ▶ Empereurs ([MIT bitcoin-core developpeurs](#) et d'autres...)

Pour faire une transaction



Tx : ".0000231 BTC pour Binta, signé Amadou"

Pour faire une transaction



Les mineurs incluent la tx dans un bloc et cherchent un **bon nonce**

Pour faire une transaction

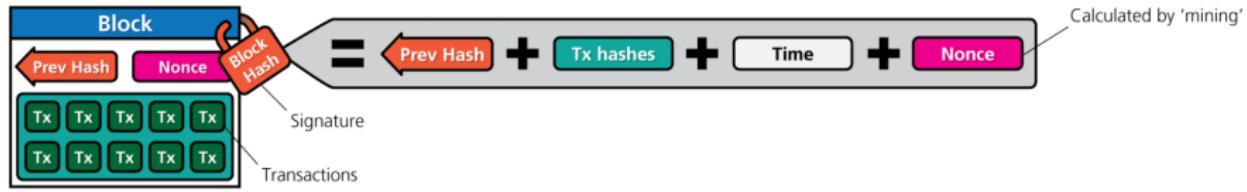
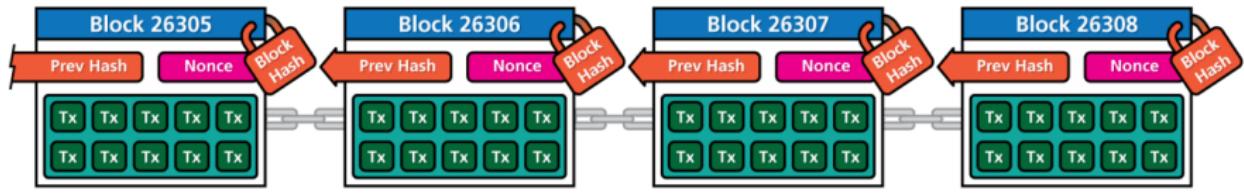


Illustration by CryptoGraphics.info

Le 1^{er} mineur à trouver un **bon nonce** valide et publie le bloc

- il contient une récompense (*coinbase*)

Pour faire une transaction



Les autres mineurs :

- ▶ abandonnent leur quête
- ▶ ajoutent le nouveau block à la chaîne
- ▶ recommencent la course pour valider un nouveau bloc de transactions

A quand son garba payé avec son téléphone ?

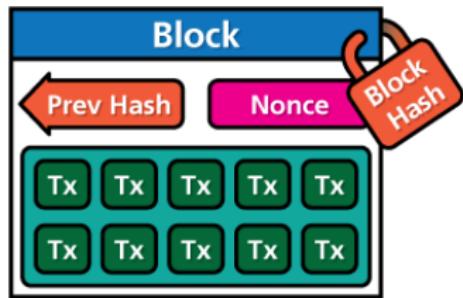
Pizza for bitcoins ? Le 18 mai 2010, laslo sur bitcointalk.org



Le Bitcoin l'unité de compte d'un journal comptable ouvert infalsifiable

Limites de la Blockchain bitcoin 1/5

Vitesse de traitement des transactions



Tx = 200 transactions

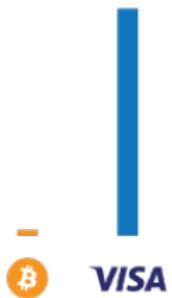
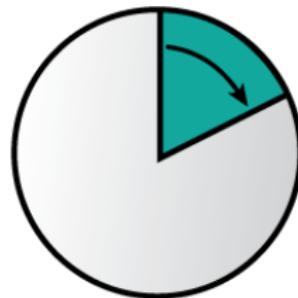
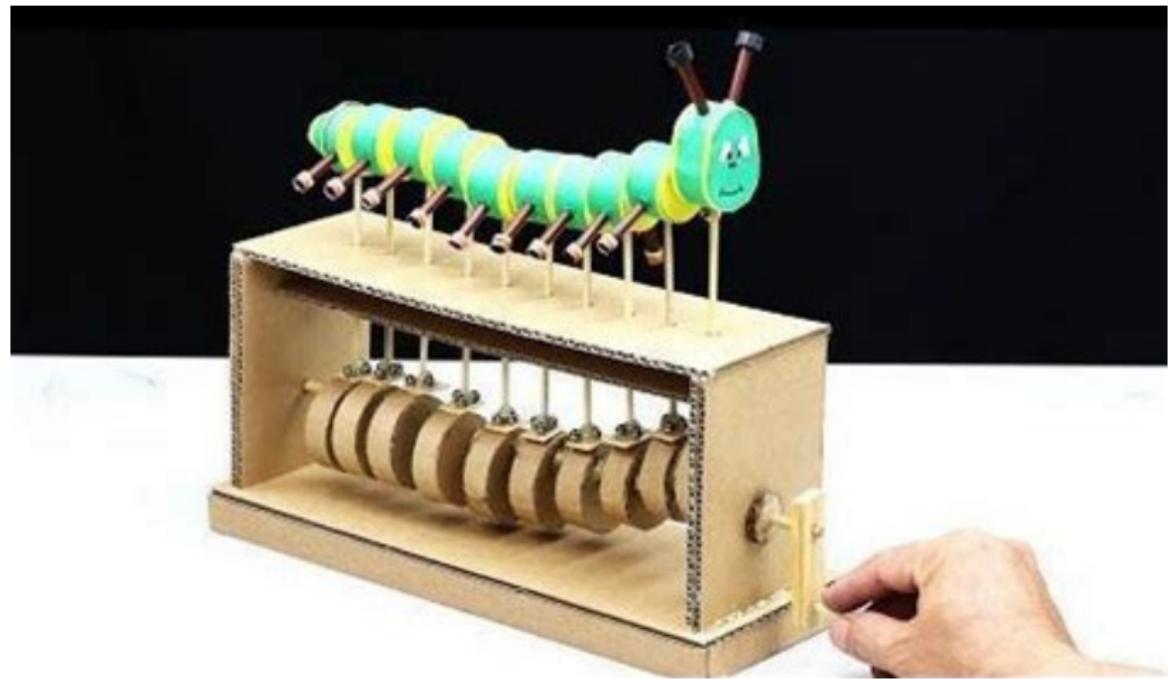


Illustration by CryptoGraphics.info

Limites de la Blockchain bitcoin 2/5

Jeux d'instructions limités



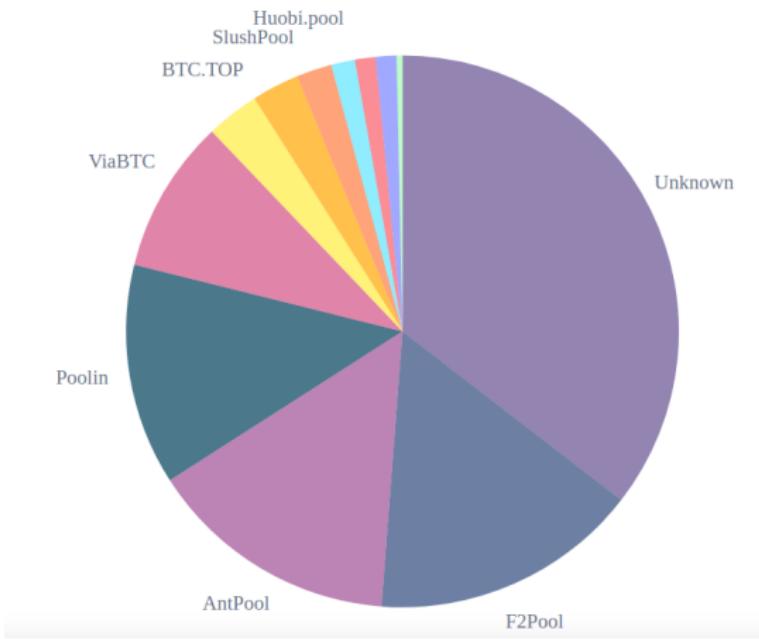
Limites de la blockchain bitcoin 3/5

Coût énergétique



Limites de la blockchain bitcoin 4/5

Concentration du hashrate (juin 2021)



Limites de la blockchain Bitcoin 5/5

Politique : forks

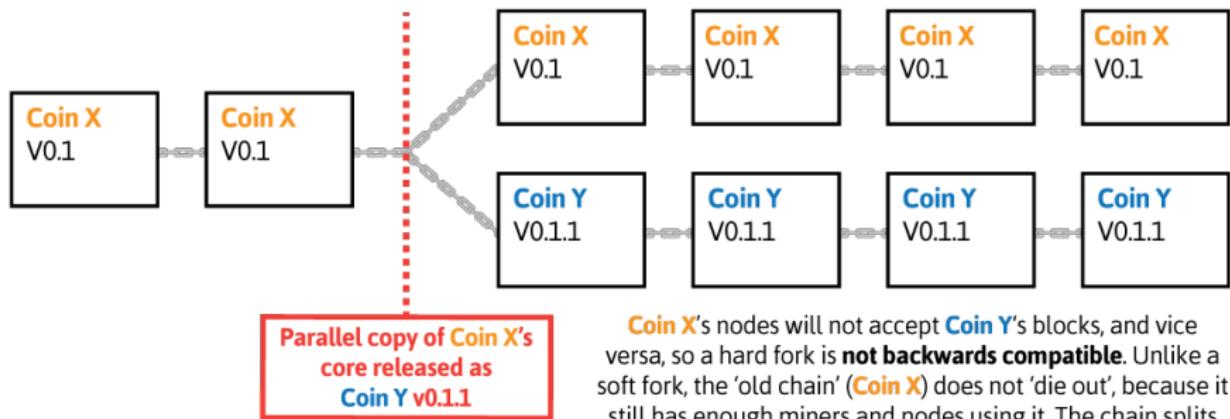


Illustration by CryptoGraphics.info

Blockchain de 2^e génération : Etherum

Un système d'exploitation décentralisé

Blockchain de 2^e génération : Ethereum



- ▶ Système comptable classique
- ▶ Machine Turing complet

Blockchain de 2^e génération : Etherum

```
function send(address _to, uint256 _value) {  
    if (balances[msg.sender] >= _value) {  
        balances[msg.sender] -= _value;  
        balances[_to] += _value;  
    }  
}
```

- ▶ dApps et smart-contracts (solidity)
- ▶ ETH et gaz

Blockchain de 2^e génération : Etherum

Etherum

- ▶ Pas assez sécurisé
- ▶ Coûteux
- ▶ Difficile à améliorer

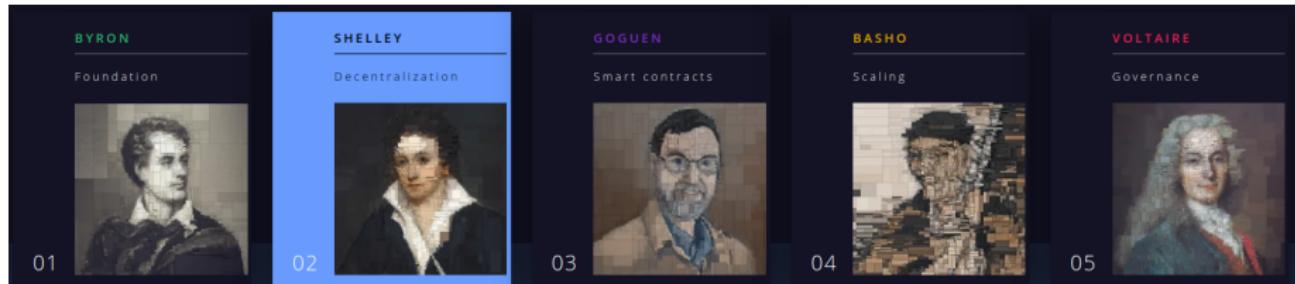


Cardano : blockchain de 3^e génération

1, 2, et ... 3 !

Originalité du projet

1^{er} déploiement scientifique d'une blockchain



Le Fonctionnement de Cardano

- ▶ Utilisateurs
 - ▶ Achat, vente, stockage et échange d'ADA
 - ▶ dApps et *smart-contracts* sécurisés
- ▶ Acteurs
 - ▶ délégation (*staking*), pools,
 - ▶ décentralisation, efficience
- ▶ Décideurs
 - ▶ Ouroboros, consensus par preuve d'engagement (POS ou *Proof of stake*)
- ▶ Empereurs
 - ▶ Votes & Trésor



Le Fonctionnement de Cardano

▶ Utilisateurs

- ▶ Achat, vente, stockage et échange d'ADA
- ▶ dApps et *smart-contracts* sécurisés

▶ Acteurs

- ▶ délégation (*staking*), pools,
- ▶ décentralisation, efficience

▶ Décideurs

- ▶ Ouroboros, consensus par preuve d'engagement (POS ou *Proof of stake*)

▶ Empereurs

- ▶ Votes & Trésor

```
-- | Checks if a date is before the given end date.
beforeEnd :: Date -> EndDate -> Bool
beforeEnd (Date d) (Fixed e) = d <= e
beforeEnd (Date _) Never      = True

-- | Check that the date in the redeemer is before the limit in the datum.
validateDate :: Data -> Data -> Data -> ()
-- The 'check' function takes a 'Bool' and fails if it is False.
-- This is handy since it's more natural to talk about booleans.
validateDate datum redeemer _ = check $ case (fromData datum, fromData redeemer) of
  -- We can decode both the arguments at the same time: 'Just' means that
  -- decoding succeeded.
  (Just endDate, Just date) -> beforeEnd date endDate
  -- One or the other failed to decode.
  _                                -> False
```



Le Fonctionnement de Cardano

- ▶ Utilisateurs
 - ▶ Achat, vente, stockage et échange d'ADA
 - ▶ dApps et *smart-contracts* sécurisés
- ▶ Acteurs
 - ▶ délégation (*staking*), *pools*,
 - ▶ décentralisation, efficience
- ▶ Décideurs
 - ▶ Ouroboros, consensus par preuve d'engagement (POS ou *Proof of stake*)
- ▶ Empereurs
 - ▶ Votes & Trésor



Le Fonctionnement de Cardano

- ▶ Utilisateurs
 - ▶ Achat, vente, stockage et échange d'ADA
 - ▶ dApps et *smart-contracts* sécurisés
- ▶ Acteurs
 - ▶ délégation (*staking*), *pools*,
 - ▶ décentralisation, efficience
- ▶ Décideurs
 - ▶ Ouroboros, consensus par preuve d'engagement (POS ou *Proof of stake*)
- ▶ Empereurs
 - ▶ Votes & Trésor



Le Fonctionnement de Cardano

- ▶ Utilisateurs
 - ▶ Achat, vente, stockage et échange d'ADA
 - ▶ dApps et *smart-contracts* sécurisés
- ▶ Acteurs
 - ▶ délégation (*staking*), *pools*,
 - ▶ décentralisation, efficience
- ▶ Décideurs
 - ▶ Ouroboros, consensus par preuve d'engagement (POS ou *Proof of stake*)
- ▶ Empereurs
 - ▶ Votes & Trésor



Applications

- ▶ Objets connectés
- ▶ Services financiers décentralisés (DeFI, Decentralised Finance)
- ▶ Accessibilité aux services financiers
- ▶ Paiement internationaux
- ▶ Financement participatif
- ▶ Création de marchés de pairs à pairs
- ▶ Dépôts de garanties
- ▶ Logistique
- ▶ Identité numérique
- ▶ Monnaie dirigée

Perspectives

Un révolution techno-sociale ?

Token-économique

Qu'est ce que la monnaie ?

- ▶ Classiquement

- ▶ Réserve de valeur
- ▶ Moyen de change
- ▶ Unité de compte

Tokens (jetons)

- ▶ Aujourd'hui

Marchés des crypto-monnaies

Une histoire de confiance (Aglietta & Orléan 1998)

Token-économique

Qu'est ce que la monnaie ?

- ▶ Classiquement
- ▶ Aujourd'hui

Tokens (jetons)

Une histoire de confiance
(Aglietta & Orléan 1998)

Marchés des crypto-monnaies

- ▶ L'habitude (méthodique)
- ▶ L'obligation (autorité)
- ▶ La confiance (éthique)

Token-économique

Qu'est ce que la monnaie ?

- ▶ Classiquement
- ▶ Aujourd'hui

Une histoire de confiance
(Aglietta & Orléan 1998)

Tokens (jetons)

- ▶ Protocole
- ▶ Utilitaires ou applicatifs
- ▶ Adossés à des commodités (*stable coins*)
- ▶ non *fongible* (NFT)

Marchés des crypto-monnaies

Token-économique

Qu'est ce que la monnaie ?

- ▶ Classiquement
- ▶ Aujourd'hui

Une histoire de confiance
(Aglietta & Orléan 1998)

Tokens (jetons)

Marchés des crypto-monnaies

- ▶ le marché du crédit : \$ 250 billions
- ▶ Le marché des actions : \$ 80 billions
- ▶ le marché de l'or : \$ 7 billions
- ▶ le marché des cryptos : \$ 1,5 billions

Comment avoir des ADA ?

C'est légal mais de plus en plus contrôlé.

avec des BTC

- ▶ Acheter des BTC Orange, MTN money, FCFA... .
- ▶ Plateformes d'échange pair à pair ex. [localbitcoins](#)
- ▶ Maisons de change

Directement

Restreint par la BCEAO

- ▶ Un vendeur, un donneur physique (ex. moi)
- ▶ Une CB d'une autre zone monétaire que FCFA
- ▶ Acheter en ligne sur des plateformes reconnues
 - ▶ [binance](#) (CH), [kraken](#) (A), [coinbase](#) (USA)
 - ▶ voir [coingecko](#) pour classement

Comment garder ses ADA ?

Yoroi (portefeuille léger)

Daedalus (noeud complet)



Comment garder ses ADA ?

Daedalus (noeud complet)



Yoroi (portefeuille léger)



Ouvrir un porte-feuille électronique

1. Installer yoroi-wallet pour android ou plugin de navigateur
2. Noter les mots de sauvegarde
3. Partager votre adresse publique
4. Recevez des ADA ou lovelace

Délégation et stacking

Gagner +5 à 7% d'ADA en minant

Déléguer une pool c'est regroupements d'individus qui valident ensemble des transactions contre rémunération

POA

STKH1

Proof of Africa



Afrikpool

<https://cardano.afrikpool.org/>

Liens

Cardano

- ▶ Plan de déploiement Cardano
- ▶ Explorateur de bloc pour Cardano
- ▶ [Cardano-node \(github\)](#)

Délégation

- ▶ <https://adapools.org>
- ▶ formulaire :<https://forms.gle/vjaGwDx3oQLrToLo6>

Evènements Blockchains

- ▶ 15 juillet 2021 Concours de Hackaton blockchain ([encode.club](#))
- ▶ mars 2022 Conférence Blockchain en Afrique du Sud

Merci à tous

