



Jeudi 20 juillet 2023

# L'intelligence Artificielle pour les Juristes

Partie 3 : Blockchain et automatisation  
en l'absence de confiance

Issa Traoré (PhD)  
Malik Koné (PhD)

# Sommaire

## 1. Blockchain et Bitcoin

### Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

## 2. Crypto-économie

### Notions de départ

La monnaie

Que sont les cryptomonnaies ?

Le marché des cryptomonnaies

Pour conclure sur la  
crypto-économie

## 3. Smart-contract

Cardano : blockchain de 3<sup>e</sup>  
génération

A quoi peuvent servir les smart  
contract ?

## 4. Cryptographie

Cryptographie

# Notions de départ

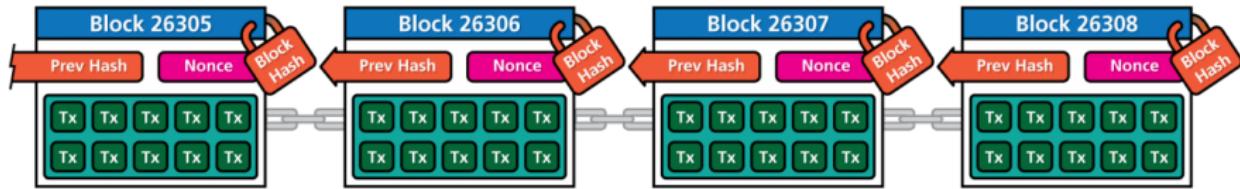


Illustration by CryptoGraphics.info

## Blockchain

- ▶ Décentralisation
- ▶ Consensus
- ▶ Cryptographie
- ▶ Applications décentralisées (dApp)

## Cryptoéconomie

- ▶ Tokens ou jetons
- ▶ Marchés financiers
- ▶ Porte-monnaie de crypto (Yoroi-wallet)

# Sommaire

## 1. Blockchain et Bitcoin

Notions de départ

### Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

## 2. Crypto-économie

Notions de départ

La monnaie

Que sont les cryptomonnaies ?

Le marché des cryptomonnaies

Pour conclure sur la

crypto-économie

## 3. Smart-contract

Cardano : blockchain de 3<sup>e</sup> génération

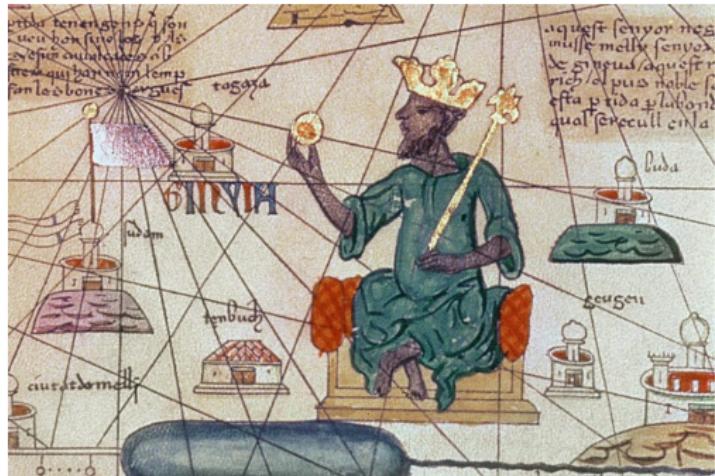
A quoi peuvent servir les smart contract ?

## 4. Cryptographie

Cryptographie

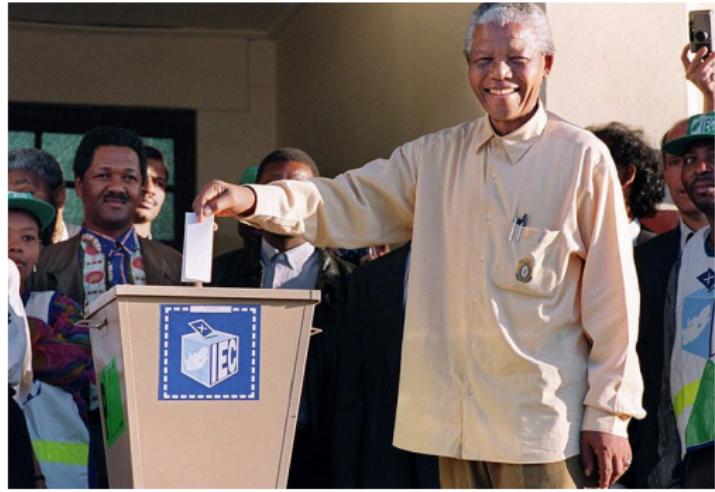
# Les rôles sur la blockchain

- ▶ Les empereurs
  - ▶ Ils créent
- ▶ les élus
  - ▶ Ils écrivent
- ▶ les mineurs
  - ▶ Ils fouillent
- ▶ les utilisateurs
  - ▶ Ils utilisent



# Les rôles sur la blockchain

- ▶ Les empereurs
  - ▶ Ils créent
- ▶ les élus
  - ▶ Ils écrivent
- ▶ les mineurs
  - ▶ Ils fouillent
- ▶ les utilisateurs
  - ▶ Ils utilisent



# Les rôles sur la blockchain

- ▶ Les empereurs
  - ▶ Ils créent
- ▶ les élus
  - ▶ Ils écrivent
- ▶ les mineurs
  - ▶ Ils fouillent
- ▶ les utilisateurs
  - ▶ Ils utilisent



# Les rôles sur la blockchain

- ▶ Les empereurs
  - ▶ Ils créent
- ▶ les élus
  - ▶ Ils écrivent
- ▶ les mineurs
  - ▶ Ils fouillent
- ▶ les utilisateurs
  - ▶ Ils utilisent



# Sommaire

## 1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

### La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

## 2. Crypto-économie

Notions de départ

La monnaie

Que sont les cryptomonnaies ?

Le marché des cryptomonnaies

Pour conclure sur la

crypto-économie

## 3. Smart-contract

Cardano : blockchain de 3<sup>e</sup> génération

A quoi peuvent servir les smart contract ?

## 4. Cryptographie

Cryptographie

*Toute action engendre une réaction (3<sup>e</sup> loi de Newton)*

# La Naissance du Bitcoin

## Cyber-Anarchisme

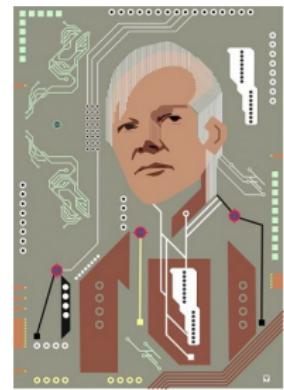
From : Satoshi Nakamoto [satoshi@vistomail.com](mailto:satoshi@vistomail.com)

Subject : Bitcoin P2P e-cash 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.



# La Naissance du Bitcoin

## Cypherpunk (Hal Finney)



[What is Cryonics?](#) [Membership](#) [About](#) [Blog](#) [Library](#) [Contact](#) [🔍](#)



# Sommaire

## 1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

### Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

## 2. Crypto-économie

Notions de départ

La monnaie

Que sont les cryptomonnaies ?

Le marché des cryptomonnaies

Pour conclure sur la

crypto-économie

## 3. Smart-contract

Cardano : blockchain de 3<sup>e</sup> génération

A quoi peuvent servir les smart contract ?

## 4. Cryptographie

Cryptographie

# Que vaut la blockchain ?



2009

???

SSL/TLS - 1996



HTTP - 1990



1995

TCP/IP - 1974



1984

Ethernet - 1974



1979

Cela dépendra de son utilité

# Sommaire

## 1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

### Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

## 2. Crypto-économie

Notions de départ

La monnaie

Que sont les cryptomonnaies ?

Le marché des cryptomonnaies

Pour conclure sur la

crypto-économie

## 3. Smart-contract

Cardano : blockchain de 3<sup>e</sup> génération

A quoi peuvent servir les smart contract ?

## 4. Cryptographie

Cryptographie



# Sommaire

## 1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

**Quel est le problème résolu**

Les limites

Pour conclure sur la blockchain

## 2. Crypto-économie

Notions de départ

La monnaie

Que sont les cryptomonnaies ?

Le marché des cryptomonnaies

Pour conclure sur la

crypto-économie

## 3. Smart-contract

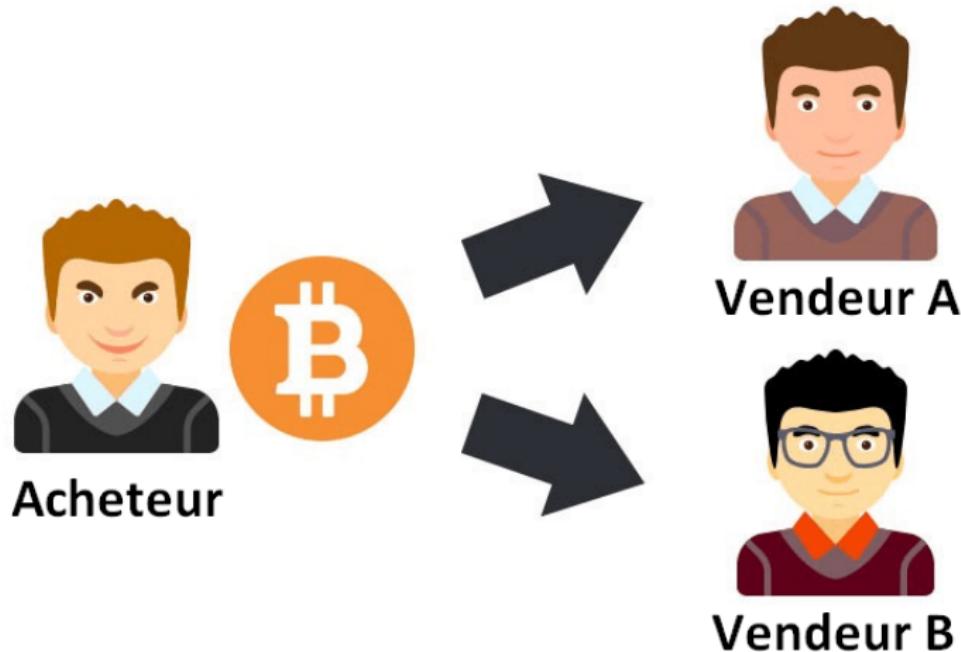
Cardano : blockchain de 3<sup>e</sup> génération

A quoi peuvent servir les smart contract ?

## 4. Cryptographie

Cryptographie

# La double dépense



# Comment le problème est-il résolu ?

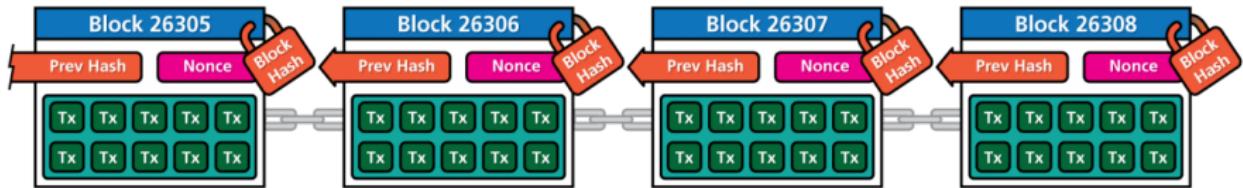


Illustration by CryptoGraphics.info

avec un journal comptable électronique

- ▶ organisés en blocks **infalsifiables** : SHA256 HASH
- ▶ de façon unique : block
- ▶ qui s'**enchainent** les uns aux autres : chain
- ▶ dans un réseau **publique et décentralisé** : pairs

Il faut former la plus longue chaîne possible !

# Comment le problème est-il résolu ?

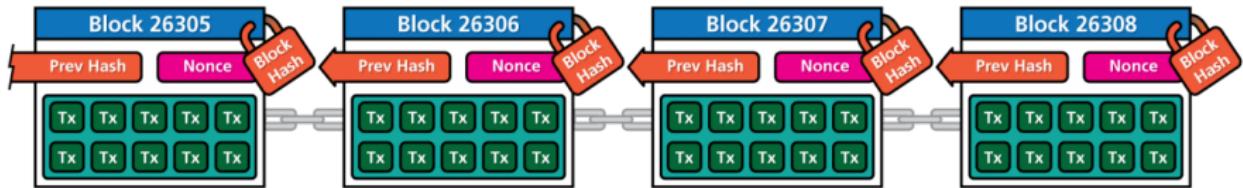


Illustration by CryptoGraphics.info

avec un journal comptable électronique

- ▶ organisés en blocks **infalsifiables** : SHA256 HASH
- ▶ de façon unique : block
- ▶ qui s'**enchainent** les uns aux autres : chain
- ▶ dans un réseau **publique et décentralisé** : pairs

Il faut former la plus longue chaîne possible !

# Comment le problème est-il résolu ?

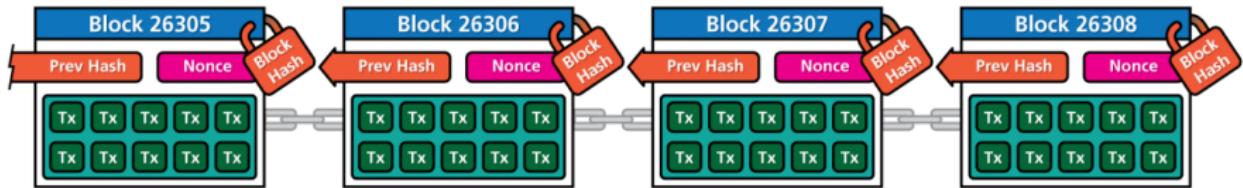


Illustration by CryptoGraphics.info

avec un journal comptable électronique

- ▶ organisés en blocks **infalsifiables** : SHA256 HASH
- ▶ de façon unique : block
- ▶ qui s'**enchainent** les uns aux autres : chain
- ▶ dans un réseau **publique et décentralisé** : pairs

Il faut former la plus longue chaîne possible !

# Comment le problème est-il résolu ?

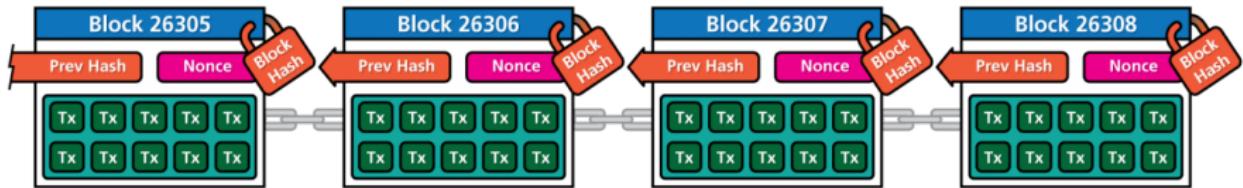


Illustration by CryptoGraphics.info

avec un journal comptable électronique

- ▶ organisés en blocks **infalsifiables** : SHA256 HASH
- ▶ de façon unique : block
- ▶ qui s'**enchainent** les uns aux autres : chain
- ▶ dans un réseau **publique et décentralisé** : pairs

Il faut former la plus longue chaîne possible !

# Comment le problème est-il résolu ?

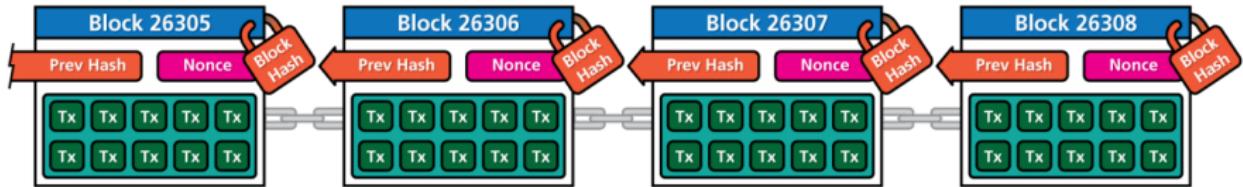


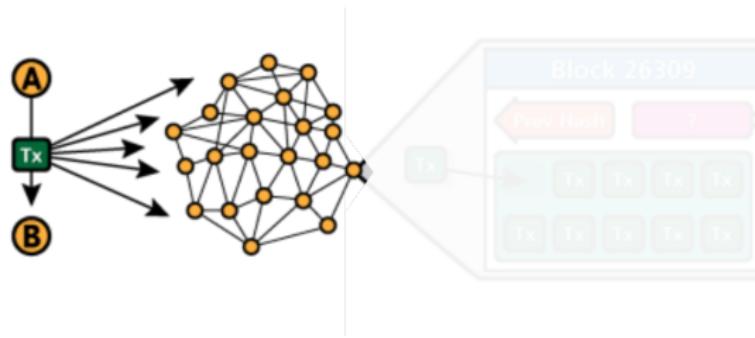
Illustration by CryptoGraphics.info

avec un journal comptable électronique

- ▶ organisés en blocks **infalsifiables** : SHA256 HASH
- ▶ de façon unique : block
- ▶ qui s'**enchainent** les uns aux autres : chain
- ▶ dans un réseau **publique et décentralisé** : pairs

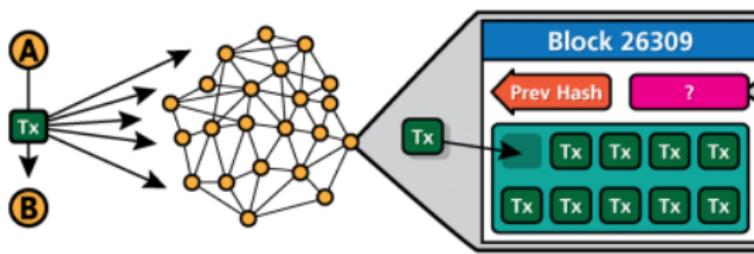
Il faut former la plus longue chaîne possible !

# Plus techniquement comment cela fonctionne ?



Tx : ".1 BTC pour Bob, signé Alice"

# Plus techniquement comment cela fonctionne ?



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

# Plus techniquement comment cela fonctionne ?

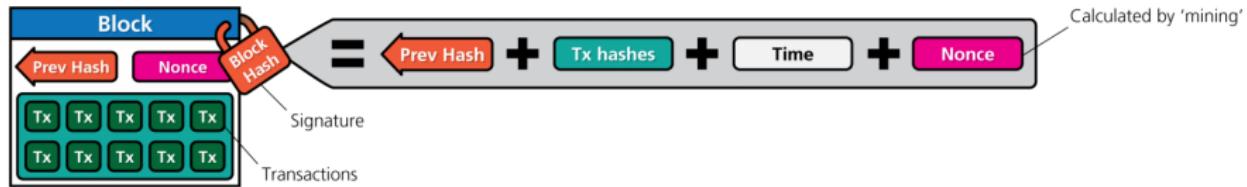


Illustration by CryptoGraphics.info

Le 1<sup>er</sup> mineur à trouver un **bon nonce**, publie le bloc

- ▶ il contient une récompense (coinbase)

# Plus techniquement comment cela fonctionne ?

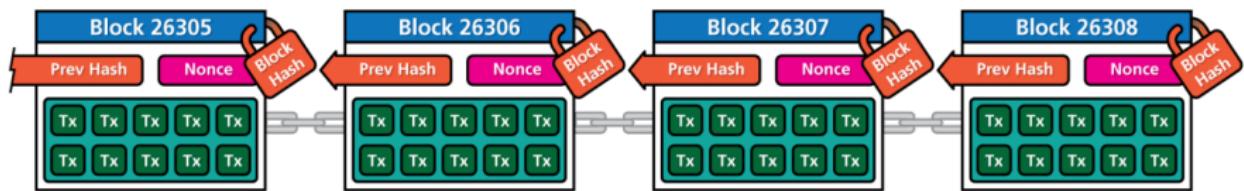


Illustration by CryptoGraphics.info

Les autres mineurs :

- ▶ Vérifient le nonce
- ▶ Ajoutent le nouveau block à la chaîne
- ▶ Recommencent la course pour
  1. allonger la chaîne
  2. obtenir des bitcoins

# Alors c'est quoi le Bitcoin dans tout ça ?



## À quoi ça sert ?

- ▶ C'est une unité de compte
- ▶ C'est la récompense pour les mineurs
- ▶ ça devient un moyen d'échange
- ▶ ça devient une réserve de valeur

# Alors c'est quoi le Bitcoin dans tout ça ?



## À quoi ça sert ?

- ▶ C'est une unité de compte
  - ▶ C'est la récompense pour les mineurs
- ▶ ça devient un moyen d'échange
- ▶ ça devient une réserve de valeur

# Alors c'est quoi le Bitcoin dans tout ça ?



## À quoi ça sert ?

- ▶ C'est une unité de compte
  - ▶ C'est la récompense pour les mineurs
- ▶ ça devient un moyen d'échange
- ▶ ça devient une réserve de valeur

On ne le mange pas mais il fait manger depuis 2009 !



- ▶ 18/05/2010, les Pizza à 10000 BTC de Laslo ([bitcointalk.org](http://bitcointalk.org))

# Sommaire

## 1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

**Les limites**

Pour conclure sur la blockchain

## 2. Crypto-économie

Notions de départ

La monnaie

Que sont les cryptomonnaies ?

Le marché des cryptomonnaies

Pour conclure sur la

crypto-économie

## 3. Smart-contract

Cardano : blockchain de 3<sup>e</sup> génération

A quoi peuvent servir les smart contract ?

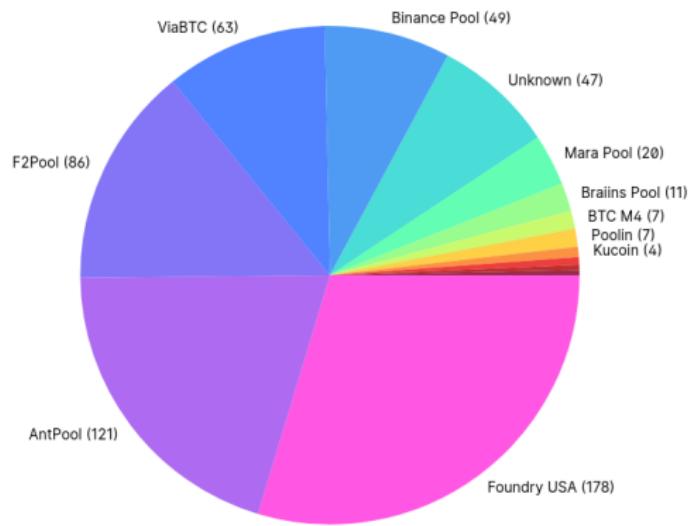
## 4. Cryptographie

Cryptographie

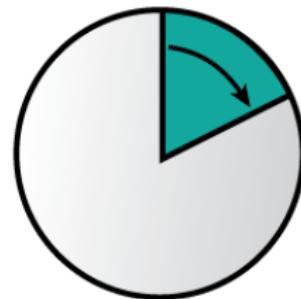
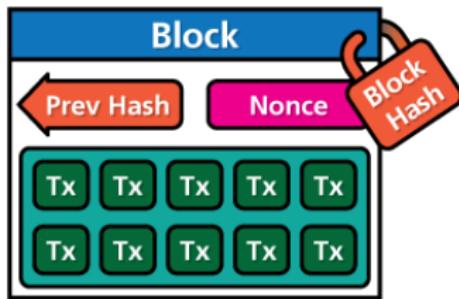
# Coût énergétique



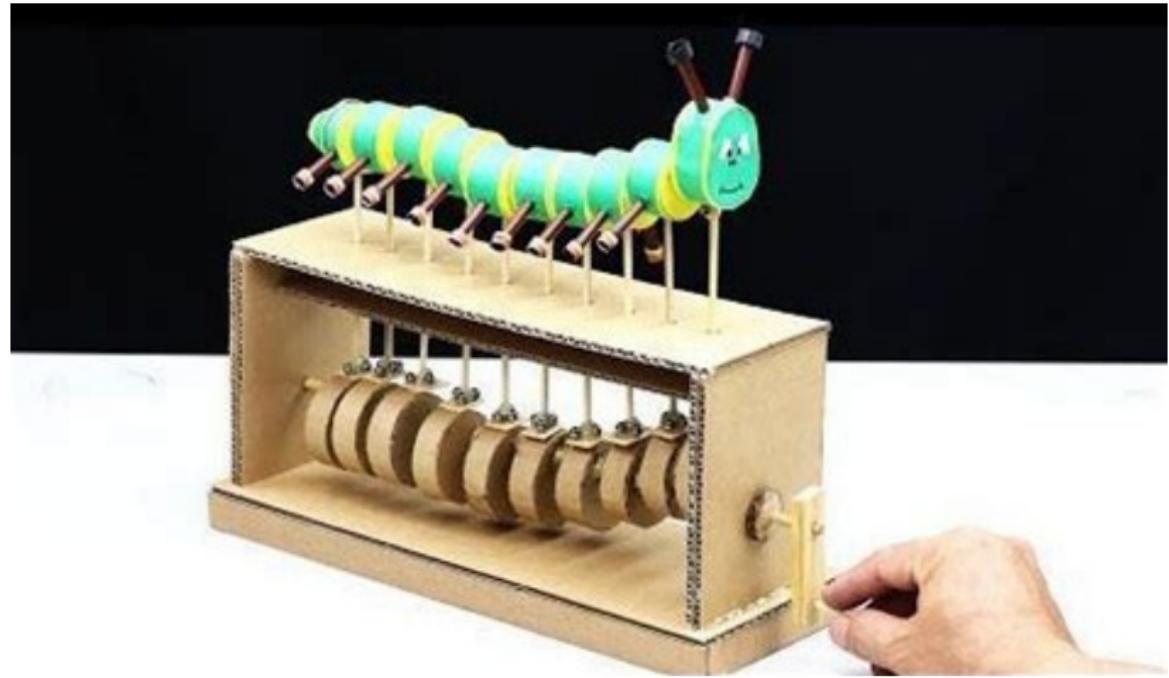
# Concentration du hashrate (juillet 2023)



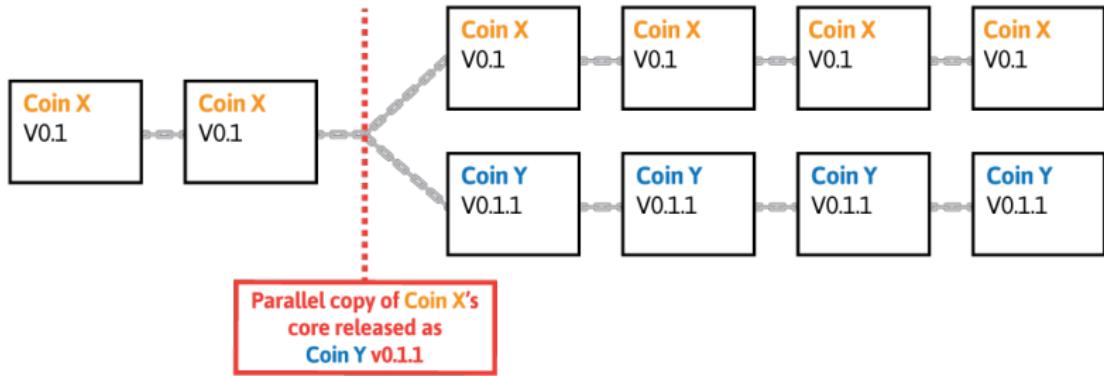
# Vitesse de traitement des transactions



# Jeux d'instructions limités



# Difficile à adapter : Hard-forks



# Sommaire

## 1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

**Pour conclure sur la blockchain**

## 2. Crypto-économie

Notions de départ

La monnaie

Que sont les cryptomonnaies ?

Le marché des cryptomonnaies

Pour conclure sur la

crypto-économie

## 3. Smart-contract

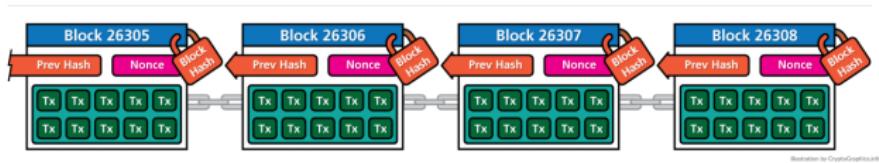
Cardano : blockchain de 3<sup>e</sup> génération

A quoi peuvent servir les smart contract ?

## 4. Cryptographie

Cryptographie

# La blockchain



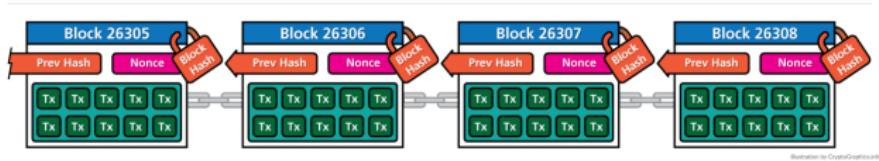
c'est

- ▶ Une technologie d'archivage sécurisée
- ▶ Distribuée
- ▶ Utilisant la cryptographie
- ▶ Fonctionnant sans autorité centrale ou tier de confiance
- ▶ Plus robuste

mais...

- ▶ Gourmande en espace et en ressources
- ▶ Lente
- ▶ Pas nécessairement anonyme
- ▶ Difficile à améliorer et à faire évoluer
- ▶ Plus compliquée

# La blockchain



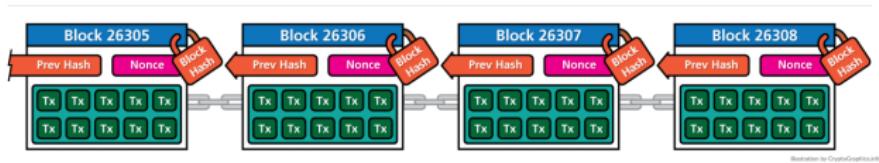
c'est

- ▶ Une technologie d'archivage sécurisée
- ▶ Distribuée
- ▶ Utilisant la cryptographie
- ▶ Fonctionnant sans autorité centrale ou tier de confiance
- ▶ Plus robuste

mais...

- ▶ Gourmande en espace et en ressources
- ▶ Lente
- ▶ Pas nécessairement anonyme
- ▶ Difficile à améliorer et à faire évoluer
- ▶ Plus compliquée

# La blockchain



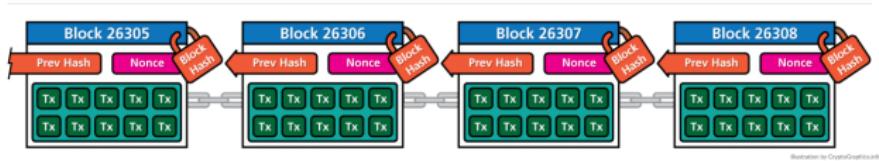
c'est

- ▶ Une technologie d'archivage sécurisée
- ▶ Distribuée
- ▶ Utilisant la cryptographie
- ▶ Fonctionnant sans autorité centrale ou tier de confiance
- ▶ Plus robuste

mais...

- ▶ Gourmande en espace et en ressources
- ▶ Lente
- ▶ Pas nécessairement anonyme
- ▶ Difficile à améliorer et à faire évoluer
- ▶ Plus compliquée

# La blockchain



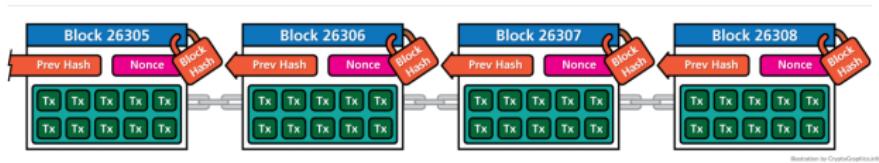
c'est

- ▶ Une technologie d'archivage sécurisée
- ▶ Distribuée
- ▶ Utilisant la cryptographie
- ▶ Fonctionnant sans autorité centrale ou tier de confiance
- ▶ Plus robuste

mais...

- ▶ Gourmande en espace et en ressources
- ▶ Lente
- ▶ Pas nécessairement anonyme
- ▶ Difficile à améliorer et à faire évoluer
- ▶ Plus compliquée

# La blockchain



c'est

- ▶ Une technologie d'archivage sécurisée
- ▶ Distribuée
- ▶ Utilisant la cryptographie
- ▶ Fonctionnant sans autorité centrale ou tier de confiance
- ▶ Plus robuste

mais...

- ▶ Gourmande en espace et en ressources
- ▶ Lente
- ▶ Pas nécessairement anonyme
- ▶ Difficile à améliorer et à faire évoluer
- ▶ Plus compliquée

# Sommaire

## 1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

## 2. Crypto-économie

Notions de départ

La monnaie

Que sont les cryptomonnaies ?

Le marché des cryptomonnaies

Pour conclure sur la

crypto-économie

## 3. Smart-contract

Cardano : blockchain de 3<sup>e</sup>  
génération

A quoi peuvent servir les smart  
contract ?

## 4. Cryptographie

Cryptographie

# Notions de départ

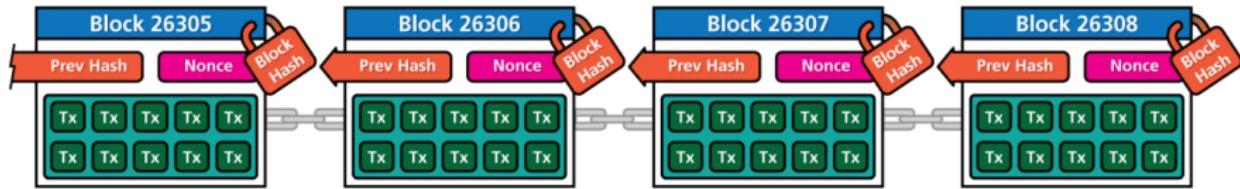


Illustration by CryptoGraphics.info

## Blockchain

- ▶ Décentralisation
- ▶ Consensus
- ▶ Cryptographie
- ▶ Applications décentralisées (dApp)

## Cryptoéconomie

- ▶ Tokens ou jetons
- ▶ Marchés financiers
- ▶ Porte-monnaie de crypto (Yoroi-wallet)

# Sommaire

## 1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

## 2. Crypto-économie

Notions de départ

## La monnaie

Que sont les cryptomonnaies ?

Le marché des cryptomonnaies

Pour conclure sur la

crypto-économie

## 3. Smart-contract

Cardano : blockchain de 3<sup>e</sup> génération

A quoi peuvent servir les smart contract ?

## 4. Cryptographie

Cryptographie

*Fiduciaire, Scripturale, deviendrait-elle Crypturale ?*

# La monnaie

Rappelez vous, c'est...

- ▶ Unité de valeur,
- ▶ Unité de change
- ▶ Unité et de compte
- ▶ Un jeu d'écriture

Une histoire de confiance



pecu

# La monnaie

Rappelez vous, c'est...

- ▶ Unité de valeur,
- ▶ Unité de change
- ▶ Unité et de compte
- ▶ Un jeu d'écriture

Une histoire de confiance



barres de sel

# La monnaie

Rappelez vous, c'est . . .

- ▶ Unité de valeur,
- ▶ Unité de change
- ▶ Unité et de compte
- ▶ Un jeu d'écriture



Une histoire de confiance

épices et pièces

# La monnaie

Rappelez vous, c'est . . .

- ▶ Unité de valeur,
- ▶ Unité de change
- ▶ Unité et de compte
- ▶ Un jeu d'écriture

Une histoire de confiance



poids Akan

# La monnaie

Rappelez vous, c'est . . .

- ▶ Unité de valeur,
- ▶ Unité de change
- ▶ Unité et de compte
- ▶ Un jeu d'écriture

Une histoire de confiance



poids Akan

# La monnaie

Rappelez vous, c'est...

- ▶ Unité de valeur,
- ▶ Unité de change
- ▶ Unité et de compte
- ▶ Un jeu d'écriture

Une histoire de confiance



tally-stick, stocks & foil

# La monnaie

Rappelez vous, c'est...

- ▶ Unité de valeur,
- ▶ Unité de change
- ▶ Unité et de compte
- ▶ Un jeu d'écriture

Une histoire de confiance



billet de 1778

# La monnaie

Rappelez vous, c'est...

- ▶ Unité de valeur,
- ▶ Unité de change
- ▶ Unité et de compte
- ▶ Un jeu d'écriture



## Une histoire de confiance

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

Wall-street ou le *stock-exchange*

- ▶ valeur légale
- ▶ presque entièrement digitalisée

# La monnaie

Rappelez vous, c'est...

- ▶ Unité de valeur,
- ▶ Unité de change
- ▶ Unité et de compte
- ▶ Un jeu d'écriture

Une histoire de confiance

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



M. Jean-Claude Kassi Brou

# La monnaie

Rappelez vous, c'est . . .

- ▶ Unité de valeur,
- ▶ Unité de change
- ▶ Unité et de compte
- ▶ Un jeu d'écriture

Une histoire de confiance

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



# La monnaie

Rappelez vous, c'est...

- ▶ Unité de valeur,
- ▶ Unité de change
- ▶ Unité et de compte
- ▶ Un jeu d'écriture

Une histoire de confiance

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



sur les îles de Yap

# Sommaire

## 1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

## 2. Crypto-économie

Notions de départ

La monnaie

**Que sont les cryptomonnaies ?**

Le marché des cryptomonnaies

Pour conclure sur la

crypto-économie

## 3. Smart-contract

Cardano : blockchain de 3<sup>e</sup>  
génération

A quoi peuvent servir les smart  
contract ?

## 4. Cryptographie

Cryptographie

# Une cryptomonnaie c'est un peu comme

- ▶ des unités téléphoniques
- ▶ des points de fidélité
- ▶ des jetons de baby-foot

Mais :

- ▶ pas de faussaires
- ▶ pas d'intermédiaires
- ▶ pas d'obligation d'usage



# Une cryptomonnaie c'est un peu comme

- ▶ des unités téléphoniques
- ▶ des points de fidélité
- ▶ des jetons de baby-foot

Mais :

- ▶ pas de faussaires
- ▶ pas d'intermédiaires
- ▶ pas d'obligation d'usage



## Leurs usages

- ▶ Protocolaire
- ▶ Applicatifs (dont NFT)
- ▶ Gouvernance



**CARDANO**

# Leurs usages

- ▶ Protocolaire
- ▶ Applicatifs (dont NFT)
- ▶ Gouvernance



*Non Fongible Token (NFT)*

# Leurs usages

- ▶ Protocolaire
- ▶ Applicatifs (dont NFT)
- ▶ Gouvernance



# Exemple d'un achat en Bitcoin

Paiement au El-Salvador en un éclair (avec le réseau *lightning*)



# Sommaire

## 1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

## 2. Crypto-économie

Notions de départ

La monnaie

Que sont les cryptomonnaies ?

**Le marché des cryptomonnaies**

Pour conclure sur la  
crypto-économie

## 3. Smart-contract

Cardano : blockchain de 3<sup>e</sup>  
génération

A quoi peuvent servir les smart  
contract ?

## 4. Cryptographie

Cryptographie

# Le marché des cryptomonnaies



Dizaines de milliers de jetons

- ▶ memes coins
- ▶ stable coins
- ▶ /shit/ coins

Marchés des cryptomonnaies

- ▶ les crédits : \$ 250 billions
- ▶ Les actions : \$ 80 billions
- ▶ l'or : \$ 7 billions
- ▶ les cryptos : \$ 1 billion

# Le marché des cryptomonnaies



Dizaines de milliers de jetons

- ▶ memes coins
- ▶ stable coins
- ▶ /shit/ coins

Marchés des cryptomonnaies

- ▶ les crédits : \$ 250 billions
- ▶ Les actions : \$ 80 billions
- ▶ l'or : \$ 7 billions
- ▶ les cryptos : \$ 1 billion

# Le marché des cryptomonnaies



Dizaines de milliers de jetons

- ▶ memes coins
- ▶ stable coins
- ▶ /shit/ coins

ref. coingecko et coinmarketcap

Marchés des cryptomonnaies

- ▶ les crédits : \$ 250 billions
- ▶ Les actions : \$ 80 billions
- ▶ l'or : \$ 7 billions
- ▶ les cryptos : \$ 1 billion

# Sommaire

## 1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

## 2. Crypto-économie

Notions de départ

La monnaie

Que sont les cryptomonnaies ?

Le marché des cryptomonnaies

**Pour conclure sur la  
crypto-économie**

## 3. Smart-contract

Cardano : blockchain de 3<sup>e</sup>  
génération

A quoi peuvent servir les smart  
contract ?

## 4. Cryptographie

Cryptographie

## En résumé

La crypto-économie est balbutiante

- ▶ Petit marché
- ▶ peu de régulation

Mais dans monde multipolaire

- ▶ un potentiel de croissance énorme

# Sommaire

## 1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

## 2. Crypto-économie

Notions de départ

La monnaie

Que sont les cryptomonnaies ?

Le marché des cryptomonnaies

Pour conclure sur la

crypto-économie

## 3. Smart-contract

Cardano : blockchain de 3<sup>e</sup> génération

A quoi peuvent servir les smart contract ?

## 4. Cryptographie

Cryptographie

# Cardano : blockchain de 3<sup>e</sup> génération

1, 2, et ⋯ 3 !

# Originalité du projet

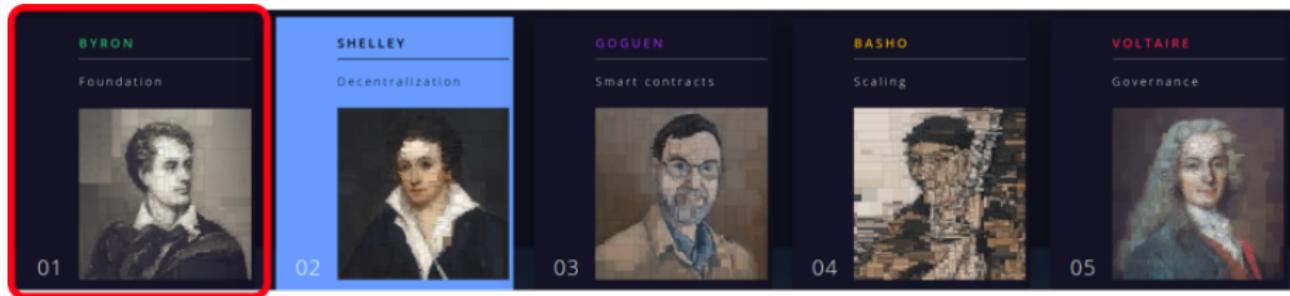
1<sup>er</sup> blockchain scientifique



## CARDANO

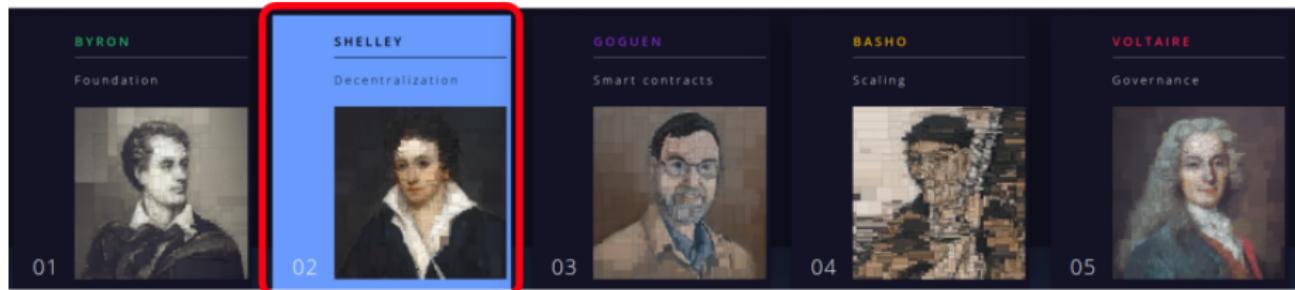
<b>BYRON</b> Foundation  01	<b>SHELLEY</b> Decentralization  02	<b>GOGUEN</b> Smart contracts  03	<b>BASHO</b> Scaling  04	<b>VOLTAIRE</b> Governance  05
---	---	---	---	--

# Les fondations



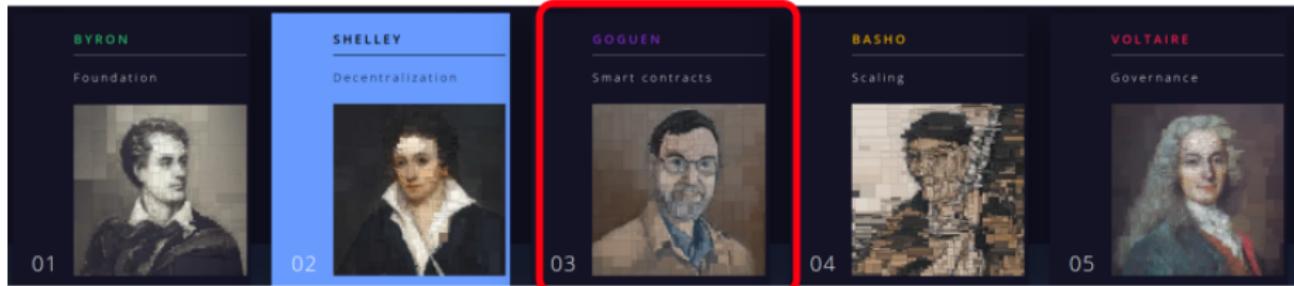
Ouroboros Proof of Stake

# La décentralisation



Stacking et pools

# Les smart-contract



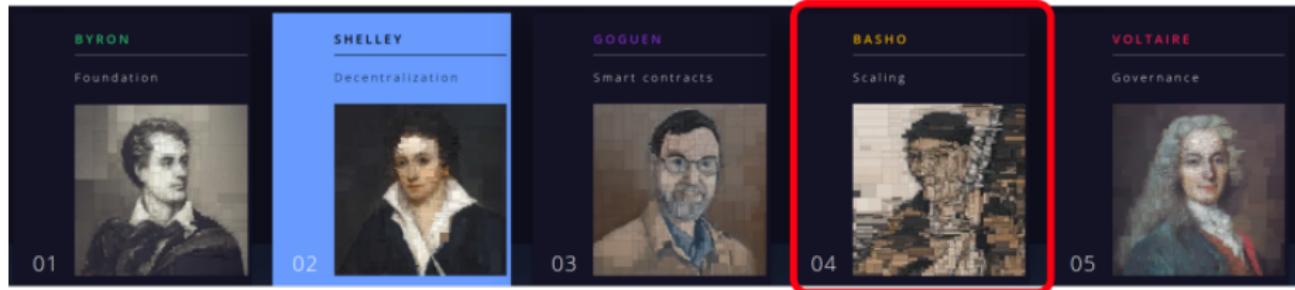
```
-- | Checks if a date is before the given end date.
beforeEnd :: Date -> EndDate -> Bool
beforeEnd (Date d) (Fixed e) = d <= e
beforeEnd (Date _) Never     = True

-- | 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
```

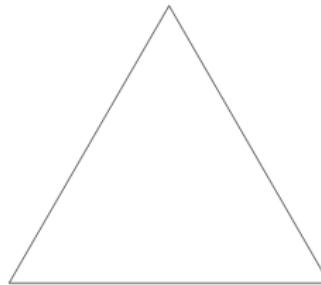


## Smart-contract

# Mise à l'échelle : plus Grand, plus Vite plus Robuste



Sécurité

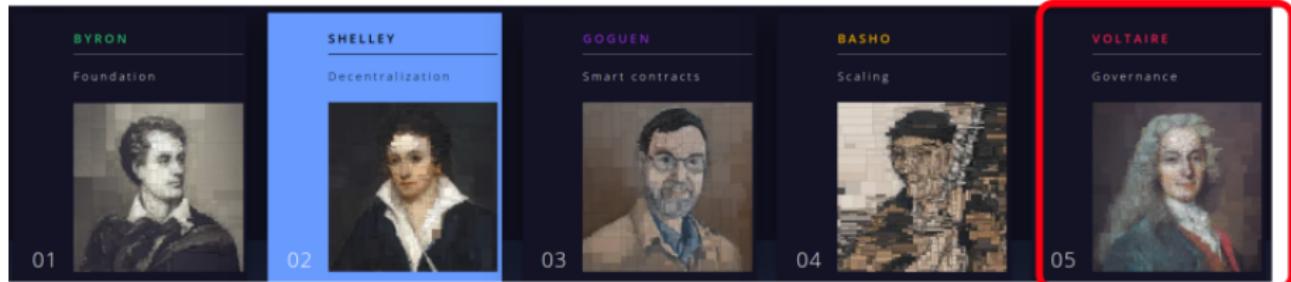


Décentralisation

Agrandissement  
(mise à l'échelle)

Le triangle du dilemme

# La gouvernance : responsabilité et répartition du pouvoir



Voter pour le Trésor

# Sommaire

## 1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

## 2. Crypto-économie

Notions de départ

La monnaie

Que sont les cryptomonnaies ?

Le marché des cryptomonnaies

Pour conclure sur la

crypto-économie

## 3. Smart-contract

Cardano : blockchain de 3<sup>e</sup> génération

A quoi peuvent servir les smart contract ?

## 4. Cryptographie

Cryptographie

# Application purement financières

- ▶ Sous-monnaies
  - ▶ stable coins
- ▶ produits dérivés
- ▶ contrat hedging
  - ▶ assurances, SchellingCoin
- ▶ Compte d'épargne
- ▶ Application notariale
- ▶ contrat de travail
- ▶ loterie
- ▶ marché distribués



# Applications semi-financières

## Monnaies et données

Être payés pour, ou fournir, des données

gestions des identités

- ▶ gestion de nom de domaine (nameCoin)
- ▶ gestoin d'ID
- ▶ gestion de fichiers
- ▶ gestion de contenu
- ▶ réseau sociaux décentralisé



# Applications semi-financières

## Monnaies et données

Être payés pour, ou fournir, des données

## gestions des identités

- ▶ gestion de nom de domaine (nameCoin)
- ▶ gestoin d'ID
- ▶ gestion de fichiers
- ▶ gestion de contenu
- ▶ réseau sociaux décentralisé

## Autres Applications :

- ▶ Calcul distribué (seti@home, folding@home)

# Applications non-financières

- ▶ Vote en ligne
- ▶ Gouvernance décentralisé



# Applications Autonomes et Décentralisé

## DA : Decentralised Autonomous

- ▶ DAC communauté (equal vote)
- ▶ DAC corporation (votre proportional to share)

## DAO : Decentralised Autonomous Organisation

Peut fonctionner avec des individus ne parlant pas la même langue

- ▶ Automatise de la gouvernance
- ▶ Des techniques pour changer les règles de gouvernance

# Divers

- ▶ ICO : Initial coin offering
- ▶ ASIC : Application specific integrated circuits

# Sommaire

## 1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

## 2. Crypto-économie

Notions de départ

La monnaie

Que sont les cryptomonnaies ?

Le marché des cryptomonnaies

Pour conclure sur la

crypto-économie

## 3. Smart-contract

Cardano : blockchain de 3<sup>e</sup> génération

A quoi peuvent servir les smart contract ?

## 4. Cryptographie

Cryptographie

# La Cryptographie c'est quoi ?

La science des codes secrets

- ▶ Chiffrer : coder un message
- ▶ Déchiffrer : décoder un message

Les clés

- ▶ Impossible à deviner
- ▶ Utilisés pour chiffrer et déchiffrer

Mais comment se les échanger ?



# La Cryptographie c'est quoi ?

La science des codes secrets

- ▶ Chiffrer : coder un message
- ▶ Déchiffrer : décoder un message



Les clés

- ▶ Impossible à deviner
- ▶ Utilisés pour chiffrer et déchiffrer

Mais comment se les échanger ?

# La Cryptographie c'est quoi ?



## La science des codes secrets

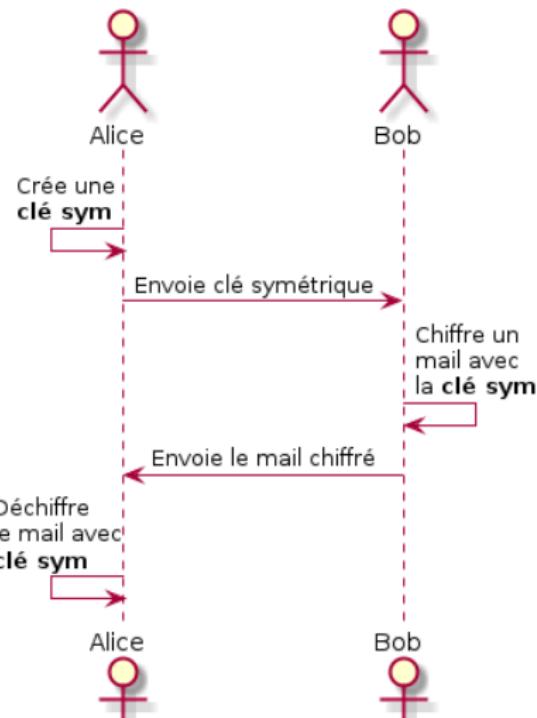
- ▶ Chiffrer : coder un message
- ▶ Déchiffrer : décoder un message

## Les clés

- ▶ Impossible à deviner
- ▶ Utilisés pour chiffrer et déchiffrer

## Mais comment se les échanger ?

# Cryptographie symétrique



## Communication à clé symétrique

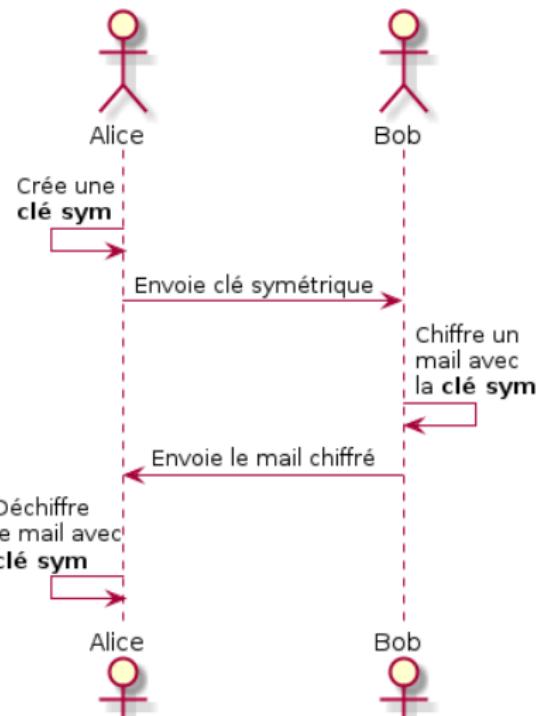
La même clé est utilisée pour :

- ▶ chiffrer
- ▶ déchiffrer

Garder la clé secrète à plusieurs

- ▶ Difficile

# Cryptographie symétrique



## Communication à clé symétrique

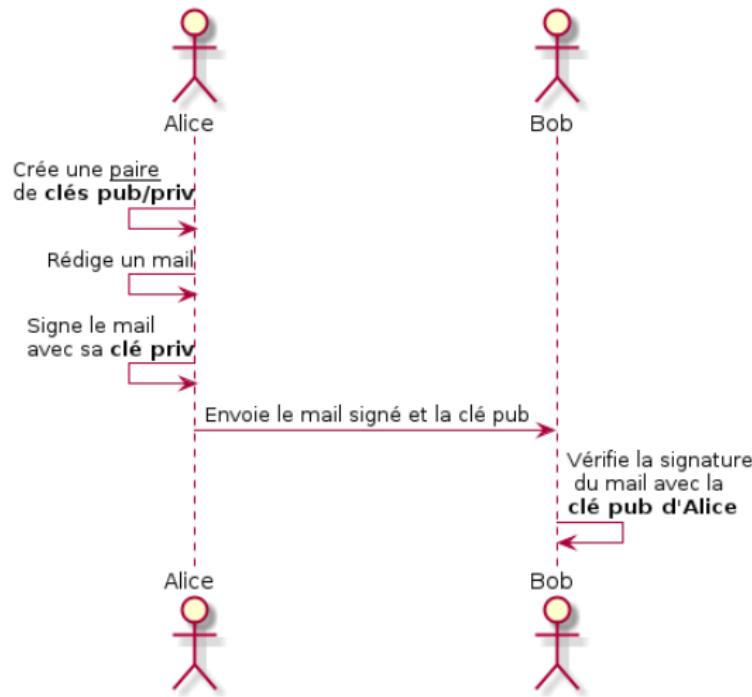
La même clé est utilisée pour :

- ▶ chiffrer
- ▶ déchiffrer

Garder la clé secrète à plusieurs

- ▶ Difficile

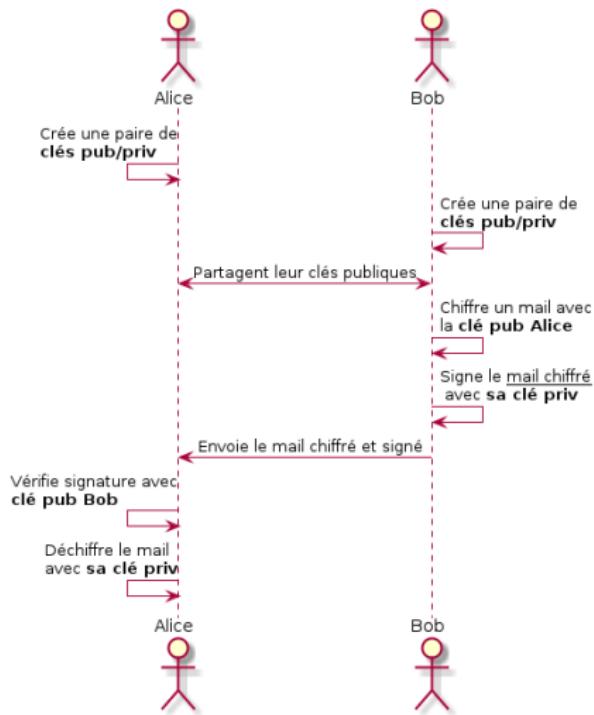
# Cryptographie assymétrique



## Les signatures

- ▶ Authentifier l'auteur du message
- ▶ Savoir si un message a été modifié

# Cryptographie assymétrique



Dans la communication

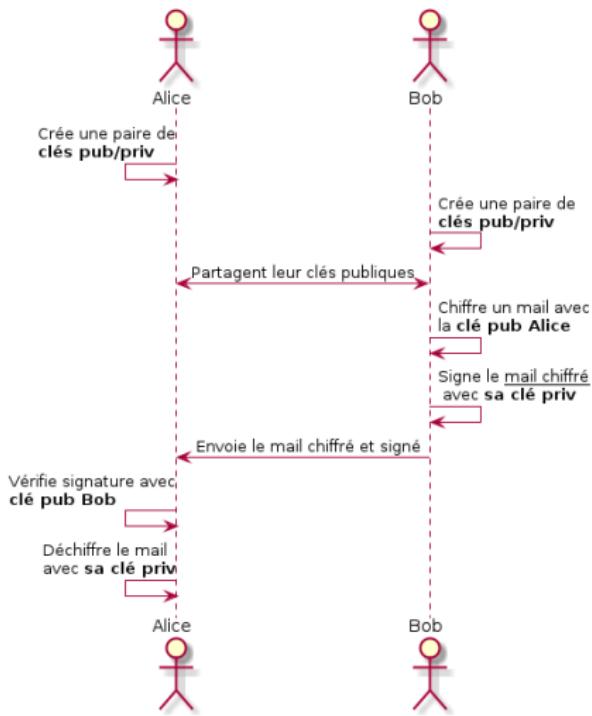
## Avantages

- ▶ Confidentialité
- ▶ Echange de clés sécurisés
- ▶ Pas d'échange initiale de clé

Limites

- ▶ Complexé
- ▶ Coûteux en calcul

# Cryptographie assymétrique



Dans la communication

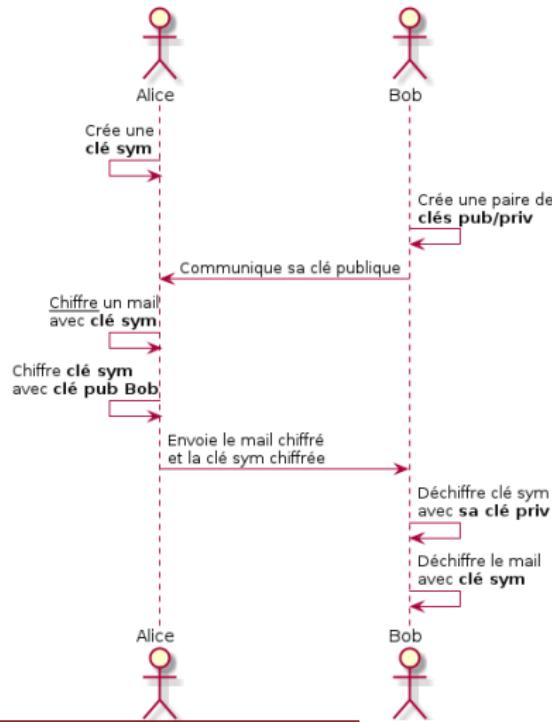
## Avantages

- ▶ Confidentialité
- ▶ Echange de clés sécurisés
- ▶ Pas d'échange initiale de clé

## Limites

- ▶ Complexe
- ▶ Coûteux en calcul

# Cryptographie en pratique



Pour l'utilisateur

Simple

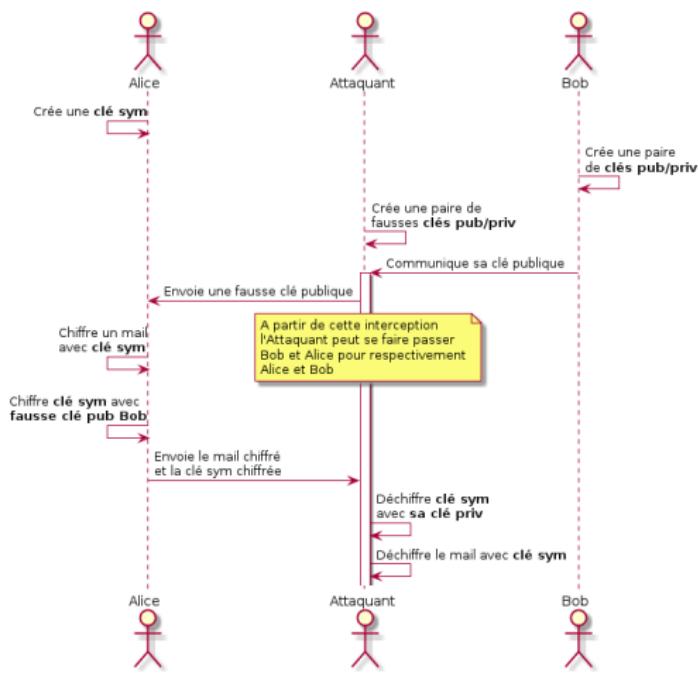
- ▶ Génération automatique des clés : avec un doigt, la voix, un iris...
- ▶ Chiffrage et déchiffrage automatiques, transparents

Complexe

- ▶ Garder sa clé privée secrète
- ▶ Communiquer sa clé publique sans qu'elle soit interceptée

# Cryptographie en pratique

## Pour l'utilisateur



## Simple

- ▶ Génération automatique des clés : avec un doigt, la voix, un iris...
- ▶ Chiffrage et déchiffrage automatiques, transparents

## Complex

- ▶ Garder sa clé privée secrète
- ▶ Communiquer sa clé publique sans qu'elle soit interceptée



Jeudi 20 juillet 2023

# L'intelligence Artificielle pour les Juristes

Merci pour votre Confiance !

Issa Traoré (PhD)  
Malik Koné (PhD)