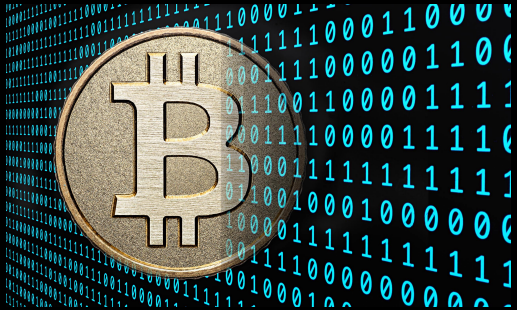
L'épopée Bitcoin

Pascal Lafourcade

Clermont 20 Mai 2019

La révolution Bitcoin 2009

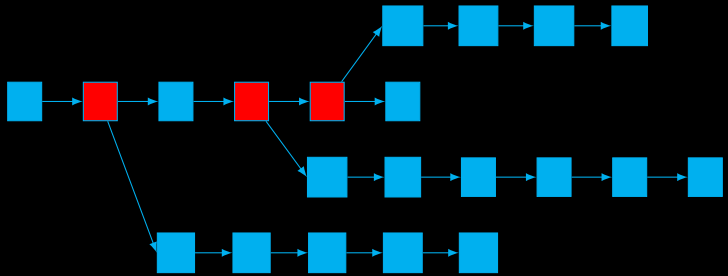


Taux de change du bitcoin

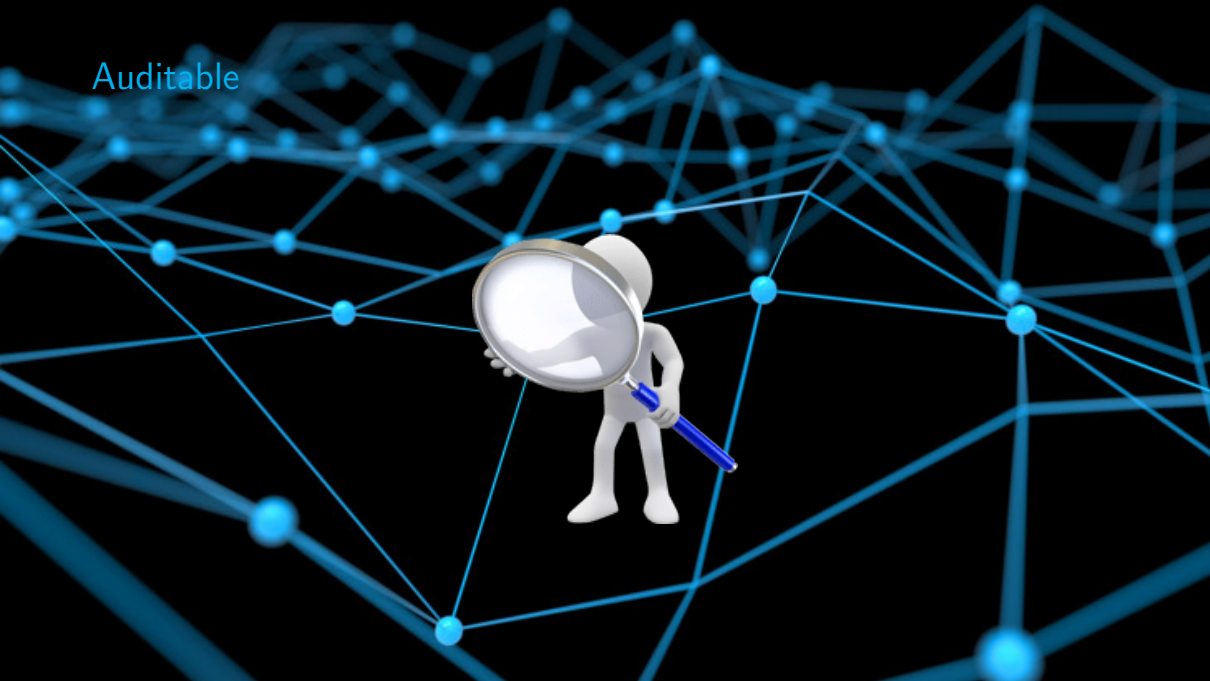

Décentralisée
Distribuée
Consensus

Inarrêtable

Infalsifiable



Auditable



Signature

Signature

signature

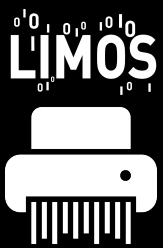
clef secréte

vérification

clef publique

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

$$H : \{0,1\}^* \to \{0,1\}^n$$



12f9a5185c8f

6b2580130ec1

85c1202645b5

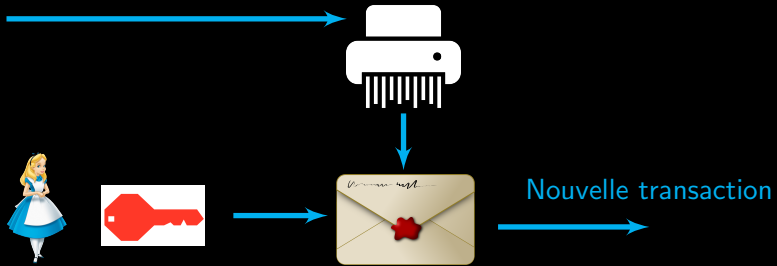
Propriété : Collision résistance

$\neq$

85c1202645b5 $=$ 85c1202645b5

Comment faire une transaction?

Précédent block de transactions



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

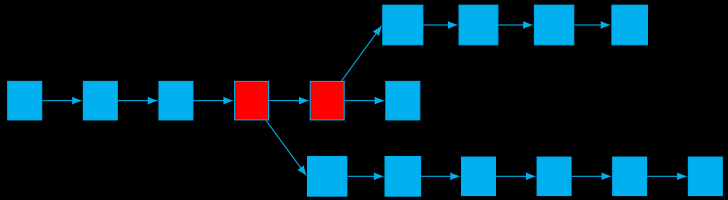
 (C,B,9,458237)=936127

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, 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, 0)) = ASCIISUM(65+66+49+50+51+52+48)
= ASCIISUM (381) = 51+56+49 = 156

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 : ASCIISUM(ASCIISUM(X, Y, Montant, nonce)) divisible par 3 et 5
Hash du block précédent : 42

Alice donne à Dave 5 BTC : $A, D, 5$

Bob donne à Charlie 9 BTC : $B, C, 9$

Bob donne à Dave 7 BTC : $B, D, 7$

Charlie donne à Alice 3 BTC : $C, A, 3$

Quelques solutions

ASCIISUM(ASCIISUM(A, D, 5, 6)) = 240
ASCIISUM(ASCIISUM(A, D, 5, 12)) = 285

ASCIISUM(ASCIISUM(B,C,9,452)) = 345

ASCIISUM(ASCIISUM(B,D,7,3)) = 240
ASCIISUM(ASCIISUM(B,D,7,8)) = 245

ASCIISUM(ASCIISUM(C,A,3,9)) = 240

Miner : Objectif de hachage

Cible = 00000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076

Trouver un nonce n_i tel que

$$\text{SHA-256}(\text{SHA-256}(\text{HBlock}_{i-1}, \text{Transactions}, n_i)) = x < \textit{Cible}$$

Avoir au moins 18 zéros au début de x

Miner : Objectif de hachage

Cible = 00000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076

Trouver un nonce n_i tel que

$$\text{SHA-256}(\text{SHA-256}(\text{HBlock}_{i-1}, \text{Transactions}, n_i)) = x < \textit{Cible}$$

Avoir au moins 18 zéros au début de x

Stratégie : Tester toutes les valeurs possibles pour n_i

Miner des Bitcoins

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

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

Traçable vs Anonyme

Traçable vs Anonyme

Limitations

10 minutes

Taille des transactions

Limitations

10 minutes

Taille des transactions

Lightning Network

14 secondes

Energivore

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

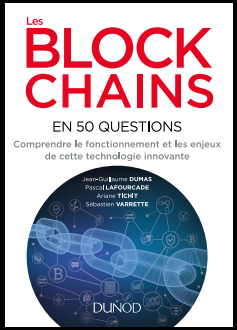
Proof of Stake
Lightning Network

Choses à retenir

- Bitcoin $\Rightarrow$ Registre distribué, infalsifiable et auditable
- Avoir les clefs privées et ne pas les perdre
- Pas de crédits possible
- Révolution Blockchain

Merci pour votre attention

Questions ?



pascal.lafourcade@uca.fr