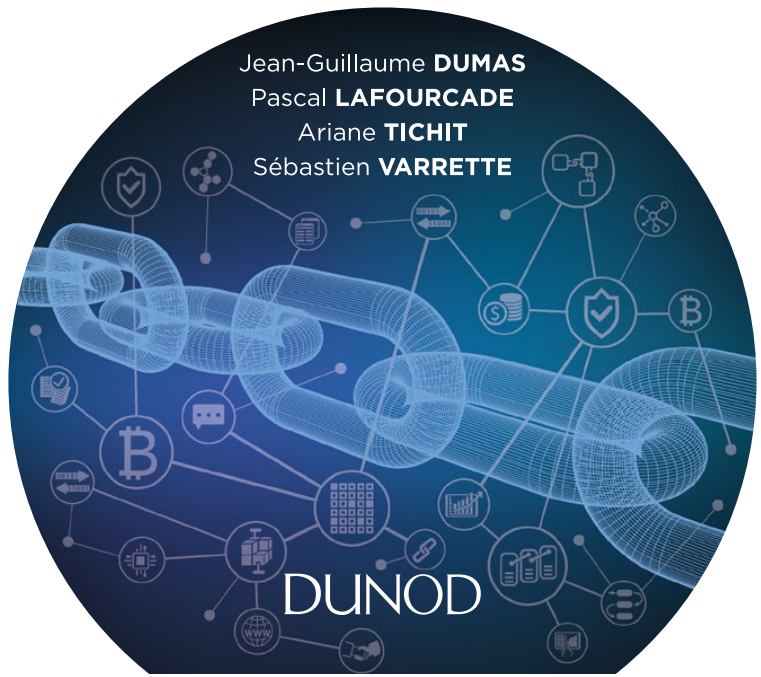
Les BLOCK CHAINS

EN 50 QUESTIONS

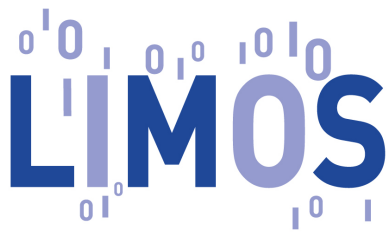
Comprendre le fonctionnement et les enjeux de cette technologie innovante



LIMOS
LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATIO

Bitcoin et la Blockchain

Pascal Lafourcade



Nice
Juin 2019

Plan

Plan

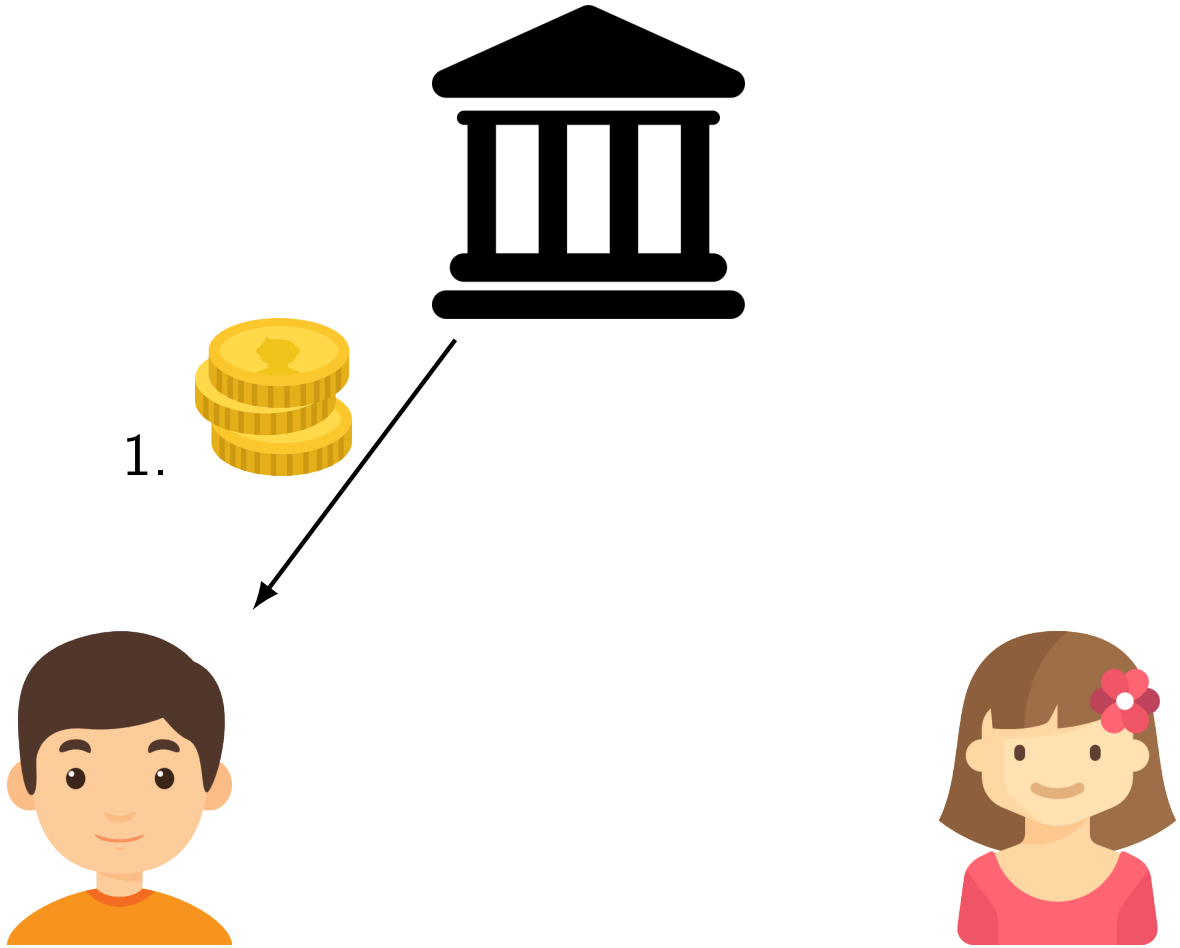
Sumériens vers 3.500 av J.C

Qu'est-ce que la monnaie?

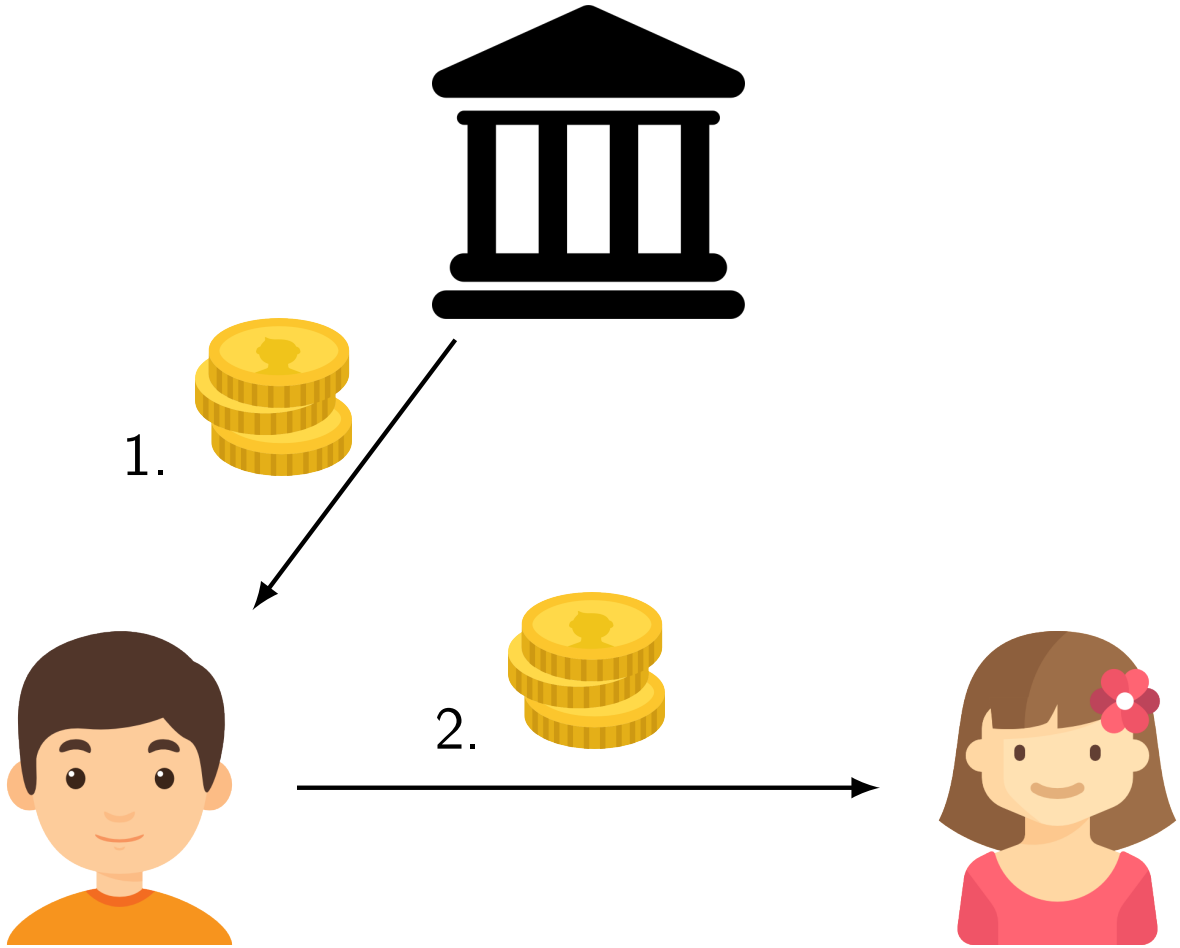
- Intermédiaire et moyens d'échanges de biens et services entre les individus
- Réserve de valeur
- Unité de compte

Nombreuses monnaies

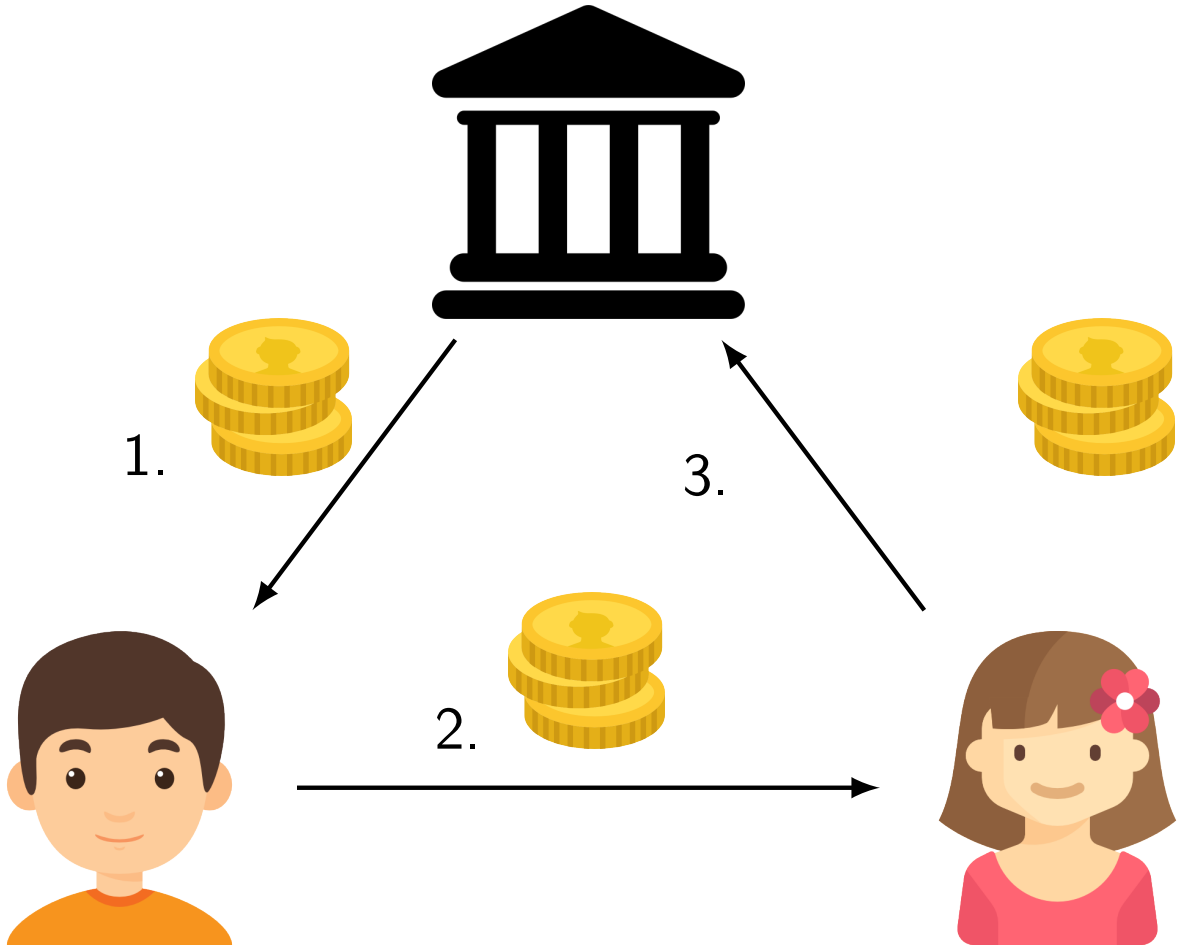
Principe : Banque centrale



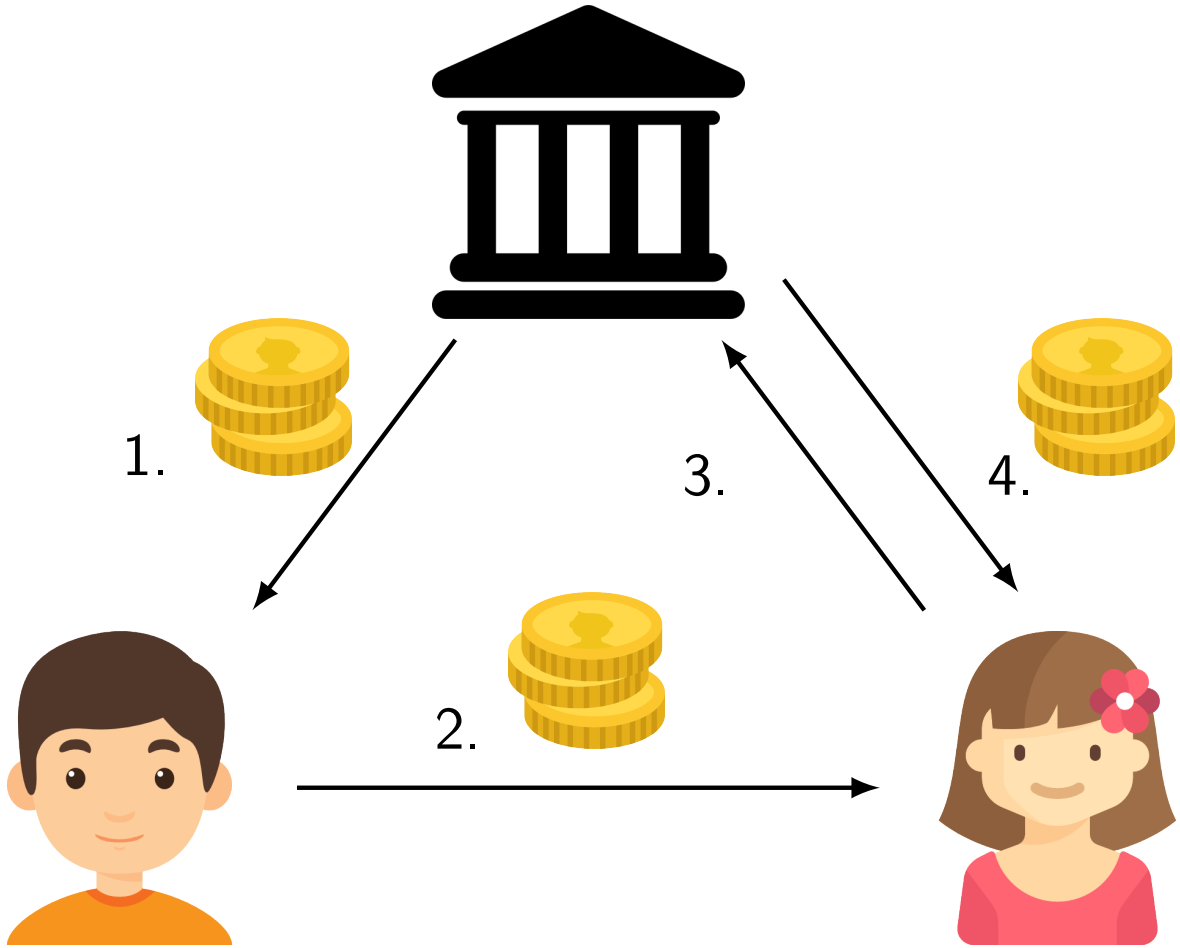
Principe : Banque centrale



Principe : Banque centrale



Principe : Banque centrale



1988 : Digitcash

Untraceable Electronic Cash †
(Extended Abstract)

David Chaum[1] *Amos Fiat*[2] *Moni Naor*[3]

[1] Center for Mathematics and Computer Science

[2] Tel-Aviv University

[3] IBM Almaden Research Center

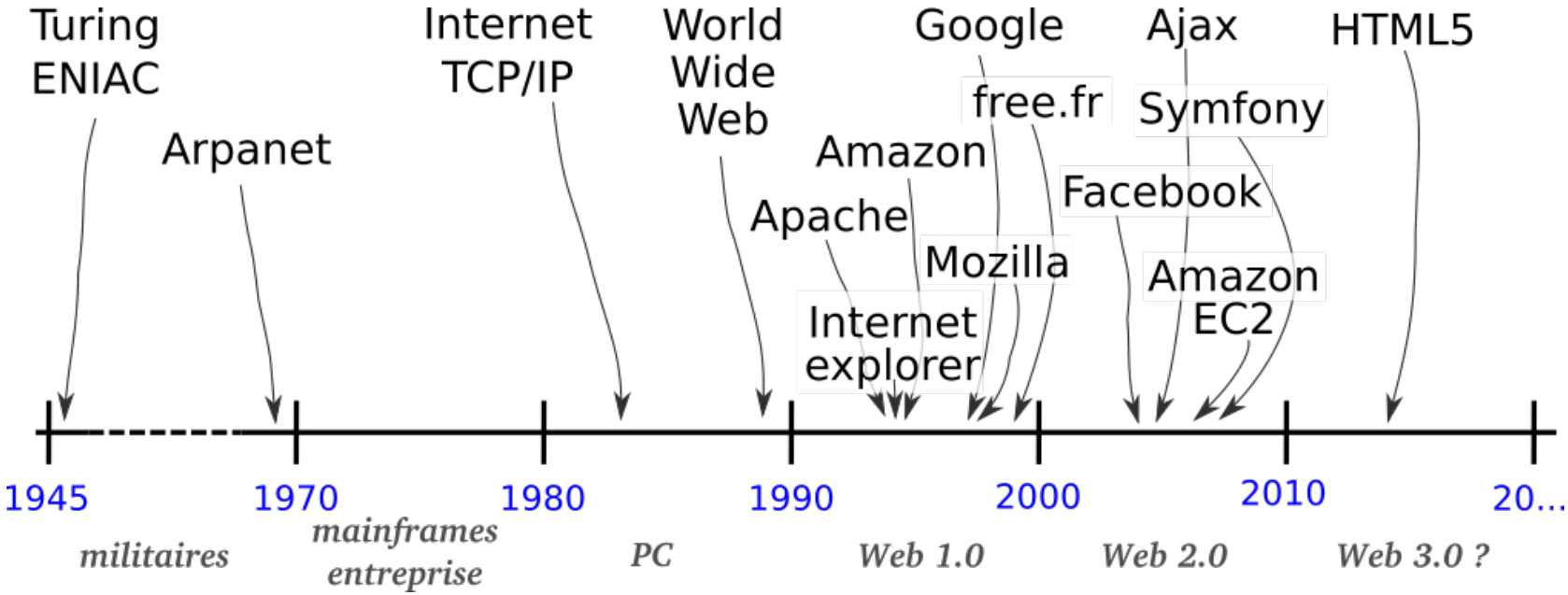
CRYPTO 1988

DigiCash™

David Chaum

- ☺ Préserve la vie privée
- 😐 À l'aide de primitives cryptographiques
- ☹ Nécessite toujours un tiers (banque)

Une idée visionnaire en avance sur son temps



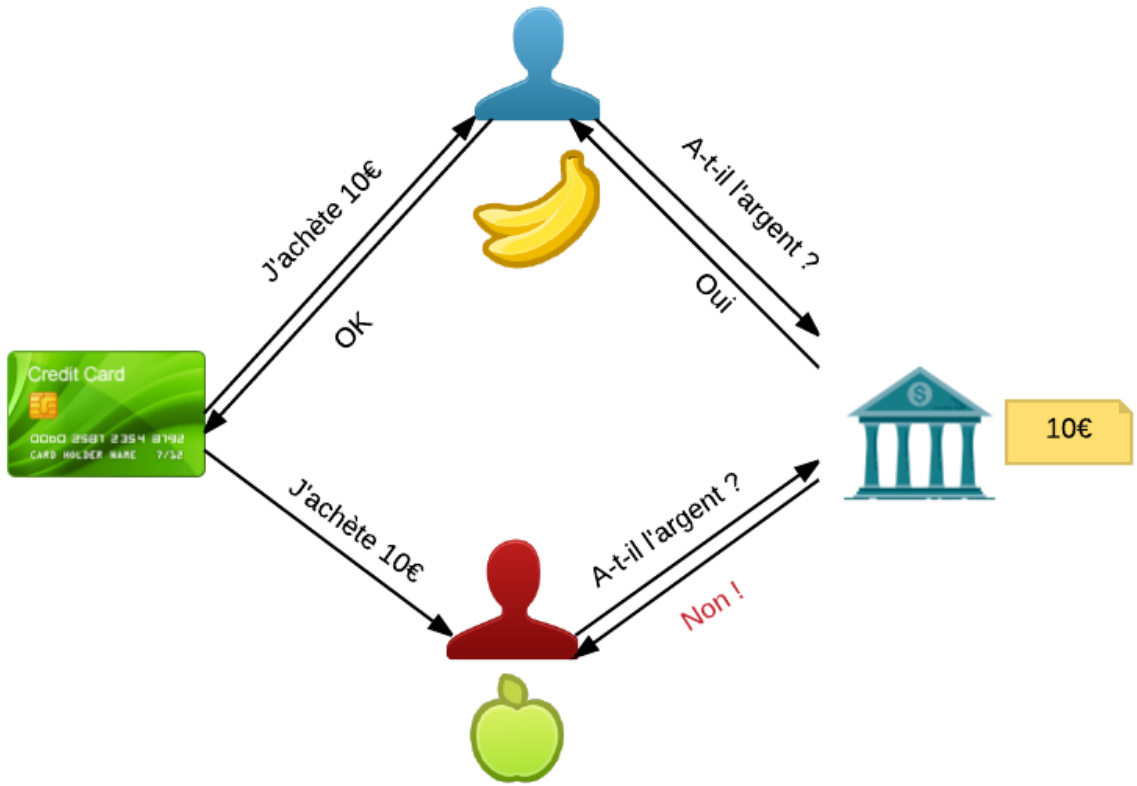
Crypto-monnaie

- Monnaie
  1. Intermédiaire et moyen d'échanges
  2. Réserve de valeur
  3. Unité de compte

- Crypto-monnaie : monnaie électronique, se passant d'un Tiers
  4. Respect de la vie privée
  5. Non-Falsifiable
  6. Éviter les doubles dépenses

Propriétés : Non-Falsifiable (Unforgeable)

Propriétés : Eviter la double dépense



- identifiation fraudeur

- "présemption d'innocence"

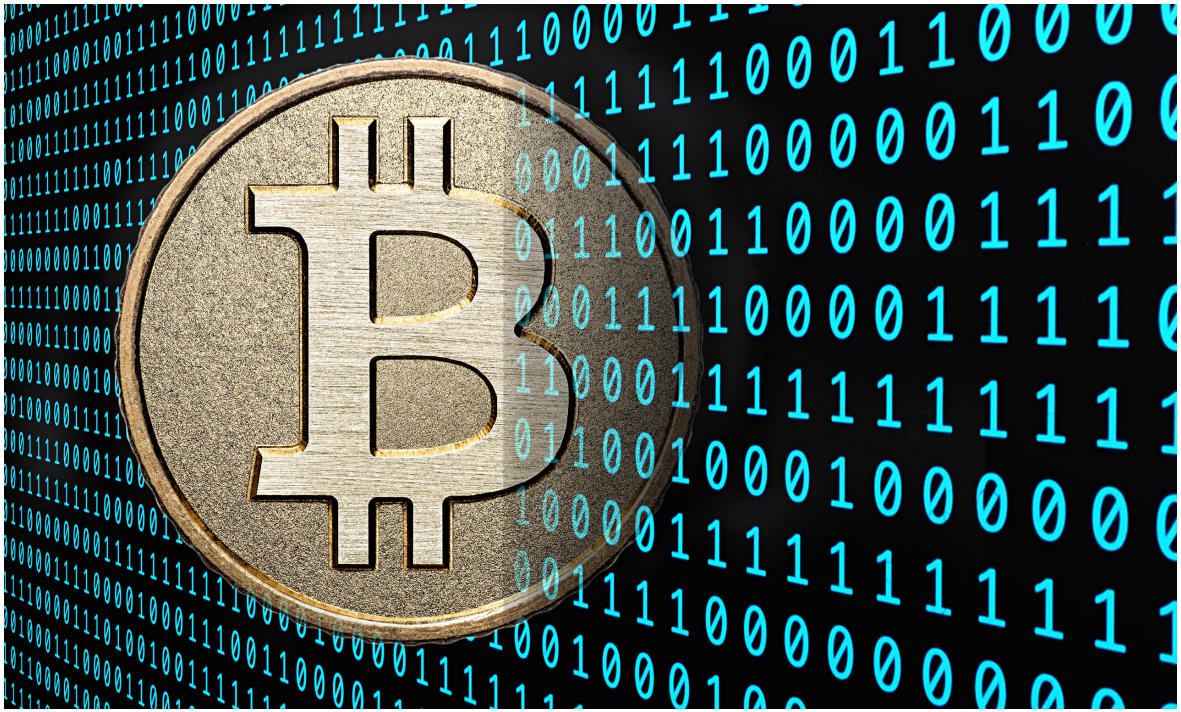
Propriétés : Respect de la vie privée

- Anonymat faible : non identification d'un acheteur
- Anonymat fort : non traçabilité d'un acheteur

Monnaies classiques et crypto-monnaies

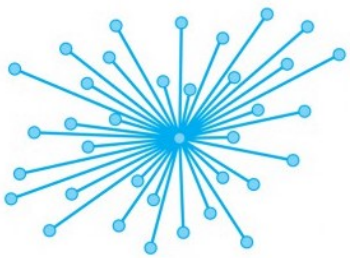
	Monnaie classique		Crypto-monnaie
	Liquide	Électronique	
Moyen d'échange	✓	✓	✓
Réserve de valeur	✓	✓	✓
Unité de compte	✓	✓	✓
Création	Banque centrale	Dette	Automatique
Vie privée	✓	✗	✓
Pair à pair	✗	✗	✓
Garantie légale, stabilisation	✓	✓	✗

La révolution Bitcoin 2009

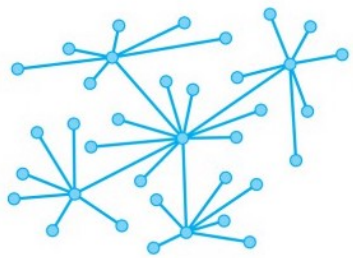


Bitcoin

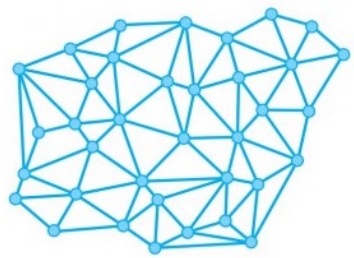
- Cryto-monnaie décentralisée et distribuée



Système centralisé



Système décentralisé

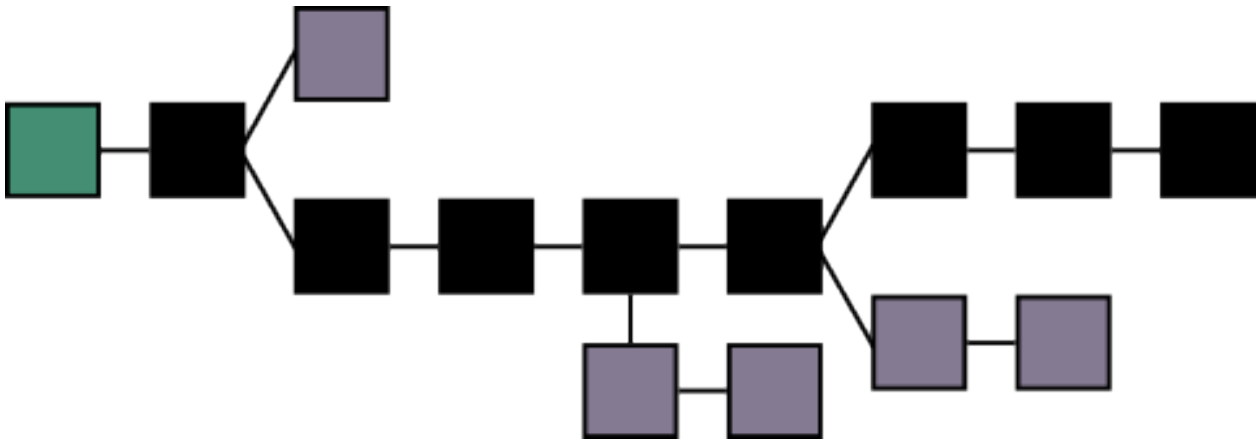


Système distribué

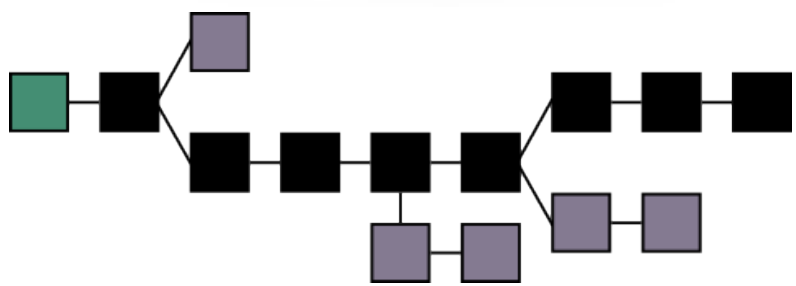
21 millions BTC

Inarrêtable car distribuée

Infalsifiable



Auditable

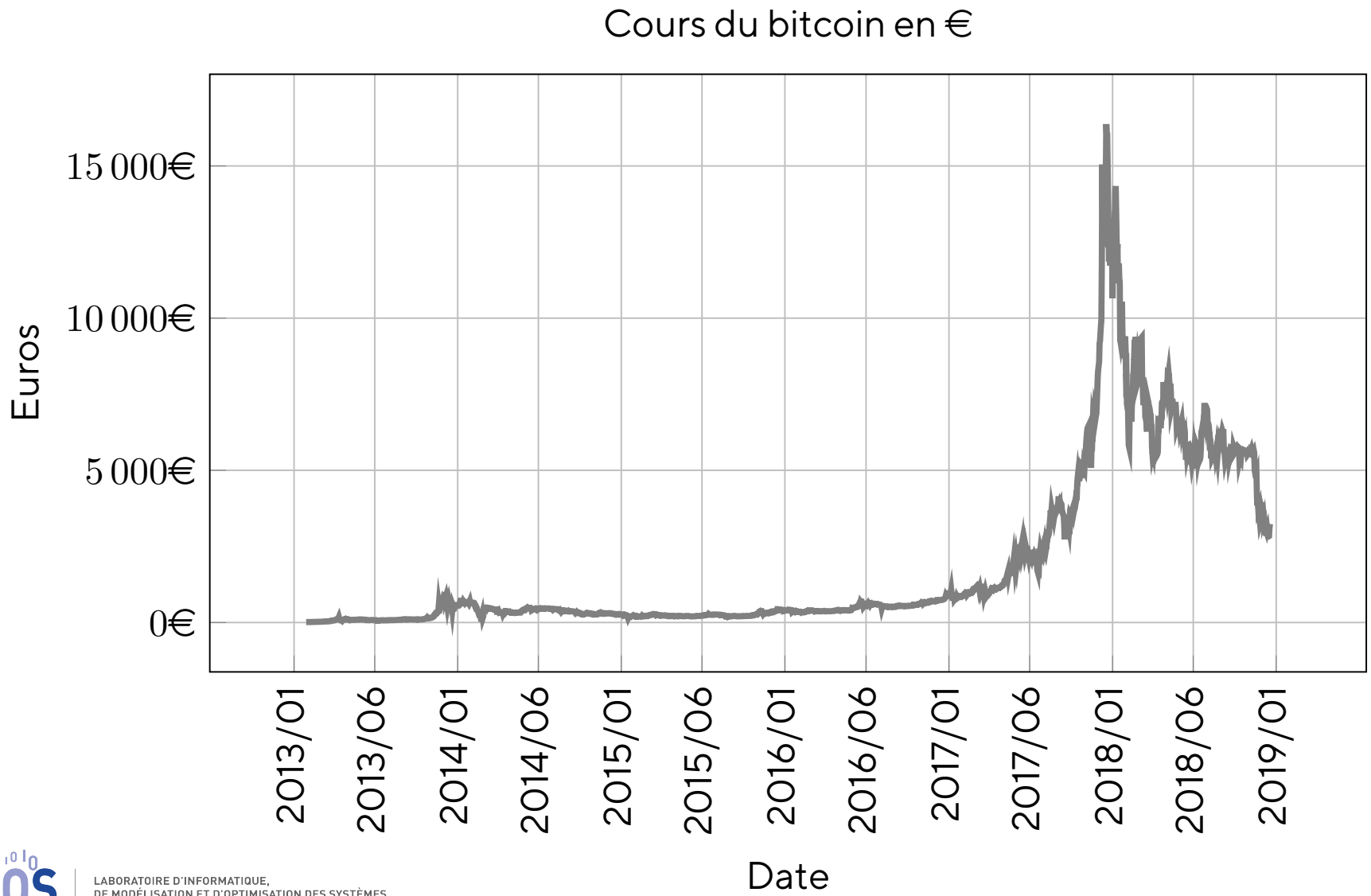


Bitcoin : monnaie électronique

Créée en 2008 par Satoshi Nakamoto (1 BTC $\approx$ 945 euros)

1	BTC = 1 Bitcoin	
0,01	BTC = 1 cBTC	= 1 centiBitcoin (ou bitcent)
0,001	BTC = 1 mBTC	= 1 milliBitcoin
0,000 001	BTC = 1 μBTC	= 1 microBitcoin
0,000 000 01	BTC = 1 Satoshi	

Taux de change du bitcoin



Clef symétrique

Exemples

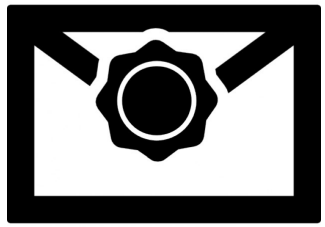
- DES
- AES

Chiffrement à clef publique

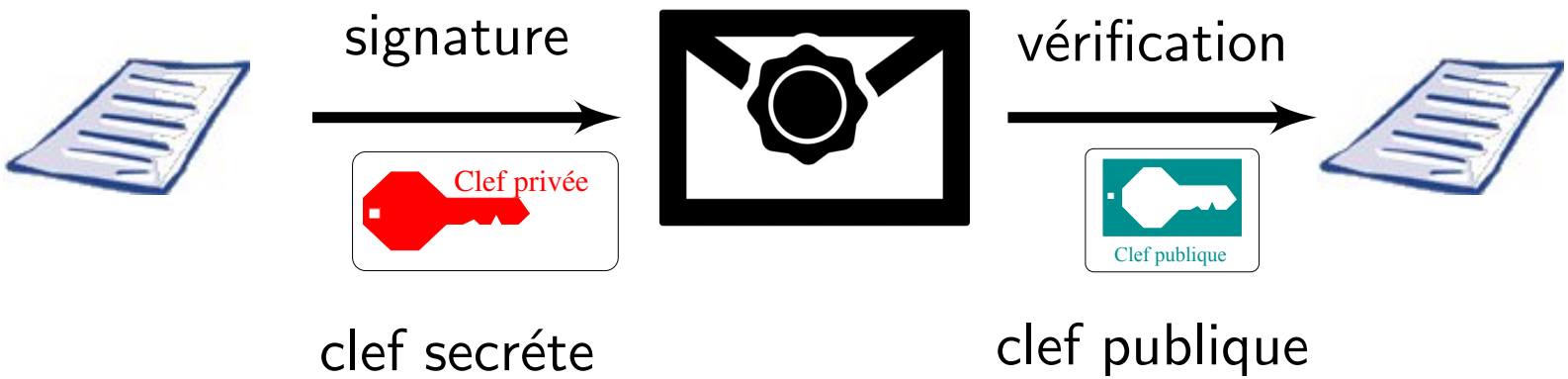
Exemples

- RSA : $c = m^e \mod n$
- ElGamal : $c \equiv (g^r, h^r \cdot m)$

Signature

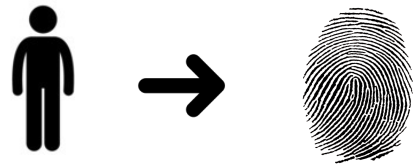


Signature

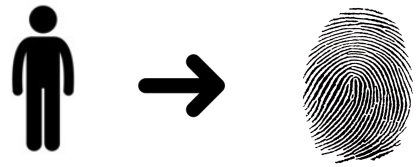


RSA: $m^d \mod n$

Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)

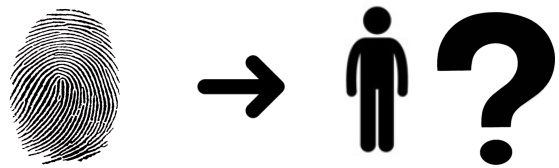


Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)

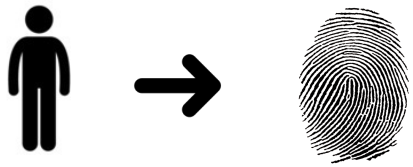


Propriétés de résistance

- Pré-image

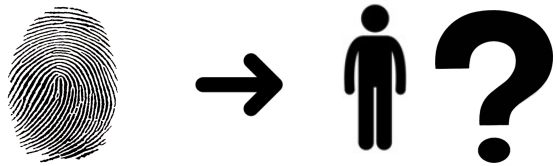


Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)

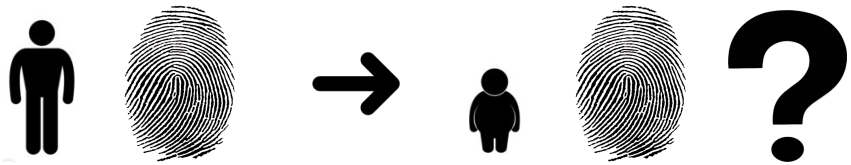


Propriétés de résistance

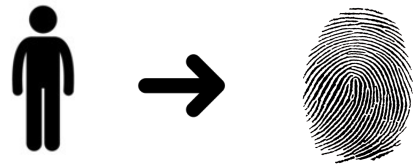
- Pré-image



- Seconde Pré-image

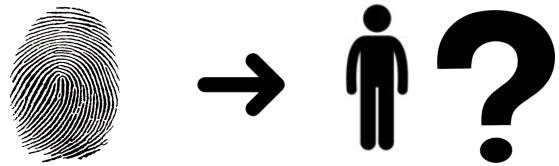


Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)

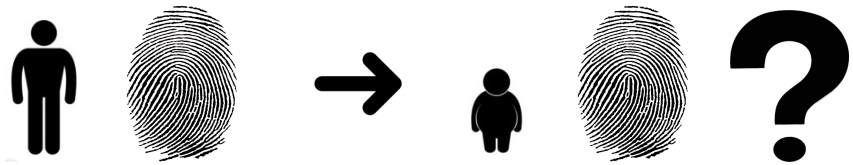


Propriétés de résistance

- Pré-image



- Seconde Pré-image



- Collision

Bitcoins : caractéristiques

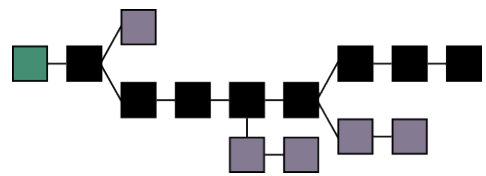
- Le nombre total de bitcoins est **fini**

  21 millions BTC

- Les transactions utilisent des **PKI**
- Numéro de compte :

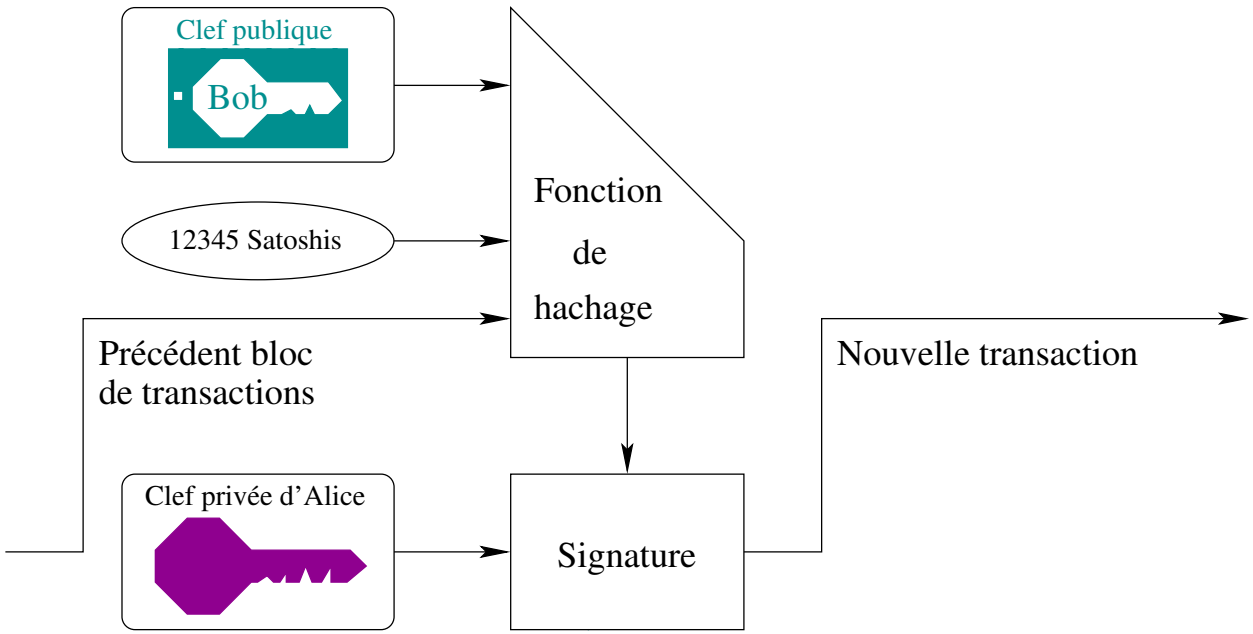
  $$\text{RIPEMD-160}(\text{SHA-256}(\text{ECDSA}_{pub}))$$

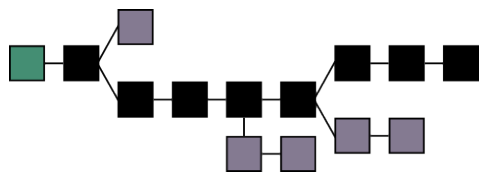
- Toutes les transactions sont **publiques**
- **Blockchain** : un système pair-à-pair qui garantit la validité des transactions



Comment faire une transaction?

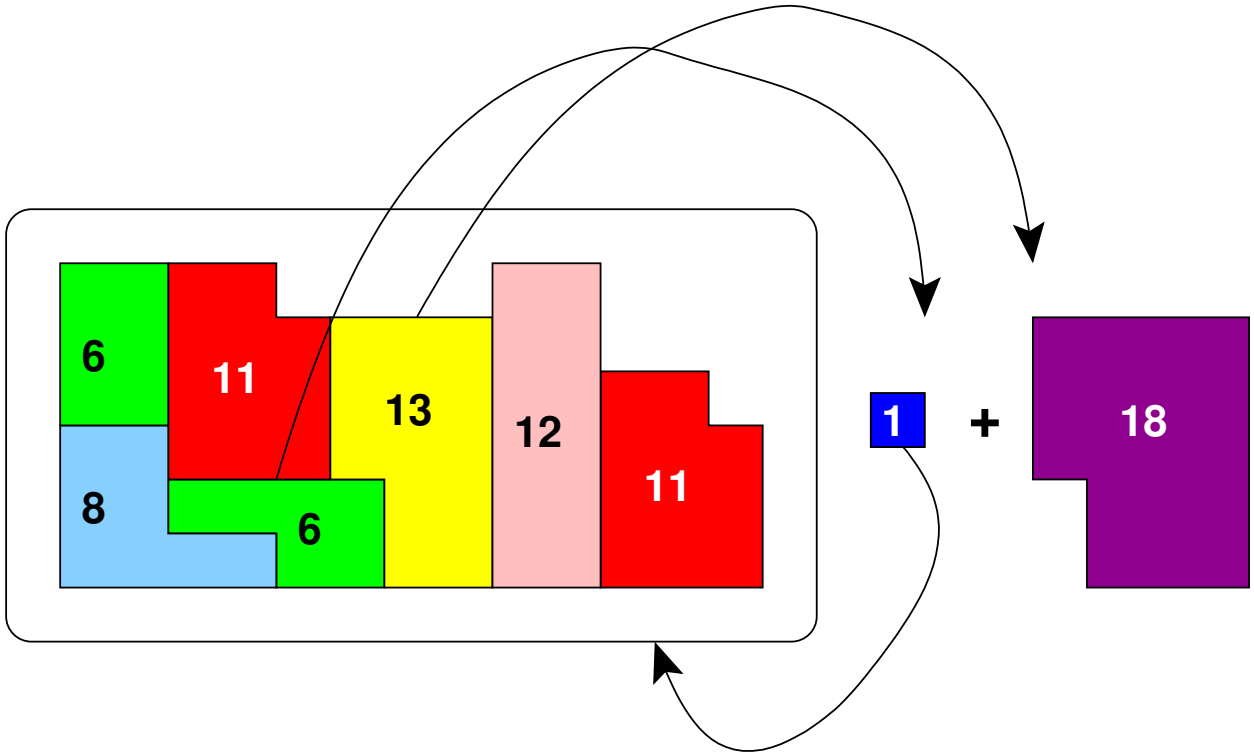
Alice donne 12345 Satochis ($\approx 5c$) à Bob.





Unspent Transaction Output UTXO

Payer 18 BTC avec des pièces



- Seuls des bitcoins possédés peuvent être dépensés

Porte-monnaie électronique

- Consultation du solde
- Réalisation d'une transaction
- Gestion du stockage des pièces
- Création de nouvelles clefs de compte

Où sont mes clefs privées ?

Solutions de portefeuille électronique

1. Sécurité
2. Disponibilité
3. Facilité

Solutions de portefeuille électronique

1. Sécurité
2. Disponibilité
3. Facilité

Matériel

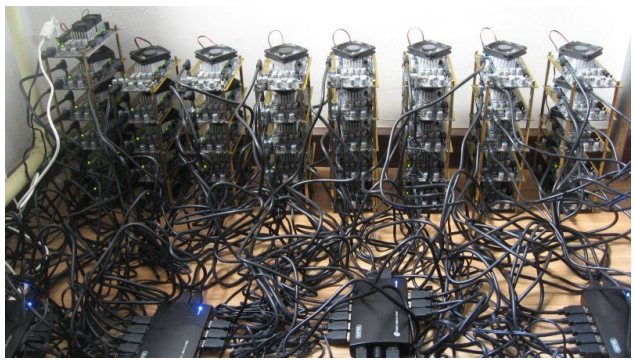
Numérique

Dématérialisé

Miner des Bitcoins

Miner des Bitcoins

Les “*mineurs*” valident les transactions contre des bitcoins



Miner des Bitcoins

- Valider = résoudre un **objectif de hachage**
- Récompense initiale 50 BTC pour une validation
- Divisée par 2 tous les 210000 validations

$$\sum_{i=0}^{32} \frac{50}{2^i} \times 210\,000 = 21 \text{ millions BTC}$$

Principe de la Blockchain

Etat de la chaîne 424210 A donne à B 3 BTC

🖨(A,B,3,424210)=458237

Etat de la chaîne 458237 C donne à B 9 BTC

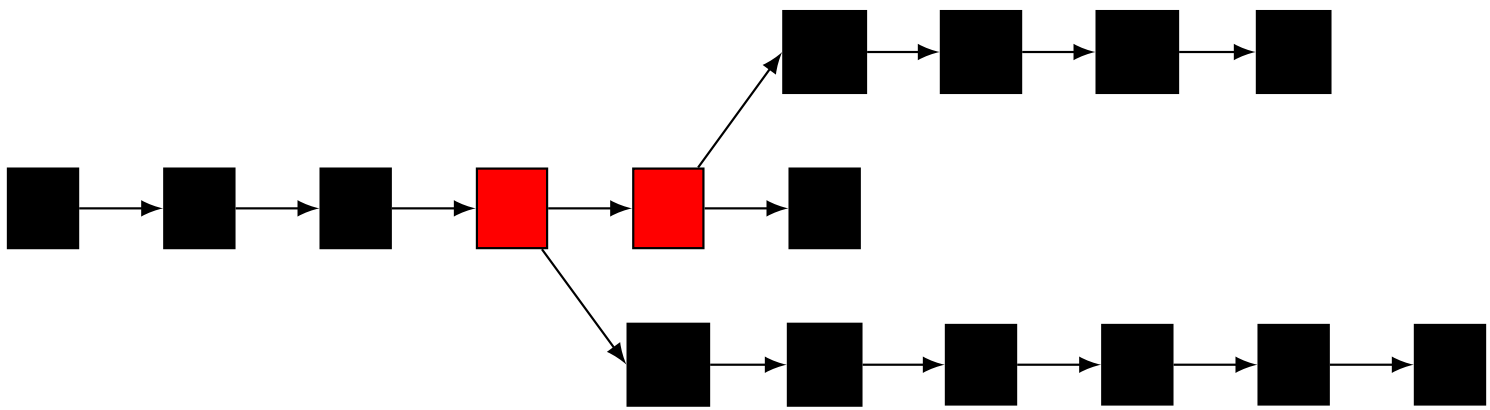
🖨(C,B,9,458237)=936127

Etat de la chaîne 936127 C donne à A 1 BTC

🖨(C,A,1,936127)=458237

Blockchain Infalsifiable

$$
\begin{aligned}
& \text{🖨}(C, A, 1, \text{🖨}(C, B, 9, \text{🖨}(A, B, 3, 424210))) \\
= \; & \text{🖨}(C, A, 1, \text{🖨}(C, B, 9, 458237)) \\
= \; & \text{🖨}(C, A, 1, 936127) \\
= \; & 458237
\end{aligned}
$$



Hachage naïf : ASCIISUM

$$H(A, B, 3) = ASCIISUM(A, B, 3) = 65 + 66 + 51 = 132$$

dec	48	49	50	51	52	53	54	55	56	57
char	0	1	2	3	4	5	6	7	8	9

dec	65	66	67	68	69	70	71	72	73	74
char	A	B	C	D	E	F	G	H	I	J

dec	75	76	77	78	79	80	81	82	83	84
char	K	L	M	N	O	P	Q	R	S	T

dec	85	86	87	88	89	90
char	U	V	W	X	Y	Z

Simulateur de preuve de travail ASCII

ASCIISUM(ASCIISUM(A,B,1234,B_{i-1},nonce)) divisible par 3 et 5

dec	48	49	50	51	52	53	54	55	56	57
char	0	1	2	3	4	5	6	7	8	9

dec	65	66	67	68	69	70	71	72	73	74
char	A	B	C	D	E	F	G	H	I	J

dec	75	76	77	78	79	80	81	82	83	84
char	K	L	M	N	O	P	Q	R	S	T

dec	85	86	87	88	89	90
char	U	V	W	X	Y	Z

ASCIISUM(ASCIISUM(A,B,1234,42,981))
= ASCIISUM(65+ 66+ 49+50+51+52+ 52+50+ 57+56+49)
= ASCIISUM (597) = 53+57+55 = 165

Ensemble des 4 transactions disponibles

dec	48	49	50	51	52	53	54	55	56	57
char	0	1	2	3	4	5	6	7	8	9

dec	65	66	67	68	69	70	71	72	73	74
char	A	B	C	D	E	F	G	H	I	J

dec	75	76	77	78	79	80	81	82	83	84
char	K	L	M	N	O	P	Q	R	S	T

dec	85	86	87	88	89	90
char	U	V	W	X	Y	Z

Objectif de hachage :

ASCIISUM(ASCIISUM(X,Y,Montant,B_{i-i},nonce)) divisible par 3 et 5

Hash du block précédent : 42

$$\begin{aligned} \text{Alice donne à Dave 5 BTC} &: A, D, 5 \\ \text{Bob donne à Charlie 9 BTC} &: B, C, 9 \\ \text{Bob donne à Dave 7 BTC} &: B, D, 7 \\ \text{Charlie donne à Alice 3 BTC} &: C, A, 3 \end{aligned}$$

Quelques solutions

$$\text{ASCIISUM}(\text{ASCIISUM}(\text{A,D,5,42,1323})) = \text{ASCIISUM}(489) = 165$$

$$\text{ASCIISUM}(\text{ASCIISUM}(\text{B,C,9,42,56})) = \text{ASCIISUM}(399) = 165$$

$$\text{ASCIISUM}(\text{ASCIISUM}(\text{B,D,7,42,56})) = \text{ASCIISUM}(399) = 165$$

$$\text{ASCIISUM}(\text{ASCIISUM}(\text{C,A,3,42,99})) = \text{ASCIISUM}(399) = 165$$

Miner : Objectif de hachage

Cible = 0000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076

Trouver une nombre n tel que

$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, n)) = x < \textit{Cible}$$

Avoir au moins 18 zéros au début de x

Miner : Objectif de hachage

Cible = 00000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076

Trouver une nombre n tel que

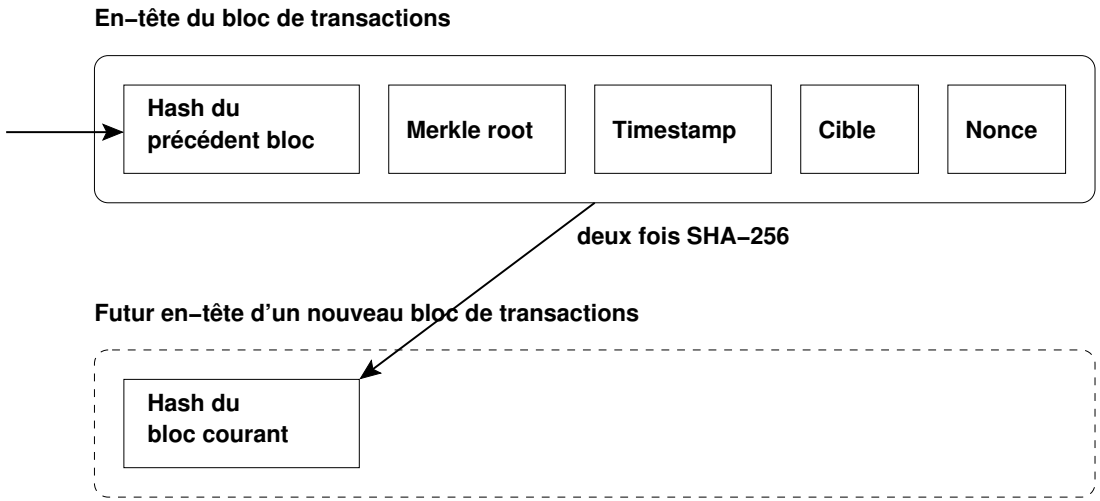
$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, n)) = x < \textit{Cible}$$

Avoir au moins 18 zéros au début de x

Stratégie : brute force

Tester toutes les valeurs possibles de n

Miner : Proof of work



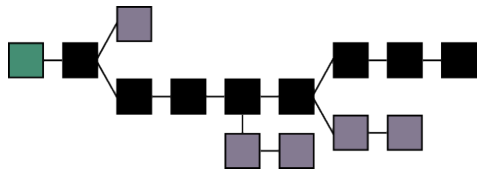
Avoir un zéro de plus au début

SHA-256(SHA-256(en-tête de bloc))

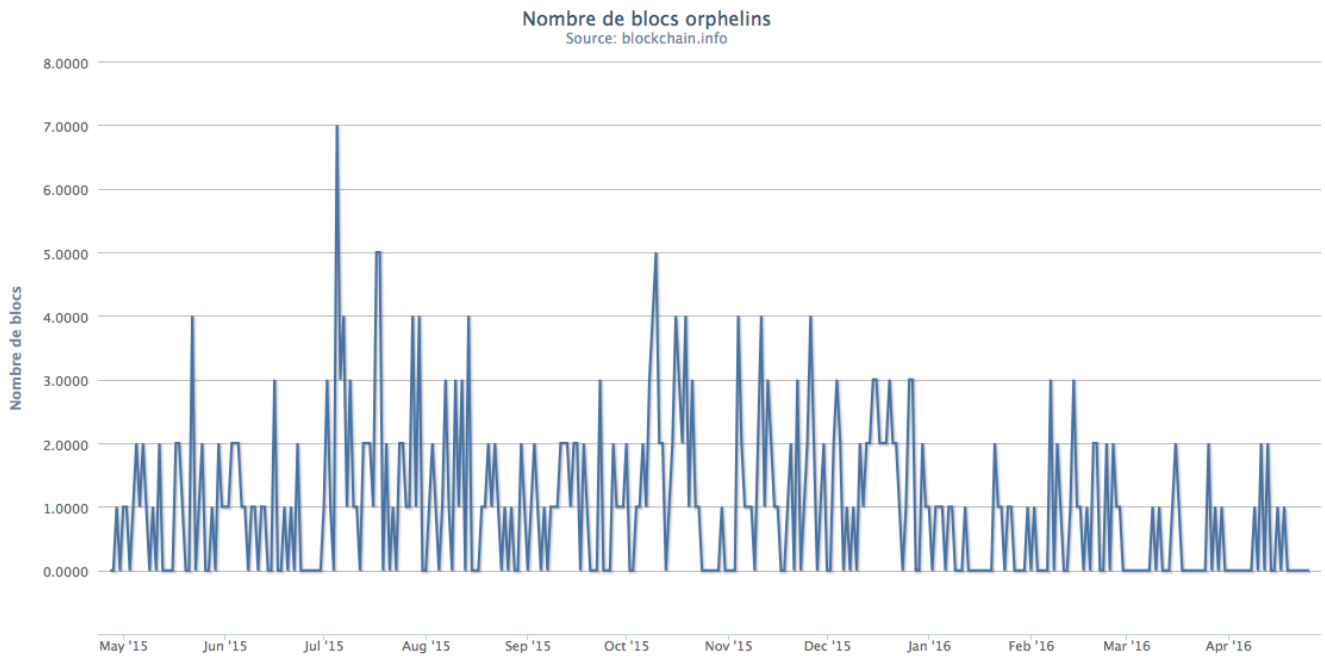
- les transactions passées (195 Go)
- les transactions à valider
- les secondes depuis 01/01/1970
- un nonce

Miner = Validation des transactions

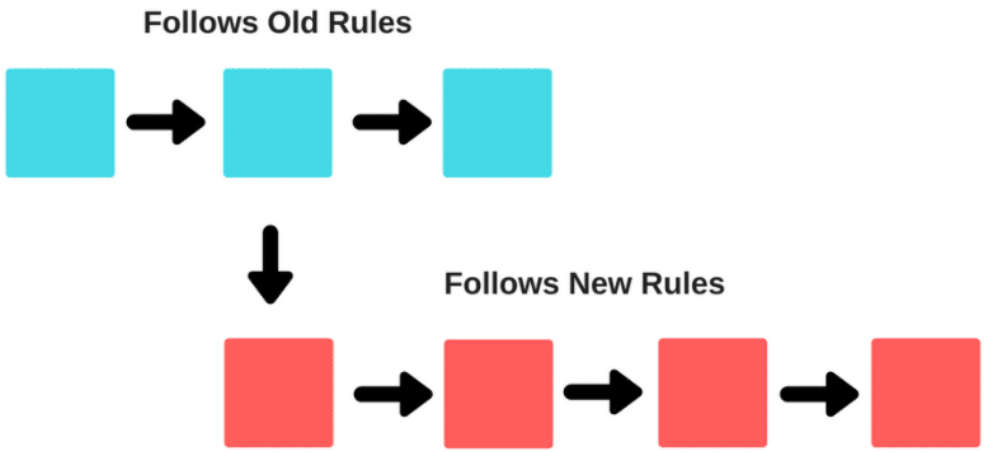
Cible: 00000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076



- La chaîne la plus longue persiste (attaque 51 %)
- Validation toutes les 10 minutes (6 confirmations)



Soft Fork

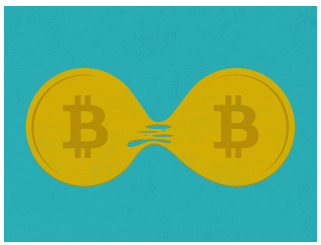


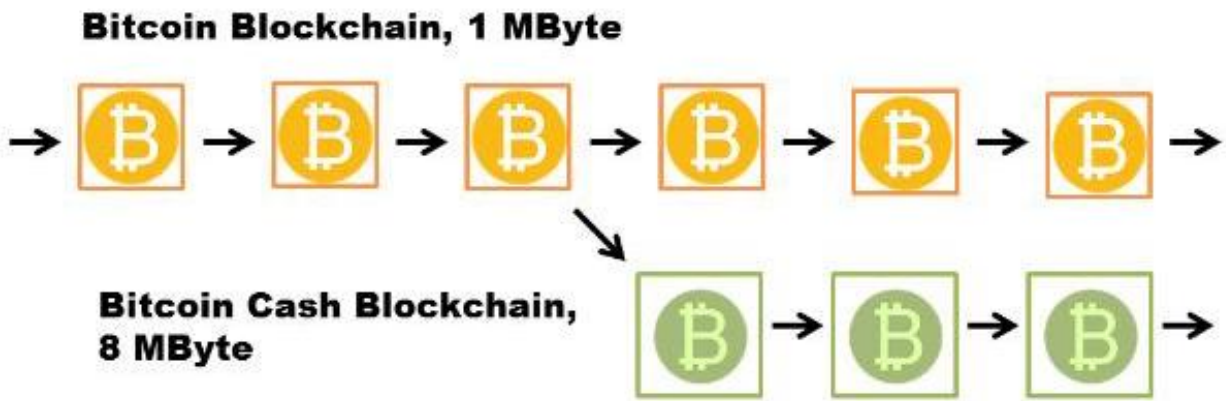
The primary difference between a soft fork and hard fork is that it is not backward compatible

Modification du code :

- Correction de bugs
- Améliorations consensuelles

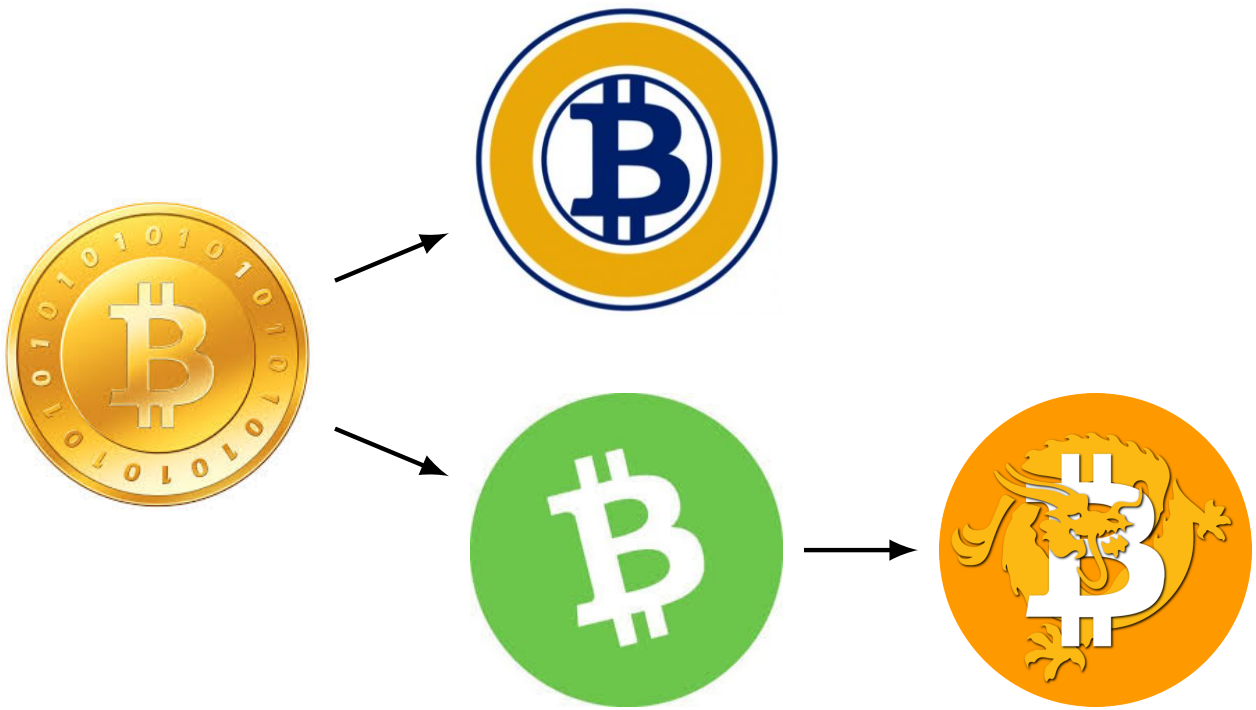
Hard Fork




Bitcoin Blockchain, 1 MByte
Bitcoin Cash Blockchain,
8 MByte

Hard Fork History

- Bitcoin Cash for Bitcoin (1 August 2017 at block 478558)
- Bitcoin Gold for Bitcoin (24 October 2017 at block 491407)
- Bitcoin SV (Satoshi Version) for Bitcoin Cash (15 November 2018 at block 556766)



Hard Fork History

Logo	Fork Name	Fork Symbol	Blockchain	Fork Date	Fork Block	Coin Distribution
	Bitcoin Zero	BZX	Bitcoin	Sunday, September 30, 2018	0	1 HXX : 1 BTC = 1 BZX
	Micro Bitcoin	MBC	Bitcoin	Wednesday, May 30, 2018	525000	1 BTC = 10000 MBC
	ClassicBitcoin	CBTC	Bitcoin	Sunday, April 01, 2018	516095	1 BTC = 10000 CBTC
	Bitcoin Lite	BTCL	Bitcoin	Tuesday, January 30, 2018	0	1 BTC = 1 BTCL
	Bitcoin Atom	BCA	Bitcoin	Wednesday, January 24, 2018	505888	1 BTC = 1 BCA
	Bitcoin Interest	BCI	Bitcoin	Monday, January 22, 2018	505083	1 BTC = 1 BCI
	BitVote	BTV	Bitcoin	Sunday, January 21, 2018	505050	1 BTC = 1 BTV
	Bitcoin Smart	BCS	Bitcoin	Sunday, January 21, 2018	505050	1 BTC = 100 BCS
	Bitcoin Rhodium	BTR	Bitcoin	Wednesday, January 10, 2018	0	1 BTC = 1 BTR
	Bitcoin Private	BTCP	Bitcoin	Monday, January 01, 2018	0	1 BTC/ZCL = 1 BTCP
	Bitcoin All	BTA	Bitcoin	Monday, January 01, 2018	0	1 BTC = 1 BTA
	Bitcoin Pizza	BPA	Bitcoin	Monday, January 01, 2018	501888	1 BTC = 1 BPA
	BitcoinBoy	BCB	Bitcoin	Sunday, December 31, 2017	501888	1 BTC = 100 BCB
	Bitcoin Ore	BCO	Bitcoin	Sunday, December 31, 2017	501949	1 BTC = 1 BCO
	Bitcoin Uranium	BUM	Bitcoin	Sunday, December 31, 2017	0	1 BTC = 1 BUM
	Quantum Bitcoin	QBTC	Bitcoin	Thursday, December 28, 2017	0	1 BTC = 1QBTC
	Bitcoin SegWit2X x11	B2X	Bitcoin	Thursday, December 28, 2017	501451	1 BTC = 1 B2X
	Bitcoin File	BIFI	Bitcoin	Wednesday, December 27, 2017	501225	1 BTC = 1000 BIFI
	Bitcoin God	GOD	Bitcoin	Wednesday, December 27, 2017	501225	1 BTC = 1 GOD
	Bitcoin Top	BTT	Bitcoin	Tuesday, December 26, 2017	501118	1 BTC = 1 BTT

Logo	Fork Name	Fork Symbol	Blockchain	Fork Date	Fork Block	Coin Distribution
	Bitcoin New	BTN	Bitcoin	Monday, December 25, 2017	501000	1 BTC = BTN
	Lightning Bitcoin	LBTC	Bitcoin	Tuesday, December 19, 2017	499999	1 BTC = 1 LBTC
	Bitcoin Stake	BTCS	Bitcoin	Tuesday, December 19, 2017	499999	1 BTC = 100 BTCS
	Bitcoin Faith	BTF	Bitcoin	Tuesday, December 19, 2017	500000	1 BTC = 1 BTF
	Bitcoin World	BTW	Bitcoin	Sunday, December 17, 2017	499777	1 BTC = 10000 BTW
	UnitedBitcoin	UB	Bitcoin	Tuesday, December 12, 2017	498777	1 BTC = 1 UB
	Bitcoin Hot	BTH	Bitcoin	Tuesday, December 12, 2017	498848	1 BTC = 100 BTH
	BitcoinX	BCX	Bitcoin	Tuesday, December 12, 2017	498888	1 BTC = 10000 BCX
	Super Bitcoin	SBTC	Bitcoin	Tuesday, December 12, 2017	498888	1 BTC = 1 SBTC
	Bitcoin Silver	BTSI	Bitcoin	Friday, December 01, 2017	0	1 BTC = 1 BTSI
	Bitcoin Nano	BTN	Bitcoin	Friday, December 01, 2017	501888	1 BTC = 1000 BTN
	Bitcoin Diamond	BCD	Bitcoin	Friday, November 24, 2017	495866	1 BTC = 10 BCD
	Bitcore	BTX	Bitcoin	Thursday, November 02, 2017	0	1 BTC = 0.5 BTX
	Bitcoin Gold	BTG	Bitcoin	Tuesday, October 10, 2017	491407	1 BTC = 1 BTG
	Bytether	BTH	Bitcoin	Tuesday, August 01, 2017	478558	1 BTC = 1 BTH
	Oil BTC	OBTC	Bitcoin	Tuesday, August 01, 2017	498888	1 BTC = 1 OBTC
	Bitcoin Clashic	BCHC / B	Bitcoin	Tuesday, August 01, 2017	478558	1 BTC = 1 BCHC / B
	Bitcoin Cash	BCH	Bitcoin	Tuesday, August 01, 2017	478559	1 BTC = 1 BCH

Un hard fork rend-il plus riche ?

- Instantanément : doublement du nombre de pièces (même solde dans chaque branche)
- Pouvoir d'achat a priori inchangé à l'instant de la scission (répartition dans les deux monnaies)

L'exemple de Bitcoin Gold

23/10/2017 :	BTC $\approx$	5 910$
24/10/2017 :	BTG $\approx$	480$
25/10/2017 :	BTC $\approx$	5 380$

Un hard fork rend-il plus riche ?

- Instantanément : doublement du nombre de pièces (même solde dans chaque branche)
- Pouvoir d'achat a priori inchangé à l'instant de la scission (répartition dans les deux monnaies)
- Ensuite : chaque crypto-monnaie fluctue en propre

L'exemple de Bitcoin Gold

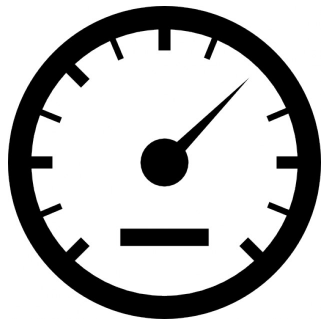
23/10/2017 :	BTC ≈	5 910$
24/10/2017 :	BTG ≈	480$
25/10/2017 :	BTC ≈	5 380$
10/03/2019 :	BTC ≈	3 895$
	BTG ≈	12$

Traçable

Traçable

Snark

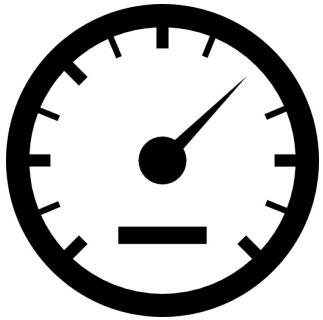
Limitations



10 minutes = 1 block

Taille des transactions 1 Mo

Limitations



10 minutes = 1 block

Taille des transactions 1 Mo

Lightning Network

ETHEREUM

12 secondes

Energivore

Bitcoin 61,71 TWh/year = 6 585 585 US Houses/year

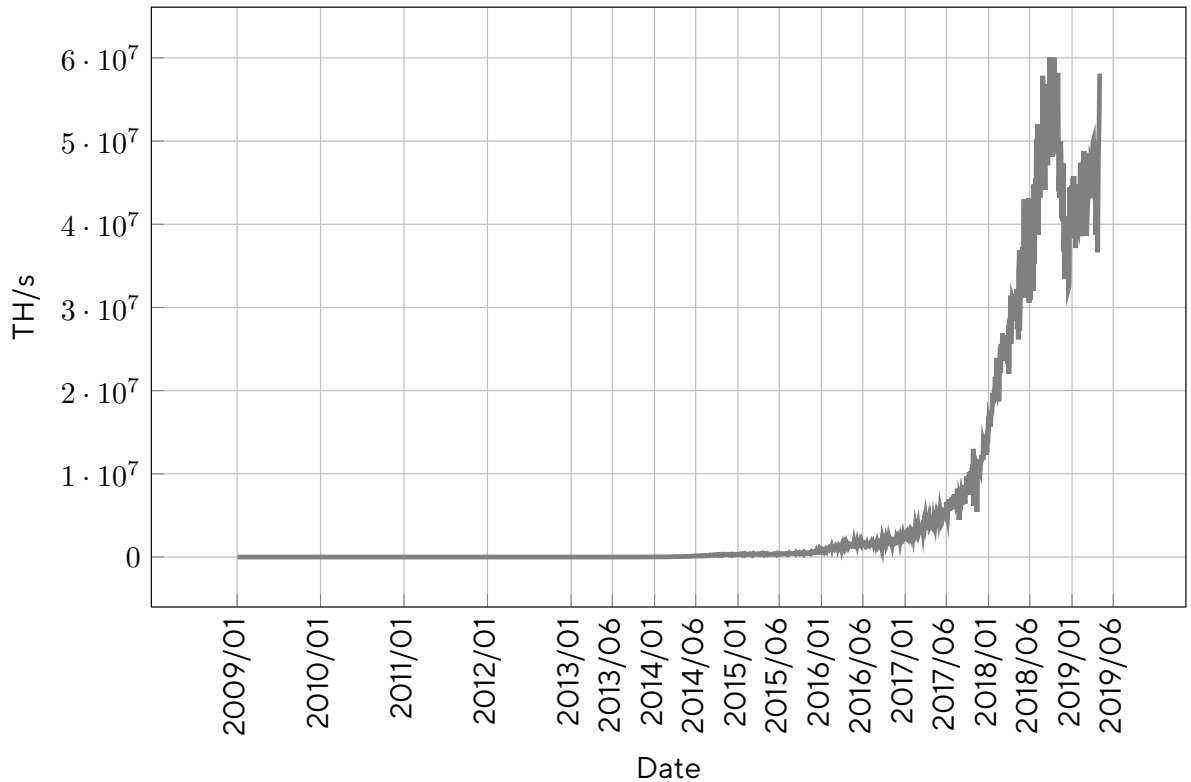
Energivore

Bitcoin 61,71 TWh/year = 6 585 585 US Houses/year

Proof of Stake

Lightning Network

Énergivore



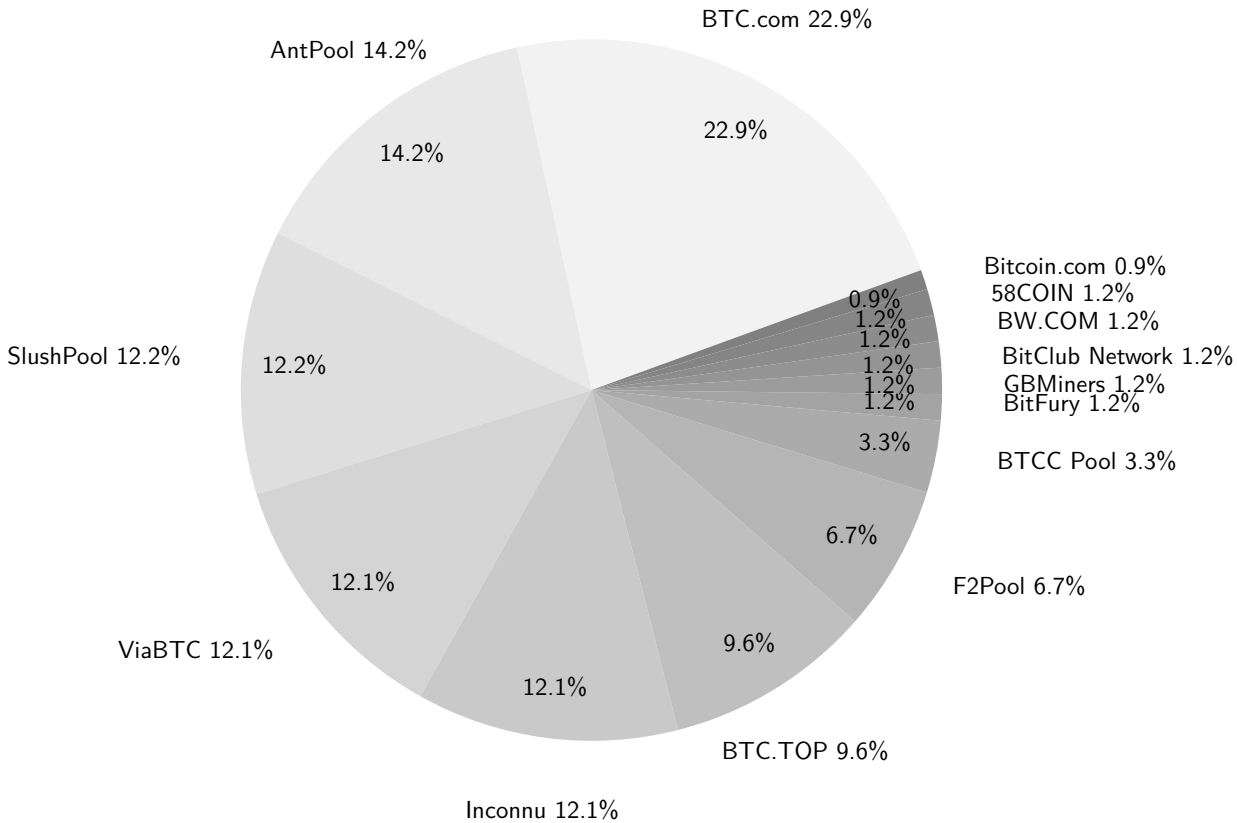
Estimation: plusieurs TWh annuels (comparable à un petit état).

Un bloc toutes les 10 minutes

Machine	Type	Vitesse MH/s	Efficacité MH/J	Coût MH/s/€	Minage moyen Années/bloc
Core i5-2400	CPU	14	0.15	0.09	25.3 Millions
PS3	Cell	21	0.35	0.09	16.9 Millions
ATI 830	GPU	325	1.98	3.30	1.1 Millions
Ebit E11++	ASIC	44 000 000	22 200.00	8 885.00	13.6

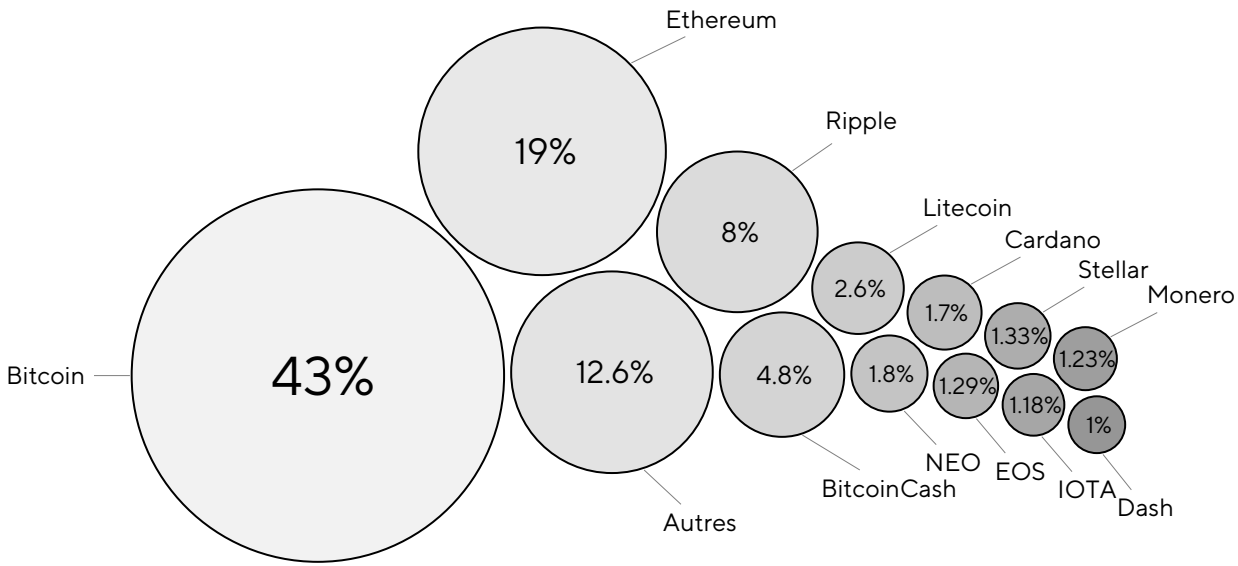
- Cible : 74 zéros initiaux, $\frac{1}{2^{74}}$ chances de miner
- $44\,000\,000$ MH/s $= 4.4\,10^{13}$ H/s $\approx 2^{45.3}$ H/s
- $2^{28.7} \approx 4.3\,10^{8}$ s $\approx 5\,000$ jours ≈ 13.6 années de calcul d'un Ebit E11++
- Réseau mondial $\approx 700\,000$ E11

Fermes de mineurs



Plan

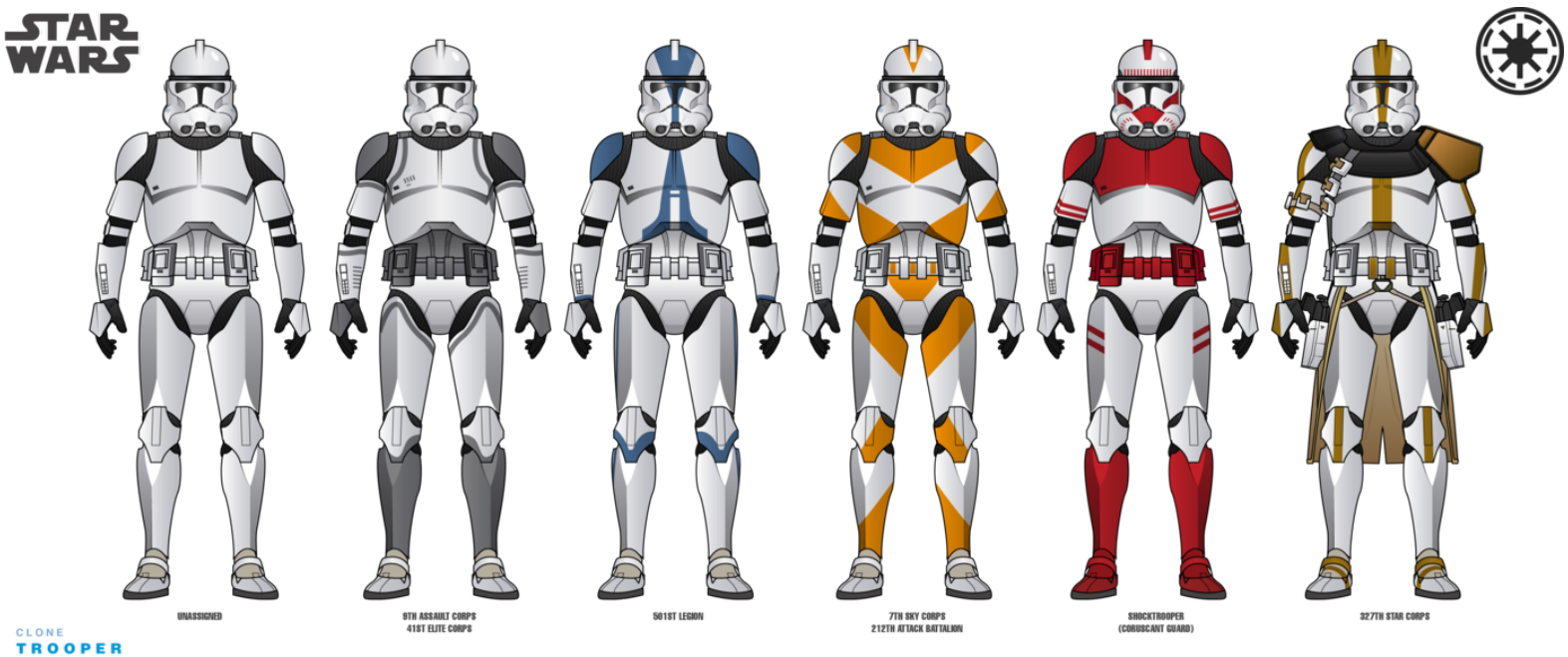
Diversité monétaire



Autres crypto-monnaies

Classification I : Pourris

Classification II : Clones de Bitcoin



Classification III : Plus utile

Classification IV : Autres preuves de travail

ethereum

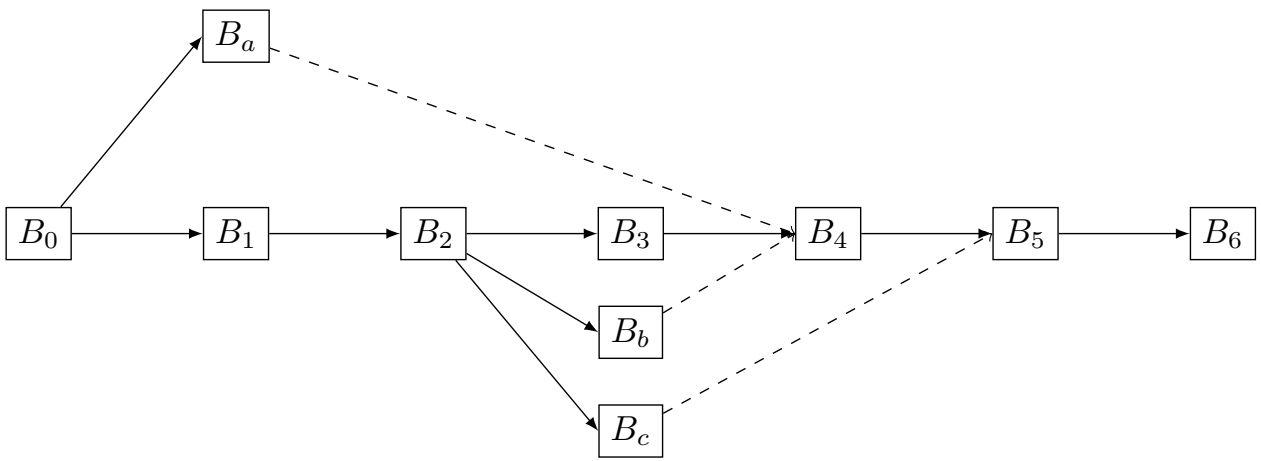
Etherum

Unité	wei
wei	1 wei
Kwei (babbage)	10^3 wei
Mwei (lovelace)	10^6 wei
Gwei (shannon)	10^9 wei
microether (szabo)	10^{12} wei
milliether (finney)	10^{15} wei
ether	10^{18} wei

ethereum

Vitesse : 12 secondes

Récompenser les oncles



B_4 reçoit $3 \times \left(1 + \frac{2}{32}\right) = 3.185$ ethers

B_b reçoit $\frac{7}{8} \times 3 = 2.625$ ethers, B_a reçoit $\frac{5}{8} \times 3 = 1.875$ ethers

Peercoin : Âge des pièces

Pour 10 pièces

Jours	0	1	2	...
Âge	10	10	20	...

Après V 0.3 :

- Attendre 30 jours
- Maximum 90 jours

Peercoin : Âge des pièces

Pour 10 pièces

Jours	0	1	2	...
Âge	10	10	20	...

Après V 0.3 :

- Attendre 30 jours
- Maximum 90 jours

Objectif de hachage

$$H < C \times A \times \frac{1}{2^{32} \times D}$$

- C : Nombre de pièces
- A : Âge jour des pièces
- D : Difficulté

Scalability ?

- Bitcoin 3-4 transactions / seconde
- Etherum 15 transactions / seconde
- VISA 65 000 transactions / seconde

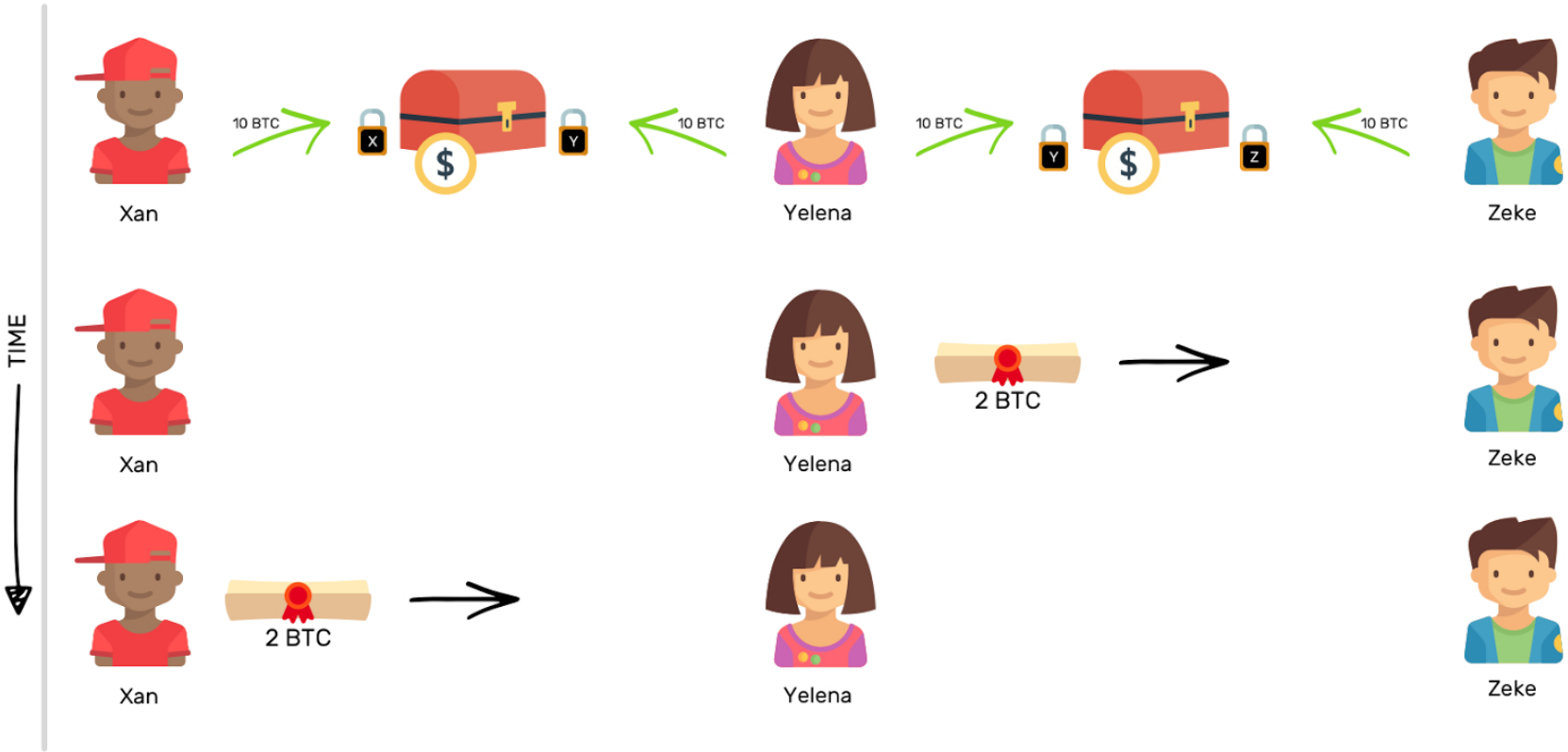
Scalability ?

- Bitcoin 3-4 transactions / seconde
- Etherum 15 transactions / seconde
- VISA 65 000 transactions / seconde

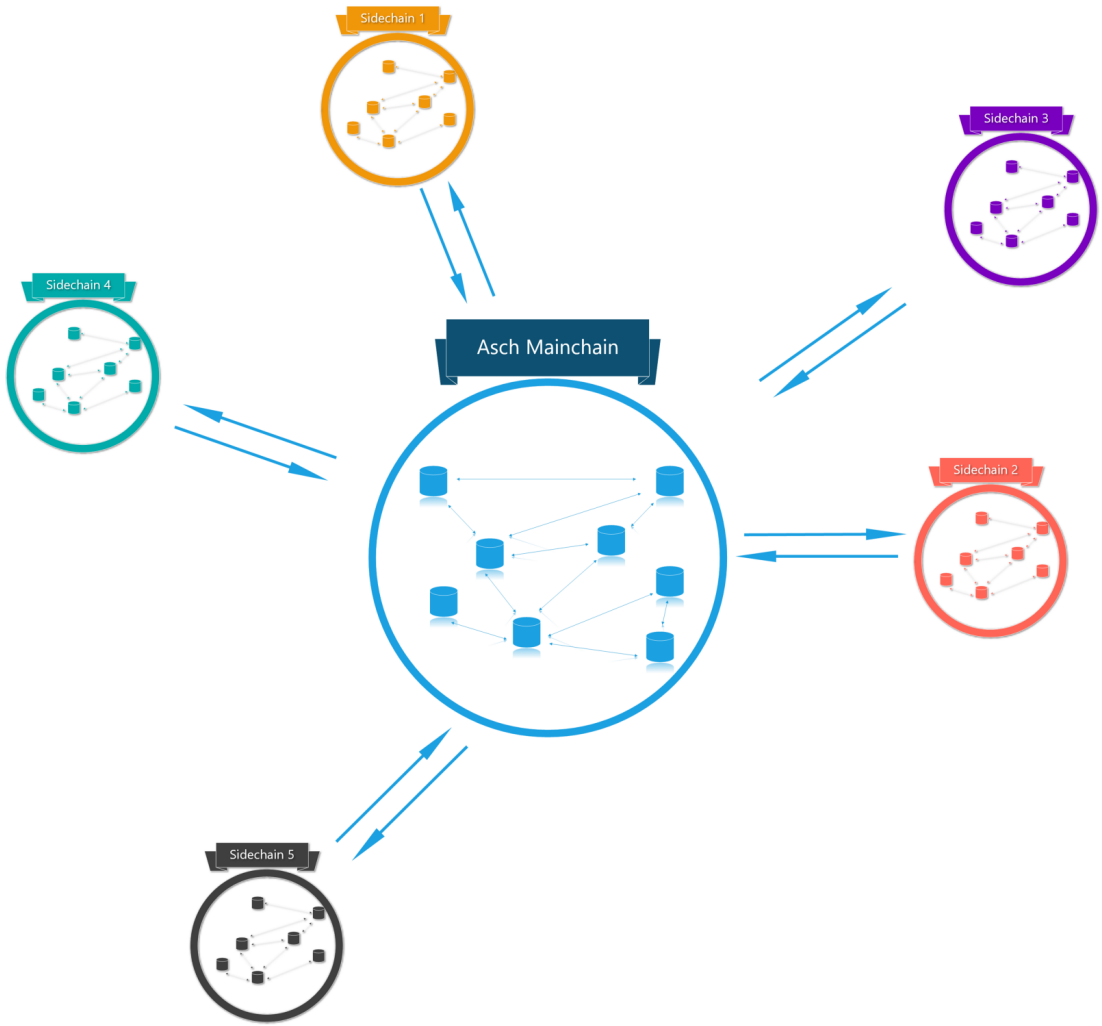
Solutions:

- Extend the block size
- Decrease the block interval
- Reduce the number of transactions on the chain :
  1. State Channel (BitcoinJ, Lightning Network, Rainden Network, Sprites, REvive, Rapido, Duplex Micropayment Channel, Channel Factory ...)
  2. Side Chain (Pegged Sidechain, Minimal Viable Plasma, Plasma Cash)

State Channel : Lightning Network



Side Chain Idea



Limitations:

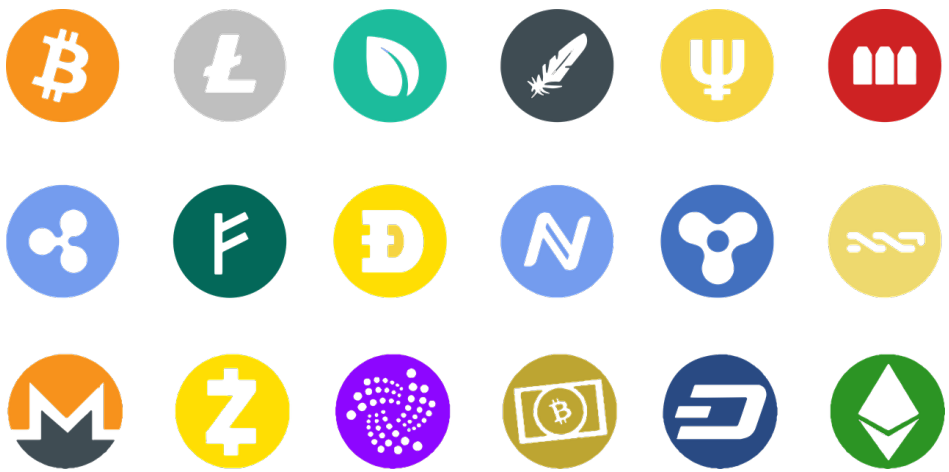
State Channel

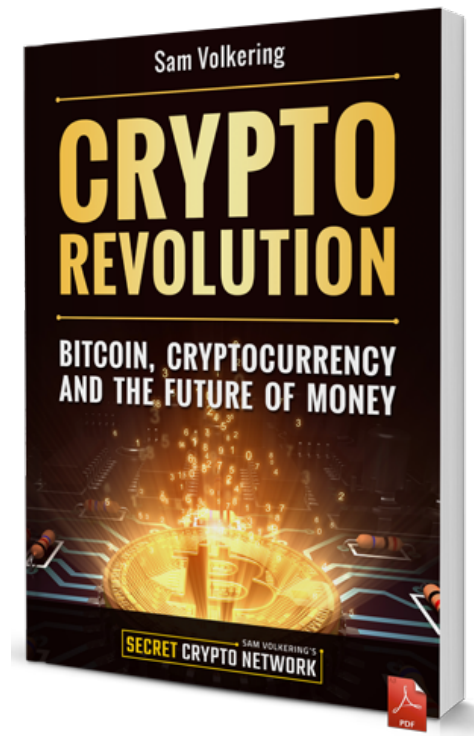
- Intermediate amount or failure
- Continuous internet connection
- Solution uses watchtowers (energy consumption)

Side Chain

- Massive withdraw implies congestion on the main chain

Pluriculture des créations monétaires

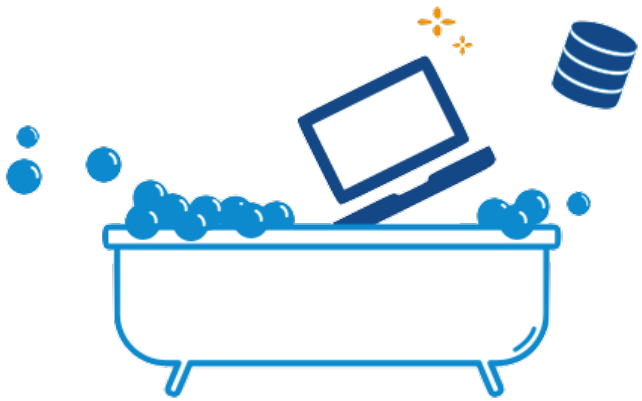




Qui s'approprie ces nouvelles monnnaies ?

Un exemple : ĞGraphHopper

Freins



Bitcoin : Crypto-monnaie dématérialisée décentralisée

- Preuve de travail = Objectif de Hachage
- Création de la monnaie = récompense aux mineurs
- Miner = difficile + energivore

Bitcoin : Crypto-monnaie dématérialisée décentralisée

- Preuve de travail = Objectif de Hachage
- Création de la monnaie = récompense aux mineurs
- Miner = difficile + energivore

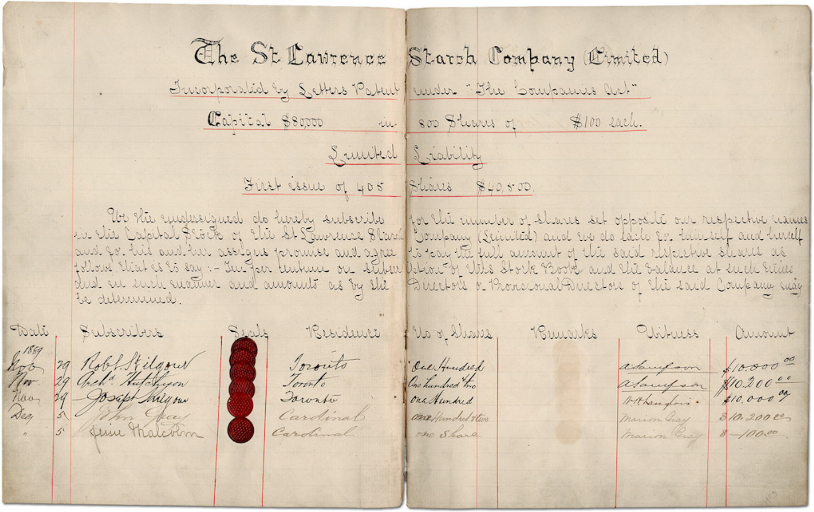


- Perte ou vol de la clef secrète = irréversible
- Monnaie anonyme et traçable

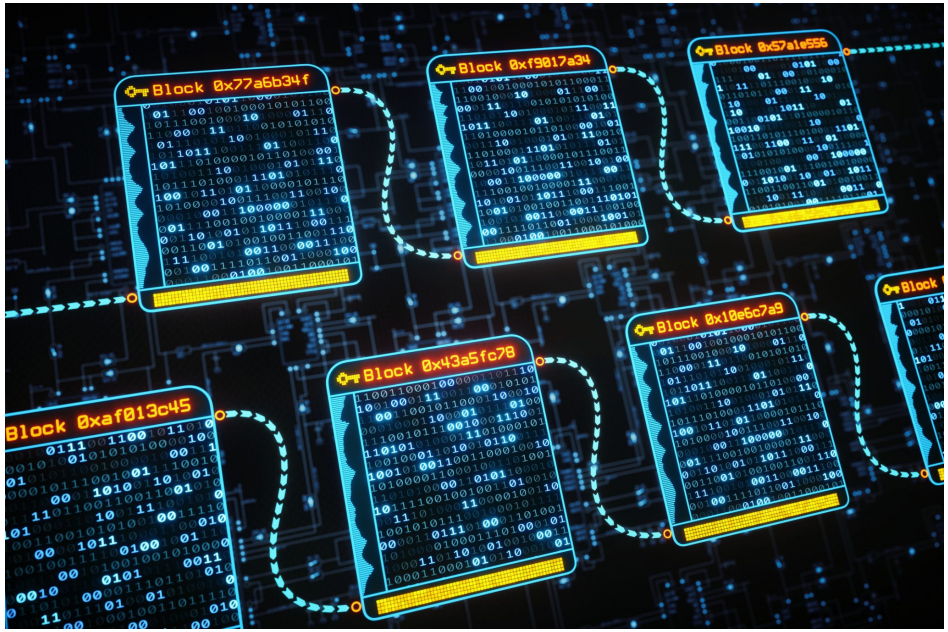


Plan

Blockchain


The St Lawrence Starch Company (Limited)
Incorporated by Letters Patent under "The Companies Act"
Capital $80,000 in 800 Shares of $100 each.
Limited Liability
First issue of 405 Shares $40,500

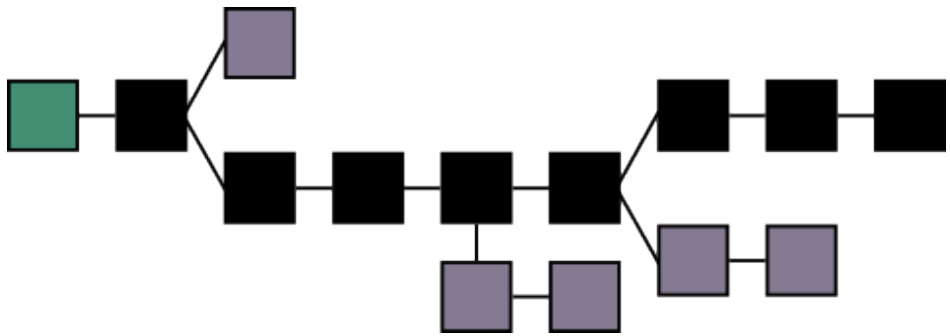
Blockchain



Registre distribué, sécurisé, infalsifiable

Fondamentaux d'une blockchain

- Registre distribué
  - ⇨ tous les participants ont une copie
- Protocole de consensus
  - ⚠ instant t, quelle est la copie officielle ?
- Crypto-monnaie
  - 👍 incitation à participer

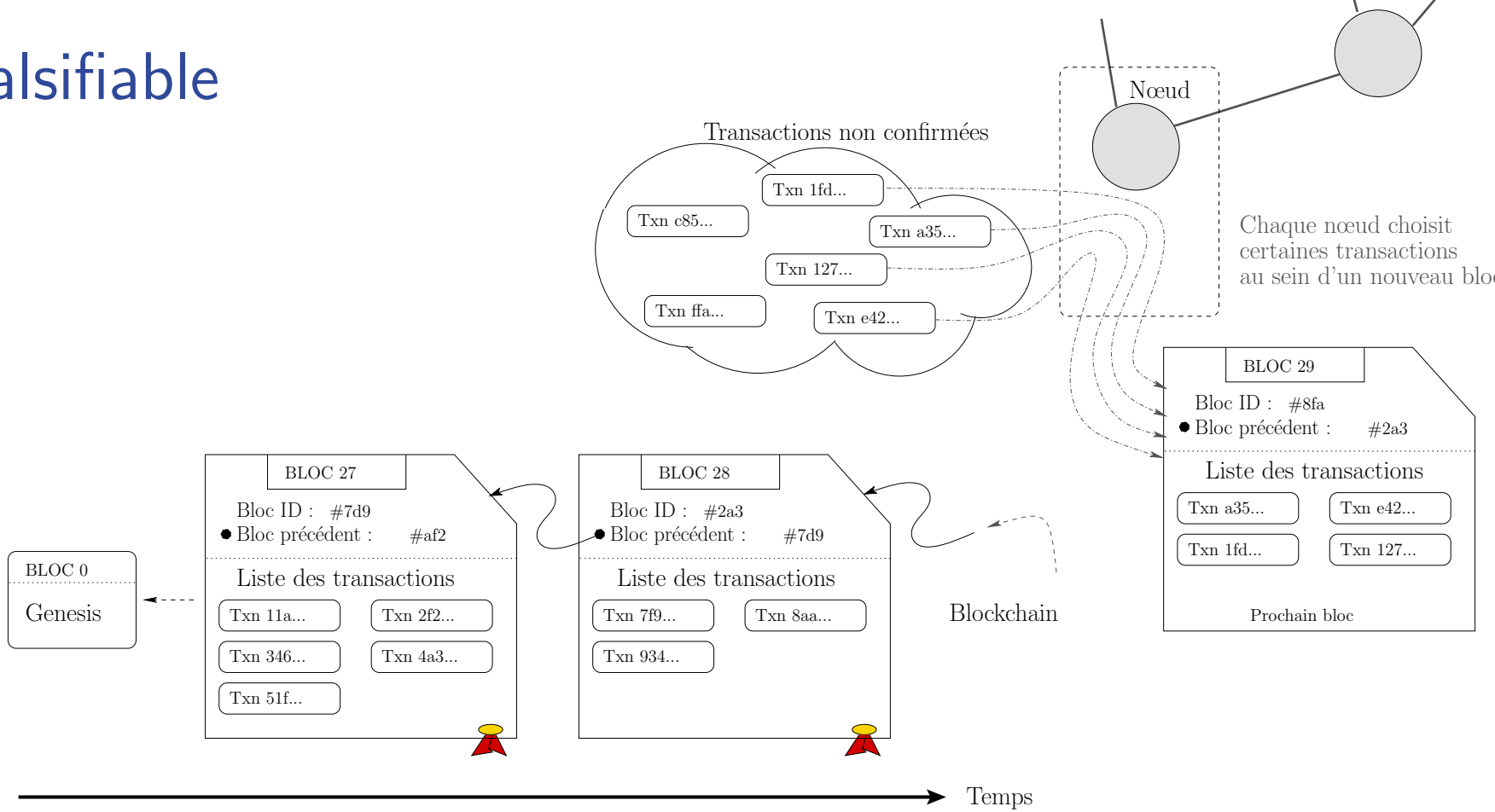


Inarrêtable, Infalsifiable, Auditable

Mineurs valident des transactions

Tiennent à jour le registre distribué

Infalsifiable

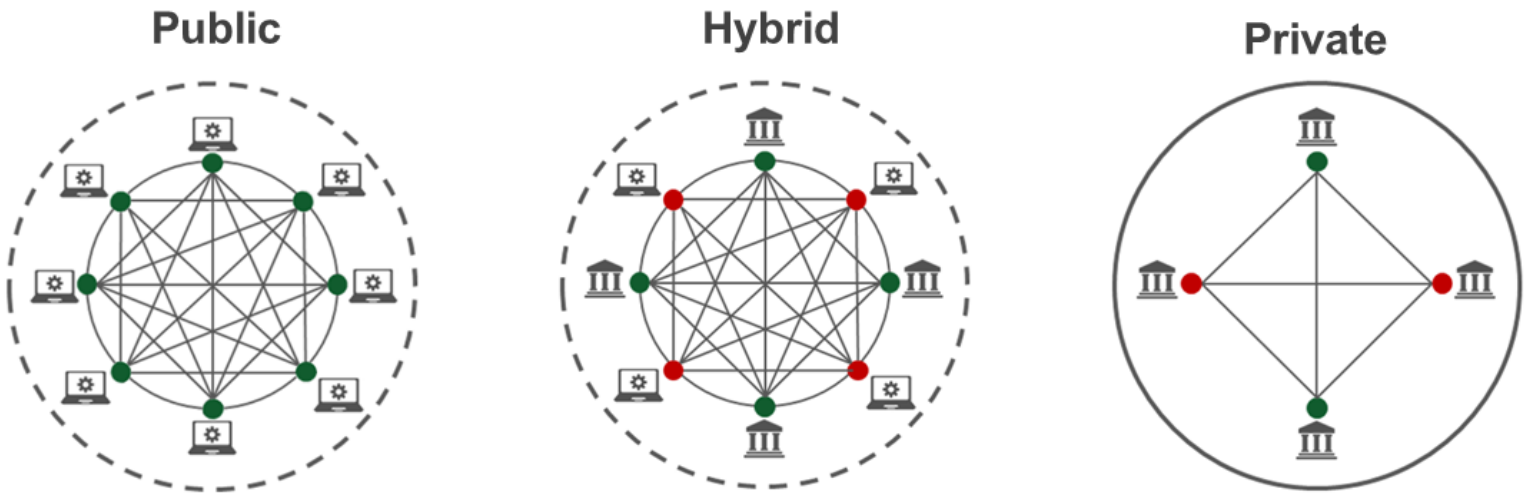


- Un résumé de chaque bloc de transaction est ajouté à chaque nouveau bloc de transactions
- La copie valide est sélectionnée aléatoirement & uniformément
- En cas de doute, seule la plus longue chaîne persiste

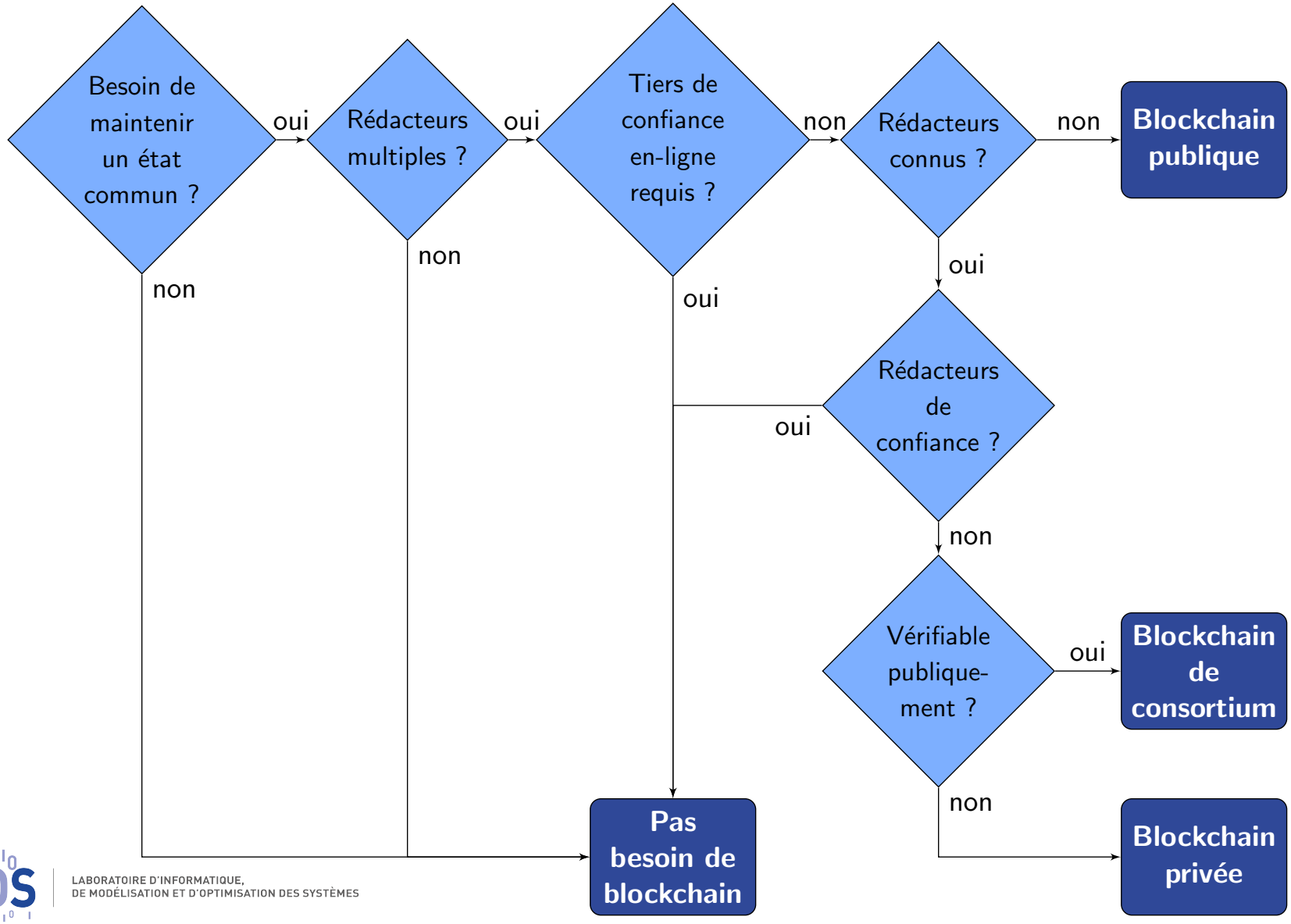
LIMOS
LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Décision des mineurs

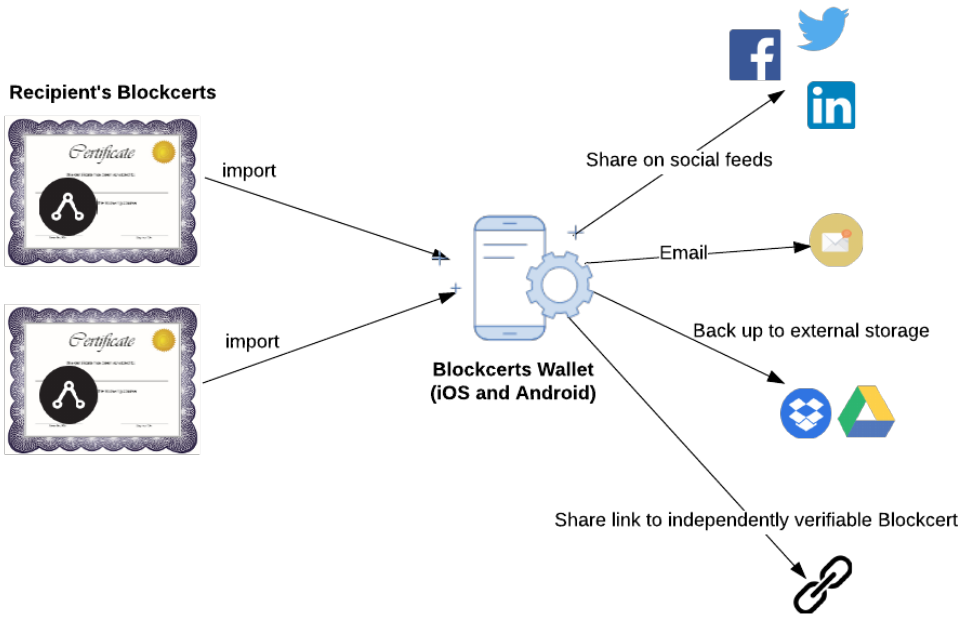
Blockchain Privée vs Publique



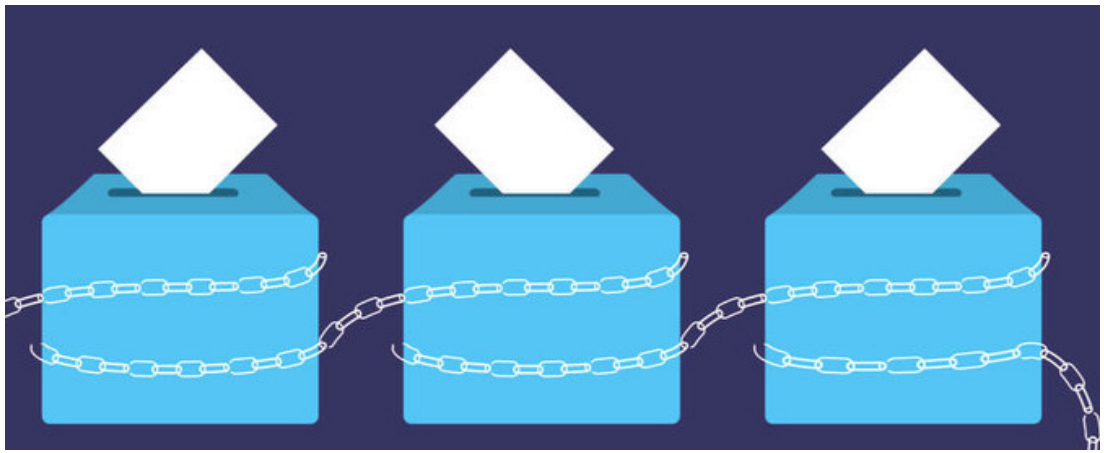
Ai-je besoin d'une blockchain ?



Blockchain Application : MIT Diploma



Blockchain Applications : Verify Your Vote, DABSTERS



Properties

Universal Verifiability, Individual Verifiability, Privacy, Receipt-Freeness, Prevent Double Vote, Vote and Go, ...

Blockchain Applications : Auction

Properties

Universal Verifiability, Individual Verifiability, Privacy, Receipt-Freeness, Prevent Double Spedning, Non-Repudiation ...

Blockchain Applications

Certificates (Laposte, EDF ...)
E-commerce
E-Health
...

Plan

Smart Contract

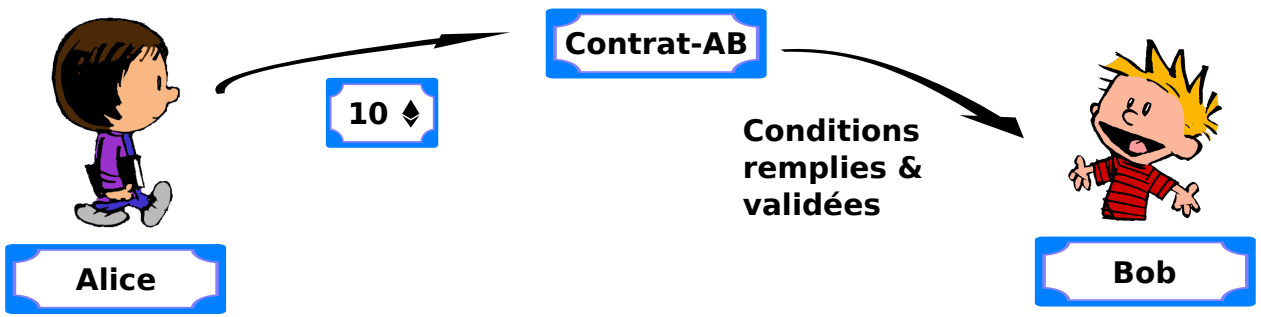
Quelques idées

- 1 contrat = transaction avec un FROM sans TO
- Pour l'utiliser : faire une transaction avec du GAS.
- Etherum Wallet connecté sur testnet de Etherum

Contrat intelligent

ETHEREUM

- Entités : Alice, Bob, Contrat-AB
- Instance d'une classe de règles opérationnelles (méthodes)
  - Mise en gage du montant par Alice (sur la blockchain)
    - 👍 *Assurance de la disponibilité des fonds*
  - Compilation et déploiement du contrat
  - Déclenchement automatique de changement d'état
    - ⇨ *Fonction des transactions/événements d'autres contrats/comptes*



Contrat : maximum d'un tableau d'entier

```
pragma solidity ^0.4.24;

contract MaxTools {

    function max (int[] data) public pure returns(int) {
        int result = data[0];
        for (uint i = 1; i < data.length; i++) {
            if (data[i] > result) {
                result = data[i];
            }
        }

        return result;
    }
}
```

Contrat : Convertisseur euros en dollars

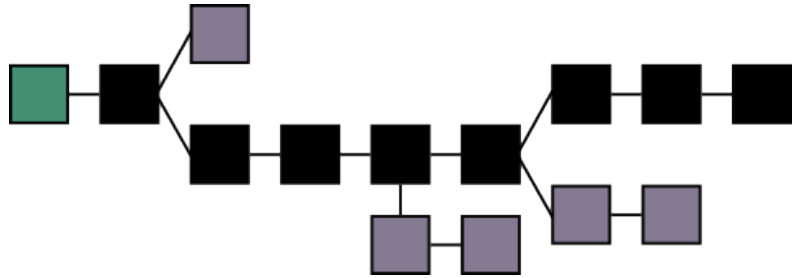
```
pragma solidity ^0.4.24;
contract JugTools {function max (int[] data) public pure returns(int);}

contract JugConverter {
    uint rate;
    address oracle;
    int[] rateHistory;

    JugTools tools;
    constructor(uint _rate, address _oracle) public {
        setRate(_rate);
        oracle = _oracle;
        tools = JugTools(0x1bD0d334118E9BFFD1316a3312fd369FaEB6b3E6);
    }

    modifier oracleOnly() {
        require(msg.sender == oracle, "Must be oracle");
        _;
    }

    event Result(uint);
    event NewWithdrawal(string);

    function setRate(uint _rate) internal {
        rate = _rate;
        rateHistory.push(int(_rate));
    }

    function eurToUsd(uint eur) public view returns(uint) {
        return eur * rate / 100;
    }

    function usdToEur(uint dol) public payable returns(uint) {
        uint256 amount = uint256(msg.value);
        require(amount >= 0.001 * 10**18, "Amount must be greater than 0.001 ETH");
```

Plan

Quelques attaques sur les protocoles de blockchains

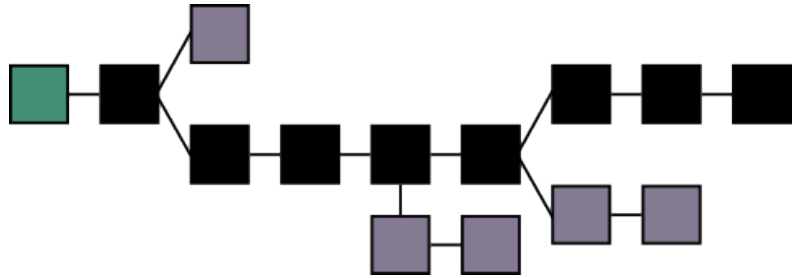
- **Attaque par devancement** (*Race attack*, double dépense)
- **Attaque à 51%** ou attaque majoritaire
- **Attaque Sybil** ou attaque multi-identités
- **Attaque rien à perdre** (sur PoS, *many-forks*)
- **Attaque ré-entrante** (contrats & prog. concurrente)
- **Attaque sur IOTA** (Mauvaise cryptographie)

Attaque par devancement: double dépense



- 2 transactions simultanées des mêmes 10฿
  - ⇨ seule 1 des 2 transactions perdure

Attaque par devancement: double dépense



- 2 transactions simultanées des mêmes 10฿
  - ⇨ seule 1 des 2 transactions perdure

Contre mesures

Seule la plus longue chaîne persiste

Attaque à 51%

- Réorganisations de la chaîne, données normales :
  - 1 ou 2 blocs en arrière (profondeur, *depth*)
  - remplacés par 1 ou 2 blocs (longueur, *length*)
  - cf. probabilité de minage simultané

Attaque à 51%

- Réorganisations de la chaîne, données normales :
  - 1 ou 2 blocs en arrière (profondeur, *depth*)
  - remplacés par 1 ou 2 blocs (longueur, *length*)
  - cf. probabilité de minage simultané

ETC, 5 janvier 2019, 219 500 ETC (≈$1.1M)

Block	Depth	Length	Double spent
7245623	4	7	–
7248488	5	6	–
7249343	57	74	600 ETC
7254419	32	53	4 000 ETC
7254568	123	140	5 000 ETC
7255033	60	79	9 000 ETC
7255204	25	35	9 000 ETC
7255476	37	46	15 700 ETC
7255542	67	85	15 700 ETC
7255662	62	110	24 500 ETC
7255998	69	86	5 000 ETC
7261497	44	54	26 000 ETC
7261603	35	44	52 800 ETC
7261647	8	9	–
7261676	37	47	52 200 ETC

PoS: Attaque “rien à perdre” (*Nothing at stake*)

⚠ Multiplier les forks ne coûte plus rien ...

⇨ ... DDoS ?

PoS: Attaque “rien à perdre” (*Nothing at stake*)

⚠ Multiplier les forks ne coûte plus rien ...

⇨ ... DDoS ?

Contre mesures

- **Slasher** : *punitive PoS*
  - diminue les récompenses si mauvais comportement
- **Tezos** : dépôt d'une caution gelée >> récompense
  - Risque : perte immédiate de toutes les cautions
  - Libérée 2 semaines après validation
  - Liste de priorité des valideurs (*liveness*)

Décentralisation = calcul distribué

⚠ Attaques ré-entrantes

⇨ Exemple de l'exploit *The DAO*, 17 juin 2016

Contrat type DAO

```
function withdraw(unit amount) {
  client = msg.sender:
  if (balance[client] >= amount} {
    if (client.call.sendMoney(amount)) {
      balance[client] -= amount;
    }
  }
}
```

Décentralisation = calcul distribué

⚠ Attaques ré-entrantes

⇨ Exemple de l'exploit *The DAO*, 17 juin 2016

Contrat type DAO

```
function withdraw(unit amount) {
  client = msg.sender:
  if (balance[client] >= amount} {
    if (client.call.sendMoney(amount)) {
      balance[client] -= amount;
    }
  }
}
```

Exploit type-DAO.

```
function sendMoney(unit amount) {
  victim = msg.sender;
  balance += amount;
  victim.withdraw(amount);
}
```

Décentralisation = calcul distribué

⚠ Attaques ré-entrantes

⇨ Exemple de l'exploit *The DAO*, 17 juin 2016

Contrat type DAO

```
function withdraw(unit amount) {
  client = msg.sender:
  if (balance[client] >= amount} {
    if (client.call.sendMoney(amount)) {
      balance[client] -= amount;
    }
  }
}
```

Exploit type-DAO.

```
function sendMoney(unit amount) {
  victim = msg.sender;
  balance += amount;
  victim.withdraw(amount);
}
```

Contre mesures

mutex, sémaphores, etc.

IOTA : S-box [1]

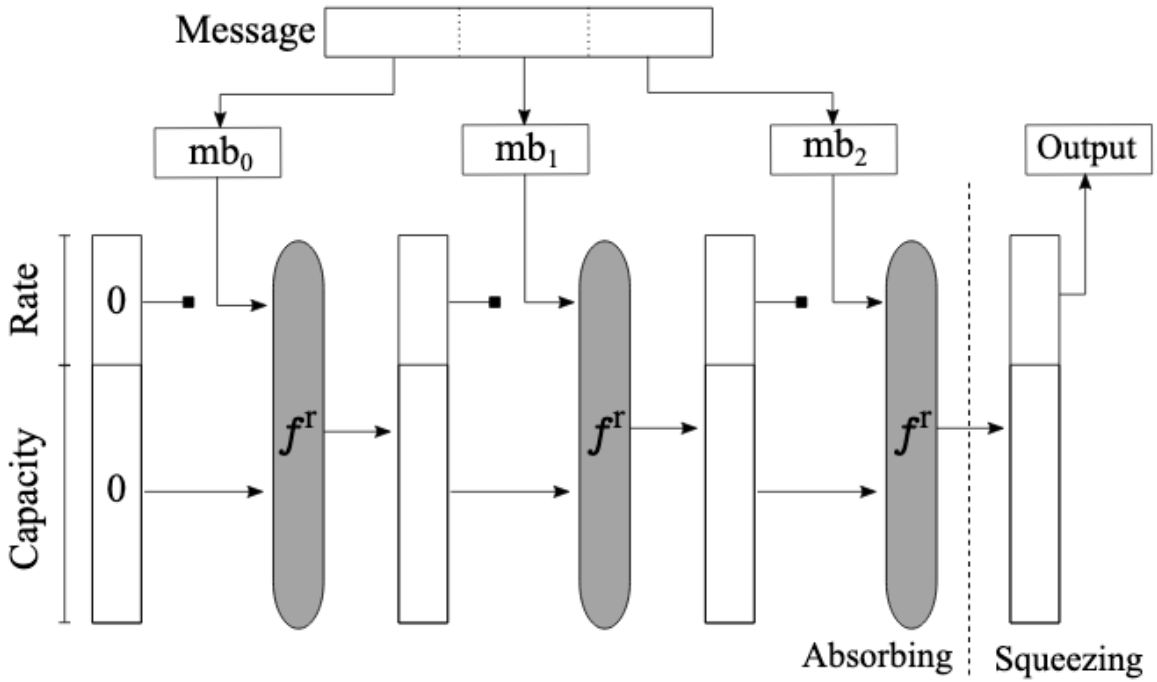


Fig. 1. The Curl-P construction.

[1] *Cryptanalysis of Curl-P and Other Attackson the IOTA Cryptocurrency* by Ethan Heilman, Neha Narula, Garrett Tanzer, James Lovejoy, Michael Colavita, Madars Virza, and Tadge Dryja

IOTA : S-box

AES 256 en Hexa

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Curl-P-27

	-1	0	1
-1	1	1	-1
0	0	-1	1
1	-1	0	0

23-bit collision resistance !

Plan

5 Choses à retenir

- La révolution Blockchain est en marche
- Un formidable outil
- Systèmes décentralisés
- De nombreuses applications mais bien comprendre les limites
- La cryptographie est au centre de la sécurité

Merci pour votre attention

Questions ?

pascal.lafourcade@uca.fr

LIMOS
LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Mathinfoly #2019

Cryptographie, blockchain et vérification de programmes

Du 24 au 31 août - INSA - Lyon - France

`http://www.mathinfoly.org/`

Programme

- Initiation à la cryptographie, introduction aux blockchains et à la logique propositionnelle - Pascal Lafourcade
- Writing and Verifying Functional Programs in Coq - Cătălin Hriţcu

Dépôt du dossier de candidature jusqu'au 30 juin.

Contact : +33 6 98 04 93 01

`mathinfoly2019@plaisir-maths.fr`

LIMOS LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Rencontre **E**ntreprises **DOC**torants en **S**écurité

+

AIRBUS CRYPTO EXPERTS
Quarkslab SECURING EVERY BIT OF YOUR DATA
AMOSSYS
MINISTÈRE DES ARMÉES
gemalto security to be free
THALES Together • Safer • Everywhere
IDNOMIC
Worldline
UBISOFT

+

= REDOCS

REDOCS

Edition 2019 :

- **Date** : 21 au 25 Octobre 2019
- **Lieu**: Gif-sur-Yvette



- **Inscriptions** : by email `redocs-org@irisa.fr`
  - CV académique
  - email d'autorisation du directeur de thèse
    + prise en charge du déplacement

Sujets REDOCS'19

Entreprises :

Sujets :

- Analyse de logs par des méthodes de machine learning
- Mise en œuvre de techniques stéganographiques basées sur le machine-learning pour le déploiement d'attaque par logiciel malveillant
- ?

`https://gdr-securite.irisa.fr/redocs/`