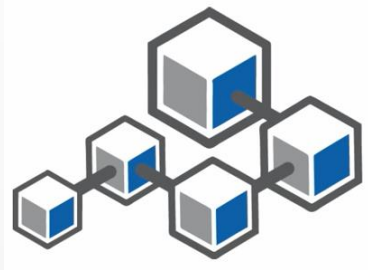


Cycle de vie d'une transaction Blockchain

Plongée en profondeur dans la blockchain

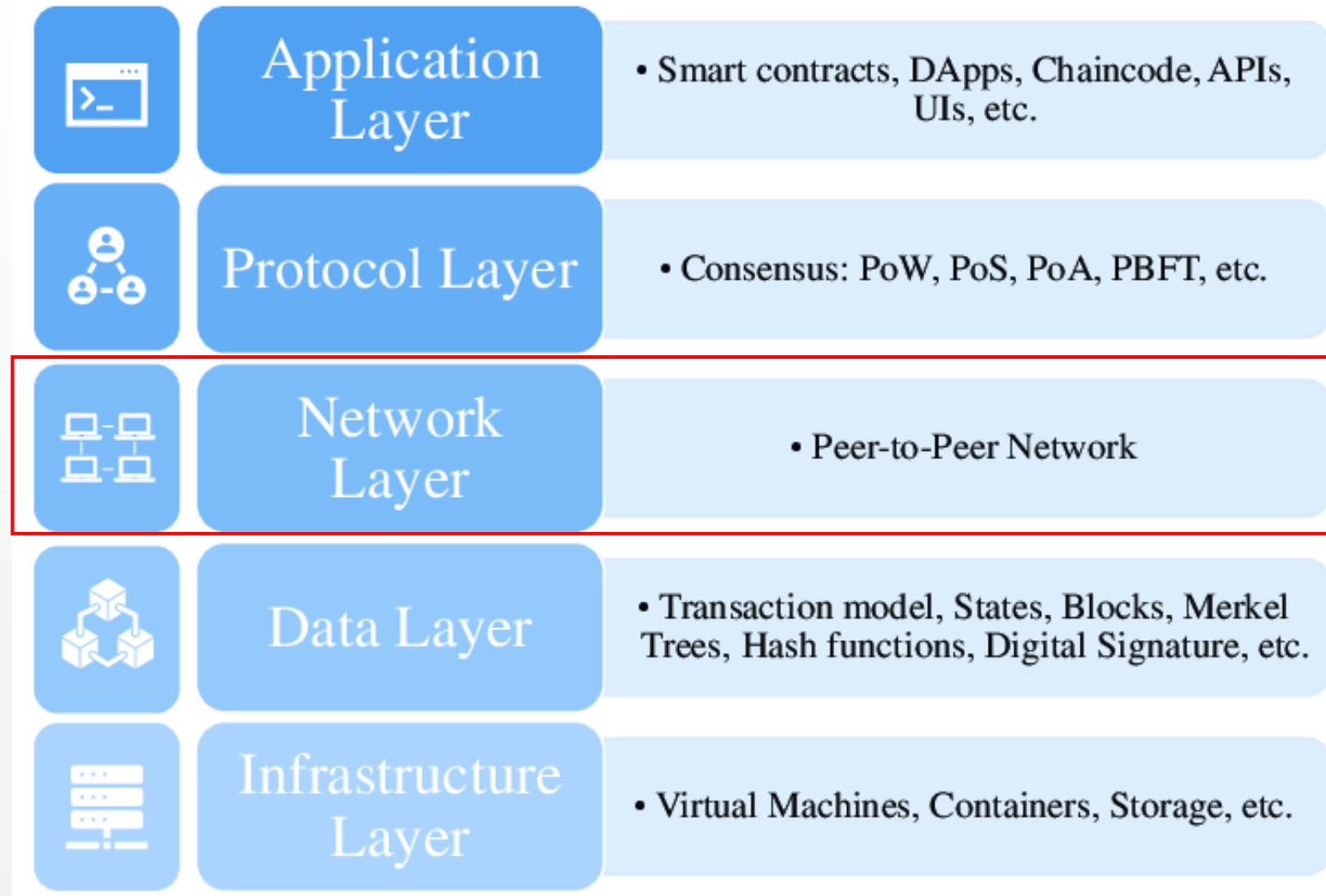


Abdelkader Ouared

abdelkader.ouared@univ-tiaret.dz



Les couches de blockchain



Cycle de vie d'une transaction Blockchain

APERÇU DU CYCLE DE VIE

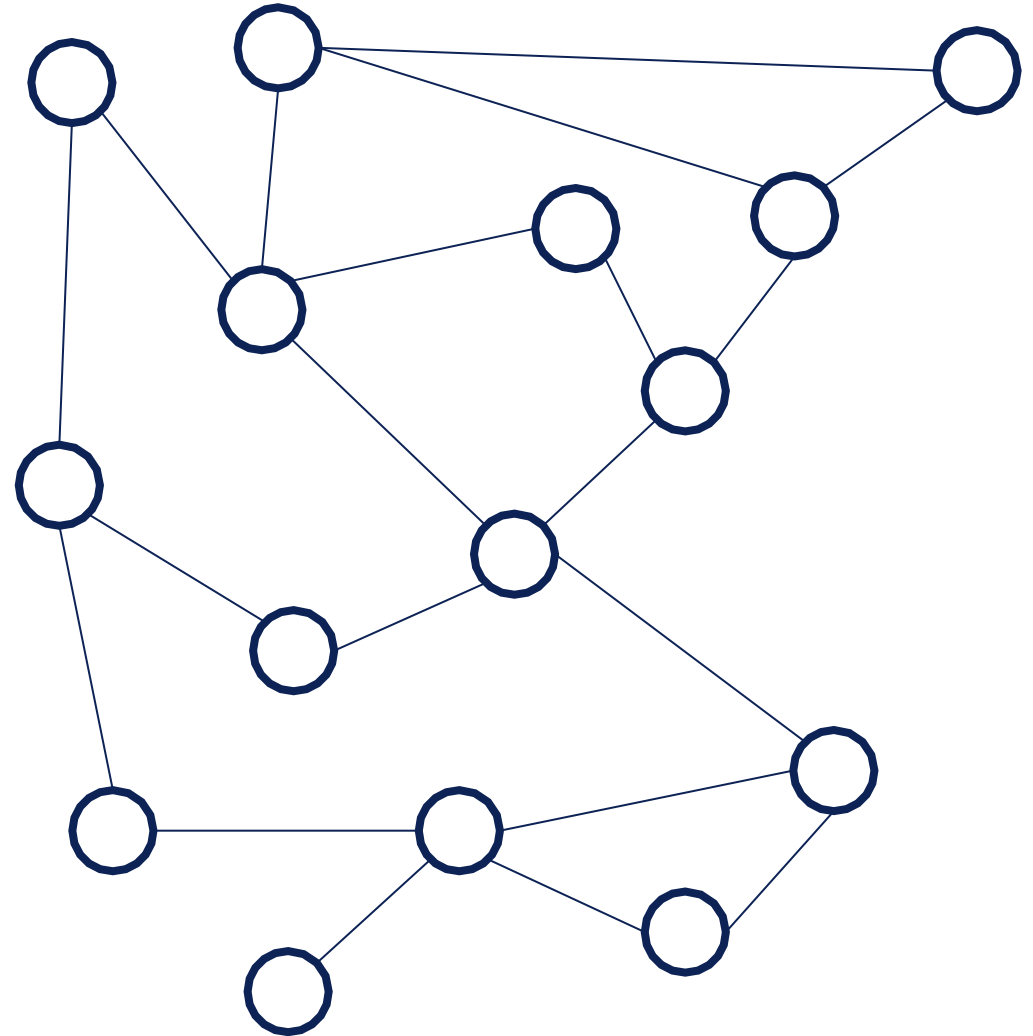
APERÇU DU CYCLE DE VIE

Création de Compte:

- Cette étape consiste à **créer une adresse unique** sur la blockchain, qui servira d'identifiant pour effectuer des transactions.
- Un compte est associé à une paire de clés cryptographiques :
 - une **clé publique** (l'adresse de compte visible)
 - une **clé privée** (utilisée pour signer des transactions et assurer la sécurité).
- Lors de la création d'un compte, un utilisateur génère ces clés grâce à **un algorithme cryptographique**. La clé publique est ensuite utilisée pour recevoir des actifs, tandis que la clé privée doit rester secrète pour sécuriser les fonds.



ACCOUNT CREATION



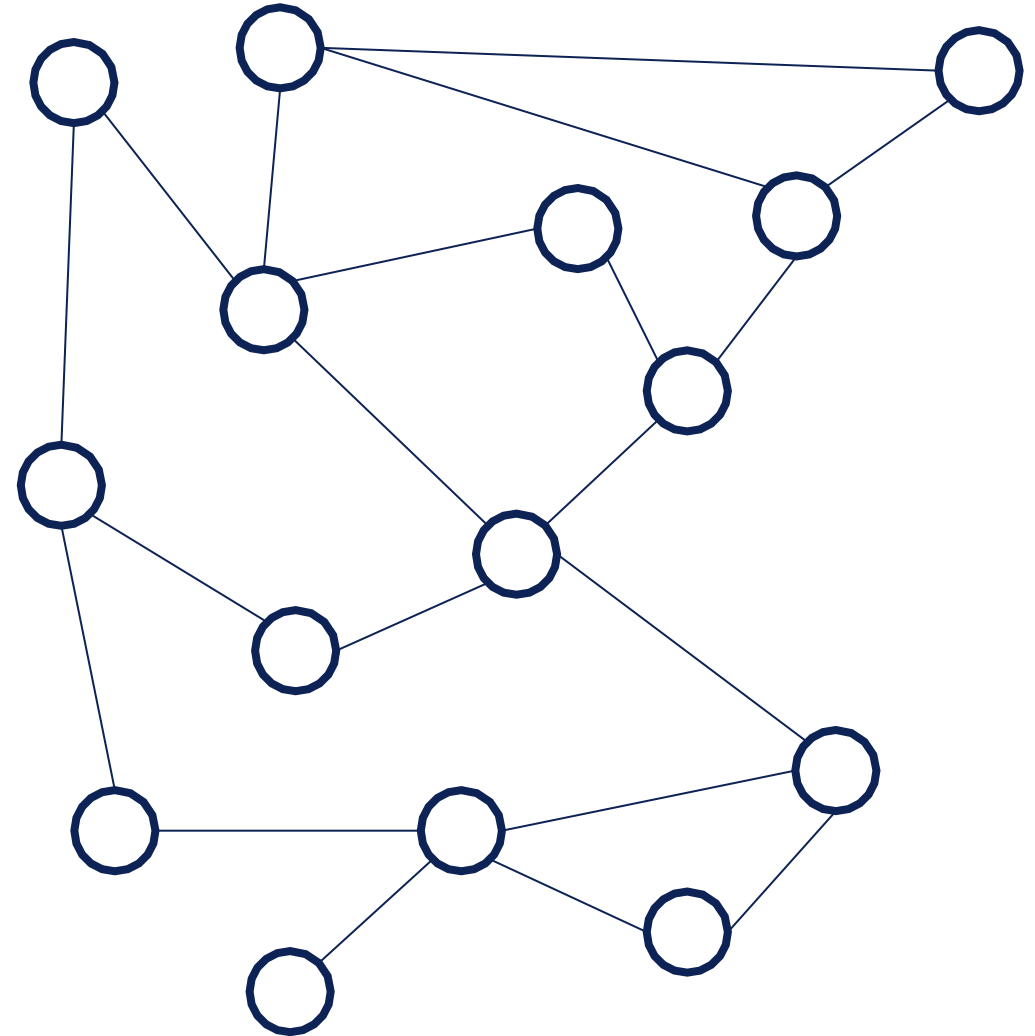
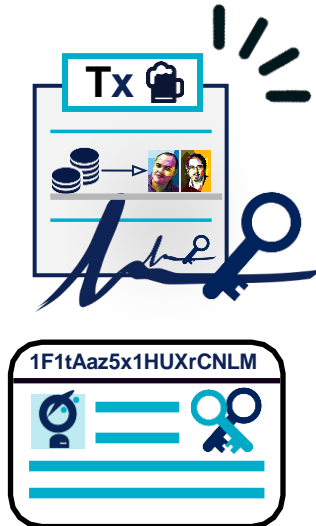
APERÇU DU CYCLE DE VIE

Préparation de la Transaction

- À cette étape, les détails de la transaction **sont spécifiés** et **configurés**. Cela inclut des informations *comme l'adresse du destinataire, le montant de l'actif à transférer*, et d'autres données nécessaires (comme les frais de transaction ou les conditions spécifiques).
- L'utilisateur **crée une structure** de transaction qui rassemble tous les paramètres.
- Dans certains cas, il peut aussi définir **des conditions spécifiques**, comme des **délais d'expiration** ou **des critères de vérification supplémentaires**.

**TRANSACTION
PREPARATION**

ACCOUNT CREATION



APERÇU DU CYCLE DE VIE

Besoin ?

- Assurer que seul le propriétaire légitime d'un compte initie la transaction.
- Garantir la sécurité et l'authenticité de la transaction sur la blockchain.

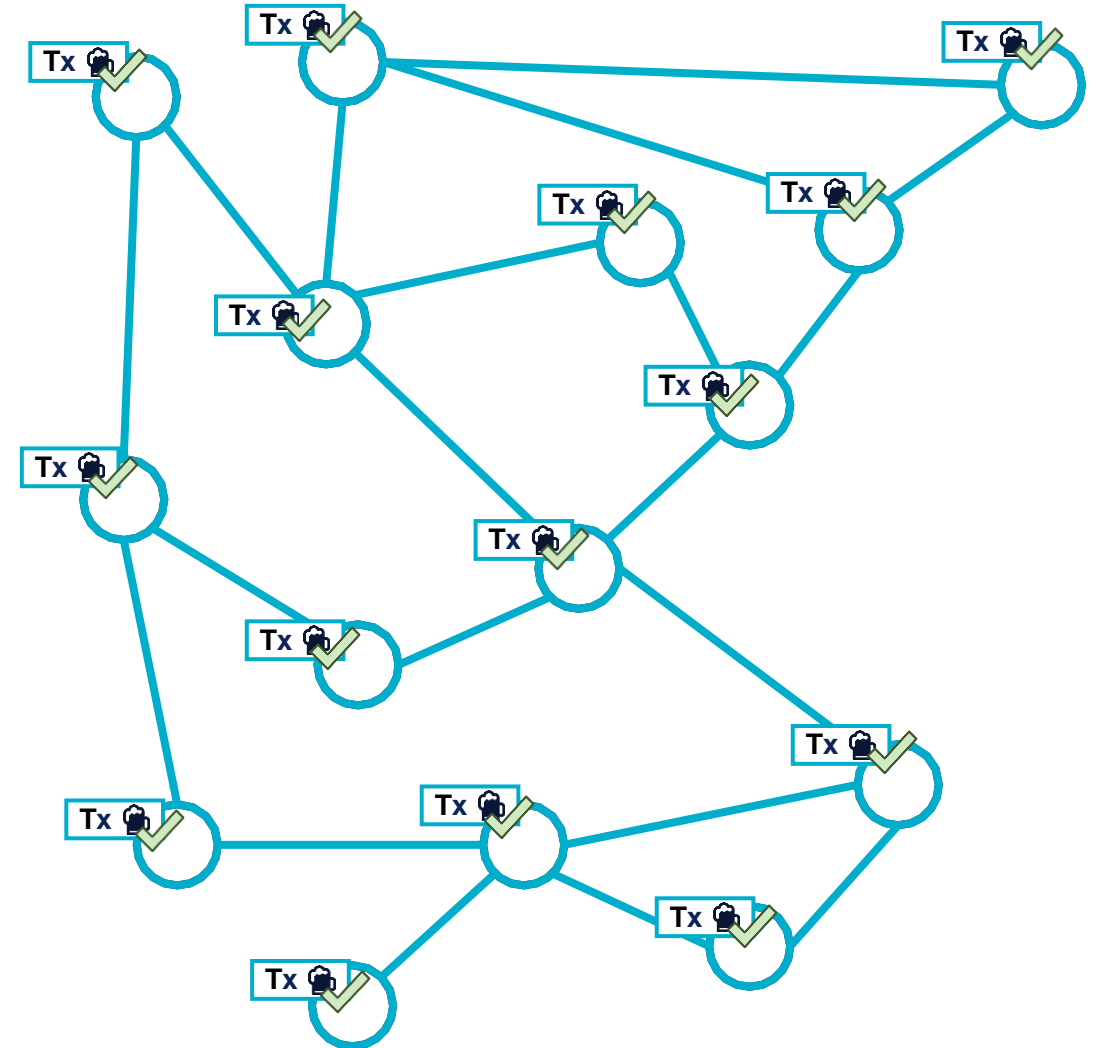
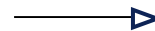
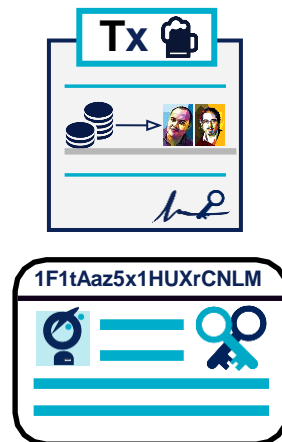
Solution

- **Signature numérique** : Utilisation de la clé privée pour prouver l'identité de l'expéditeur.
- **Envoi aux nœuds** : La transaction signée est vérifiée par des validateurs du réseau blockchain.

**TRANSACTION
SUBMISSION**

TRANSACTION
PREPARATION

ACCOUNT CREATION



APERÇU DU CYCLE DE VIE

Exécution de la Transaction

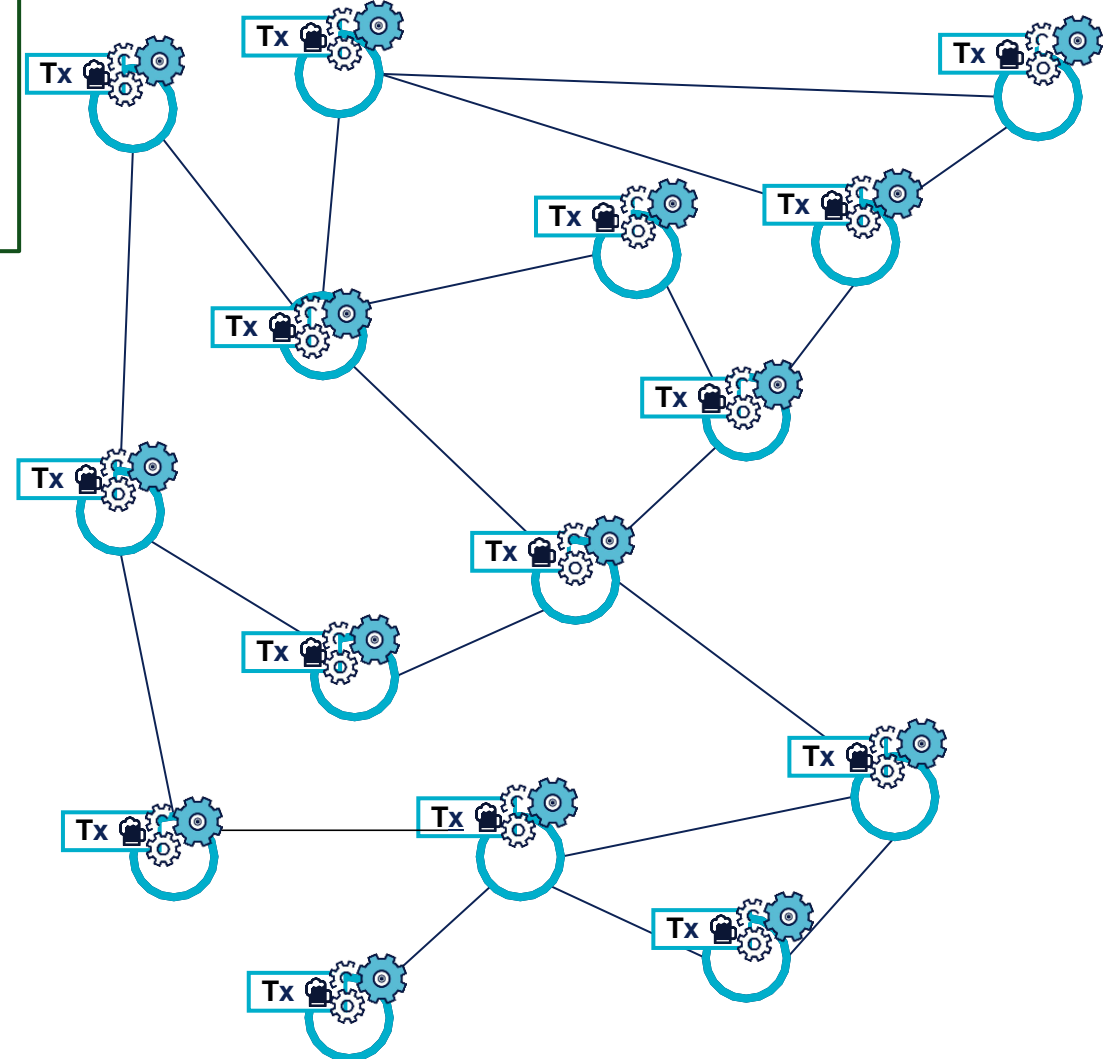
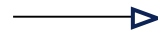
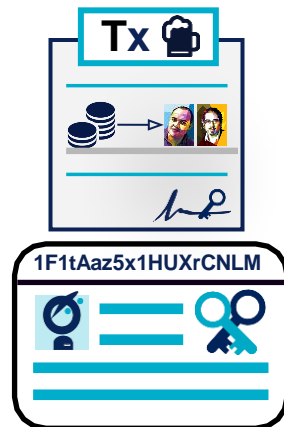
- La transaction est exécutée et validée sur la blockchain. Cela implique son ajout au registre distribué, qui est répliqué sur tous les nœuds du réseau.
- Les nœuds de la blockchain **vérifient** les détails de la transaction (**validité de la signature**, **montant suffisant**, etc.). Si tout est en ordre, la transaction est incluse dans **le prochain bloc à miner**. Une fois le bloc validé et ajouté à la blockchain, la transaction devient immuable et visible par tous.

**TRANSACTION
EXECUTION**

TRANSACTION
SUBMISSION

TRANSACTION
PREPARATION

ACCOUNT CREATION



APERÇU DU CYCLE DE VIE

Exécution de la Transaction

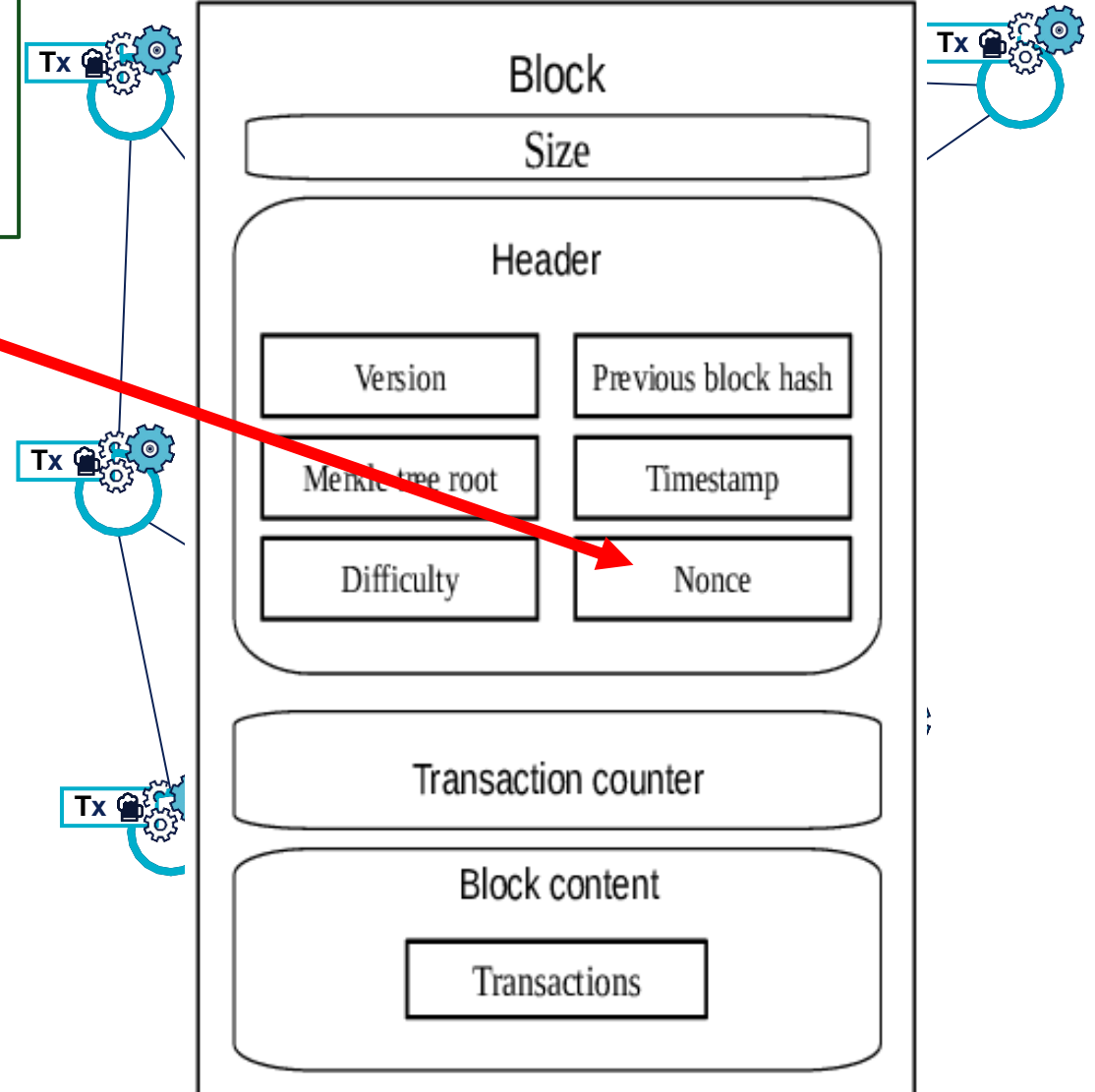
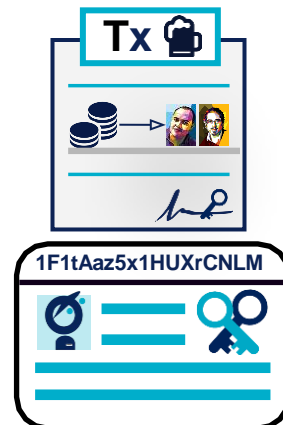
- La transaction est exécutée et validée sur la blockchain. Cela implique son ajout au registre distribué, qui est répliqué sur tous les nœuds du réseau.
- Les nœuds de la blockchain **vérifient** les détails de la transaction (**validité de la signature**, **montant suffisant**, etc.). Si tout est en ordre, la transaction est incluse dans **le prochain bloc à miner**. Une fois le bloc validé et ajouté à la blockchain, la transaction devient immuable et visible par tous.

**TRANSACTION
EXECUTION**

TRANSACTION
SUBMISSION

TRANSACTION
PREPARATION

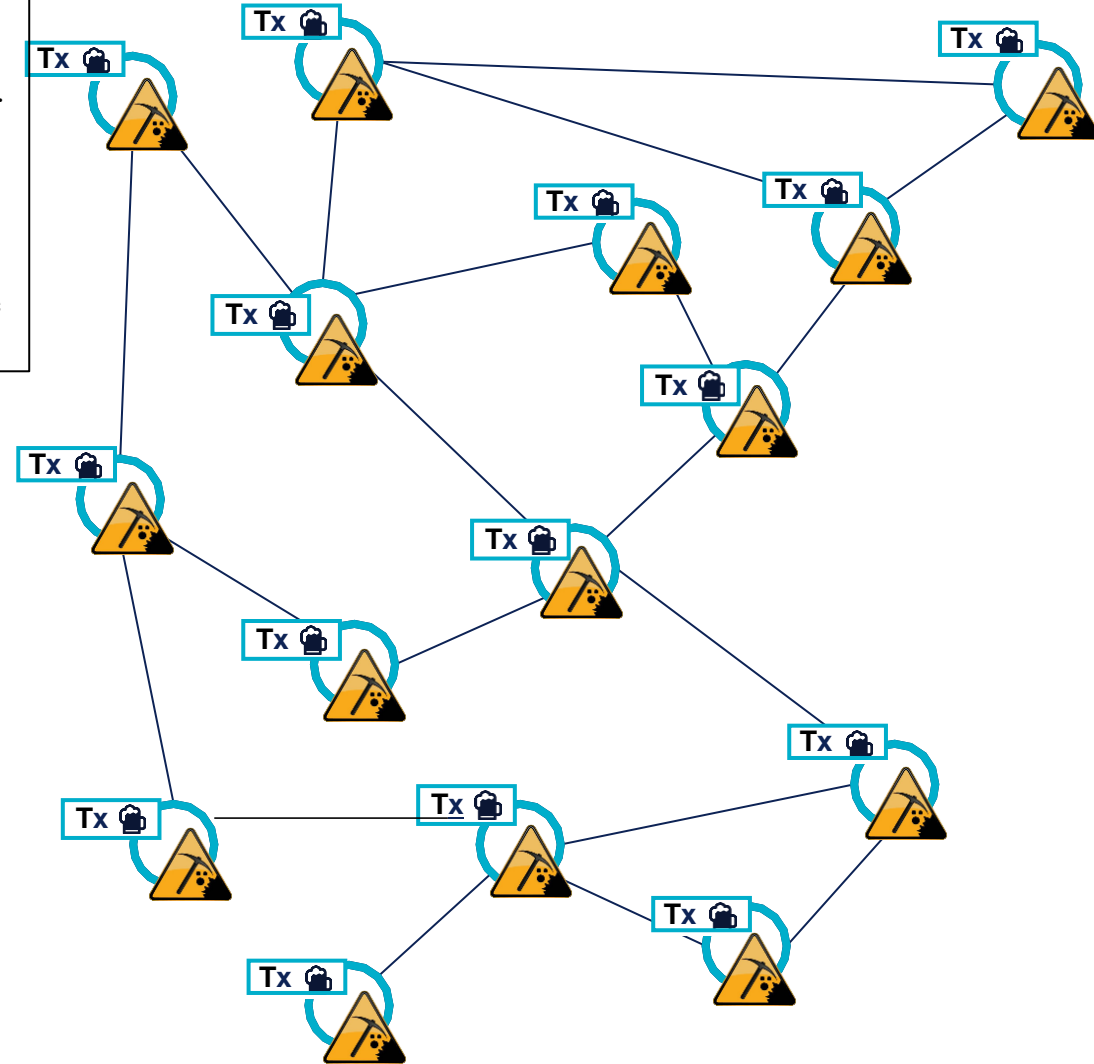
ACCOUNT CREATION



APERÇU DU CYCLE DE VIE

Mining Process (Processus de Minage)

- Valide les transactions et les enregistre dans la blockchain de façon permanente.
 - Dans une blockchain de type Proof of Work (PoW), comme celle de Bitcoin, le minage implique la résolution de problèmes mathématiques complexes pour ajouter un nouveau bloc contenant les transactions validées.
- **Processus :**
 - Les mineurs collectent les transactions non confirmées et les regroupent dans un bloc candidat.
 - Pour valider ce bloc, ils doivent résoudre un problème cryptographique en trouvant un "hash" (empreinte numérique) spécifique, conforme aux règles de difficulté du réseau.
 - Une fois la solution trouvée, **le mineur qui l'a résolue diffuse le bloc au réseau. Les autres nœuds vérifient la validité du bloc.**
 - Si le bloc est accepté, il est ajouté à la chaîne existante.
 - Le mineur reçoit une récompense sous forme de crypto-monnaie, appelée **récompense de bloc** (Block Reward), ainsi que les frais de transaction des transactions incluses dans le bloc.



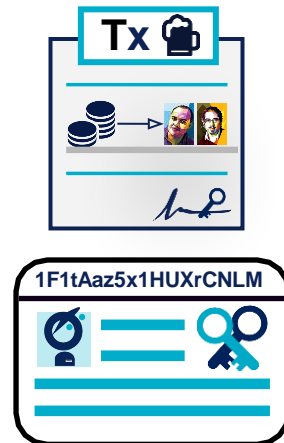
MINING PROCESS

TRANSACTION
EXECUTION

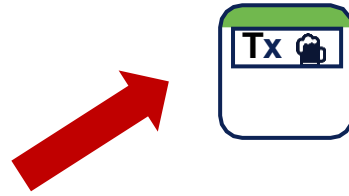
TRANSACTION
SUBMISSION

TRANSACTION
PREPARATION

ACCOUNT CREATION



APERÇU DU CYCLE DE VIE



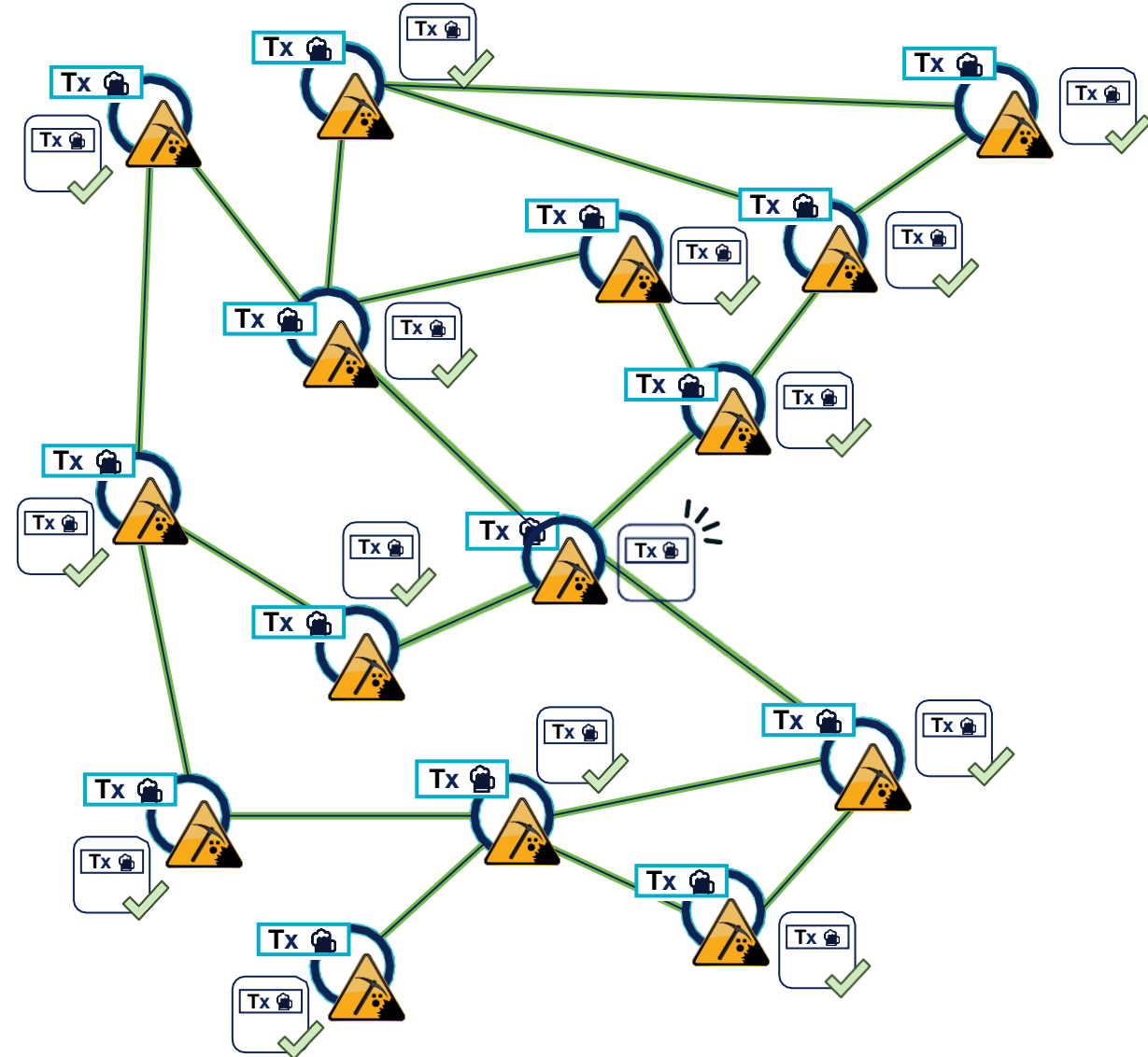
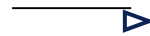
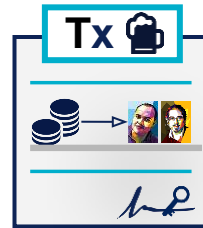
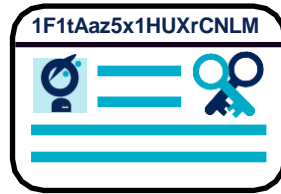
MINING PROCESS

TRANSACTION
EXECUTION

TRANSACTION
SUBMISSION

TRANSACTION
PREPARATION

ACCOUNT CREATION



APERÇU DU CYCLE DE VIE

Une **première confirmation** est obtenue lorsque la transaction est incluse dans un bloc miné, et chaque bloc suivant renforce sa sécurité. Après l'ajout du bloc contenant la transaction, **chaque nouveau bloc augmente le nombre de confirmations**, rendant la transaction plus immuable, avec un minimum généralement **requis de 3 à 6 confirmations** pour la considérer comme sécurisée. Ces confirmations rendent les transactions pratiquement impossibles à modifier, protégeant ainsi contre les annulations ou les retours en arrière.

TRANSACTION CONFIRMATION

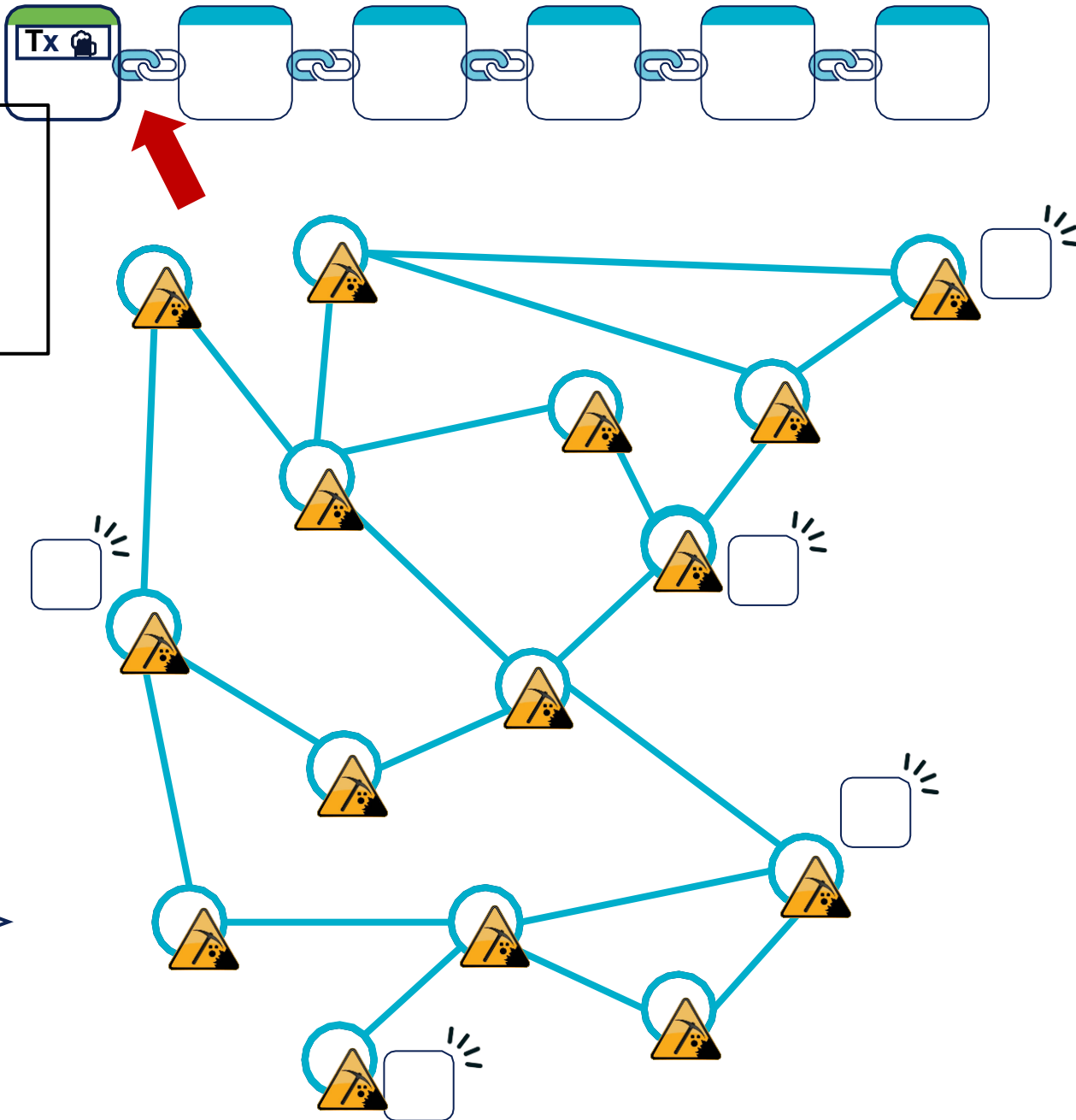
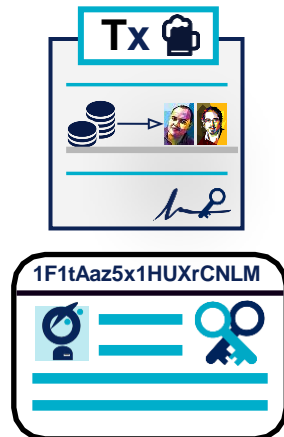
MINING PROCESS

TRANSACTION EXECUTION

TRANSACTION SUBMISSION

TRANSACTION PREPARATION

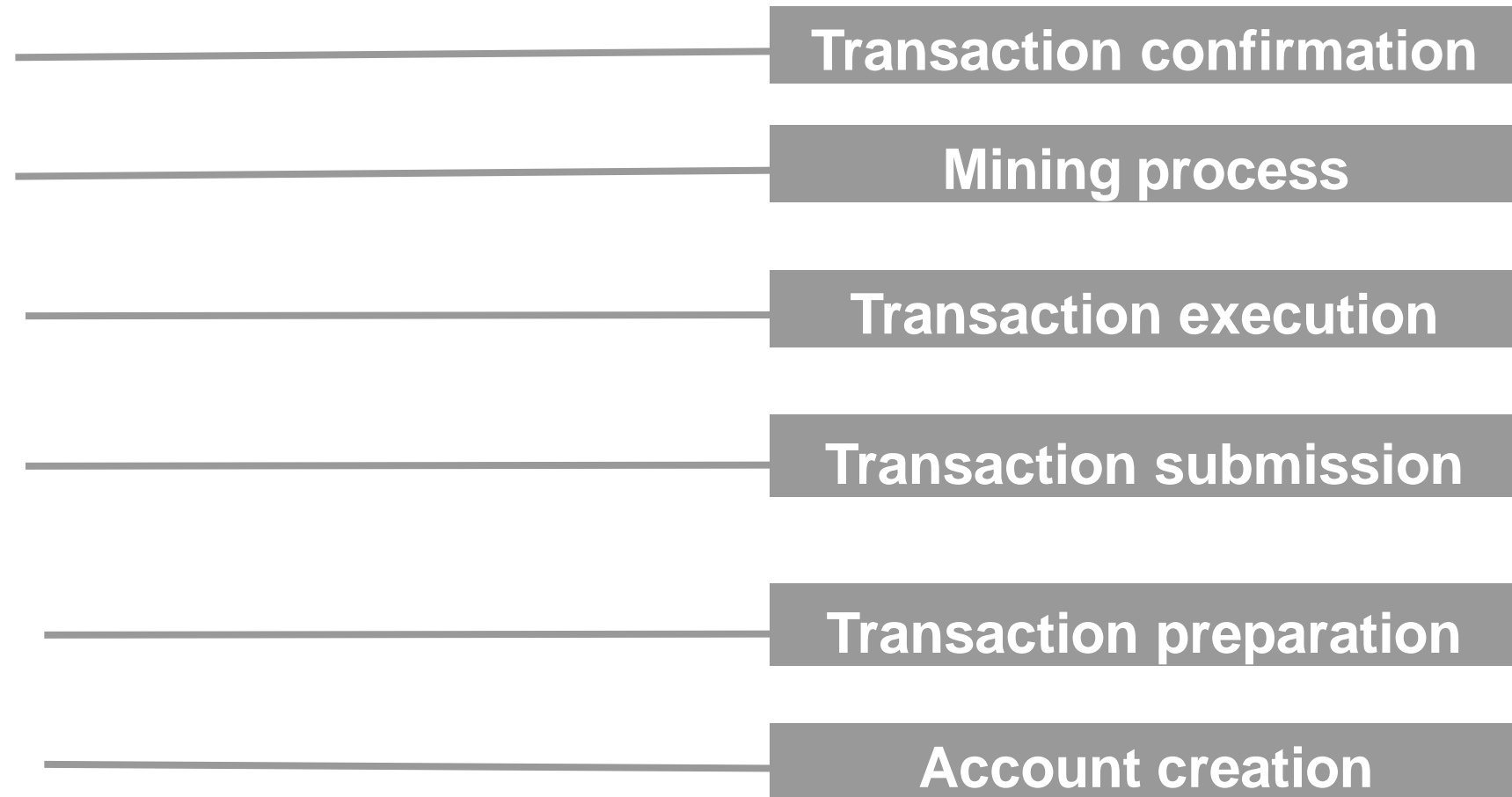
ACCOUNT CREATION





Plongée en profondeur dans la blockchain

Cycle de vie d'une transaction :



Aux Origines de la Confidentialité Numérique : Le Mouvement Cypherpunk

Cypherpunk et Crypto-anarchie

- **Cypherpunk** : Mouvement d'activistes prônant la protection de la vie privée et la liberté d'expression grâce à la cryptographie. Ils soutiennent que la cryptographie permet de se libérer de la surveillance et garantit la sécurité des communications.
- **Crypto-anarchie** : Philosophie associant cryptographie et principes anarchistes, visant à éliminer les intermédiaires et promouvoir l'autonomie individuelle.
- **Impossible2Possible (I2P)** : Réseau anonyme permettant des communications sécurisées et privées sur Internet, rendant la surveillance difficile.



Qu'est-ce qu'une cryptomonnaie ?

Une cryptomonnaie est une monnaie virtuelle qui utilise la cryptographie pour garantir les propriétés essentielles de la monnaie.

Acceptabilité

Uniformité

Durabilité

Transférabilité

Divisibilité

QUELQUES CRYPTO-MONNAIES CÉLÈBRES



Bitcoin



• **Dash**



Litecoin



• **Dogecoin**



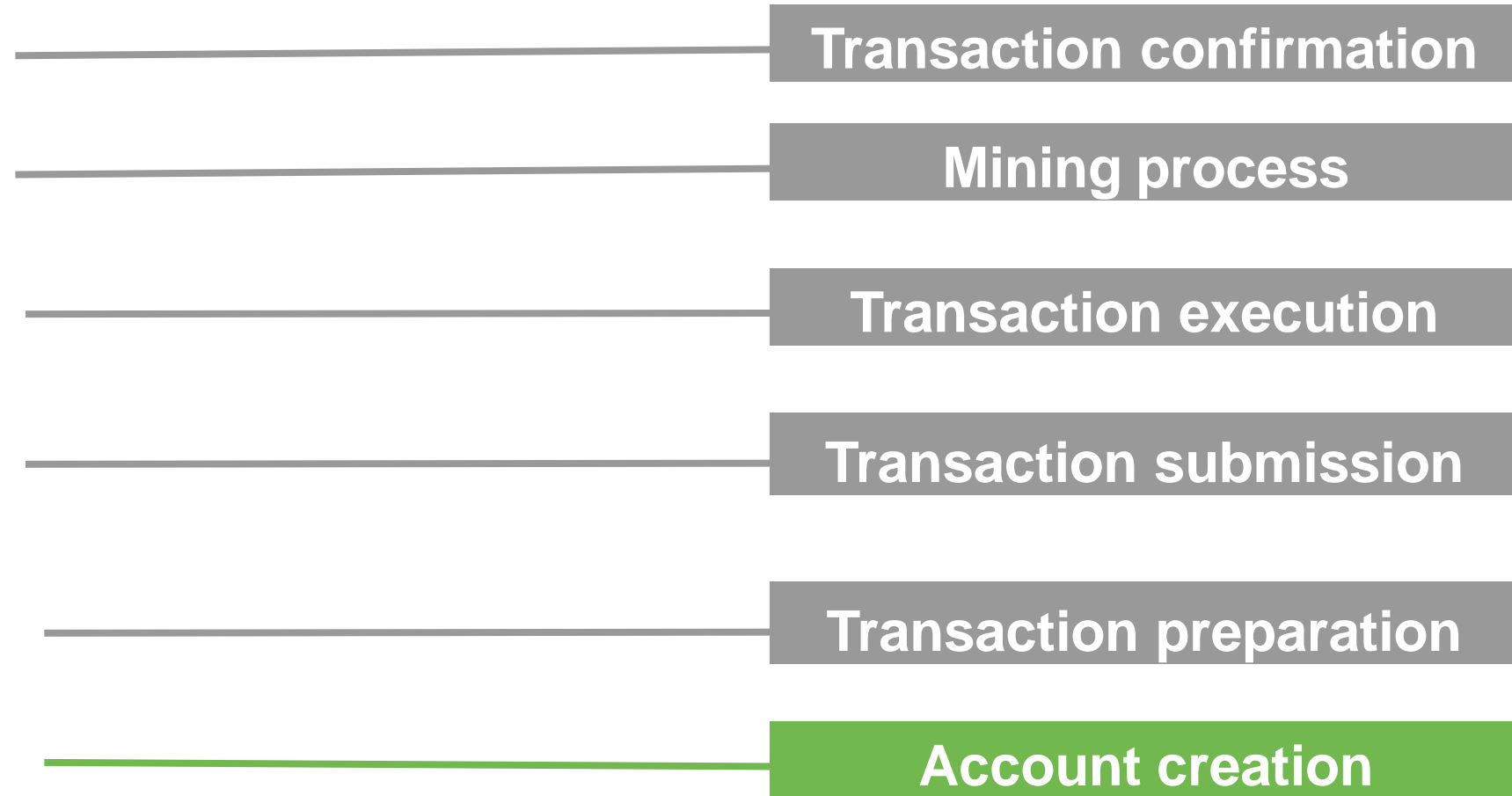
Ether



Ripple

Cycle de vie d'une transaction

Création de compte



QU'EST-CE QU'UN COMPTE ?

Un compte est **un objet identifié de manière unique** qui pourra émettre **des transactions** et **stocker de la monnaie**.

Deux problèmes :

- comment créer un identifiant unique **sans autorité centrale** ?
- Comment s'assurer que les transactions ont été émises **légitimement** à partir d'un compte ?

QU'EST-CE QU'UN COMPTE ?

Un compte est **un objet technique** qui pourra émettre **des transactions monnaie**.

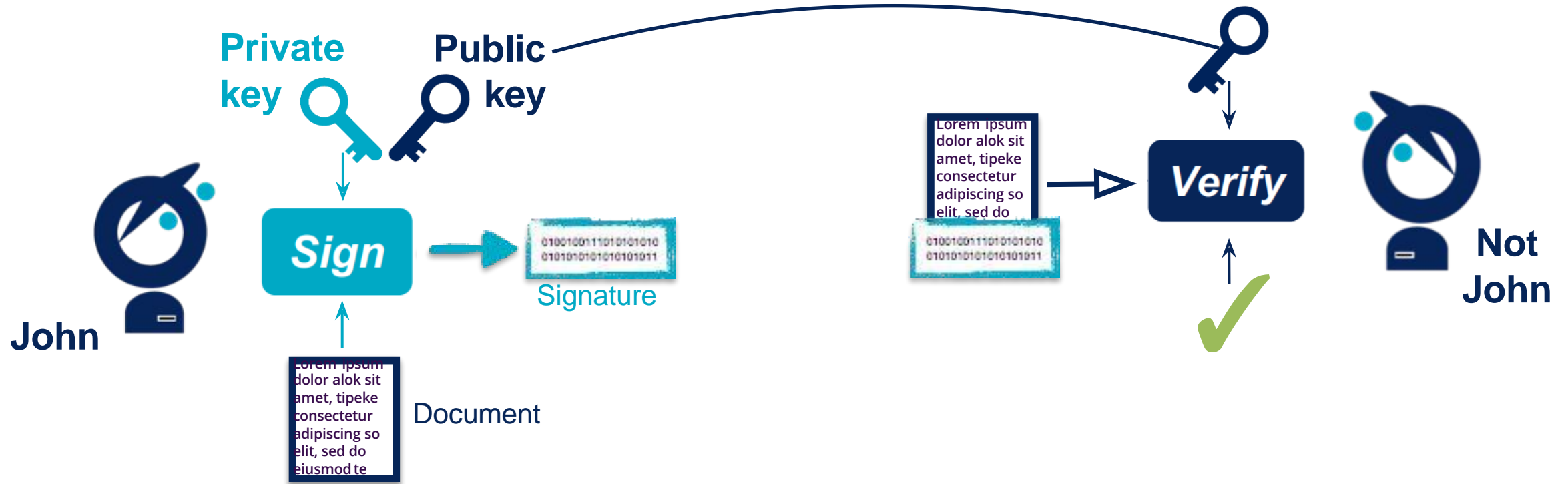
La cryptographie
comme solution

Deux problèmes :

- comment créer une **autorité centrale** ?
- Comment s'assurer que les transactions émises **légitimement** ont été



CRYPTOGRAPHIE : SIGNATURE ÉLECTRONIQUE



CRYPTOGRAPHIE : FONCTION DE HASH CRYPTOGRAPHIQUE

```
01010001000110001011
11010100101110101010
10010101010101010101
01010110101001010101
01010101010100101010
10100101010101010100
1010100101101
```

Any size



0x32ab7f65

Fixed size

```
01010001000110001011
11010100101110101010
10010101010101010101
01010110101001010101
01010101010100101010
10100101010101010100
1010100101101
```

Original input



0x32ab7f65

Hash value

```
01010001000110001011
11010100101110101010
10010101010101010101
01010110101001010101
01010101010100101010
10100101010101010100
1010100101100
```

Small change



0x**47f42e10**

Big change

Original
input

```
11001000100010010101
01010101010101101010
10101011010101010101
01010101010100010101
01001010010001001010
00100010000011111101
01110111111111
```



```
01010001000110001011
11010100101110101010
10010101010101010101
01010110101001010101
01010101010100010101
10100101010101010100
1010100101101
```

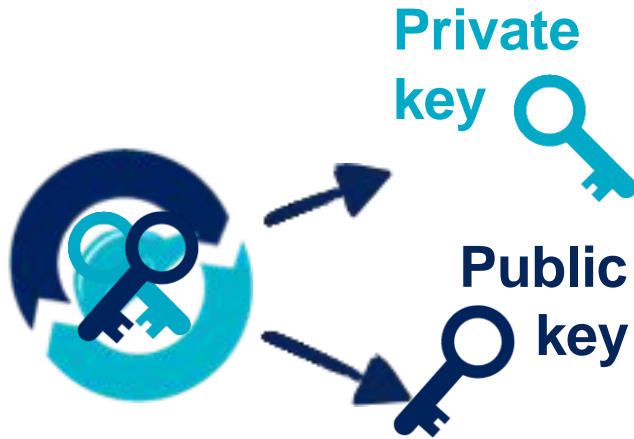
Different
input



0x32ab7f65

CRÉATION DE COMPTE : MÉCANISME STANDARD

1. Key generation



Most blockchain use
Elliptic Curve Algorithms
(courbes elliptiques)

2. Public Key Hashing

[hachage SHA-256 & RIPEMD-160]



Ensure shorter address
Protect against attack
on Public key

3. Address Encoding

Standard Address =>
Base58Check encoding for
Bitcoin

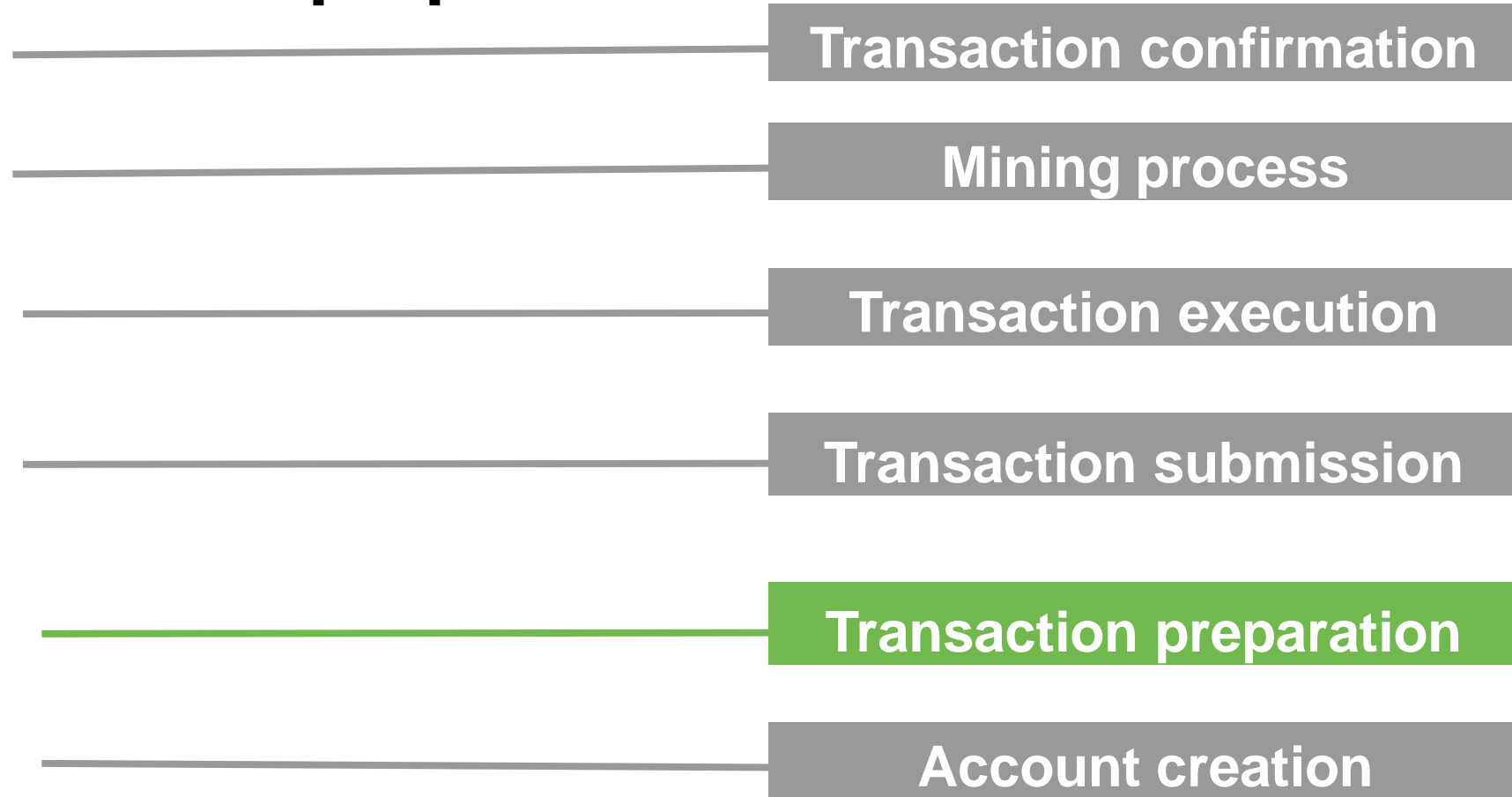


```
0bed7abd61247635c197  
3eb38474a2516ed1d884
```

Make it (a bit more)
readable

Cycle de vie d'une transaction :

Transaction preparation



QU'EST-CE QU'UNE TRANSACTION



La transaction « payez-nous-un-café »

Émetteur



Montant



Destinataires



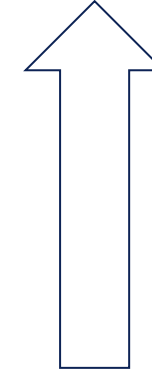
Scripts de transactions

“Envoyer à des adresses”

GRAND LIVRE

Temps ↓

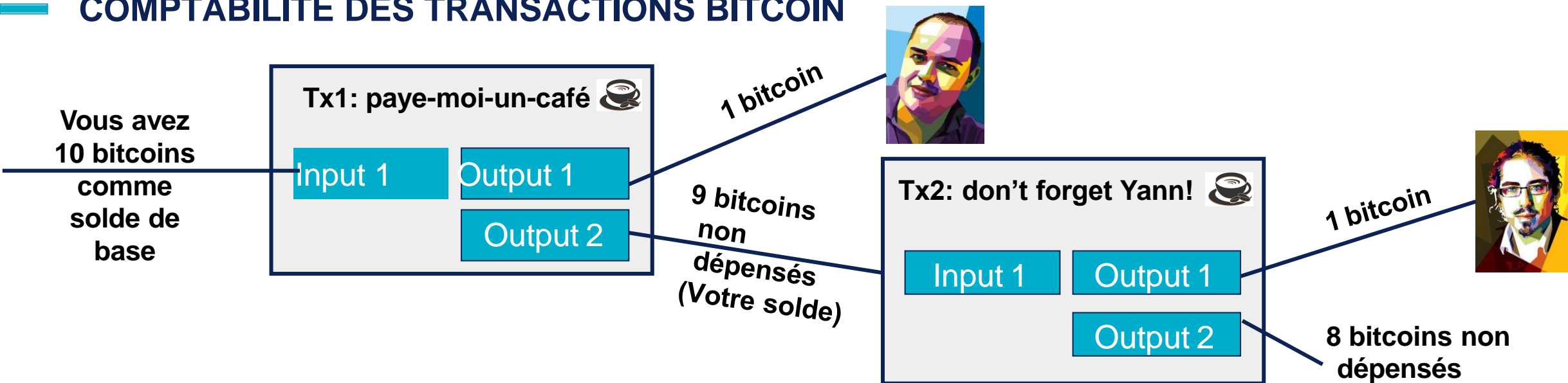
Créez 25 coins et enregistrez-les à votre nom	affirmé par les mineurs
Transférez 17 coins de votre compte à Erwan, signées par vous.	signé par vous
Transférer 8 coins d'Erwan à Yann	signé par Erwan
Transférez 5 coins de Yann à vous	signé par Yann
Transférez 15 coins de vous à Erwan	signé par vous



Il faudra peut-être remonter jusqu'à la genèse (genesis)!

Est valide?

COMPTABILITÉ DES TRANSACTIONS BITCOIN



❑ Une transaction consiste à transférer des fonds d'une ou plusieurs entrées vers une ou plusieurs sorties

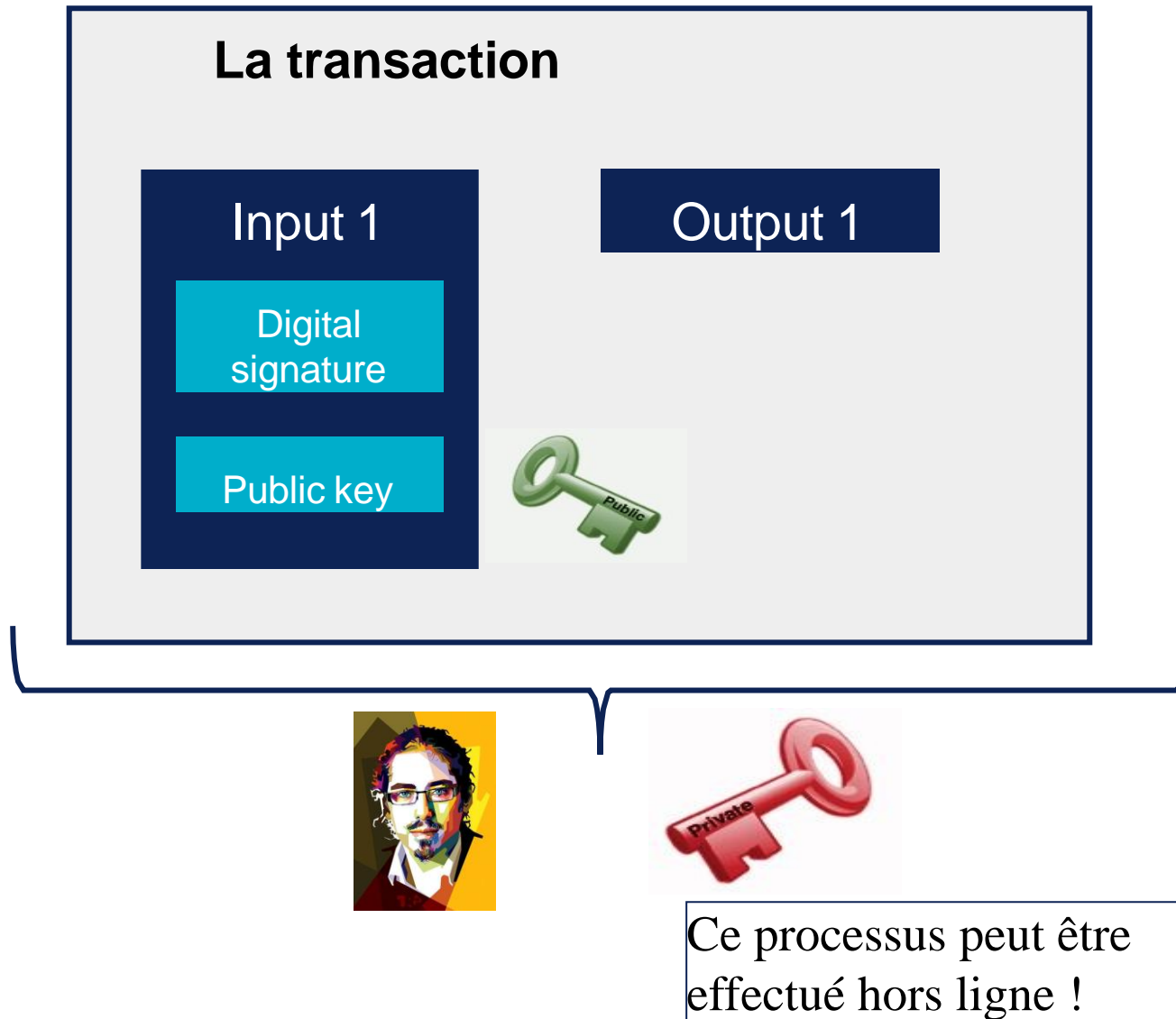
- **Entrées** : Sources de fonds utilisés dans la transaction.
- **Sorties** : Destinations et montants envoyés dans la transaction
- Dans chaque transaction, les entrées doivent être égales ou supérieures aux sorties

Inputs Des bitcoins à dépenser	Chaque entrée est une référence signée d'un trnx précédent
Outputs Attribuer à de nouveaux propriétaires	Chaque sortie ne peut être utilisée que par 1 seule entrée pour éviter les doubles dépenses

Les sorties non dépensées = le solde de quelqu'un
C'est ce que nous appelons les bitcoins (ajoutez tous les bitcoins non dépensés d'un grand livre public pour savoir combien de bitcoins possède la chaîne)

Montant de la sortie de change = Somme des entrées - (Montant envoyé + Frais)

SIGNATURE DE TRANSACTION



1. Vous effectuez la transaction, vous devez donc **signer votre transaction avec votre clé privée**
2. Vous devez joindre **la signature** et **votre clé publique** à la transaction afin que tout le monde puisse la vérifier.

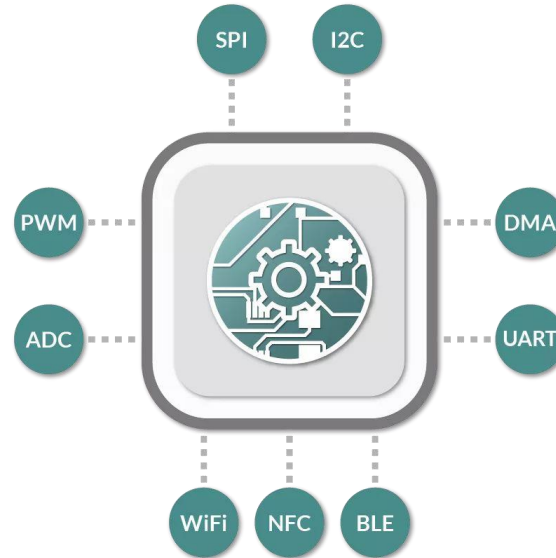
SCRIPTS DE TRANSACTION ?



L'expéditeur choisit le script en fonction de ses besoins et du type de transaction

Exemples:

- l'expéditeur veut simplement envoyer des fonds à une adresse [script P2PKH]
- Pour une transaction nécessitant plusieurs signatures [script P2SH]
- Si les frais sont un critère important [P2WPKH ou P2WSH]



ByteCode exécuté dans une machine virtuelle



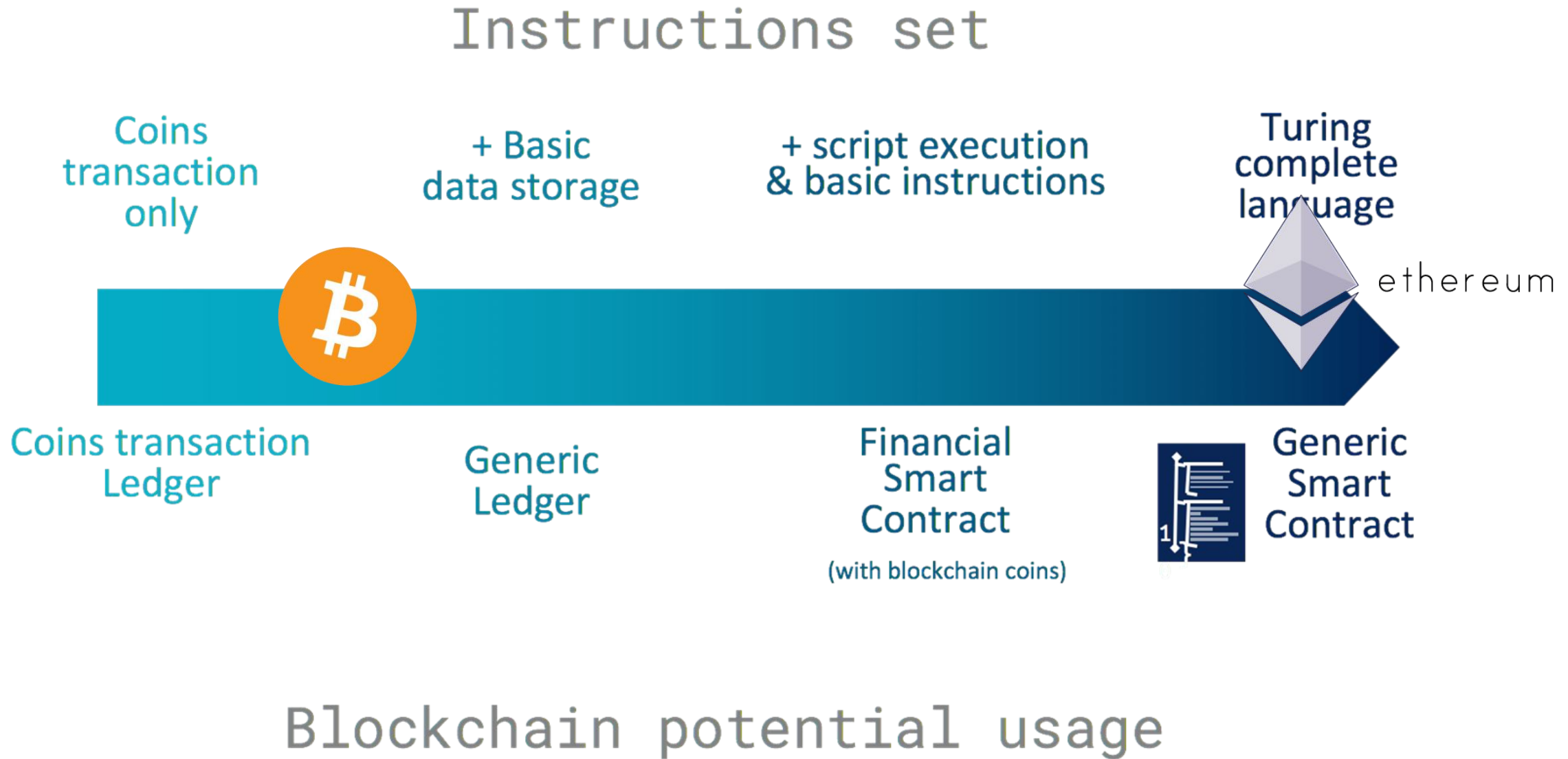
Ensemble d'instructions souvent limité

Pas de boucle dans Bitcoin



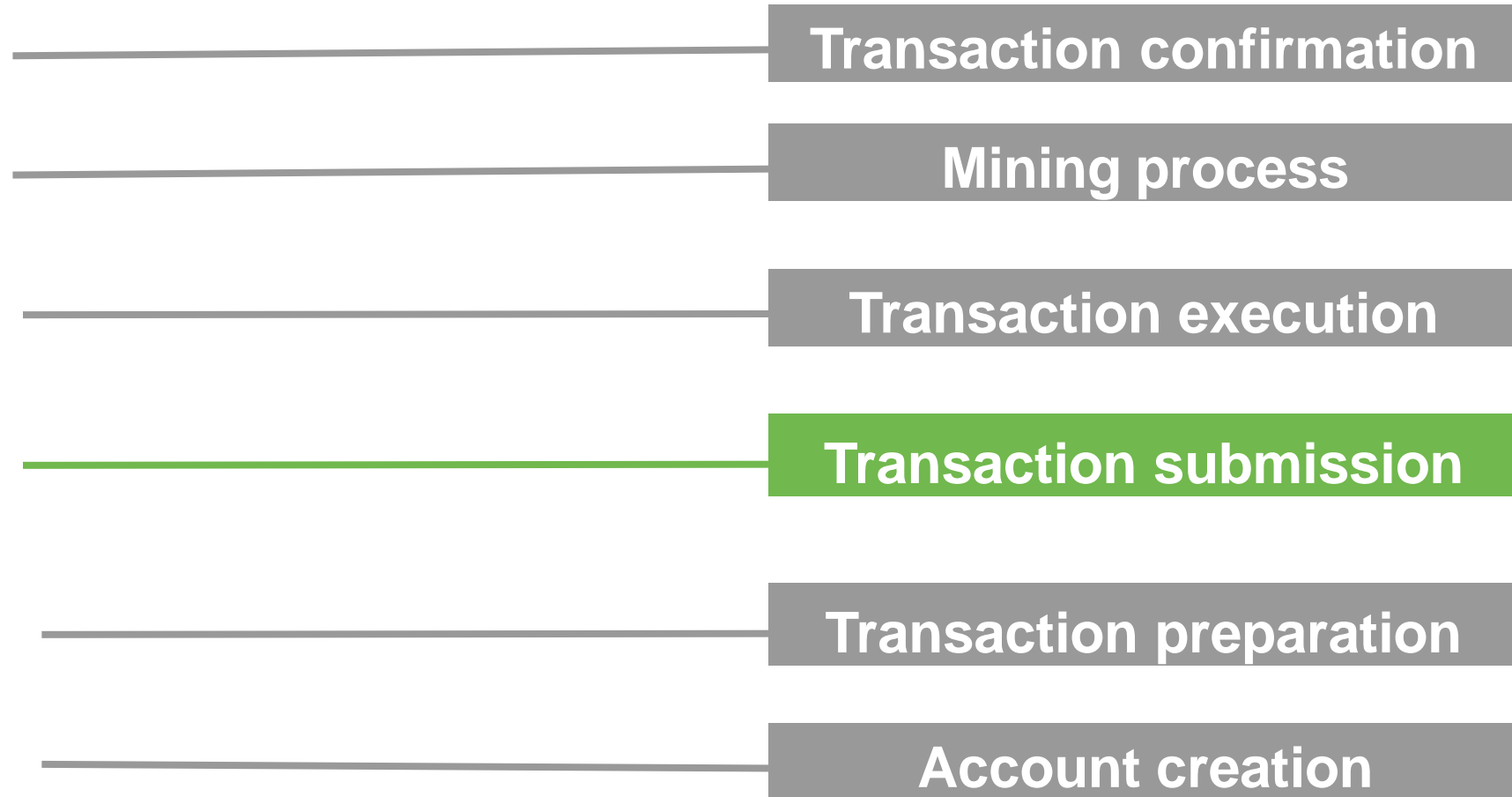
Bitcoin utilise un langage basé sur une pile

LES CAPACITÉS DE SCRIPTING SONT DIFFÉRENTES D'UNE BLOCKCHAIN À L'AUTRE !



Cycle de vie d'une transaction :

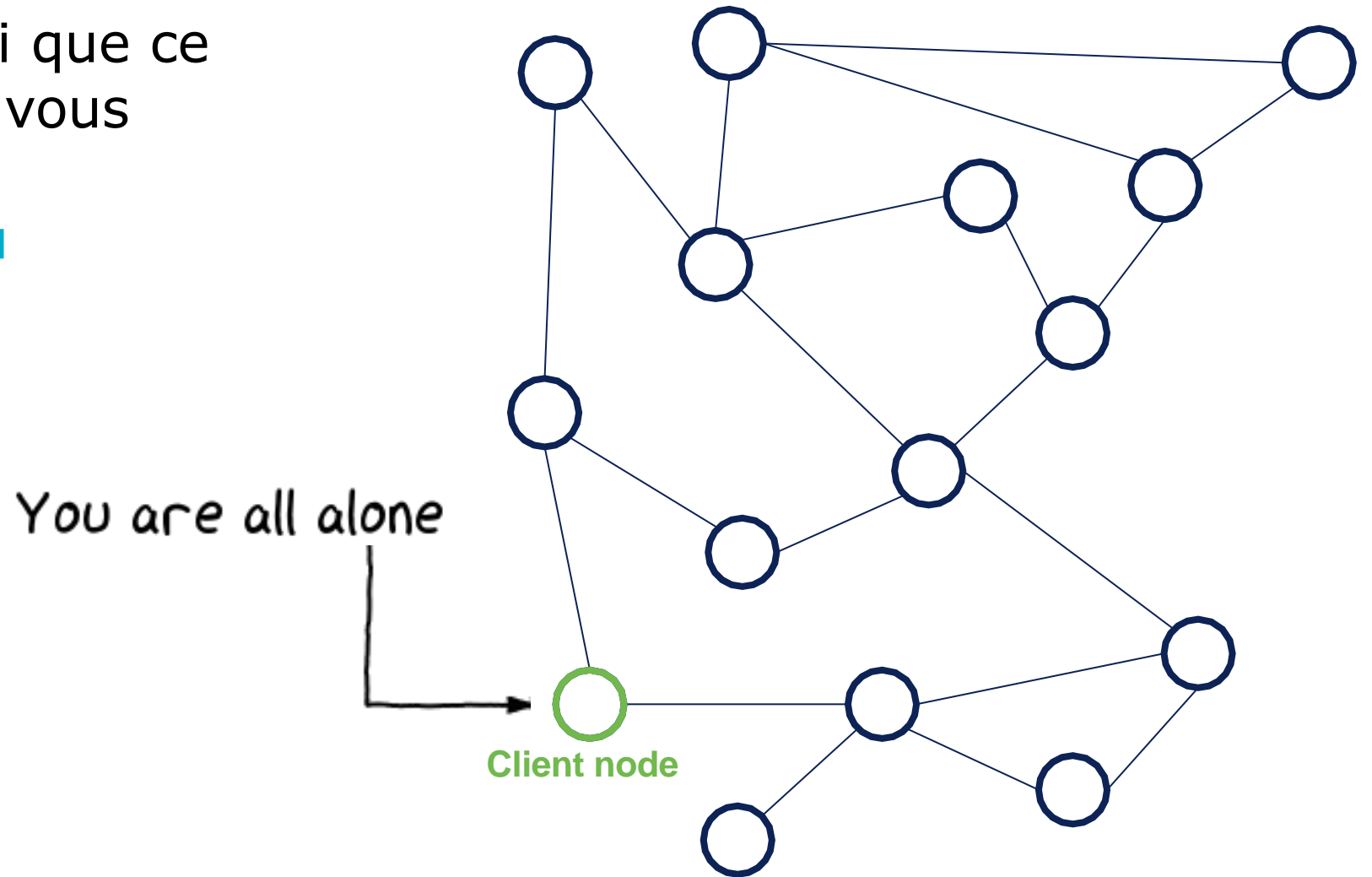
Transaction submission



PREMIÈRE ÉTAPE : TROUVEZ VOS AMIS

Pour pouvoir faire quoi que ce soit sur la blockchain, vous devez d'abord...

Découvrez le réseau blockchain !

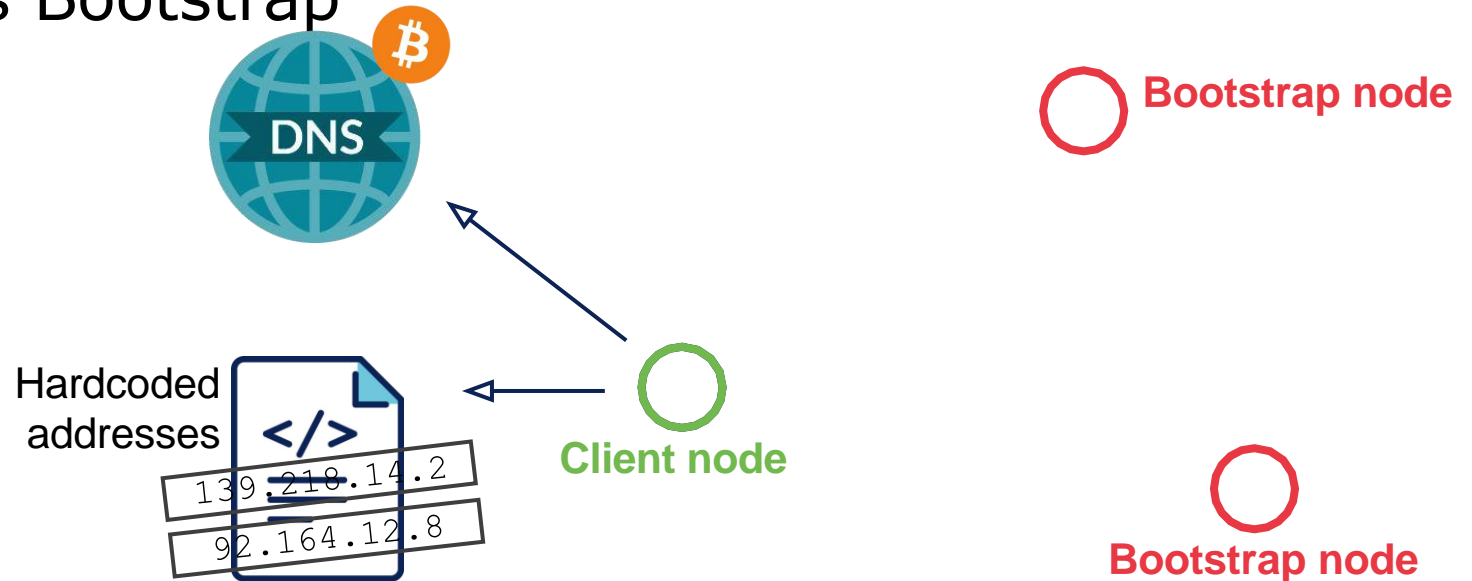


PREMIÈRE ÉTAPE : TROUVEZ VOS AMIS

Pour pouvoir faire quoi que ce soit sur la blockchain, vous devez d'abord...

Découvrez le réseau blockchain !

1. Trouver des nœuds Bootstrap

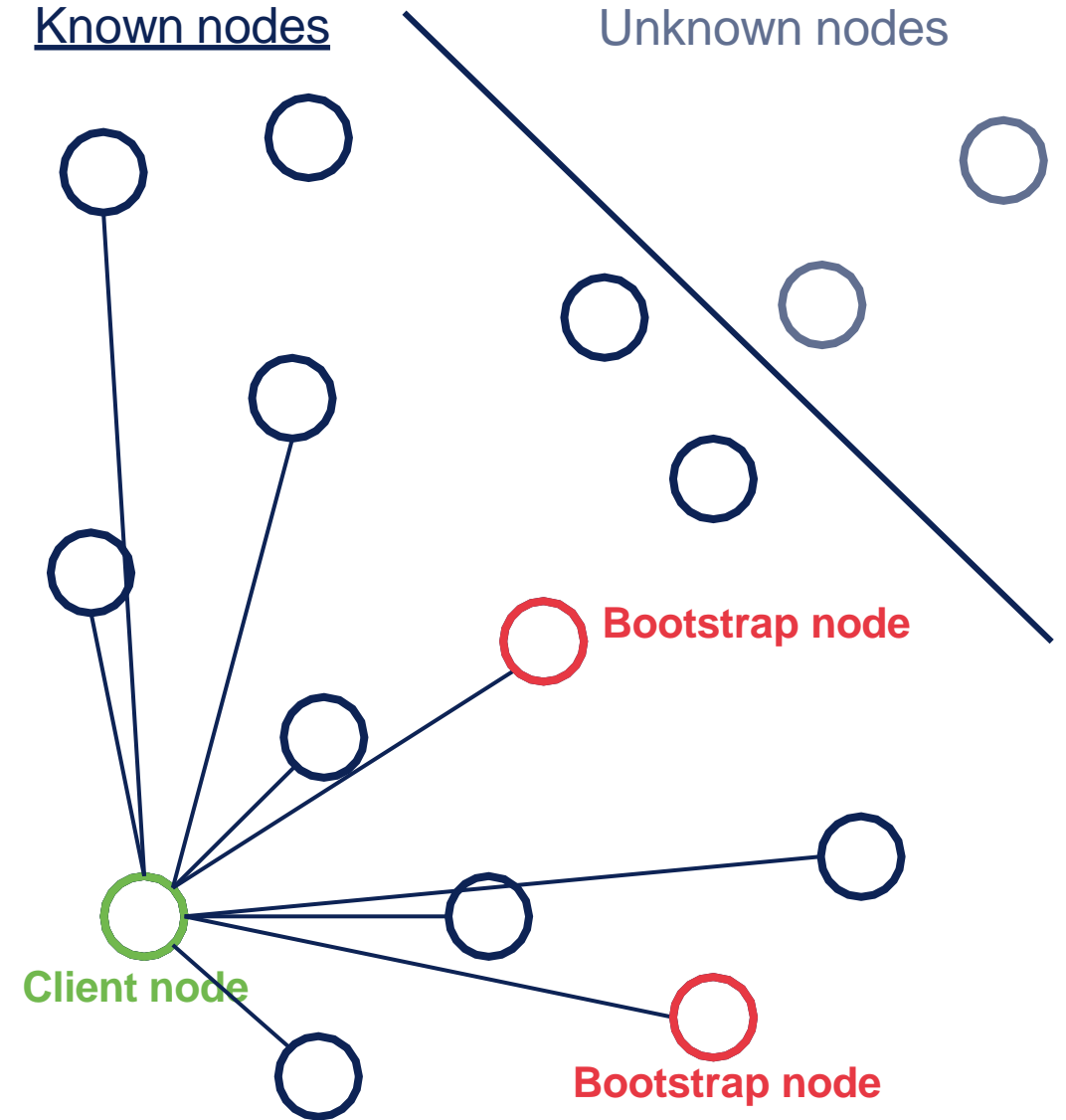


PREMIÈRE ÉTAPE : TROUVEZ VOS AMIS

Pour pouvoir faire quoi que ce soit sur la blockchain, vous devez d'abord.....

Découvrez le réseau blockchain !

1. Trouver des nœuds Bootstrap
2. Identifier des nœuds pairs



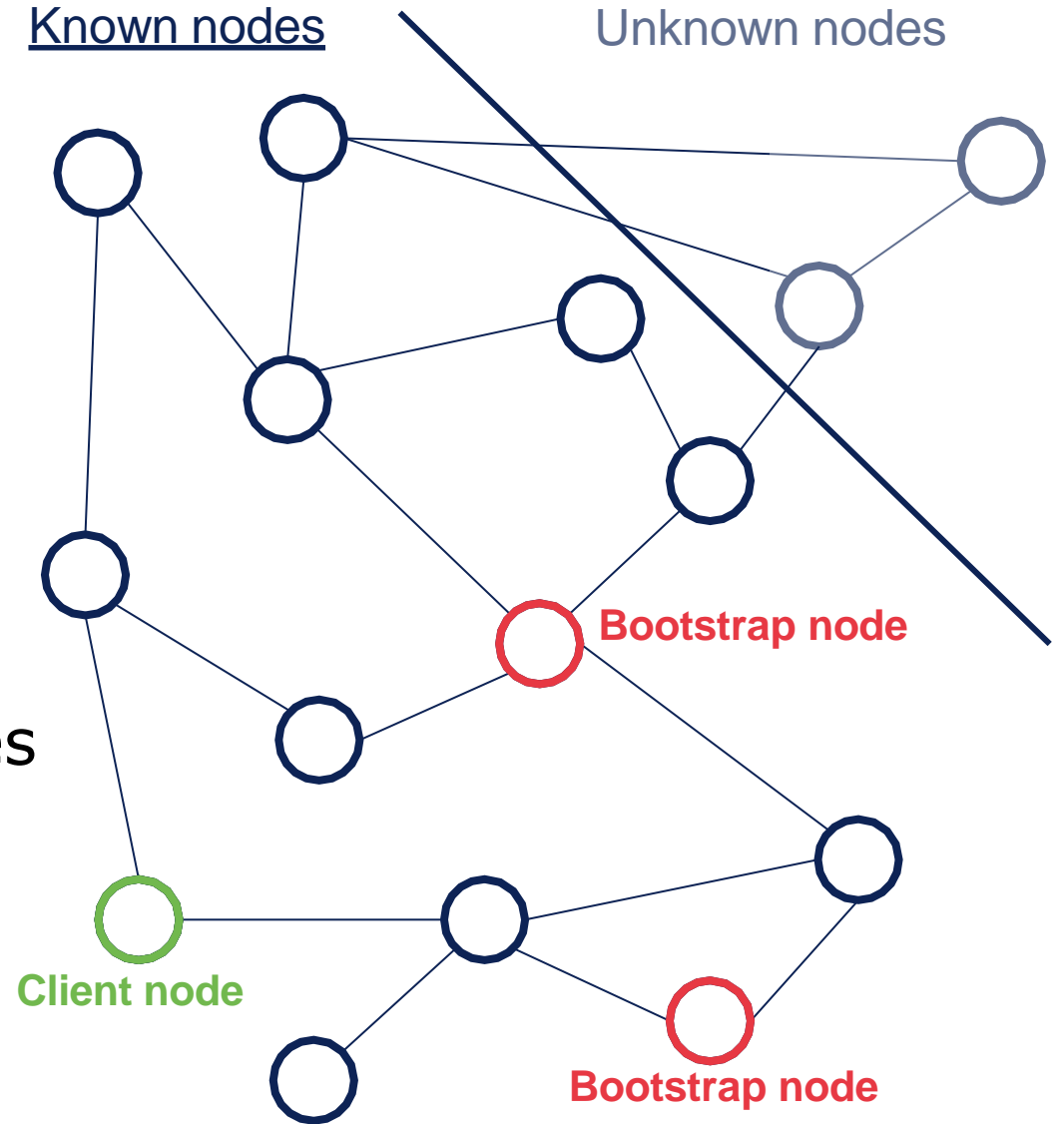
PREMIÈRE ÉTAPE : TROUVEZ VOS AMIS

Pour pouvoir faire quoi que ce soit sur la blockchain, vous devez d'abord...

Découvrez le réseau blockchain !

1. Trouver des nœuds Bootstrap
2. Identifier des nœuds pairs
3. Se connecter à des nœuds aléatoires

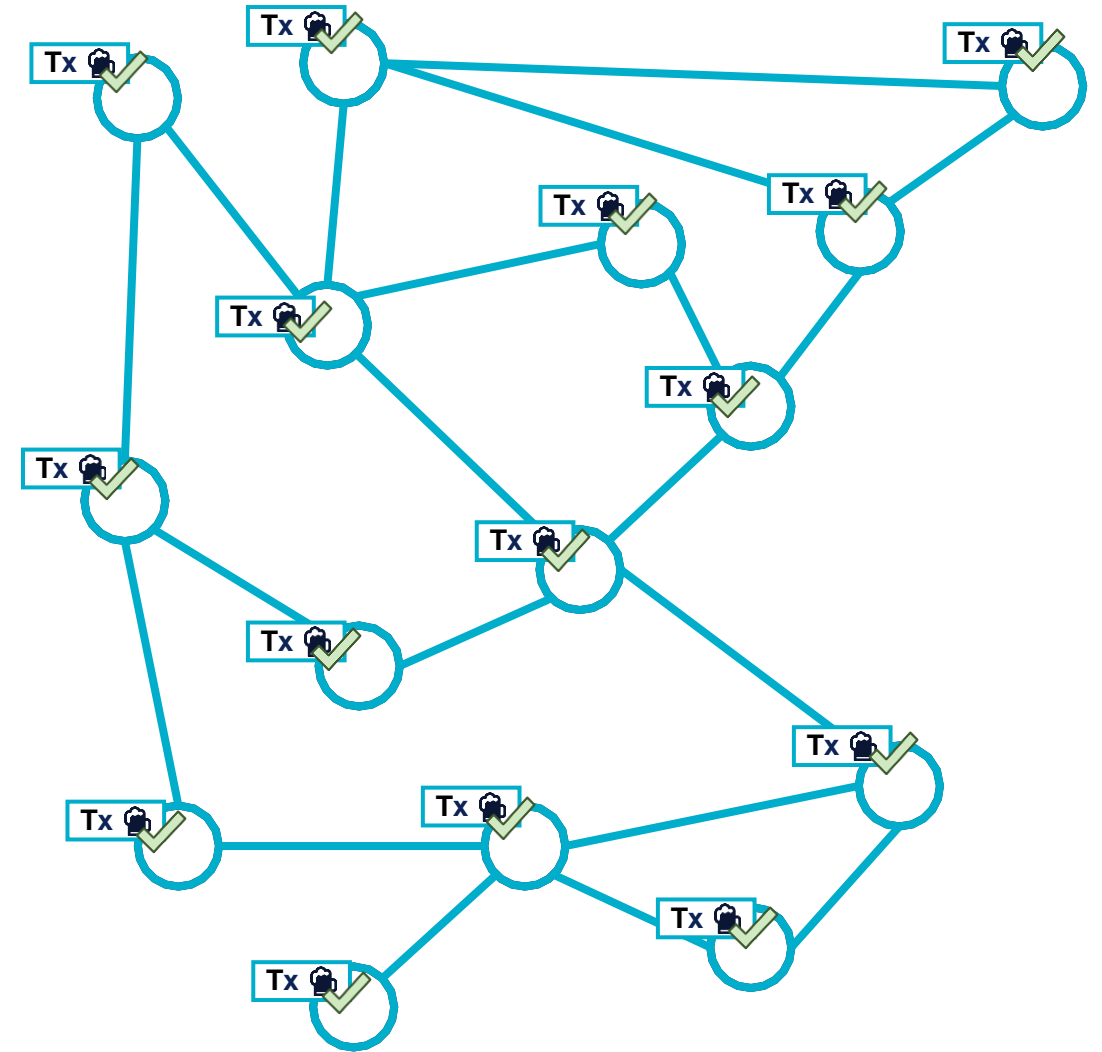
L'ensemble du réseau est finalement interconnecté



DEUXIÈME ÉTAPE : PARLEZ AVEC VOS AMIS

Principe

Transmettez simplement chaque transaction à vos voisins !



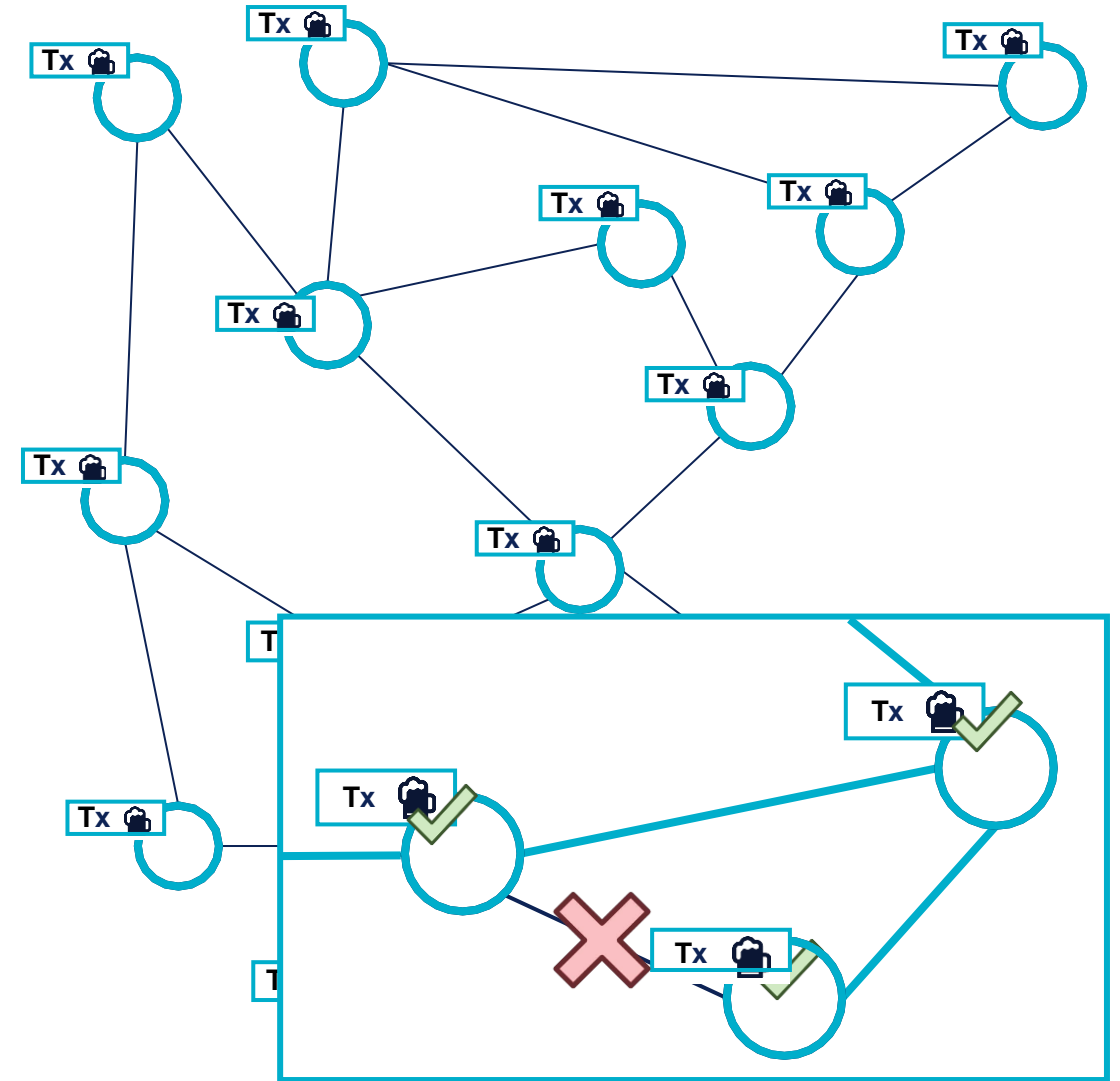
SECOND STEP: GOSSIP WITH YOUR FRIENDS

Principe

Transmettez simplement chaque transaction à vos voisins !

Pourquoi c'est cool ?

Fiable en cas de panne



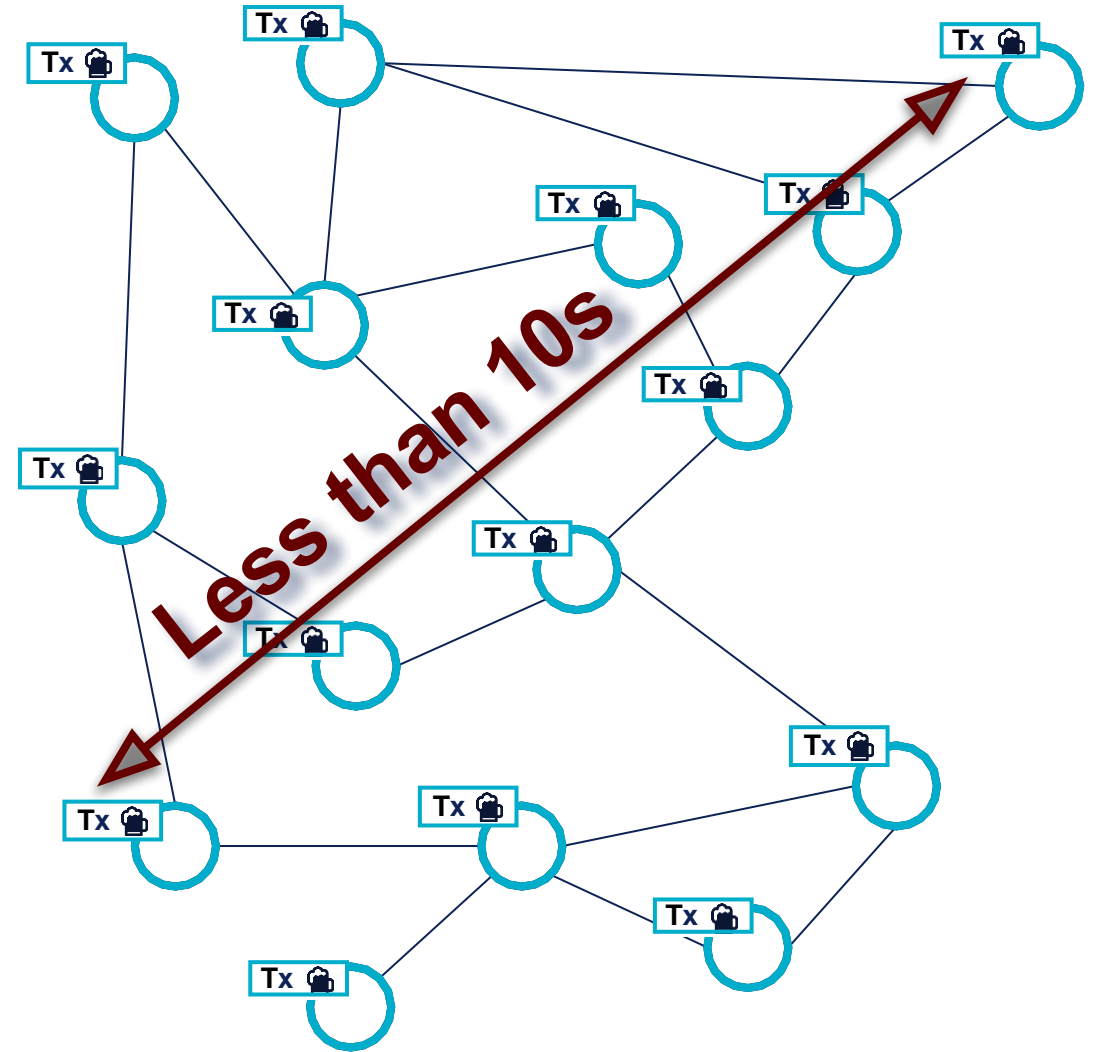
DEUXIÈME ÉTAPE : PARLEZ AVEC VOS AMIS

Principe

Transmettez simplement chaque transaction à vos voisins !

Pourquoi c'est intéressant ?

- **Fiable en** cas de panne
- **Livraison garantie** dans un délai limité



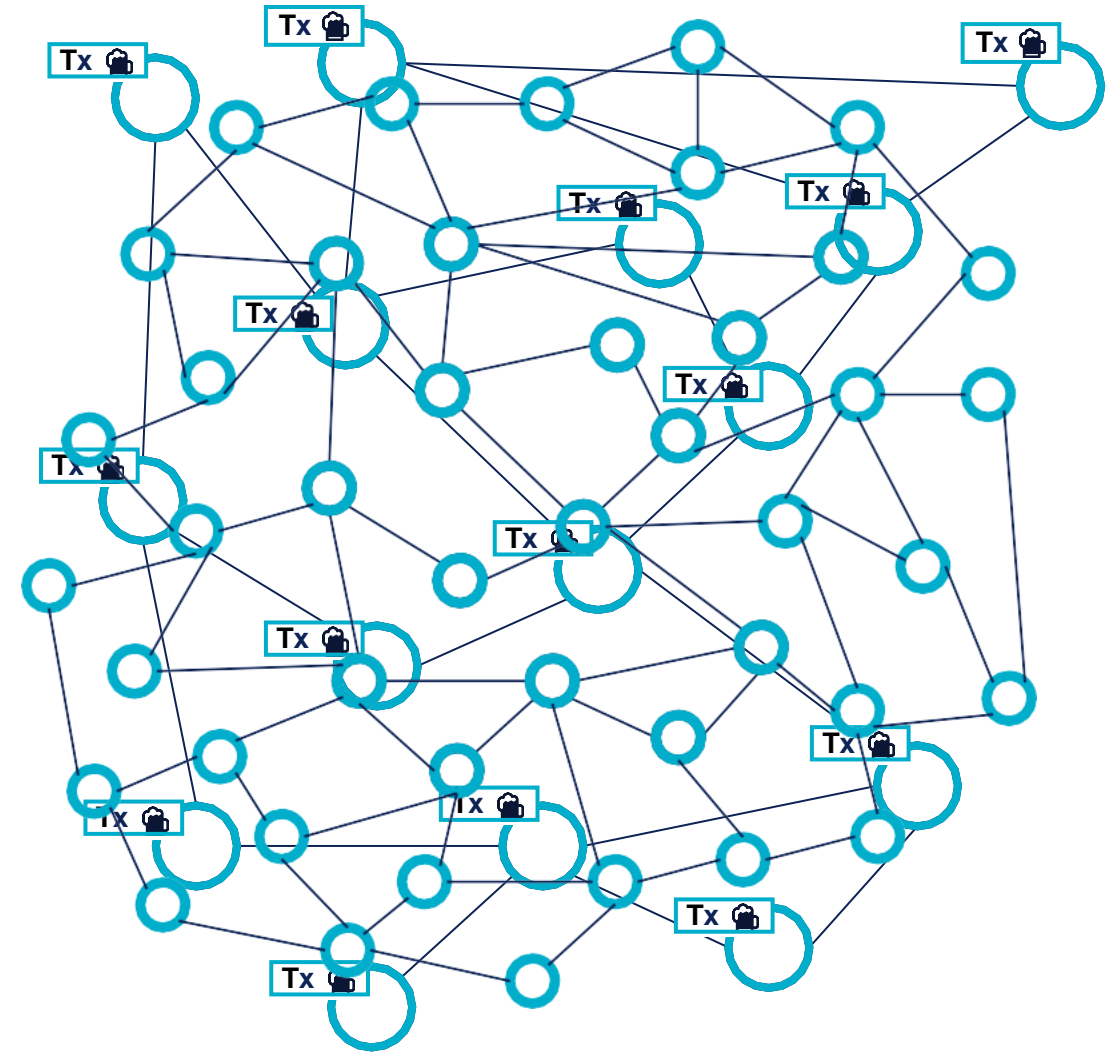
DEUXIÈME ÉTAPE : PARLEZ AVEC VOS AMIS

Principe

Transmettez simplement chaque transaction à vos voisins !

Pourquoi c'est intéressant ?

- **Fiable en** cas de panne
- **Livraison garantie dans un délai limité**
- **Échelle** avec le nombre de pairs




LES MAUVAISE TRANSACTIONS NE PASSERONT PAS !

La validité de la transaction **est d'abord vérifiée** avant d'être acceptée et transférée

Il devrait y avoir un consensus **sur les règles de validation** parmi les clients

Les mises à jour des règles de validation **sont propagées via les mises à jour logicielles**

- 
- ☒ Valid transaction format.....
 - ☒ Valid transaction.... instructions used....
 - ☒ Valid signature from the author.....
 - ☒ Transaction integrity not tampered.....
 - ☒ Coins spent are available.....

ALLONS au Memory POOL!

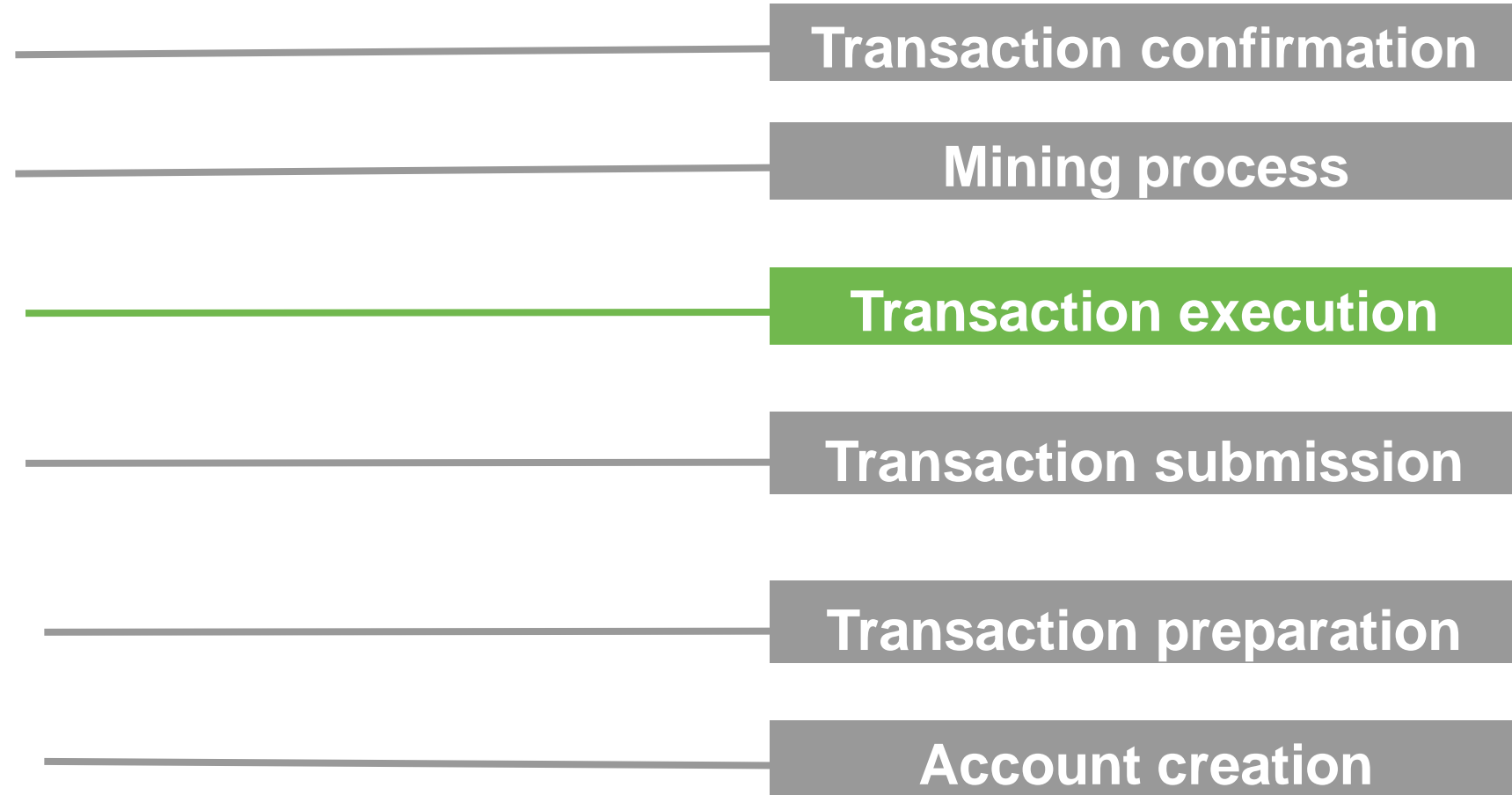
Les transactions acceptées sont placées dans **un pool de transactions géré indépendamment** par chaque nœud

Transaction Pool	Transactions	Frais	Classé par frais
	Payez-nous-un-café	30	
	Acheter Crypto Kitty	25	
	Acheter un jeton frauduleux ICO	12	
	Acheter des médicaments	7	
	Acheter un jeton frauduleux ICO	0	



Mining node A

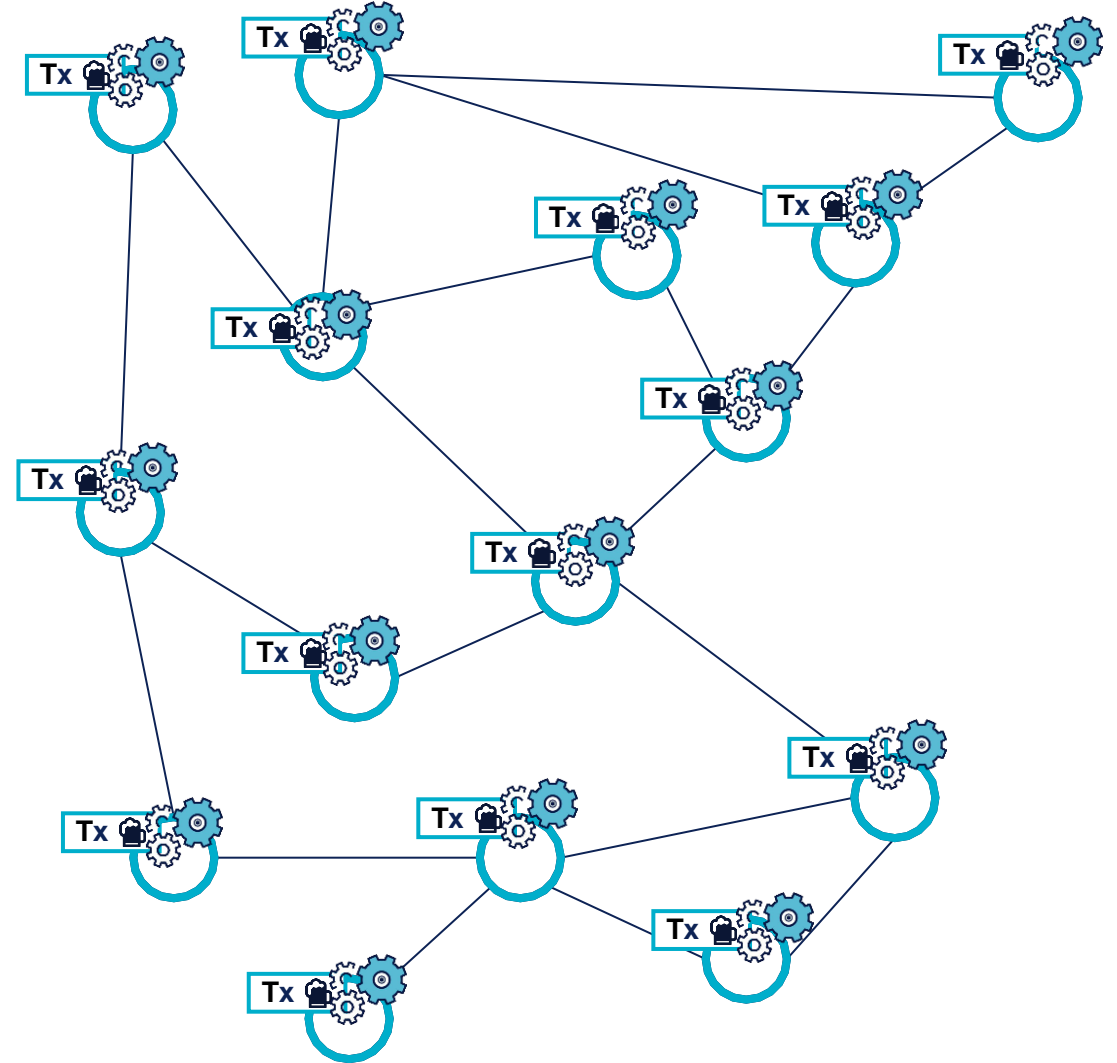
Cycle de vie d'une transaction : Mining process



Un modèle peu SCALABLE

Tous les nœuds
exécutent toutes
les transactions

L'ajout de nouveaux
nœuds **n'augmente**
pas la puissance de
calcul



PROTECTIONS CONTRE LE MAL

Menace 1

Boucle infinie dans les scripts de transaction

Solution



Pas de boucle ou de Goto dans le langage de script



Payer pour chaque exécution **d'instruction**

Menace 2

Attaque par **relecture de transaction**

Solution

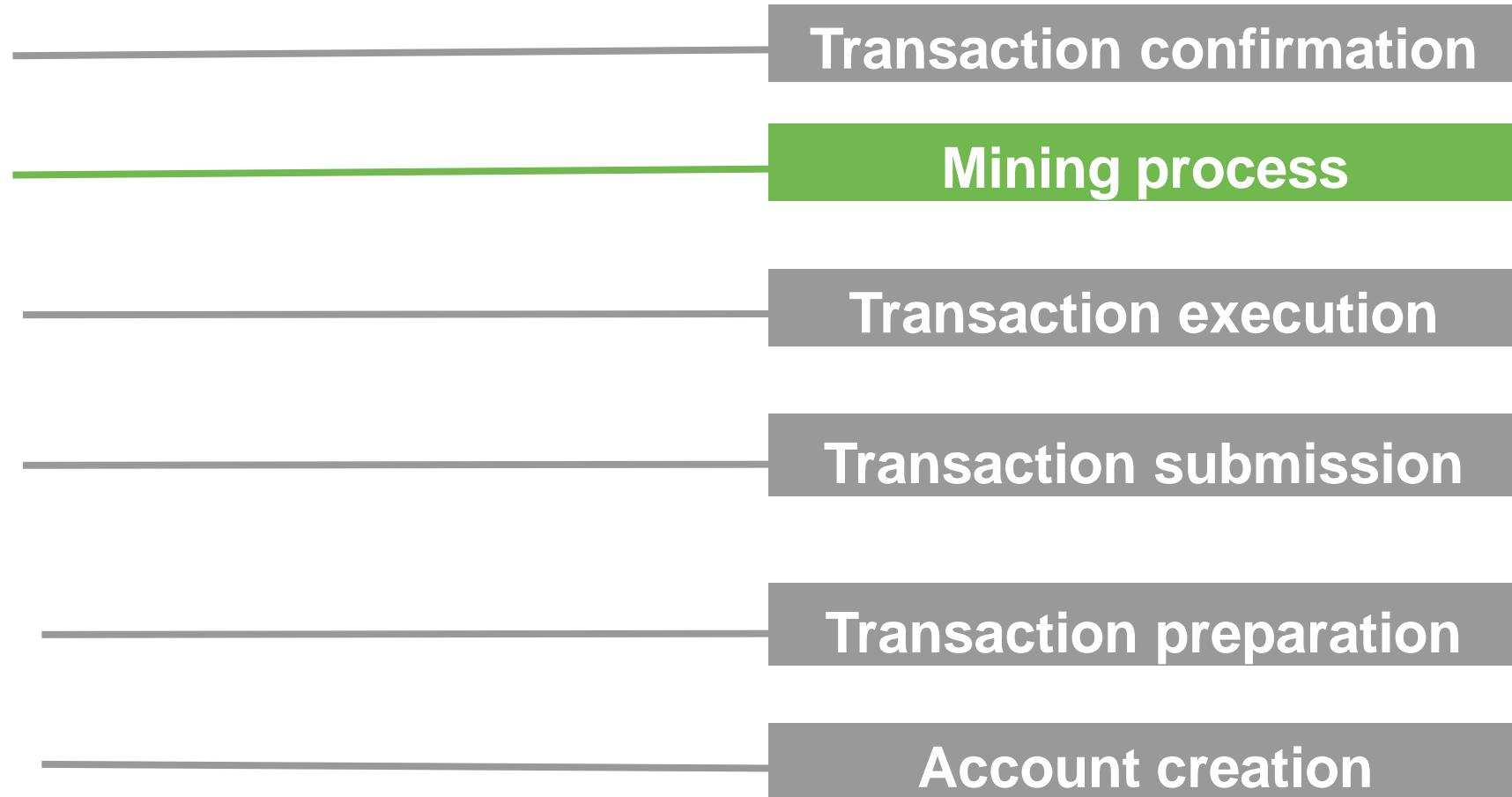


Enchaînement de transactions



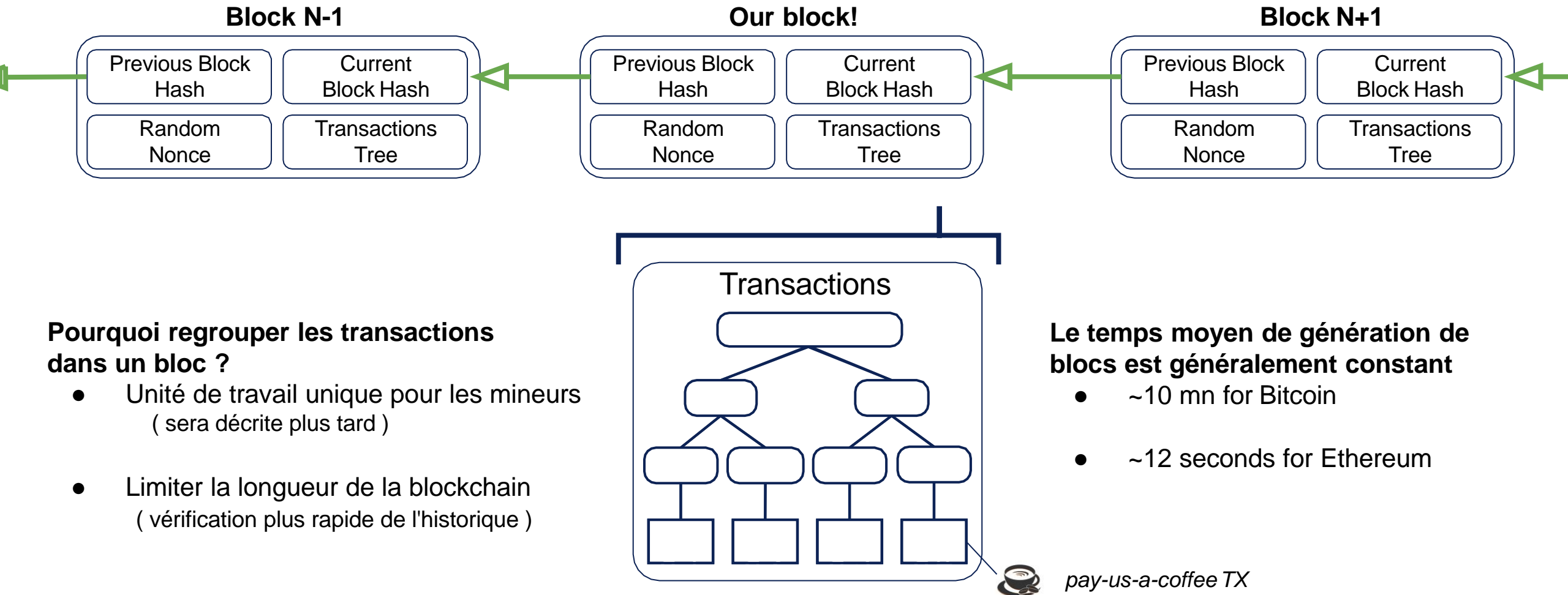
ID incrémentiel par transaction/compte

Cycle de vie d'une transaction : Propagation de bloc



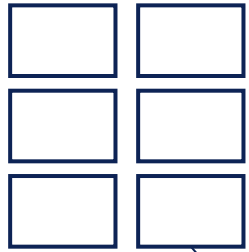
AVONS-NOUS DIT BLOCKCHAIN ? QU'EST-CE QUE C'EST ?

Maintenant que notre transaction « payez-nous-une-café » est exécutée et validée, elle doit être **incluse** dans un **bloc nouvellement créé**

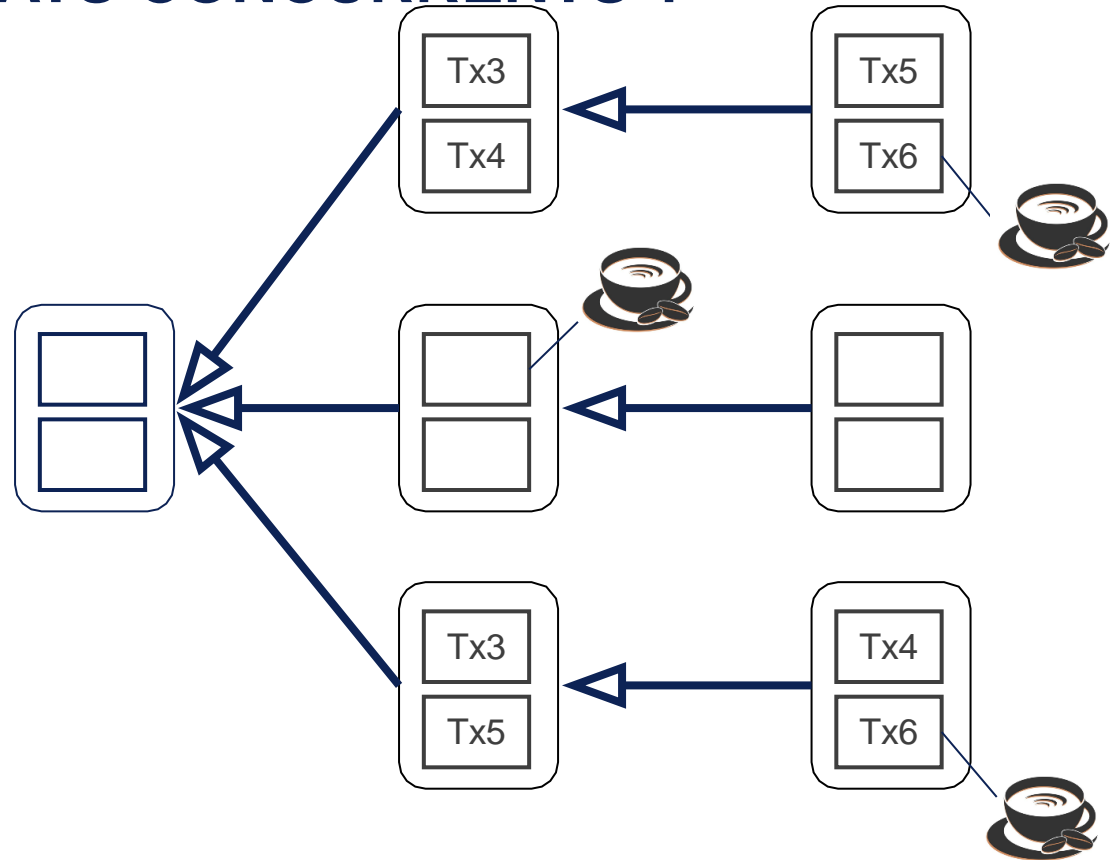


COMMENT RESOUDRE LES ETATS CONCURRENTS ?

Comment regrouper
les transactions en blocs



payez-nous-un-café TX



Processus distribué =
besoin d'arbitrer entre **plusieurs états valides**

Les attaques les plus connues

Attaque Sybil

fausse multitude de nœuds utilisant des identités forgées

Double Dépense

dépenser deux fois le même argent

Types de censure des transactions

empêcher trnx d'être inclus dans la blockchain

ALGORITHME DE CONSENSUS

« Comment trouver la vérité dans un monde rempli de menteurs »

- **Convenir d'un état de blockchain unique** parmi toutes les possibilités valables
- **Empêcher les mauvais acteurs d'influencer le résultat**
- **Assurez-vous qu'un consensus sera finalement atteint** malgré les nœuds défectueux et malveillants



Solution = Mining!

2 réponses principales pour éviter ces attaques

- Choisissez au **hasard** le **prochain** producteur de blocs !
- Assurez-vous que **jouer** avec la blockchain **n'est pas gratuit**



LA PREUVE DE TRAVAIL, LA TECHNIQUE MINIÈRE LA PLUS COURANTE

Un défi informatique doit être relevé.

pour pouvoir créer un bloc valide

Challenge: **Trouver une valeur de hachage aléatoire** inférieure à un seuil (difficulté)

$\text{hash}(\text{block} + \text{random value}) < \text{difficulty}$

Bitcoin case
₿

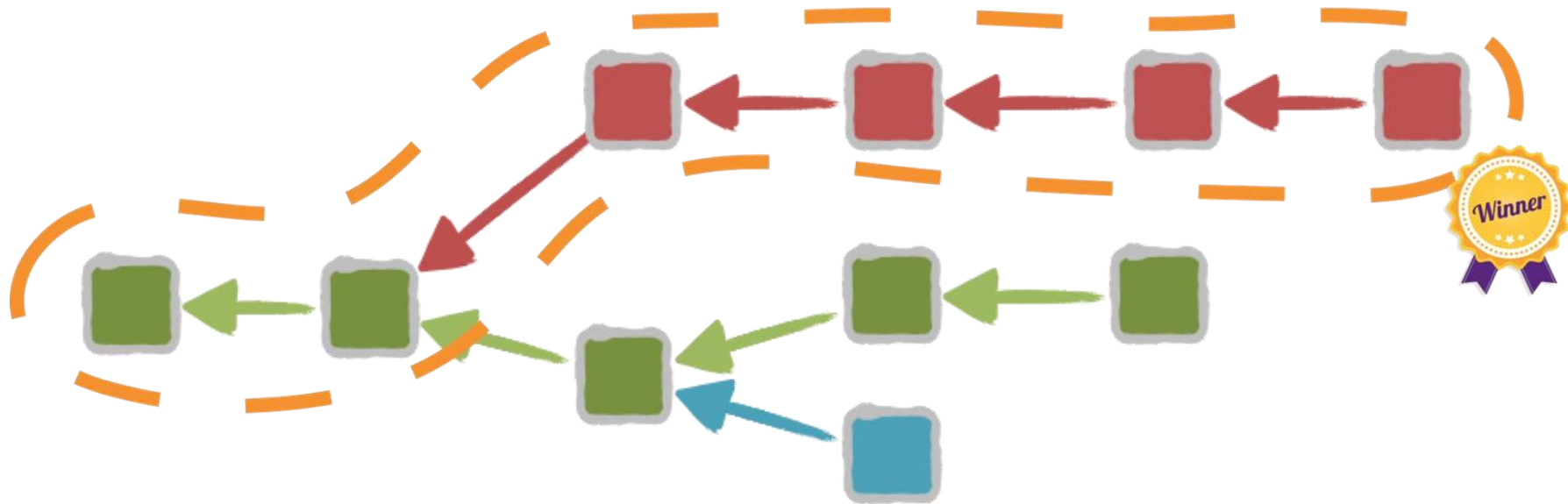
```
while block_hash > difficulty:  
    nonce = random_number()  
    block_hash = hash(concatenate(block, nonce))
```

La difficulté est régulièrement ajustée pour maintenir un temps moyen de génération de blocs constant

RÉSOLUTION DES FOURCHES (**FORKS**)

Que se passe-t-il lorsque 2 mineurs trouvent un bloc en même temps ?

The process continues and
The longest blockchains wins !



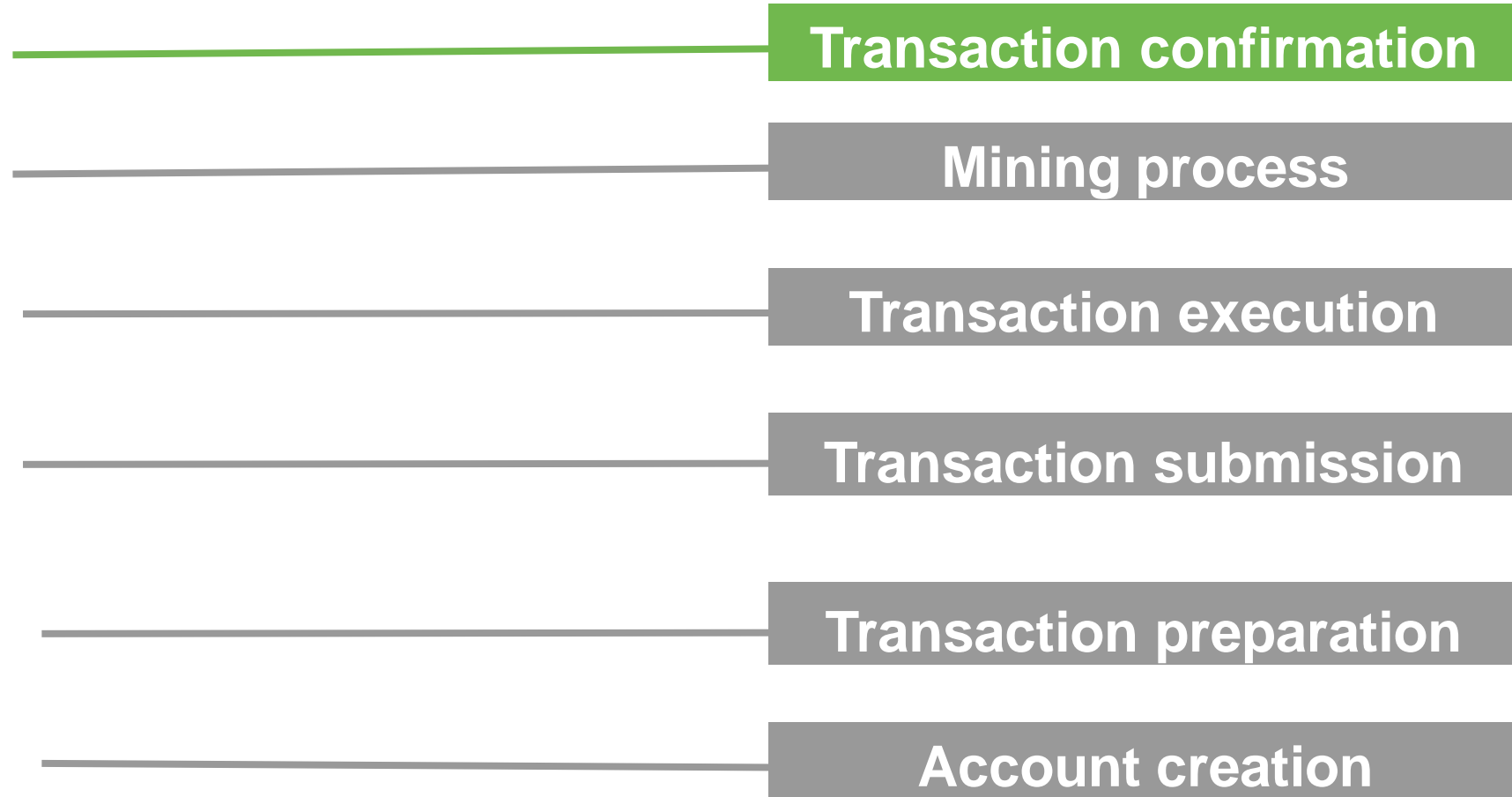
QUE FAIT UN MINEUR ?

1. **Collecter les transactions** du pool
2. **Validate** transactions
3. Investissez dans **le pouvoir et l'électricité !**
4. Essayez de **créer un nouveau bloc** comme décrit précédemment
5. Finalement, **obtenez des récompenses** sous forme de **nouveaux bitcoins créés**

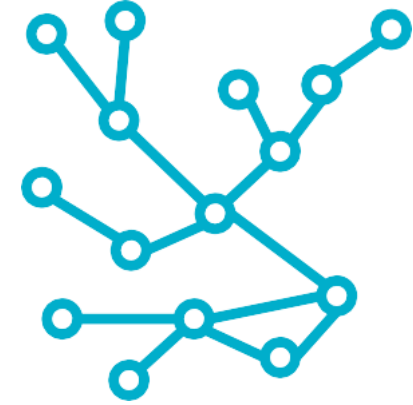


Cycle de vie d'une transaction :

Transaction confirmation



AVANT : LA PROPAGATION DE BLOCS (PAS SI SIMPLE)



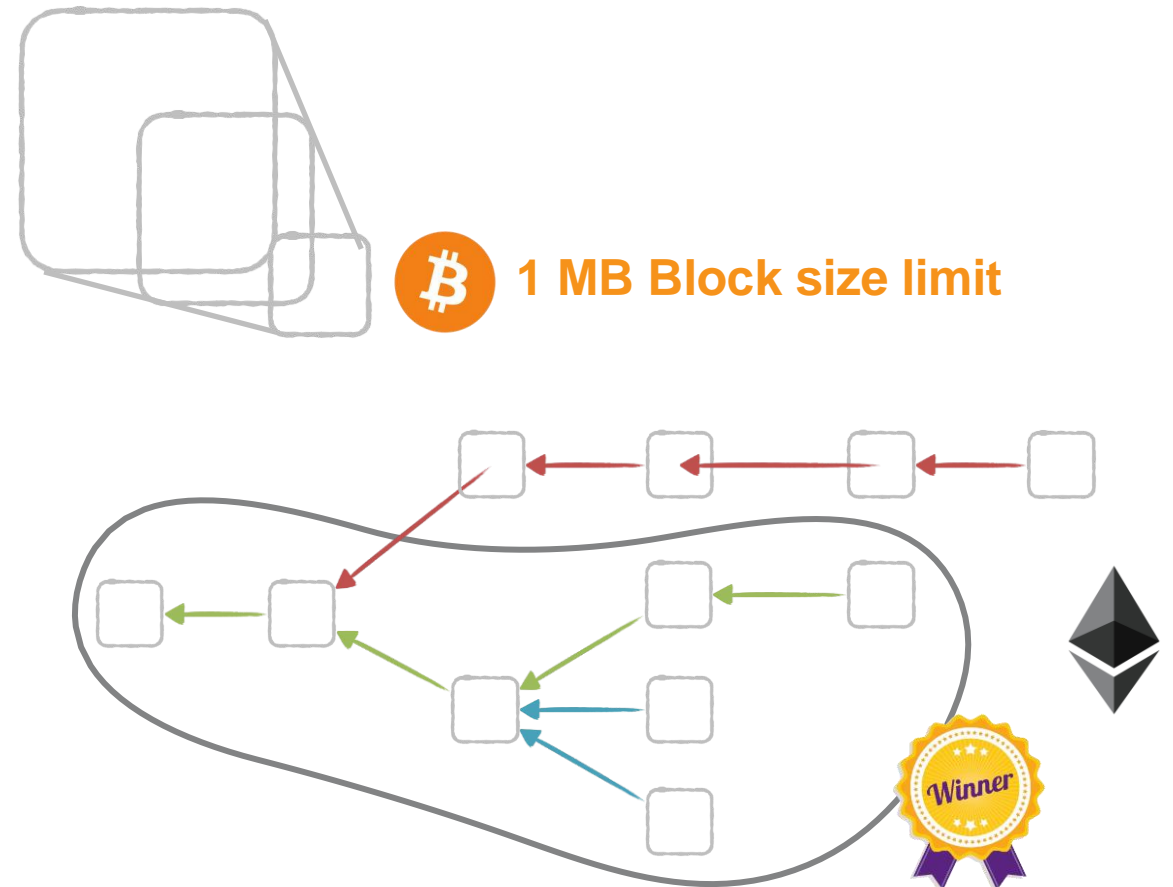
- Comme les transactions, les blocs sont **propagés** dans le réseau à l'aide du **protocole Gossip**
- Sur Bitcoin **50%** des blocs sont propagés en moins de 6 secondes

Problème: Un temps de propagation élevé **est mauvais pour la sécurité**

High propagation time lead to **centralisation**

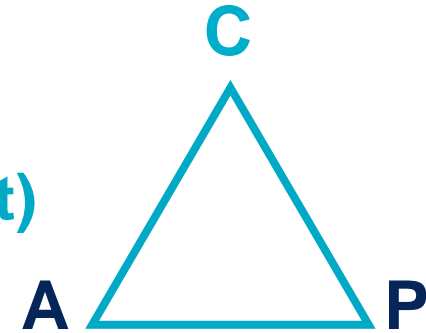
Solutions:

- **Low block size** and **high block time**

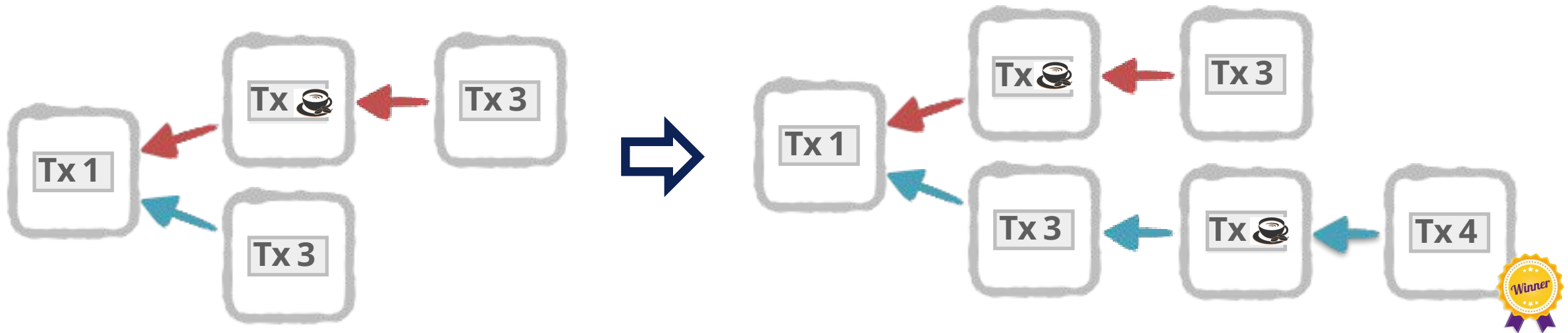


LE PROBLÈME DE LA CONFIRMATION DE TRANSACTION

- **Problème** : les blockchains **finissent par être cohérentes (consistent)**



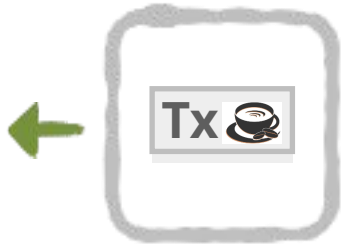
- **Les transactions peuvent être réorganisées à court terme dans** le cadre de la résolution des forks



The **CAP** theorem says that a **distributed system** can deliver only two of three desired characteristics: **consistency, availability and partition tolerance**

COMMENT ÊTRE SÛR DE VOTRE TRANSACTION

Plus une transaction est ancienne moins il est probable qu'elle puisse être annulée

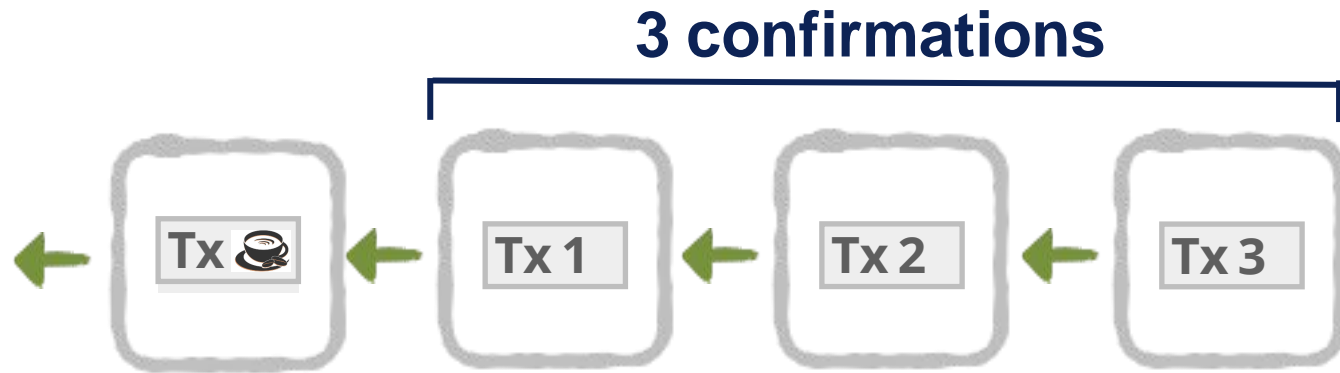


0 confirmation

Pas sûr que nous aurons votre café !

COMMENT ÊTRE SÛR DE VOTRE TRANSACTION

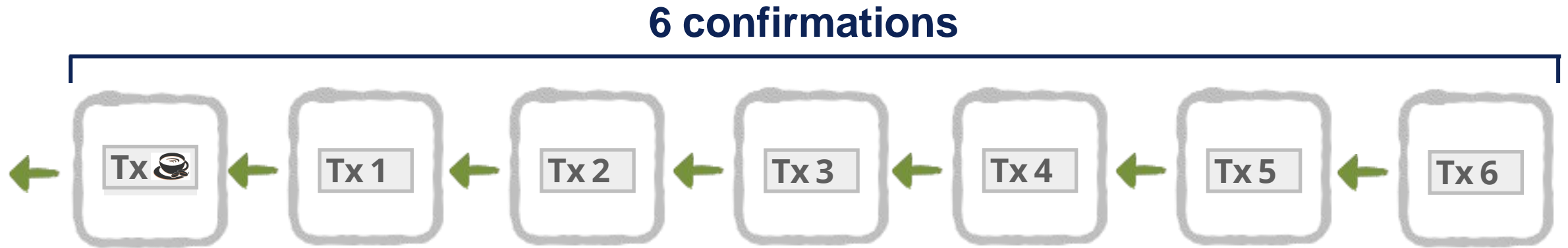
Plus une transaction est ancienne moins il est probable qu'elle puisse être annulée



Nous pouvons prendre notre café !

COMMENT ÊTRE SÛR DE VOTRE TRANSACTION

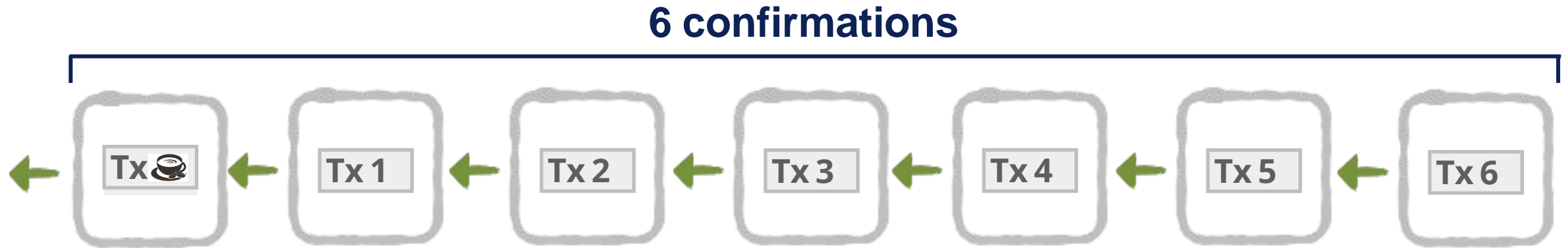
Plus une transaction est ancienne moins il est probable qu'elle puisse être annulée



Nous pouvons prendre notre café !

COMMENT ÊTRE SÛR DE VOTRE TRANSACTION

Plus une transaction est ancienne moins il est probable qu'elle puisse être annulée



6 blocks-old transactions are considered close to **100% safe**

Questions ?!!

