

Proof of Africa



CARDANO

Blockchain de 3ème génération

Samedi 5 juin 2021



Plan

Introduction

Bitcoin : Blockchain de 1^{re} génération

Etherum : Blockchain de 2^e génération

Cardano : blockchain de 3^e génération

Token-economie

Conclusion

Les concepts de base

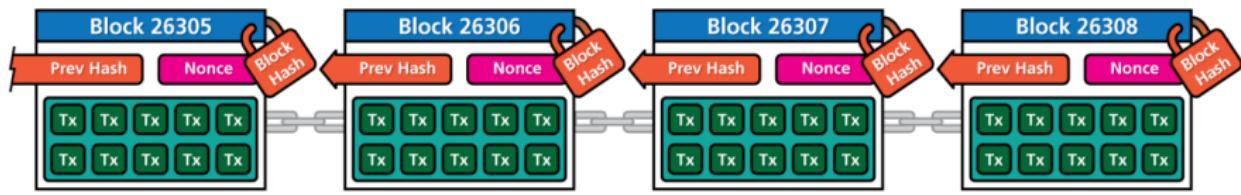


Illustration by CryptoGraphics.info

Blockchain

- ▶ Enregistrements décentralisés

Token-économie

Les concepts de base

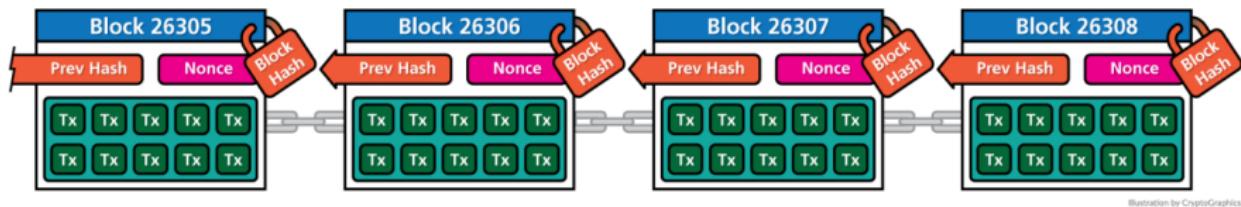


Illustration by CryptoGraphics.info

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus

Token-économie

Les concepts de base

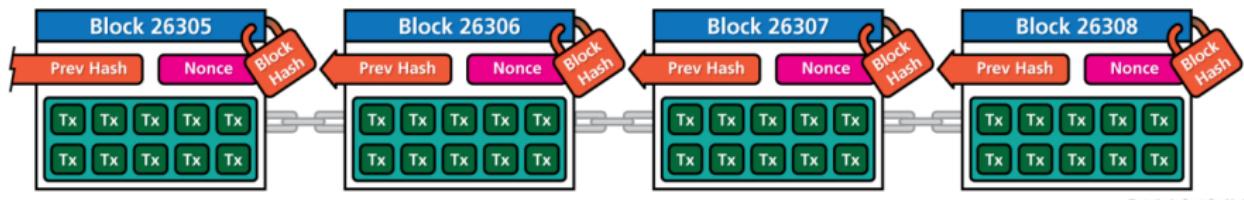


Illustration by CryptoGraphics.info

Blockchain

- ▶ Enregistrements décentralisés
- ▶ Algorithmes de consensus
- ▶ Cryptographie

Token-économie

Les concepts de base

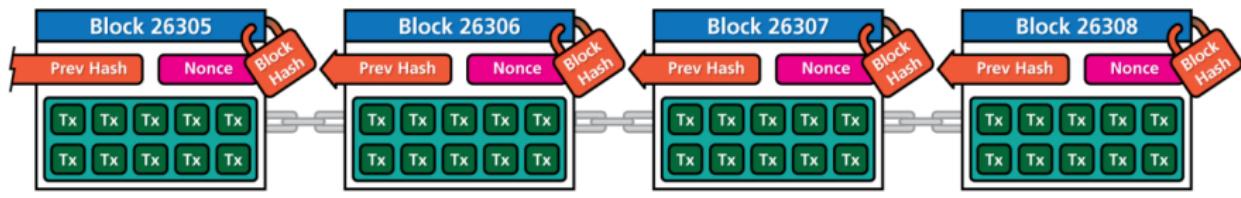


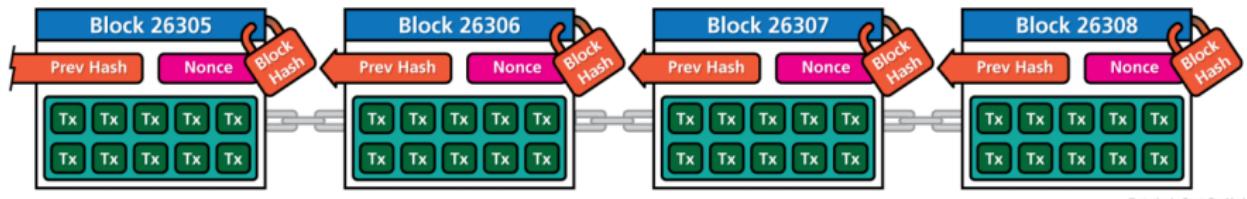
Illustration by CryptoGraphics.info

Blockchain

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

Token-économie

Les concepts de base



Blockchain

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

Token-économie

- ▶ Tokens ou jetons

Les concepts de base

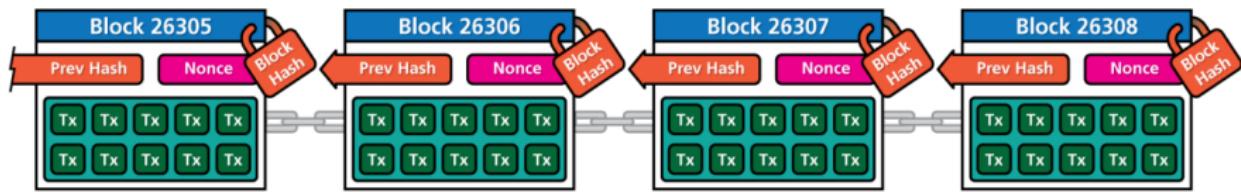


Illustration by CryptoGraphics.info

Blockchain

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

Token-économie

- ▶ Tokens ou jetons
- ▶ Marchés financiers

Les concepts de base

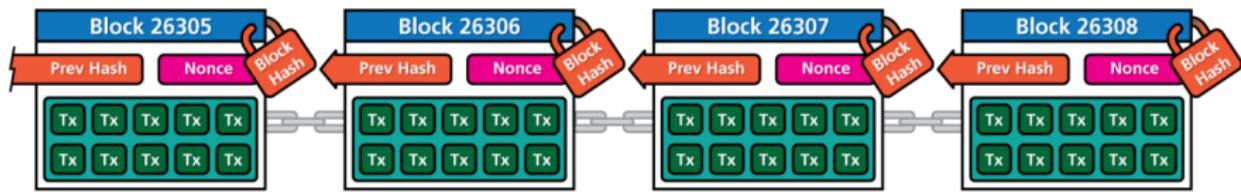


Illustration by CryptoGraphics.info

Blockchain

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

Token-économie

- ▶ Tokens ou jetons
- ▶ Marchés financiers
- ▶ Portefeuilles électroniques (Yoroi-wallet)

La blockchain du Bitcoin

Toute action engendre une réaction (3^e loi de Newton)

La Naissance du Bitcoin

Cyber-Anarchisme

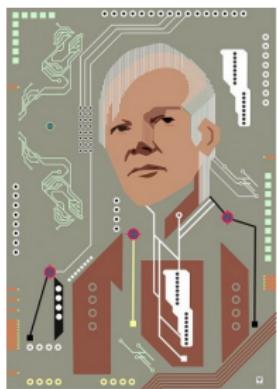
From : Satoshi Nakamoto satoshi@vistomail.com

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.



Quel problème résoud la 1^{re} blockchain ?

Connecter, échanger, librement

HTTP - 1990



1995

TCP/IP - 1974



1984

Ethernet - 1974



1979

Quel problème résoud la 1^{re} blockchain ?

Connecter, échanger, librement

SSL/TLS - 1996



HTTP - 1990



TCP/IP - 1974



Ethernet - 1974



Quel problème résoud la 1^{re} blockchain ?

Connecter, échanger, librement



2009

???

SSL/TLS - 1996



1998

HTTP - 1990



1995

TCP/IP - 1974



1984

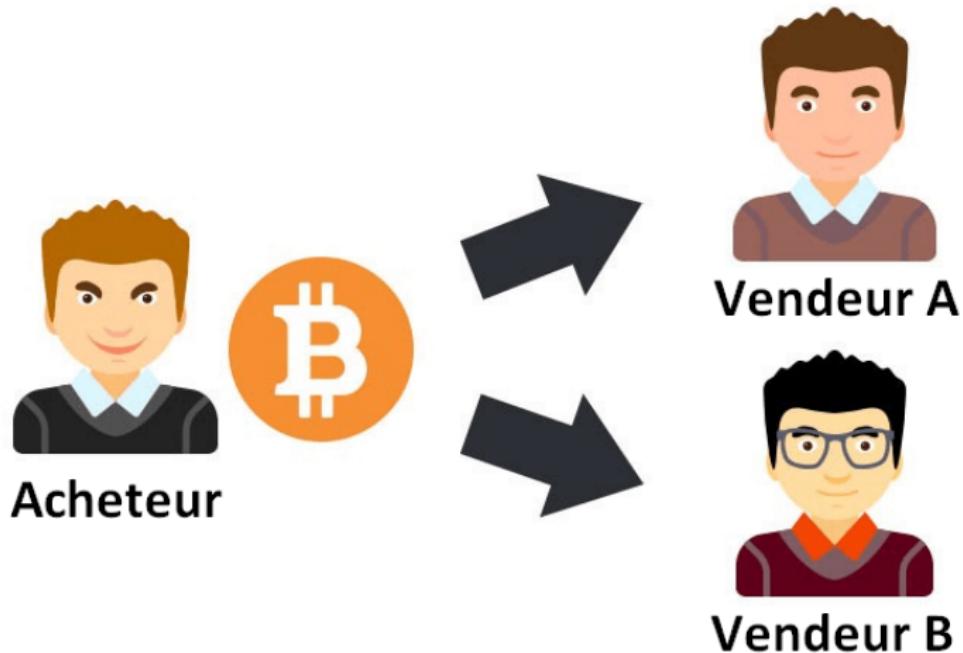
Ethernet - 1974



1979

Les obstacles

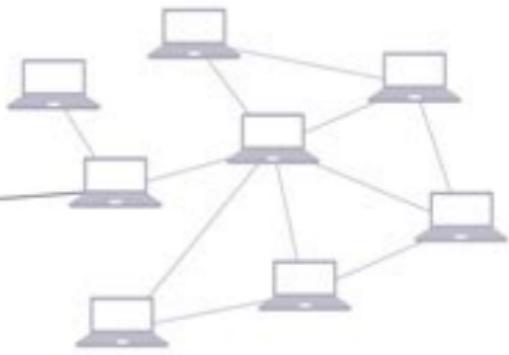
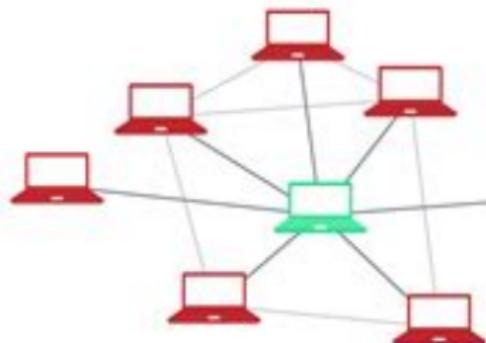
La double dépense



Les obstacles

La double dépense

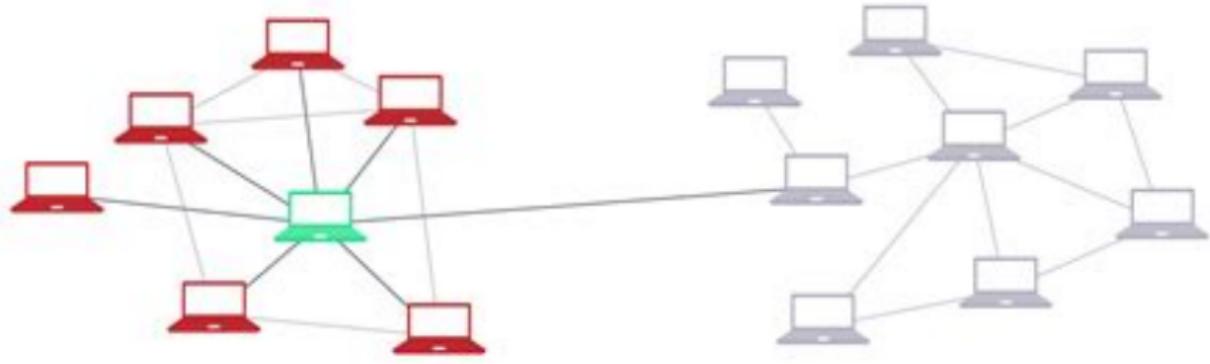
L'attaque de Sybil



Les obstacles

La double dépense

L'attaque de Sybil



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

Comment le problème est résolu ?

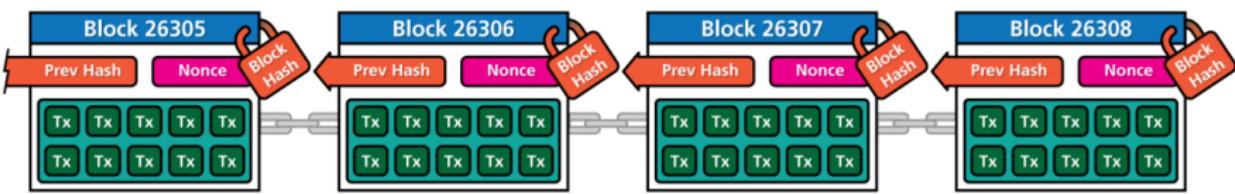


Illustration by CryptoGraphics.info

avec une blockchain

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 résolu ?

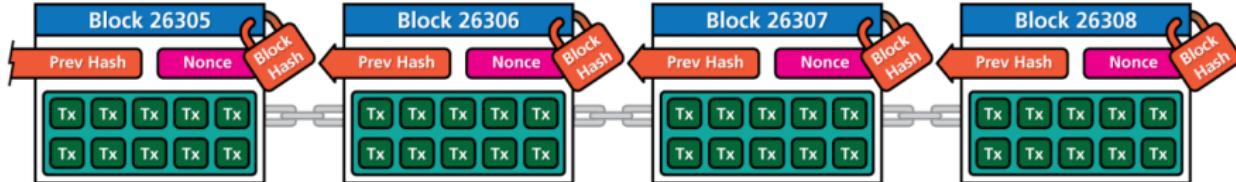


Illustration by CryptoGraphics.info

avec une blockchain

et des rôles (Chaum 92)

- ▶ Utilisateurs
- ▶ Acteurs (mineur)
- ▶ Décideurs
- ▶ Empereurs (MIT bitcoin-core developpeurs et d'autres...)

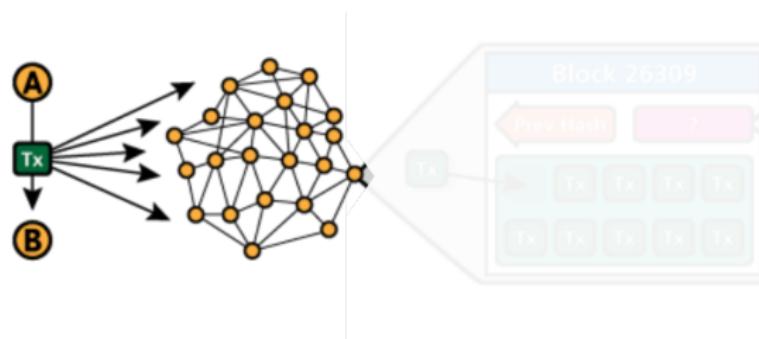
Comment le problème est-il résolu ?

Block 0

General info			Technical details		
	—		0	—	
Hash	000000000019d6689c085se165831e934ff763ae46a2a6c172b3f1b60a8ce26f				
Mined on	2009-01-03 18:15 (12 years ago)	Miner	Unknown		
Coinbase data	The Times 03/Jan/2009 Chancellor on brink of second bailout for				
Transaction count	1	Fee per kB	0.00000000 BTC	USD	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	Coidays destroyed	0.00		
Generation	50.00000000 BTC	Reward	50.00000000 BTC		
Transactions included in this block					
Block #	Hash	Inputs #	Outputs #	Coindays destroyed	Output (BTC)
0		1	1	0.00	50.00000000
				0.50	0.00000000
					0.204

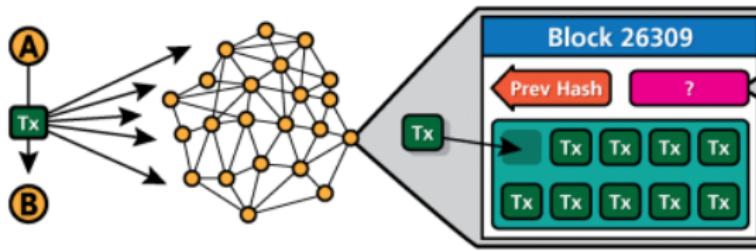
Le block 123 456

Pour faire une transaction



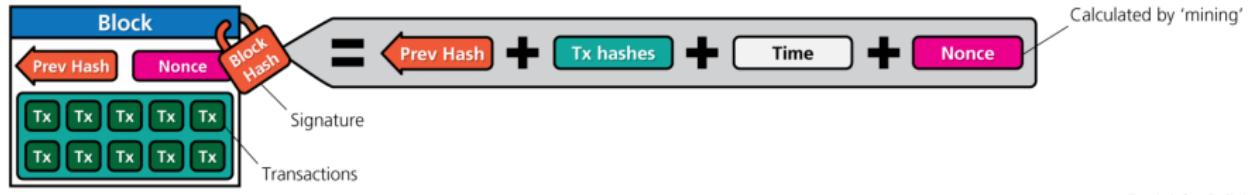
Tx : ".00012300 BTC pour Binta, signé Amadou"

Pour faire une transaction



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

Pour faire une transaction



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

- il contient une récompense (*coinbase*)

Pour faire une transaction

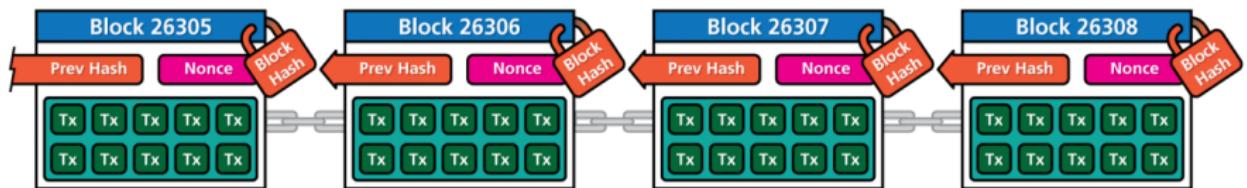


Illustration by CryptoGraphics.info

Les autres mineurs :

- ▶ Vérifie le nonce
- ▶ ajoutent le nouveau block à la chaîne
- ▶ recommencent la course pour valider un nouveau bloc de transactions et obtenir une récompense

La pizza à 10 000 BTC



- ▶ le 18 mai 2010, laslo sur bitcointalk.org
- ▶ Le Bitcoin est devenu une l'unité de compte d'journal comptable ouvert infalsifiable

A quand son garba payé en QR code ?

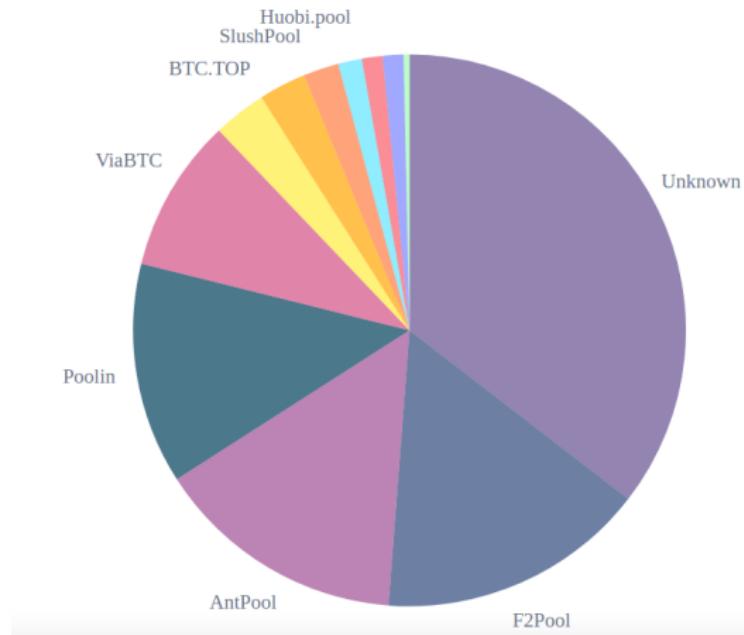
Limites de la blockchain bitcoin 1/5

Coût énergétique



Limites de la blockchain bitcoin 2/5

Concentration du hashrate (juin 2021)



Limites de la blockchain Bitcoin 3/5

Politique : forks

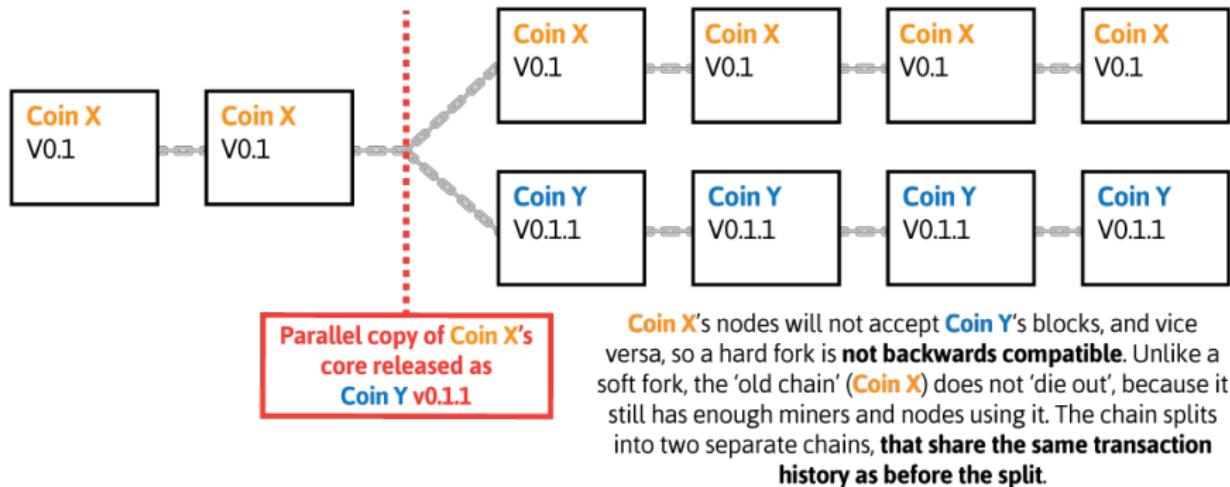
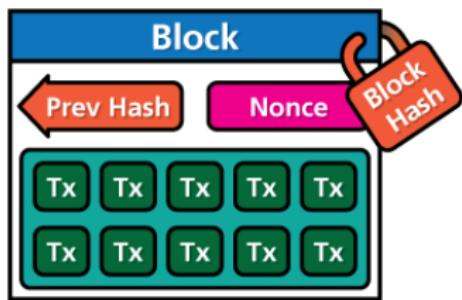


Illustration by CryptoGraphics.info

Limites de la Blockchain bitcoin 4/5

Vitesse de traitement des transactions



Tx = 200 transactions

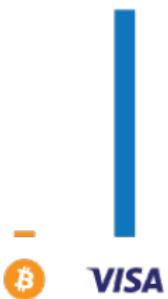
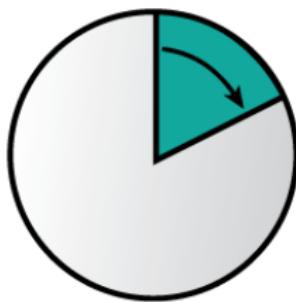
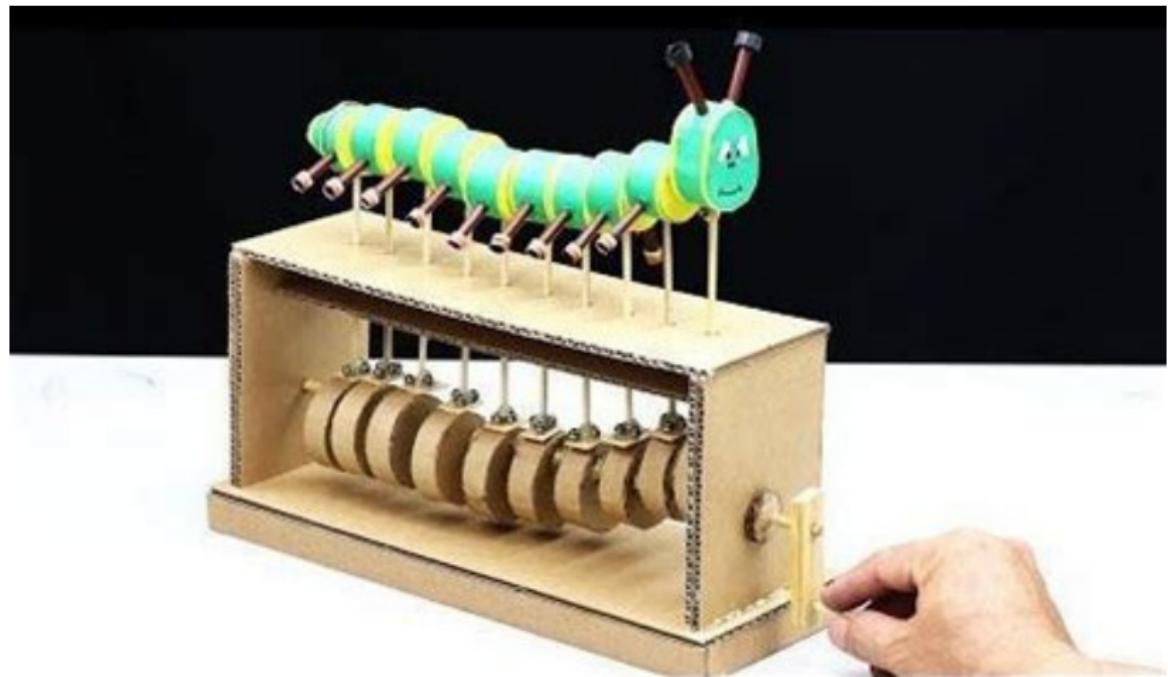


Illustration by CryptoGraphics.info

Limites de la Blockchain bitcoin 5/5

Jeux d'instructions limités



Blockchain de 2^e génération : Etherum

Un système d'exploitation décentralisé

Distributed applications (smart contracts)

DeFI

- ▶ Services financiers décentralisés (DeFI)
- ▶ Financement participatif
- ▶ Dépots de garanties (emprunt)
- ▶ Création de marchés de pairs à pairs
- ▶ Paiement internationaux



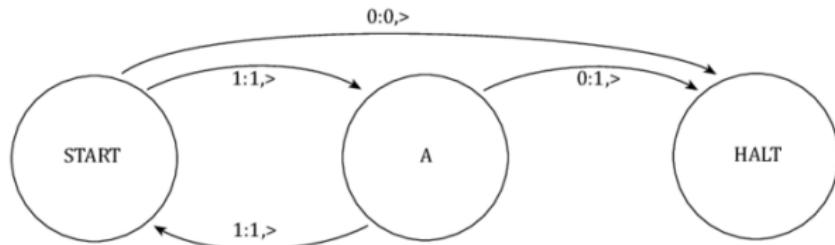
Distributed applications (smart contracts)

DEFI

- ▶ Logistique
- ▶ Identité numérique
- ▶ Monnaie dirigée
- ▶ Objets connectés



Blockchain de 2^e génération : Etherum



- ▶ 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;  
    }  
}
```

- ▶ Machine Turing complet
- ▶ dApps et smart-contracts (solidity)

Blockchain de 2^e génération : Etherum



- ▶ Machine Turing complet
- ▶ dApps et smart-contracts (solidity)
- ▶ ETH, ETC et gaz

Les limites d'Etherum

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

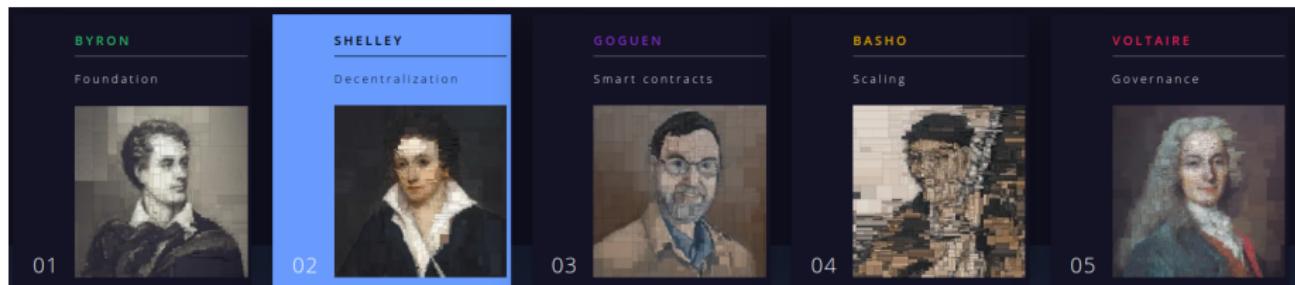


Cardano : blockchain de 3^e génération

1, 2, et ... 3 !

Originalité du projet

1^{er} blockchain scientifique



CARDANO

Le Fonctionnement de Cardano

- ▶ Utilisateurs
 - ▶ Achat, vente, stockage et échange d'ADA



Le Fonctionnement de Cardano

▶ Utilisateurs

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

```
-- | 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

- ▶ Acteurs

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



Le Fonctionnement de Cardano

- ▶ Utilisateurs

- ▶ Acteurs

- ▶ Décideurs

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



Le Fonctionnement de Cardano

- ▶ Utilisateurs
- ▶ Acteurs
- ▶ Décideurs
- ▶ Empereurs
 - ▶ Votes & Trésor



Un révolution techno-sociale ?

La monnaie

Qu'est ce que la monnaie ?

- ▶ unité de valeur, de change et de compte

Une histoire de confiance
(Aglietta & Orléan 1998)



La monnaie

Qu'est ce que la monnaie ?

- ▶ un jeu d'écriture

Une histoire de confiance
(Aglietta & Orléan 1998)



La monnaie

Qu'est ce que la monnaie ?

Une histoire de confiance
(Aglietta & Orléan 1998)

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



La monnaie

Qu'est ce que la monnaie ?

Une histoire de confiance
(Aglietta & Orléan 1998)

- ▶ L'habitude (méthodique)



Les Crypto-monnaies



Jetons (tokens)

Marchés des crypto-monnaies

- ▶ de protocole

Les Crypto-monnaies



Jetons (tokens)

Marchés des crypto-monnaies

- ▶ utilitaires ou applicatifs
 - ▶ *stable coins*
 - ▶ non *fongible* (NFT)

Les Crypto-monnaies



Jetons (tokens)

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 :**
\$ 1 500 milliards

Comment avoir des ADA ?

avec des BTC

- ▶ Acheter des BTC
- ▶ Plateformes d'échange pair à pair ex. localbitcoins
- ▶ Maisons de change (ayael au plateau)

Directement

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

Comment garder ses ADA ?

Daedalus (noeud complet)



Yoroi (portefeuille léger)



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 à une pool c'est se regrouper pour valider ensemble des transactions, contre rémunération

Afrikpool



POA

Proof of Africa

STKH1



Conclusion

Cardano

- ▶ Plan de déploiement Cardano
- ▶ Explorateur de bloc pour Cardano
- ▶ Cardano-node (github)

Délégation

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

Evènements Blockchains

- ▶ mars 2022 Conférence Blockchain en Afrique du Sud

C'est l'heure du air drop

1. Créer un wallet (suivre les instructions)
2. Copier l'adresse publique dans le formulaire ci-dessous
3. <https://tinyurl.com/anzy45fk>
4. Transférer à un ami
5. Déléguer ensemble

Merci à tous

Yoroi-wallet

