ARCHITECTURES DE CONFIANCE

Infrastructures centralisées

- Infrastructures à clefs symétriques (Kerberos)
- PKI à clef publique (classique) : PKIX (certificats X509)
- Confiance en la racine du système (Root of Trust)

Infrastructures distribuées

- PGP : chaque utilisateur peut signer les certificats
- Confiance aux certificats signés par des utilisateurs en qui on a confiance
- « Web of Trust »

Blockchain (ou distributed ledger)

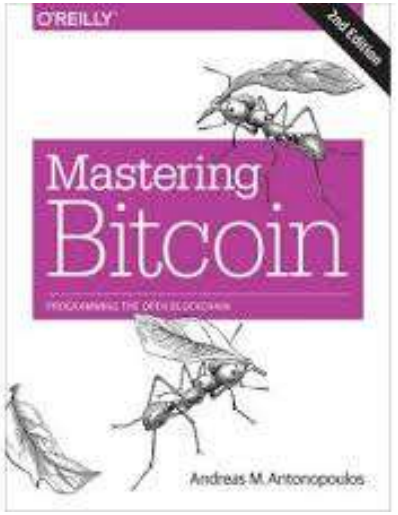
- Registre séquentiel unique qui enregistre TOUTES les transactions
- Chacun peut, facilement, vérifier le registre, I.e. la validité des transactions
- Ajouter une transaction demande du travail et rapporte
  - Analogie avec l'or et les mineurs
- Confiance dans la validité du registre et ses pairs:
  - Toute erreur (transaction non valide) finira par être vue par un pair

HTTP://WWW.SUNCHAIN.FR

Blockchain - références

- **Bitcoin and Cryptocurrency Technologies**
  http://bitcoinbook.cs.princeton.edu
  (12 cours en video)

- Mastering Bitcoin –Unlicking Digital Currencies-
  A.M. Antonopoulos, O'Reilly
  https://github.com/bitcoinbook/bitcoinbook



- Liens
  - Blockchain.info – le cours de BTC etc
  - Ethereum.org – blockchain programming
  - Hyperledger.org – standards for blockchains (MOOCs)
  - R3CEV.com (registre distribué basé sur Corda)

- Exposés
  - Wikipedia « blockchain »
  - Silvio Micali : ALGORAND: The Efficient and Democratic Ledger
    https://www.youtube.com/watch?v=Xauku8XWoSE
  - **Christine Hennebert (CEA – LETI) « Cryptographie dans la blockchain »**
  - Terence Spies (HPE) « Blockchain mechanics »
  - …

LA BLOCKCHAIN, UNE NOUVELLE FAÇON DE CONCEVOIR

La technologie **BlockChain** apporte à la **transaction**
ce qu'Internet apporte à la communication

La technologie **BlockChain** ou **Distributed Ledger**

FOURNIT	PERMET	POUR PLUS DE
INTÉGRITÉ TRAÇABILITÉ	NON RÉPUDIATION AUDITABILITÉ	CONFIANCE EGALITÉ TRANSPARENCE

Par l'intermédiaire d'une **valeur** : crypto-monnaie, token

QUI DIT CRYPTO-MONNAIE, DIT CRYPTOGRAPHIE

La **cryptographie** est **omniprésente** dans l'architecture d'une blockchain

Deux fonctions cryptographiques massivement utilisées :

FONCTION DE HASHAGE

Pour générer une empreinte de taille fixe

1. **Robuste aux collisions**

   Toute modification des données initiales induit une empreinte différente

2. **Fonction à sens unique**

   Remonter aux données à partir de l'empreinte est réputé extrêmement difficile

3. **Utilisée**
   - comme identifiant
   - pour garantir l'intégrité
   - comme preuve d'existence
   - à la réalisation d'une preuve de travail
   - pour chainer les blocs de façon infalsifiable

SIGNATURE NUMÉRIQUE

Repose sur un crypto-système asymétrique à clé publique / clé privée

1. **Algorithme de signatire (ECDSA)**

2. **Permet de vérifier**
   - L'intégrité d'une transaction signée
   - L'identité du signataire

3. **Utilise la signature pour prouver la possession d'une adresse**

Objectif:

- Blockchains
- Bitcoin
- Smart contracts

Comment fonctionnent-ils ? Quel intérêt ?

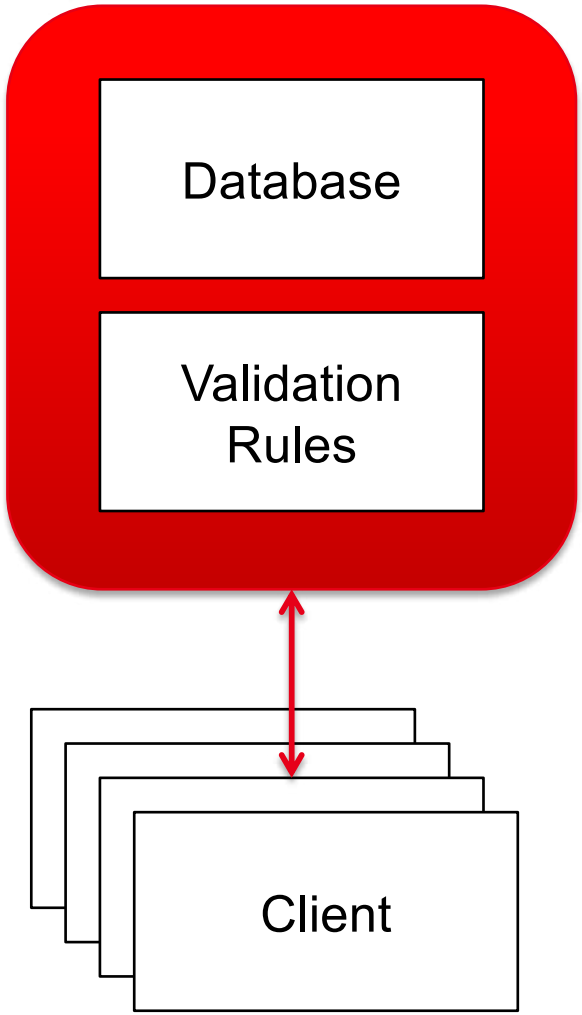
Principe général:

- **Blockcha in = Registre connu de tous qui contient toutes les transactions à partir de l'état initial public.**

- **L'ajout d'un nouveau bloc à la fin de la chaîne peut être fait par n'importe qui mais doit être validé par un consensus majoritaire**

- **Chacun peut vérifier la validité de tout l'historique**
  - Le nombre de transactions est "raisonable"
    - Exemple: bitcoin 255.500 transactions par jour en 11/2020

Ce que permettent les blockchains (ou ledger)

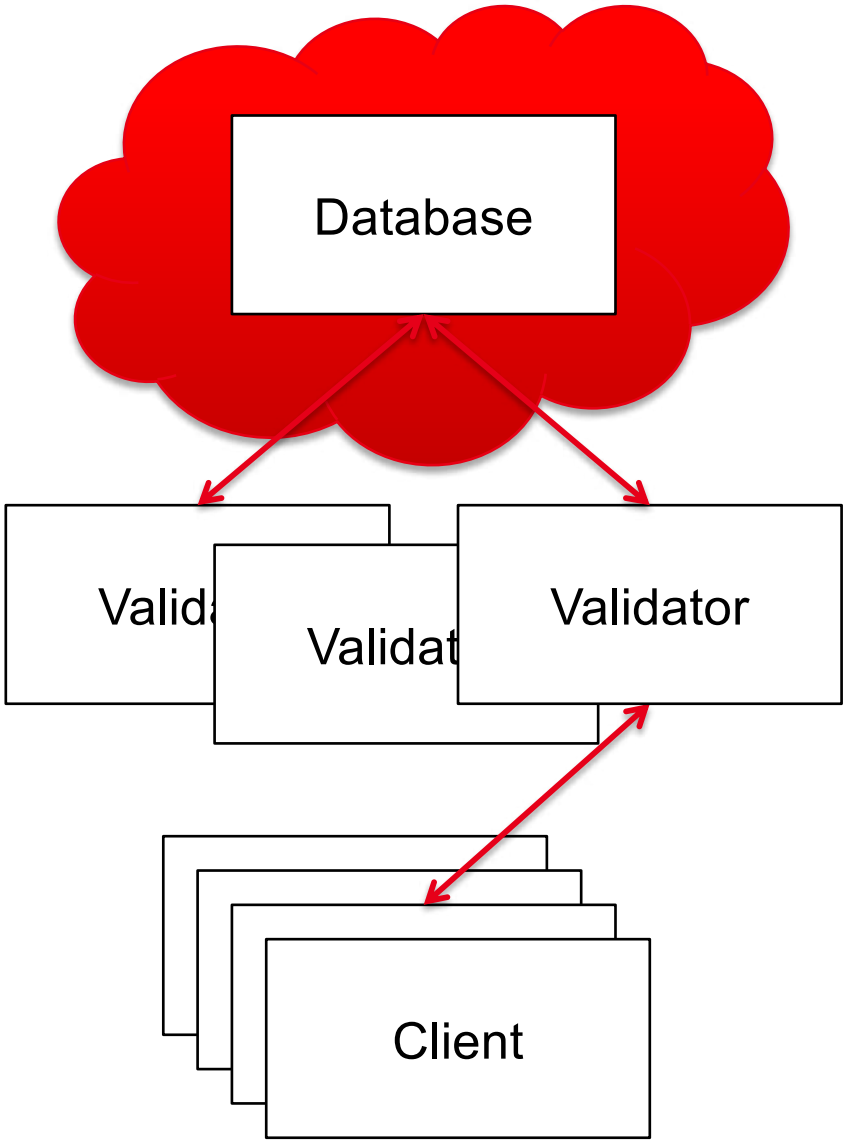


Accè en écriture à une base de données de confiance

Transactions,

datation (timestamping), contrats, etc.

Ce que permettent les blockchains (ou ledger)



Le contrôle d'accès est remplace par un consensus distribué

L'état de la base de données doit être validé par un accord majoritaire

(consensus distribué)

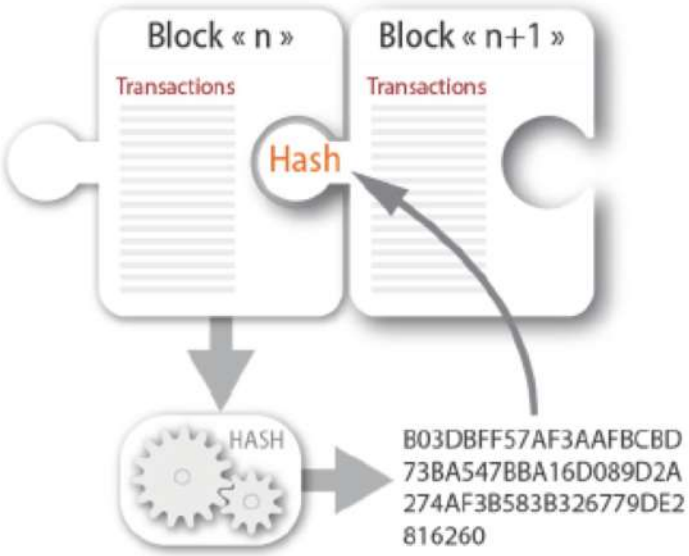
Le consensus distribué permet:

- Le maintien par- des tiers non sûrs de la base en état propre
  (sans leur déléguer la confiance)
- Des règles transparentes de validation des transactions
- La suppression de l'authentification
- ….

SOMMAIRE

FONCTION DE HASHAGE

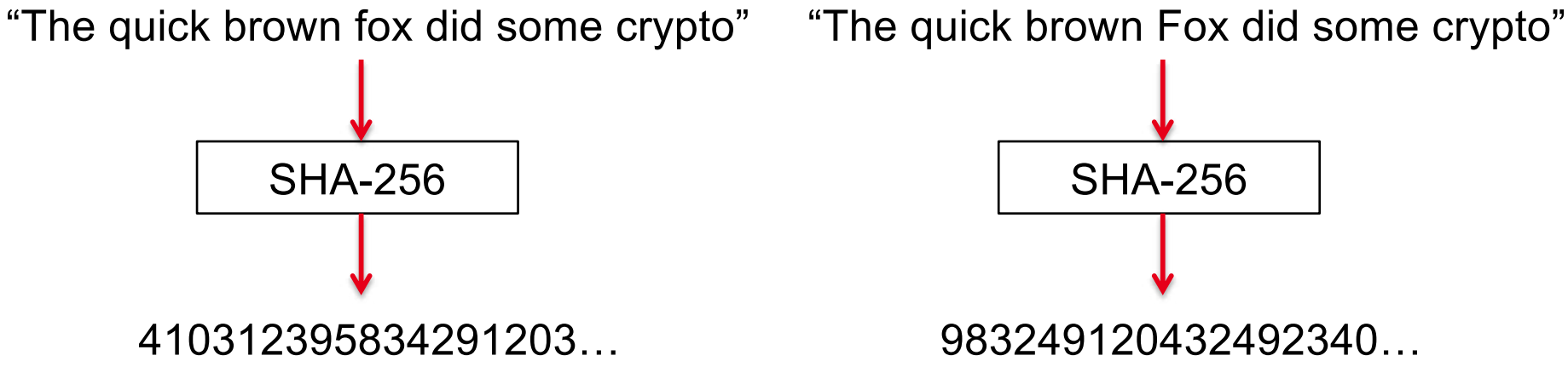
L'**empreinte du bloc « n »** est intégrée dans l'entête du **bloc « n+1 » suivant** :



Une fonction hash (ex SHA-256) prend en entrée un bloc de données

et retourne en sortie un entier de taille fixe

Tout changement de l'entrée perturbe complètement la sortie



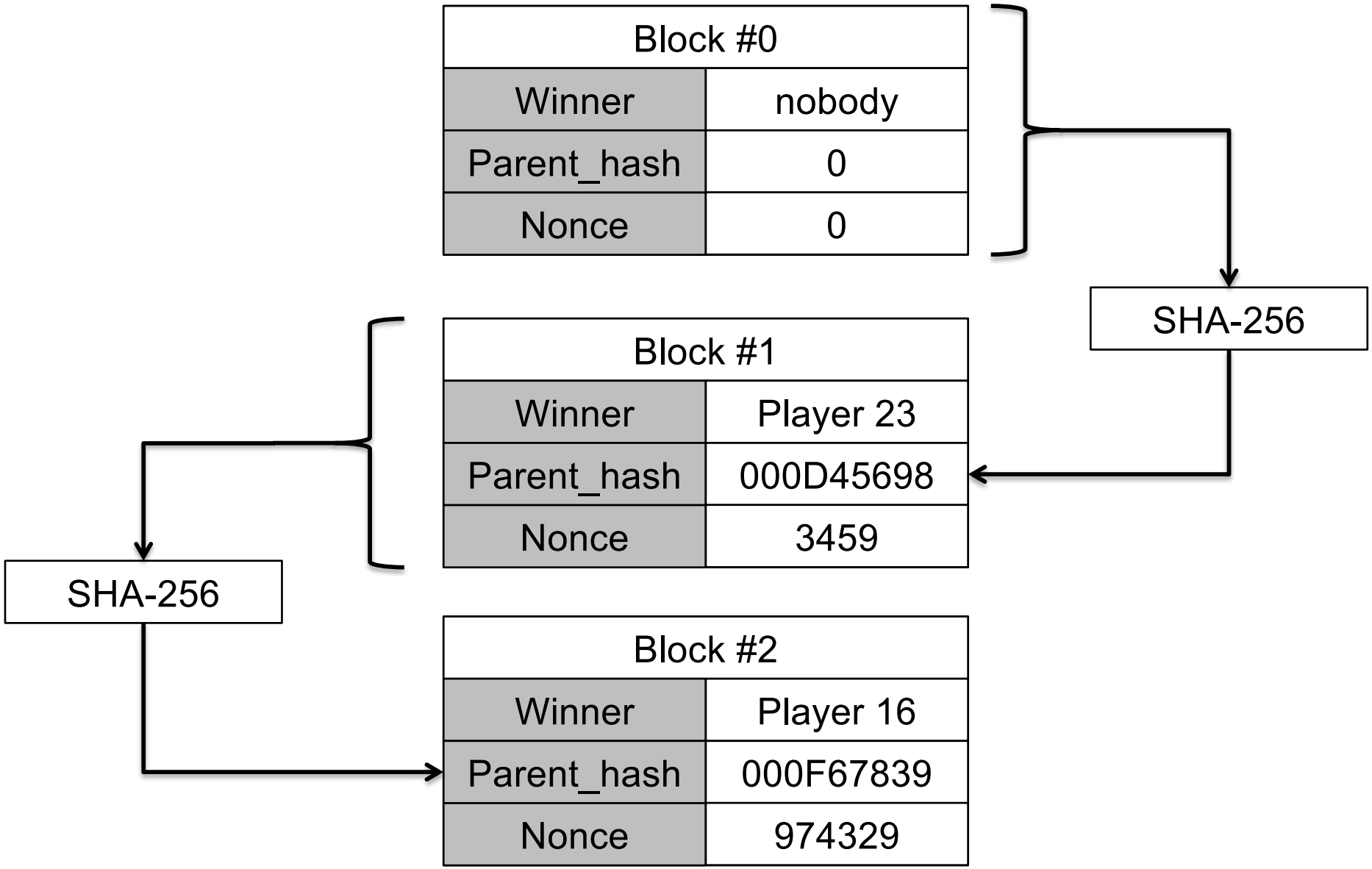
PROOF OF WORK

Etant donné un entier h (de 256 bits),
il est calculatoirement impossible de trouver une entrée x dont le hash est h

On considère que trouver x dont le hash commence par N zeros demande 2^N opérations

***Proof of work*: algorithme par force brute :**
incrémenter un "nonce" jusqu'à trouver le nombre de 0 demandé

in 3e-05 seconds, nonce = 0 yielded 0 zeros. value = 4c8f1205f49e70248939df9c7b704ace62c2245aba9e81641edf…
in 0.000138 seconds, nonce = 12 yielded 1 zeros. value = **0**5017256be77ad2985b36e75e486af325a620a9f29c54…
in 0.000482 seconds, nonce = 112 yielded 2 zeros. value = **00**ae7e0956382f55567d0ed9311cfd41dd2cf5f0a7137…
in 0.014505 seconds, nonce = 3728 yielded 3 zeros. value = **000**b5a6cfc0f076cd81ed3a60682063887cf055e47b…
in 0.595024 seconds, nonce = 181747 yielded 4 zeros. value = **0000**af058b74703b55e27437b89b1ebcc46f45ce55d6….
in 3.491151 seconds, nonce = 1037701 yielded 5 zeros. value = **00000**e55bd0d2027f3024c378e0cc511548c94fbeed0e….
in 32.006105 seconds, nonce = 9913520 yielded 6 zeros. value = **00000**77a77854ee39dc0dc996dea72dad8852afbde6….
in 590.89462 seconds, nonce = 186867248 yielded 7 zeros. value = **0000000**225060b16117b23dbea9ce6be86ac439d….
in 4686.171007 seconds, nonce = 1424462909 yielded 8 zeros. value = **00000000**2dd743724609a9f57260e2492908d….

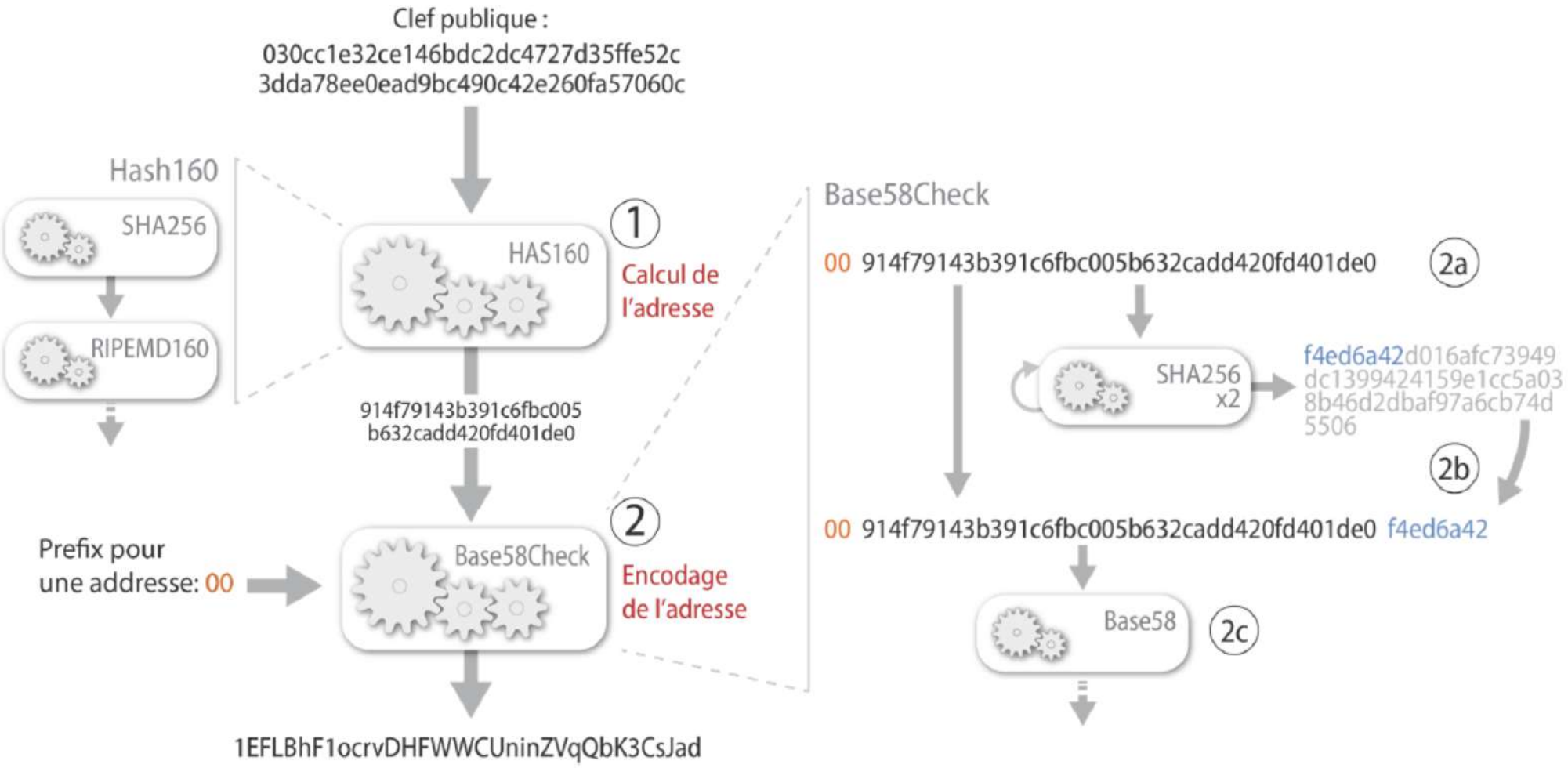

Block #0
Winner
nobody
Parent_hash
0
Nonce
0
SHA-256
Block #1
Winner
Player 23
Parent_hash
000D45698
Nonce
3459
SHA-256
Block #2
Winner
Player 16
Parent_hash
000F67839
Nonce
974329

Algorithme pour ajouter un bloc au registre:

1. **Vérifier les hashs de tous les blocs précédents**
2. **Construire un nouveau bloc (chainé au précédent) avec un nonce aléatoire**
3. **Hasher le nouveau bloc. A-t-il N zéro au début?**
   - Non? Goto 2
   - Oui? Envoyer votre bloc à tout le monde

Peut-on mentir en fournissant un hash forgé ?

CONSTRUCTION DES ADRESSES



Difficuté: compléter le message avec une partie aléatoire (nonce) telle que le hash du message ainsi complété ait un préfixe imposé (ici 00)

PREUVE DE TRAVAIL

La **preuve de travail** a pour objectif de **valider** les blocs de transactions et de **garantir l'équilibre** de la crypto-monnaie

Elle consiste en un **challenge cryptographique** de difficulté élevée.
Le validateur (ou miner) qui réussit ce challenge le premier remporte l'**incitation**.

La challenge cryptographique est réalisé par « **brute force** »
avec une **fonction de hashage**.

Considérons le document suivant :

document = « Ceci est mon document ! »

Si nous fixons notre difficulté à :

difficulty = 0000ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff

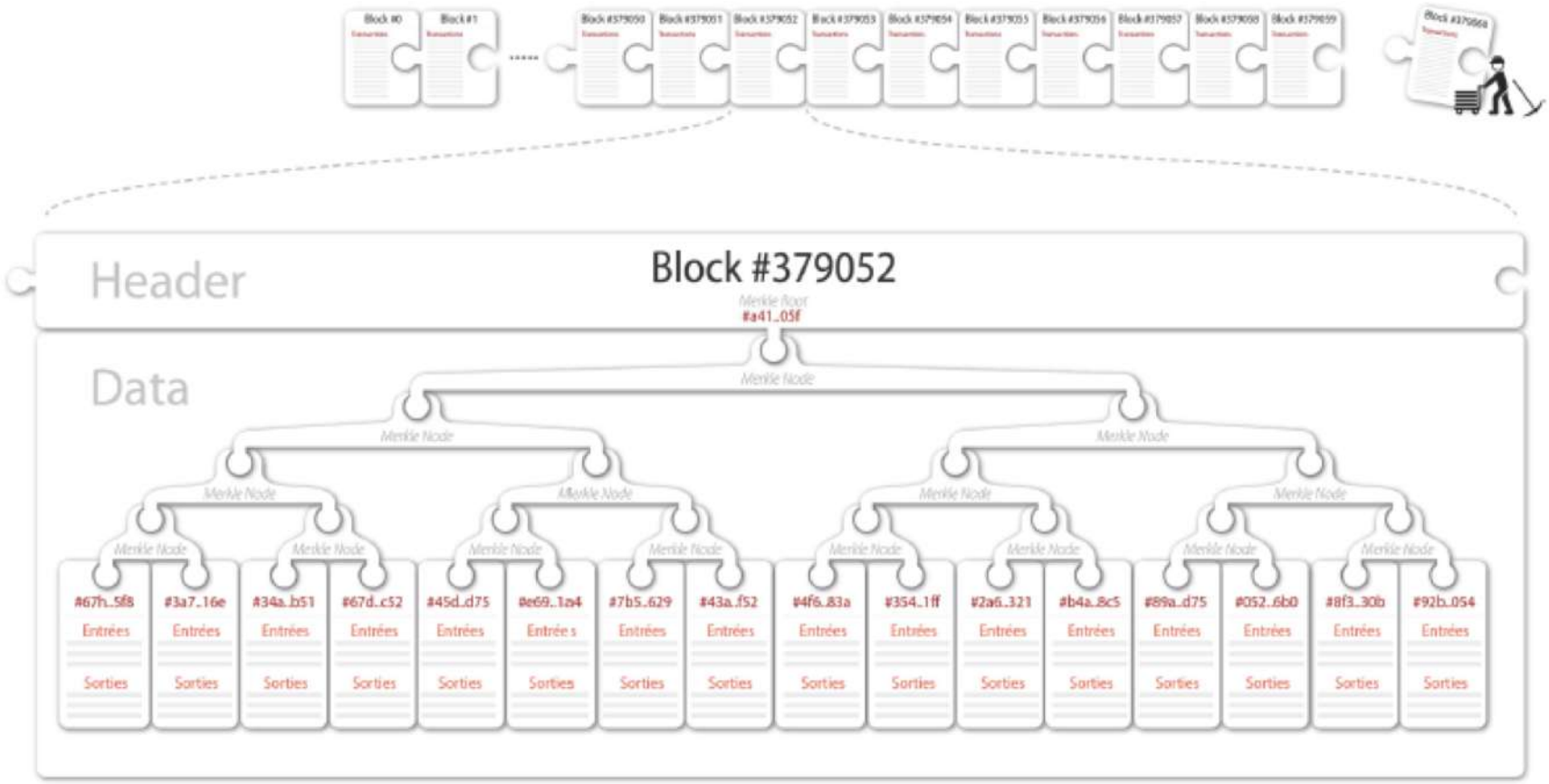
Le principe de preuve par le travail va consister à trouver une « tare » (*nonce* en anglais), telle que :

SHA256(texte + tare) < difficulty

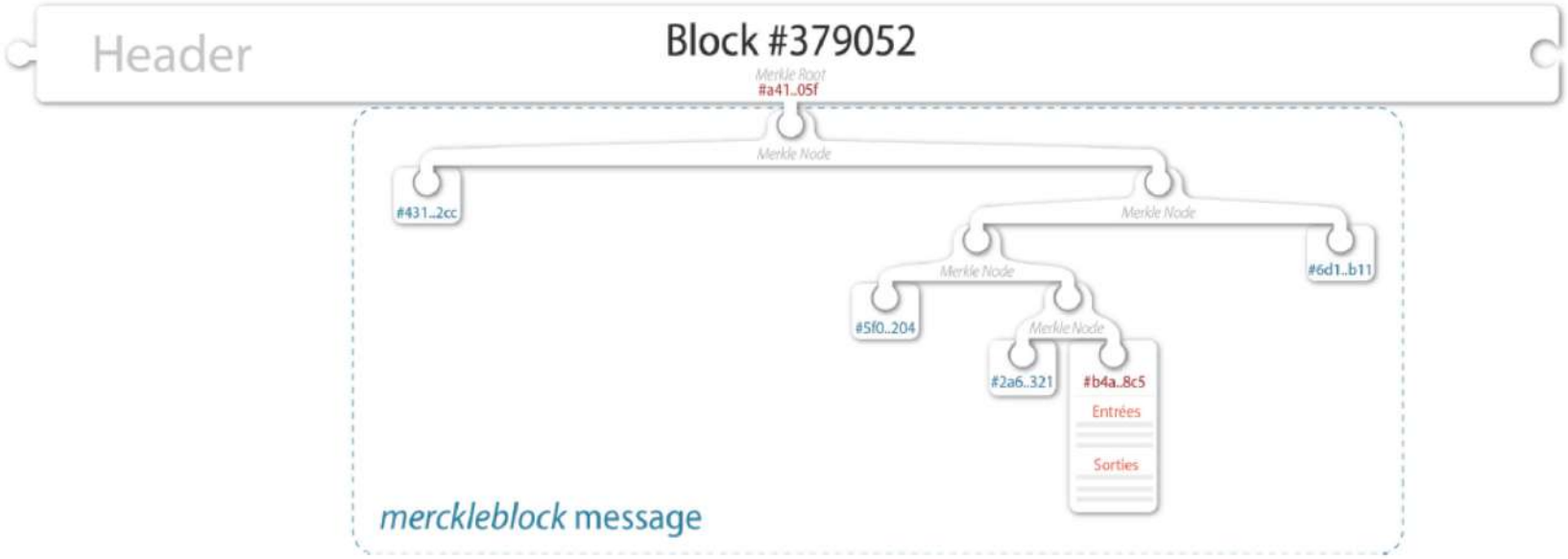
Autrement dit, de trouver une chaine qui, ajoutée à notre texte, permettra d'obtenir une empreinte commençant par 0000

Inconvénient: énergie consommée. Alternatives: preuve de participation (proof of stake), etc

LES TRANSACTIONS PEUVENT ETRE AGGLOMERES EN ARBRE DE MERKLE



PRÉSENCE D'UNE TRANSACTION DANS UN BLOC



Le protocole SPV (Simple Payment Verification) permet de vérifier **l'intégrité de l'arbre** ainsi que **l'appartenance d'une transaction** au bloc.

Les nœuds du réseau qui disposent de la copie complète du registre tiennent à jour une base de données des **sorties non dépensées**.

SOMMAIRE

Fonctions de hashage

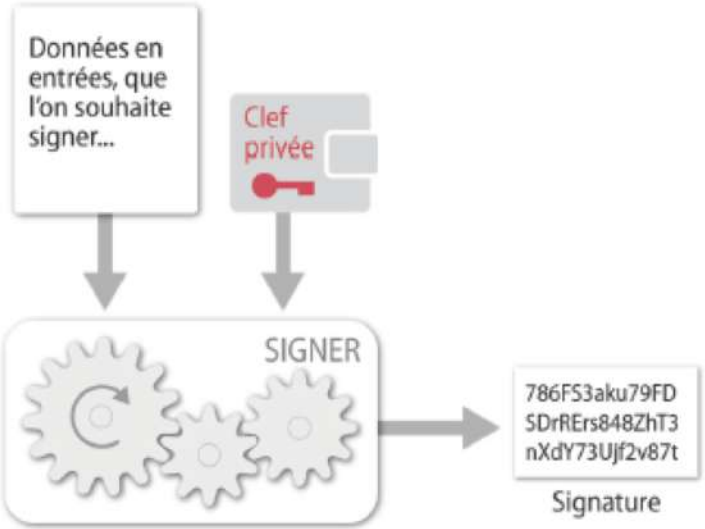
Signature Numérique

Tout cela pour sécuriser une transaction de pair-à-pair

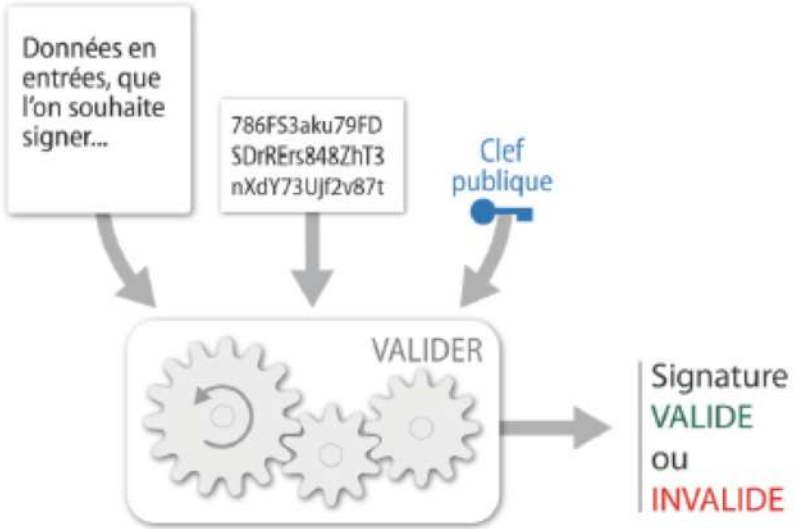
En conclusion

SIGNATURE NUMÉRIQUE

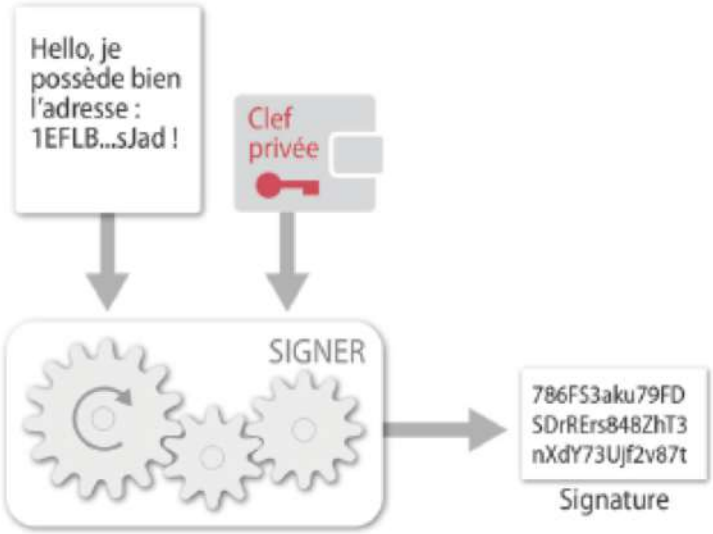
SIGNATURE



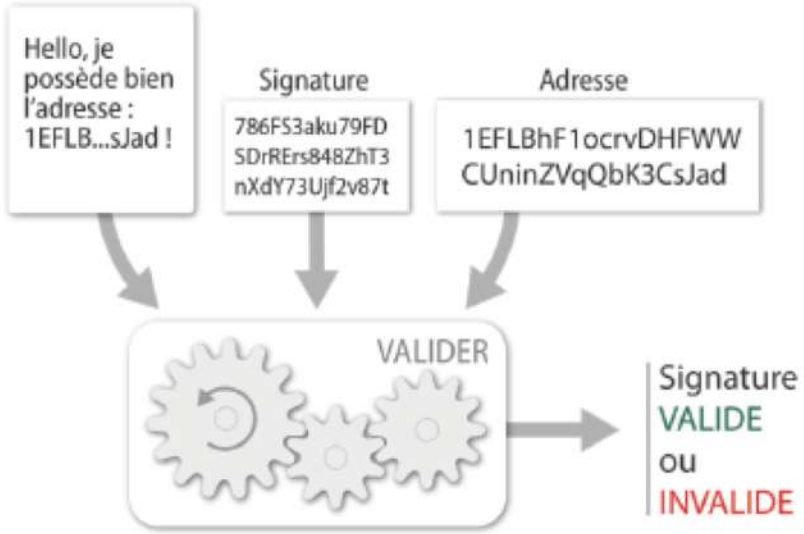
VÉRIFICATION



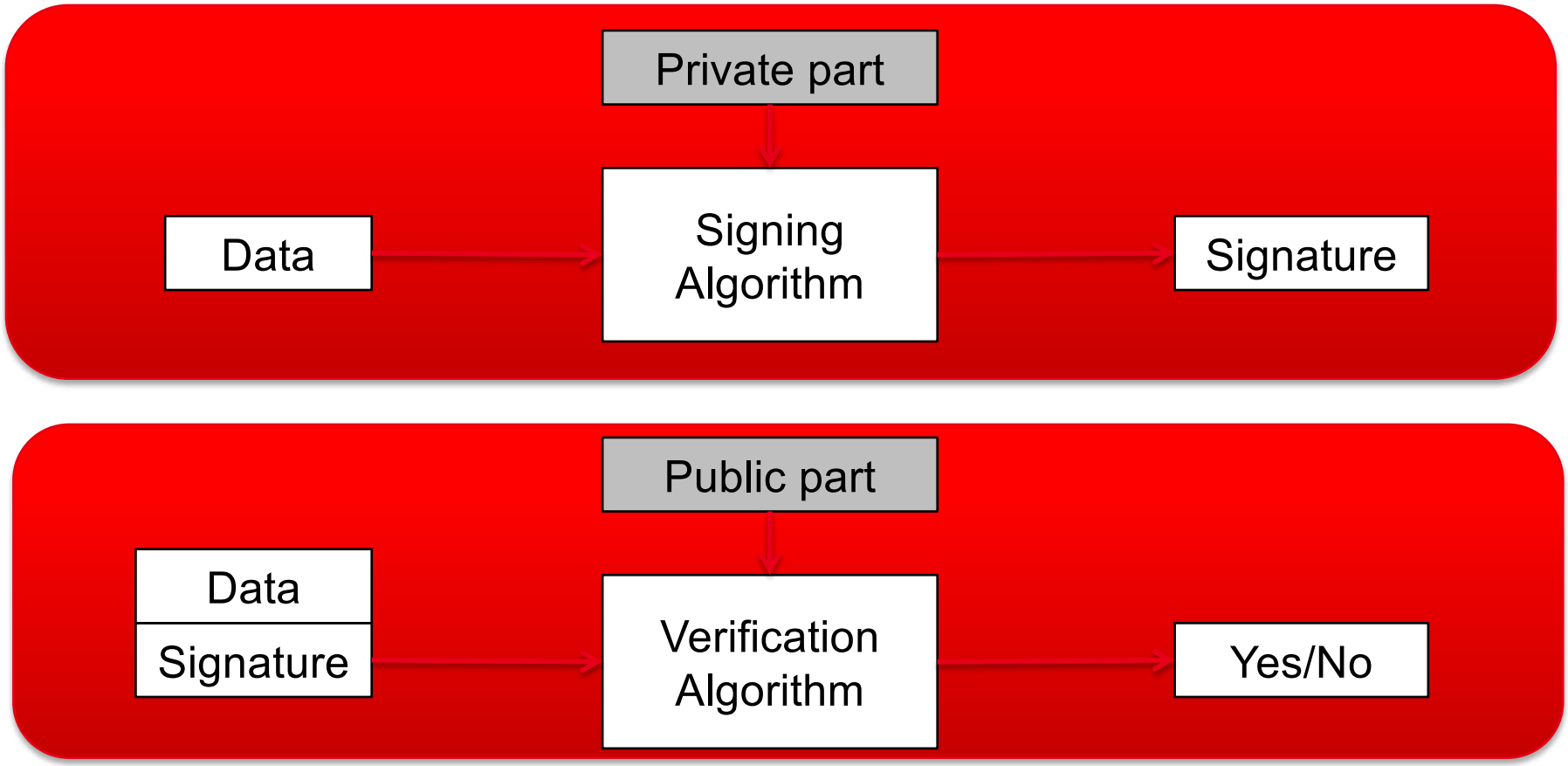
SIGNATURE

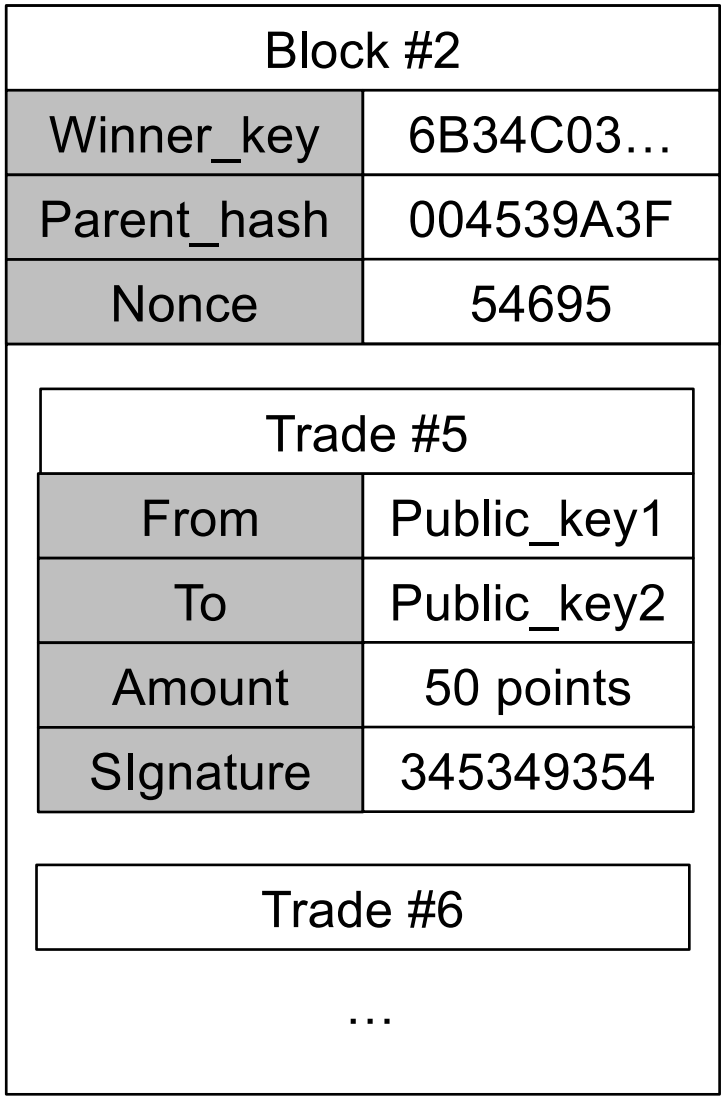


VÉRIFICATION



Signing key	
Public part	454F4D3E1..
Private part	56F23F2D..




Block #2
Winner_key
6B34C03…
Parent_hash
004539A3F
Nonce
54695
Trade #5
From
Public_key1
To
Public_key2
Amount
50 points
SIgnature
345349354
Trade #6
…

Block #0	
Winner Key	nobody
Parent_hash	0
Nonce	0

Block #1	
Winner Key	045F45F…
Parent_hash	000D45698
Nonce	3459

Block #2	
Winner Key	8234DB4…
Parent_hash	000F67839
Nonce	3459

Trade #8423	
From	Public_key1
To	Public_key2
Amount	50 points
SIgnature	345349354

Trade #8424	
From	Public_key2
To	Public_key3
Amount	50 points
SIgnature	734589345

SOMMAIRE

Fonctions de hashage

Crypto-système ECC

Signature Numérique

Tout cela pour sécuriser une transaction de pair-à-pair

En conclusion

TRANSACTION SUR UNE BLOCKCHAIN

Alice et **Bob** possèdent un portefeuille de valeur (crypto-monnaie).
Alice veut acheter un bien (ou service) à **Bob** et va procéder à son règlement via une transaction

Le processus de paiement se déroule en 5 étapes :

1. Bob présente la facture à Alice et une demande de paiement
2. Alice prépare la transaction et la signe
3. La transaction signée est diffusée sur le réseau blockchain
4. Un validateur la vérifie et l'intègre à la blockchain, au registre distribué
5. Le paiement est effectif, Bob reçoit la valeur dans son portefeuille

Ce processus est transparent et chacun peut vérifier l'état de la transaction dans le registre

Le bien (ou service) est (généralement) transmis hors blockchain

Validateurs= “miners”, points = “bitcoins”

Transactions transmettent de la valeur (bitcoins) d’une clef à une autre clef

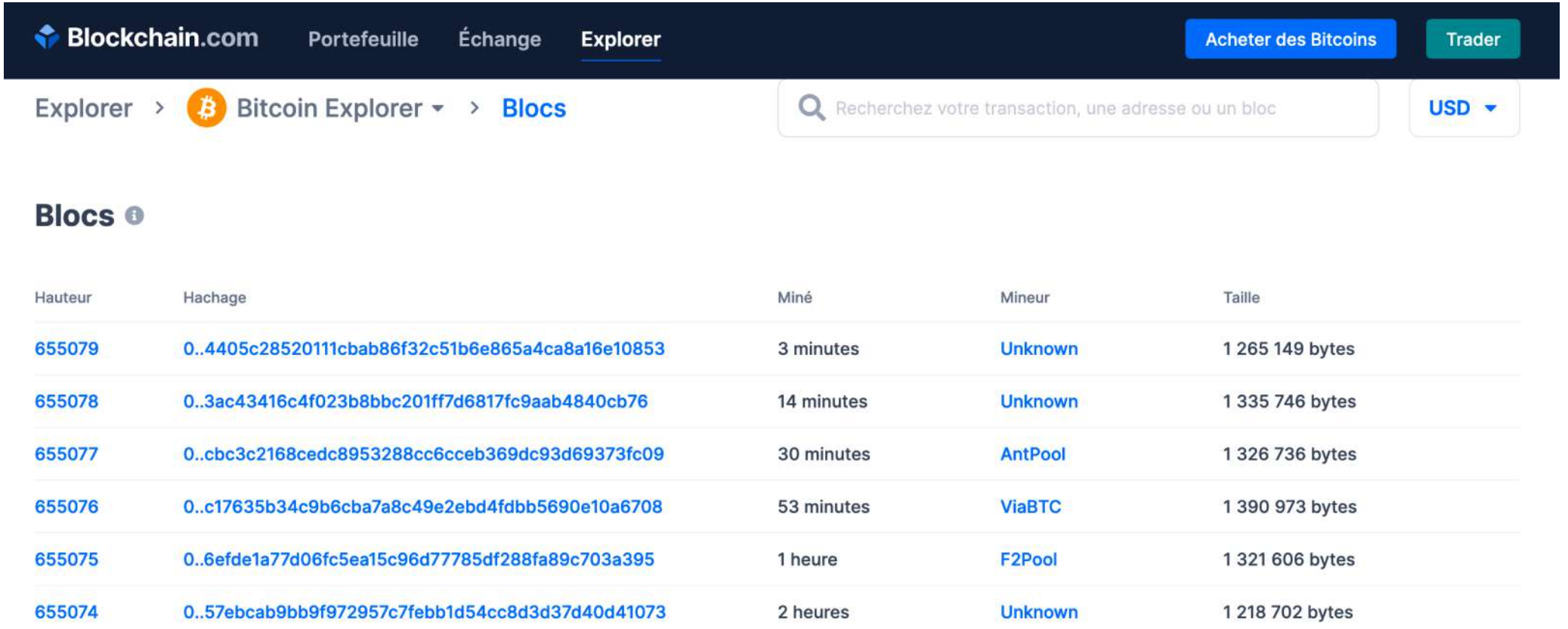
La blockchain empêche de dépenser plus que l’on ne pissède (et sans autorité centrale)

Règle du jeu: code du noeud de la transation

Le consensus des mineurs remplace l’autorité centrale

- Nombre limité de bitcons (21 million)
- Récompense par bloc
- La difficulté des preuves croit

[blockchain.info]



Hauteur	Hachage	Miné	Mineur	Taille
655079	0..4405c28520111cbab86f32c51b6e865a4ca8a16e10853	3 minutes	Unknown	1 265 149 bytes
655078	0..3ac43416c4f023b8bbc201ff7d6817fc9aab4840cb76	14 minutes	Unknown	1 335 746 bytes
655077	0..cbc3c2168cedc8953288cc6cceb369dc93d69373fc09	30 minutes	AntPool	1 326 736 bytes
655076	0..c17635b34c9b6cba7a8c49e2ebd4fdbb5690e10a6708	53 minutes	ViaBTC	1 390 973 bytes
655075	0..6efde1a77d06fc5ea15c96d77785df288fa89c703a395	1 heure	F2Pool	1 321 606 bytes
655074	0..57ebcab9bb9f972957c7febb1d54cc8d3d37d40d41073	2 heures	Unknown	1 218 702 bytes

Transactions des blocs

Hachage	d6b0861bbd1d669970913623286eba285cd4ae069408eb6b49b77...				2020-11-02 05:56
	COINBASE (Pièces Nouvellement Générées)		→	1EioJVmQ9NVWGdZKvnQ3gpw5V4fj8trvpa	7.24667562 BTC
				OP_RETURN	0.00000000 BTC
Frais	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 218 bytes)				7.24667562 BTC 1 confirmations
Hachage	c0c772e8283e075cafadd78c9476e9b001b395fa606eb8b65b6d57...				2020-11-02 05:46
	1Gv3ZrLaqYHu9M5GXEoKAzGVnSBczaMaBn	0.00284406 BTC	→	3KNz8boT5Dnk3Ds4yjj2EgEWejdPqSRPs6	0.00087635 BTC
Frais	0.00196771 BTC (1041.116 sat/B - 260.279 sat/WU - 189 bytes)				0.00087635 BTC 1 confirmations
Hachage	6c32bfa84377e5b08eb3d8ac882c9aa75e1a3dbb4c6abd61b4be0f...				2020-11-02 05:53
	bc1qf60m7evl3yvzaevgjrqd595ee7jyn84wq6tn...	2.22850482 BTC	→	3JawNsXe6UxJ5SveH4f2Qssoa8qLACTxd7	0.00750000 BTC
				bc1qf60m7evl3yvzaevgjrqd595ee7jyn84wq6tn...	2.21960342 BTC
Frais	0.00140140 BTC (368.789 sat/B - 184.881 sat/WU - 380 bytes)				2.22710342 BTC 1 confirmations

Détails

Hachage	d6b0861bbd1d669970913623286eba285cd4ae069408eb6b49b778d3bc44f...
Statut	Confirmé
Heure reçue	2020-11-02 05:56
Taille	218 octets
Poids	764
Inclus dans le bloc	655079
Confirmations	1
Total des entrées	0.00000000 BTC
Total des sorties	7.24667562 BTC
Frais	0.00000000 BTC
Frais par octet	0.000 sat/B
Frais par unité de poids	0.000 sat/WU
Valeur lors de la transaction	99 288,73 $US

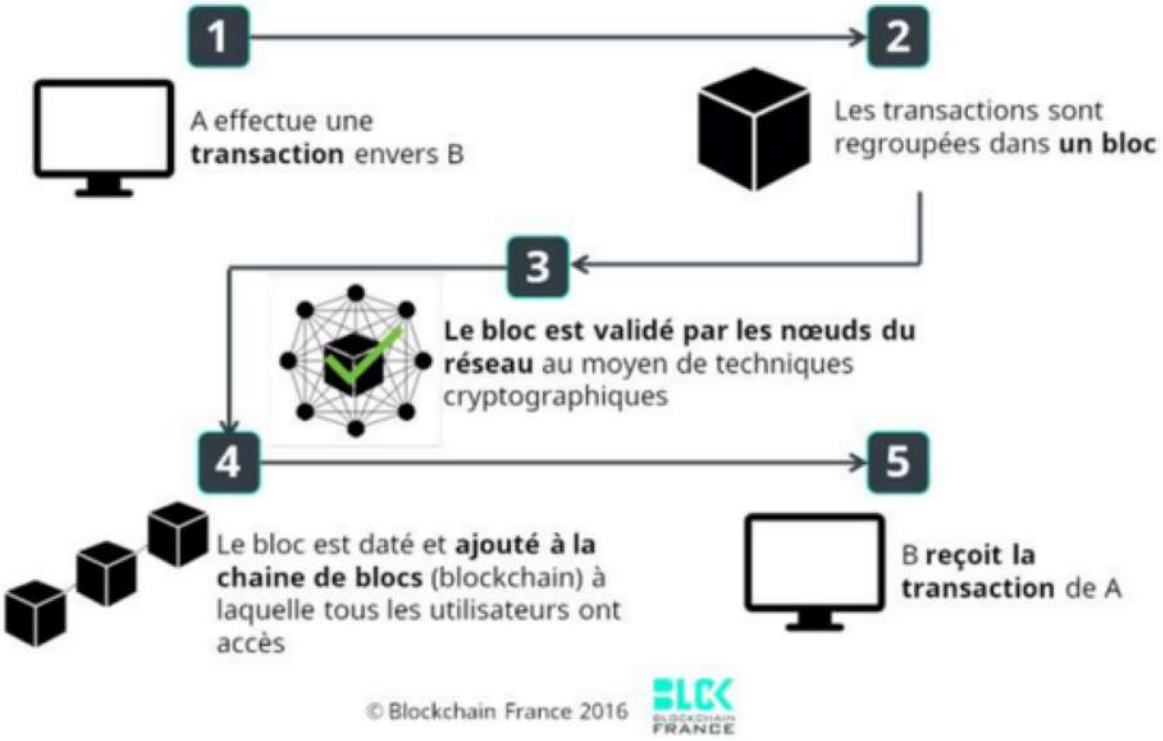
EXEMPLE D'UNE PLATEFORME DE MINAGE

Hashnest.com permet d'acheter ou vendre des hashrates

Keepkey.com

TRANSACTION SUR UNE BLOCKCHAIN

La blockchain contient l'historique de tous les échanges depuis sa création

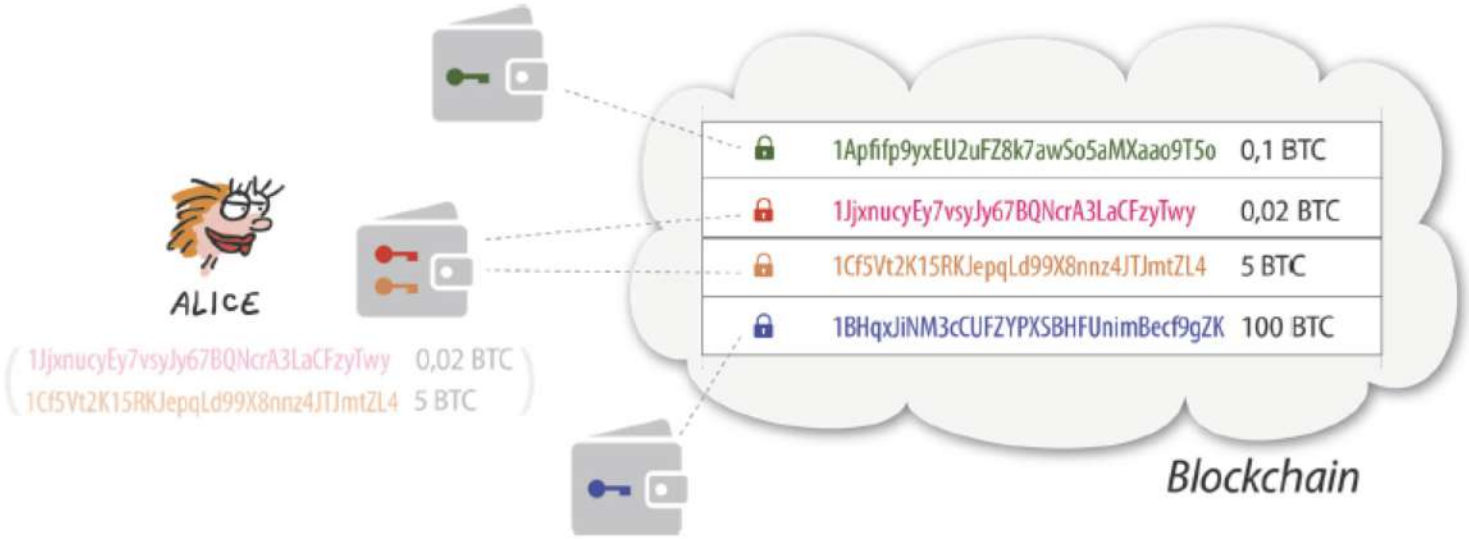


ALICE POSSÈDE DES COIN (CRYPTO-MONNAIE)

La **crypto-monnaie** est gérée via un **portefeuille électronique**

Un **Coin** est rattaché à une **adresse** gérée par le portefeuille.
Il est **enregistré** dans la blockchain et est **protégé** par un **verrou**.
Pour être dépensé dans une transaction, il faut posséder **la clé** de son verrou.

Le **portefeuille d'Alice** ne contient pas de Coin
mais des **clés** permettant de les dépenser



Seules les **adresses** sont **visibles** lorsque l'on effectue une **transaction**

BOB PRÉSENTE SA FACTURE

Bob génère une **adresse** et une **clé de déverrouillage**.
L'adresse est codée sous forme de **QRCode** et présentée à **Alice**.
La **clé de déverrouillage** est conservée **secrète** par **Bob**.

Pour des raisons de **sécurité** et de **confidentialité**,
une adresse n'a pas vocation à être utilisée plusieurs fois

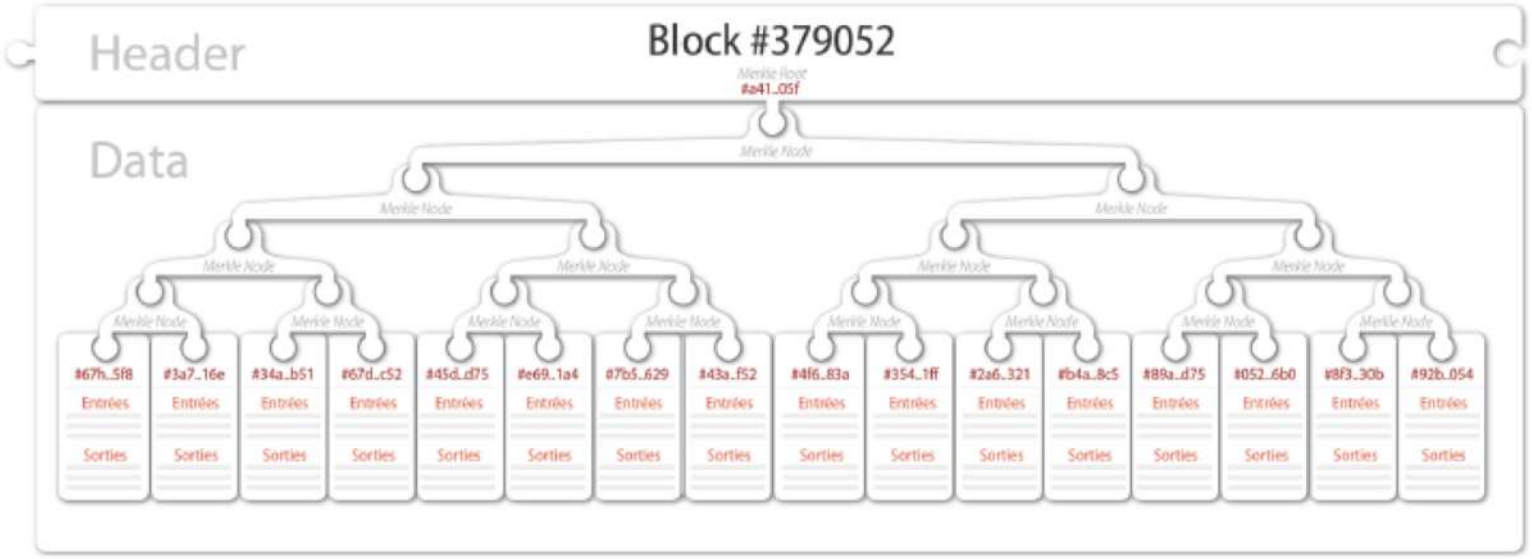
ALICE PRÉPARE SA TRANSACTION

La transaction est composée :

- d'une **adresse « entrée »** qui fait référence à des SolarCoin détenus par **Alice** et enregistrés dans la blockchain
- d'une **adresse « sortie »** qui est l'adresse envoyée par **Bob** sous forme de QRCode
- d'une **adresse « sortie UTXO »** pour que **Alice** récupère la monnaie
- éventuellement de **frais de transaction** pour les **validateurs**

LA TRANSACTION EST VÉRIFIÉE

La **transaction** est ajoutée au **bloc** des transactions **courantes**.
Toutes les transactions du bloc sont **vérifiées**.



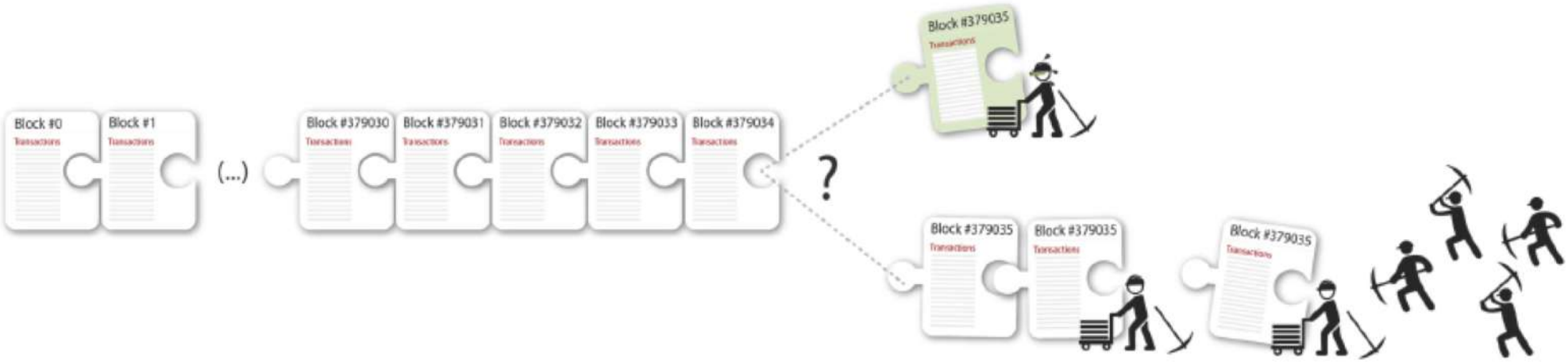
Chaque **« entrée »** d'une transaction est nécessairement
la **« sortie UTXO »** non dépensée d'une autre transaction

Une transaction n'est **acceptée** que si ses entrées contiennent les
clés de déverrouillage des sorties qu'elle utilise

La vérification est basée sur l'usage de la cryptographie

LE BLOC EST VALIDÉ ET INTÉGRÉ À LA CHAINE DE BLOCS

Le bloc est **validé** et **accroché** à la **chaine de blocs**.
Ce travail est réalisé par des **mineurs** et fait appel à la **cryptographie**.
Les mineurs touchent les **frais de transaction**.



BOB DÉLIVRE L'ÉNERGIE HORS BLOCKCHAIN

Le **transaction** n'est **définitive** que lorsque son **bloc** est **recouvert** par plusieurs autres blocs.

L'énergie est délivrée sur événement (transaction définitive) selon les termes du Smart Contract.
Le tarif peut être réglementé.
L'énergie est délivrée sur le réseau électrique, hors blockchain.

SOMMAIRE

Fonctions de hashage

Signature Numérique

Tout cela pour sécuriser une transaction de pair-à-pair

En conclusion