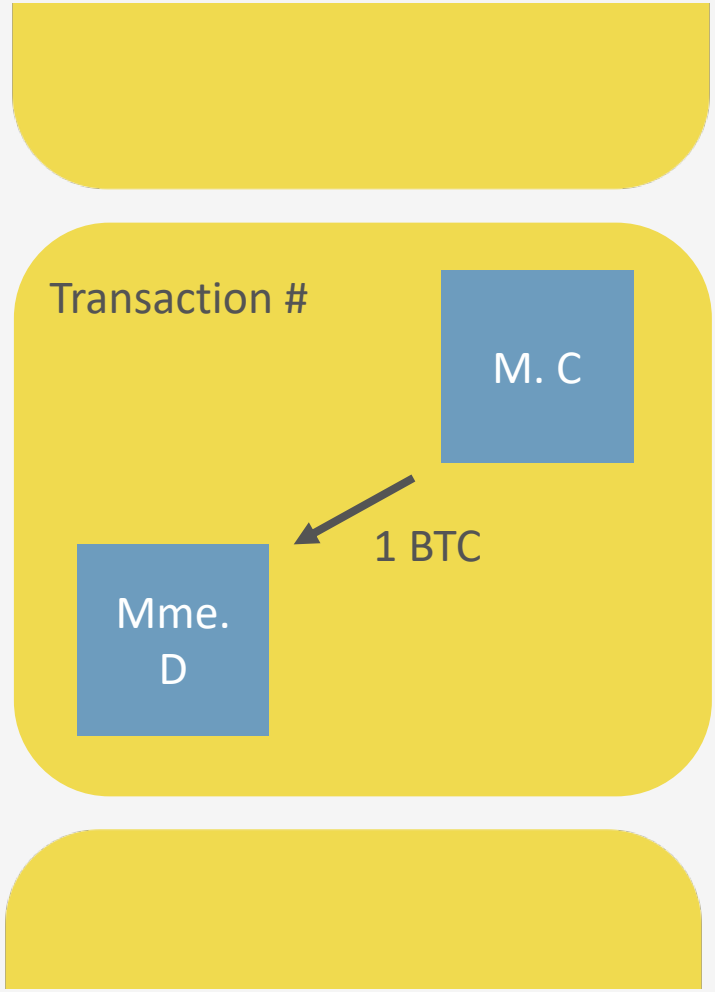
DIGITAL & CREATIVE BUSINESS LAW

Blockchain et Bitcoin

Expliqués aux juristes (et aux non-juristes !) par un juriste

NEXT avocats – www.next-law.fr
15 rue du Temple – 75004 Paris
contact@next-law.fr – 01 75 43 86 23

La blockchain est un registre électronique de transactions entre 2 personnes



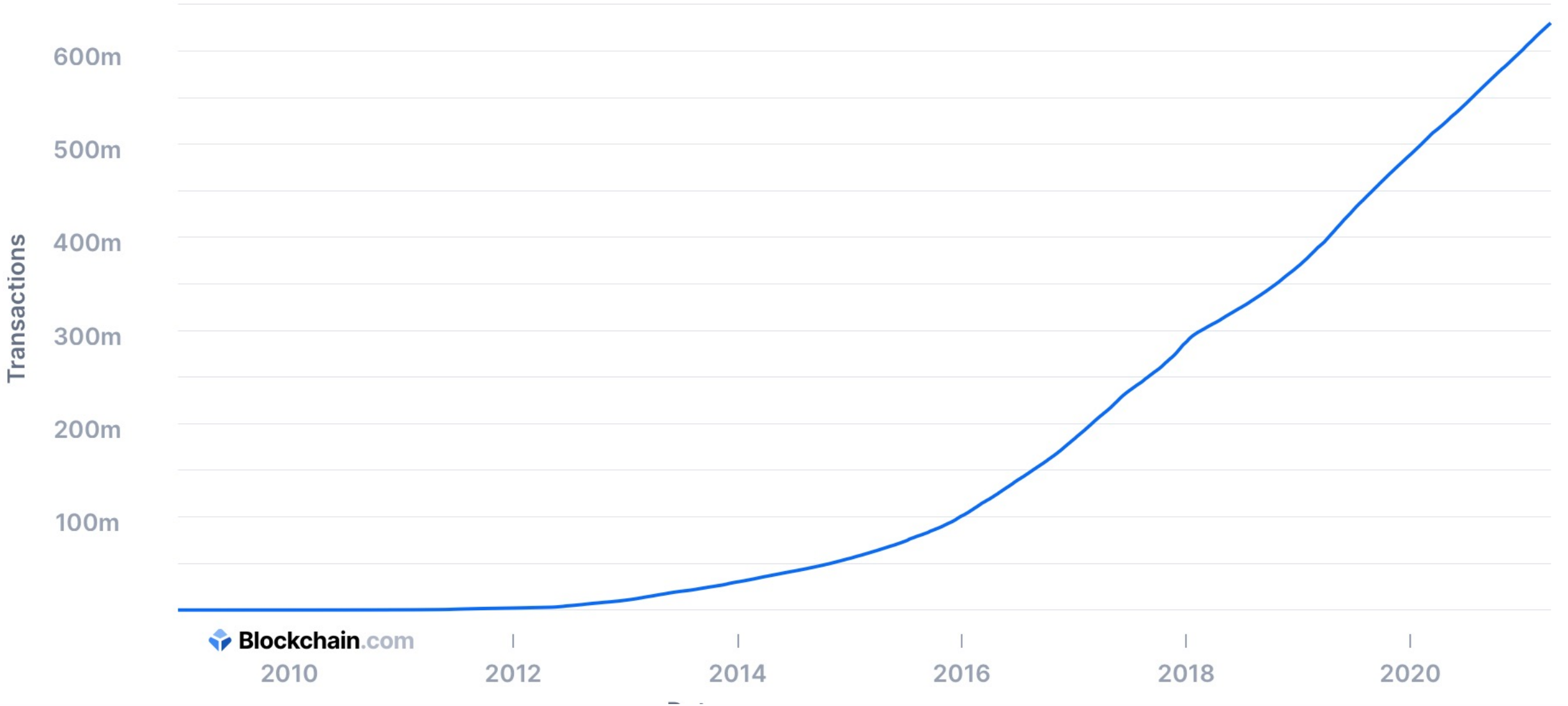
Au 15 mars 2021, la blockchain des Bitcoins faisait 325,64 Go.

Elle tient sur le disque dur d'un ordinateur portable.

Elle comporte 624 864 millions de transactions.

Total Number of Transactions

The total number of transactions on the blockchain.



Pourquoi cela vaut de l'argent ?

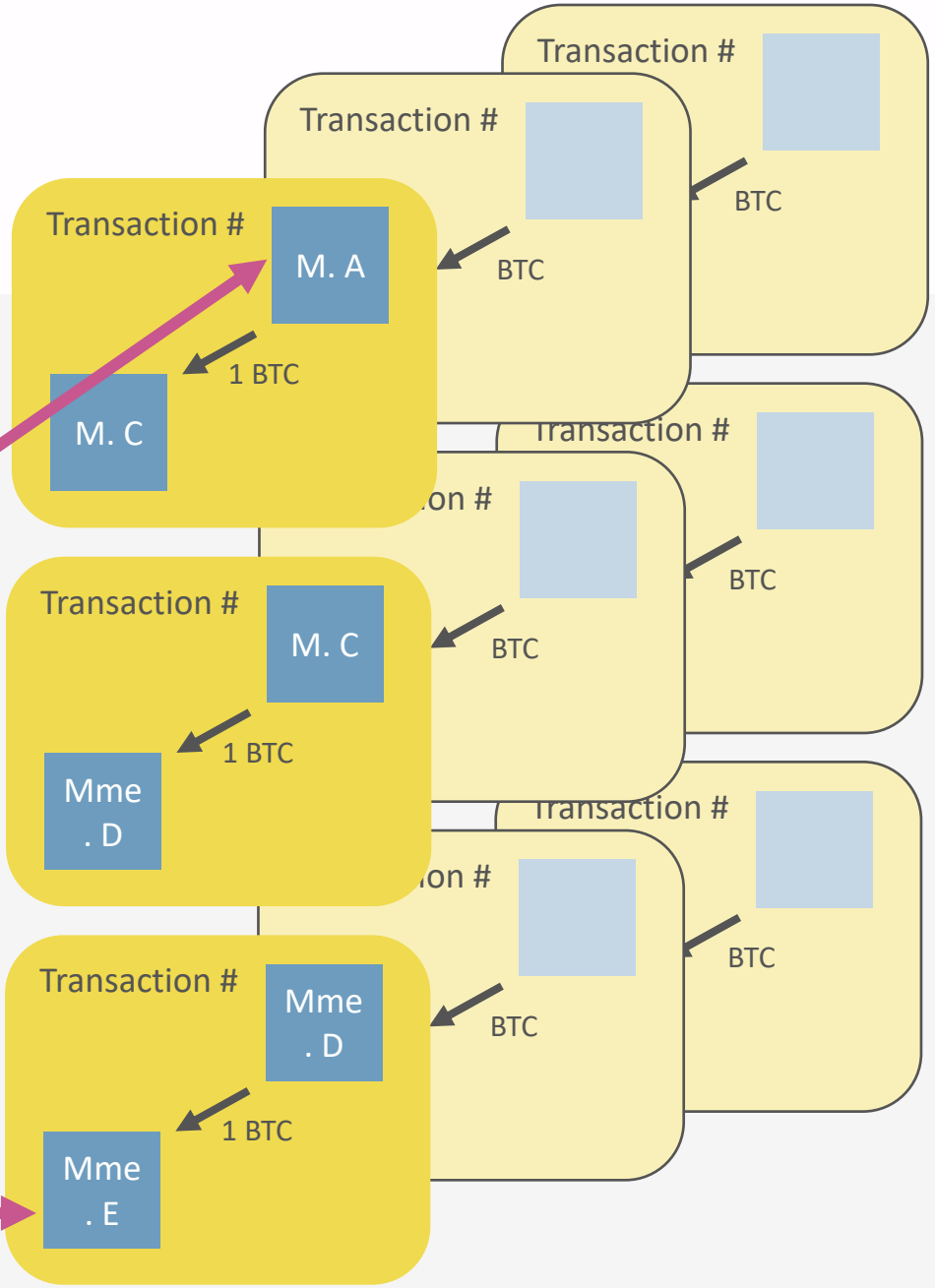
- Le « Bitcoin » est un protocole informatique dont les utilisateurs accordent une valeur de type « monétaire » aux informations qu'il permet de stocker et transmettre.

- Cette confiance est justifiée par l'intégrité des transactions enregistrées au moyen de technologies cryptographiques aujourd'hui non démontrées comme non fiables.

Toutes les transactions sont publiques.

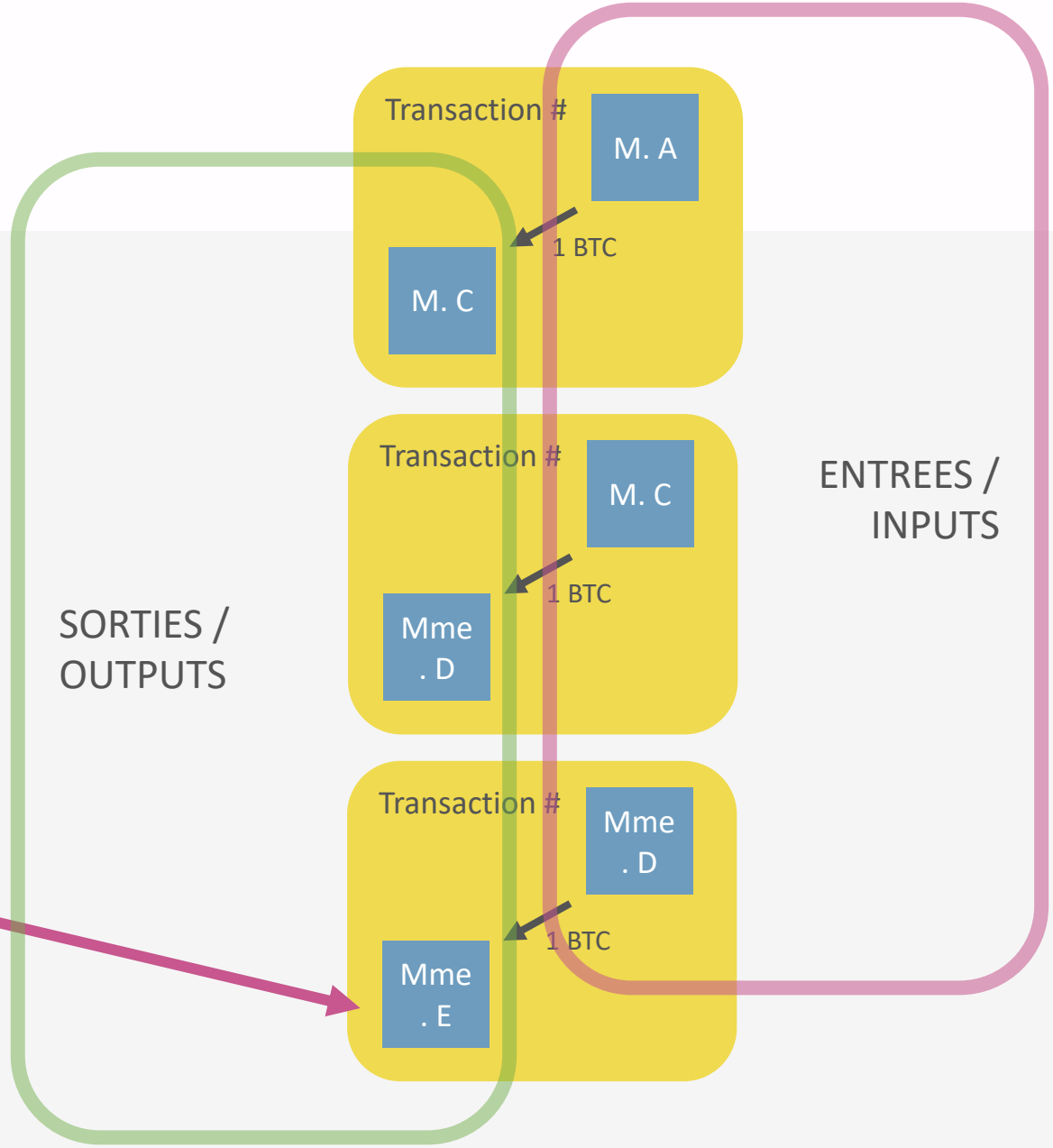
Elles peuvent être tracées depuis le premier possesseur d'un bitcoin…

…jusqu'à son dernier.



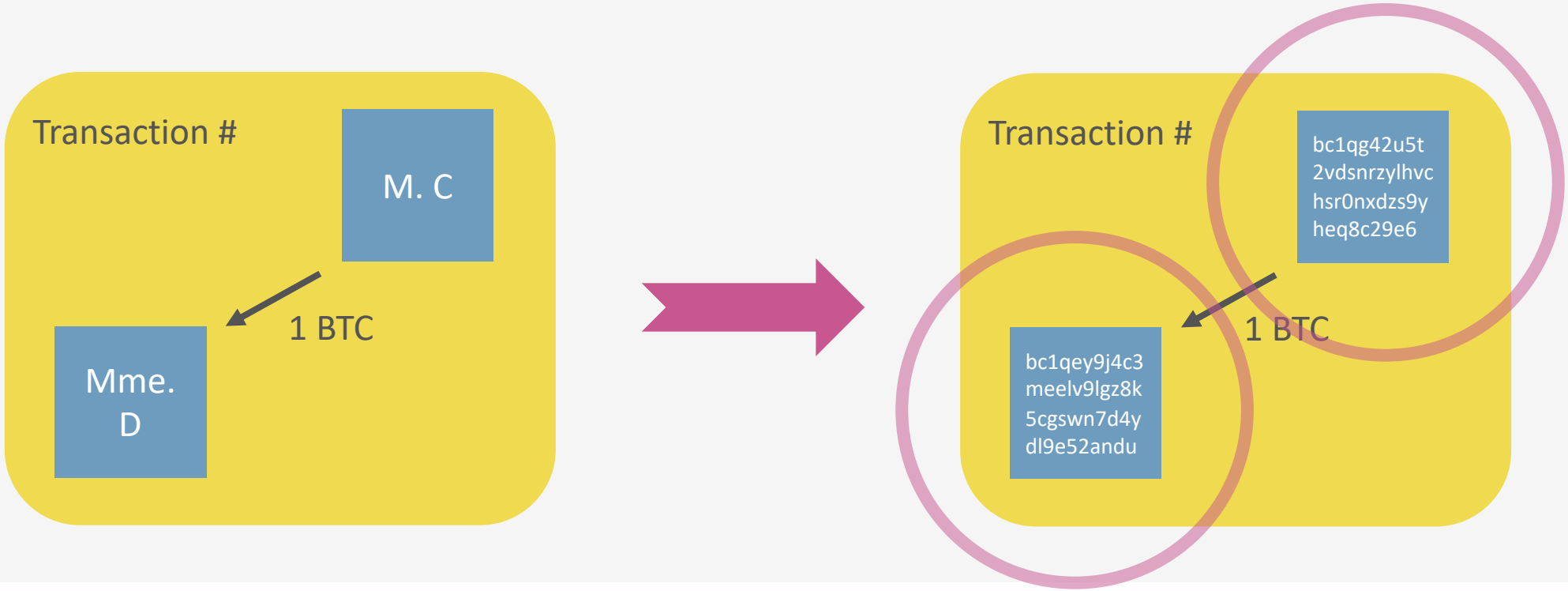
Le total de Bitcoins possédés par une personne correspond à la somme des transactions auxquelles cette personne a participé comme bénéficiaire et qui sont encore « non dépensées » :

« *Unspent transaction outputs (UTXO)* »



Mais les possesseurs de Bitcoin sont anonymes

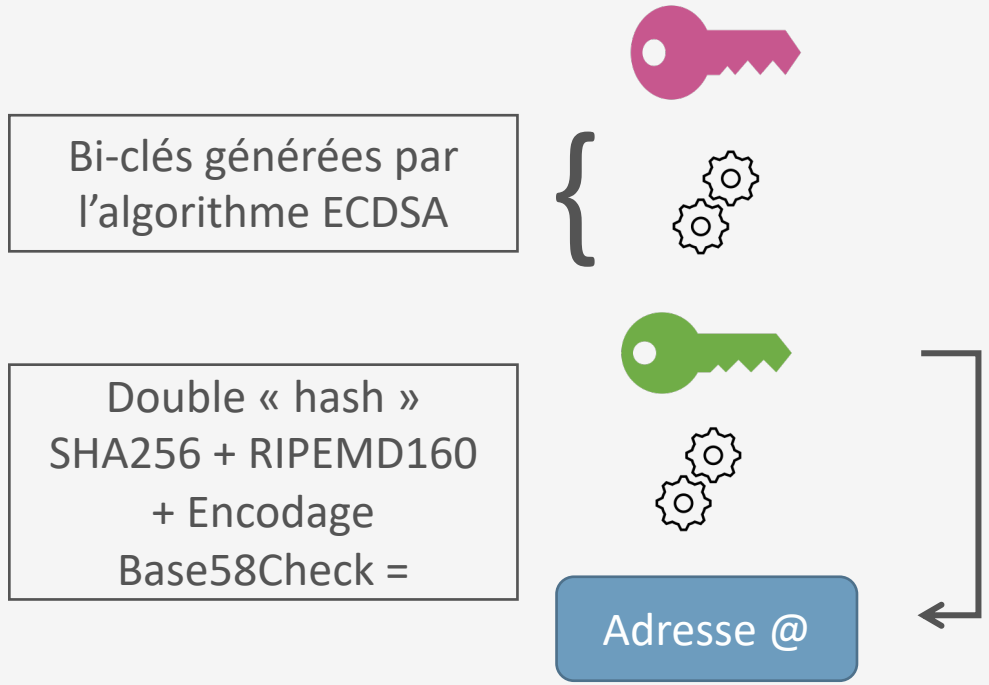
La personne possédant un Bitcoin est uniquement identifiée par sa clé cryptographique publique ou par le « hash » de sa clé publique, également appelée « adresse »



Pour participer aux transactions il faut une adresse

- Les adresses sont créées et stockées dans un portefeuille (wallet)

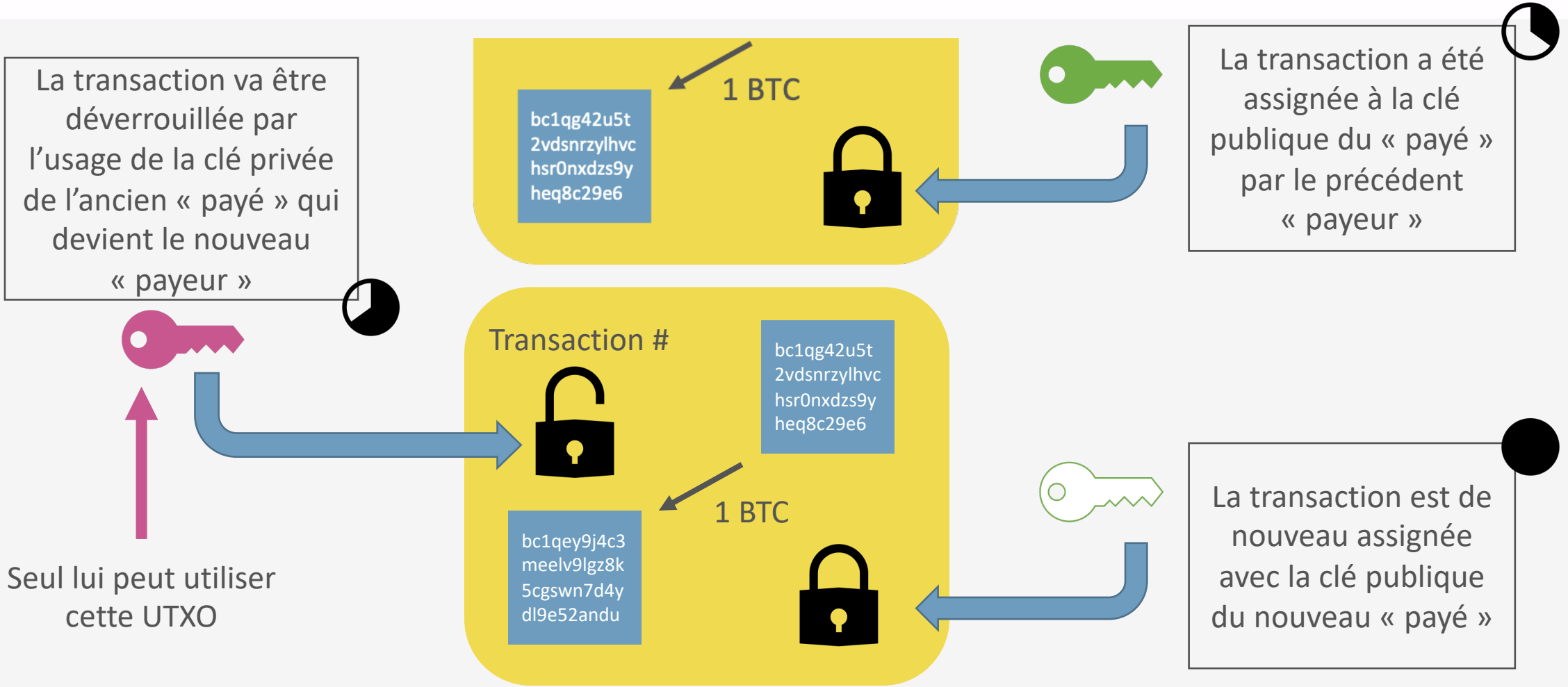
- Le portefeuille est un logiciel (pour ordinateur ou smartphone) ou un site web qui en fait fonction et qui génère les adresses et conserve les clés cryptographiques associées



De la clé publique à l'adresse

- La clé publique est longue. Exemple en notation hexadécimale :
  - 0223c1d72g690bfeacd59f8839dfca3v1e5dfde4912db5eb797e614e005c32d6d6 ➔ **clé publique**
- Les transactions utilisent un « double hash » de la clé publique par commodité :
  - Bc1qey9j4c3meelv9lgz8k5cgswn7d4ydl9e52andu ➔ **adresse**

Qu'est-ce qui sécurise chaque transaction ?

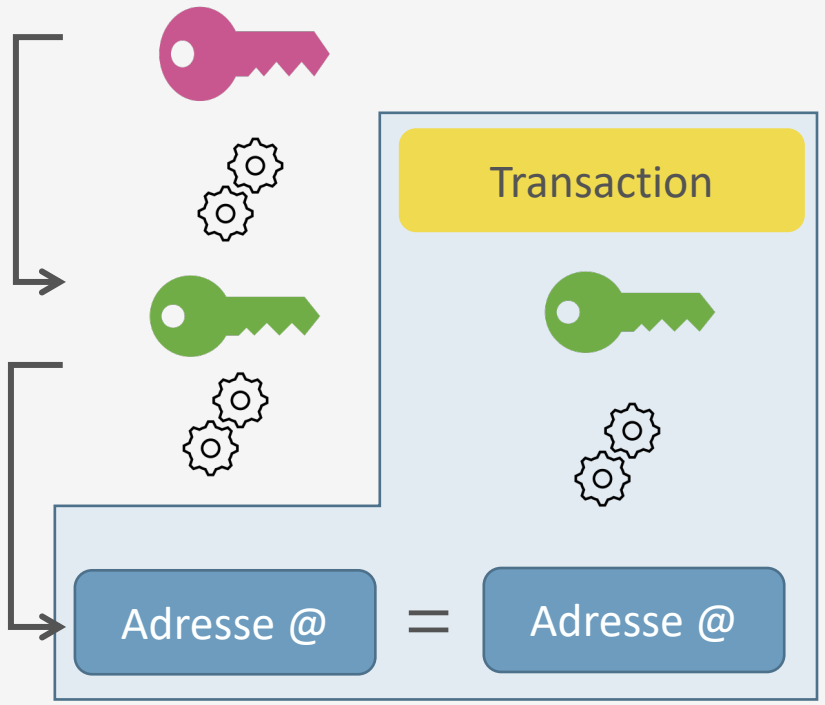


Qu’est-ce que « verrouiller/déverrouiller » une transaction signifie ?

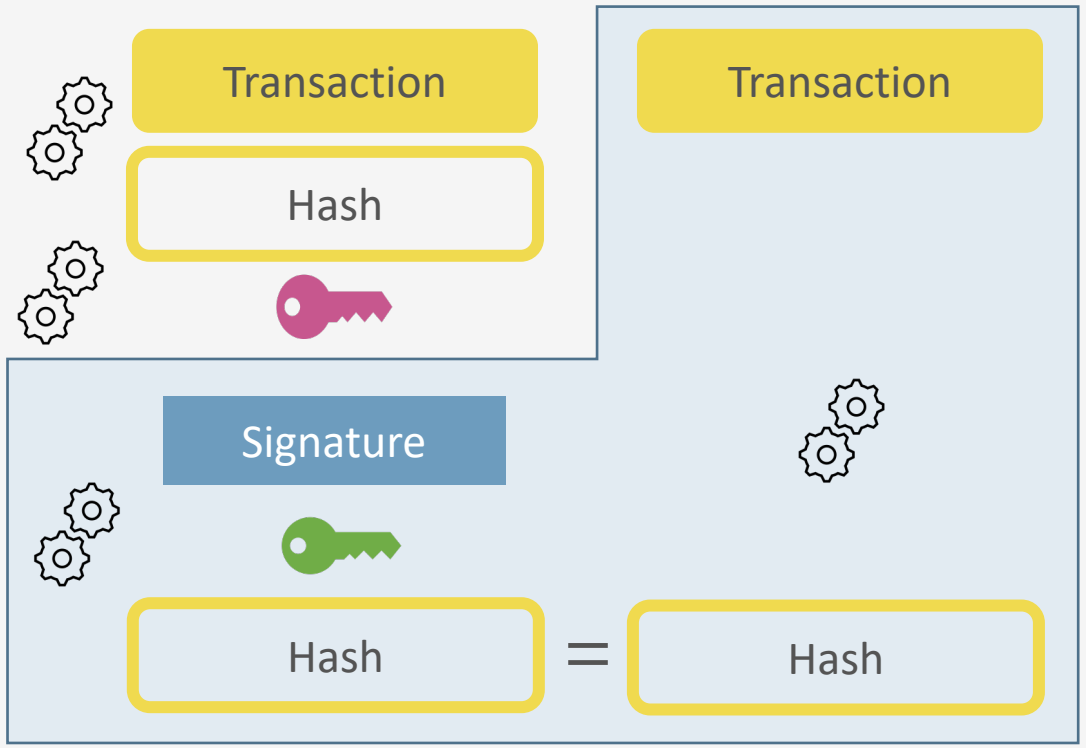
- Pour mobiliser les Bitcoins, il faut prouver qu’on est bien le bénéficiaire d’un UTXO (adresse figurant en sortie (output) de la transaction non dépensée).

- Envoyer un paiement en « Bitcoin » c’est activer une « sortie/output » d’une transaction figurant dans la chaine avec sa clé privée et la destiner à une personne désignée avec la clé publique (adresse) de celle-ci.

Déblocage de la transaction par le possesseur du Bitcoin



Conclusion 1 : l'adresse @ est bien celle de la clé publique



Conclusion 2 : c'est bien le possesseur de la clé publique qui a signé la transaction

Quelques précisions

- Il est possible de fractionner les Bitcoins relatifs à une transaction pour n'en utiliser qu'une partie. Le reste constituera une transaction « vers soi-même » (« change »).

- Il est possible de réunir les Bitcoins relatifs à plusieurs transactions pour procéder à un paiement.

- Ces opérations sont effectuées de manière transparente pour l'utilisateur par le « wallet »

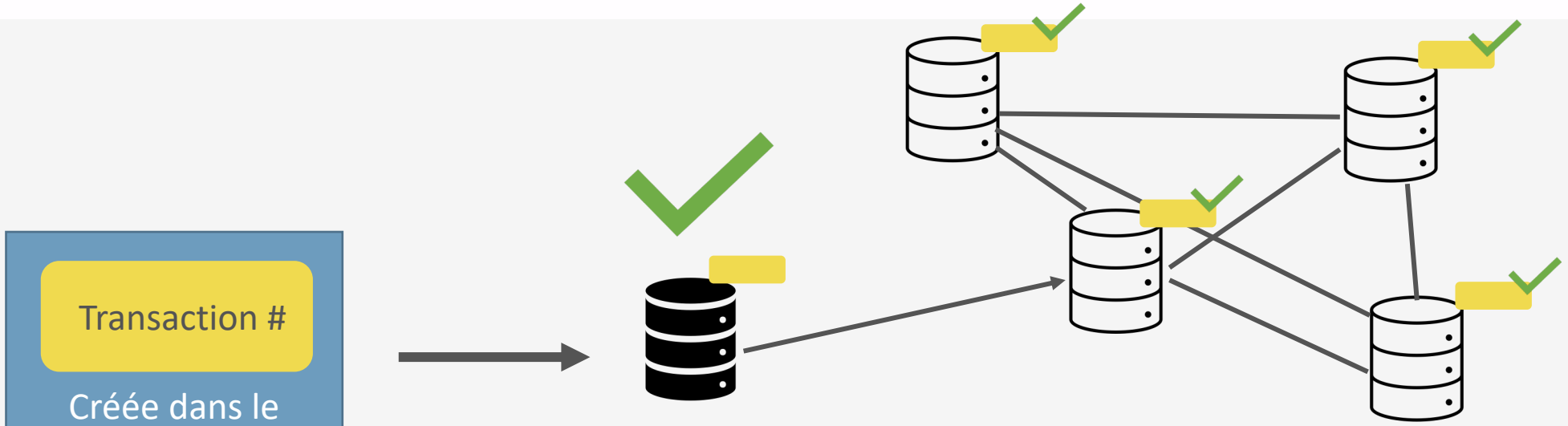
Comment publier tout ça ?

- La Blockchain permet :

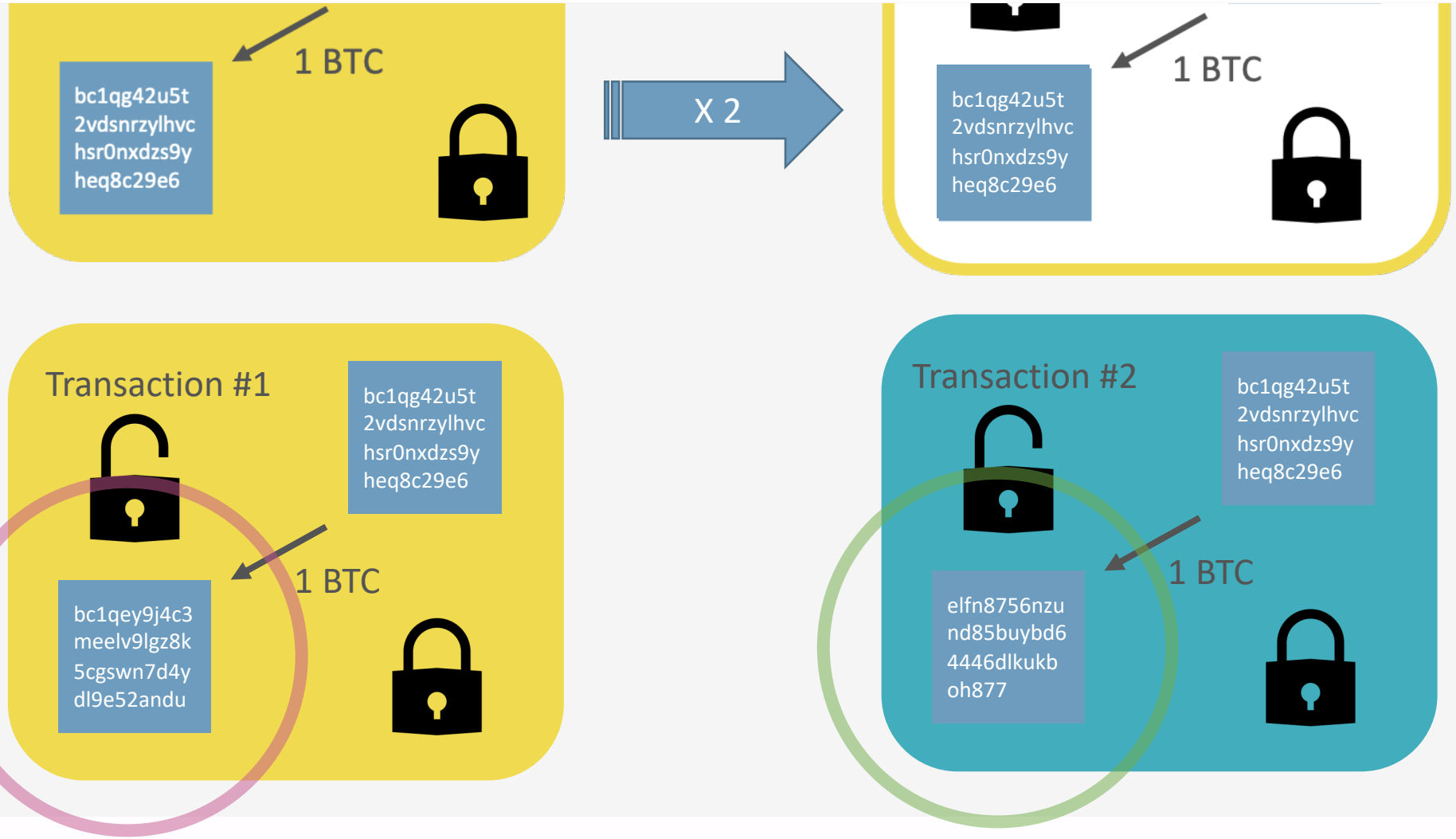
  - De diffuser l'information de manière décentralisée : chaque « nœud / node » contient l'historique de l'ensemble des transactions

  - De veiller à l'absence de « double paiement » : par le mécanisme du « minage ».

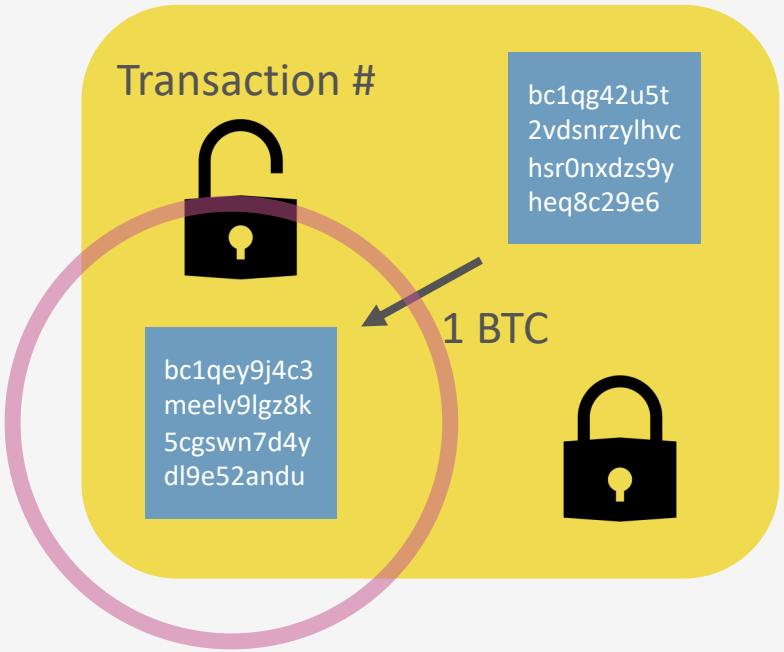
Diffusion d'une transaction

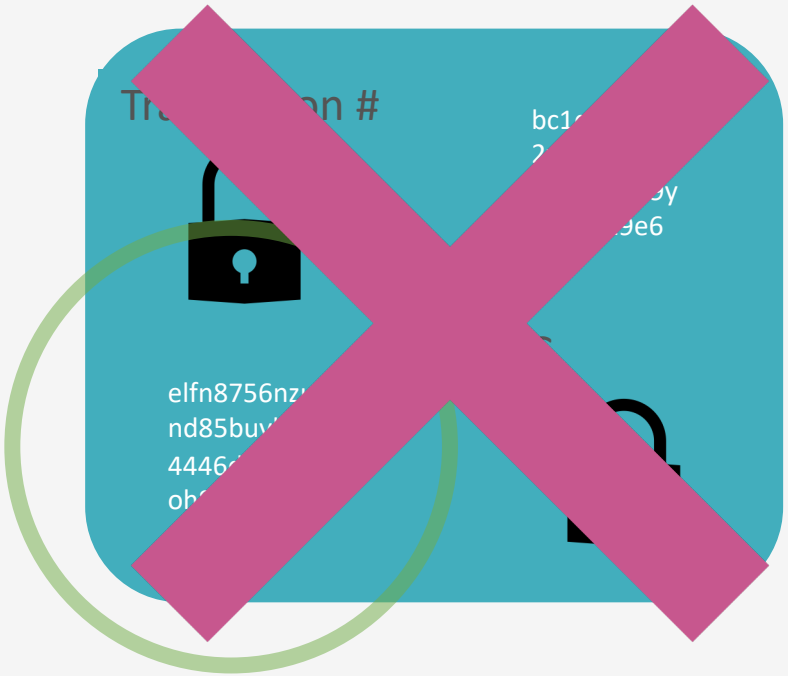


Pourquoi ne pas payer 2 fois avec la même UTXO ?



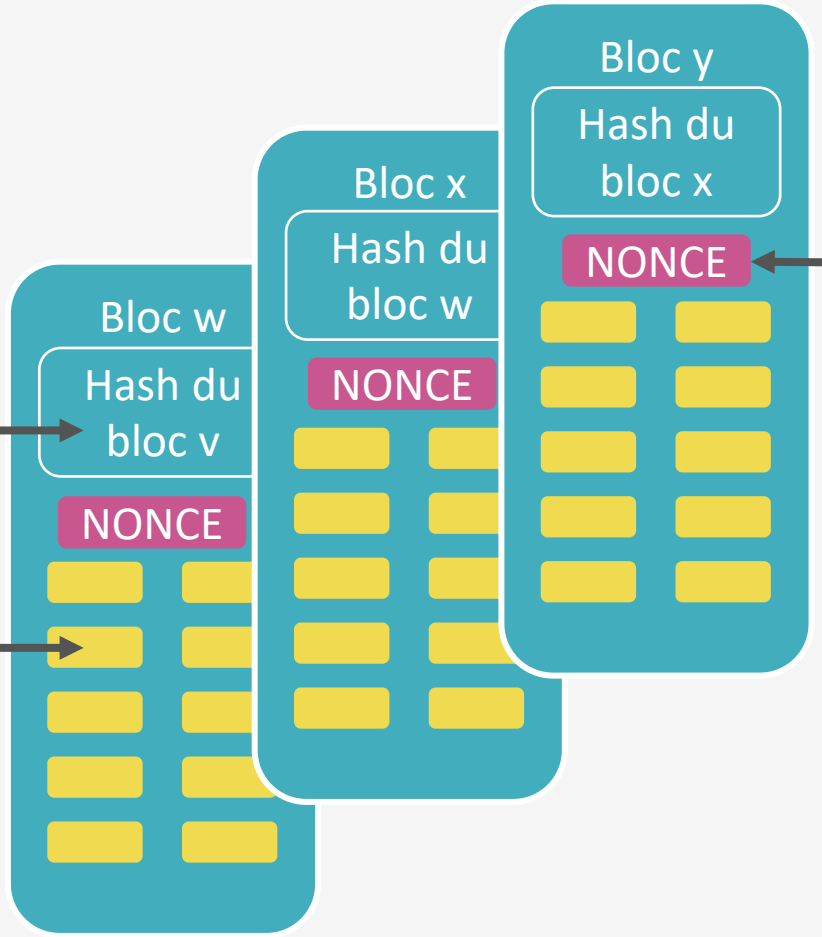
Le minage ne validera qu'une seule des deux transactions





Comment ?

2 Chaque bloc est lié au précédent par l'enregistrement du « hash » du précédent bloc



1 Chaque transaction est enregistrée dans un bloc

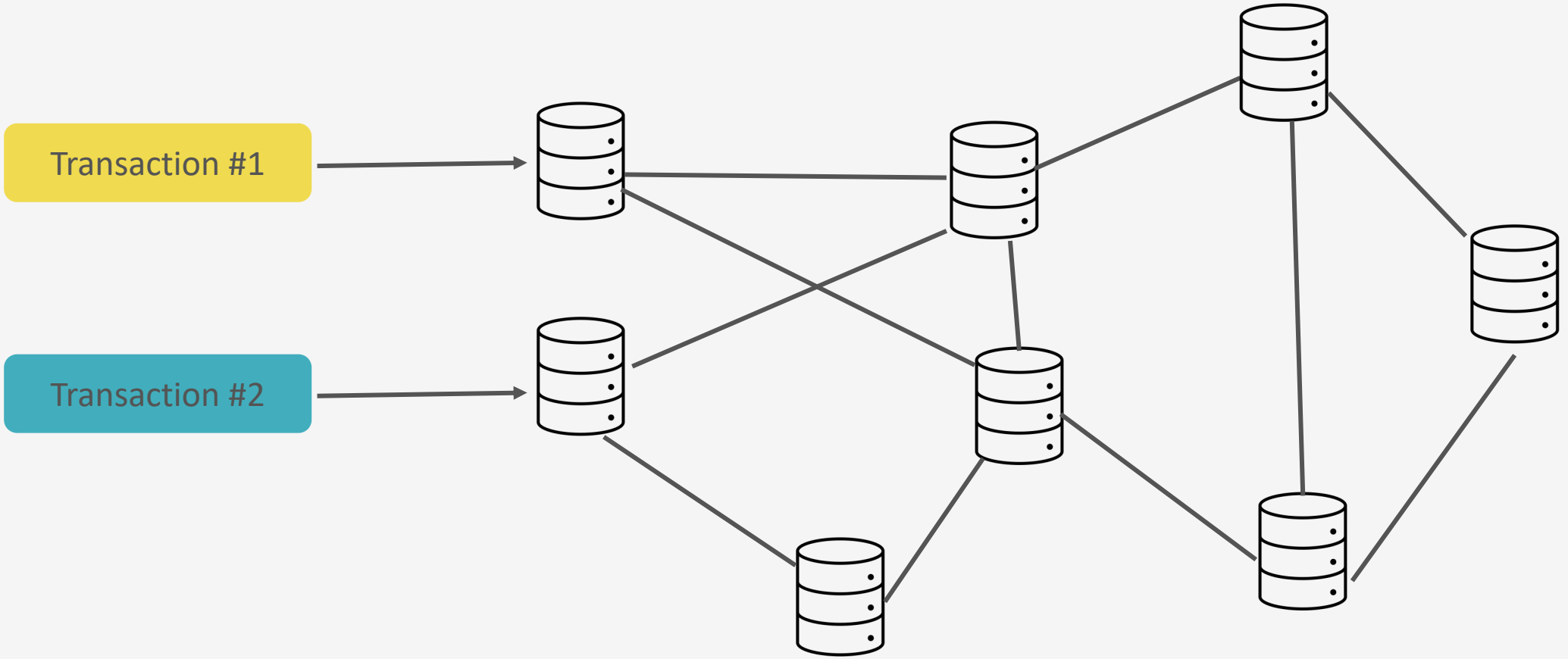
Un bloc ne peut être créé que par le nœud ayant réussi à calculer le « nonce ».

3 Le « nonce » est un valeur alphanumérique arbitraire dont l'inscription dans le bloc permettra au « hash » du bloc de répondre à la contrainte de débuter par une suite de 0

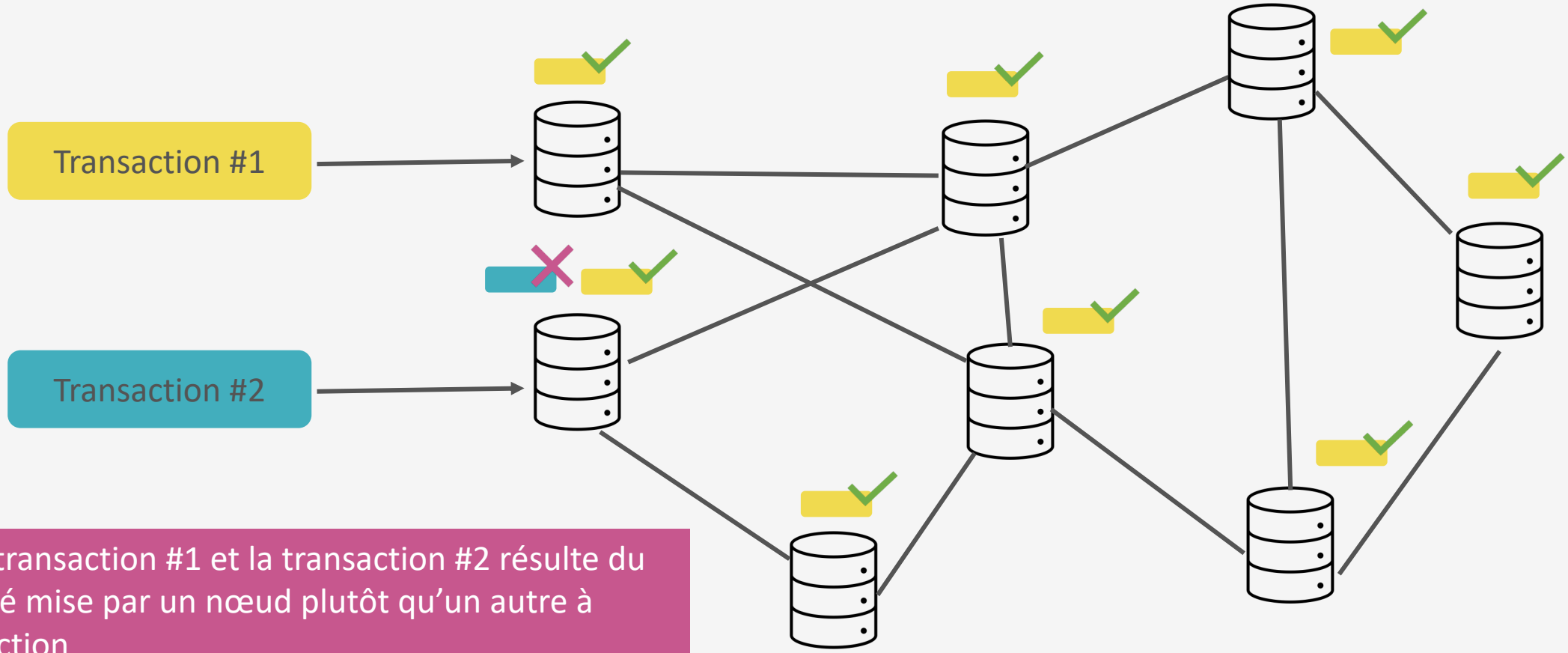
Hash du bloc y

Ex. Hash du bloc miné le 8/4/21 à 14h51 GMT :
000000000000000005f590b70379b8b4c3bf94c3729ab149c0b9927d66f214

Les transactions sont adressées à 2 nœuds différents pour être inscrites dans un bloc



Le premier nœud qui réussi à miner un bloc dans lequel figure l'une des transaction la valide et diffuse le bloc à tous les autres nœuds



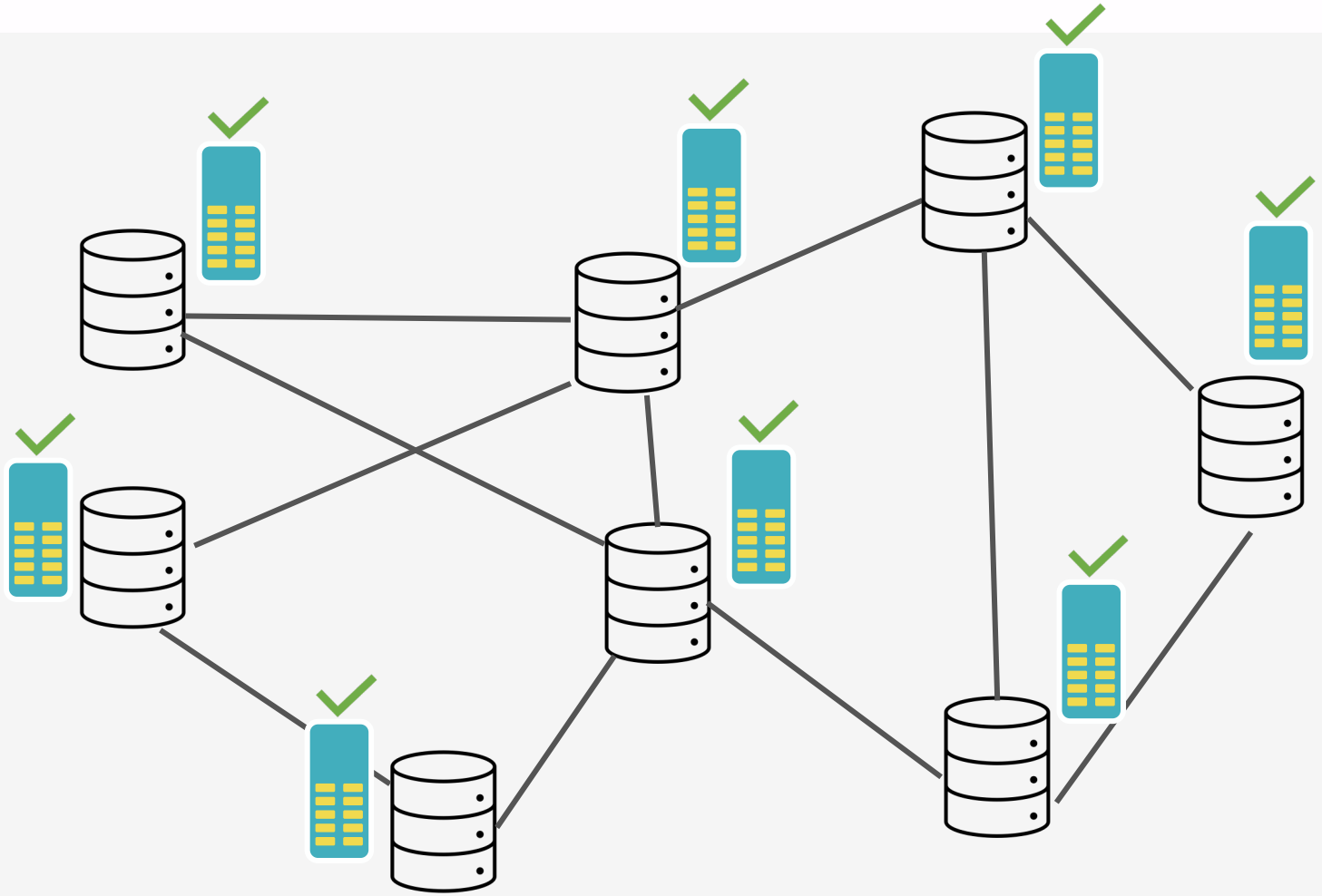
Le choix entre la transaction #1 et la transaction #2 résulte du hasard : la rapidité mise par un nœud plutôt qu'un autre à miner une transaction

La protection assurée par le minage

Le protocole Bitcoin règle automatiquement la difficulté pour les nœuds à calculer le nonce à environ 10 minutes de temps de calcul (« proof of work »)

La quantité d'effort de calcul à produire pour miner un bloc rend impossible le minage « frauduleux » de blocs pour revenir en arrière sur les blocs déjà validés

Il faudrait contrôler 51% des nœuds pour contrôler le réseau



Quelques précisions

- Le Bitcoin est divisé en Satoshi. 1 Satoshi = 0,00000001 BTC

- Le minage d'un bloc permet au mineur d'être rémunéré
  - Par des frais en Bitcoin prélevés sur l'opération
  - Par l'obtention d'une « récompense » en Bitcoin

- Le protocole Bitcoin prévoit un nombre fini de Bitcoins : 21 millions

DIGITAL & CREATIVE BUSINESS LAW

INFORMATIQUE INTERNET RESEAUX SOCIAUX E-COMMERCE

DONNEES PERSONNELLES RGPD DATA PRIVACY

TRANSITION DIGITALE ACTIFS NUMERIQUES

CREATION SPECTACLES DIVERTISSEMENT AUDIOVISUEL

L'actualité du droit du numérique
et de la création décryptée. Suivez-nous :

twitter.com/NextAvocats

www.linkedin.com/company/next-avocats/

www.instagram.com/next_avocats/