Bitcoin

Éric BERTHOMIER
eric.berthomier@free.fr

16 mars 2022

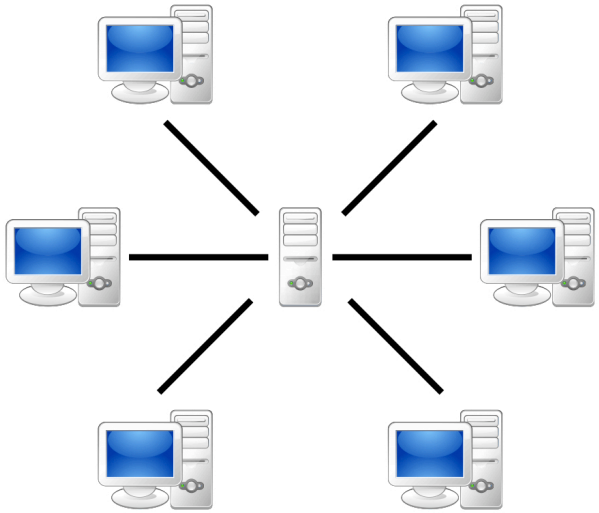
Version 1.0 - Version Stagiaire

la cryptomonnaie

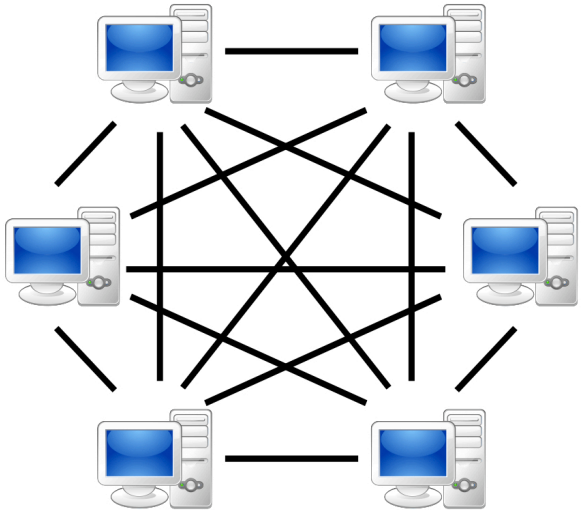
La cryptomonnaie s'appuie sur différentes technologies informatiques :

- La BlockChain
- P2P (Peer To Peer)
- Cryptographie à clés publiques
- Fonctions de hashage
- L'arbre de Merkle (Merkle Tree)
- La preuve de travail (Proof of Work (POW))

P2P : Peer To Peer

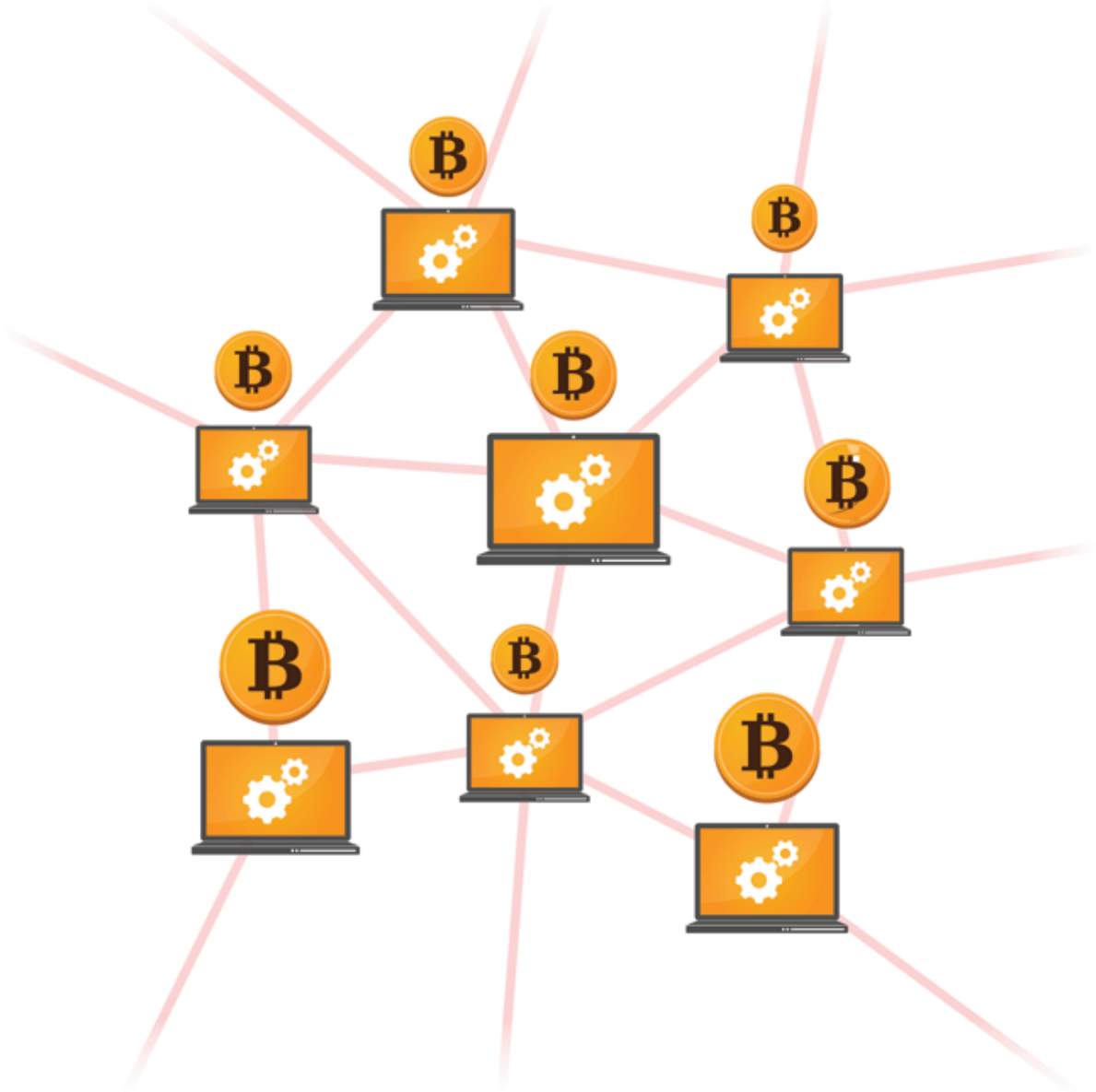


Server-based

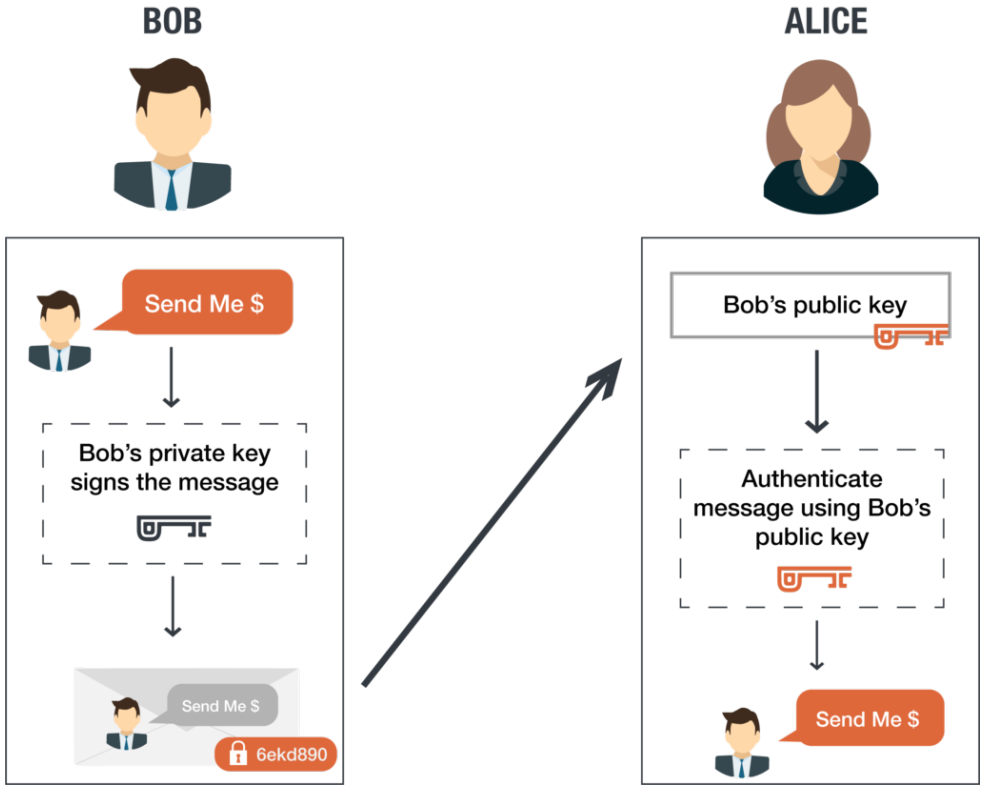


P2P-network

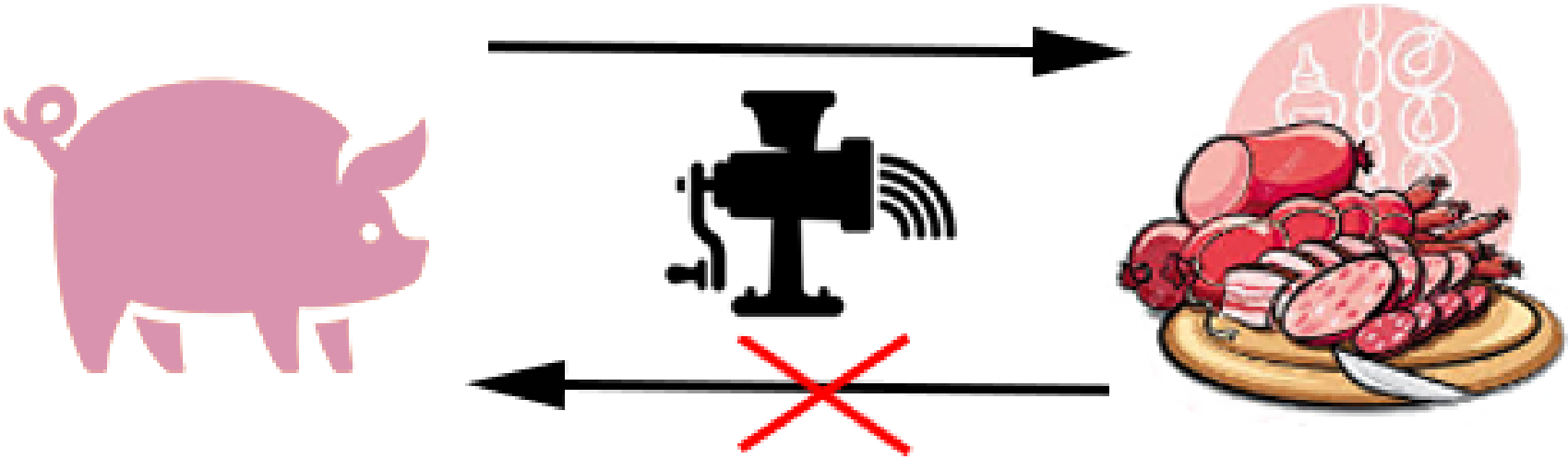
P2P pour le bitcoin



Cryptographie à clés publiques

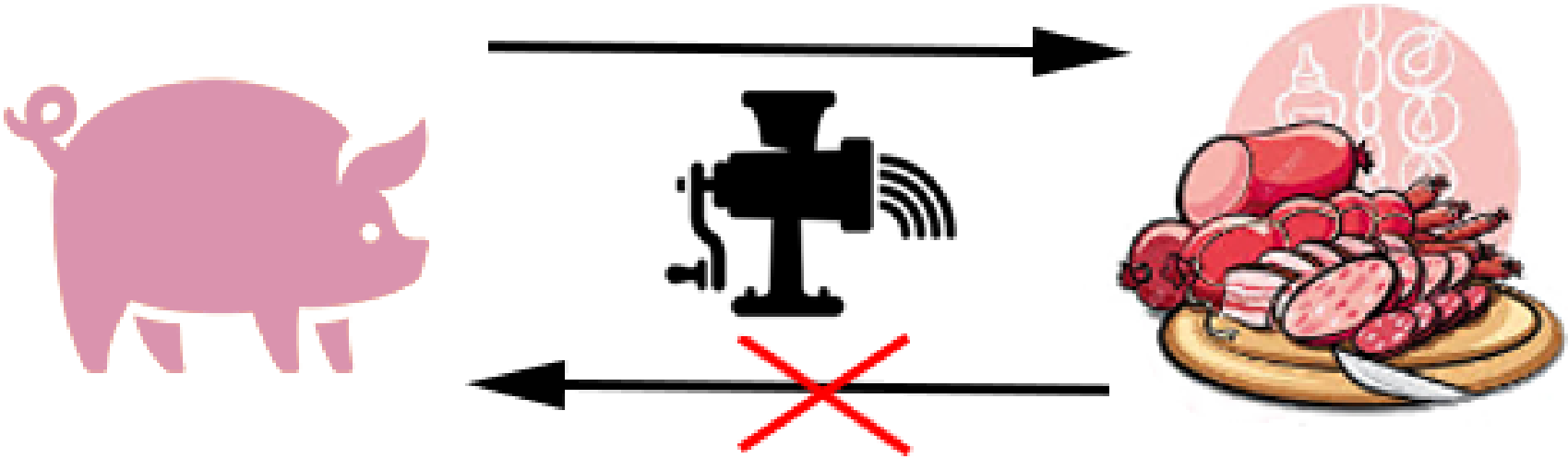


Fonction de hashage



À une donnée entrée ne correspond qu'une seule et unique donnée en sortie.

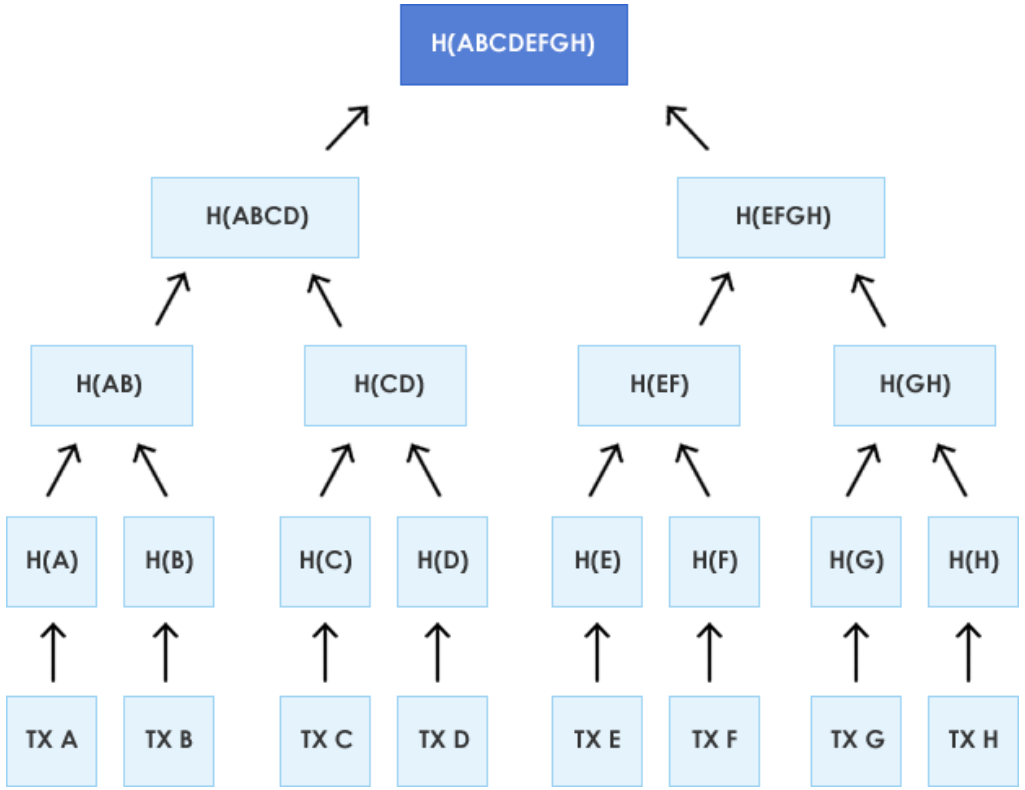
Fonction de hashage



À une donnée entrée ne correspond qu'une seule et unique donnée en sortie.
Il est impossible de partir du haché pour revenir à la source.

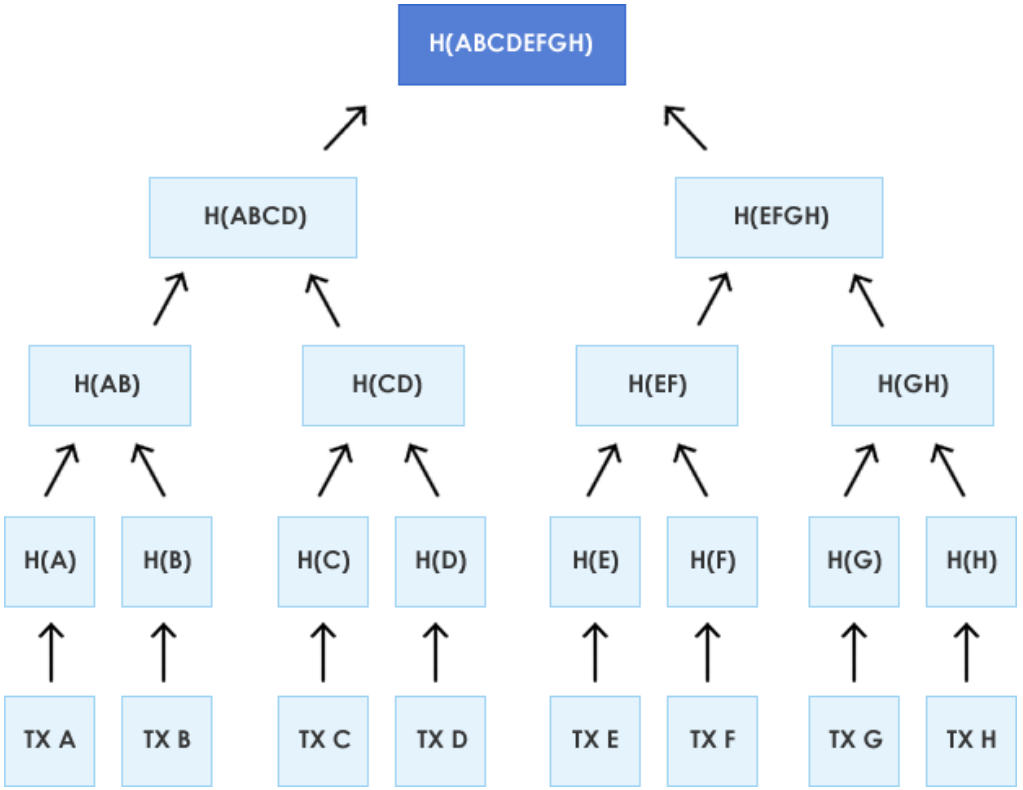
Arbre et racine de Merkle (Root and Merkle Tree)

La racine de Merkle est une empreinte numérique condensée de l'ensemble des transactions du bloc.



Arbre et racine de Merkle (Root and Merkle Tree)

La racine de Merkle est une empreinte numérique condensée de l'ensemble des transactions du bloc.



La moindre modification d'une transaction dans le bloc modifie la racine.

Principe de la Preuve de Travail (Proof of Work)

Difficile à résoudre . . .

8				4	9		5	
2	6	9	5					
							7	
					7			
				2			4	5
	9				6			
		1			2	7		9
9		6			5		8	1
		8						

Principe de la Preuve de Travail (Proof of Work)

Facile à prouver...

8				**4**	**9**		**5**	
2	**6**	**9**	**5**					
							7	
					7			
				2			**4**	**5**
	9				**6**			
		1			**2**	**7**		**9**
9		**6**			**5**		**8**	**1**
		8						

8	1	7	6	**4**	**9**	2	**5**	3
2	**6**	**9**	**5**	7	3	8	1	4
5	3	4	2	1	8	9	**7**	6
6	4	2	3	5	**7**	1	9	8
7	8	3	9	**2**	1	6	**4**	**5**
1	**9**	5	4	8	**6**	3	2	7
4	5	**1**	8	6	**2**	**7**	3	**9**
9	2	**6**	7	3	**5**	4	**8**	**1**
3	7	**8**	1	9	4	5	6	2

Preuve de Travail (Proof of Work)

- La preuve de travail (ou le protocole de consensus) empêche toute attaque du réseau en rendant non rentable la production de contenus contrefaits.

Preuve de Travail (Proof of Work)

- La preuve de travail (ou le protocole de consensus) empêche toute attaque du réseau en rendant non rentable la production de contenus contrefaits.
- Bitcoin utilise Hashcash, système de preuve de travail conçu par Adam Back.

Preuve de Travail (Proof of Work)

- La preuve de travail (ou le protocole de consensus) empêche toute attaque du réseau en rendant non rentable la production de contenus contrefaits.
- Bitcoin utilise Hashcash, système de preuve de travail conçu par Adam Back.
- L'épreuve consiste donc, pour une chaîne alphanumérique donnée, à y ajouter une chaîne alphanumérique aléatoire jusquà ce que le hash (lempreinte numérique) de l'ensemble soit inférieur à un seuil donné.

Preuve de Travail (Proof of Work)

- La preuve de travail (ou le protocole de consensus) empêche toute attaque du réseau en rendant non rentable la production de contenus contrefaits.
- Bitcoin utilise Hashcash, système de preuve de travail conçu par Adam Back.
- L'épreuve consiste donc, pour une chaîne alphanumérique donnée, à y ajouter une chaîne alphanumérique aléatoire jusquà ce que le hash (lempreinte numérique) de l'ensemble soit inférieur à un seuil donné.
- Ce seuil est mis régulièrement et automatiquement à jour pour que l'intervalle moyen entre deux blocs reste de dix minutes.

Preuve de Travail (Proof of Work)

- La preuve de travail (ou le protocole de consensus) empêche toute attaque du réseau en rendant non rentable la production de contenus contrefaits.
- Bitcoin utilise Hashcash, système de preuve de travail conçu par Adam Back.
- L'épreuve consiste donc, pour une chaîne alphanumérique donnée, à y ajouter une chaîne alphanumérique aléatoire jusquà ce que le hash (lempreinte numérique) de l'ensemble soit inférieur à un seuil donné.
- Ce seuil est mis régulièrement et automatiquement à jour pour que l'intervalle moyen entre deux blocs reste de dix minutes.

Preuve de Travail (Proof of Work)

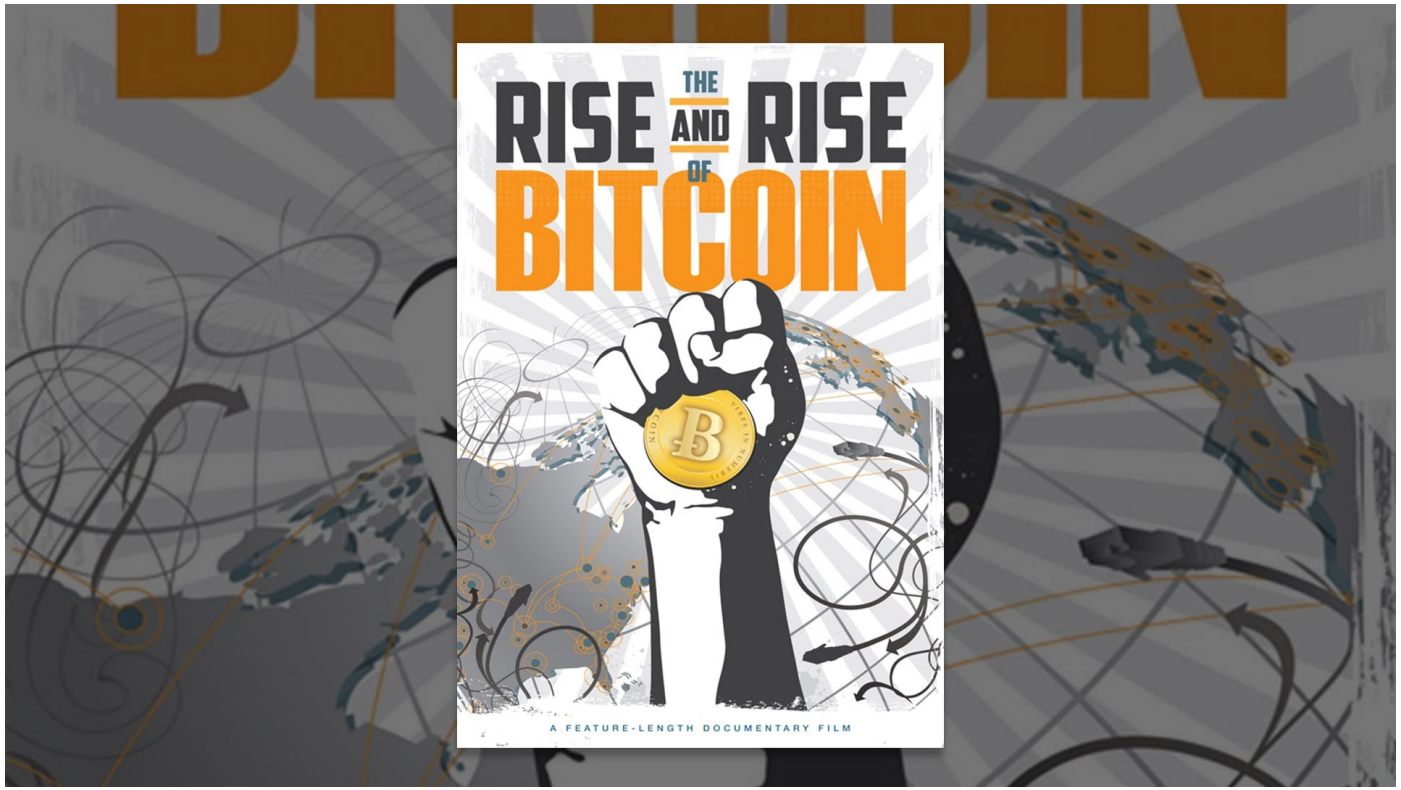
- La preuve de travail (ou le protocole de consensus) empêche toute attaque du réseau en rendant non rentable la production de contenus contrefaits.
- Bitcoin utilise Hashcash, système de preuve de travail conçu par Adam Back.
- L'épreuve consiste donc, pour une chaîne alphanumérique donnée, à y ajouter une chaîne alphanumérique aléatoire jusquà ce que le hash (lempreinte numérique) de l'ensemble soit inférieur à un seuil donné.
- Ce seuil est mis régulièrement et automatiquement à jour pour que l'intervalle moyen entre deux blocs reste de dix minutes.

Démonstration

Preuve de Travail (Proof of Work)

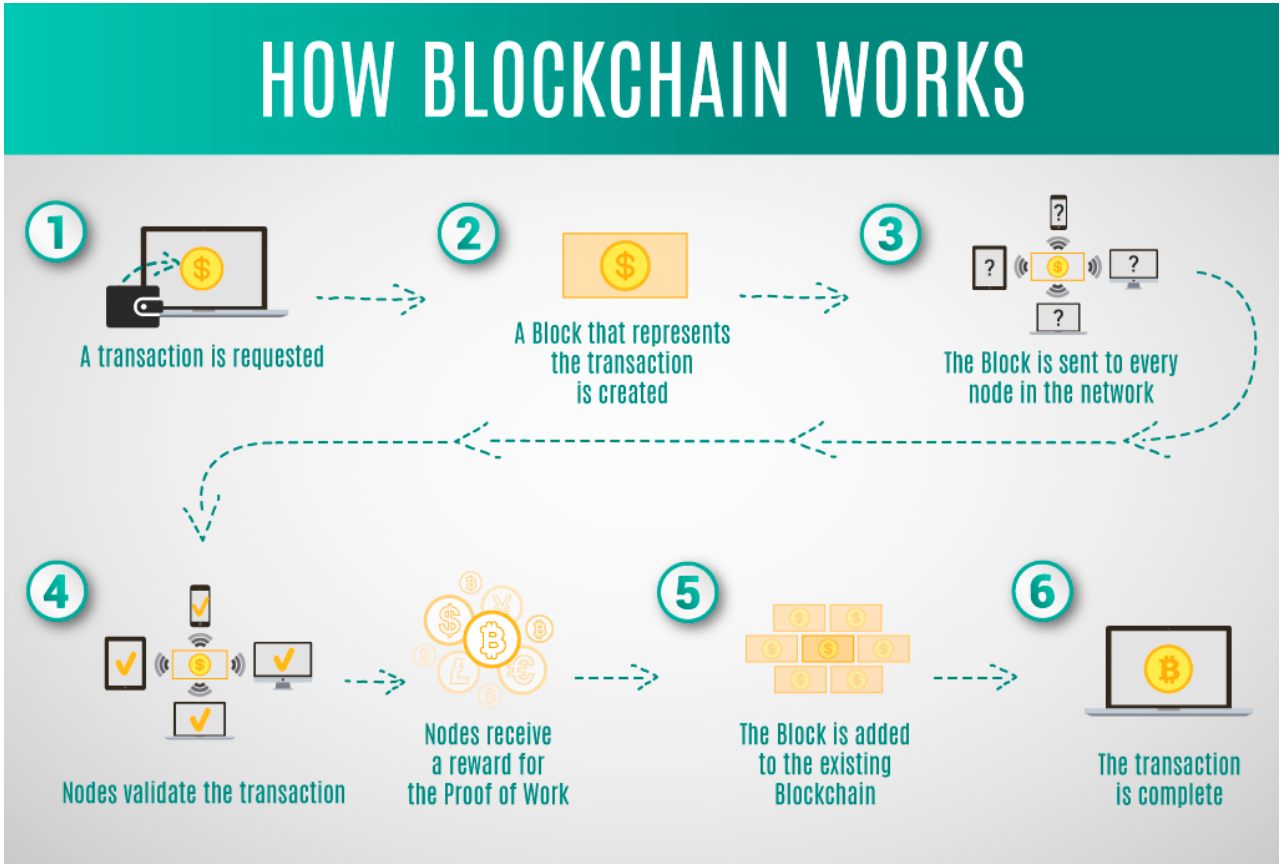
Current Depth	0
Block Size (bytes)	918,064
Nonce	754648945
Merkle Root	45ea2ad8313003f955ec659fa6149fe71761aefb1a9380cd7042424f58937f1c
Bits (difficulty target)	386,964,396
Version	536870912
IP Relayed By	174.129.227.34:8333

Présentation générale du BitCoin



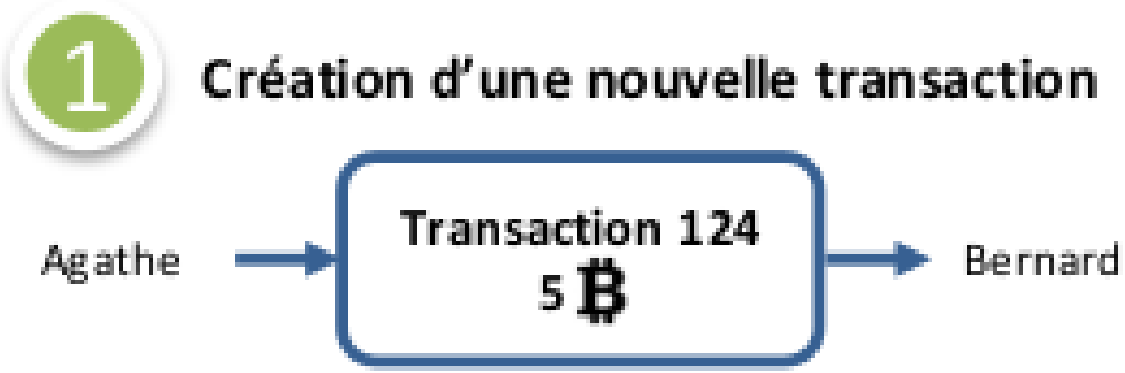
Extrait du documentaire

Fonctionnement du bitcoin



https://www.blockchain.com/explorer?utm_campaign=expnav_explorer

Exemple illustré (1/6)



Agathe identifie Bernard grâce à sa clé publique. La nouvelle transaction se voit attribuée une signature digitale générée par la clé privée d'Agathe qui contient les informations relatives à la transaction.

Source : http://www.smartgrids-cre.fr/media/documents/dossiers/blockchain/Schema_blockchain.pdf

Exemple illustré (2/6)

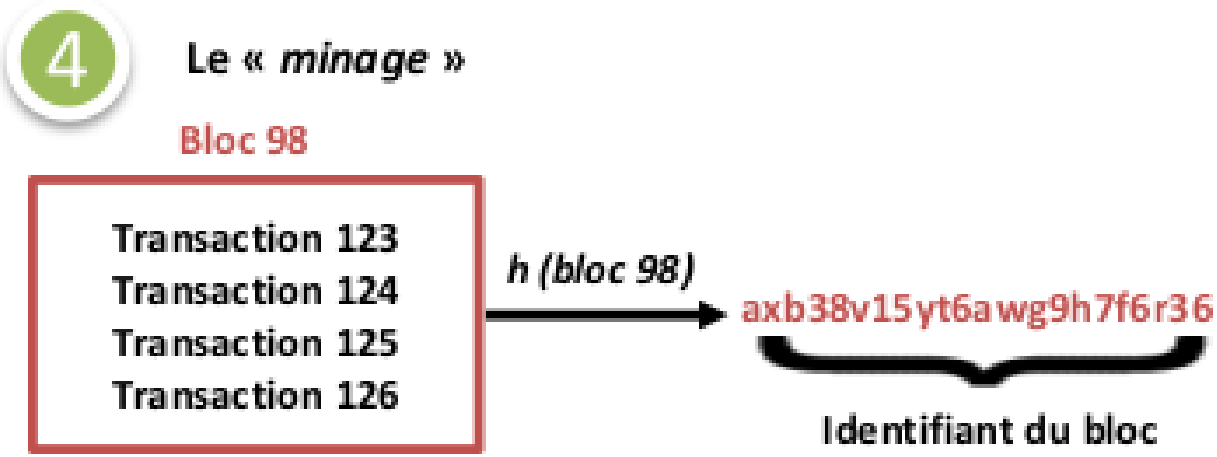
Exemple illustré (3/6)

La liste d'attente des transactions

Transaction 123	Transaction 126
Transaction 124	Transaction 127
Transaction 125	Transaction 128

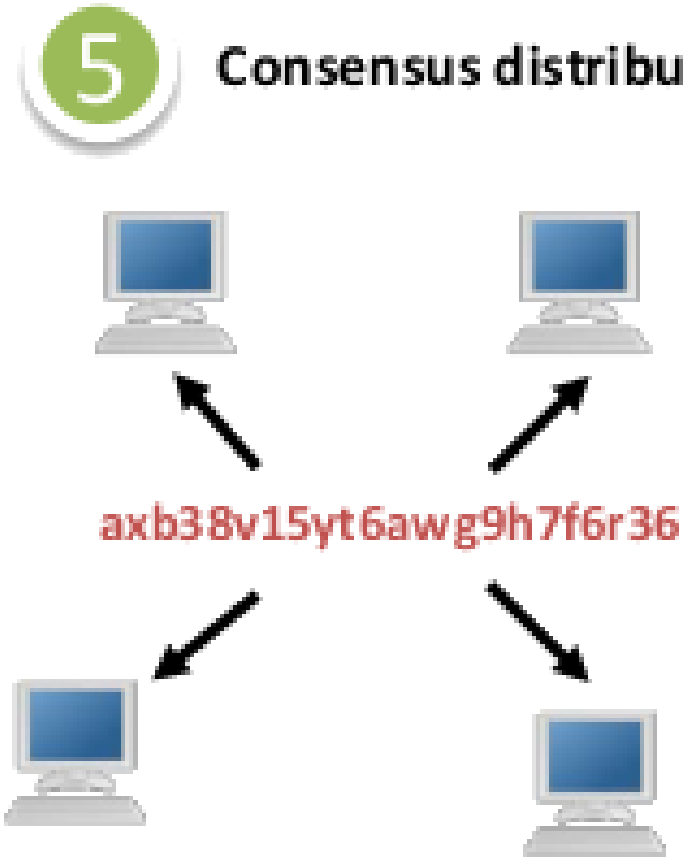
Une fois la transaction vérifiée, elle rejoint la liste d'attente des transactions qui est diffusée sur tout le réseau.

Exemple illustré (4/6)



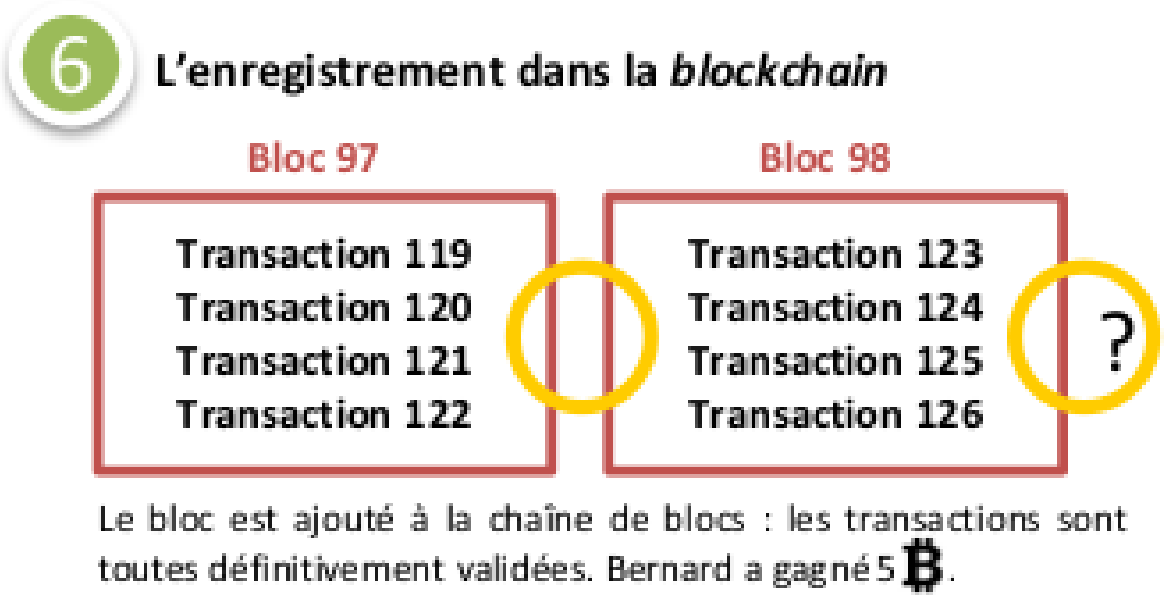
Un « *mineur* » regroupe plusieurs transaction dans un bloc auquel il applique une fonction cryptographique dite de « *hash* ». La solution trouvée constitue l'identifiant du bloc en attente de validation.

Exemple illustré (5/6)



L'identifiant (la solution) trouvé est diffusé sur le réseau à tous les « *mineurs* » qui doivent le valider pour que le bloc soit ajouté à la blockchain avec ce « *hash* ».

Exemple illustré (6/6)



Une transaction en BitCoins

- Lorsque vous effectuez une transaction en bitcoins, celle-ci doit être approuvée par le réseau ($> 51\%$) avant d'être incluse dans un nouveau bloc de la blockchain.

Une transaction en BitCoins

- Lorsque vous effectuez une transaction en bitcoins, celle-ci doit être approuvée par le réseau ($> 51\%$) avant d'être incluse dans un nouveau bloc de la blockchain.
- Pour être approuvée, le protocole utilise la norme Proof of Work. Dans le cadre du BitCoin, on nomme ceci Minage.

Une transaction en BitCoins

- Lorsque vous effectuez une transaction en bitcoins, celle-ci doit être approuvée par le réseau ($> 51\%$) avant d'être incluse dans un nouveau bloc de la blockchain.
- Pour être approuvée, le protocole utilise la norme Proof of Work. Dans le cadre du BitCoin, on nomme ceci Minage.
- Ce travail est récompensé par les éventuels frais associés à la transaction et par le Bitcoin lui-même (pour les plus rapides).

Minage

Le minage

- Pour pouvoir générer des nouveaux blocks et valider l'ensemble des éléments nécessaires à une transaction, il faut énormément de calculs, ce qui signifie une consommation d'énergie.

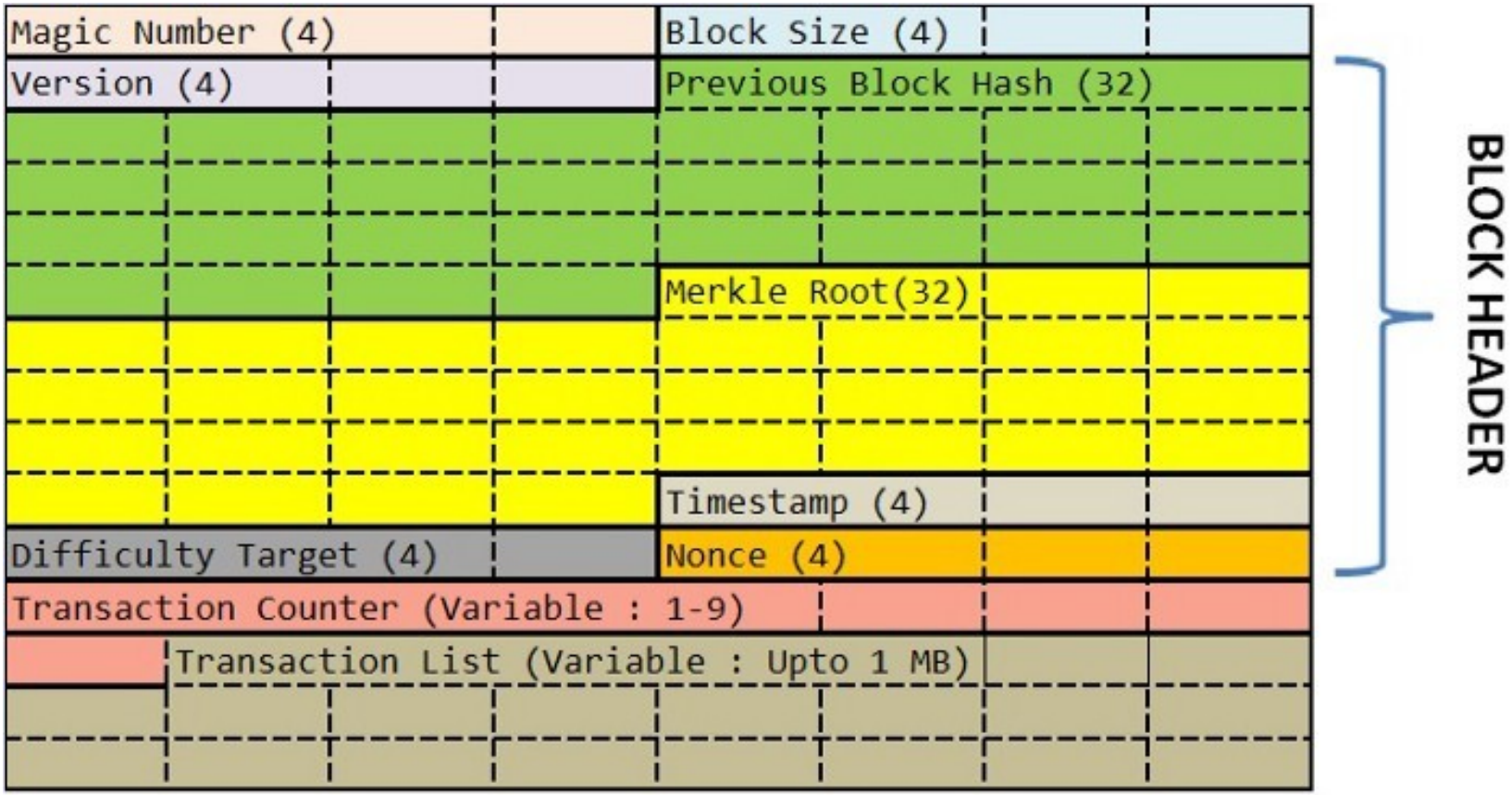
Le minage

- Pour pouvoir générer des nouveaux blocks et valider l'ensemble des éléments nécessaires à une transaction, il faut énormément de calculs, ce qui signifie une consommation d'énergie.
- Afin de rétribuer ceux qui font vivre cette chaîne, le mineur ou plutôt le pool de mineurs qui trouve la solution à un problème défini en premier est rémunéré en Bitcoins.

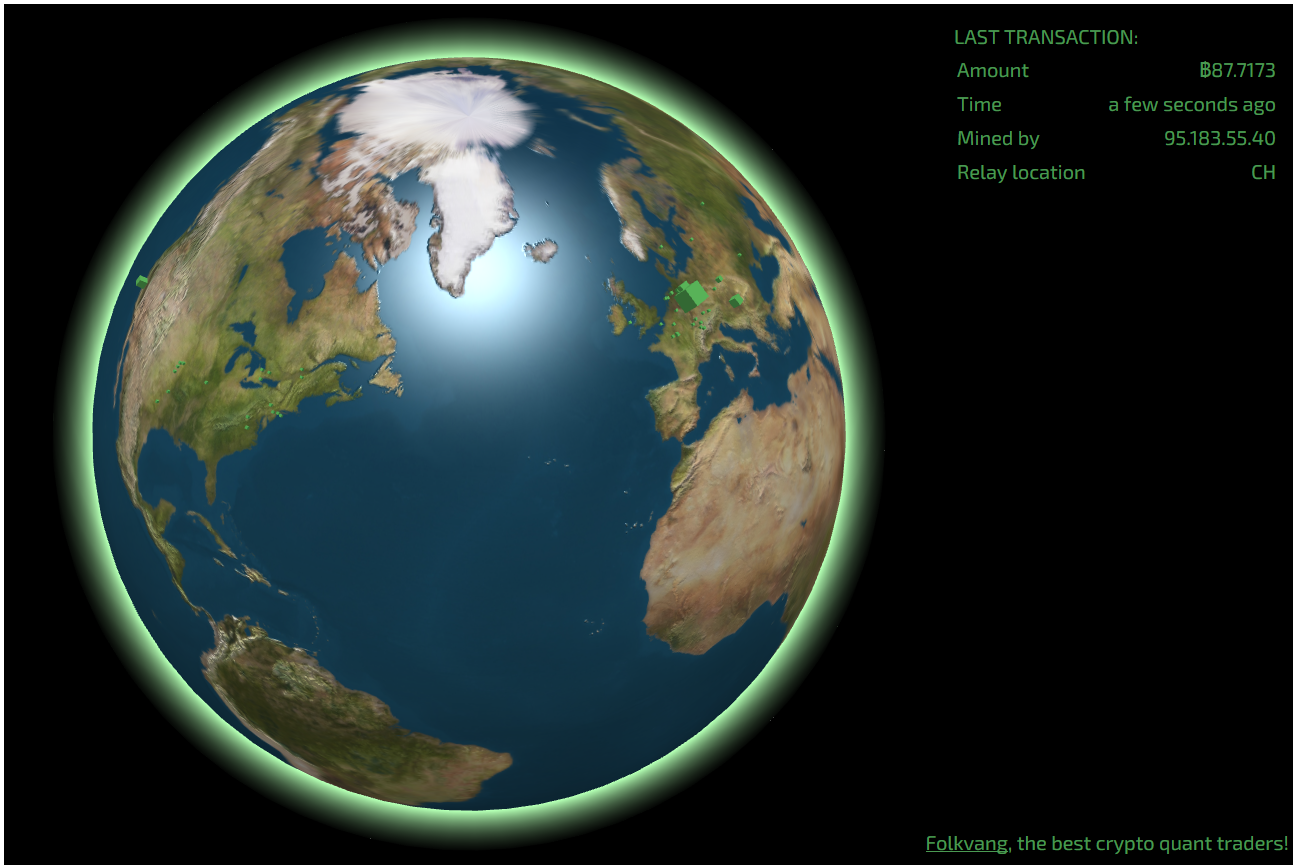
Le minage

- Pour pouvoir générer des nouveaux blocks et valider l'ensemble des éléments nécessaires à une transaction, il faut énormément de calculs, ce qui signifie une consommation d'énergie.
- Afin de rétribuer ceux qui font vivre cette chaîne, le mineur ou plutôt le pool de mineurs qui trouve la solution à un problème défini en premier est rémunéré en Bitcoins.
- Cette rémunération baisse tous les 4 ans de moitié et est en 2019 de 12,5 ฿.

Structure d'un block



Transactions temps réel



https://blocks.wizb.it/

Bibliographie

- Documentaire : Bitcoin Big Bang - L'improbable épopée de Mark Karpeles
- Documentaire : Rise and Rise of Bitcoin
- Le Journal du Coin
- Medium
- GitHub