Code d'Armor

la révolution des blockchains

"La 2ème révolution numérique"

Version 6 - 18/12/2017

Code d'Armor

la révolution des blockchains

CLICKBAIT APPROVED

"La 2ème révolution numérique"

Code d'Armor

Pierre-Yves Lapersonne

software developer

pylapp.github.io

wahou !

*“Grâce à la **blockchain**, vous allez **disrupter** les **usages digitaux** avec une technologie d’avant-garde **cypherpunk** du darkweb clandestin avec des **cybermonnaies** en écrivant des killers features !”*

Jean-Michel Markéteu, *justifiant sa part variable*, 2017

wahou !

*“Grâce à la **blockchain**, vous allez **disrupter** les **usages digitaux** avec une technologie d’avant-garde **cypherpunk** du darkweb clandestin avec des **cybermonnaies** en écrivant des killers features !”*

Code d'Armor

plan

Blockchain
Altcoin
Ethereum, smart contract, *ĐApp*
Usages

introduction

Code d'Armor

Un étrange mélange

cypherpunk + cryptanarchisme + architectures distribuées
+ monnaie + esprit libriste

Crédit : *The Matrix*, 1999, Warner Bros

Plusieurs visages

Wei Dai	*b-money*, cryptographie
Nick Szabo	*bit gold*, smart contracts
Vitalik Buterin	*Ethereum*
Don Tapscott	*Blockchain Research Institute*
Gavin Andresen	*Fondation Bitcoin*
Marc Andreessen	influenceur

Satoshi Nakamoto	implémentation de *Bitcoin*

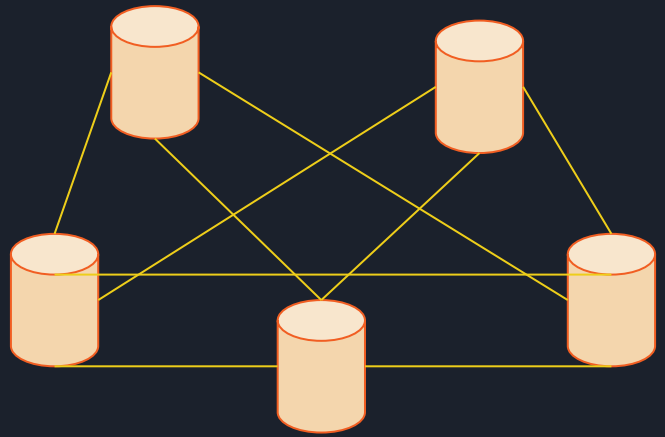
blockchains

Code d'Armor

#1 - un registre...

“Base de données distribuée transparente sécurisée anonyme et infalsifiable fonctionnant sans organe de contrôle”

d’après Blockchain France



#1 - un registre...

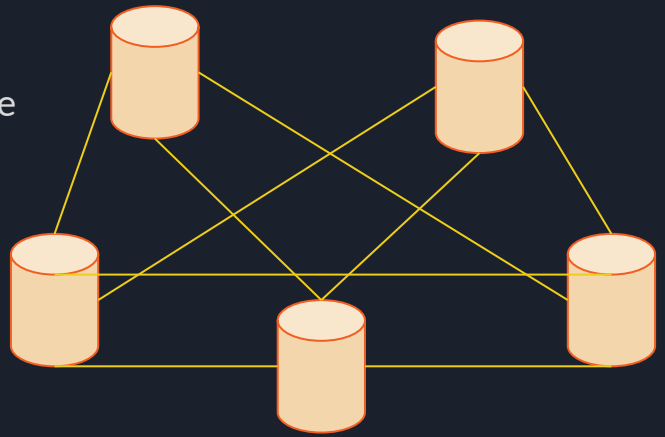
P2P

“Base de données distribuée transparente sécurisée anonyme et infalsifiable fonctionnant sans organe de contrôle”

d’après Blockchain France

selon la blockchain...

décentralisée



- Transactions anonymes avec Dash
- Anonymat renforcé avec Zcash
- Pas vraiment d’anonymat avec Bitcoin

#2 - enregistrant des transactions...

> *“Opération pouvant être par exemple commerciale, boursière, de saisie ou de consultation d’une information”*

d’après Larousse

#2 - enregistrant des transactions...

“Opération pouvant être par exemple commerciale, boursière, de saisie ou de consultation d’une information”

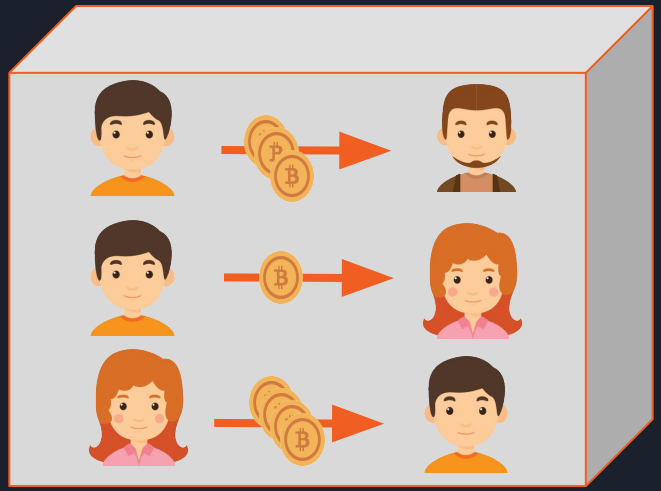
d’après Larousse

ou ça peut être d’autres choses

#3 - inscrites dans des blocs...

> *“Objet ayant des transactions enregistrées, créé par un mineur et ajouté dans la blockchain. Il ne sera alors plus modifiable ni supprimable.”*

d’après Wikipédia

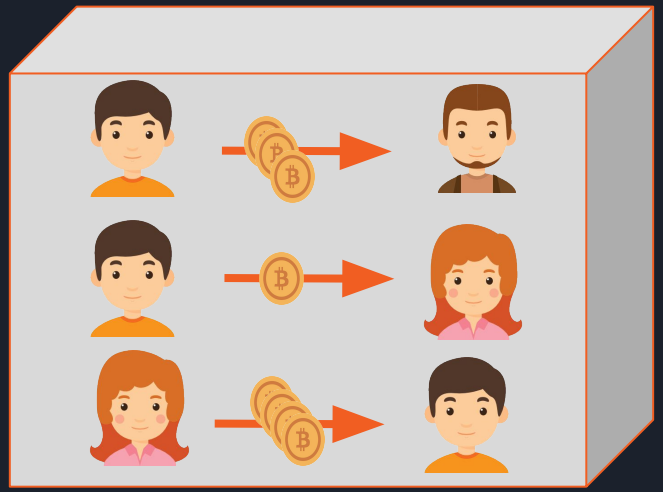


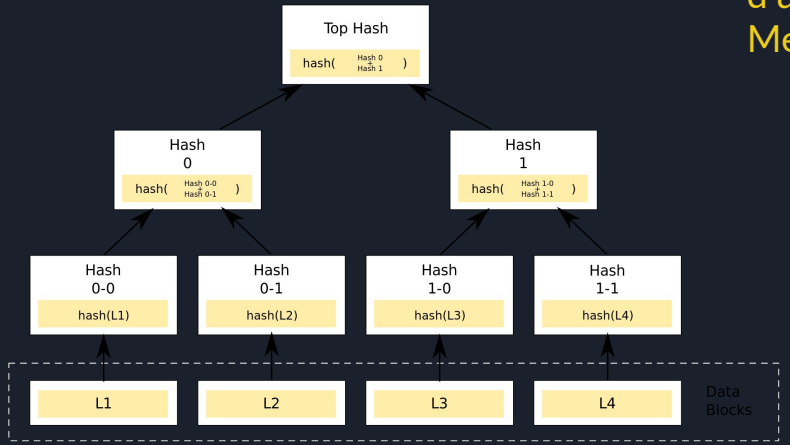
#3 - inscrites dans des blocs…

“Objet ayant des transactions enregistrées, créé par un mineur et ajouté dans la blockchain. Il ne sera alors plus modifiable ni supprimable.”

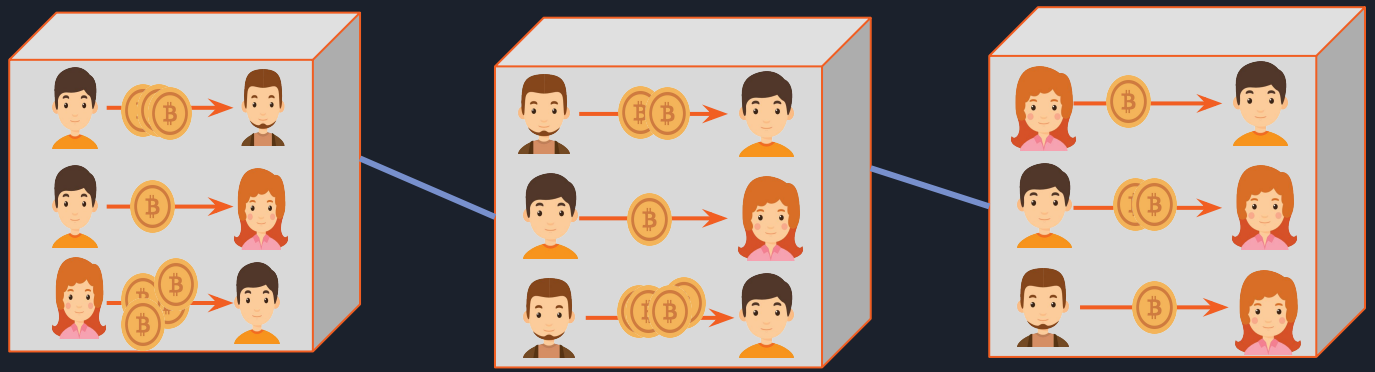
d’après Wikipédia

sous la forme d’un arbre de Merkle



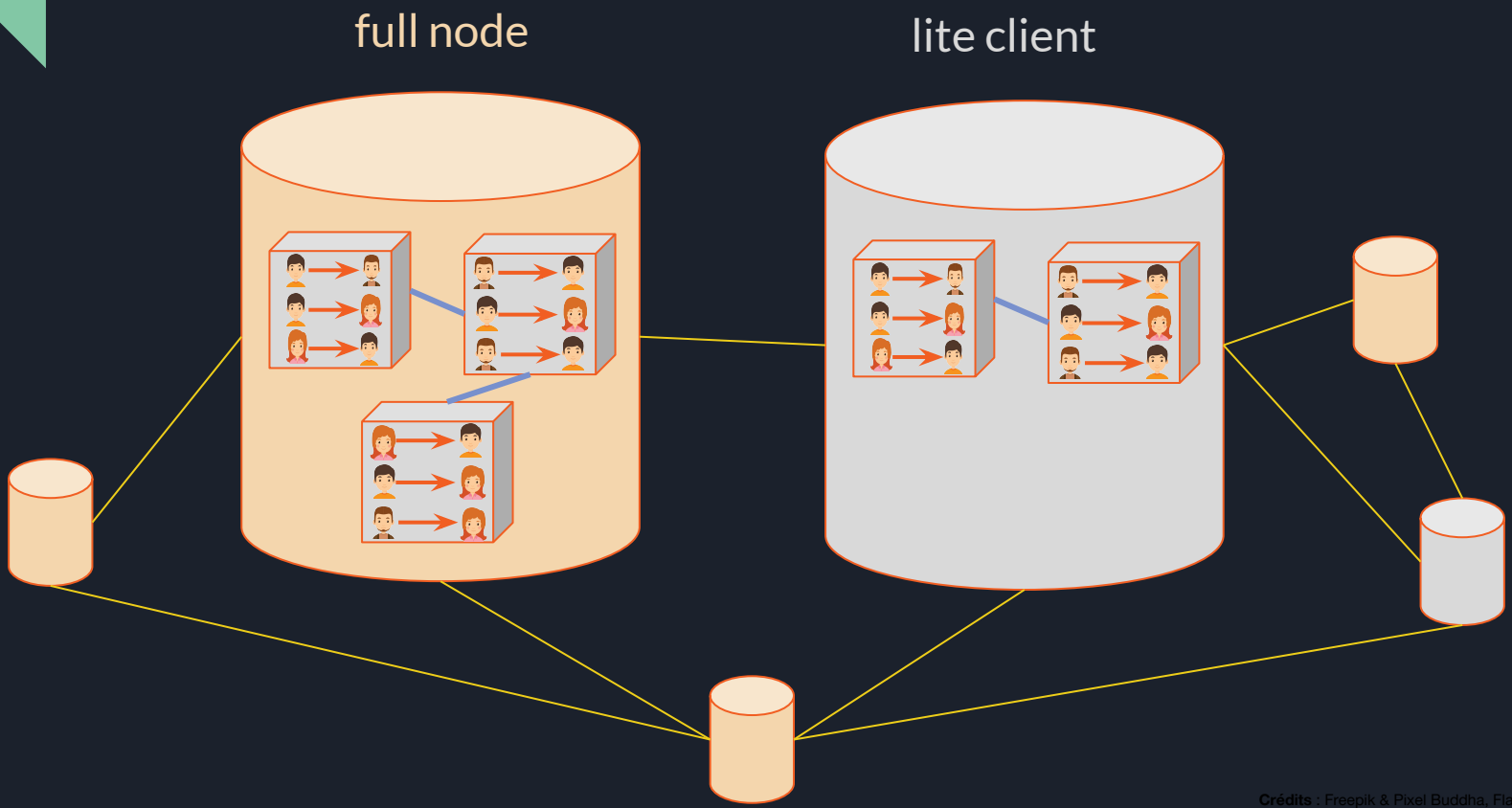


#4 - formant la chaîne de blocs...



Code d'Armor

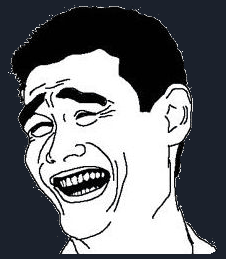
#5 - copiée dans chaque noeud du réseau.



Code d'Armor

fin.

Code d'Armor



Code d'Armor

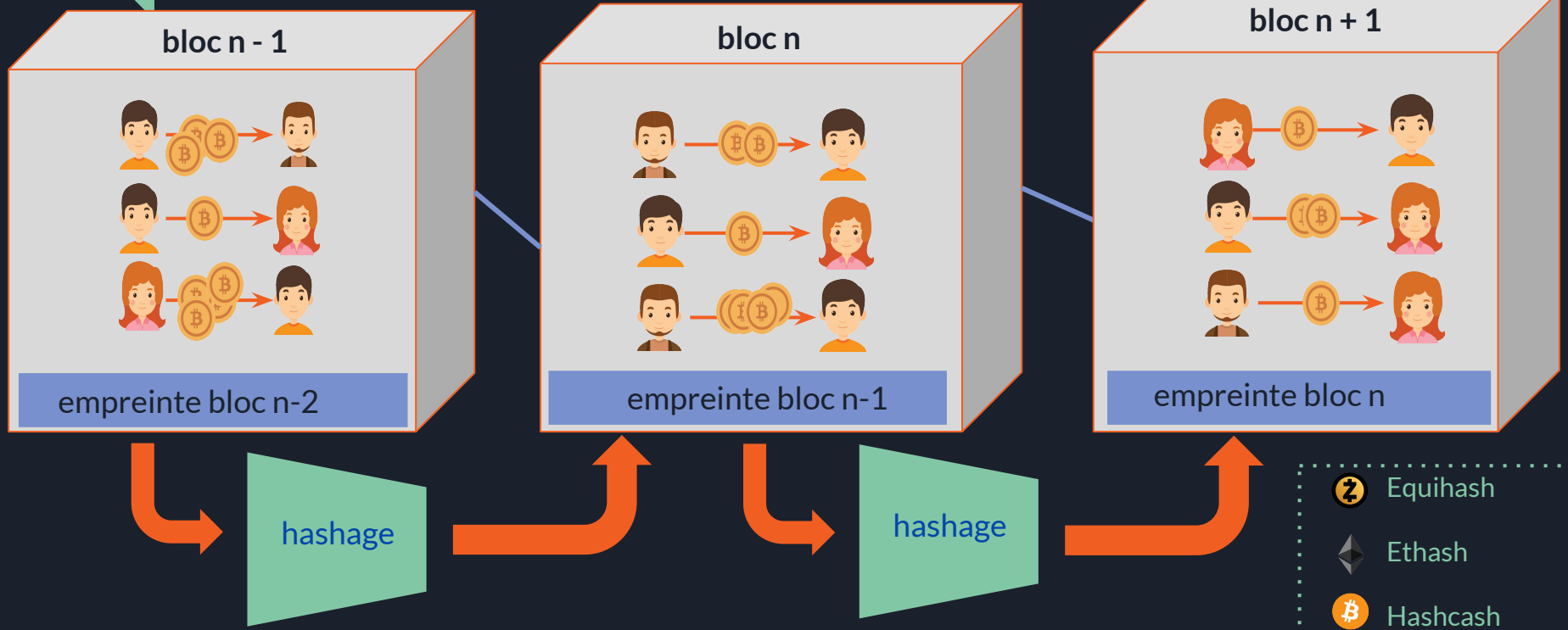
problème 1

Comment rendre infalsifiables les blocs et leurs contenus ?

Crédit : *Pere Castor*, France 3, Canal J

Code d'Armor

Une histoire de hash



Une histoire de hash

bloc n - 1

empreinte bloc n-2

bloc n

empreinte bloc n-1

bloc n + 1

empreinte bloc n

≠

empreinte bloc falsifié

hashage

hashage

- Equihash
- Ethash
- Hashcash

Code d'Armor

problème 2

Comment un bloc est créé et ajouté à la chaîne ?

Crédit : *Pere Castor*, France 3, Canal J

⛏ Une histoire de minage...

1. Création d'un bloc "en local" par un **mineur**, avec entre autres :
   - hash bloc précédent
   - arbre des transactions
   - horodatage
   - **difficulté**
   - **nonce**

2. Avoir une **empreinte** du bloc inférieure à la difficulté en fonction du *nonce*

⛏ Une histoire de minage...

1. Création d'un bloc "en local" par un **mineur**, avec entre autres :
   - hash bloc précédent
   - arbre des transactions
   - horodatage
   - **difficulté**
   - **nonce**
2. Avoir une **empreinte** du bloc inférieure à la difficulté en fonction du *nonce*

grosse puissance de calcul

très grand nombre réajusté tous les X blocs

grand nombre à trouver nombre (32 bits, ...)

via une fonction de hashage bien velue

⛏ Une histoire de minage...

1. Création d'un bloc "en local" par un **mineur**, avec entre autres :
   - hash bloc précédent
   - arbre des transactions
   - horodatage
   - **difficulté**
   - **nonce**

grosse puissance de calcul

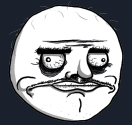
très grand nombre réajusté tous les X blocs

grand nombre à trouver nombre (32 bits, ...)

via une fonction de hashage bien velue

2. Avoir une **empreinte** du bloc inférieure à la difficulté en fonction du *nonce*

➔ Trouver le *nonce* qui convient...



Code d'Armor

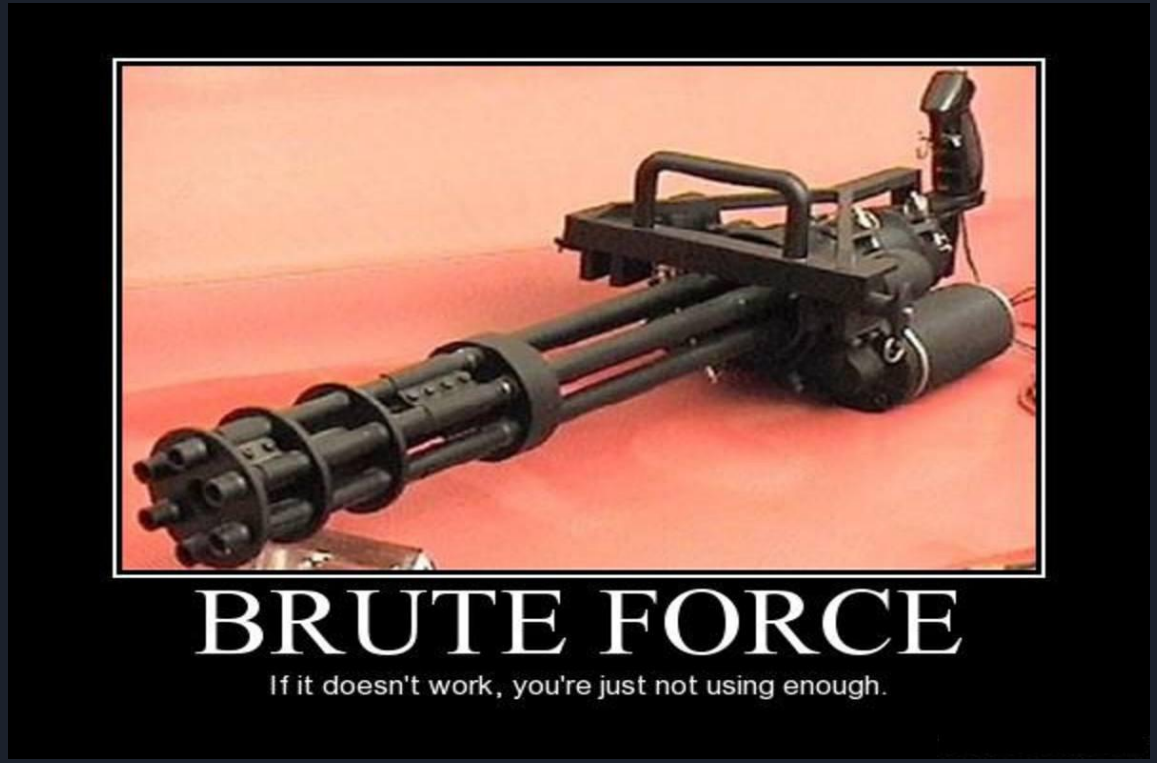
problème 3

Comment trouver le bon *nonce* ?

Crédits : *Il était une fois la vie,* RTBF, France 3, Canal +

Code d'Armor

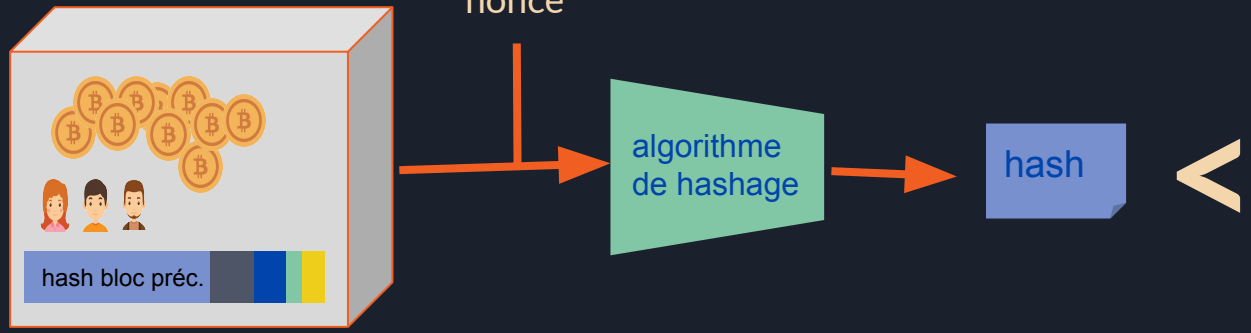
… et de consensus !



… et de consensus !

le “golden nonce”

➔ Trouver le **bon nombre** qui, hashé avec tout le reste du bloc, donne un hash inférieur à la difficulté



- 28/11/2017
- Difficulté BTC **1 347 001 430 559**
- Difficulté ETH **1 517 248 303 437 386**
- Difficulté ZEC **5 914 699**
- bitinfocharts.com

- Proof Of Work
- Proof Of Stake
- Zero-knowledge Proof

Code d'Armor

problème 3

Du coup, quel est l'intérêt pour moi d'ajouter le nouveau bloc ?

Le mineur vainqueur remporte...

➔ les frais de transactions (variables)

➔ une récompense (fixe)

- 12.5 BTC
- 12.5 BCH
- 12.5 BTG
- 25 LTC
- 12.5 ZEC
- 3 ETH
- 5 ETC
- 5.79 XMR

- 28/11/2017
- Récompense en cryptomonnaie diminue naturellement en fonction du nombre de blocs minés
- bitinfocharts.com

Code d'Armor

problème 4

Comment je peux miner ?

Crédit : *Matrix Revolutions*, 2003, Warner Bros

Code d'Armor

Comment miner ?

- Miner tout seul, dans son coin
  - avoir un bon CPU et/ou un bon GPU
  - investir dans des cartes graphiques dédiées

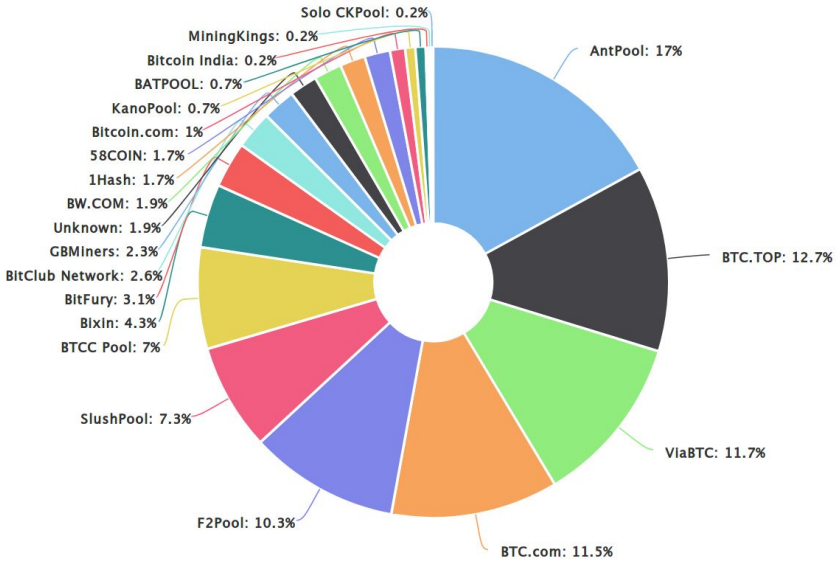
- température
- consommation électrique
- bruit
- plus très rentable en 2017 pour certaines cryptomonnaies

- Field-Programmable Gate Array
- Application-Specific Integrated Circuit

- P2Pool
- cgminer
- GUIMiner

Comment miner ?

- Passer par des *mining pools*
  - fédérer des mineurs
  - se répartir les récompenses obtenues



blockchain.info/pools

9/11/2017

Code d'Armor

Comment miner ?

- Passer par du *cloud mining*
  - fonctionnement par abonnement (souvent)
  - souscription pour un nombre de hash / seconde

- aucune garantie de miner des blocs
- aucune garantie de gagner de la cryptomonnaie
- aucune garantie que ce ne soit pas une arnaque

C'est le "Qui perd perd", vous jouez maintenant avec votre argent - Coluche

Code d'Armor

Comment miner ?

- Miner chez les autres, frauduleusement
  - prendre un outil innocent...
  - ...et l'exécuter chez les autres
  - avec leur puissance de calculs

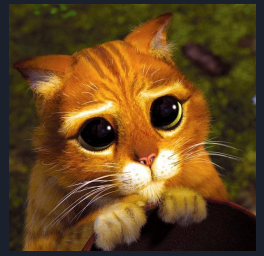
- pas très légal tout ça...
- pas très discret non plus

- En 2017, le compte CloudFlare de la société Coinhive a été piraté
- Des pirates ont récupéré pour eux les unités Monero gagnées via les sites web où Coinhive était en place

- coinhive.com
- coin-hive GitHub

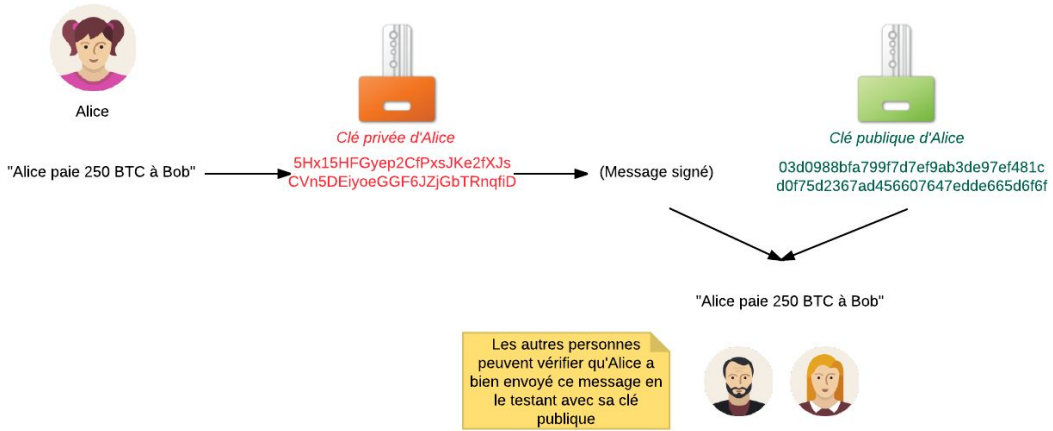
Code d'Armor

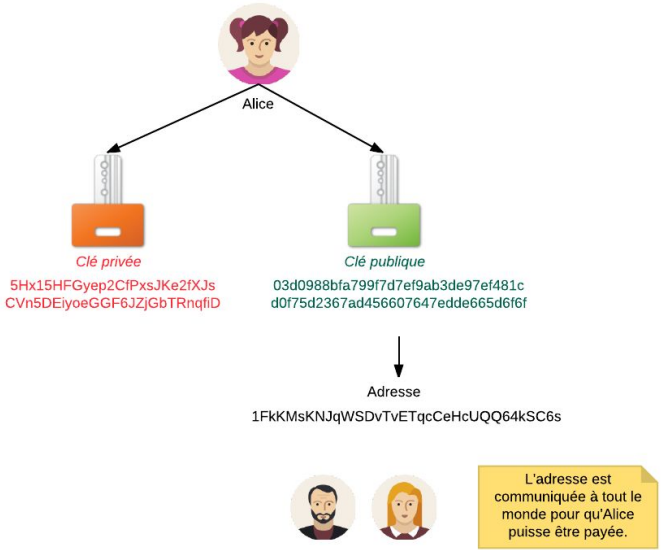
Mais, mais...



Pas plus de détails ?

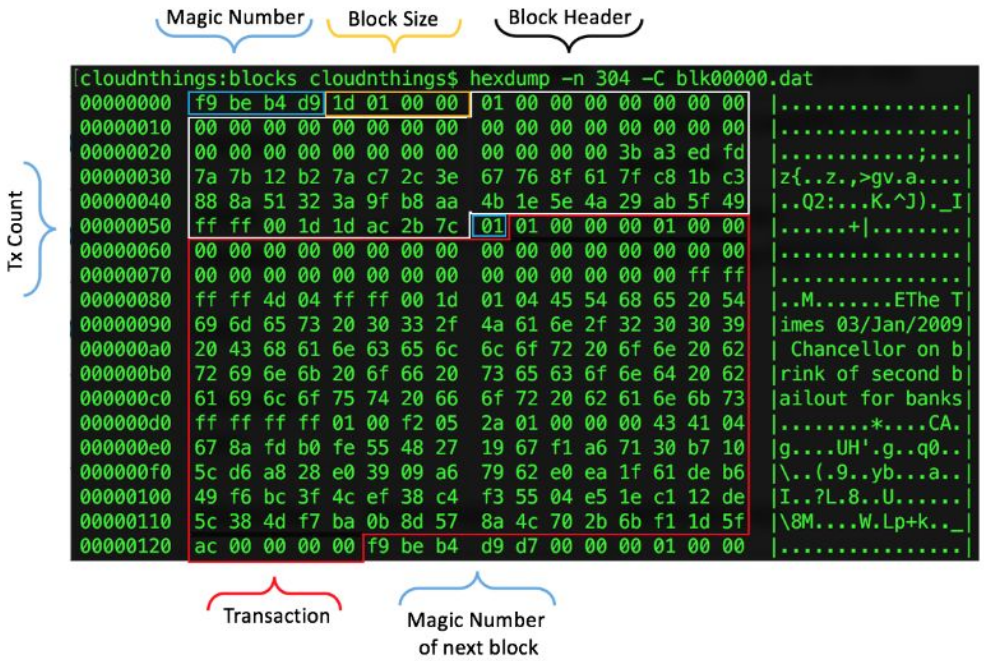
Du chiffrement asymétrique ?

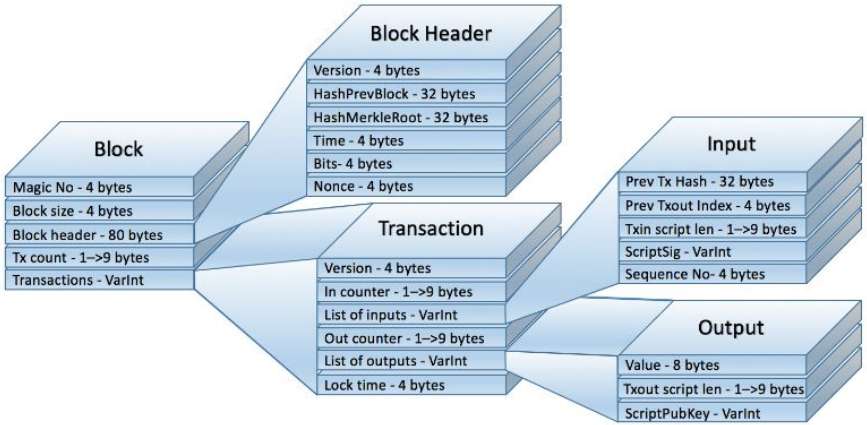




d'après Mathieu Nebra, Open Classrooms

Disséquons un bloc





What's in a block?

Disséquons un bloc

Hauteur	Âge	Transactions	Total envoyé	Relayé par	Taille (kB)
493762	8 minutes	595	2,032.23 BTC	AntPool	187.72

ici, un gros *mining pool*

Bloc #493762

Sommaire	
Nombre de transactions	595
Somme des outputs	2,032.23026046 BTC
Volume estimé des transactions	283.15492128 BTC
Frais des transactions	0.60200435 BTC
Hauteur	493762 (Chaîne principale)
Date (timestamp)	2017-11-09 12:34:15
Date de réception	2017-11-09 12:34:15
Relayé par	AntPool
Difficulté	1,452,839,779,145.92
Morceaux	402702781
Taille	187.724 kB
Poids	707.819 kWU
Version	0x20000000
nonce	1357467478
Récompense du bloc	12.5 BTC

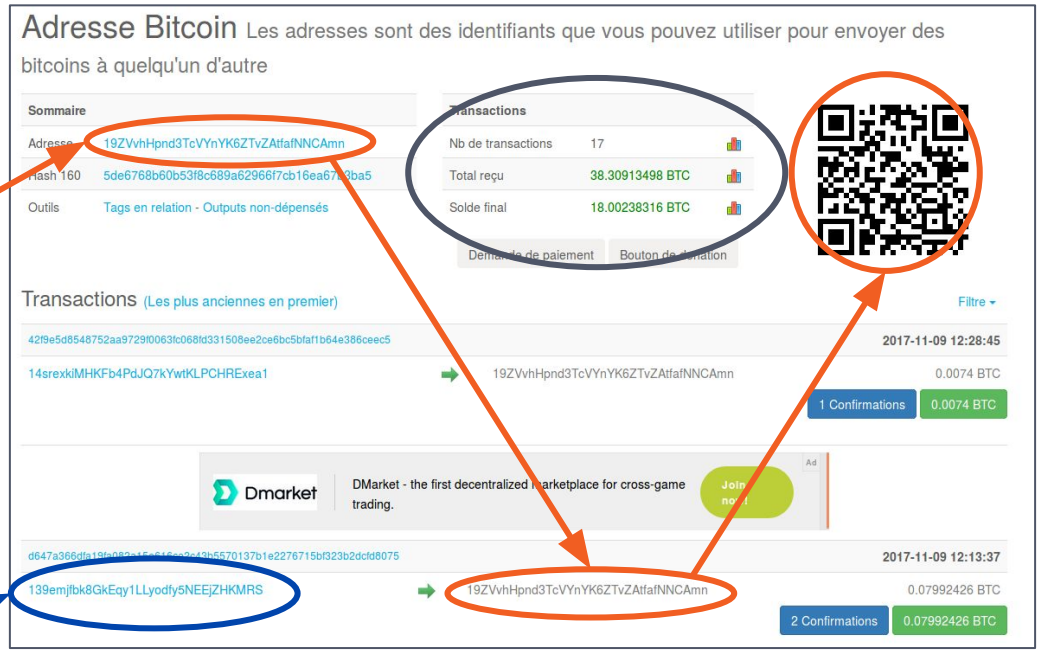
Hashes	
Hash	00000000000000000a7e15769268f5f66e3156e10d62e2dd5e0d04510790fba
Bloc précédent	00000000000000000acc1844bebaaaf68071d92e17f485b725a975f3aa875cd
Bloc(s) suivant(s)	
Merkle Root	[illegible]0f198c2e06b696bc71ba4827b8e32876fc7cc2b1d852bc8cb5b0f662eb

hash du bloc 493761

racine de l'arbre de Merkel

blockchain.info

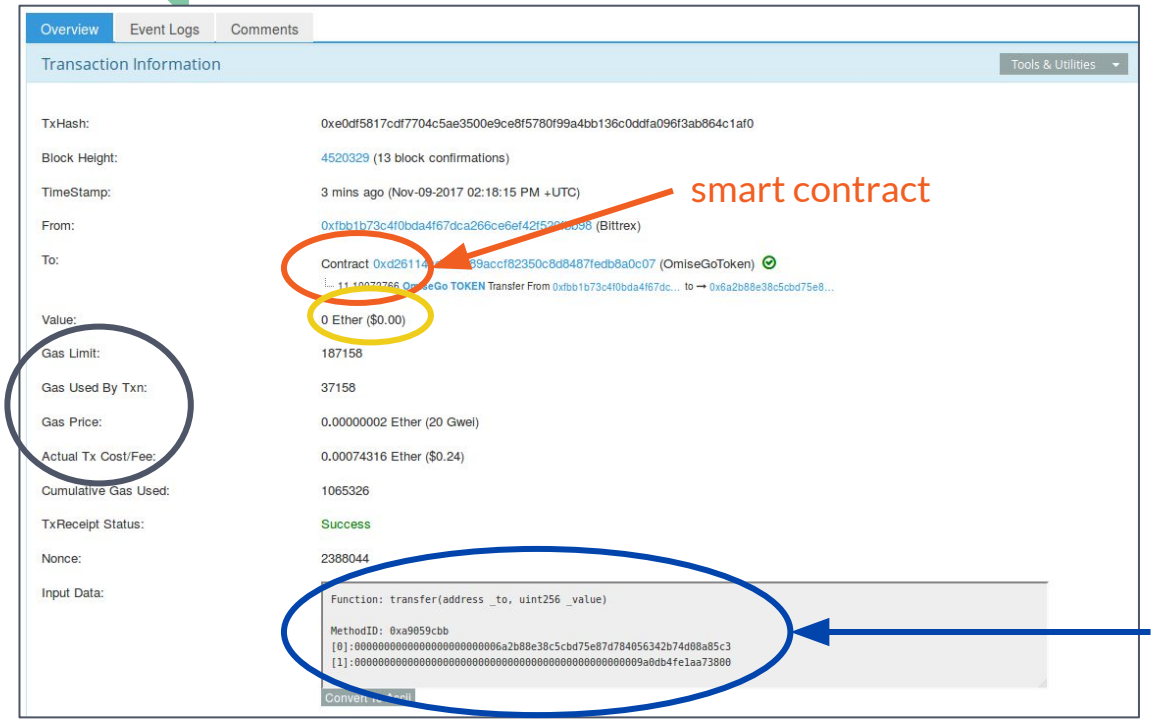
Disséquons une transaction



adresse envoyant des BTC

blockchain.info

Disséquons une transaction



etherscan.io

Des transactions en attente ?

- Les transactions ne sont pas *confirmed* automatiquement
- Pour éviter la double dépense, une attente est faite
  - ex: attendre d'avoir 6 blocks supplémentaires minés avant l'ajout de la transaction
- Les frais pour une transaction priorisent son ordre d'ajout

- blockchain.info
- bitcointicker.co

altcoins

Code d'Armor

Code d'Armor

Énormément de devises et tokens

- 28/11/2017
- 919 devises et 407 tokens recensés
- coinmarketcap.com

Avec plus ou moins de “valeur”


1 BTC ~ 9954 $


1 BCH ~ 1597 $


1 BTG ~ 350 $


1 XMR ~ 187 $


1 ETH ~ 476 $


1 ETC ~ 33 $


1 DASH ~ 623 $


1 ZEC ~ 350 $


1 LTC ~ 92 $


1 XRP = 0.267445 $


1 DOGE = 0.002032 $


1 ADC = 0.002949 $

- 28/11/2017
- coinmarketcap.com

Avec plus ou moins de “valeur”

1 GNT = 0.206636 $

1 REP = 28.57 $

1 GNO = 118.60 $

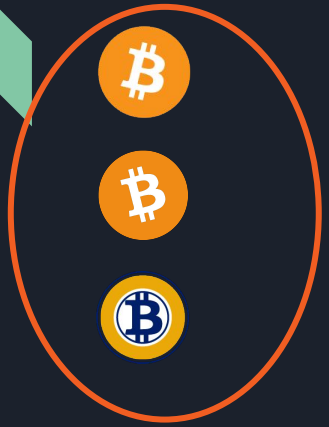
1 EOS = 2.93 $

1 SNT = 0.038051 $

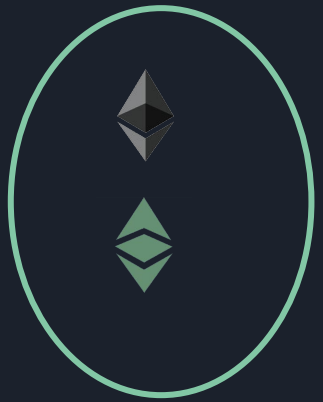
- 28/11/2017
- coinmarketcap.com

Code d'Armor

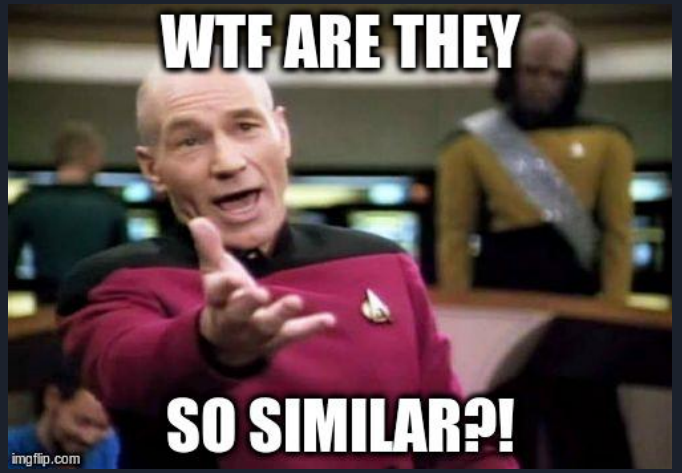
Et des conflits !



?



?



Code d'Armor

- 20/07/2017
- Adoption de SegWit par Bitcoin (BTC)
- Hard fork donnant Bitcoin Cash (BCH)

SegWit (*Segregated Witness*, BIP141) : permettrait de résoudre des problèmes de limitation de tailles de blocs qui impactent la vitesse des transaction en séparant chaque transaction en deux parties

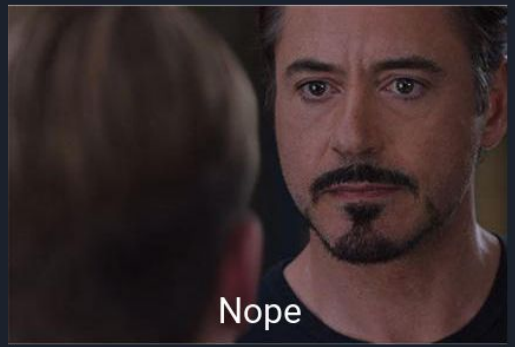
Hardfork : grosse variation de la blockchain, sans rétrocompatibilité, qui provoque une séparation en deux chaînes

Crédit : *Captain America: Civil War*, 2016, Marvel Studios

Code d'Armor

- Novembre 2017
- SegWit2X
- Hard fork ?

SUSPENDU



SegWit2x : avoir des blocs passant d'une taille de 1 Mo à une taille de 2Mo, toujours pour décongestionner le réseau

Hardfork : grosse variation de la blockchain, sans rétrocompatibilité, qui provoque une séparation en deux chaînes

Crédit : *Captain America: Civil War*, 2016, Marvel Studios

Code d'Armor

- Juillet 2016
- L'affaire *TheDAO*
- Le fond d'investissement *TheDAO* se fait voler presque 3 600 000 ETH
- Les devs d'Ethereum ont procédé à un hard fork pour annuler le vol, mais certains n'ont pas fait l'upgrade.

Le hard fork d'Ethereum a donné naissance à l'Ether Classique, ETC

Le braquage de *TheDAO* équivaut à la perte de plus de 10% du montal total de l'Ether.

Le cyber-casse du siècle, sans arme ni haine ni violence.

Crédit : *Dawn of Justice*, 2016, DC Entertainment

Ethereum, smart contract et Đapp

Code d'Armor

Code d'Armor

Ethereum ?

- Vitalik Buterin, 2013

- blockchains + cryptomonnaies
  - décentralisé
  - P2P
  - distribué
  - robustesse, intégrité

➔ et si on échangeait de la logique plutôt que des valeurs ?

Ethereum !

- Vitalik Buterin, 2013

- blockchains + cryptomonnaies
  - décentralisé
  - P2P
  - distribué
  - robustesse, intégrité

➔ et si on échangeait de la logique plutôt que des valeurs ?

= du code à mettre dans la blockchain !

Code d'Armor

Quels changements ?

- Utilisation d'une Ethereum Virtual Machine
- Les blocs contiennent les dernières transactions et les états des **programmes**

  = smart contracts
- L'exécution des programmes est contrainte via l'utilisation de **tokens** qui seront consommés

  ETH, GNT, EOS, ...

Code d'Armor

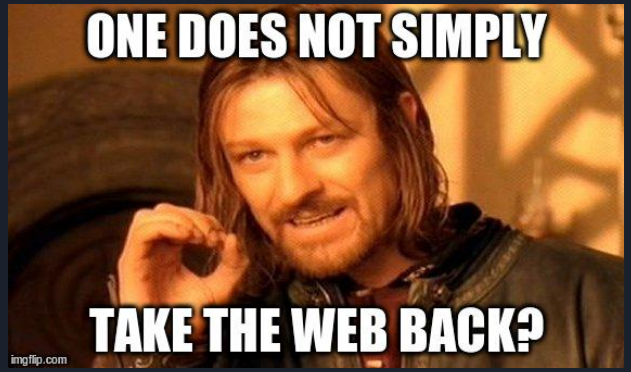
Ethereum, ce punk anar du web

- centralisé
- grands groupes = autorités
- fragile
- vulnérabilité
- sentiment de contrôle
- sentiment de sécurité
- panne = absence de service

- décentralisé, distribué
- individu = autorités
- incassable
- robuste
- davantage de contrôle / sécurité
- un noeud en panne ? ROFL

Code d'Armor

Ethereum, ce punk anar du web



No authorities to trust.

No centralisation to fail.

Just individuals cooperating under agreement for mutual benefit.

Code d'Armor

Vous aviez dit tokens ?

- ether - ETH
  - la monnaie de la blockchain

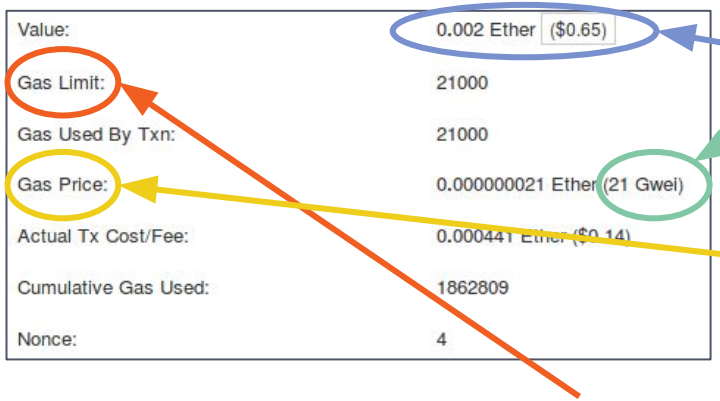
- gas
  - frais de transaction
  - chaque opération de calcul coûte du gas
  - quantité minimum par transaction
  - utilisé pour éviter d'impliquer la valeur de l'ether dans les transactions

- ether classic - ETC
  - la monnaie de l'autre blockchain

Ethereum gas price

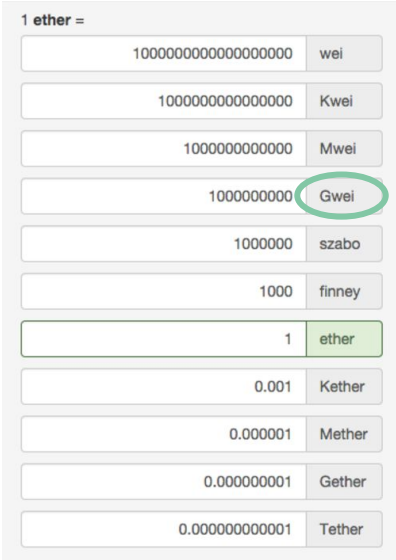
Ca sent le gaz...

Ether = Tx Fees = Gas Limit * Gas Price



coût final de la transaction, pour le mineur

wei = unité de mesure du gas price



- permet d'influencer le coût de la transaction
- plus c'est faible, moins la transaction est intéressante pour les mineurs, plus elle prendra de temps

la quantité de gas à consommer pour exécuter le code du smart contract, qui dépend de la quantité de code à exécuter par opération

- Ether, Gas limit, Gas price & fees
- Ethgasstation.info
- Ethereum gas how it works

Ethereum, smart contract et Đapp

Code d'Armor

Code d'Armor

Les smart contracts

- sont caractérisés par :
  - *address*
    - adresse permanente qui l'identifie
  - *balance*
    - pour exécuter le contrat, etc.
  - *fields*
    - modifiés par les méthodes
  - *methods*
    - fonctionnalités
  - *events*
    - éléments déclencheurs

d'après *Introduction to Ethereum*

Code d'Armor

Les smart contracts

- peuvent contenir du code
  - stocké dans des transactions
  - exécuté en fonction du gas limit
  - dans une EVM
  - écrit en Serpent, Solidity, Mutan
- si pas de code, ils sont vus comme des “comptes” de cryptomonnaie classiques
  - adresse, quantité d’ether
- restent dans la blockchain, mais peuvent mourir et avoir leur balance d’ether transférée

- Serpent lang
- Mutan lang
- Solidity lang

Les smart contracts

```
pragma solidity ^0.4.0;

contract Coin {
    // The keyword "public" makes those variables
    // readable from outside.
    address public minter;
    mapping (address => uint) public balances;

    // Events allow light clients to react on
    // changes efficiently.
    event Sent(address from, address to, uint amount);

    // This is the constructor whose code is
    // run only when the contract is created.
    function Coin() {
        minter = msg.sender;
    }

    function mint(address receiver, uint amount) {
        if (msg.sender != minter) return;
        balances[receiver] += amount;
    }

    function send(address receiver, uint amount) {
        if (balances[msg.sender] < amount) return;
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
        Sent(msg.sender, receiver, amount);
    }
}
```

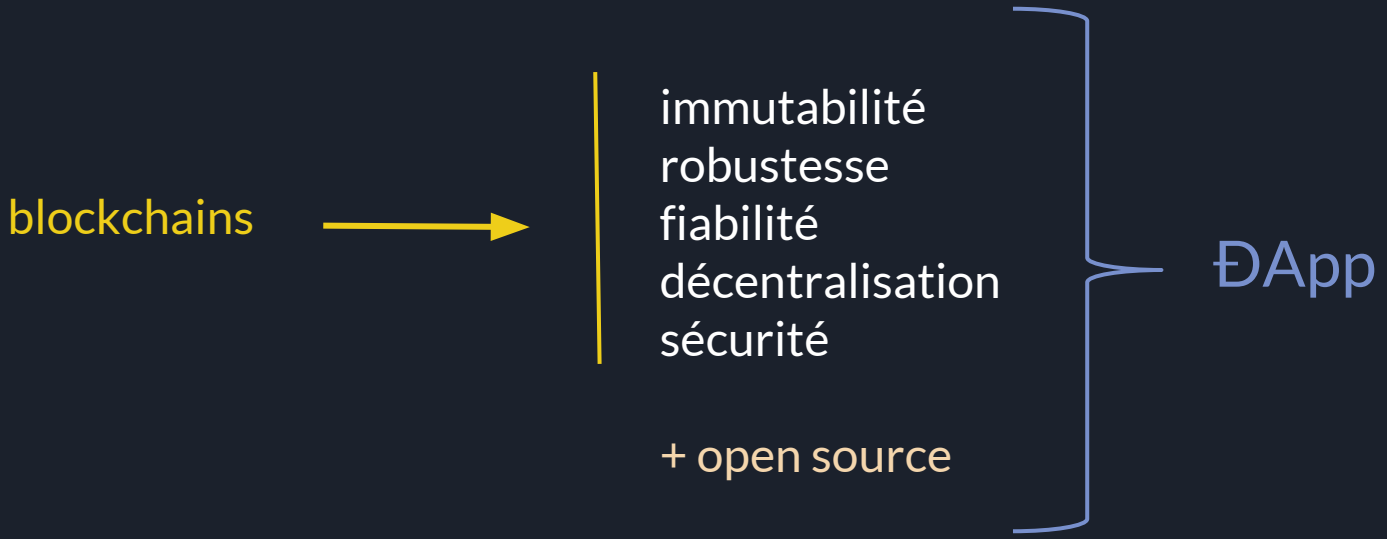
d'après *Introduction to Smart Contracts*

Ethereum, smart contract et Đapp

Code d'Armor

Pourquoi des Ðecentralized Apps ?

séquentiel | parallèle | distribué | décentralisé



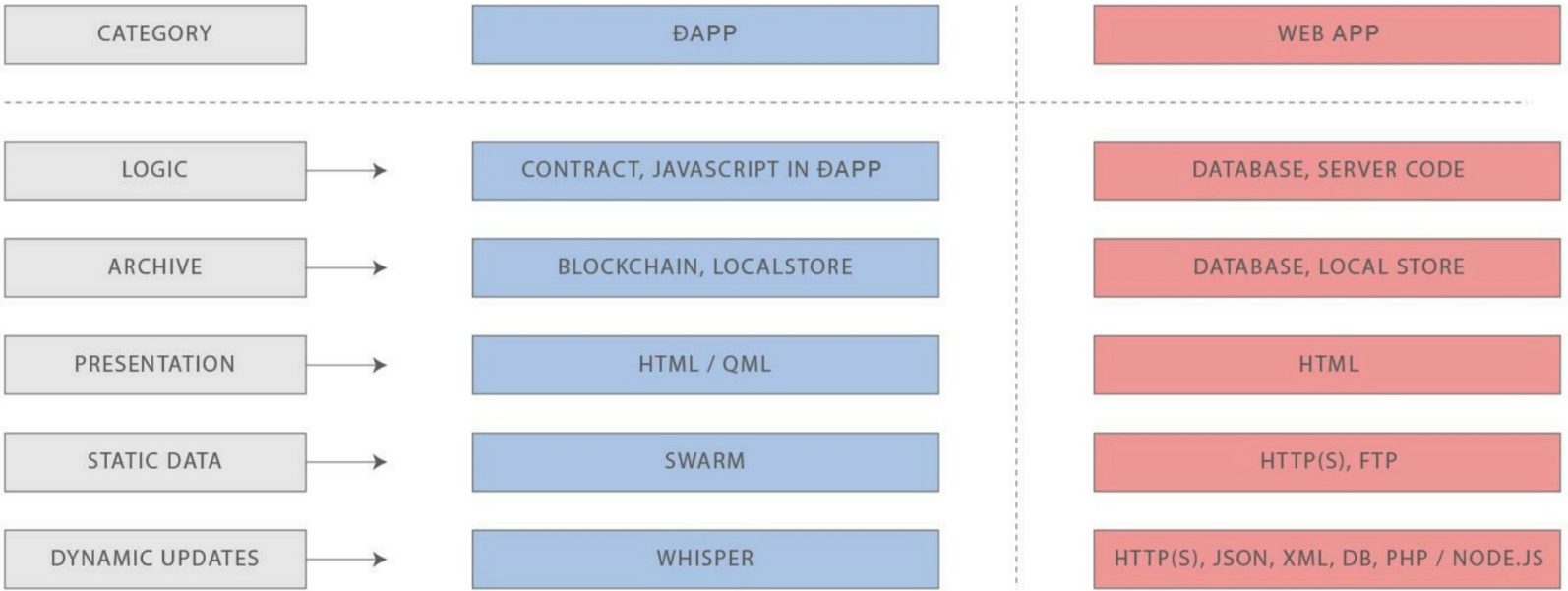
Code d'Armor

Des Đecentralized Apps pour quoi ?

- paiement
  - en cryptomonnaie
- authentification
  - stocker les *credentials* dans la blockchain
- stockage de données / logique sensibles
  - mais pas trop non plus
- traçabilité
  - avoir des logs et traces du passé
- ...

Les Đapps n'ont pas à avoir toute leur logique dans la blockchain

Comparaison ĐApp / WebApp



d'après *The Ethereum Experience*

Code d'Armor

Par où commencer ?

- Tutoriel *Ethereum France*
- Tutoriel *Dapps for beginners*
- Un autre tutoriel
- Un bon vieux gros wiki
- Faire un *Hello World*

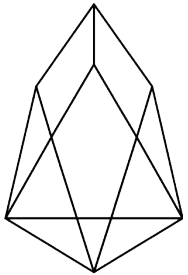
- Présentation d'Ethereum
- Introduction au Smart Contracts de Solidity
- Plein de références de ressources !

Des exemples de projets ?

Quelle plateforme utiliser ?

bitshares

hyperledger



eos

ethereum

Usages ?

Code d'Armor

Code d'Armor

Usages ?

Decentralized Autonomous Organization

Initial Coin Offering

monnaies locales

rémunération de projets open source

lutte contre les fake news

transfert de biens

billetterie

activités illégales

propriétés intellectuelles

chaînes de commandement

économie collaborative

traçabilité des produits

votes

stockage de fichiers

messagerie

spéculation

pérenniser des documents officiels

to be continued...

Usages ?

Organisation fonctionnant via un programme informatique, qui fournit des règles transparentes, immuables, inscrites dans une blockchain. Ne peut être arrêtée, fermée ou contrôlée.

Decentralized Autonomous Organization

Initial Coin Offering

Les ICO sont interdits dans plusieurs pays

monnaies locales

rémunération de projets open source

Fermetures de Silk road, Alphabay...

Publiq

transfert de biens

billetterie

dark web

propriétés intellectuelles

chaînes de commandement

économie collaborative

Connecting Food

Nous Citoyens

Swarm

Whisper

Mt. Gox

Piratage de +700000 BTC en 2014

pérenniser des documents officiels

to be continued...

Conclusion

Code d'Armor

Conclusion

- immense spéculation sur les cryptomonnaies, moins sur les tokens
- écosystème instable ou encore immature
  notamment autour de Bitcoin, Ethereum...
- tentatives des États d'interdir ou réguler les ICO et cryptomonnaies
- image encore mauvaise et incomprise des cryptomonnaies
- un **potentiel énorme** d'usages pour les blockchains et les **Đapps** !

#buzzwords

Jean-Michel Markéteu, *dernier tweet avant l'attaque de Skynet*, 2017

Code d'Armor

NO DOLLARS BUT TOKENS

NO CONTROL

Merci !

NO REGULATION

MORE PEOPLE LESS CONTROL

FREE WEB
FREE MONEY
FREE DAPPS

Chiffres

10

minutes sont nécessaires pour miner un bloc du réseau Bitcoin

Source : https://bitcoinplay.net/58-insane-facts-about-bitcoin/

81%

des opérations de hashage du réseau Bitcoin sont faits en Chine

Source : https://bitcoinplay.net/58-insane-facts-about-bitcoin/

90%

des adresses du réseau Bitcoin
ont moins de 0.1 BTC

Source : https://bitcoinplay.net/58-insane-facts-about-bitcoin/

2140

serait l’année où les 21 millions de BTC auront tous été minés

Source : https://bitcoinplay.net/58-insane-facts-about-bitcoin/

3994

Une transaction Bitcoin consomme 3994 fois plus d'énergie qu'une transaction par carte bancaire.

Octobre 2017

Source : https://bitcoinplay.net/58-insane-facts-about-bitcoin/

6354669

C’est le nombre de Terrahash par seconde du réseau Bitcoin.

Octobre 2017

Source : https://bitcoincharts.com/bitcoin/

95616012

de ETH en circulation
pour un maximum qui n’existe pas encore

9 Novembre 2017

Sources : bitinfocharts.com, https://www.quora.com/Is-there-a-limit-to-the-supply-of-Ethereum

16658740

de BTC en circulation
pour un maximum de 21 millions

9 Novembre 2017

Source : bitinfocharts.com

80704291

Octobre 2017

C’est le taux en PetaFLOPS pour les opérations de hashage du réseau Bitcoin.

Source : https://bitcoincharts.com/bitcoin/

Citations

Al Gore

“I’m a big fan of Bitcoin. Regulation of money supply needs to be depoliticized”

Source : https://bitcoincharts.com/bitcoin/

Bill Gates

"Bitcoin is a technological *tour de force*"

Source : https://bitcoincharts.com/bitcoin/

J. Assange

“Bitcoin actually has the balance and incentives right, and that is why it is starting to take off”

Source : https://bitcoincharts.com/bitcoin/

J. McAfee

“It will be everywhere, and the world will have to readjust.
World gouvernments will have to readjust”

Source : https://bitcoincharts.com/bitcoin/

T. Winklevoss

“We have elected to put our money and faith in a mathematical framework that is free of politics and human error”

Source : https://bitcoincharts.com/bitcoin/

Références

Code d'Armor

Références en vrac

Code d'Armor

- **Cryptomonnaies**
  - Audiocoin
    - http://www.audiocoin.eu/
  - Bitcoin
    - https://bitcoin.org/fr/
  - Bitcoin Cash
    - https://www.bitcoincash.org/
  - Bitcoin Gold
    - https://bitcoingold.org/
  - Dash
    - https://www.dash.org/
  - Dogecoin
    - http://dogecoin.com/
  - Ether
    - https://www.ethereum.org/
  - Ether classic
    - https://ethereumclassic.github.io/
  - Litecoin
    - https://litecoin.com/fr/
  - Monero
    - https://getmonero.org/
  - Zcash
    - https://z.cash/

Articles, vidéos et sites visités le 10/11/17

Références en vrac

Code d'Armor

➔ **Des outils bien pratiques !**

- CoinHive
  - https://github.com/cazala/coin-hive
  - https://coinhive.com/
- EOS
  - https://eos.io/
- Coindesk
  - https://www.coindesk.com/
- Realtime Bitcoin
  - http://realtimebitcoin.info/
- Blockchain.info
  - https://blockchain.info/
- Difficulty - Blockchain
  - https://blockchain.info/fr/charts/difficulty
- Global Bitcoin Nodes
  - https://bitnodes.earn.com/
- ZChain
  - https://explorer.zcha.in/statistics
- BitcoinWisdom
  - https://bitcoinwisdom.com/
- JSEcoin
  - https://jsecoin.com/
- Etherscan - Gas price
  - https://etherscan.io/chart/gasprice
- Ethereum Converter
  - https://converter.murkin.me/
- ETH Gas Station
  - https://ethgasstation.info/
- Solidity
  - https://github.com/ethereum/solidity
- ICO Alert
  - https://www.icoalert.com/

Articles, vidéos et sites visités le 10/11/17

Références en vrac

Code d'Armor

- **Cryptomonnaie, minage et pièces virtuelles**
  - Crypto monnaie : la Chine bannit les levées de fonds, le cours de l'ether plonge
    - http://www.numerama.com/business/286261-crypto-monnaie-la-chine-bannit-les-levees-de-fonds-le-cours-du-bitcoin-chute.html
  - Bitcoin : un patch non sans heurts
    - http://www.zdnet.fr/actualites/bitcoin-un-patch-non-sans-heurts-39856020.htm
  - Le minage
    - http://blogchain.fr/minage/
  - Comprendre le Bitcoin et la Blockchain
    - https://openclassrooms.com/courses/comprendre-le-bitcoin-et-la-blockchain
  - Bitcoin Cash: Why It's Forking the Blockchain And What That Means
    - https://www.coindesk.com/coindesk-explainer-bitcoin-cash-forking-blockchain/
  - Bitcoin : SegWit ou Lightning Network pour fluidifier les transactions ?
    - https://www.nextinpact.com/news/104494-bitcoin-segwit-ou-lightning-network-pour-fluidifier-transactions.htm
  - Bitcoin Cash : un fork controversé pour fluidifier les transactions
    - https://www.nextinpact.com/news/104873-bitcoin-cash-fork-controverse-pour-fluidifier-transactions.htm
  - Bitcoin & Bitcoin Cash : le fork de la crypto monnaie a bien eu lieu
    - http://www.numerama.com/tech/280098-bitcoin-bitcoin-cash-le-fork-de-la-crypto-monnaie-de-reference-est-en-cours.html
  - Crypto monnaies, tokens et DAO : comment jouer en bourse avec les entreprises Ethereum
    - http://www.numerama.com/business/272643-crypto-monnaies-tokens-et-dao-comment-jouer-en-bourse-avec-les-entreprises-de-lethereum.html
  - Bitcoin, Ethereum, LiteCoin... : comment fonctionnent les crypto-monnaies ?
    - http://www.numerama.com/business/272280-bitcoin-ethereum-litecoin-quest-ce-quune-crypto-monnaie.html
  - Comment la blockchain changera le visage de l'entreprise
    - http://www.numerama.com/business/271155-comment-la-blockchain-changera-le-visage-de-lentreprise.html
  - Générer des bitcoins
    - https://bitcoin.fr/minage/
  - Life Inside a Secret Chinese Bitcoin Mine
    - https://www.youtube.com/watch?v=K8kua5B5K3I
  - 360° Chinese Bitcoin Mine - Brit Lab - BBC Future
    - https://www.youtube.com/watch?v=d5PJnDi_uGA
  - What is Bitcoin Mining?
    - https://www.youtube.com/watch?v=GmOzih6I1zs
  - Les limites de bitcoin
    - https://bitcoin.fr/les-limites-de-bitcoin/

Articles, vidéos et sites visités le 10/11/17

Références en vrac

Code d'Armor

- **Cryptomonnaie, minage et pièces virtuelles**
  - 2016 Blockchain Ecosystem Market Map
    - http://firstpartner.net/content/2016-blockchain-ecosystem-market-map
  - BlogChain
    - http://www.blogchain.fr/
  - What's in a block?
    - https://www.linkedin.com/pulse/whats-block-sean-au
  - Bitcoin Scalability Solutions
    - https://lightning.network/lightning-network-presentation-sfbitcoinsocial-2015-05-26.pdf
  - Bitcoin, sa blockchain et ses concepts, un monde d'opportunités
    - https://fr.slideshare.net/vincent63/introduction-a-bitcoin-while-42-vincent-gauthier-slideshare
  - Bitcoin : comment ça marche et pourquoi c'est une révolution
    - https://fr.slideshare.net/straumat/bitcoin-comment-a-marche-et-pourquoi-cest-une-rvolution
  - Introduction au Bitcoin
    - https://fr.slideshare.net/hetic/hetic-event-bitcoin101victor-mertz20140328
  - Introduction aux crypto-monnaies : Bitcoin, Ethereum, DAO, ICO, smart contracts
    - http://www.frandroid.com/crypto-monnaie/455178_tout-ce-que-vous-devez-savoir-sur-les-crypto-monnaies-bitcoin-ethereum-dao-ico-smart-contracts
  - Crypto-monnaie : de la Chine à l'île de Man, les ICO cherchent une terre d'accueil
    - https://www.nextinpact.com/news/105136-crypto-monnaies-de-chine-a-ile-man-ico-cherchent-terre-daccueil.htm
  - Imaginons la première monnaie numérique consacrée à la presse et aux médias
    - https://medium.com/humanoid-content/r%C3%A9flexion-et-si-la-cryptomonnaie-sauvait-les-m%C3%A9dias-8a05b950757b
  - What is a Bitcoin fork?
    - https://blog.coinbase.com/what-is-a-bitcoin-fork-cba07fe73ef1
  - Utopia : Björk va offrir de la crypto-monnaie aux auditeurs de son nouvel album
    - http://www.numerama.com/pop-culture/303240-utopia-le-prochain-album-de-bjork-donnera-droit-a-des-crypto-monnaies-pour-ses-acquereurs.html
  - 62 Insane Facts About Bitcoin
    - https://bitcoinplay.net/58-insane-facts-about-bitcoin/
  - Why Bitcoin Matters
    - https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/?_php=true&_type=blogs&_php=true&_type=blogs&ref=marcandreessen&_r=1&
  - What does a hard fork or soft fork mean for Bitcoin and Ethereum ?
    - http://bcmy.io/blog/what-does-a-hard-fork-or-soft-fork-mean-for-bitcoin-and-ethereum/

Articles, vidéos et sites visités le 10/11/17

Références en vrac

Code d'Armor

- **Cryptomonnaie, minage et pièces virtuelles**
  - Les confessions d'un mineur de bitcoin
    - https://bitcoin.fr/Les-confessions-d-un-mineur-de-bitcoin/#main
  - Parole de mineur
    - https://bitcoin.fr/Parole-de-mineur/#main
  - Blockchains La Deuxième révolution numérique
    - https://www.lesechos.fr/29/04/2016/LesEchosWeekEnd/00029-009-ECWE_blockchains-la-deuxieme-revolution-numerique.htm
  - Qu'est-ce que la blockchain ?
    - https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/
  - Le lexique de la blockchain
    - https://blockchainfrance.net/le-lexique-de-la-blockchain/
  - Qu'est-ce qu'un smartphone blockchain ? Du rêve impossible à la révolution des usages
    - http://www.numerama.com/tech/296090-quest-ce-quun-smartphone-blockchain-du-reve-impossible-a-la-revolution-des-usages.html
  - 20 citations pour expliquer le Bitcoin
    - http://www.thebitcoin.fr/20-citations-expliquer-comprendre-bitcoin/
  - Citations sur le Bitcoin
    - http://achat-bitcoins.com/citations-bitcoin/
  - Bitcoin - The security of transaction block chains
    - https://youtu.be/8zgvzmKZ5vo
  - Why is My Bitcoin Transaction Pending for So Long?
    - https://99bitcoins.com/why-bitcoin-transaction-pending-bitcoin-fees/
  - What is the Bitcoin Mempool ?
    - https://99bitcoins.com/what-is-bitcoin-mempool/
  - Bitcoin Fees Explained - Are Bitcoin Transaction Actually Free ?
    - https://99bitcoins.com/bitcoin-fees-explained

Articles, vidéos et sites visités le 10/11/17

Références en vrac

Code d'Armor

- **Đapps, Web 3.0 et smart contracts**
  - Dapps And The Decentralized Future
    - https://blockgeeks.com/guides/dapps-the-decentralized-future/
  - Is EOS the Ethereum killer?
    - https://medium.com/chain-cloud-company-blog/is-eos-the-ethereum-killer-ad24277d8c9c
  - Introduction to Smart Contracts
    - http://solidity.readthedocs.io/en/develop/introduction-to-smart-contracts.html
  - How Decentralized Applications Could bring the Blockchain to New Industries
    - https://bitcoinmagazine.com/articles/how-decentralized-applications-could-bring-the-blockchain-to-new-industries-1455324259/
  - Qu'est-ce qu'une DAO ?
    - https://blockchainfrance.net/2016/05/12/qu-est-ce-qu-une-dao/
  - Implementing a Hypothetical Currency Application on EOS
    - https://steemit.com/eos/@eosio/implementing-a-hypothetical-currency-application-on-eos
  - district0x
    - https://district0x.io/
  - Golem
    - https://golem.network/
  - Aragon
    - https://aragon.one/
  - Gnosis
    - https://gnosis.pm/
  - Augur
    - https://augur.net/
  - UJO Music
    - https://ujomusic.com/
  - Status
    - https://status.im/
  - uPort
    - https://www.uport.me/
  - Le smart contract ou contrat intelligent est-il un contrat ?
    - https://www.legitech.lu/newsroom/articles/smart-contract-contrat-intelligent-contrat/

Articles, vidéos et sites visités le 10/11/17

Références en vrac

Code d'Armor

- **Ethereum**
  - Ethereum
    - https://www.ethereum.org/
  - The Ethereum Experience
    - https://fr.slideshare.net/ethereum/the-ethereum-experience
  - Introduction to Ethereum
    - https://fr.slideshare.net/TerekJudi/introduction-to-ethereum-54481303
  - Ethereum France
    - https://www.ethereum-france.com/
  - Ethereum : tout savoir sur la crypto-monnaie et ses contrats intelligents
    - http://www.numerama.com/business/272641-ethereum-tout-savoir-sur-la-crypto-monnaie-et-ses-contrats-intelligents.html
  - Create a cryptocurrency contract in Ethereum
    - https://www.ethereum.org/token
  - Create a Hello World contract in ethereum
    - https://www.ethereum.org/greeter
  - Ethereum: Ether, Ether Gas, Gas Limit, Gas Price & Fees
    - https://coinsutra.com/ethereum-gas-limit-gas-price-fees/
  - Ethereum “Gas” - How it Works
    - https://steemit.com/ethereum/@tomshwom/ethereum-gas-how-it-works

Articles, vidéos et sites visités le 10/11/17

Références en vrac

Code d'Armor

➔ Divers

- Bitcoin: A Peer-to-Peer Electronic Cash System
  - https://bitcoin.org/bitcoin.pdf
- Coinbase : pour bien débuter dans le monde des Bitcoin, Ethereum et Litcoin
  - https://medium.com/@ulrichrozier/coinbase-pour-bien-d%C3%A9buter-dans-le-monde-des-bitcoin-ethereum-et-litcoin-76ae9cb1c30b
- Je me lance dans le cloud-minage d'Ethereum (ETH)
  - https://medium.com/@ulrichrozier/je-me-lance-dans-le-cloud-minage-dethereum-eth-d62d8d6aaab9
- How To Buy Bitcoins
  - https://howtobuybitcoins.info
- La Maison du Bitcoin
  - https://lamaisondubitcoin.fr/
- Follow My Vote
  - https://followmyvote.com/
- Blockchains La Deuxième révolution numérique
  - https://www.lesechos.fr/29/04/2016/LesEchosWeekEnd/00029-009-ECWE_blockchains-la-deuxieme-revolution-numerique.htm
- Qu'est-ce que la blockchain ?
  - https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/
- ENS Registrar
  - http://registrar.ens.domains/
- Bitcoin Gold : le Hard Fork de Bitcoin dont personne ne parle
  - https://journalducoin.com/bitcoin/bitcoin-gold-hard-fork-de-bitcoin-dont-personne-ne-parle/
- Journal du coin
  - https://journalducoin.com/
- BTCGPU
  - https://github.com/BTCGPU
- Nouvel algorithme "Equihash" : Vers un accès égal aux monnaies numériques
  - http://www.science.lu/fr/content/nouvel-algorithme-%C2%AB-equihash-%C2%BB-vers-un-acc%C3%A8s-%C3%A9gal-aux-monnaies-num%C3%A9riques
- SegWit2x annulé ! Le hard fork du bitcoin suspendu du fait de l'absence d'un consensus clair
  - https://www.crypto-france.com/segwit2x-annulation-hard-fork-bitcoin/
- Ethash
  - https://github.com/ethereum/wiki/wiki/Ethash
- Keccak Team
  - https://keccak.team/index.html
- Equihash
  - https://z.cash/blog/why-equihash.html
- Hashcash
  - https://en.bitcoin.it/wiki/Hashcash

Articles, vidéos et sites visités le 10/11/17