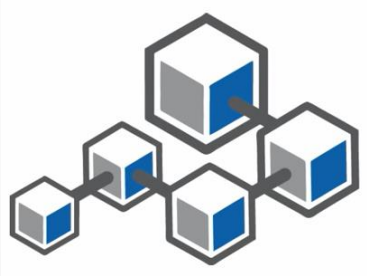
Cycle de vie d'une transaction Blockchain

Plongée en profondeur dans la blockchain

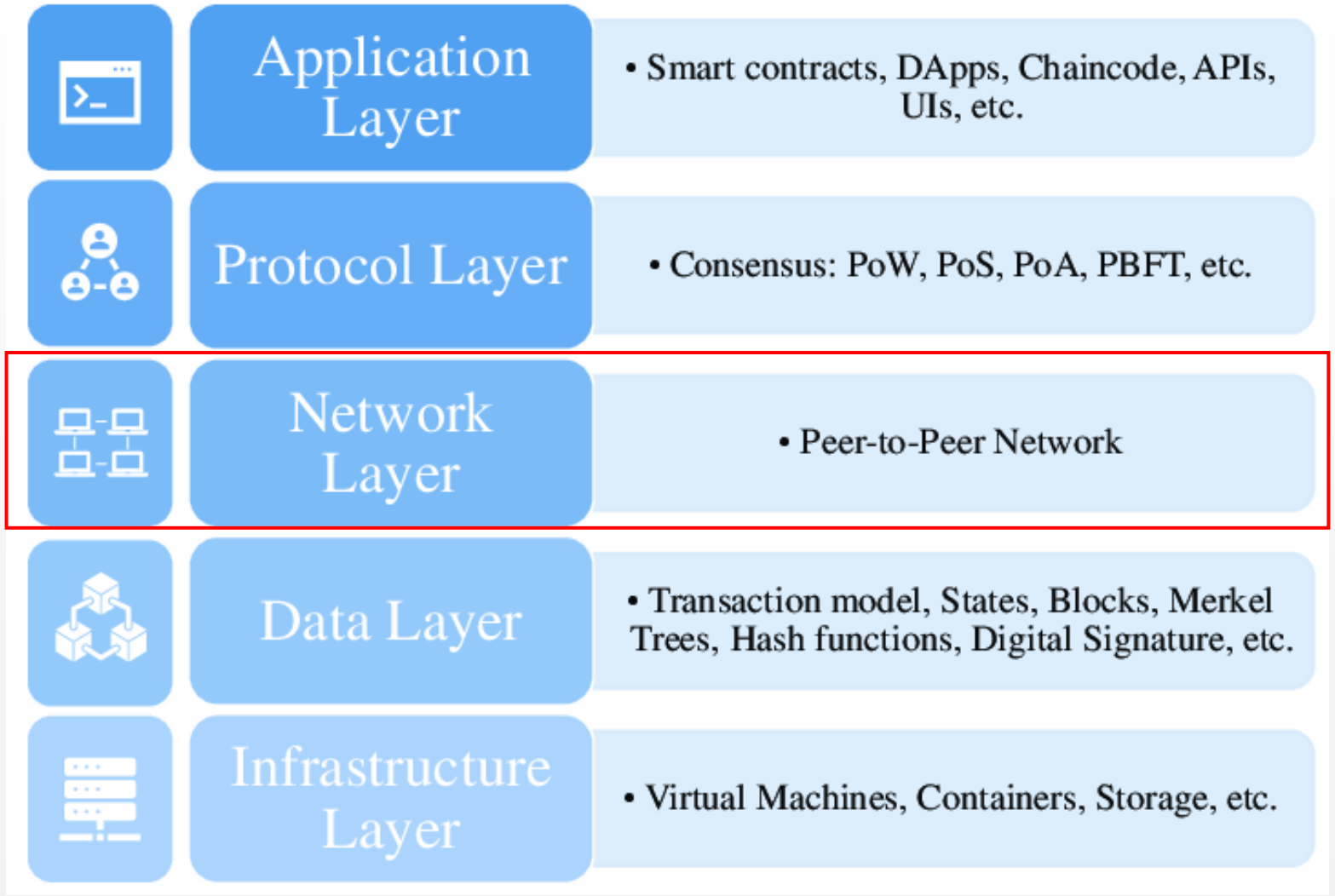


Abdelkader Ouared

abdelkader.ouared@univ-tiaret.dz

@ouared

Les couches de blockchain



Cycle de vie d'une transaction Blockchain

APERÇU DU CYCLE DE VIE

APERÇU DU CYCLE DE VIE

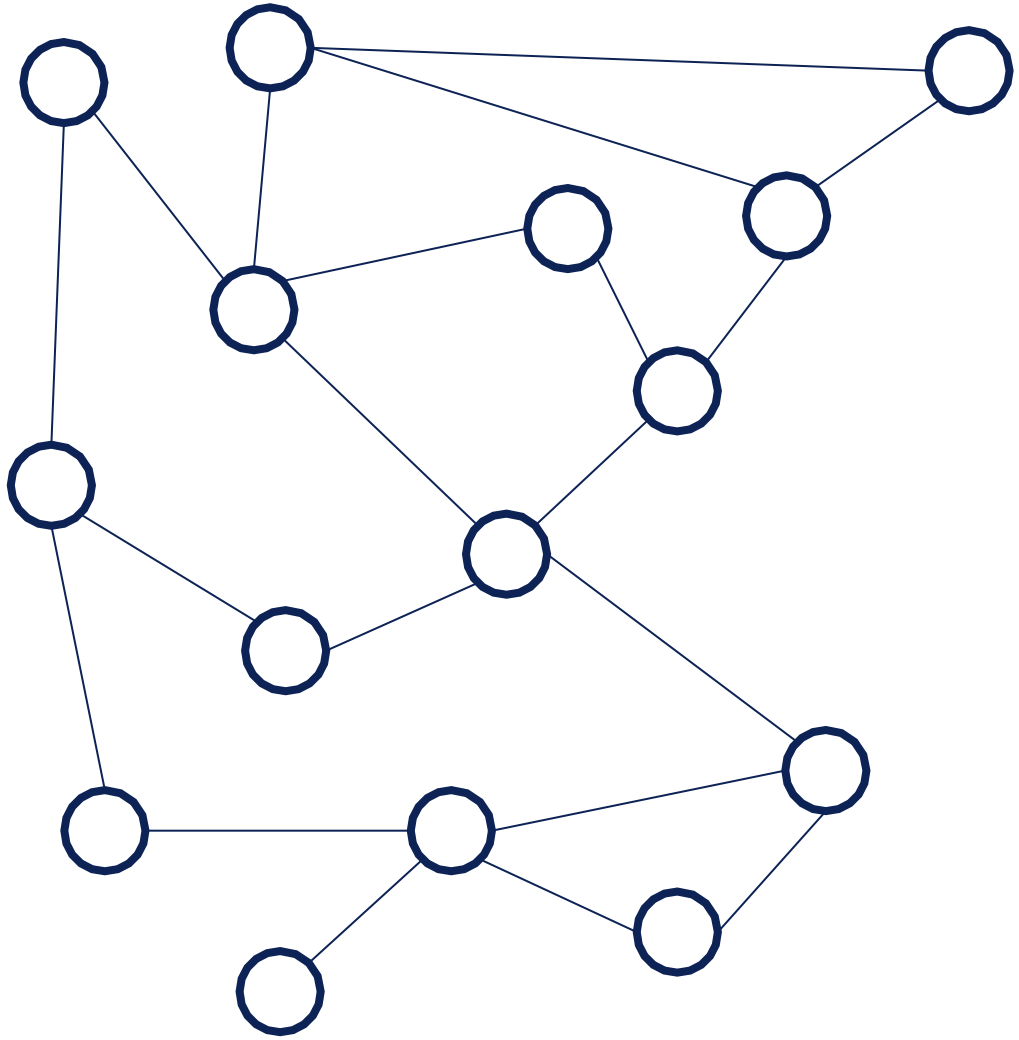
Création de Compte:

- 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.

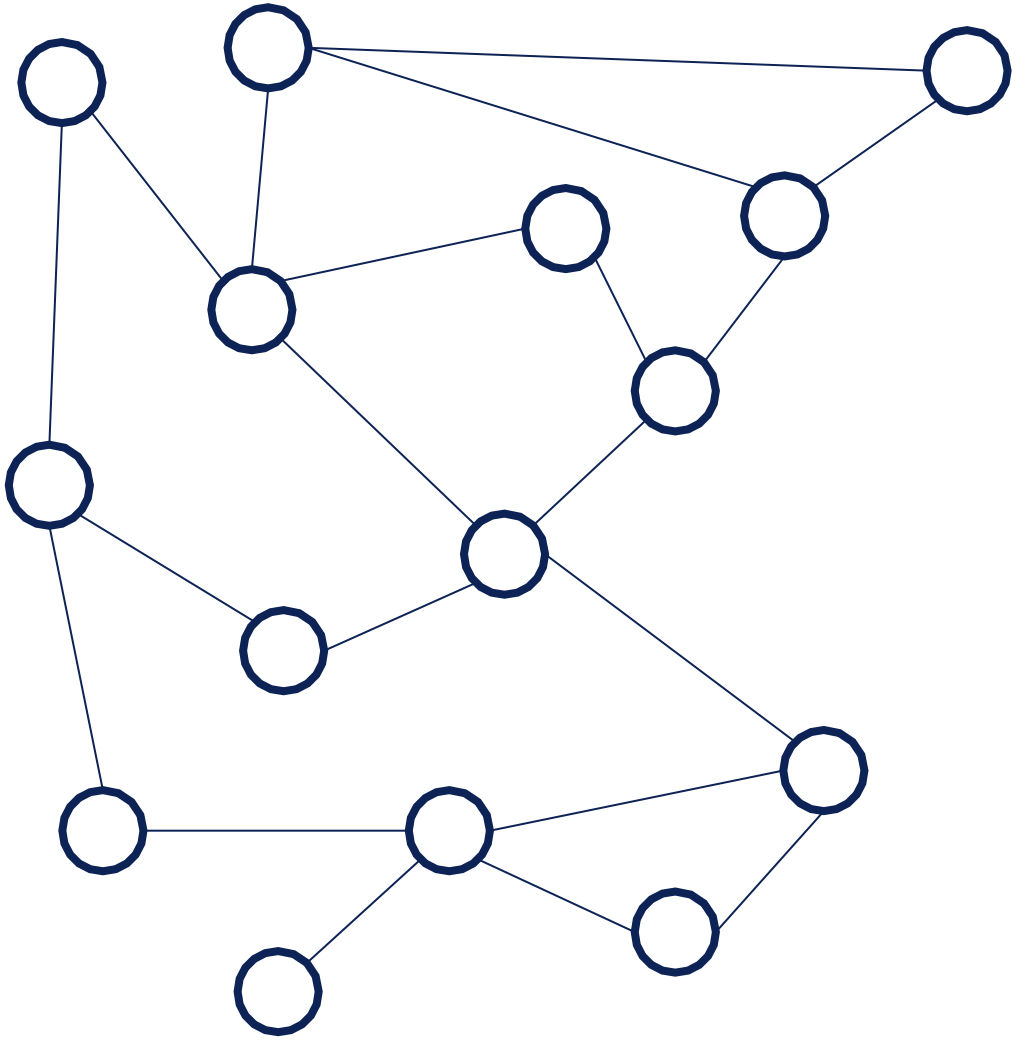


ACCOUNT CREATION

APERÇU DU CYCLE DE VIE

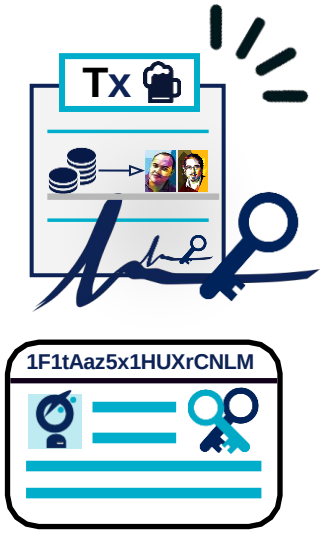
Préparation de la Transaction

- 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.

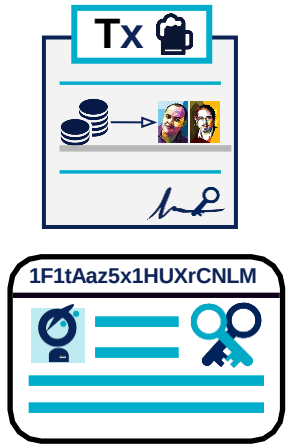
Solution

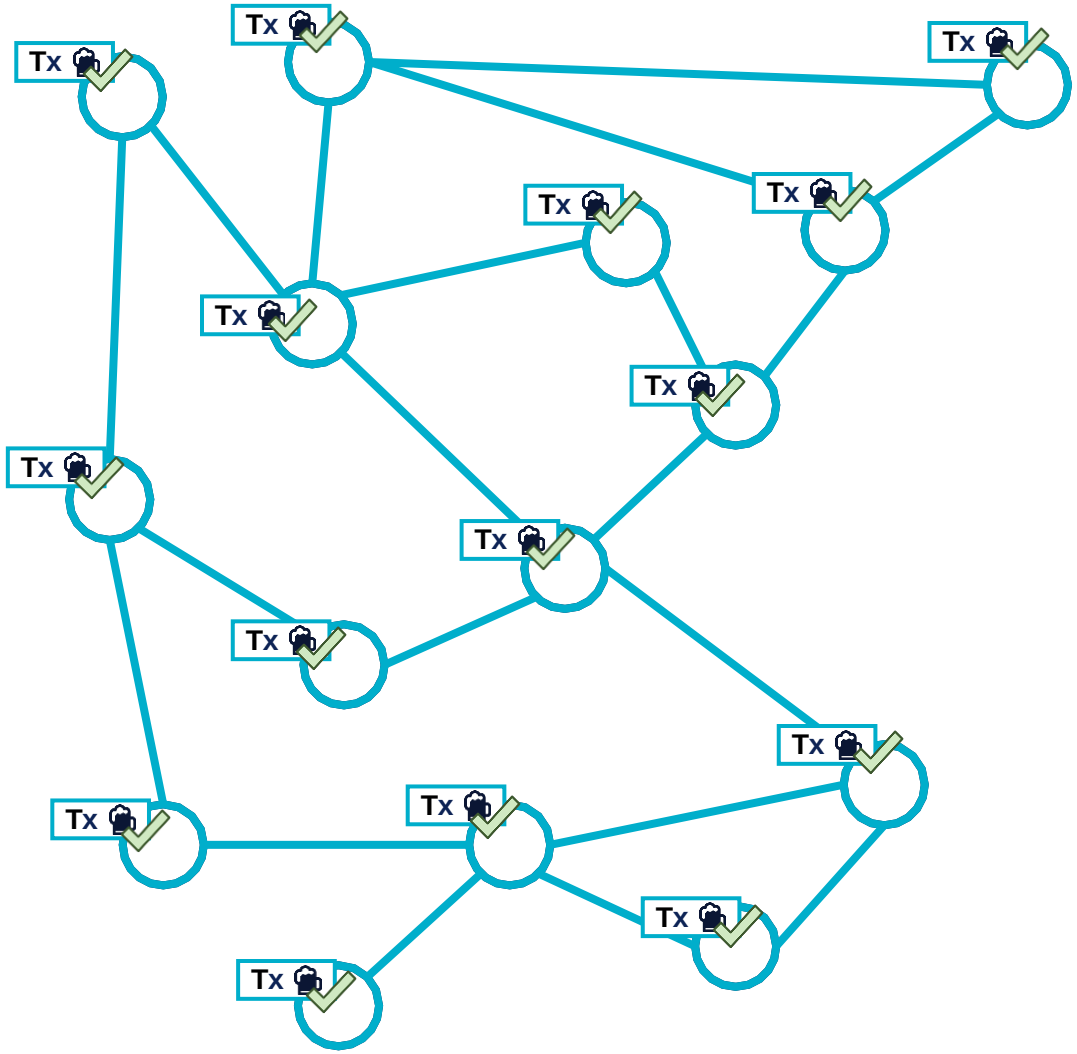
- **Signature numérique** : Utilisation de la clé privée pour prouver l'identité de l'expéditeur.
- **Envoi aux nœuds** : La transaction signée est vérifiée par des validateurs du réseau blockchain.

TRANSACTION SUBMISSION

TRANSACTION PREPARATION

ACCOUNT CREATION





APERÇU DU CYCLE DE VIE

Exécution de la Transaction

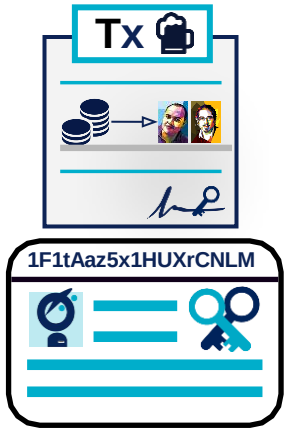
- La transaction est exécutée et validée sur la blockchain. Cela implique son ajout au registre distribué, qui est répliqué sur tous les nœuds du réseau.
- Les nœuds de la blockchain **vérifient** les détails de la transaction (validité de la signature, **montant suffisant**, etc.). Si tout est en ordre, 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.

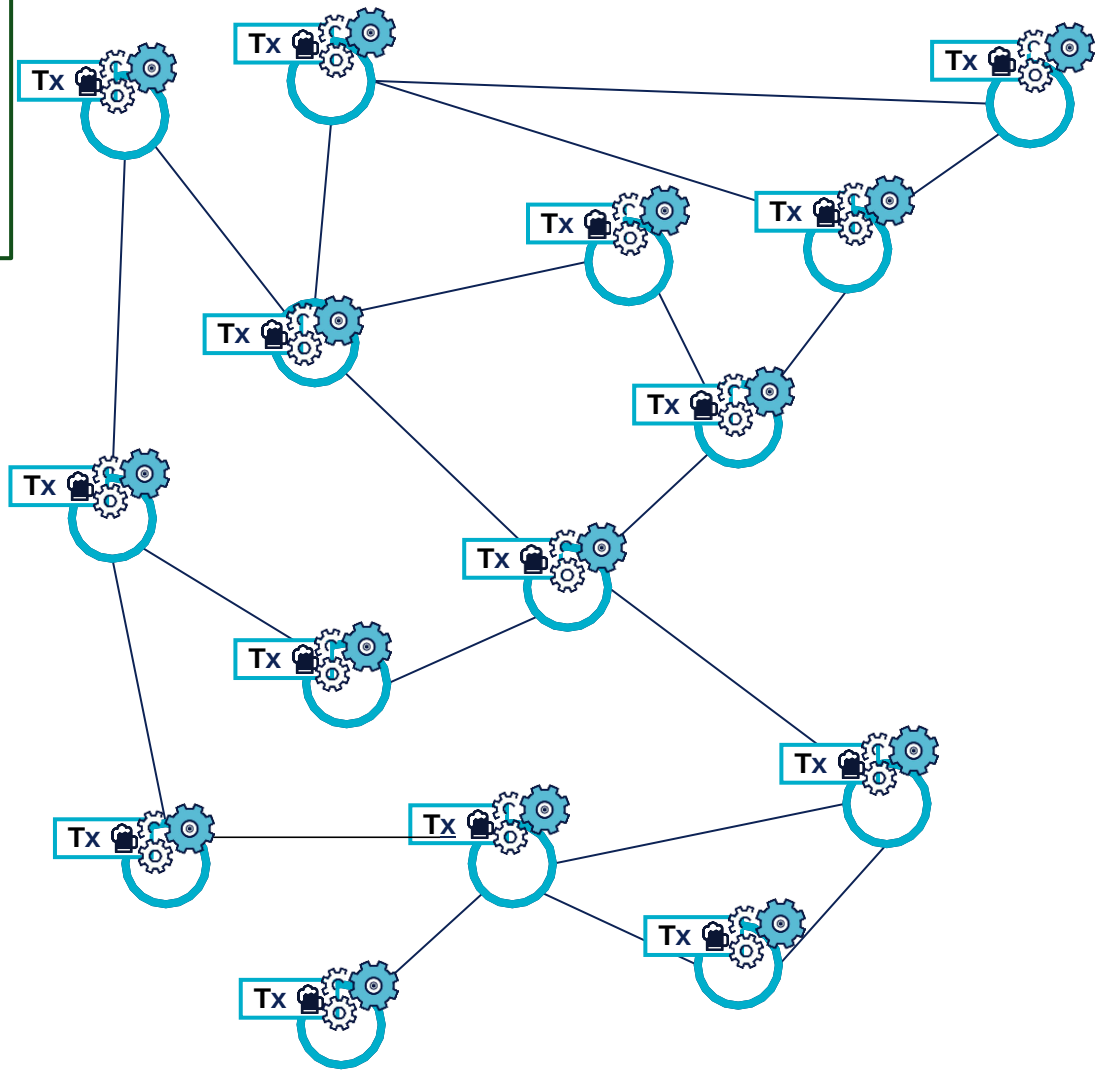
TRANSACTION EXECUTION

TRANSACTION SUBMISSION

TRANSACTION PREPARATION

ACCOUNT CREATION





APERÇU DU CYCLE DE VIE

Exécution de la Transaction

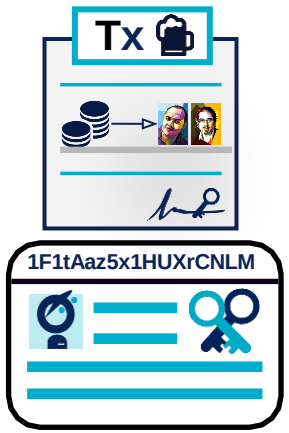
- La transaction est exécutée et validée sur la blockchain. Cela implique son ajout au registre distribué, qui est répliqué sur tous les nœuds du réseau.
- Les nœuds de la blockchain **vérifient** les détails de la transaction (validité de la signature, **montant suffisant**, etc.). Si tout est en ordre, 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.

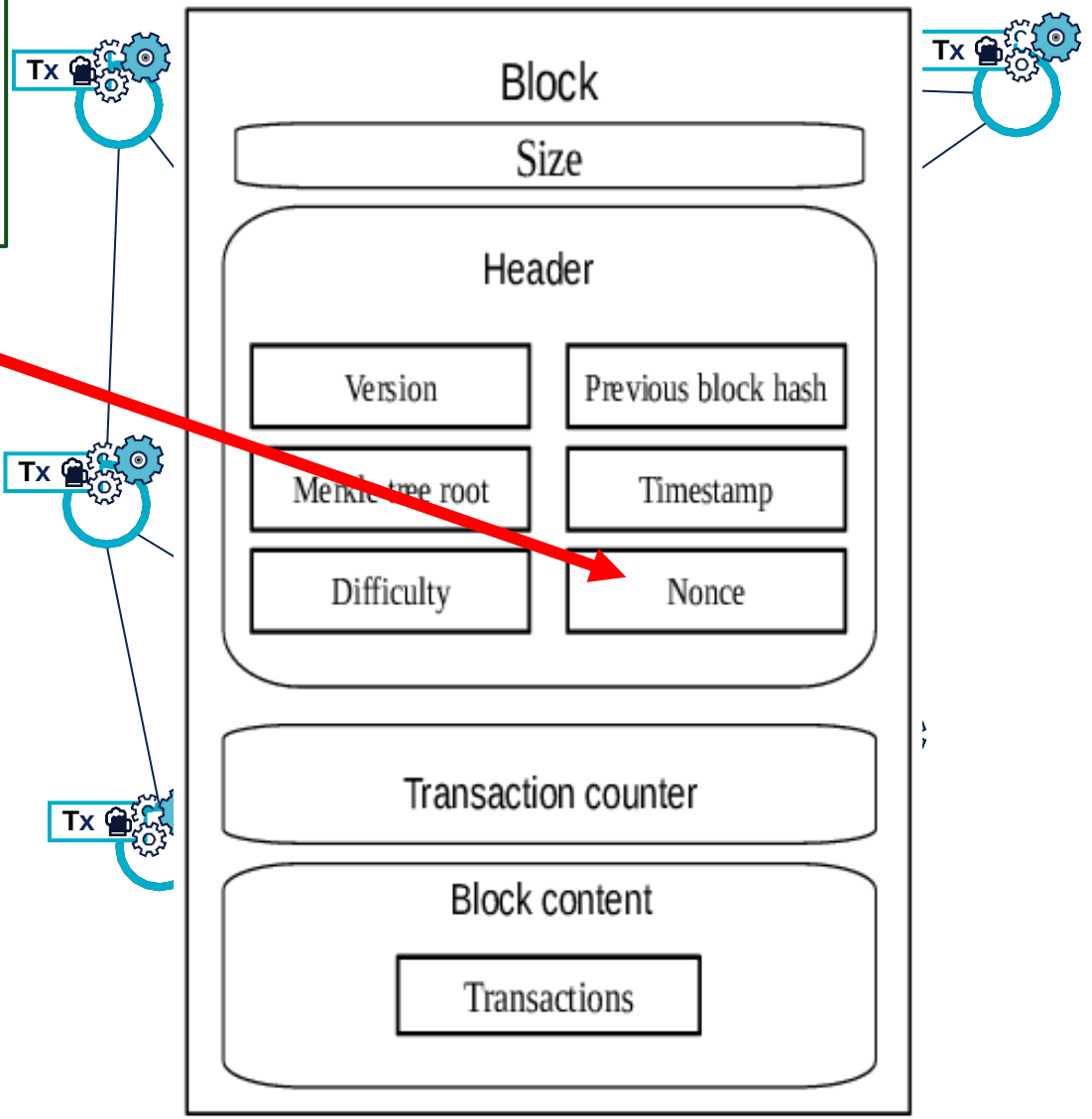
TRANSACTION EXECUTION

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.

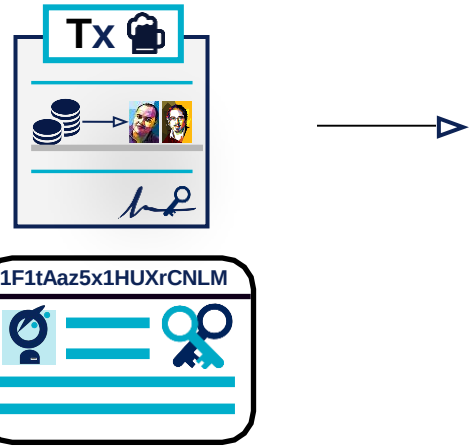
Mining Process

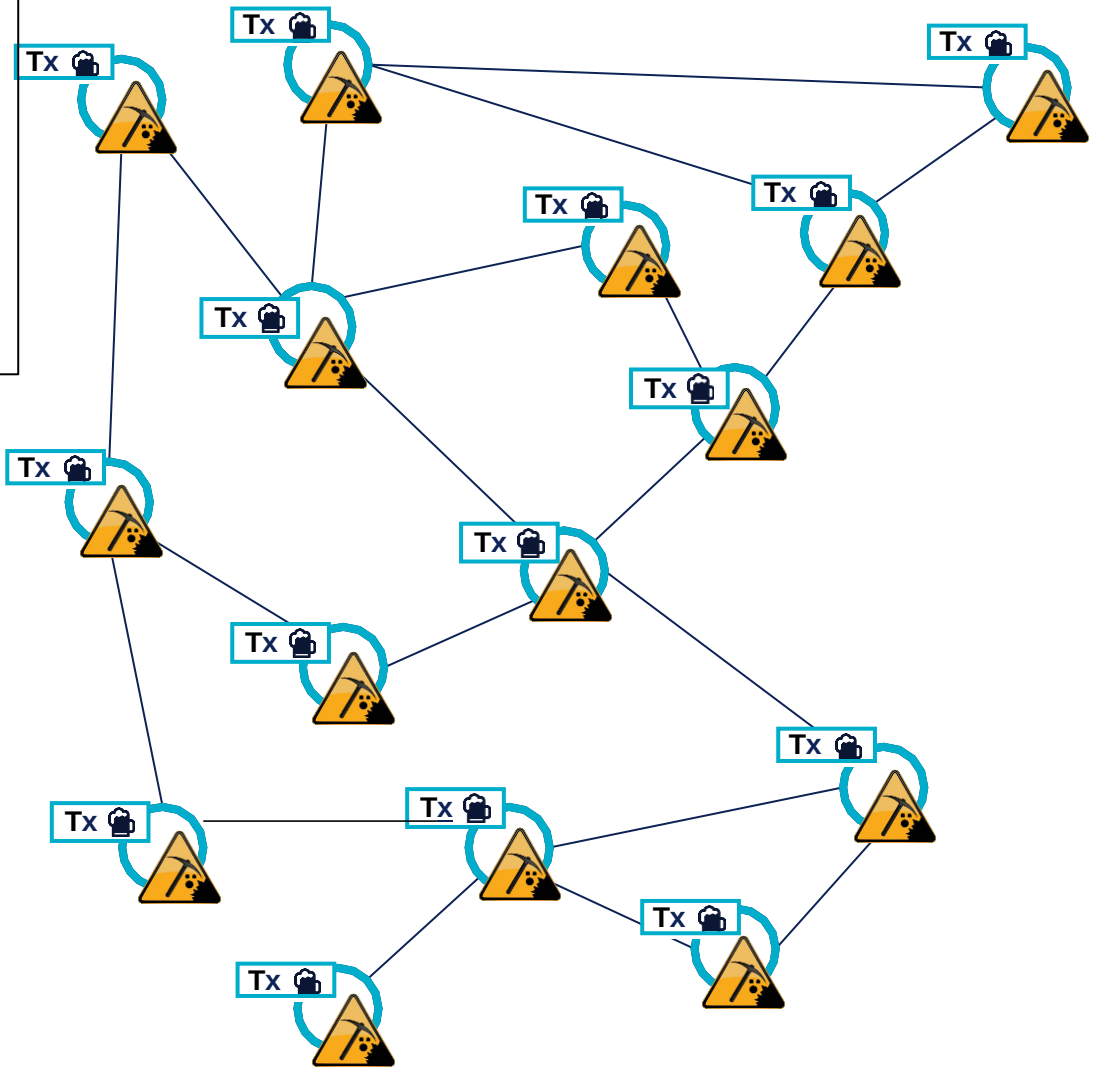
Transaction Execution

Transaction Submission

Transaction Preparation

Account Creation





APERÇU DU CYCLE DE VIE

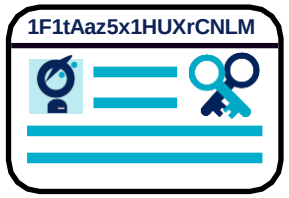
MINING PROCESS

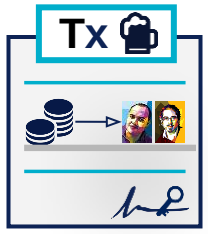
TRANSACTION EXECUTION

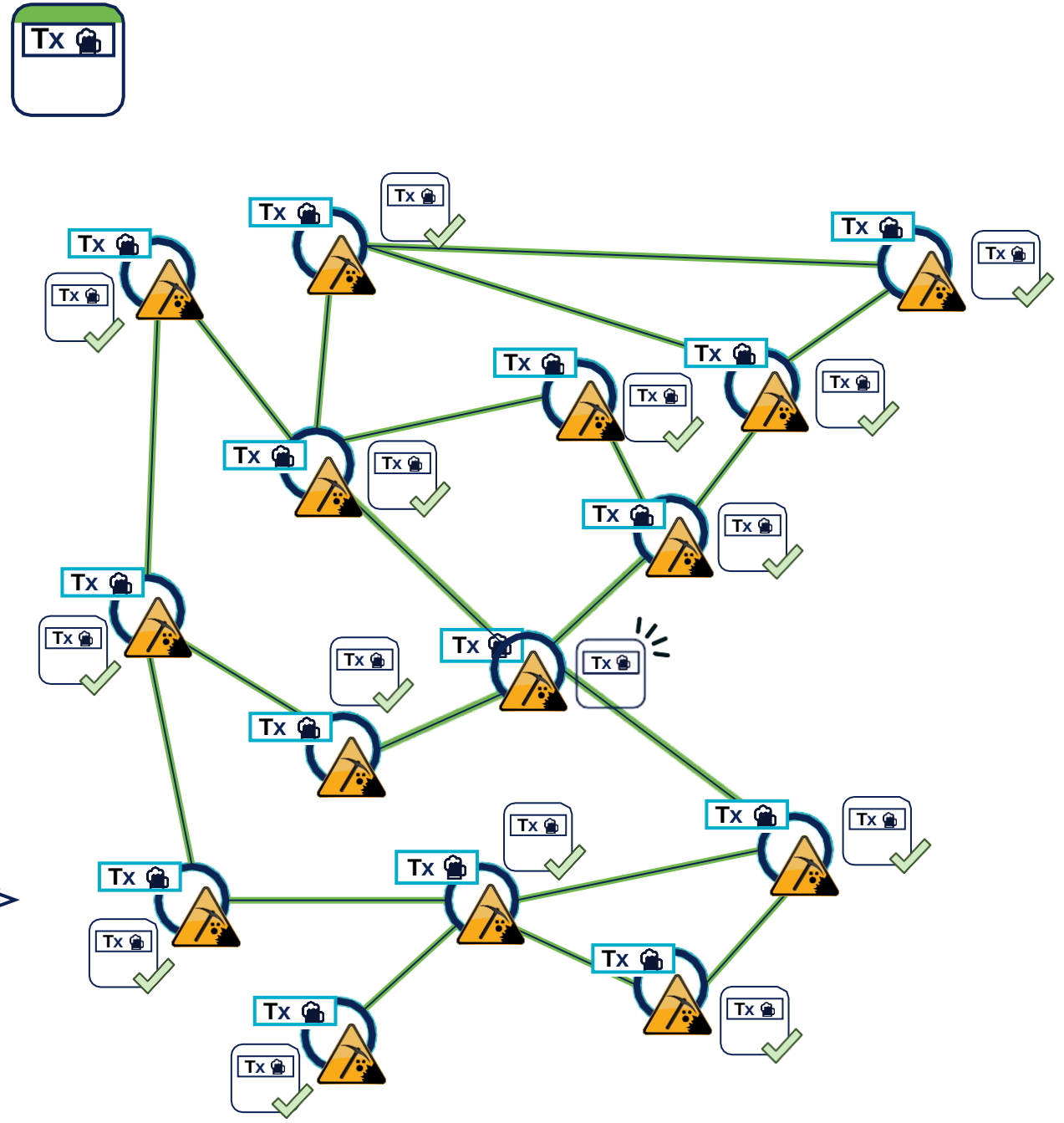
TRANSACTION SUBMISSION

TRANSACTION PREPARATION

ACCOUNT CREATION

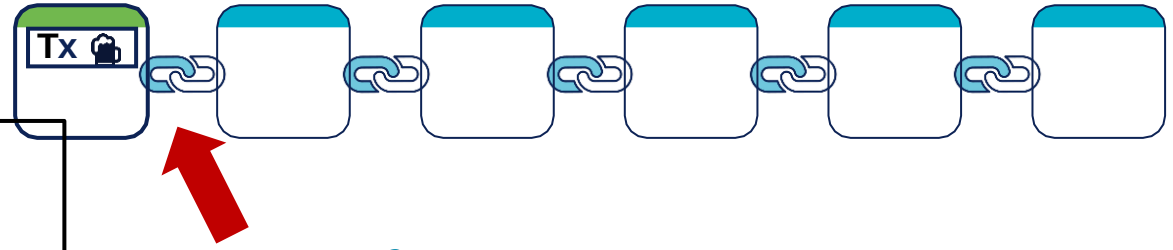






APERÇU DU CYCLE DE VIE

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

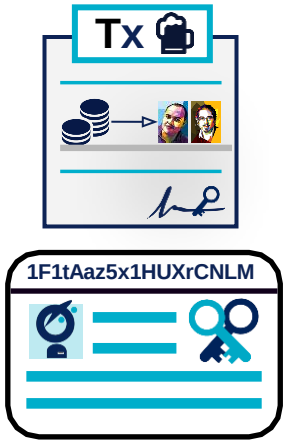
Mining Process

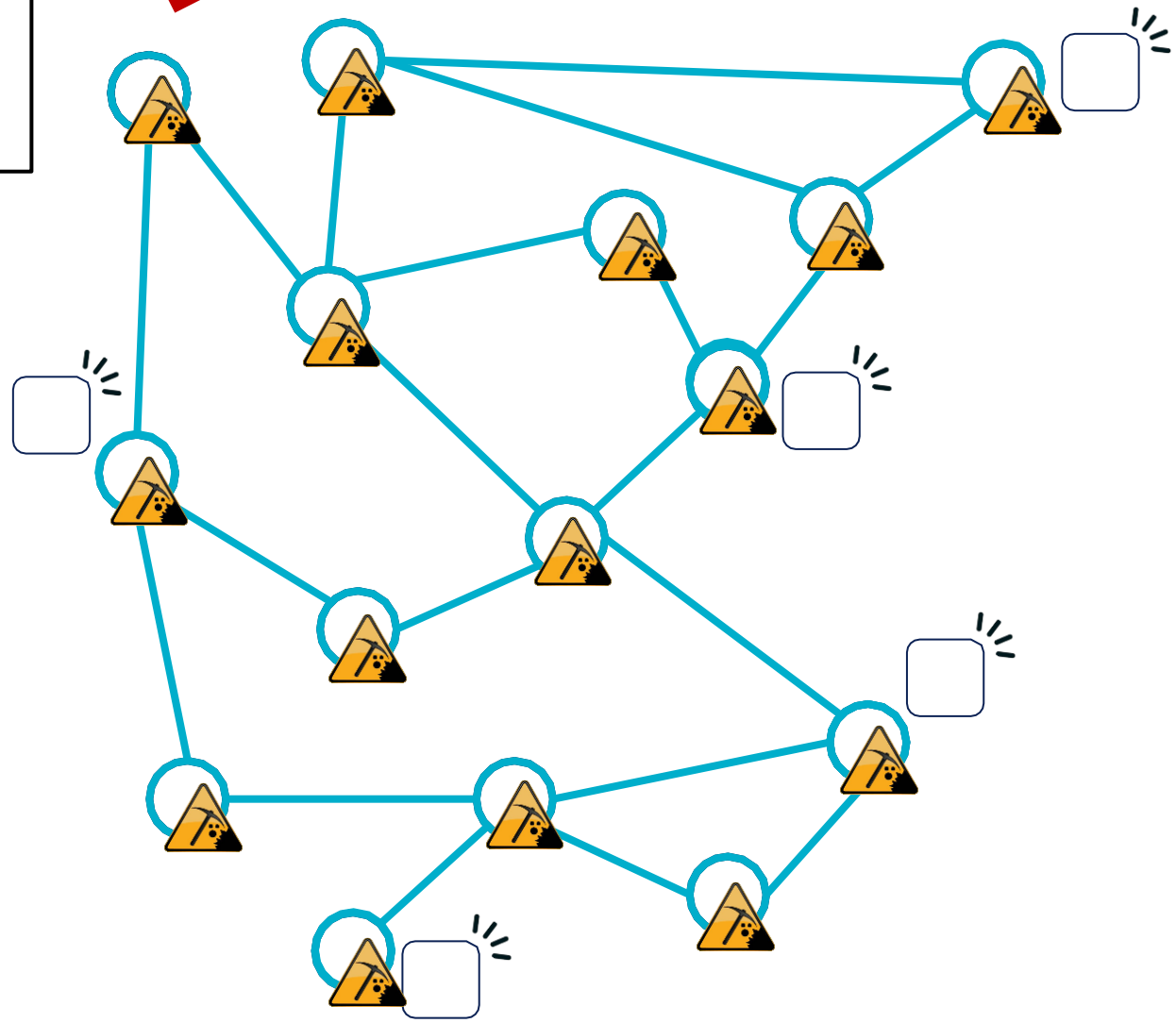
Transaction Execution

Transaction Submission

Transaction Preparation

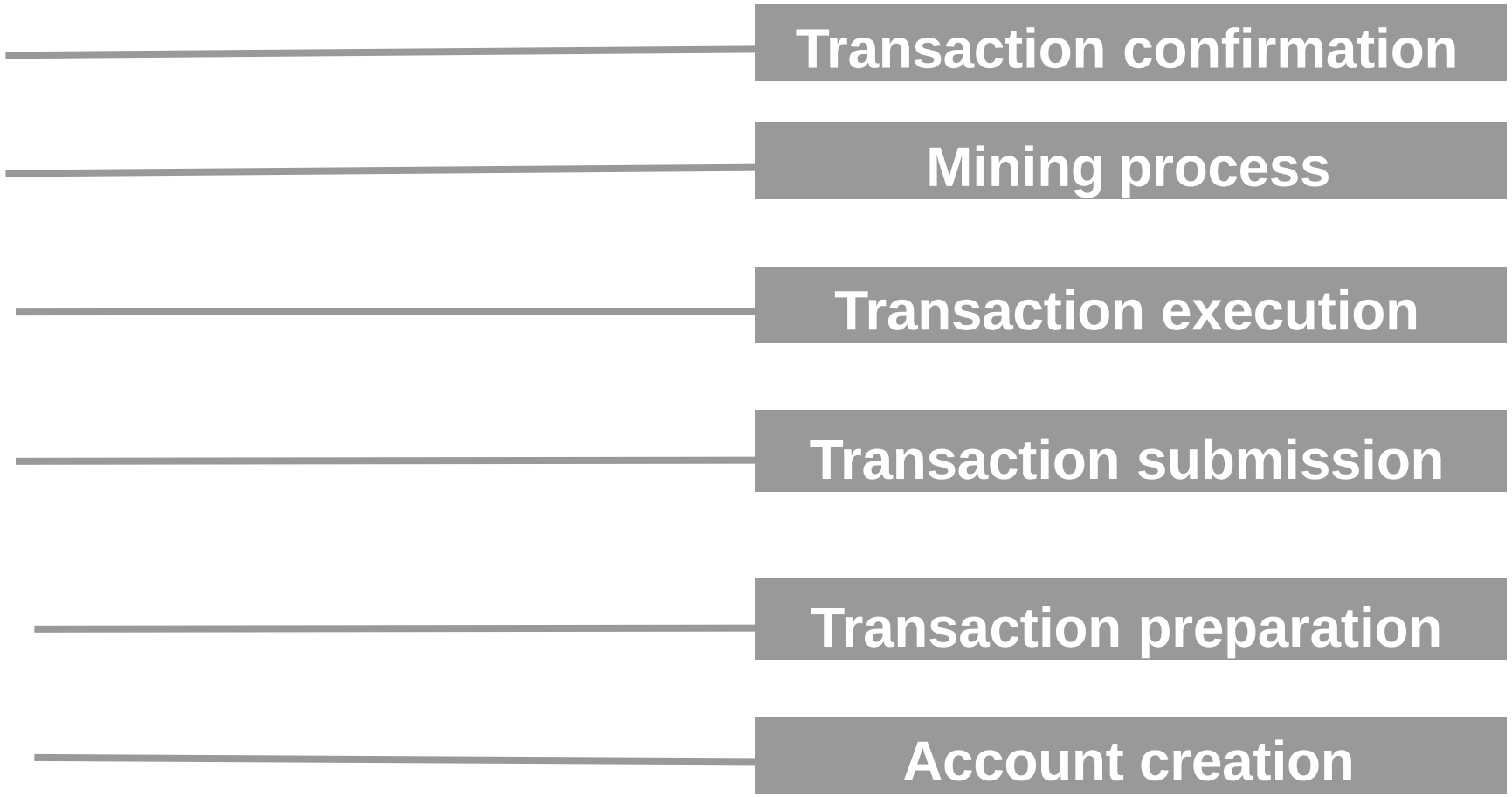
Account Creation





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

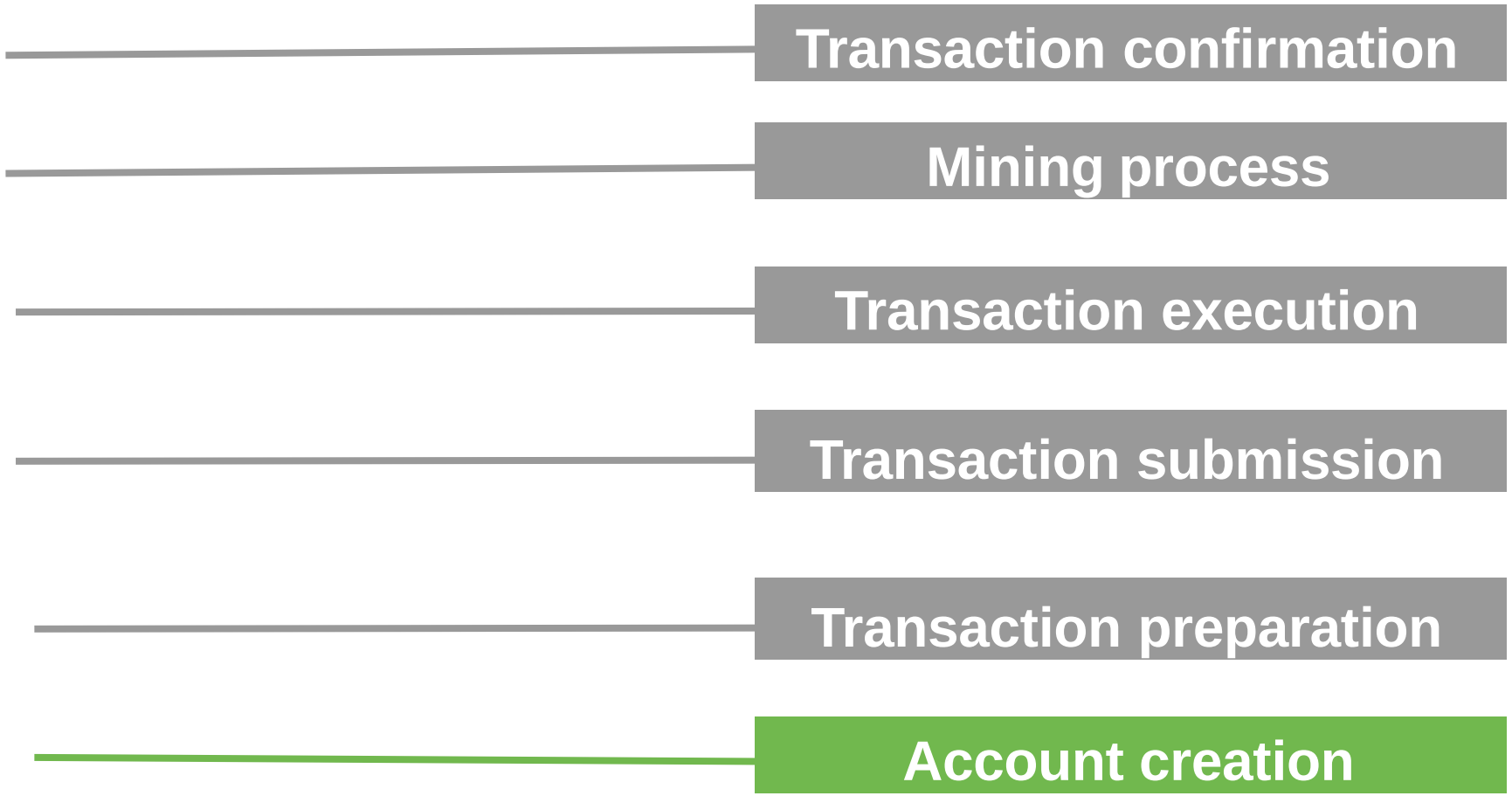
•Dogecoin

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 ?

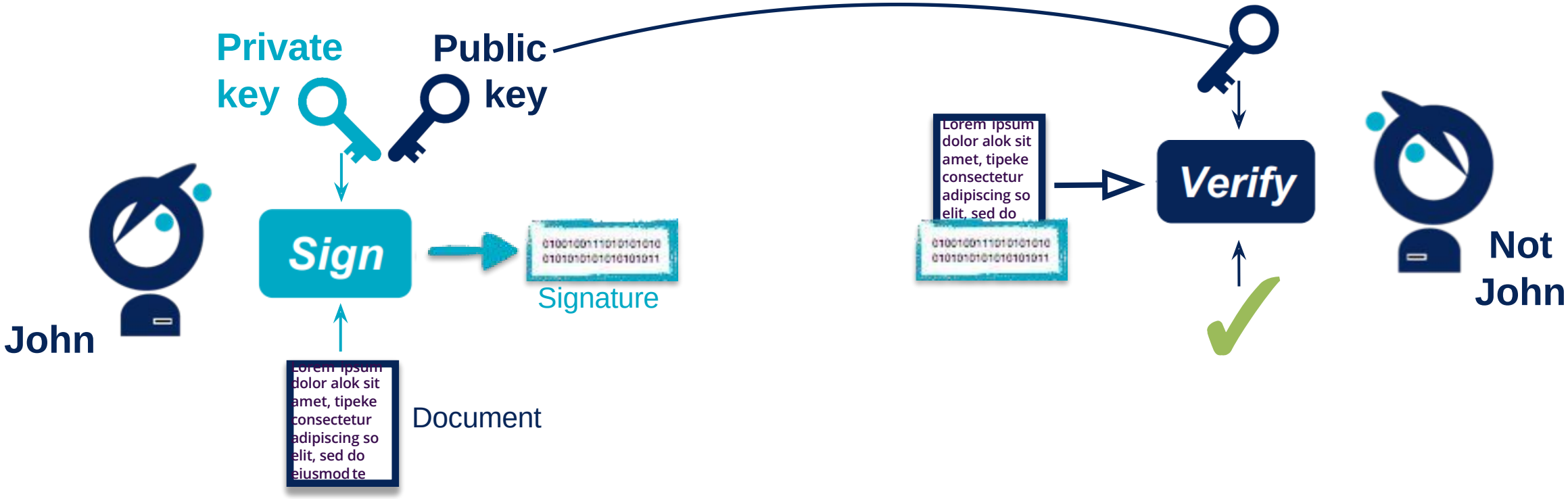
QU'EST-CE QU'UN COMPTE ?

*Un compte est **un obje** **ique** qui pourra émettre **des transa** **onnaie.***

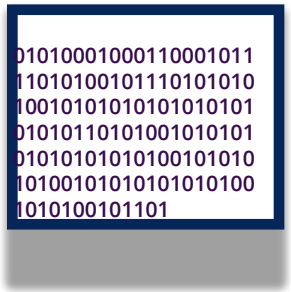
Deux problèmes :

- comment créer u utorité centrale ?
- Comment s'assu été émises légitimer

CRYPTOGRAPHIE : SIGNATURE ÉLECTRONIQUE



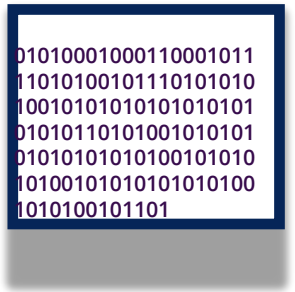
CRYPTOGRAPHIE : FONCTION DE HASH CRYPTOGRAPHIQUE



Any size

0x32ab7f65

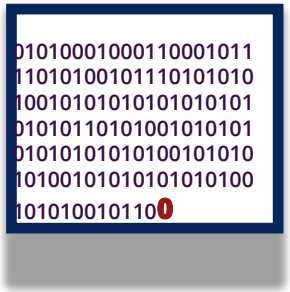
Fixed size



Original input

0x32ab7f65

Hash value

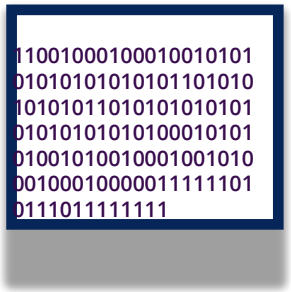


Small change

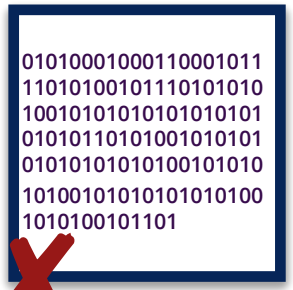
0x**47f42e10**

Big change

Original input



≠

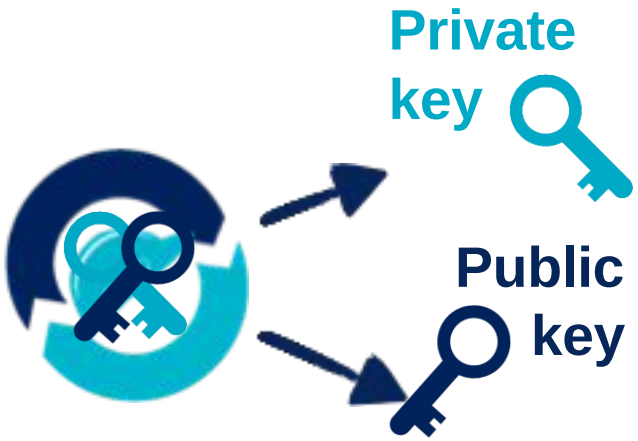


Different input

0x32ab7f65

CRÉATION DE COMPTE : MÉCANISME STANDARD

1. Key generation



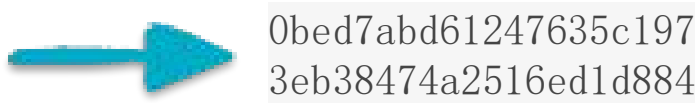
Most blockchain use Elliptic Curve Algorithms (courbes elliptiques)

2. Public Key Hashing

Ensure shorter address

Protect against attack on Public key

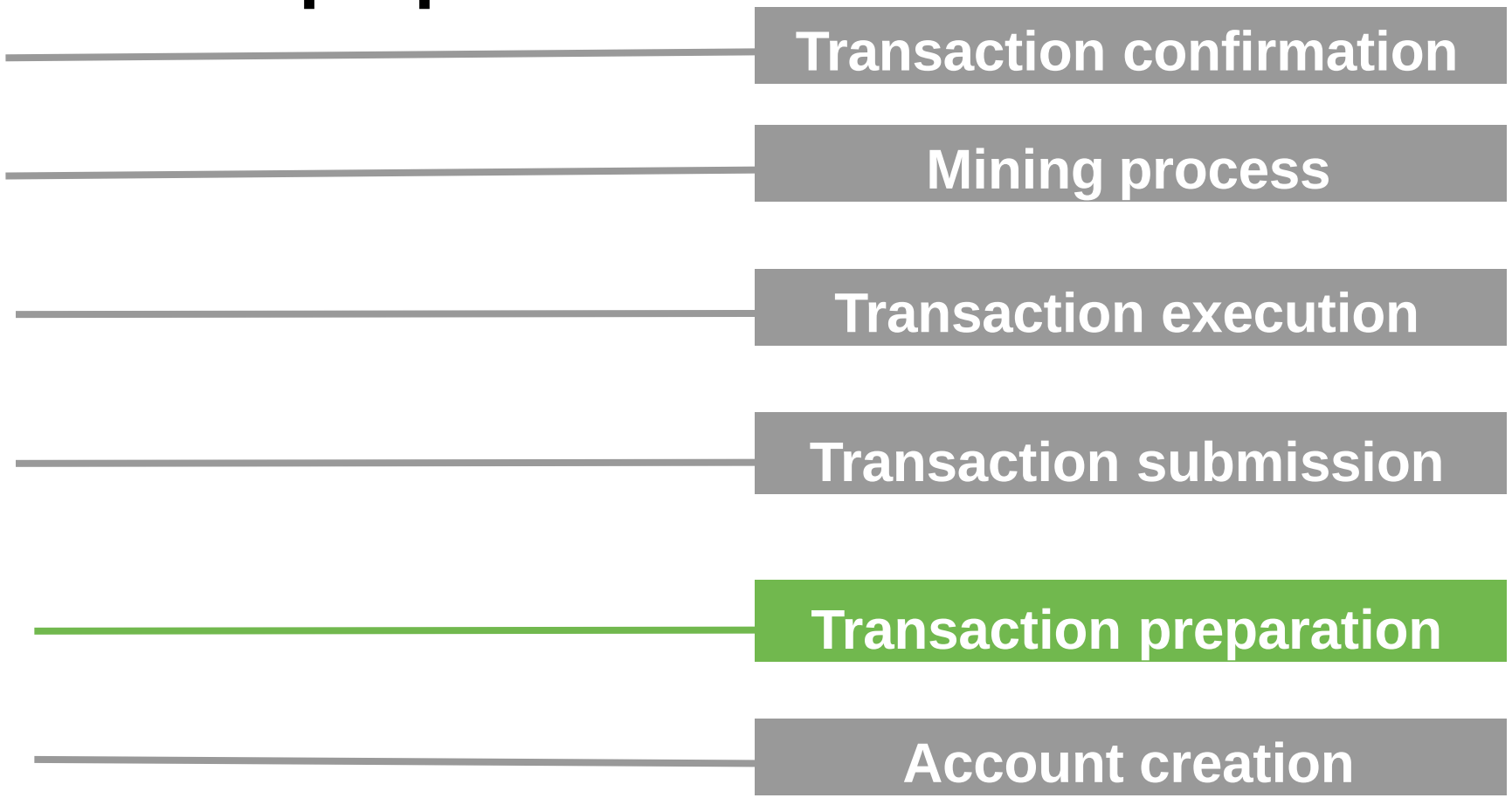
3. Address Encoding



Make it (a bit more) readable

Les algorithmes de courbes elliptiques (ECC, pour *Elliptic Curve Cryptography*) sont des techniques de cryptographie qui reposent sur les propriétés mathématiques des courbes elliptiques

Cycle de vie d'une transaction : Transaction preparation



QU'EST-CE QU'UNE TRANSACTION

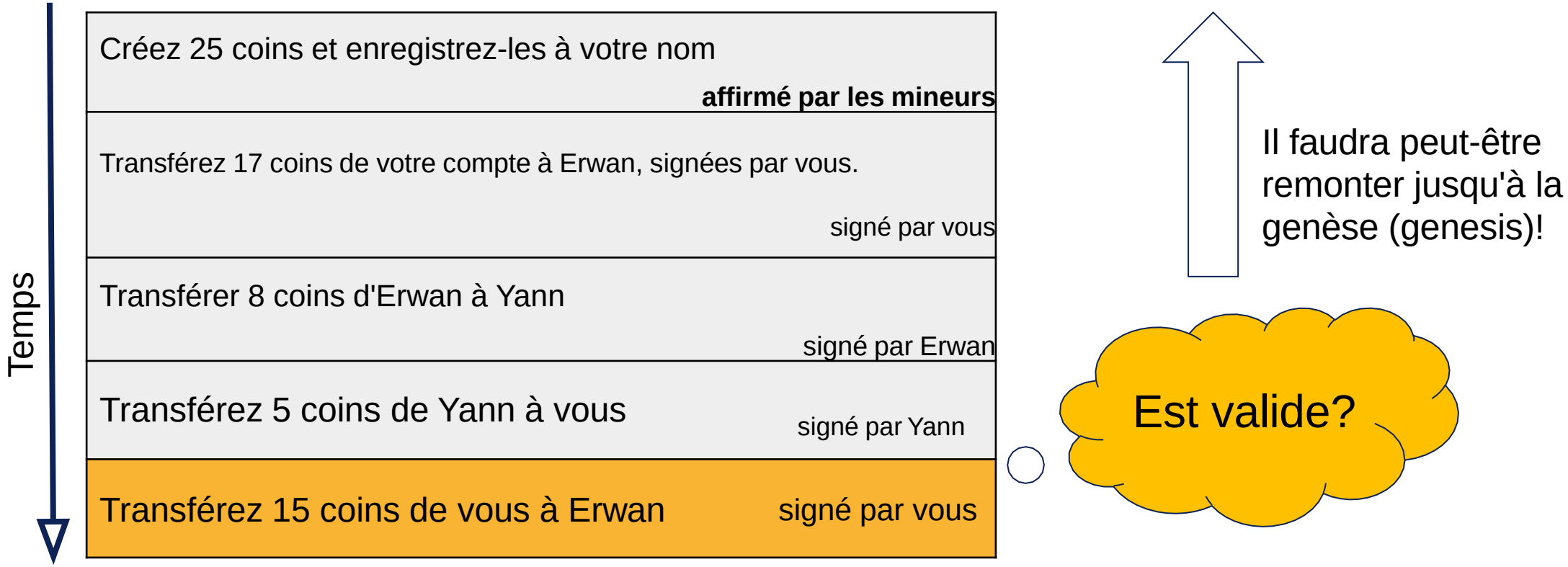
La transaction « payez-nous-un-café »

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

Vous avez 10 bitcoins comme solde de base

Tx1: paye-moi-un-café

Input 1

Output 1

Output 2

1 bitcoin

9 bitcoins non dépensés

Tx2: don't forget Yann!

Input 1

Output 1

Output 2

1 bitcoin

5 bitcoins non dépensés

Non dépensé = votre solde
10 - 1 = 9
facile!

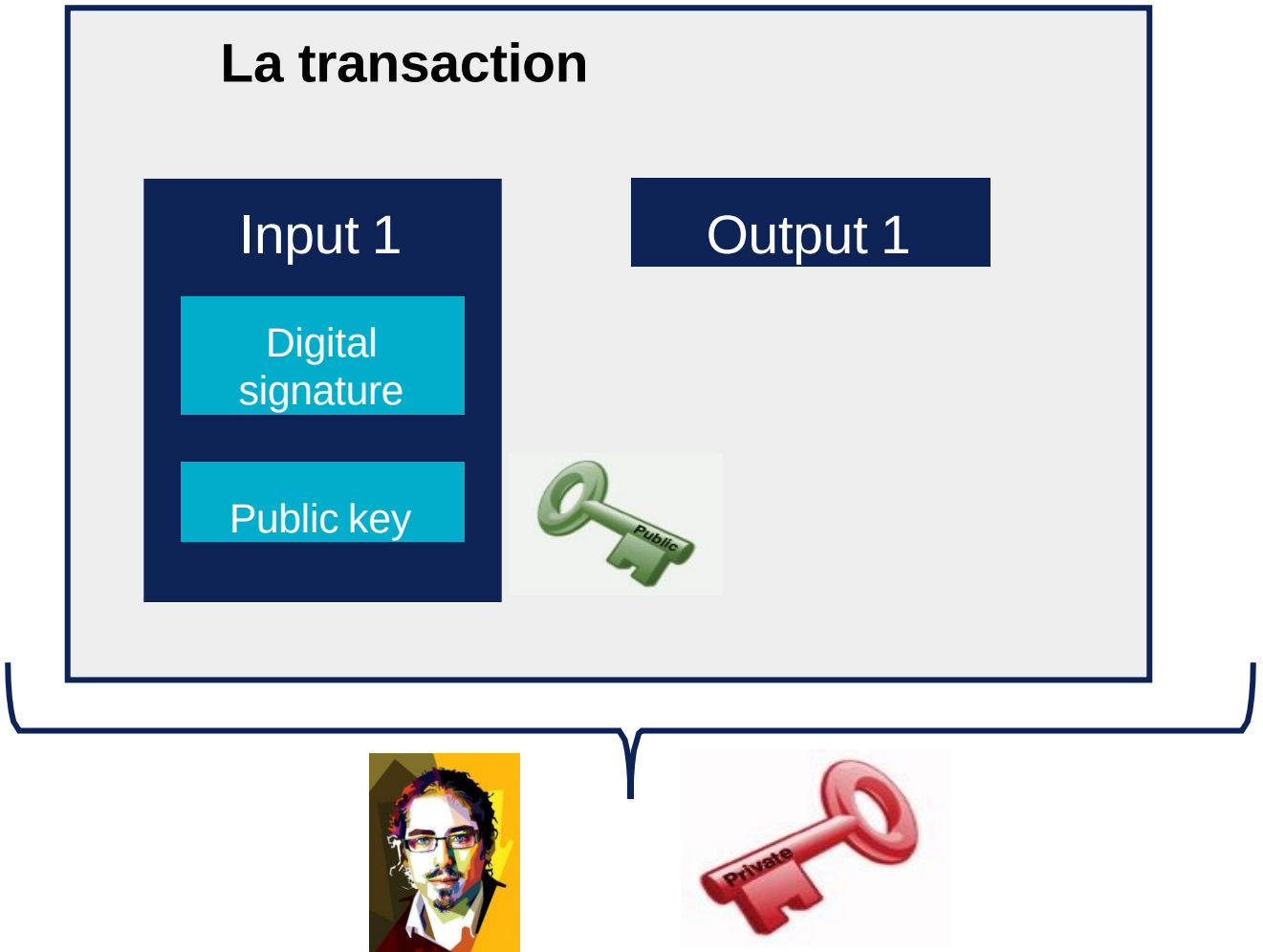
Non dépensé = votre solde
9 - 1 = 5 ?? Réellement??
Oui, vous avez donné 3 bitcoins en frais de minage
9 - 1 -5 = 3

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

Frais miniers
sum(inputs) - sum(outputs)

SIGNATURE DE TRANSACTION



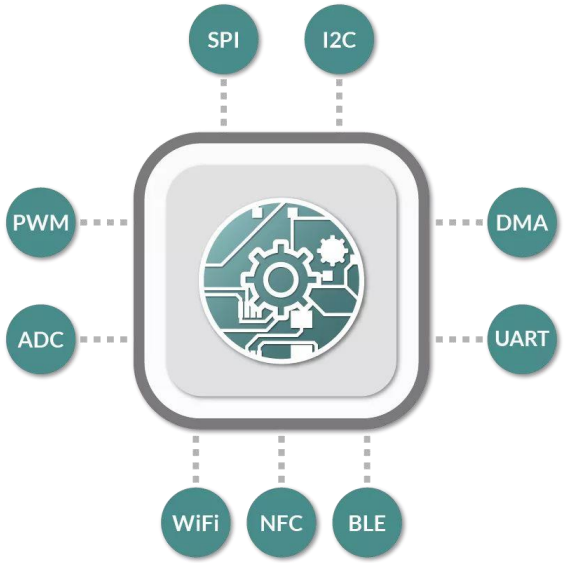
1. Vous effectuez la transation, vous devez donc **signer votre transaction avec votre clé privée**

2. Vous devez joindre **la signature** et **votre clé publique** à la transaction afin que tout le monde puisse la vérifier.

Ce processus peut être effectué hors ligne !

OK OK, MAIS DE QUELS SCRIPTS DE TRANSACTION PARLEZ-VOUS ?

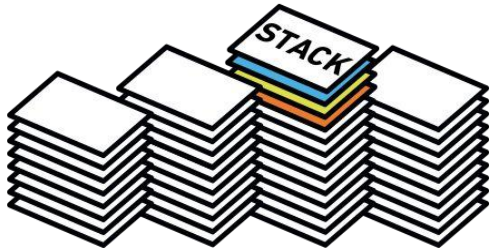
L'expéditeur choisit le script



ByteCode exécuté dans une machine virtuelle

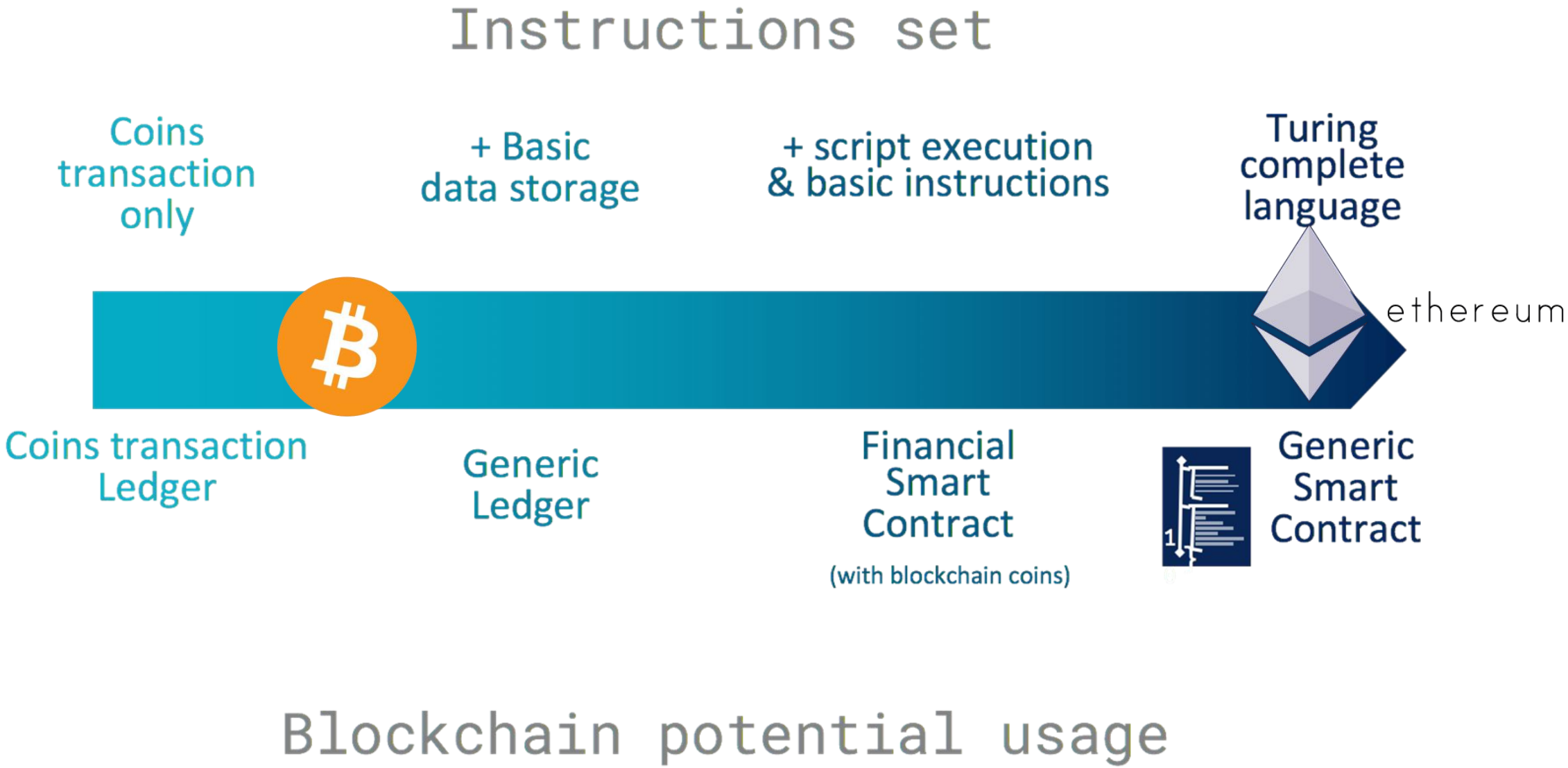
Ensemble d'instructions souvent limité

Pas de boucle dans Bitcoin

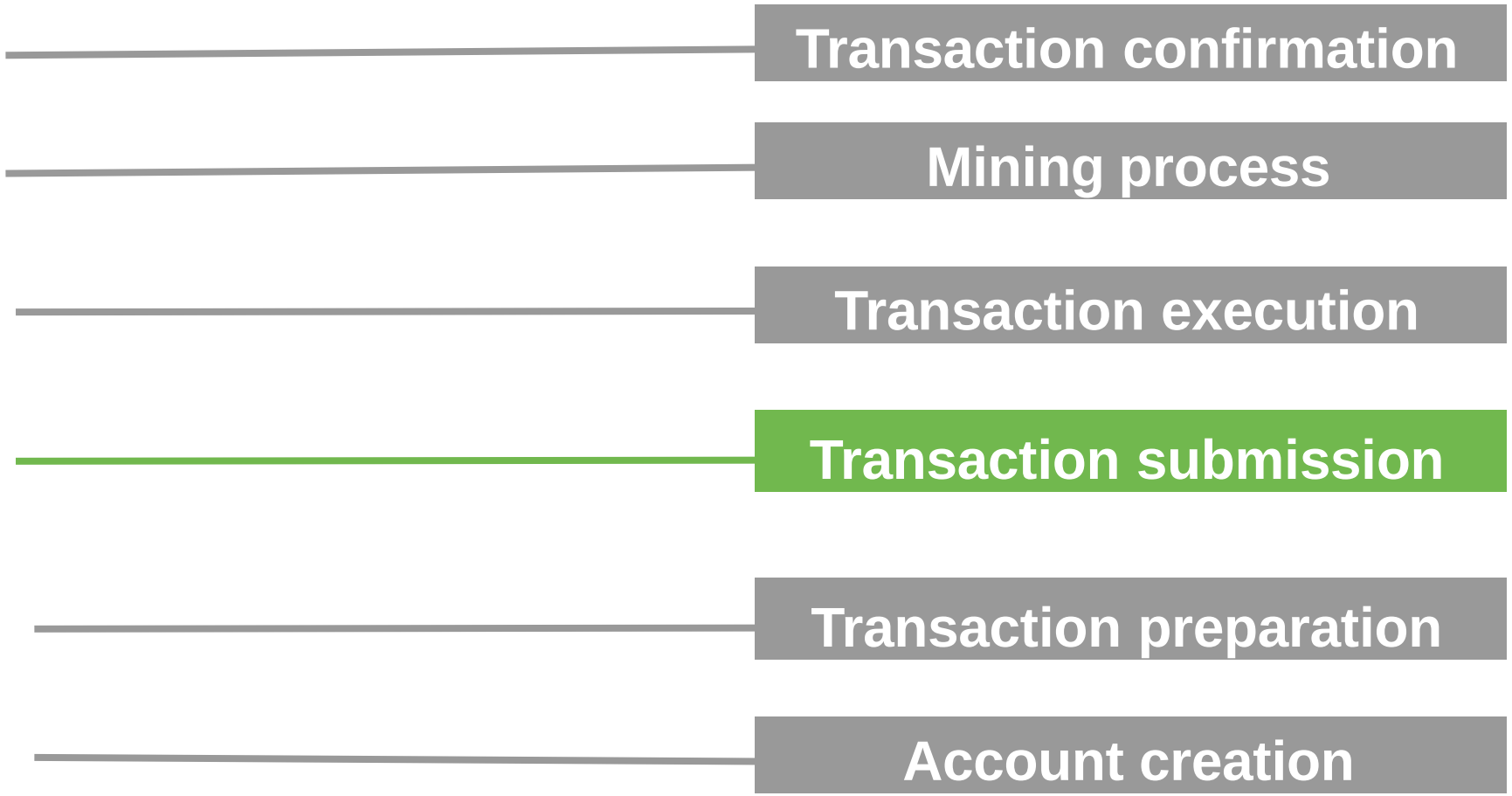


Bitcoin utilise un langage basé sur une pile

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



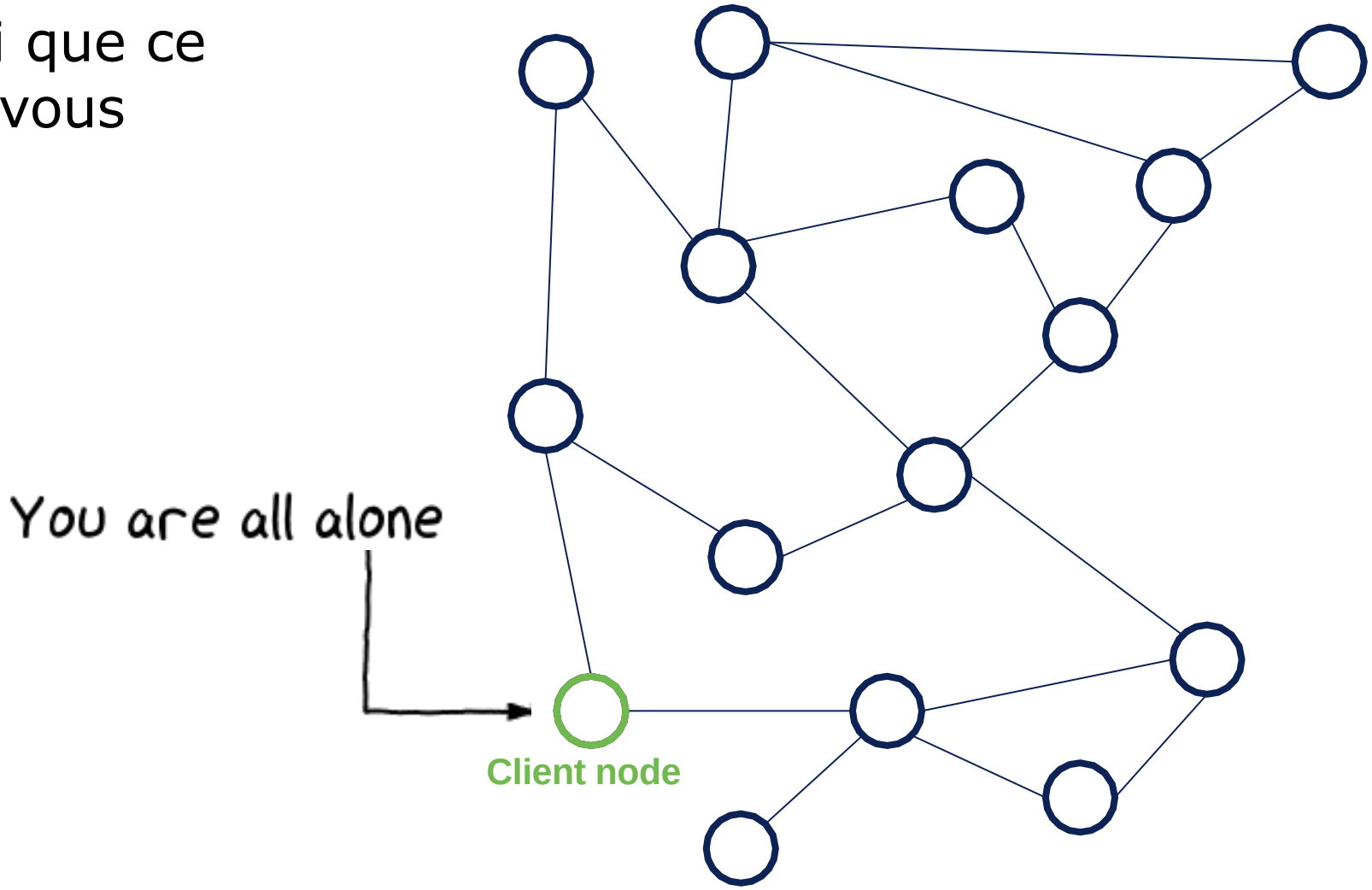
Cycle de vie d'une transaction :
Transaction submission



PREMIÈRE ÉTAPE : TROUVEZ VOS AMIS

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

Découvrez le réseau blockchain !

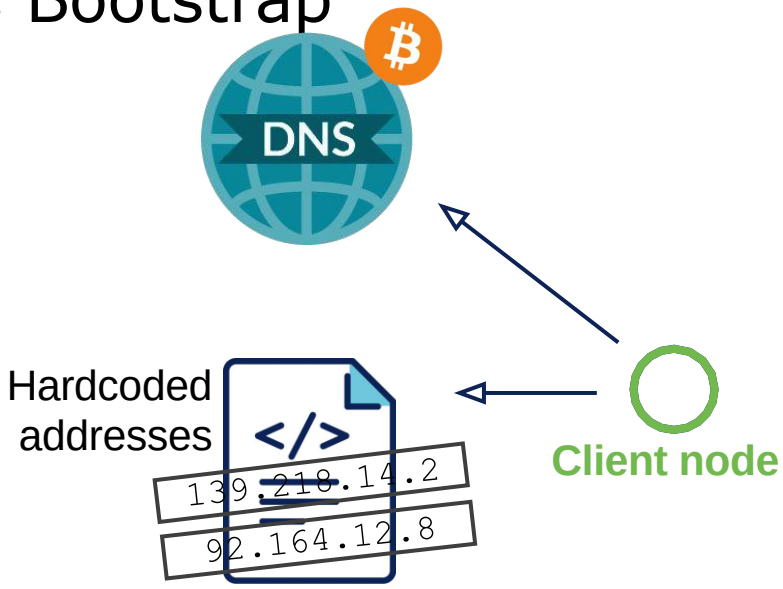


PREMIÈRE ÉTAPE : TROUVEZ VOS AMIS

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

Découvrez le réseau blockchain !

1. Trouver des nœuds Bootstrap

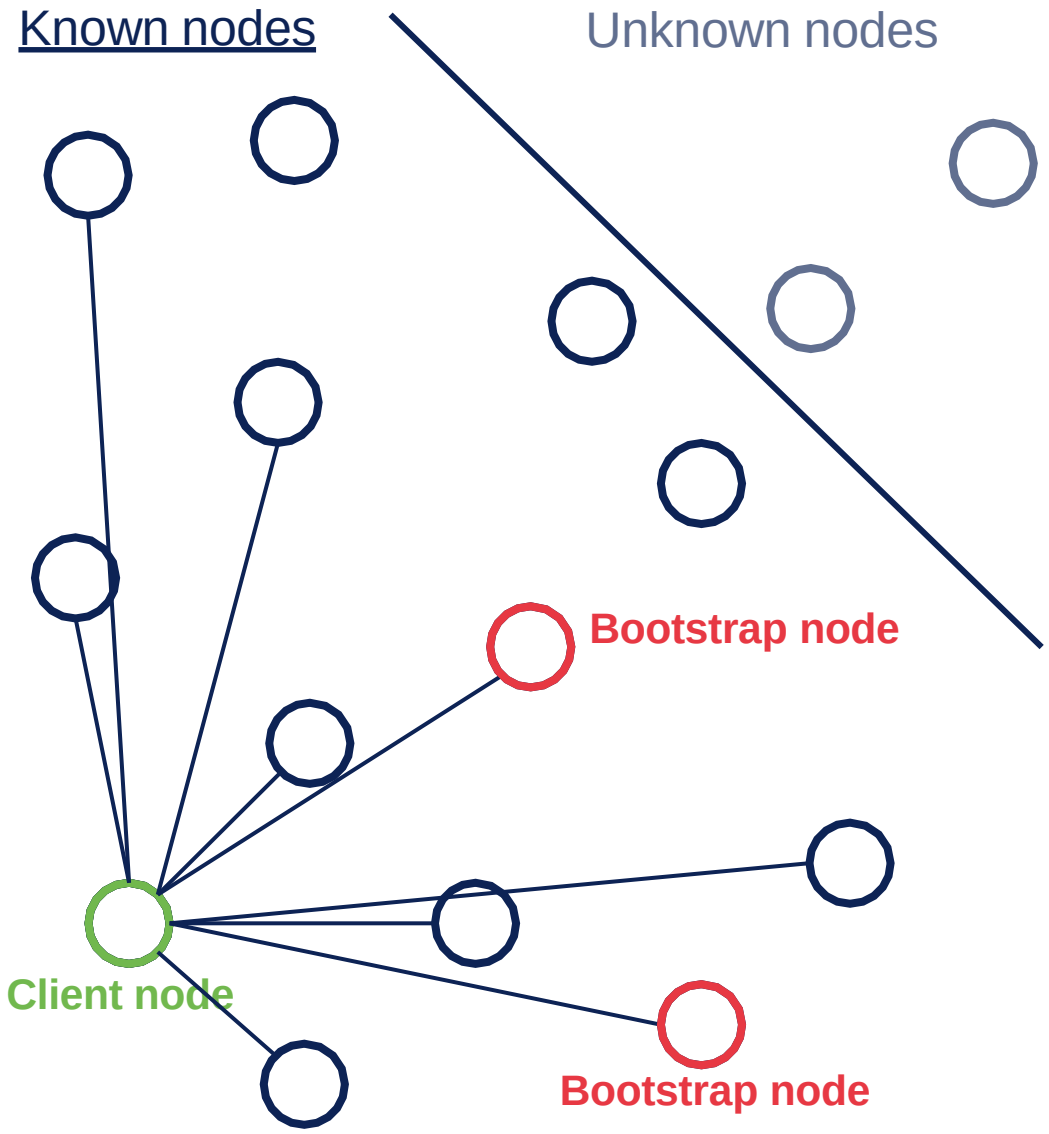


PREMIÈRE ÉTAPE : TROUVEZ VOS AMIS

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

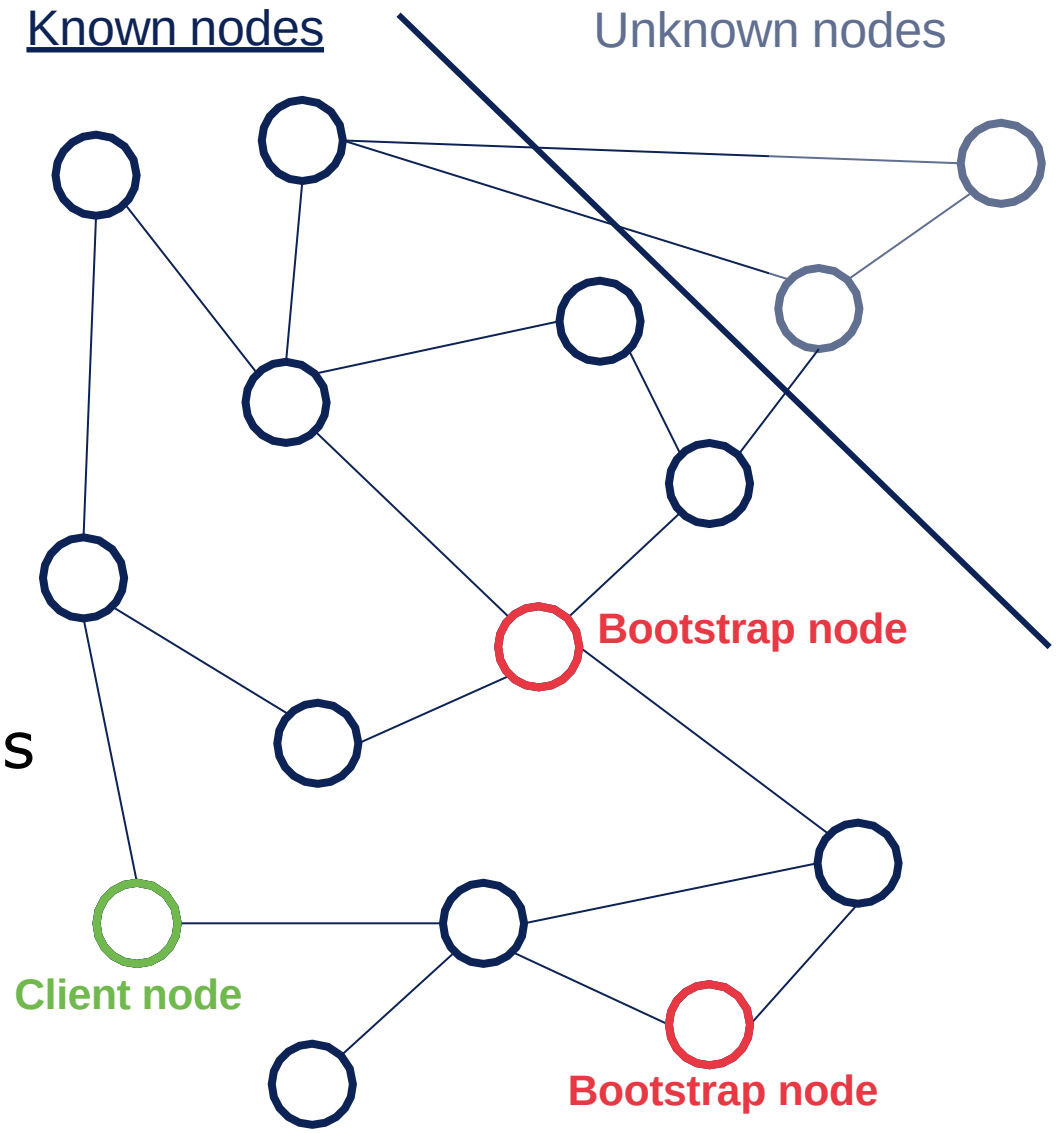


PREMIÈRE ÉTAPE : TROUVEZ VOS AMIS

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

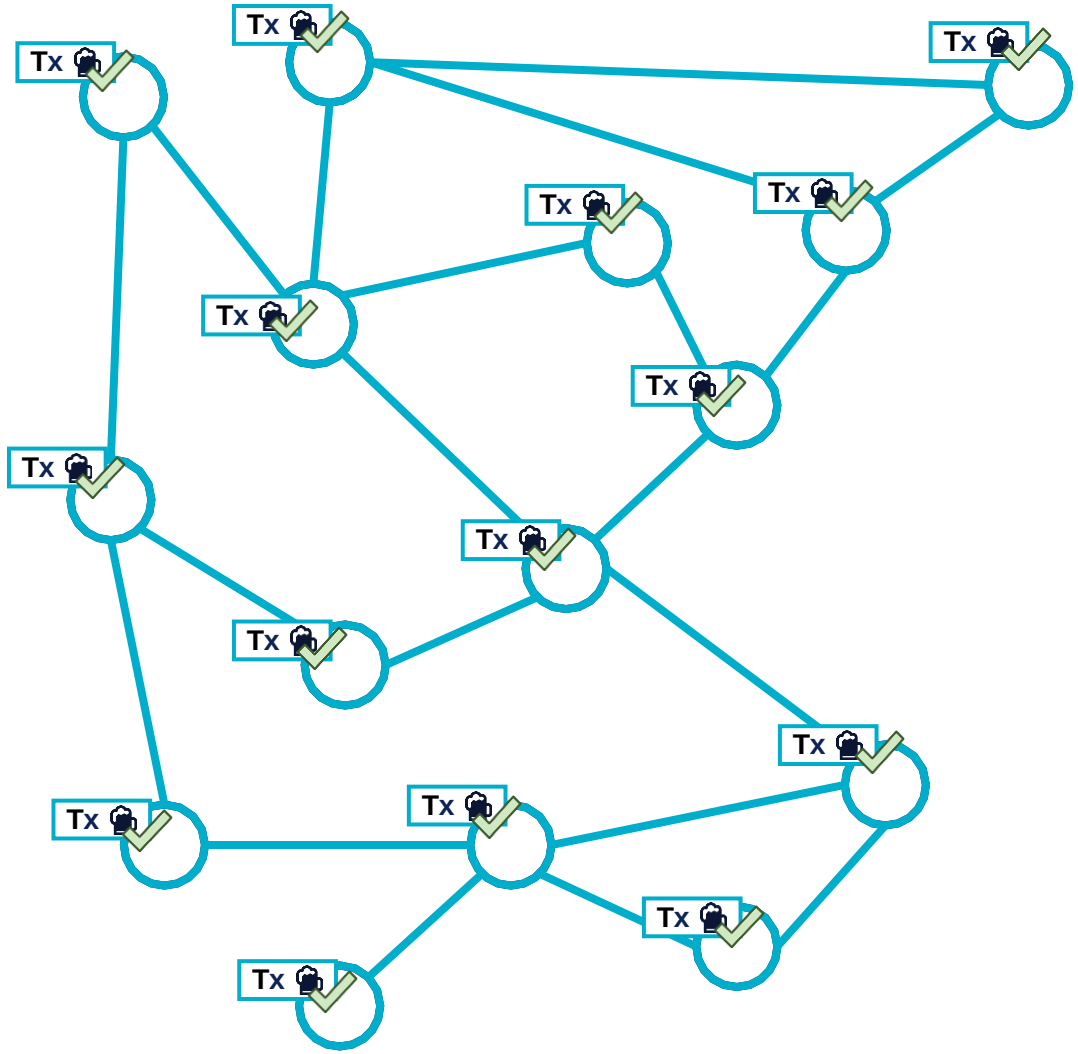
L'ensemble du réseau est finalement interconnecté



DEUXIÈME ÉTAPE : PARLEZ AVEC VOS AMIS

Principe

Transmettez simplement chaque transaction à vos voisins !



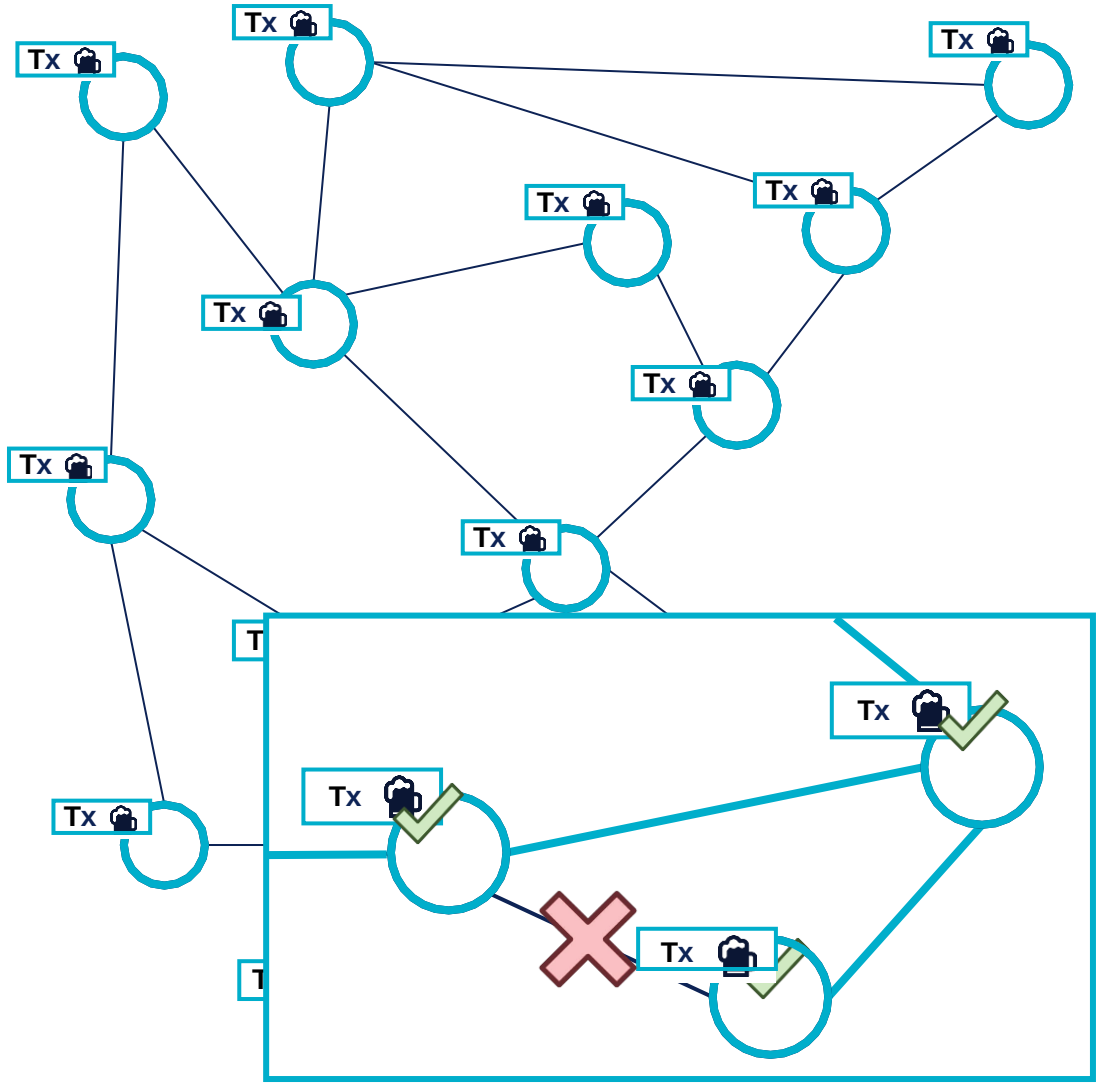
SECOND STEP: GOSSIP WITH YOUR FRIENDS

Principe

Transmettez simplement chaque transaction à vos voisins !

Pourquoi c'est cool ?

Fiable en cas de panne



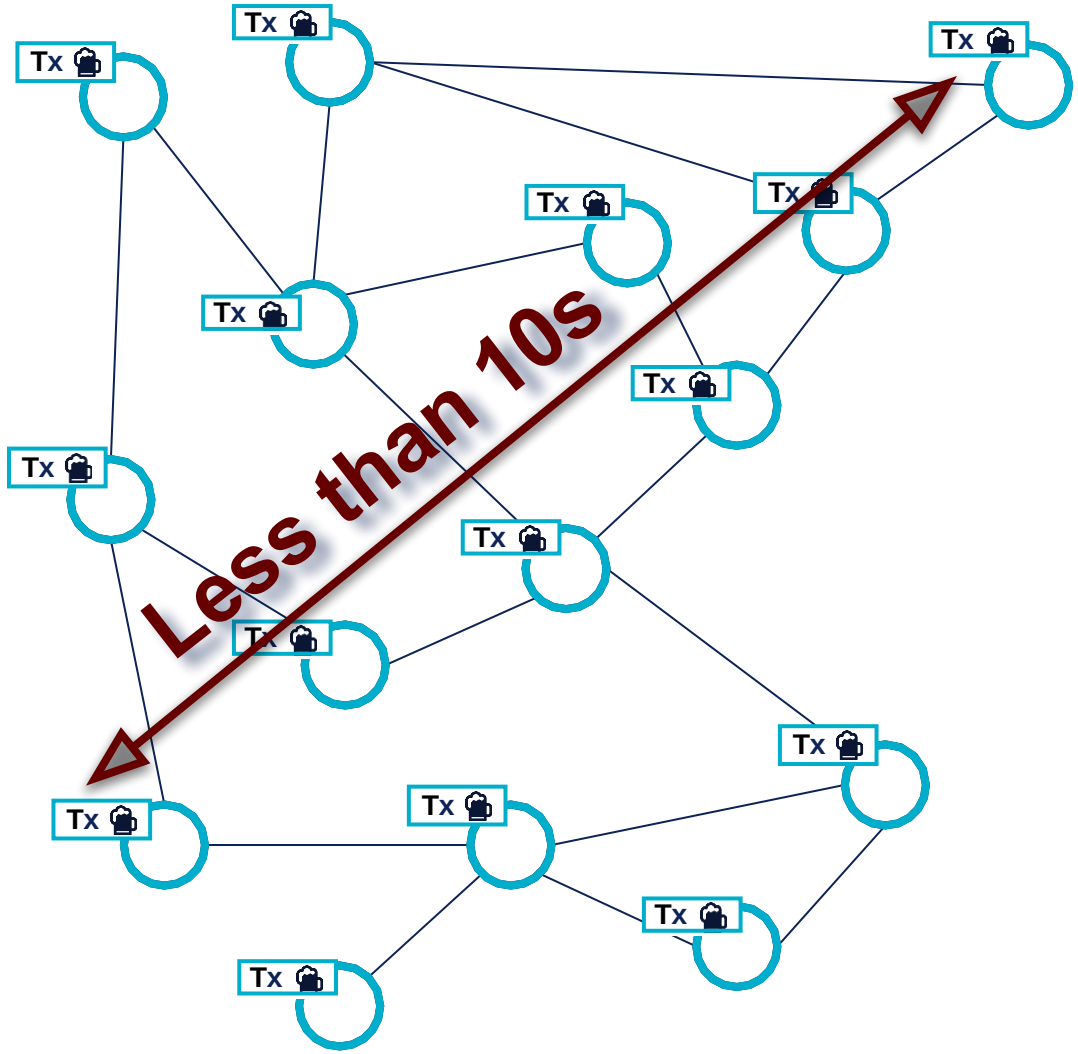
DEUXIÈME ÉTAPE : PARLEZ AVEC VOS AMIS

Principe

Transmettez simplement chaque transaction à vos voisins !

Pourquoi c'est intéressant ?

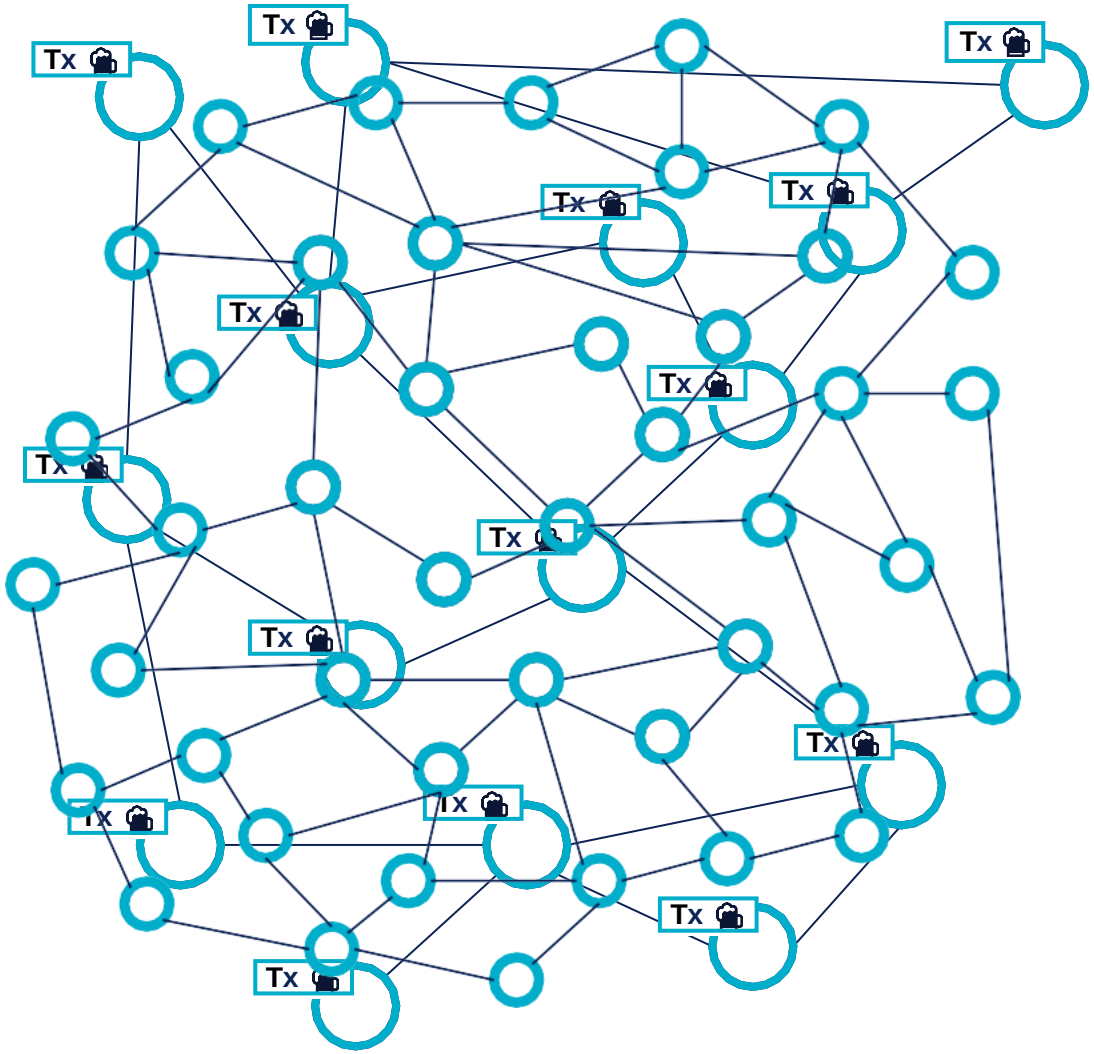
- **Fiable en** cas de panne
- **Livraison garantie dans un délai limité**



DEUXIÈME ÉTAPE : PARLEZ AVEC VOS AMIS

Principe

Transmettez simplement chaque transaction à vos voisins !



Pourquoi c'est intéressant ?

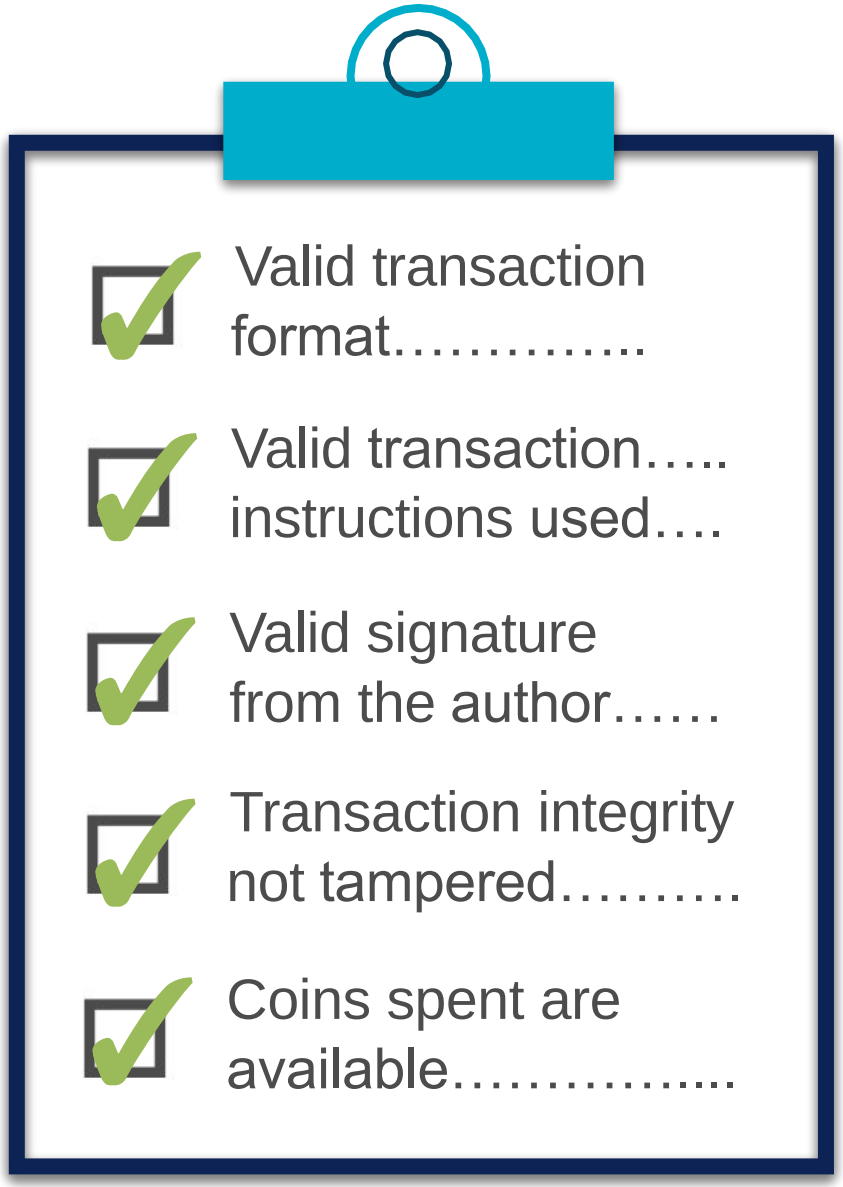
- **Fiable en** cas de panne
- **Livraison garantie dans un délai limité**
- **Échelle** avec le nombre de pairs

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**



ALLONS au Memory POOL!

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

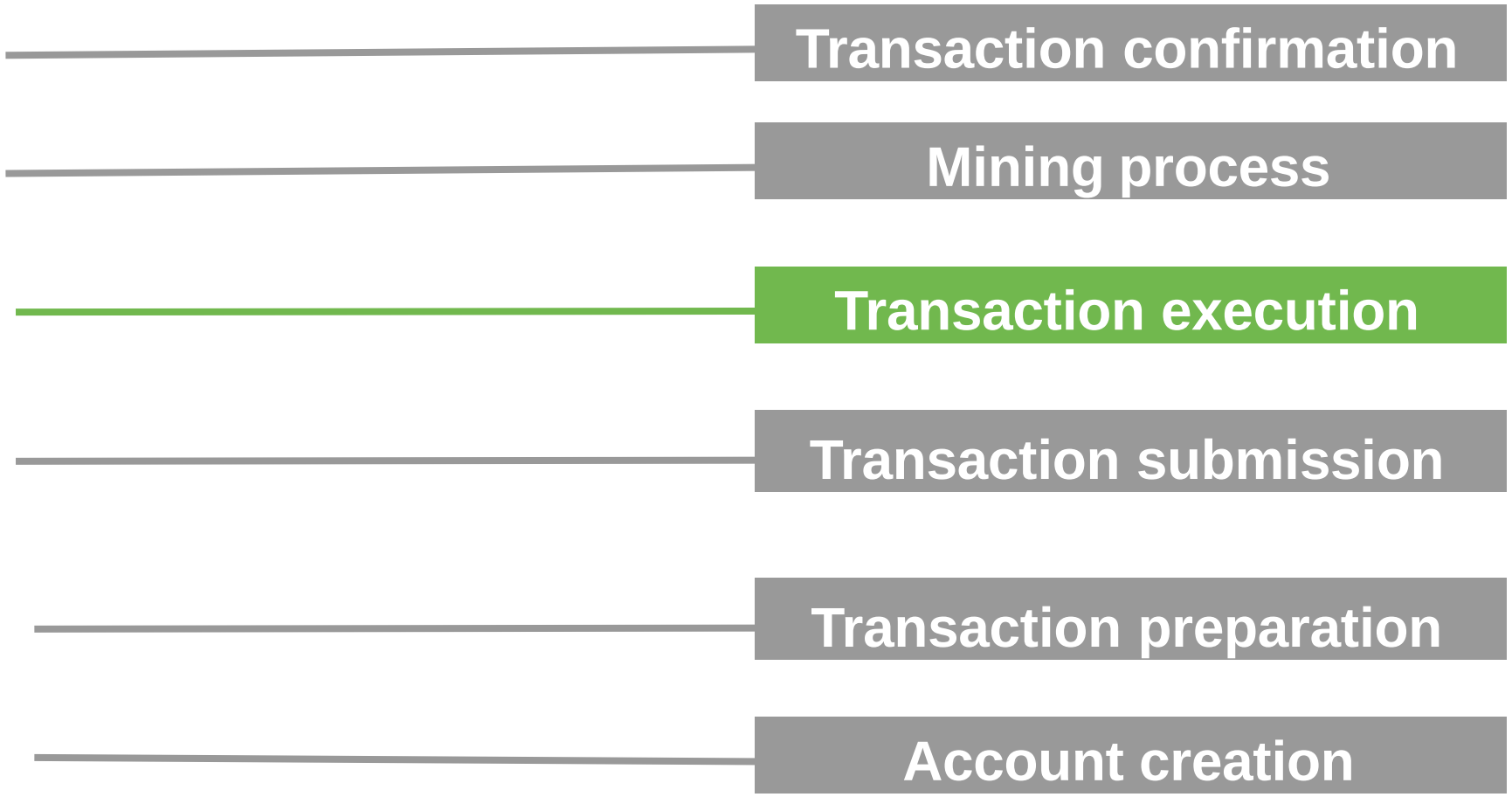
Transaction Pool

Transactions	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

Classé par frais

Mining node A

Cycle de vie d'une transaction : Mining process



BUT WHAT IS A BLOCKCHAIN STATE?

It depends...

Bitcoin State

Unspent transactions coins

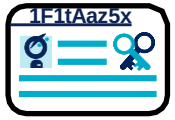
- **20 coins spendable by Bob**
- 10 coins spendable by John
- **5 coins spendable by Bob**
- 5 coins spendable by Lucie

Ethereum State

Account information

Bob has 25 coins

John has 10 coins



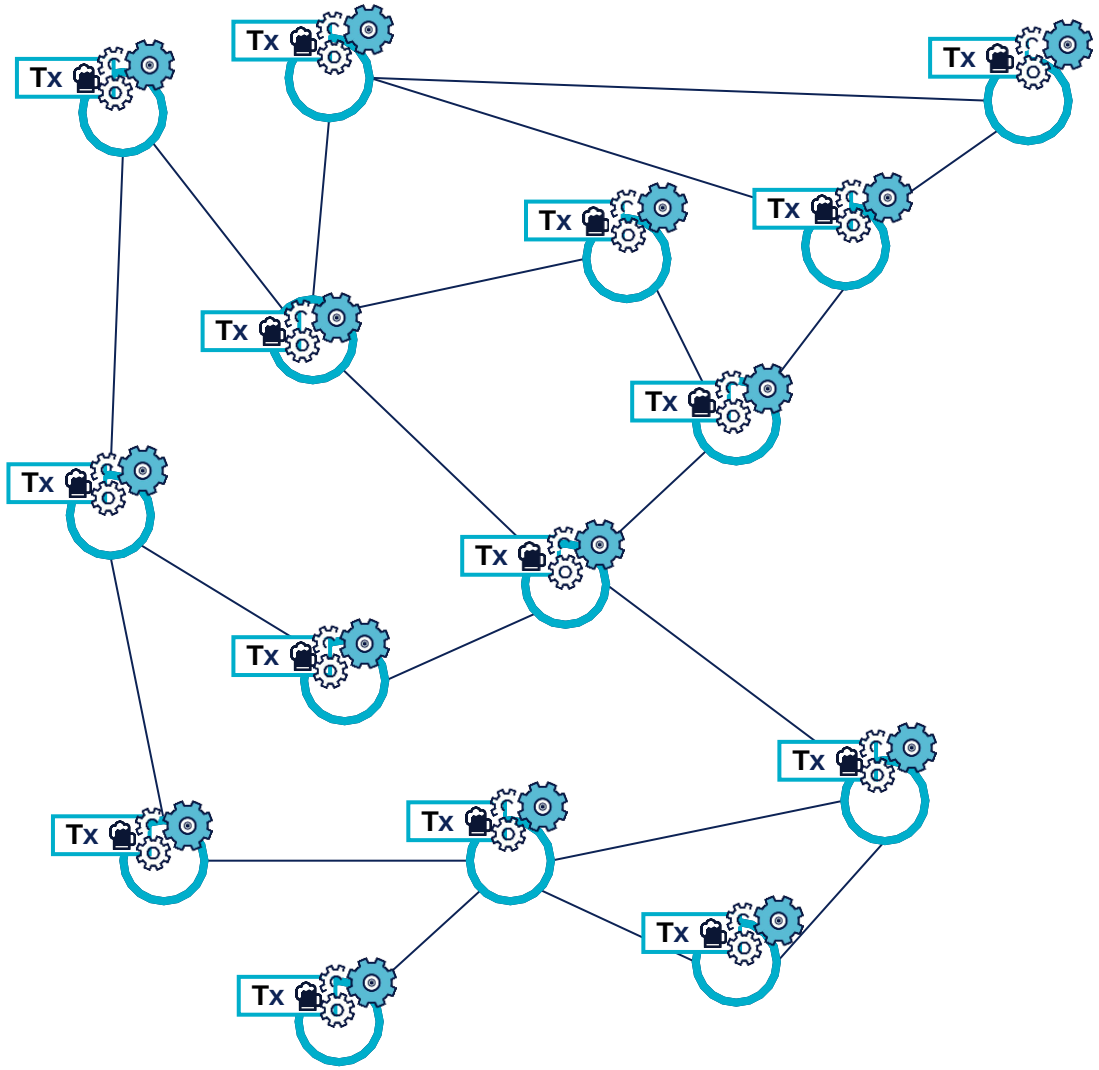
Lucie has 5 coins

Contract Foo contains A=10

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**

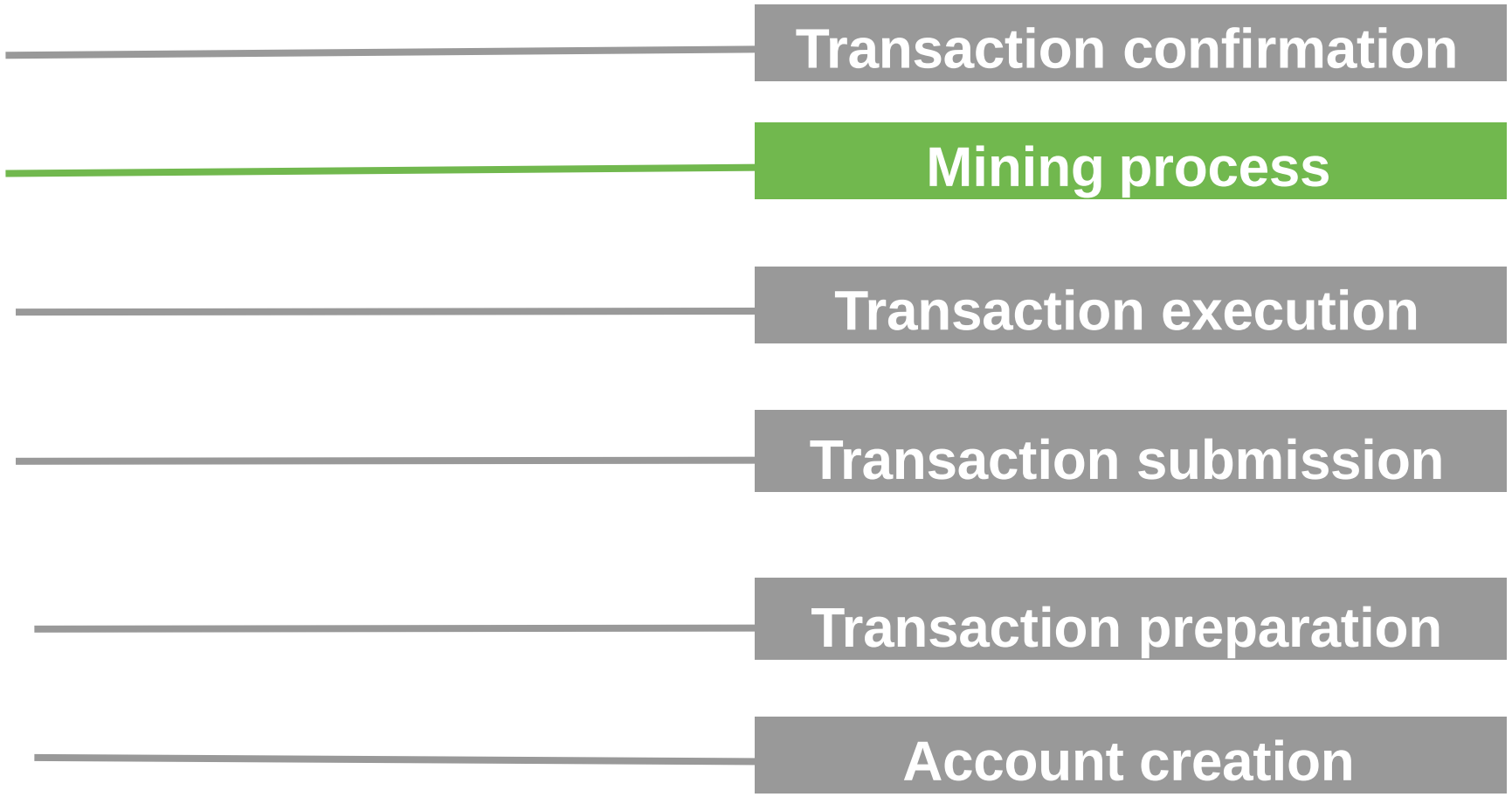
Menace 2 | Attaque par **relecture de transaction**

Solution

Enchaînement de transactions

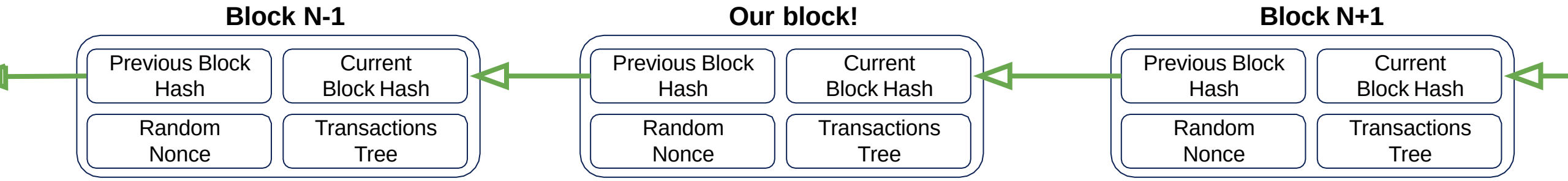
ID incrémentiel par transaction/compte

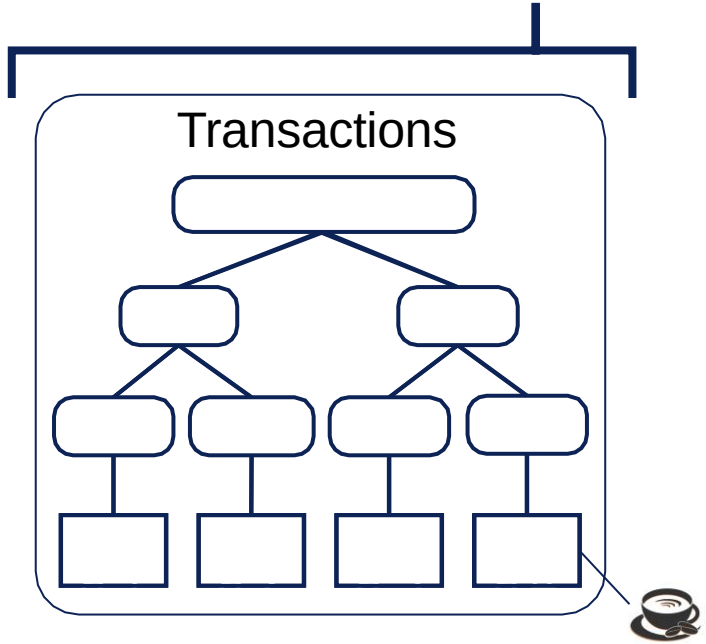
Cycle de vie d'une transaction : Propagation de bloc



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

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





Pourquoi regrouper les transactions dans un bloc ?

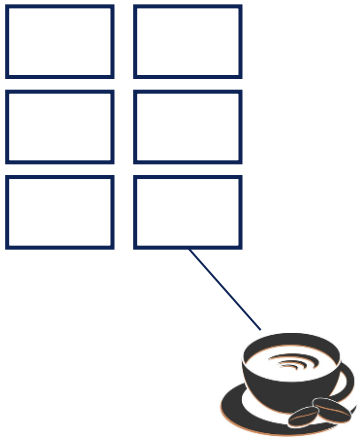
- Unité de travail unique pour les mineurs
  (sera décrite plus tard)
- Limiter la longueur de la blockchain
  (vérification plus rapide de l'historique)

Le temps moyen de génération de blocs est généralement constant

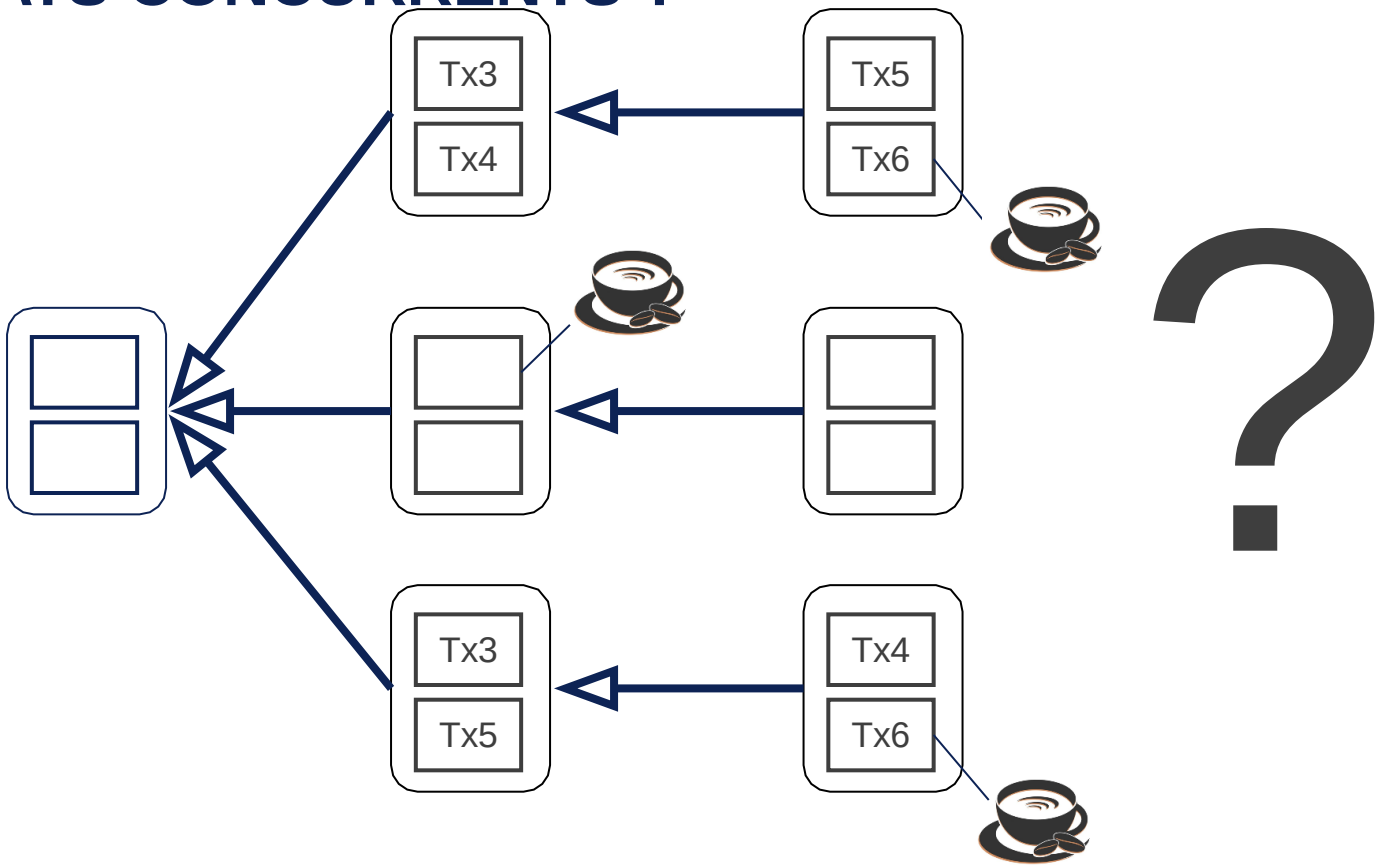
- ~10 mn for Bitcoin
- ~12 seconds for Ethereum

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

Sybil attack

fausse multitude de nœuds utilisant des identités forgées

Double spend

dépenser deux fois le même argent

Transaction censorship or delaying

empêcher trnx d'être inclus dans la blockchain

Long Range attack

Créez une blockchain longue et valide et faites-en la publicité auprès des nouveaux nœuds qui la rejoignent

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)

hash(**block** + **random value**) < **difficulty**

Bitcoin case

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

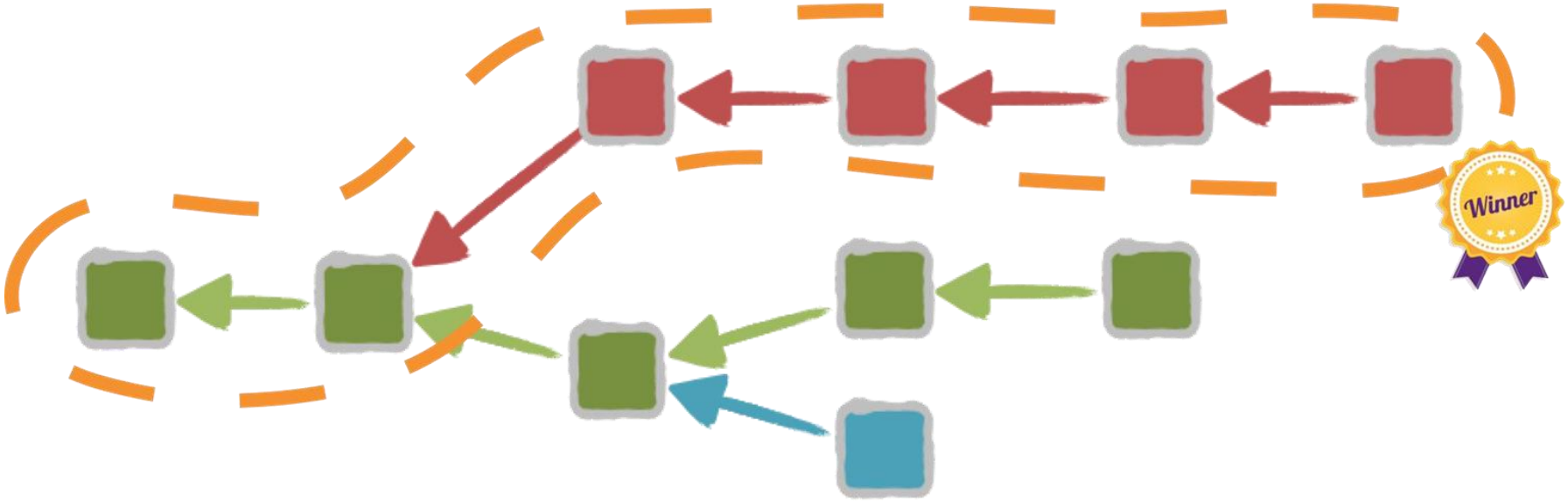
La difficulté est régulièrement ajustée pour **maintenir un temps moyen de génération de blocs constant**

RÉSOLUTION DES FOURCHES (FORKS)

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

The process continues and

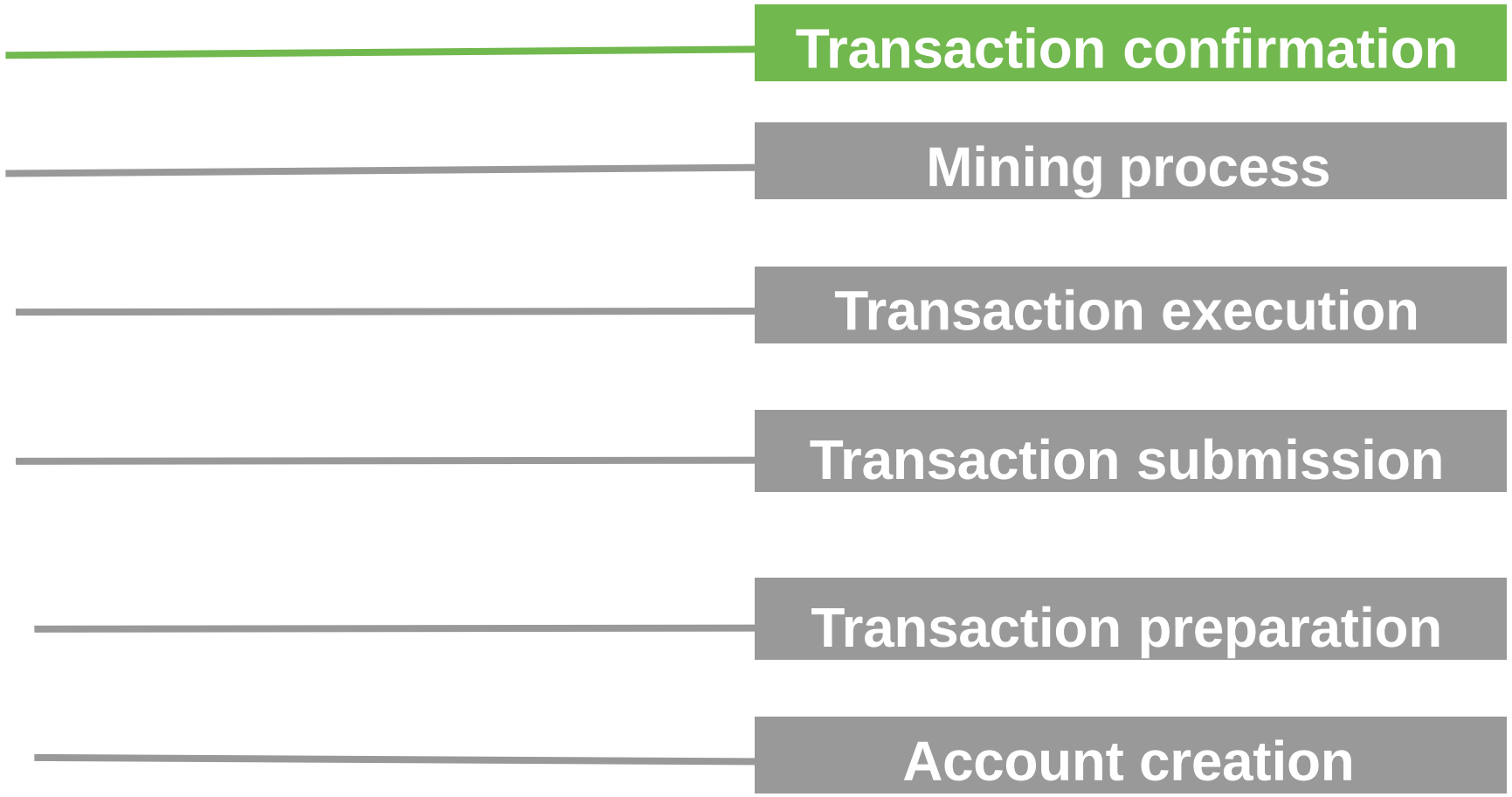
The longest blockchains wins !



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



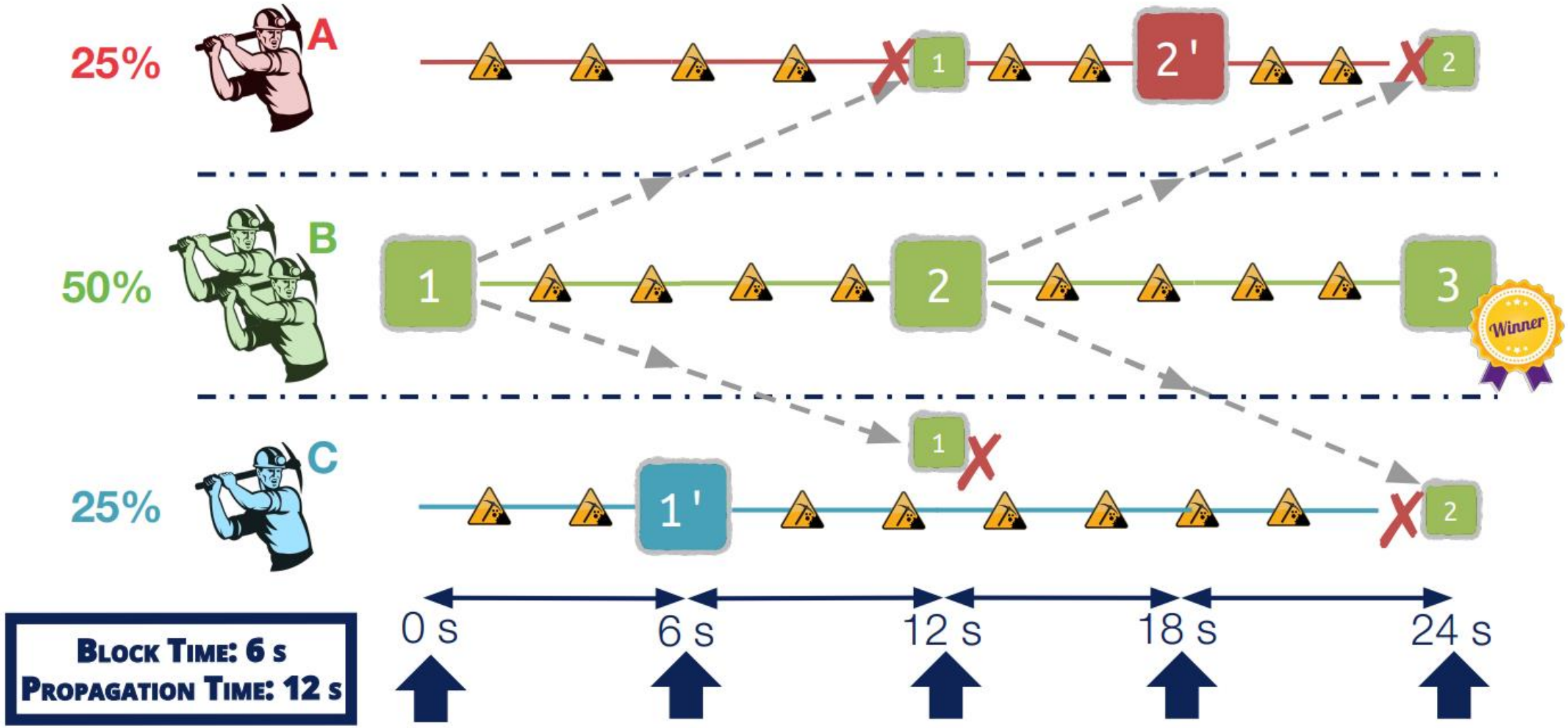
AVANT : LA PROPAGATION DE BLOCS (PAS SI SIMPLE)

- 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 mauvaispour la sécurité**

IMPACT D'UN PETIT BLOC HORAIRE

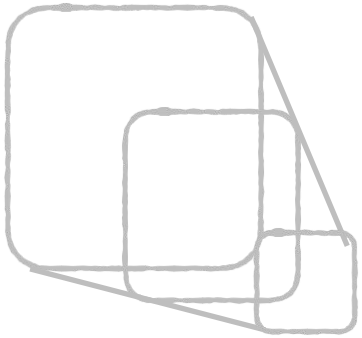


CONTRE-MESURES CONTRE LA CENTRALISATION

High propagation time lead to **centralisation**

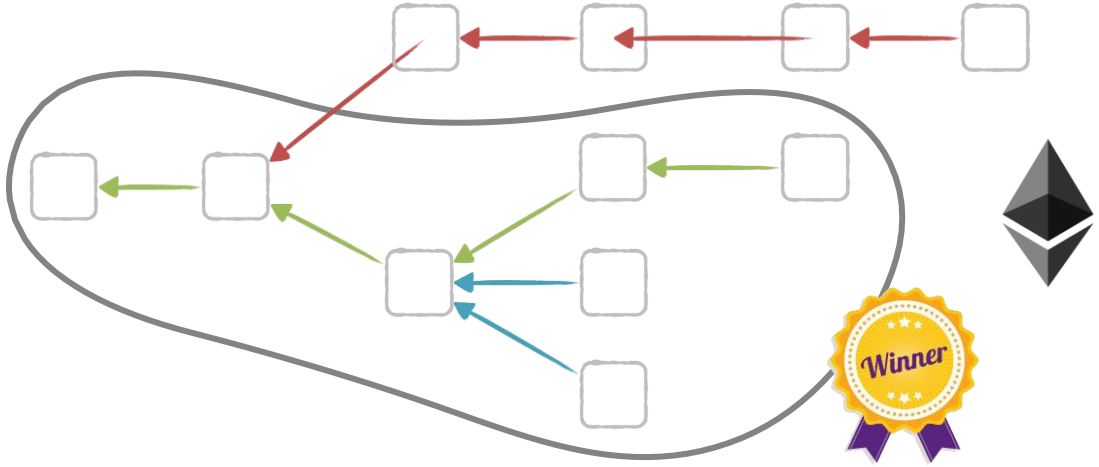
Solutions:

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

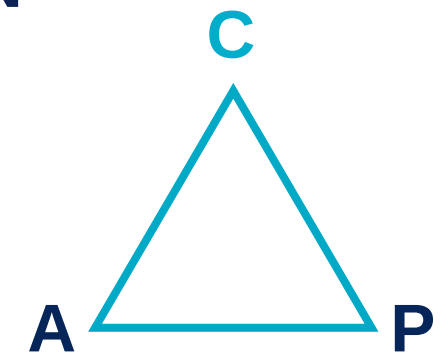


1 MB Block size limit

- Make **orphan blocks count** to select winner

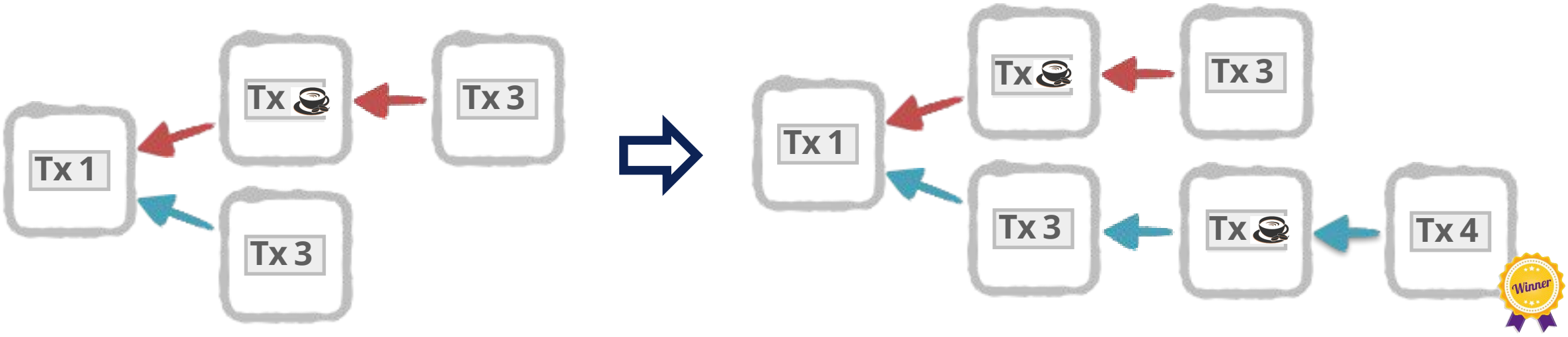


LE PROBLÈME DE LA CONFIRMATION DE TRANSACTION



- **Problem:** blockchain are **eventually consistent**

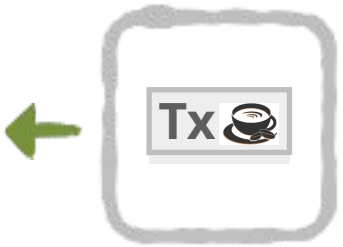
- **Transactions can be re-organized in the short term** as part of forks resolution



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

The oldest is a transaction
the less likely a transaction could be reverted

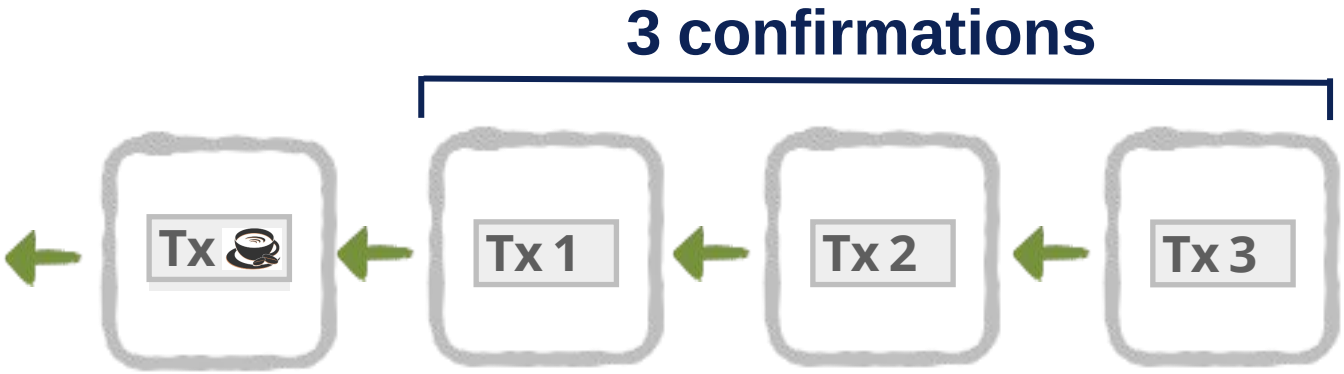


0 confirmation

Not sure we will have our beer!

COMMENT ÊTRE SÛR DE VOTRE TRANSACTION

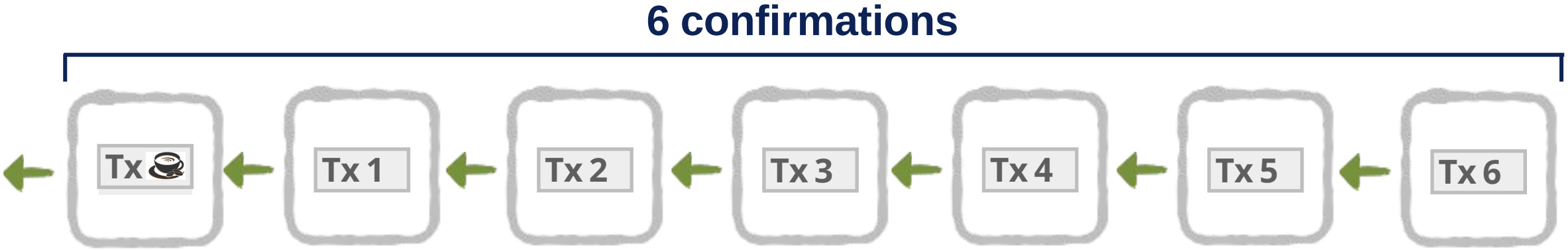
The oldest is a transaction
the less likely a transaction could be reverted



We may have our beer!

COMMENT ÊTRE SÛR DE VOTRE TRANSACTION

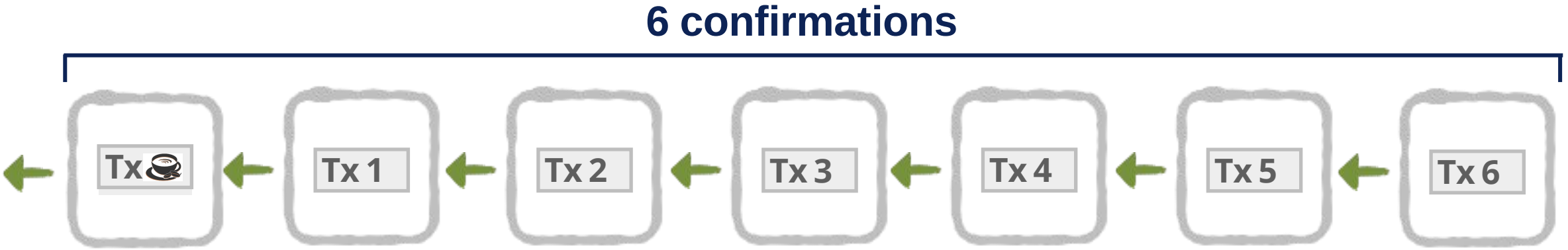
The oldest is a transaction
the less likely a transaction could be reverted



We will have our beer!

COMMENT ÊTRE SÛR DE VOTRE TRANSACTION

The oldest is a transaction
the less likely a transaction could be reverted

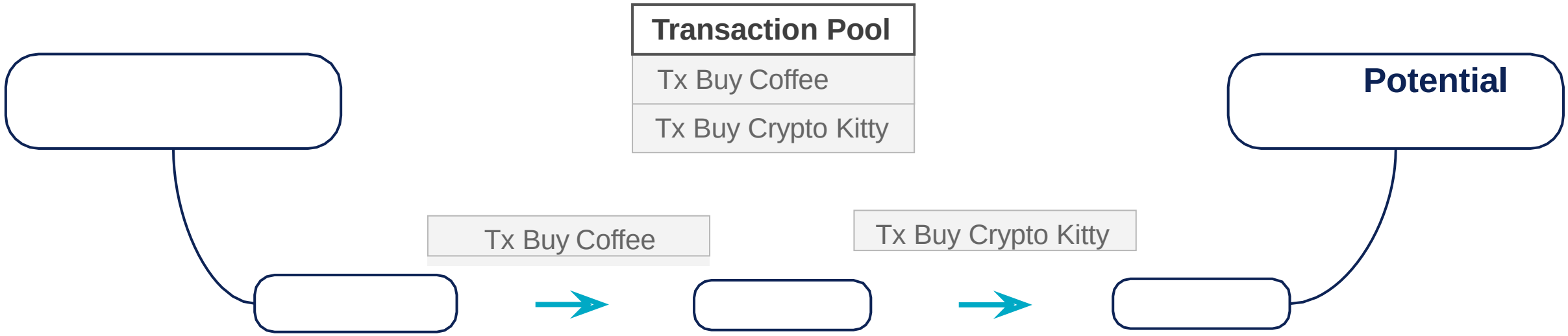


6 blocks-old transactions are considered close to **100% safe**

Questions ?!!

UN MODÈLE D'EXÉCUTION SIMPLE

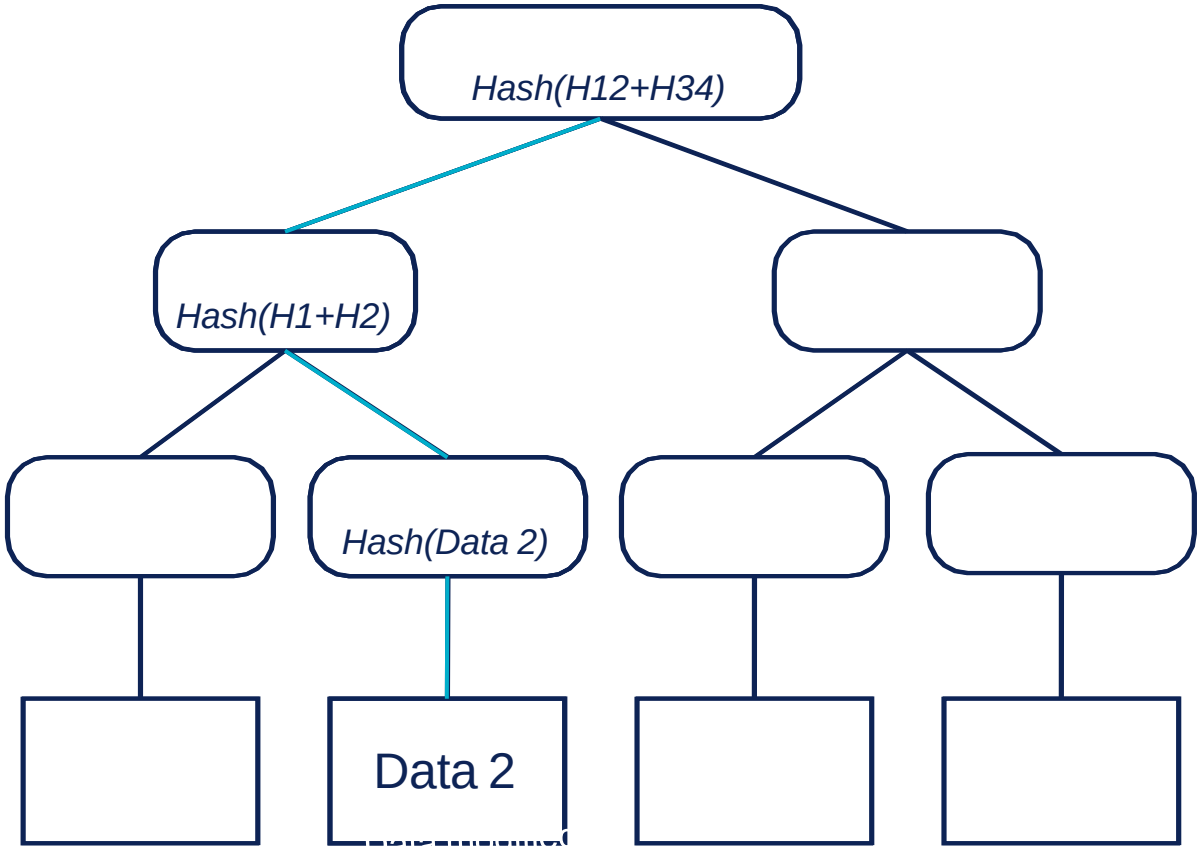
Les transactions ne sont que **des fonctions de transition d'état...**



...qui sont **exécutées séquentiellement**

COINS GROWTH ON (MERKLE) TREES

Most blockchains use **Merkle Trees** to store **transactions list** or whole **blockchain state**

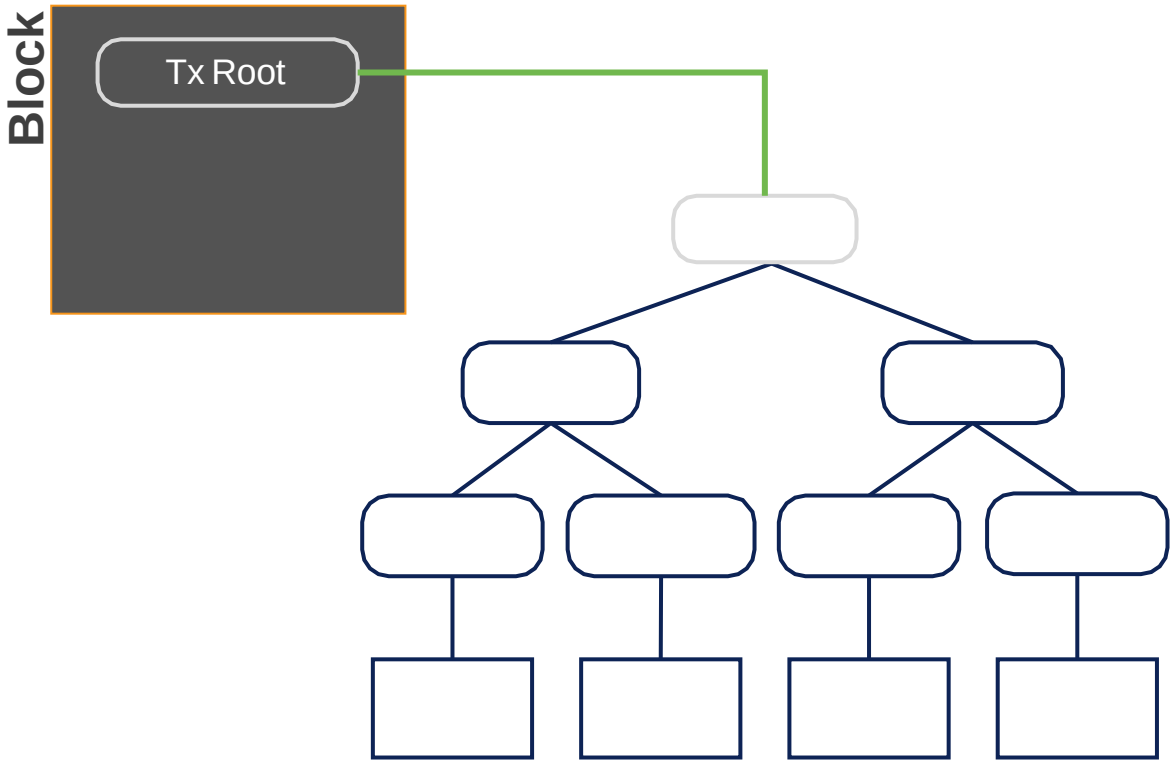


Merkle Trees are cool!

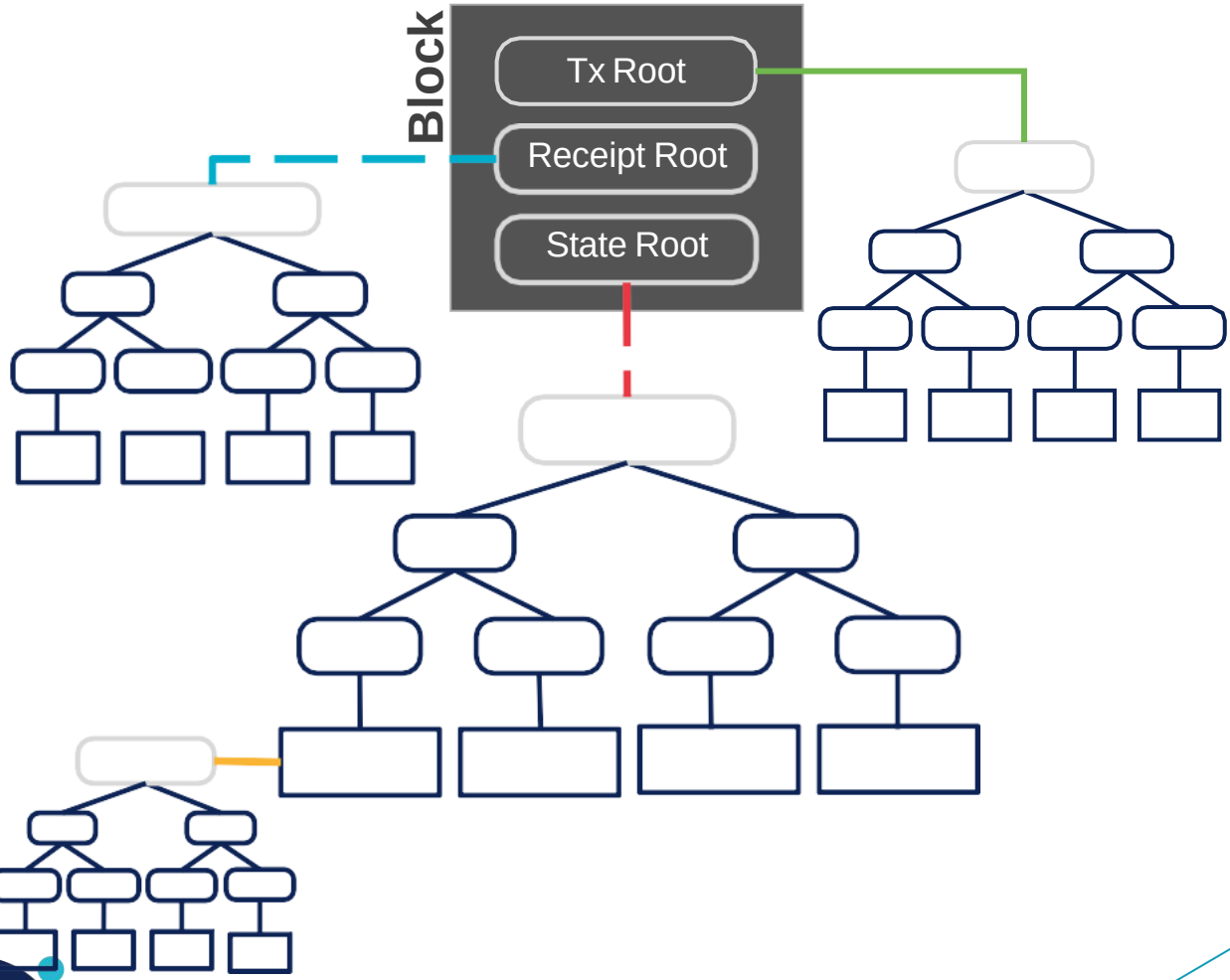
- **Performant**
- **Light Client Friendly**
- Only re-hash what changed!
  Easy to prove a transaction without downloading the whole tree!

WHERE ARE MERKLE TREES USED?

Bitcoin

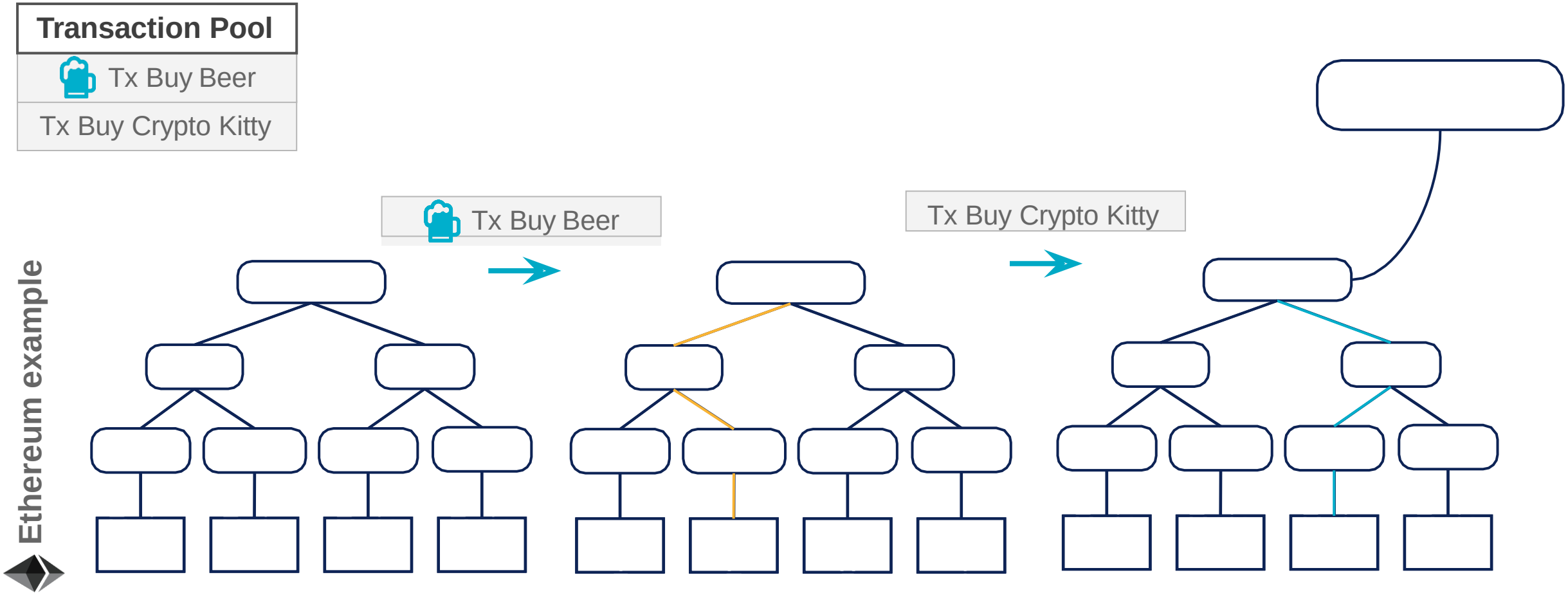


Ethereum

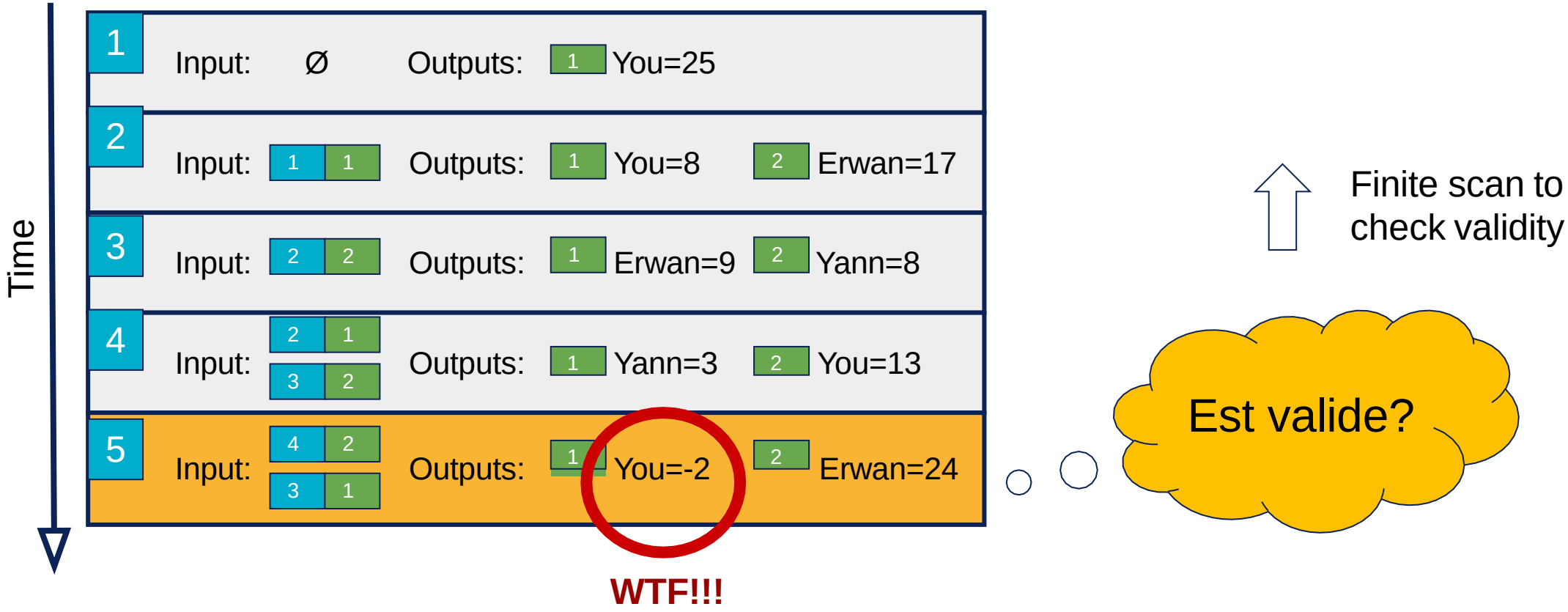


BACK TO TRANSACTIONS EXECUTION

Transactions are **executed sequentially** by nodes

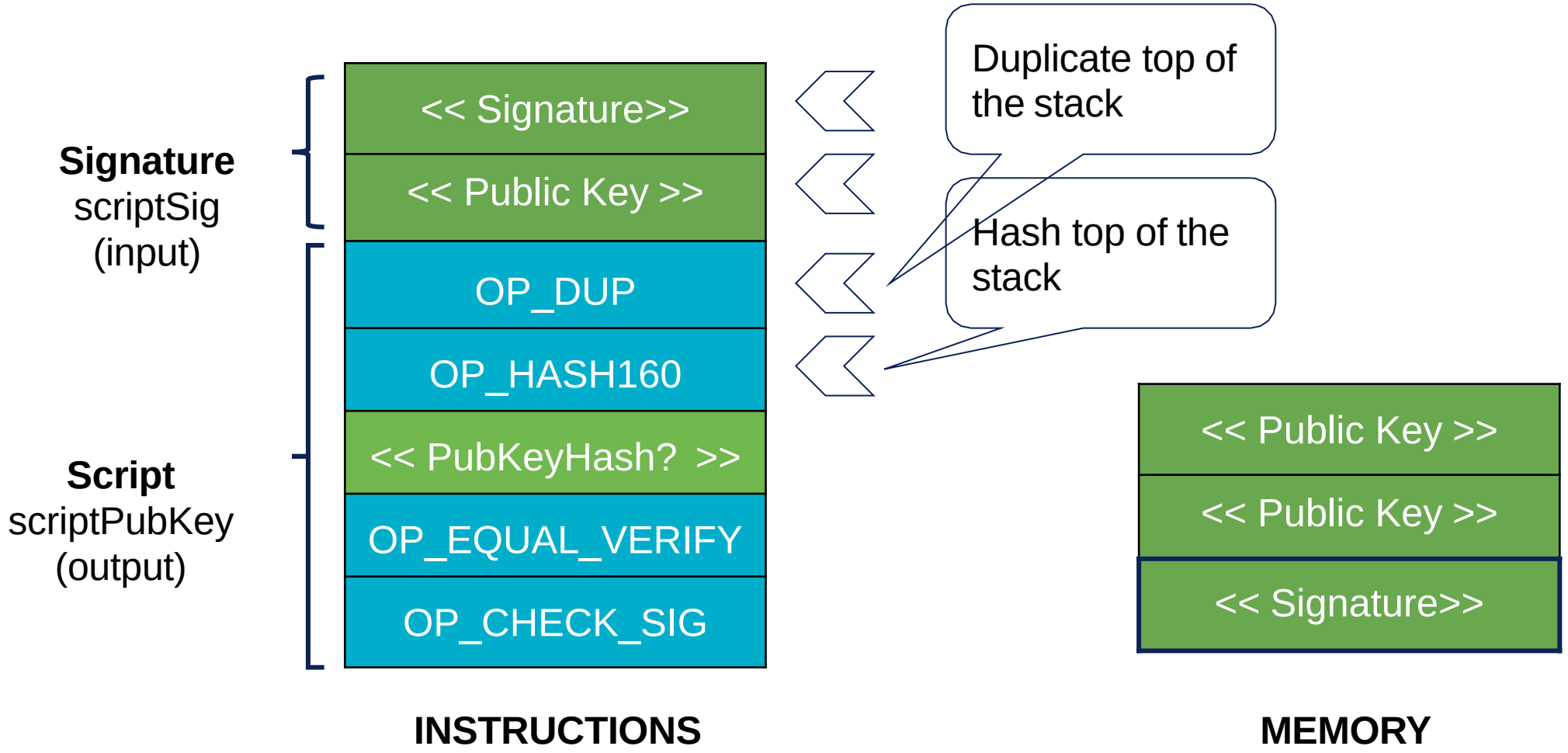


UN GRAND LIVRE BASÉ SUR LES TRANSACTIONS COMME BITCOIN



YOU ARE (often) PSEUDONYMOUS NOT ANONYMOUS

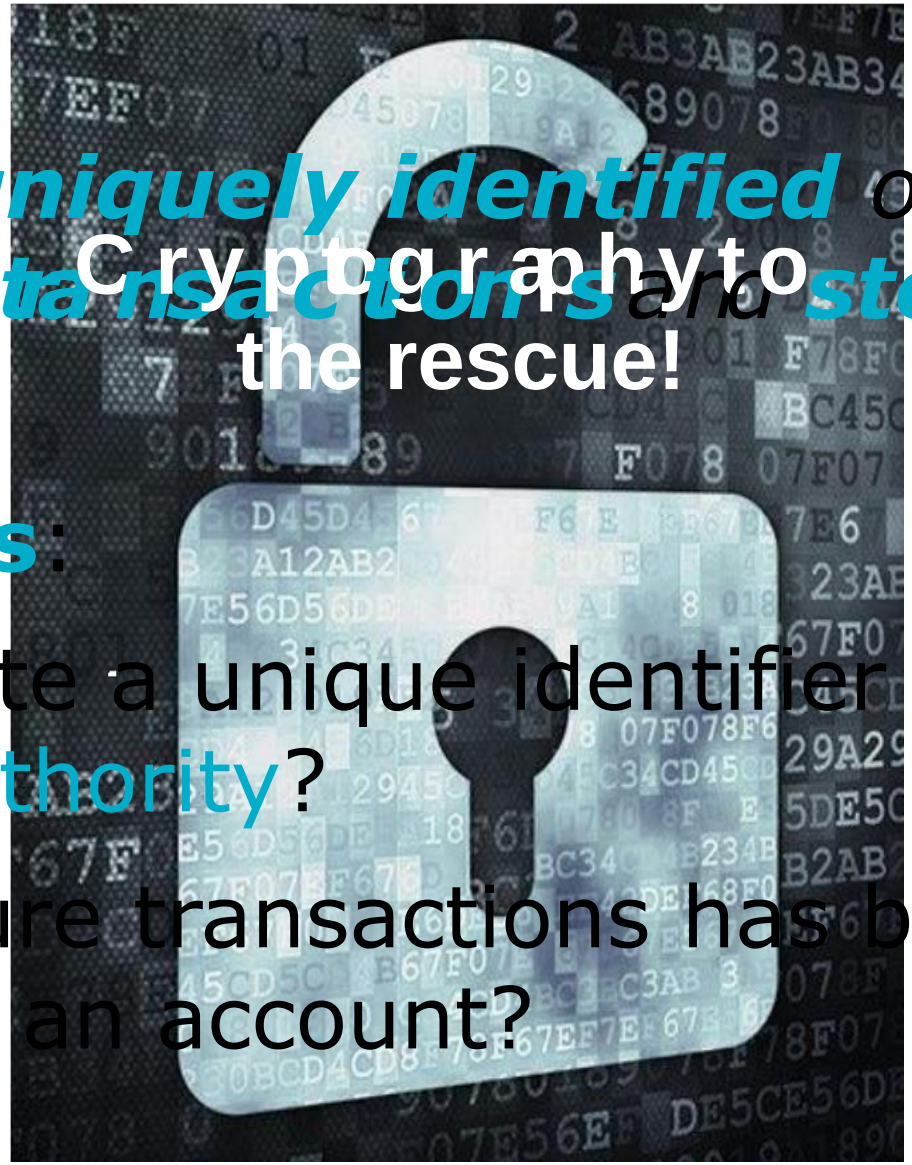
BITCOIN SCRIPT EXECUTION, A REAL LIFE EXAMPLE



Check Transaction signature script!
99% of created transactions in bitcoin are using this script!

WHAT IS AN ACCOUNT?

*An account is a **uniquely identified** object that will be able to **issue transactions** and **store currency***



Two problems:

- how to create a unique identifier without a central authority?
- how to ensure transactions has been legitimely issued from an account?

The electricity costs to mine 1 Bitcoin worldwide in US dollars

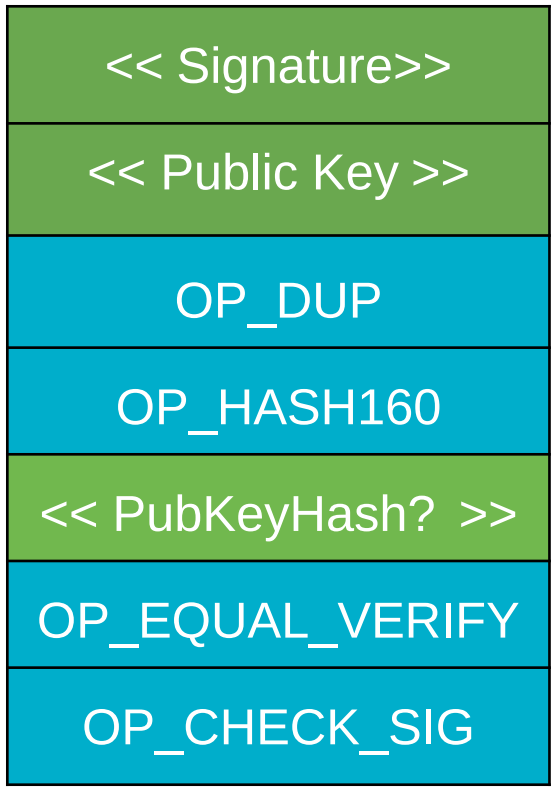
By Dieter Holger for Bitcoinist

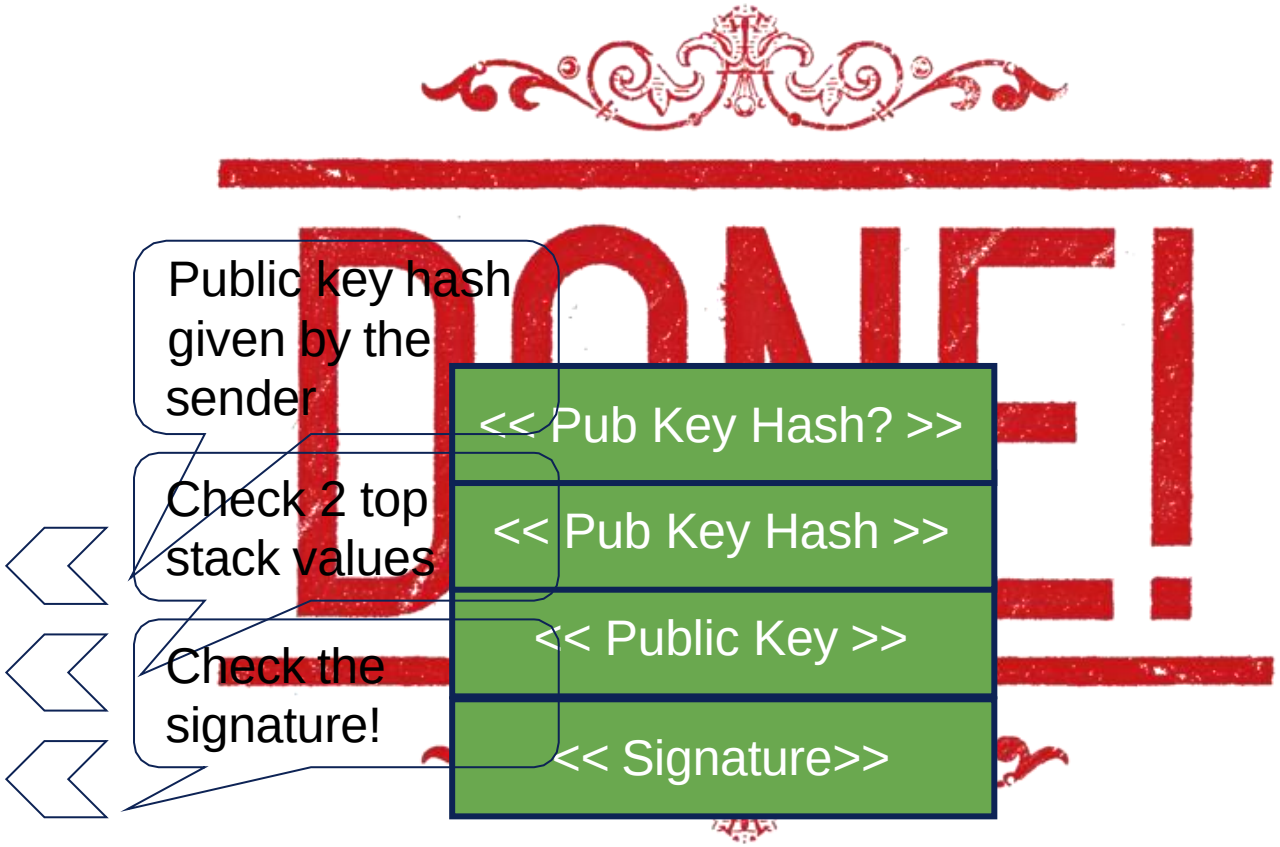
Source: Elite Fixtures

BITCOIN SCRIPT EXECUTION, A REAL LIFE EXAMPLE

Signature
scriptSig
(input)

Script
scriptPubKey
(output)





INSTRUCTIONS **MEMORY**

Check Transaction signature script!
99% of created transactions in bitcoin are using this script!


Lifecycle of a transaction:
Some definitions first!
FRIENDS
Transaction confirmation
Mining process
Transaction execution
Transaction submission
Transaction preparation
Account creation

QUE FAIT UN MINEUR ?

1. **Collect transactions** from the pool
2. **Validate** transactions
3. Invest **power and electricity**!
4. Try to **create a new block** as previously described
5. Eventually, **get rewards** in form of **new created bitcoins**

*A crypto-currency is a **virtual currency** that uses **cryptography** to guarantee currency **essential properties***

WHAT IS A LEDGER?

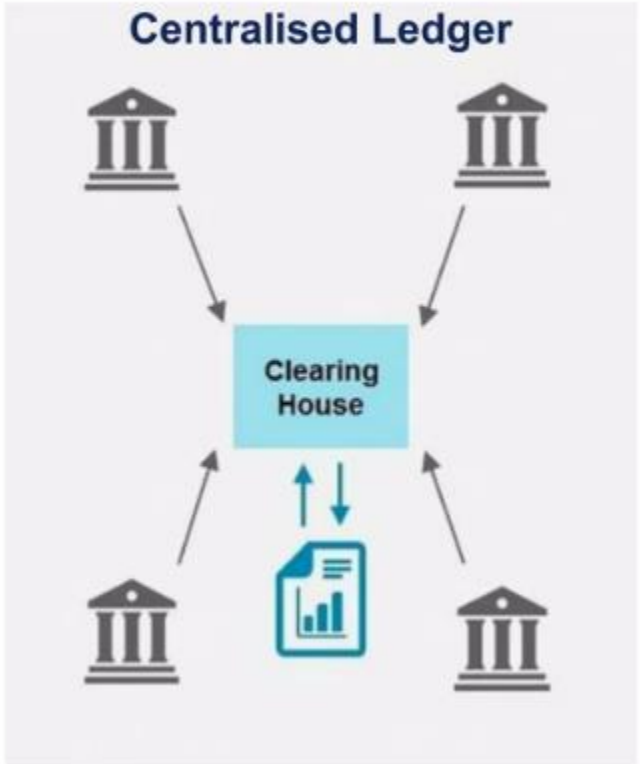
Date	Description	Credit	Debit	Balance
2/20/2011	Alice to Bob	-$10		$90
2/20/2011	Bob from Alice		+$10	$10
3/20/2011	Bob to Eve	-$5		$5

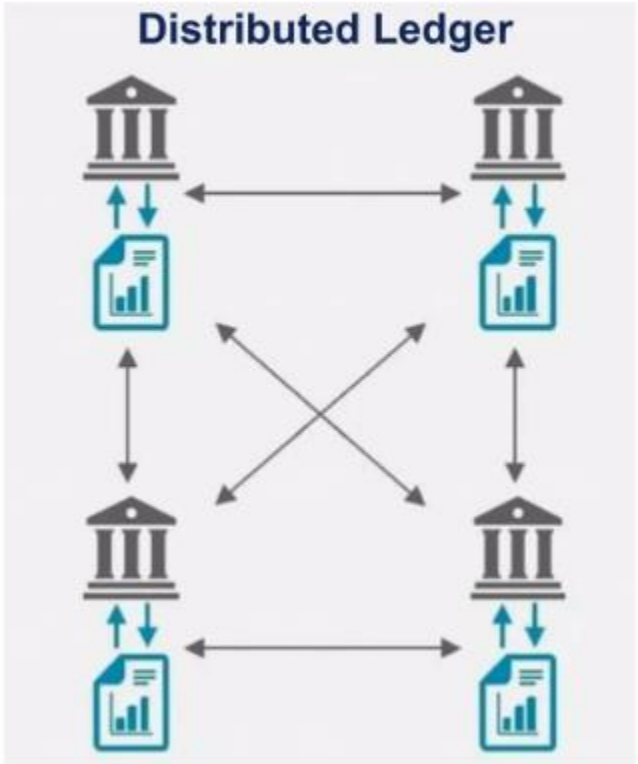
Not a very new thing !

Early 19th-century German ledger

SOME FAMOUS CRYPTO-CURRENCIES

WHAT IS A DISTRIBUTED LEDGER?





WHAT IS A BLOCKCHAIN?

A blockchain is
one of the possible implementations
of a distributed ledger

where transactions are stored
in a series of ***cryptography-linked blocks***

WHAT IS AN ACCOUNT?

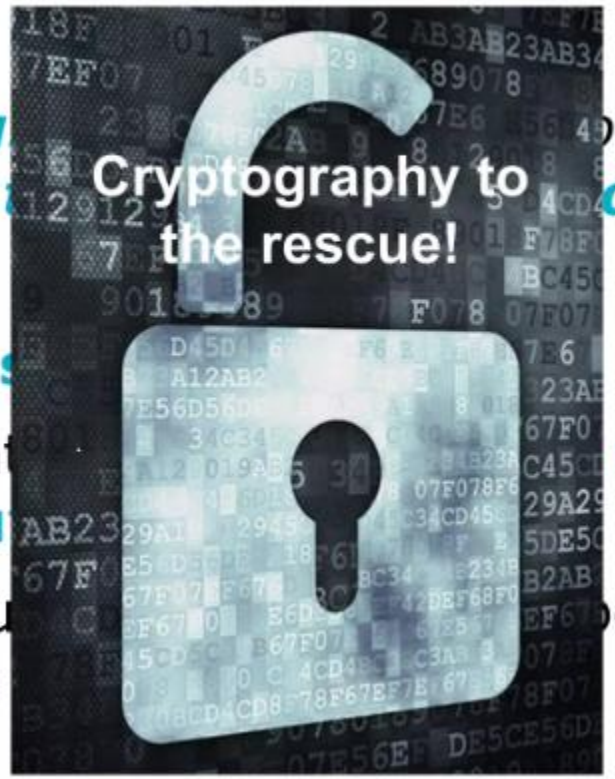
*An account is a **uniquely identified** object that will be able to **issue transactions** and **store currency***

Two problems:

- how to create a unique identifier without a central authority?
- how to ensure transactions has been legitimely issued from an account?

WHAT IS AN ACCOUNT?

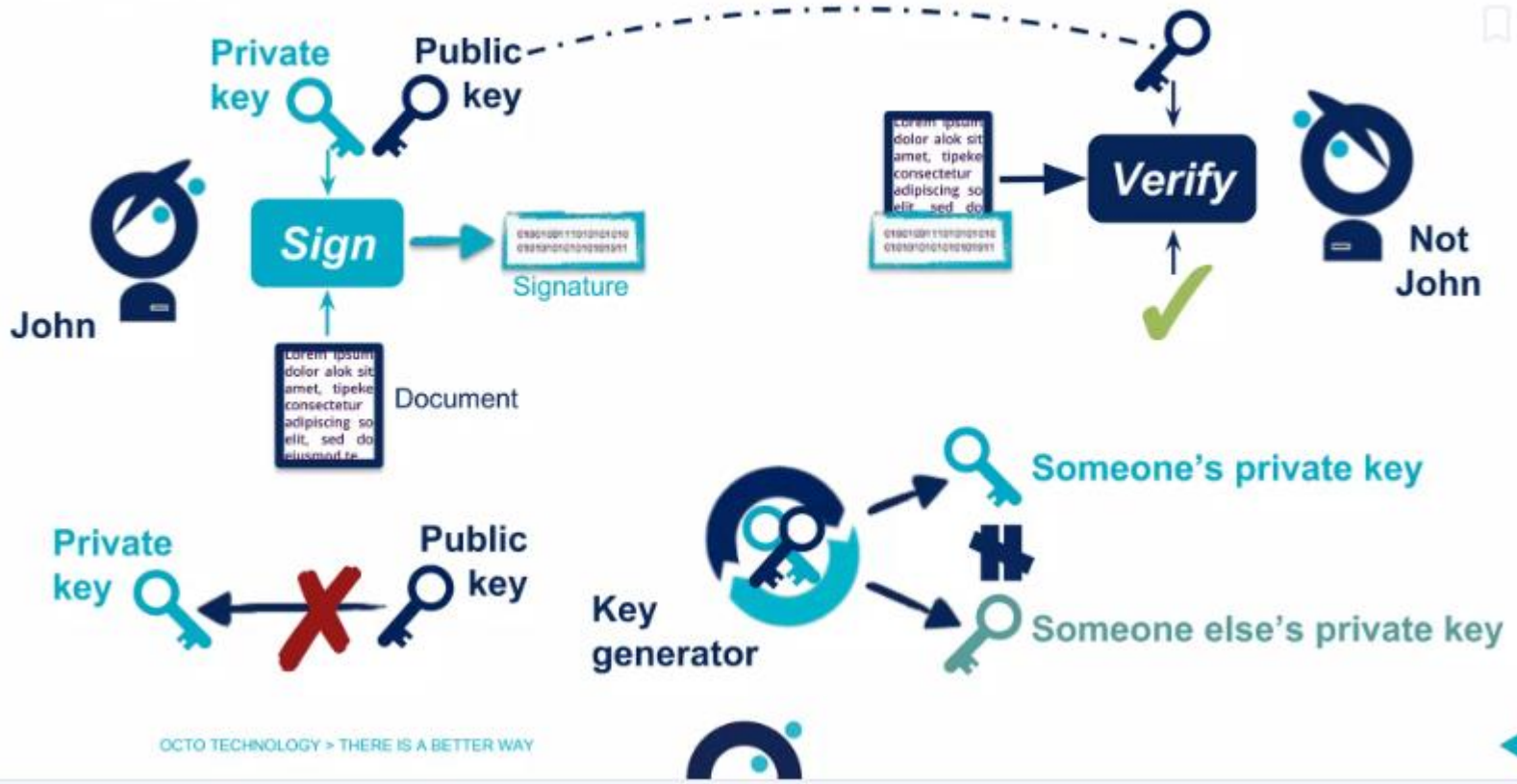
An account is a u *bject that will be able to issue* *ore currency*



Two problems

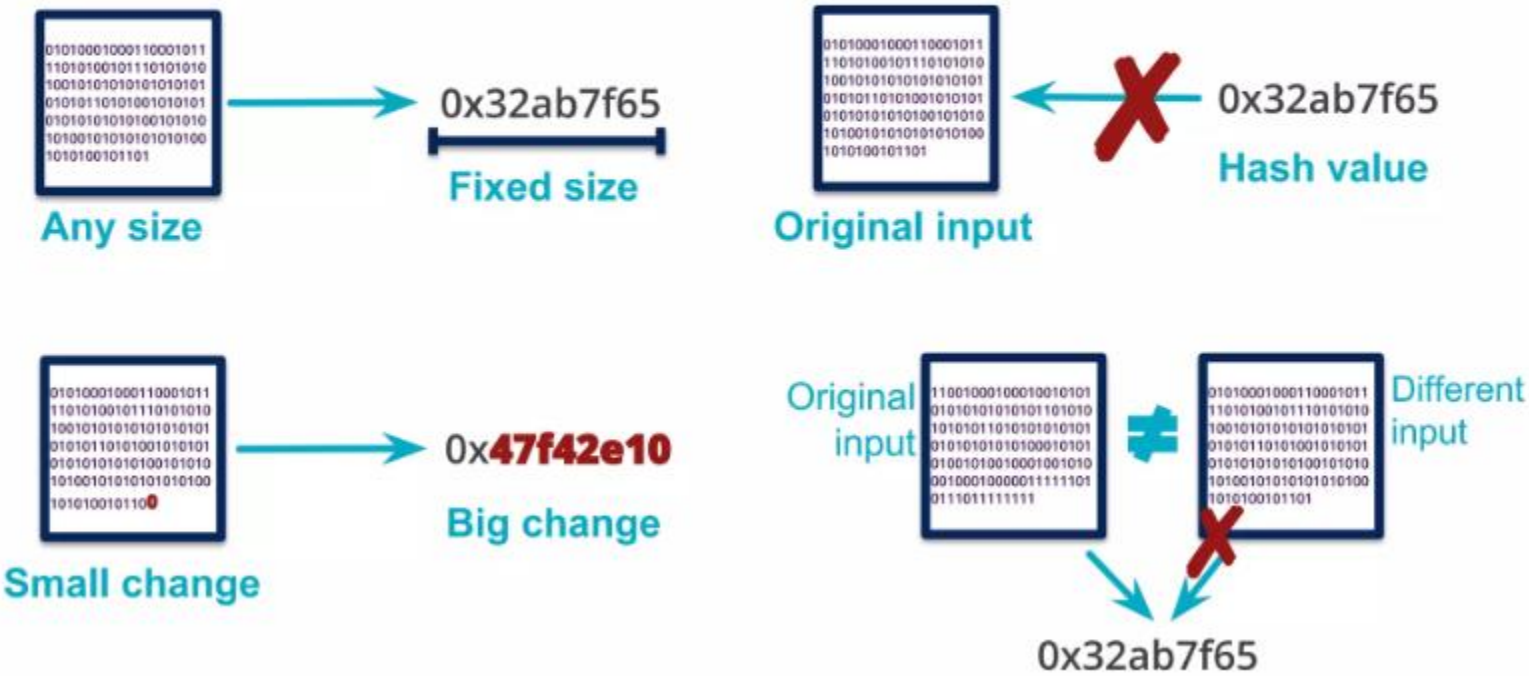
- how to creat without a central au
- how to ensu een legitimely issued from

CRYPTOGRAPHY 101: ELECTRONIC SIGNATURE
IN ONE SLIDE



CRYPTOGRAPHY 101: CRYPTOGRAPHIC HASH FUNCTION

IN ONE SLIDE



ACCOUNT CREATION: STANDARD MECHANISM

1. Key generation

Most blockchain use
Elliptic Curve Algorithms

2. Public Key Hashing

Ensure shorter address

Protect against attack
on Public key

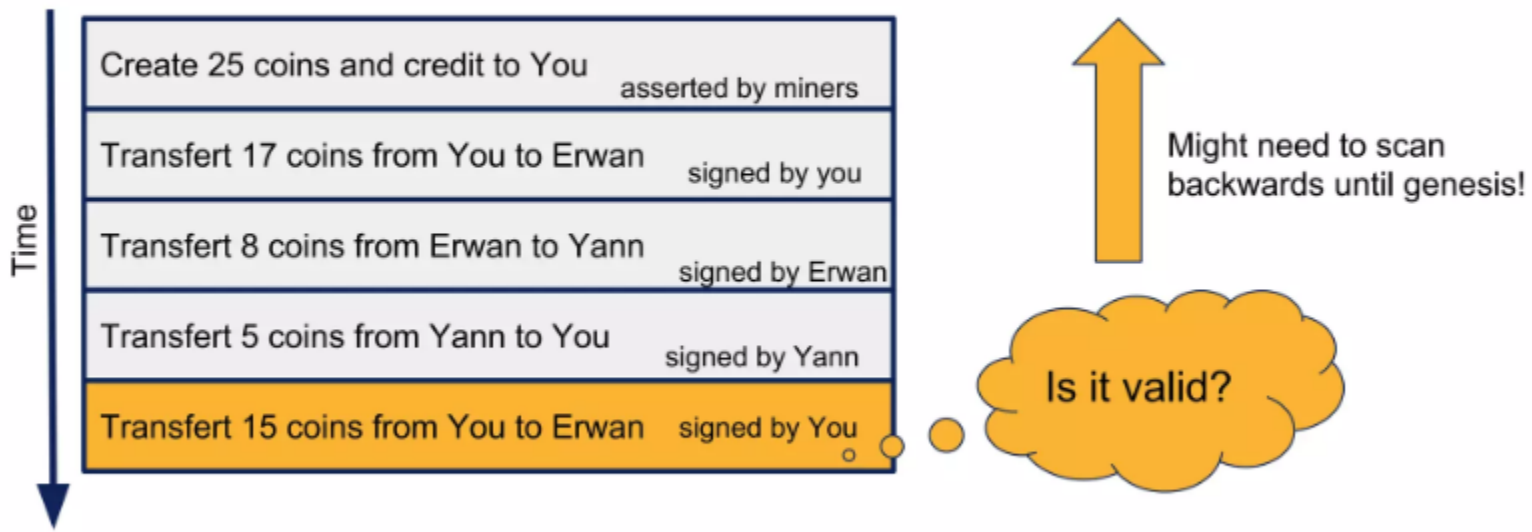
3. Address Encoding

Make it (a bit more)
readable

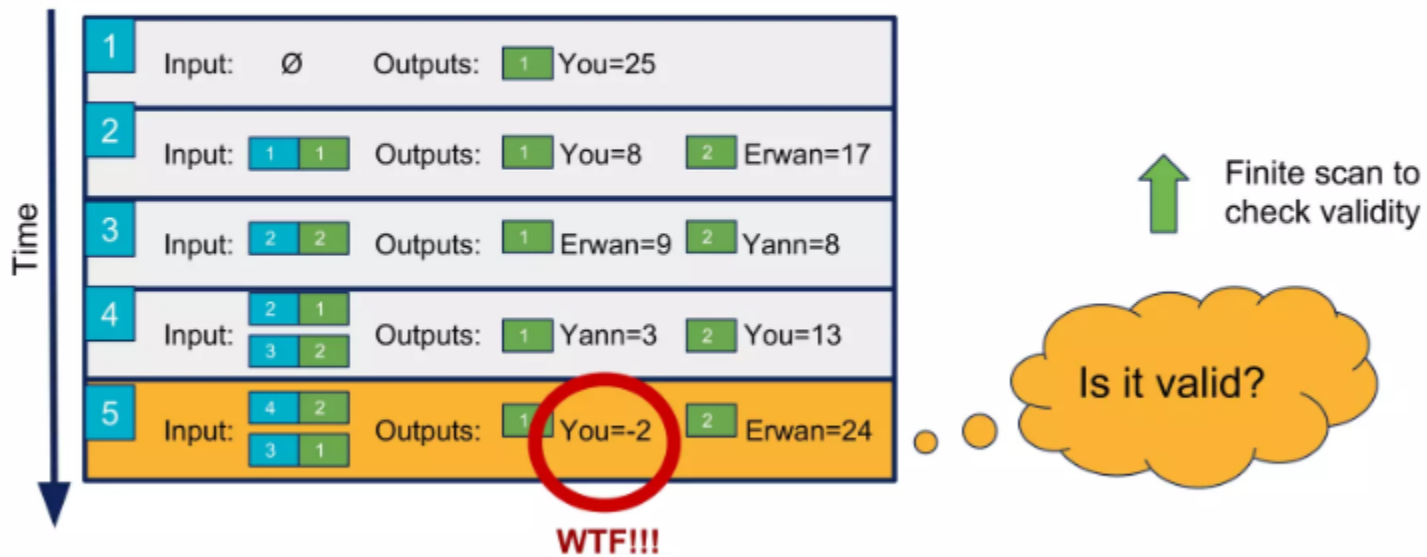

Lifecycle of a transaction:
Transaction preparation
FRIENDS
Transaction confirmation
Mining process
Transaction execution
Transaction submission
Transaction preparation
Account creation

WHAT IS A TRANSACTION

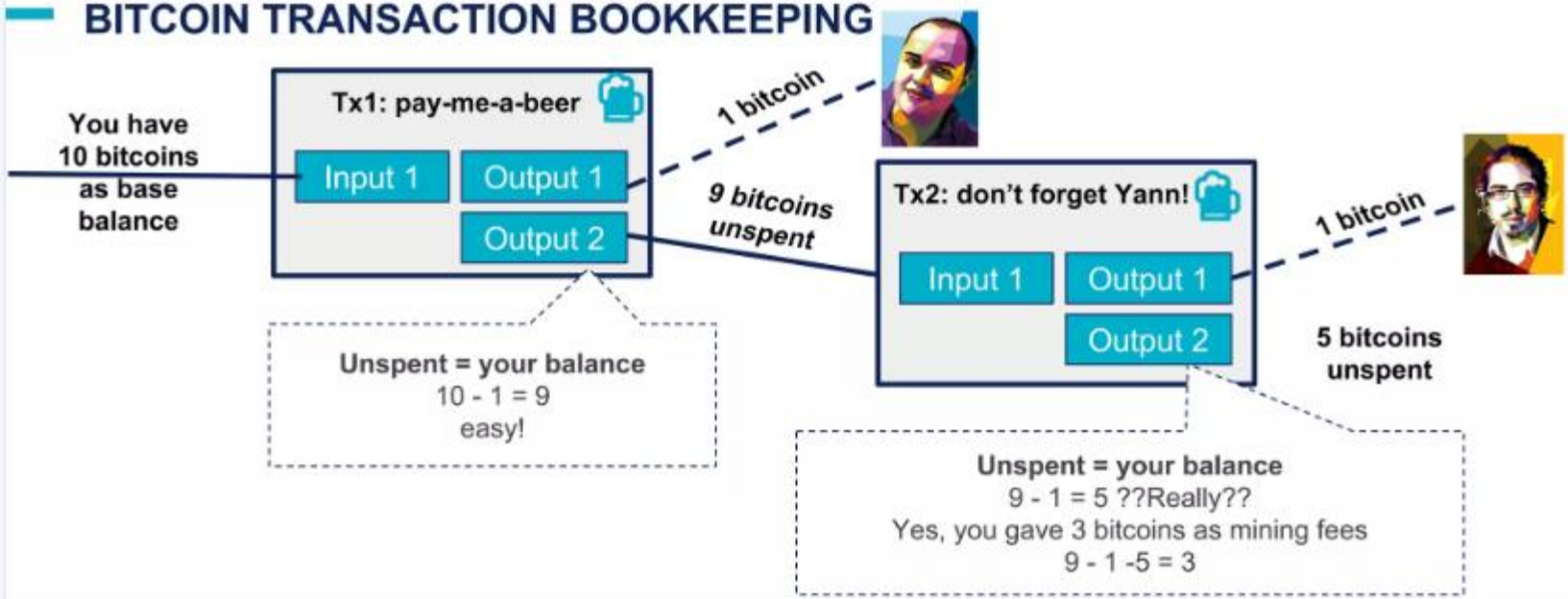
APPEND-ONLY LEDGER



A TRANSACTION-BASED LEDGER LIKE BITCOIN



BITCOIN TRANSACTION BOOKKEEPING

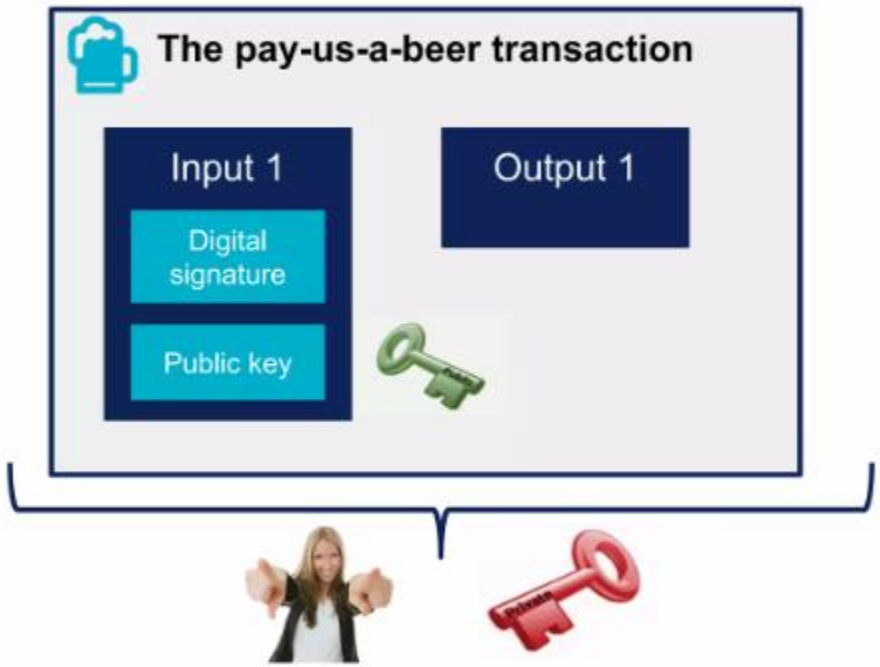


Inputs Bitcoins to spend	Each input is a signed reference from a previous trnx
Outputs Assign to new owners	Each output can be used by only 1 input do avoid double spend

Unspent outputs = balance of somebody
This is what we call bitcoins (add all unspent of a public ledger to know how many bitcoins has the chain

Mining fees
sum(inputs) - sum(outputs)

TRANSACTION SIGNATURE



1. You are paying the beer, so **you have to sign** your transaction with **your private key**
2. You have to attach the **the signature** and **your public key** to the transaction so anybody can check it

This process can be done offline!

OK OK, BUT WHAT ARE THE TRANSACTION SCRIPT YOU WERE TALKING ABOUT

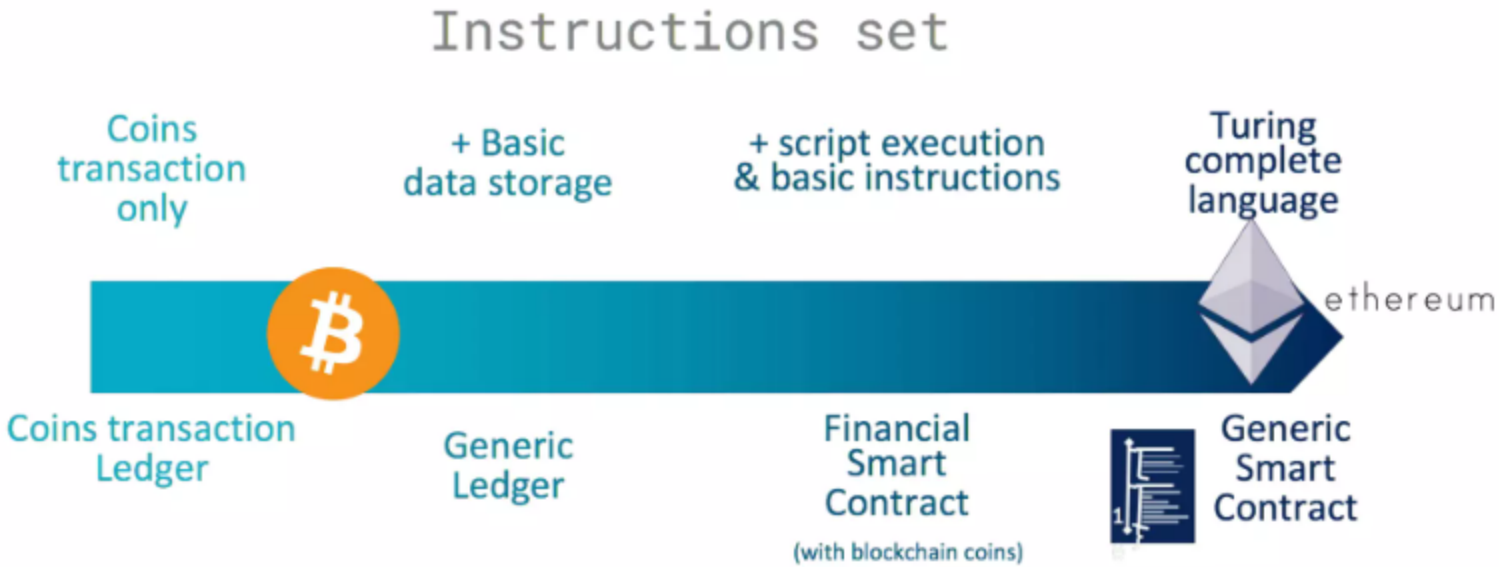
Sender choose the script
(but could be refused)

ByteCode running in a
Virtual Machine

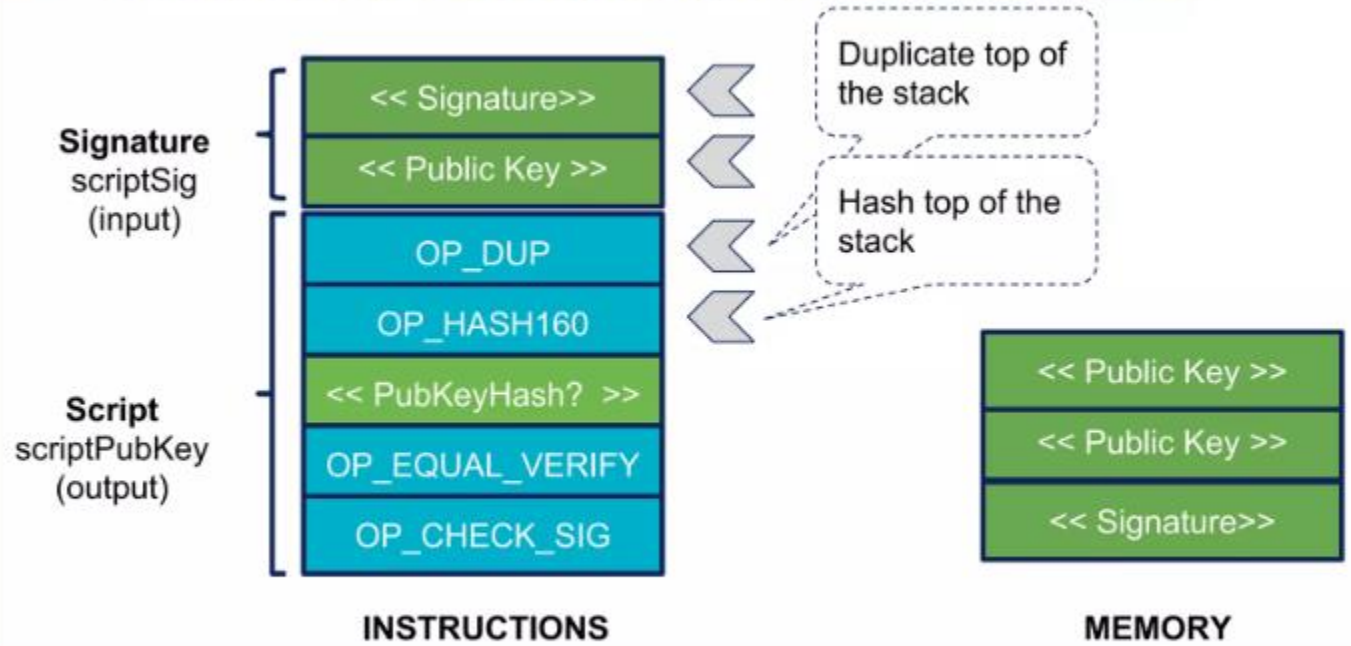
Often limited instructions set
No-Loops in bitcoin

Bitcoin is using a stack
based language

SCRIPTING CAPABILITIES ARE DIFFERENT FROM ONE BLOCKCHAIN TO ANOTHER!

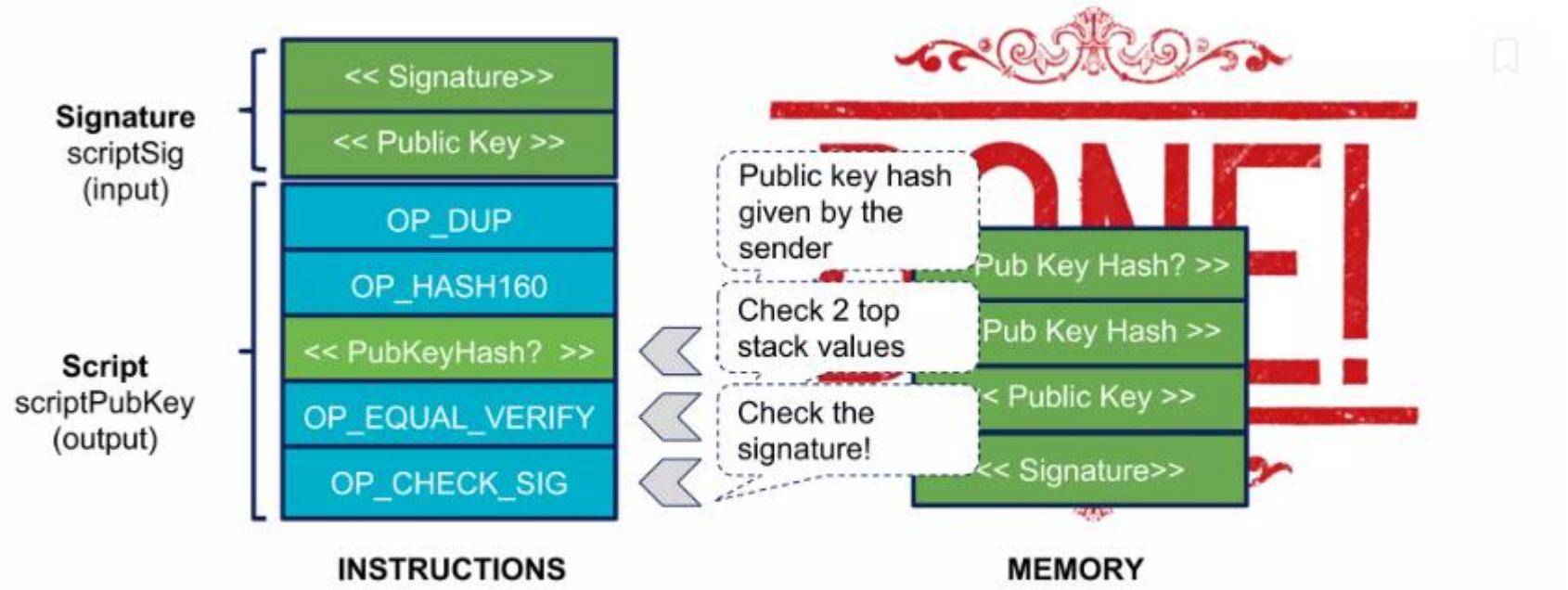


BITCOIN SCRIPT EXECUTION, A REAL LIFE EXAMPLE



Check Transaction signature script!
99% of created transactions in bitcoin are using this script!

BITCOIN SCRIPT EXECUTION, A REAL LIFE EXAMPLE



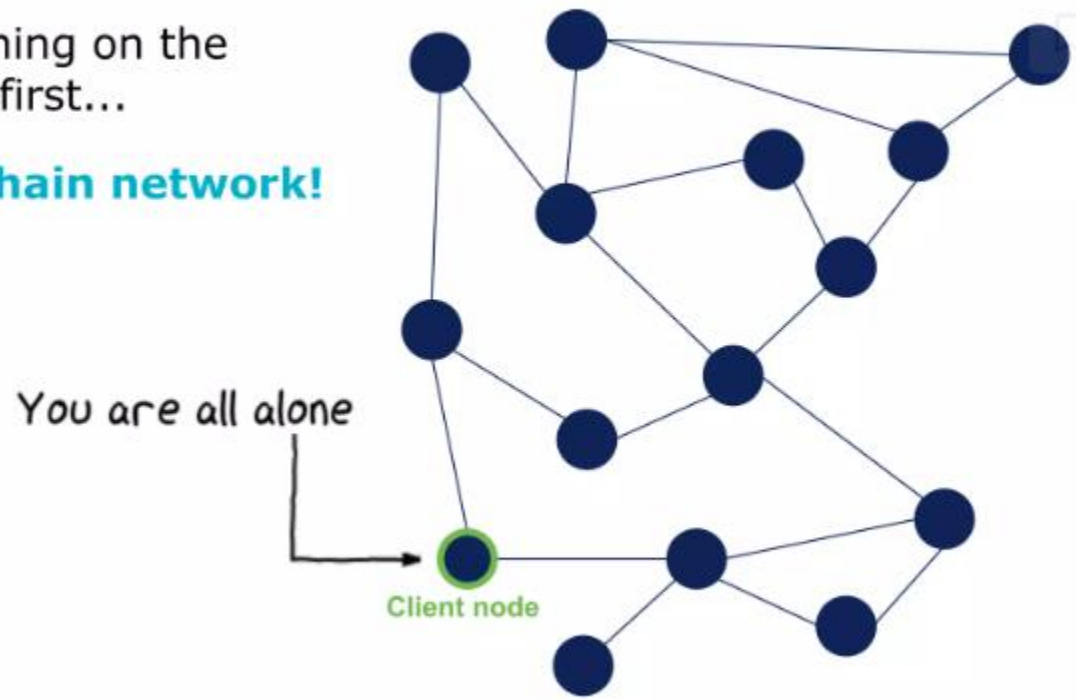
Check Transaction signature script!
99% of created transactions in bitcoin are using this script!


Lifecycle of a transaction:
Transaction submission
FRIENDS
Transaction confirmation
Mining process
Transaction execution
Transaction submission
Transaction preparation
Account creation

FIRST STEP: FIND YOUR FRIENDS

To be able to do anything on the blockchain, you must first...

Discover the blockchain network!

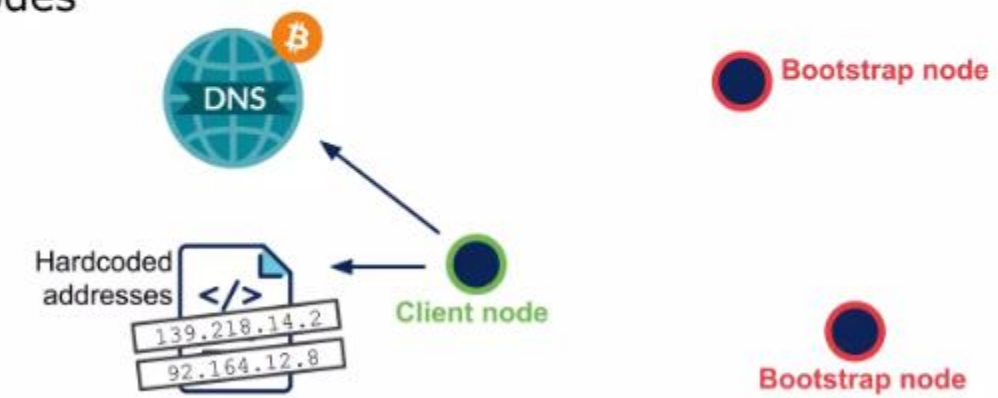


FIRST STEP: FIND YOUR FRIENDS

To be able to do anything on the blockchain, you must first...

Discover the blockchain network!

1. Find Bootstrap nodes

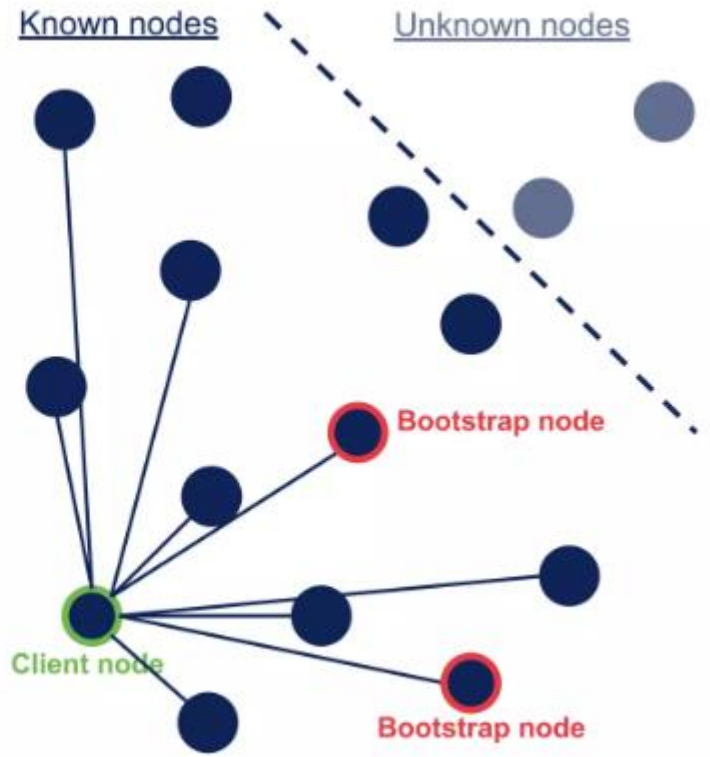


FIRST STEP: FIND YOUR FRIENDS

To be able to do anything on the blockchain, you must first...

Discover the blockchain network!

1. Find Bootstrap nodes
2. Find Peer nodes



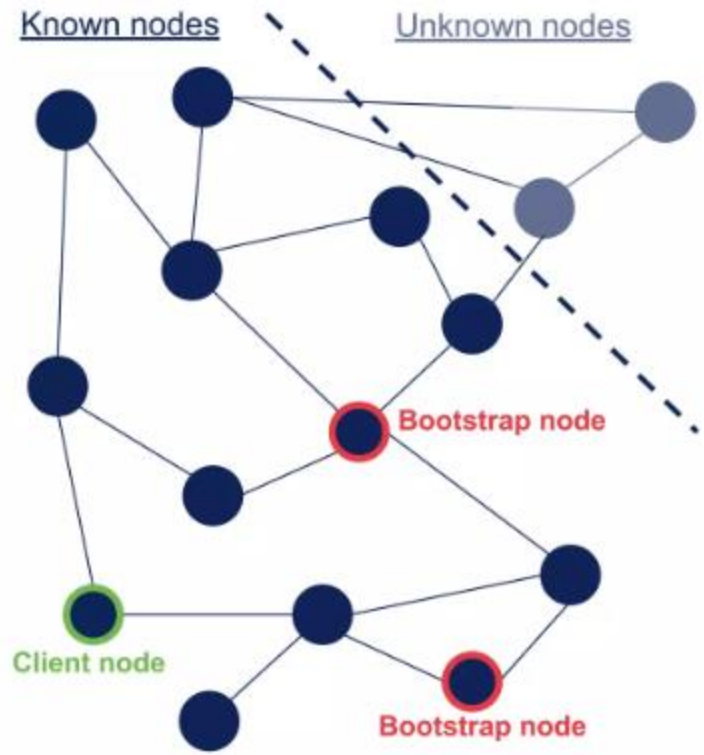
FIRST STEP: FIND YOUR FRIENDS

To be able to do anything on the blockchain, you must first...

Discover the blockchain network!

1. Find Bootstrap nodes
2. Find Peer nodes
3. Connect to random nodes

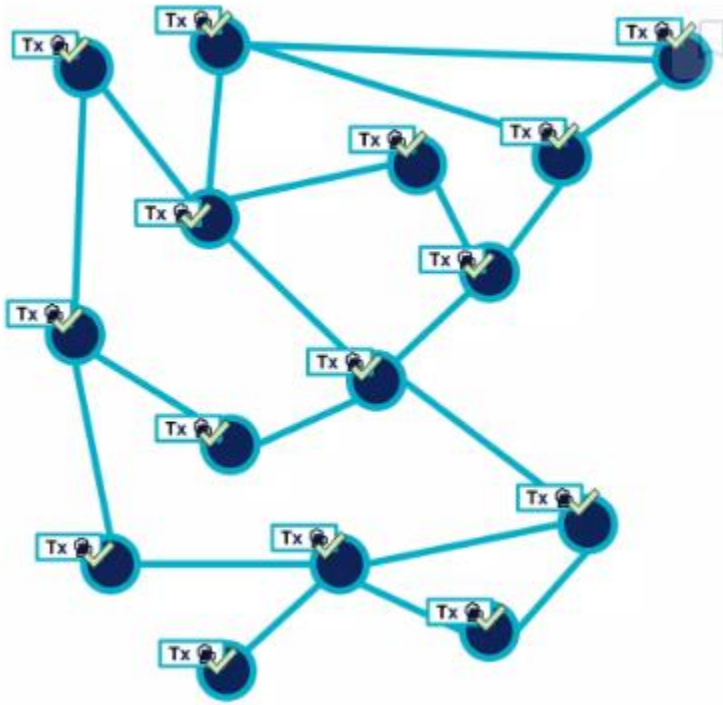
The whole network is eventually interconnected



SECOND STEP: GOSSIP WITH YOUR FRIENDS

Principle

Just forward every transaction to your neighbours!



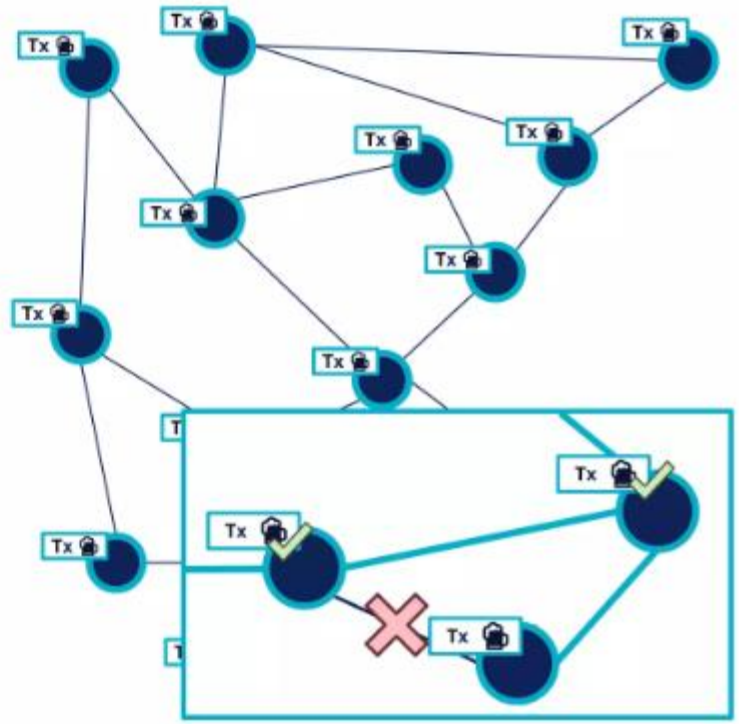
SECOND STEP: GOSSIP WITH YOUR FRIENDS

Principle

Just forward every transaction to your neighbours!

Why it is cool?

- **Reliable** in case of failure



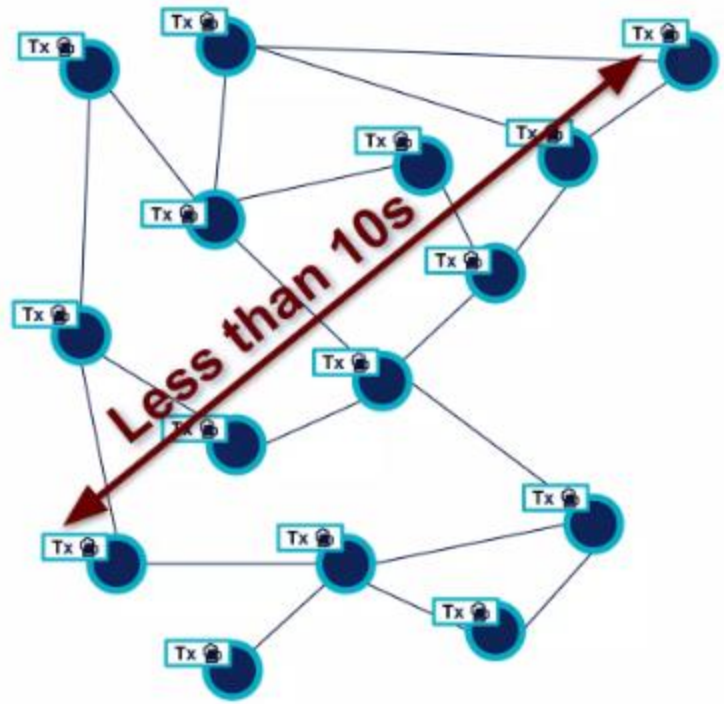
SECOND STEP: GOSSIP WITH YOUR FRIENDS

Principle

Just forward every transaction to your neighbours!

Why it is cool?

- **Reliable** in case of failure
- **Guaranteed delivery** in bounded time



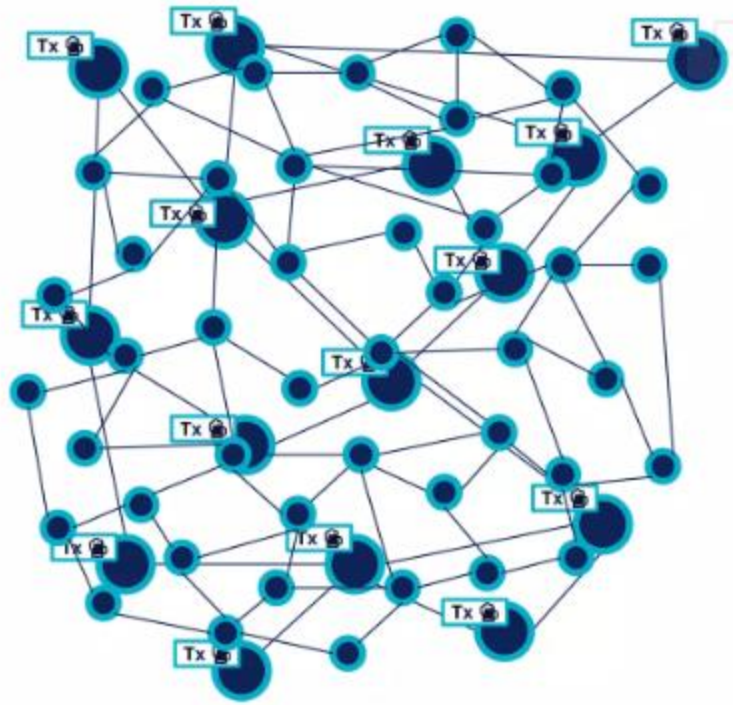
SECOND STEP: GOSSIP WITH YOUR FRIENDS

Principle

Just forward every transaction to your neighbours!

Why it is cool?

- **Reliable** in case of failure
- **Guaranteed delivery** in bounded time
- **Scale** with the number of peers



BAD TRANSACTIONS SHALL NOT PASS!

Transaction validity **is first checked** before being accepted and transferred

There should be a **consensus about validation rules** among clients

Validation rules updates are **propagated through software updates**

LET'S GO TO THE POOL!

Accepted transactions go into a **transaction pool independently** maintained by each node

Transaction Pool

Transactions	Fee
Pay-us-a-beer	30
Buy Crypto Kitty	25
Buy ICO Scam Token	12
Buy ICO Scam Token	7
Buy ICO Scam Token	0

Ordered by fee

Mining node A

Transaction Pool

Transactions	Fee
Buy Crypto Kitty	25
Buy ICO Scam Token	12
Buy ICO Scam Token	7
Buy Drugs	2
Buy ICO Scam Token	0

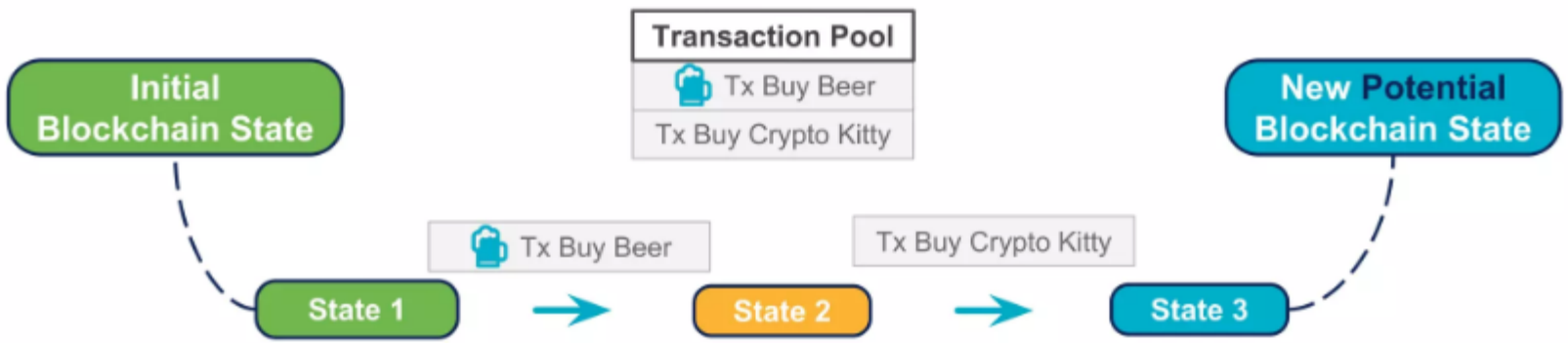
Non consistent view across all nodes

Mining node B


Lifecycle of a transaction:
Mining process
FRIENDS
Transaction confirmation
Mining process
Transaction execution
Transaction submission
Transaction preparation
Account creation

A SIMPLE EXECUTION MODEL

Transactions are just **state transition functions**...



...that are **executed sequentially**

BUT WHAT IS A BLOCKCHAIN STATE?

It depends...

Bitcoin State

Unspent transactions coins

- **20 coins spendable by Bob**
- 10 coins spendable by John
- **5 coins spendable by Bob**
- 5 coins spendable by Lucie

Ethereum State

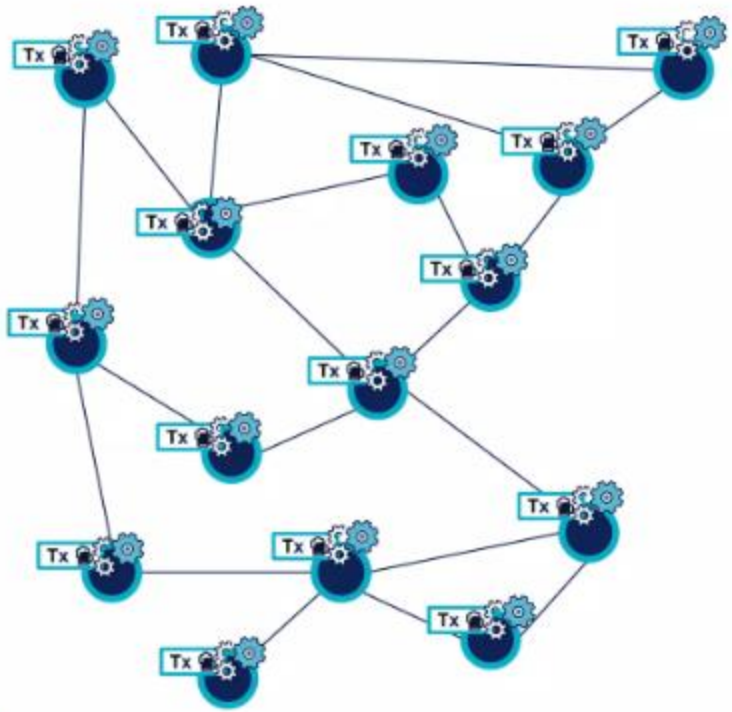
Account information

- **Bob has 25 coins**
- John has 10 coins
- Lucie has 5 coins
- Contract Foo contains A=10

A MODEL NOT VERY SCALABLE

All nodes execute
all the transactions

Adding new nodes
doesn't increase computing power



PROTECTIONS AGAINST THE EVIL

Threat 1 | **Infinite loop** in transaction scripts

Solution

No Loop or Goto in script langage

Pay for each instruction execution

Threat 2 | Transaction **Replay attack**

Solution

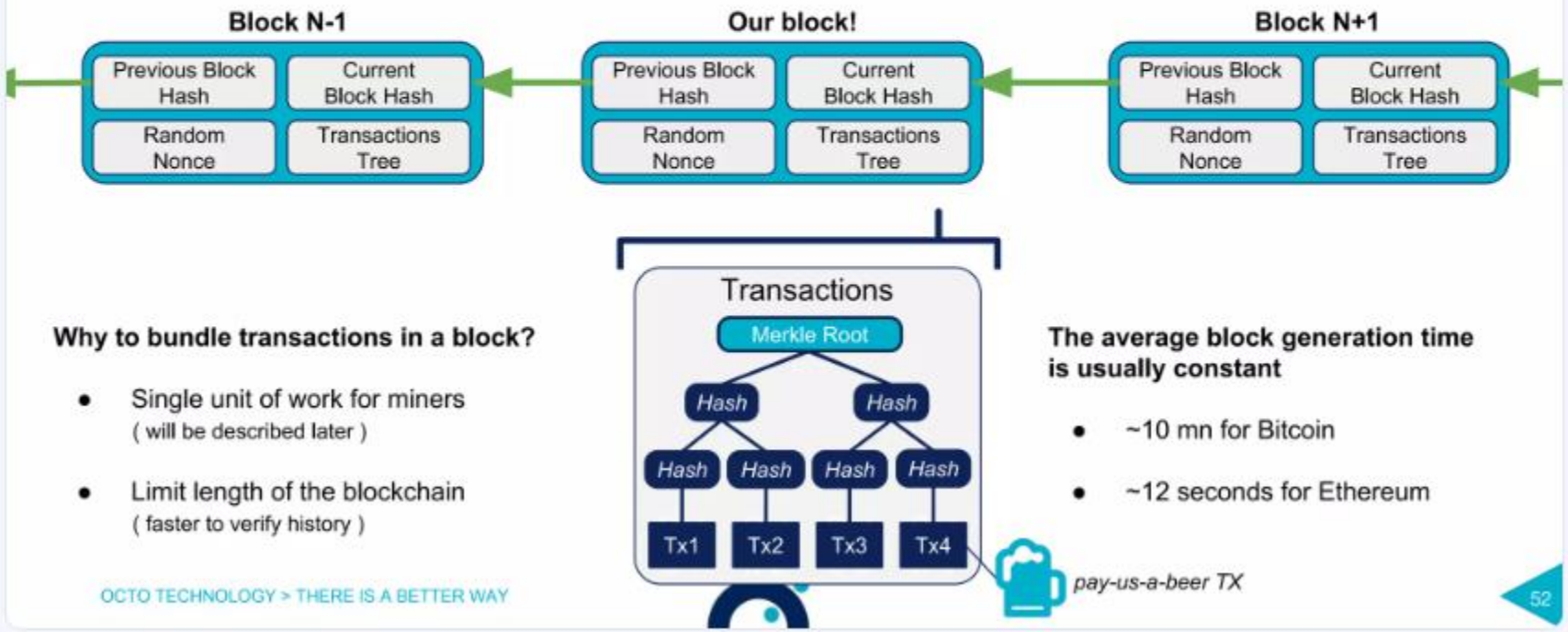
Transaction chaining

Incremental id per transaction/account


Lifecycle of a transaction:
Block propagation
FRIENDS
Transaction confirmation
Mining process
Transaction execution
Transaction submission
Transaction preparation
Account creation

DID WE SAY BLOCKCHAIN? WHAT IS IT?

Now that our pay-us-a-beer transaction is executed and validated,
it needs to be **included** in a **newly created block**



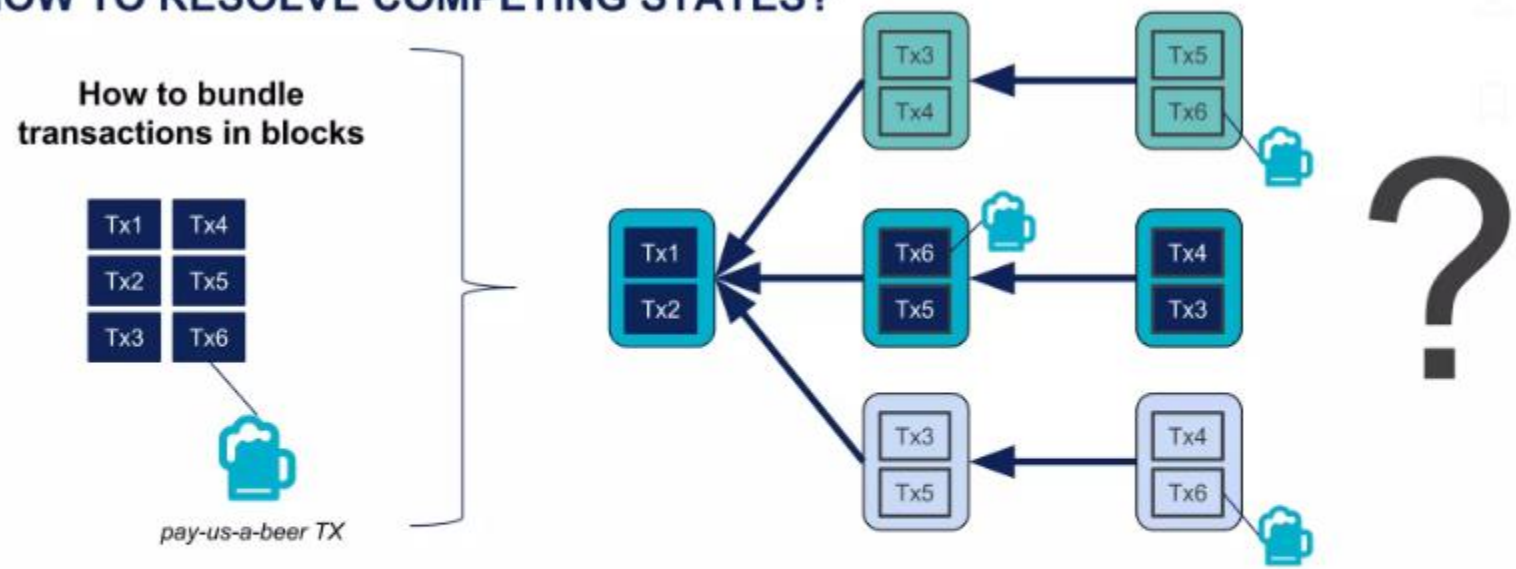
Why to bundle transactions in a block?

- Single unit of work for miners
  (will be described later)
- Limit length of the blockchain
  (faster to verify history)

The average block generation time is usually constant

- ~10 mn for Bitcoin
- ~12 seconds for Ethereum

HOW TO RESOLVE COMPETING STATES?



Distributed process =
need to arbitrate between **several valid states**

CONSENSUS ALGORITHM

" How to find a truth, in a world full of liars "

- **Agree on a unique blockchain state** amongst all valid possibilities
- **Prevent bad actors from influencing the outcome**
- **Ensure a consensus will be eventually reached** despite faulty and evil nodes

Solution = Mining!

2 main answers to avoid those attacks

- Choose the **next** block producer **randomly!**
- Ensure **messing** with the blockchain **is not for free**

PROOF OF WORK, THE MOST COMMON MINING TECHNIQUE

A **computational challenge** must be solved

to be able to create a valid block

Challenge: **Find** a **random hash** value inferior to a threshold (difficulty)

hash(**block** + **random value**) < **difficulty**

Bitcoin case

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

Difficulty is regularly adjusted to keep a **constant average block generation time**

RESOLVING FORKS

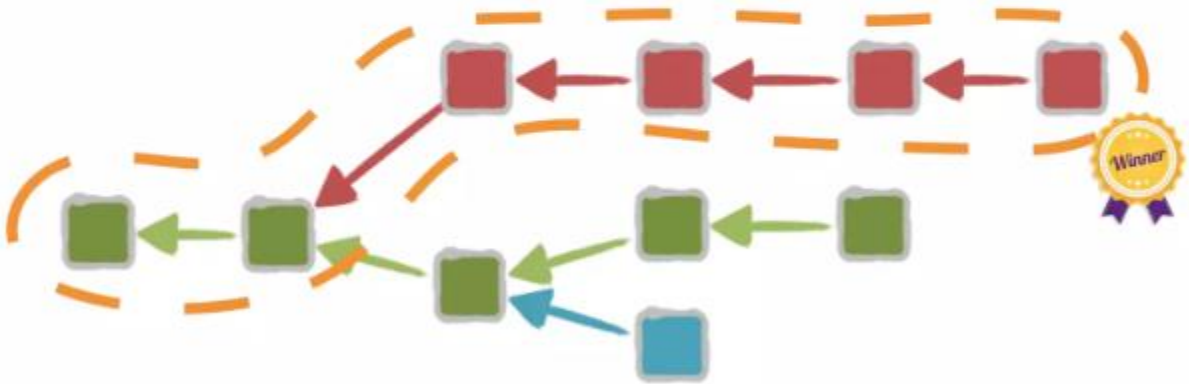
What happen when **2 miners** find a block at **the same time**?

RESOLVING FORKS

What happen when **2 miners** find a block at **the same time**?

The process continues and

`The longest blockchains wins !`



WHAT A MINER IS DOING?

1. **Collect transactions** from the pool
2. **Validate** transactions
3. Invest **power and electricity**!
4. Try to **create a new block** as previously described
5. Eventually, **get rewards** in form of **new created bitcoins**

The electricity costs to mine 1 Bitcoin worldwide in US dollars

By Dieter Holger for Bitcoinist

Source: Elite Fixtures


Lifecycle of a transaction:
Transaction confirmation
FRIENDS
Transaction confirmation
Mining process
Transaction execution
Transaction submission
Transaction preparation
Account creation

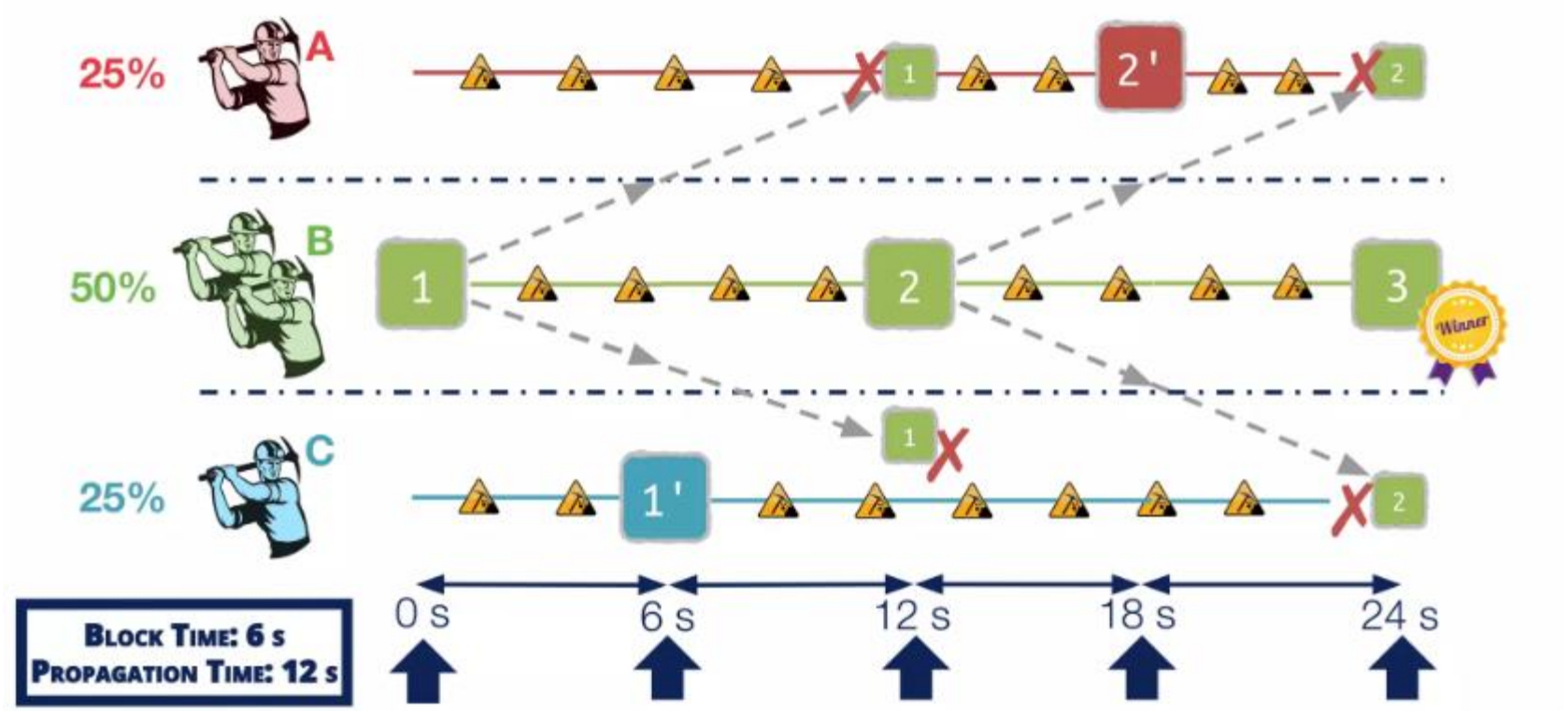
BEFORE: THE (NOT SO SIMPLE) BLOCK PROPAGATION

- Like transactions, blocks are propagated in the network using the **Gossip protocol**

- On Bitcoin | **50%** of blocks are propagated **under 6s**
  but **10%** are often propagated **> 120s**

Problem: High propagation time is **bad for security**

IMPACT OF A SMALL BLOCK TIME



CENTRALISATION COUNTER-MEASURES

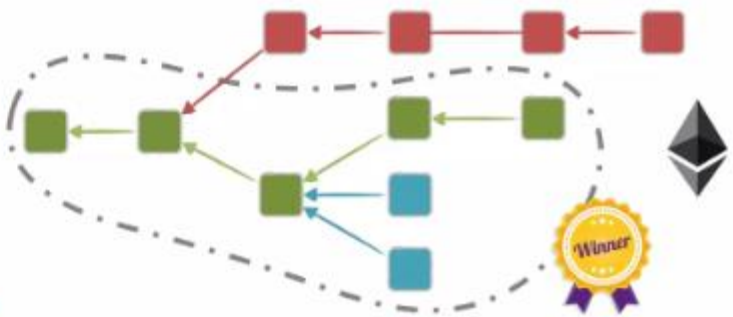
CENTRALISATION COUNTER-MEASURES

High propagation time lead to **centralisation**

Solutions:

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

- Make **orphan blocks count** to select winner



THE TRANSACTION CONFIRMATION ISSUE

- **Problem:** blockchain are **eventually consistent**

- **Transactions can be re-organized in the short term** as part of forks resolution

HOW TO BE SURE ABOUT YOUR TRANSACTION

The oldest is a transaction
the less likely a transaction could be reverted

0 confirmation

Not sure we will have our beer!

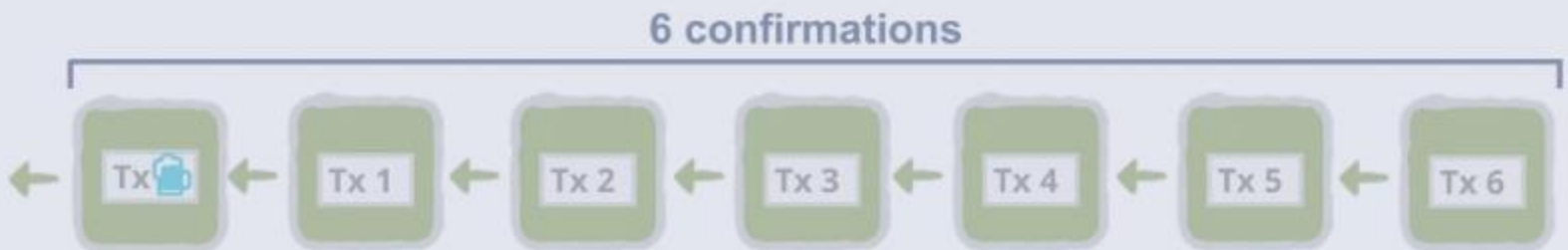
HOW TO BE SURE ABOUT YOUR TRANSACTION

The oldest is a transaction
the less likely a transaction could be reverted

We may have our beer!

HOW TO BE SURE ABOUT YOUR TRANSACTION

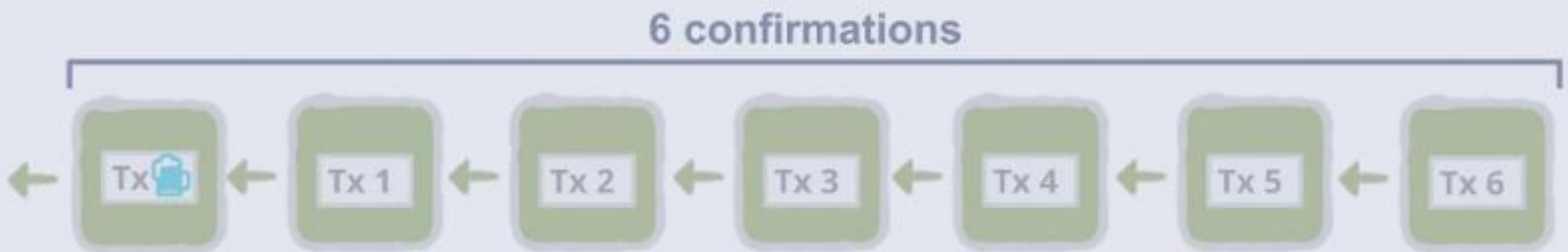
The oldest is a transaction
the less likely a transaction could be reverted



We will have our beer!

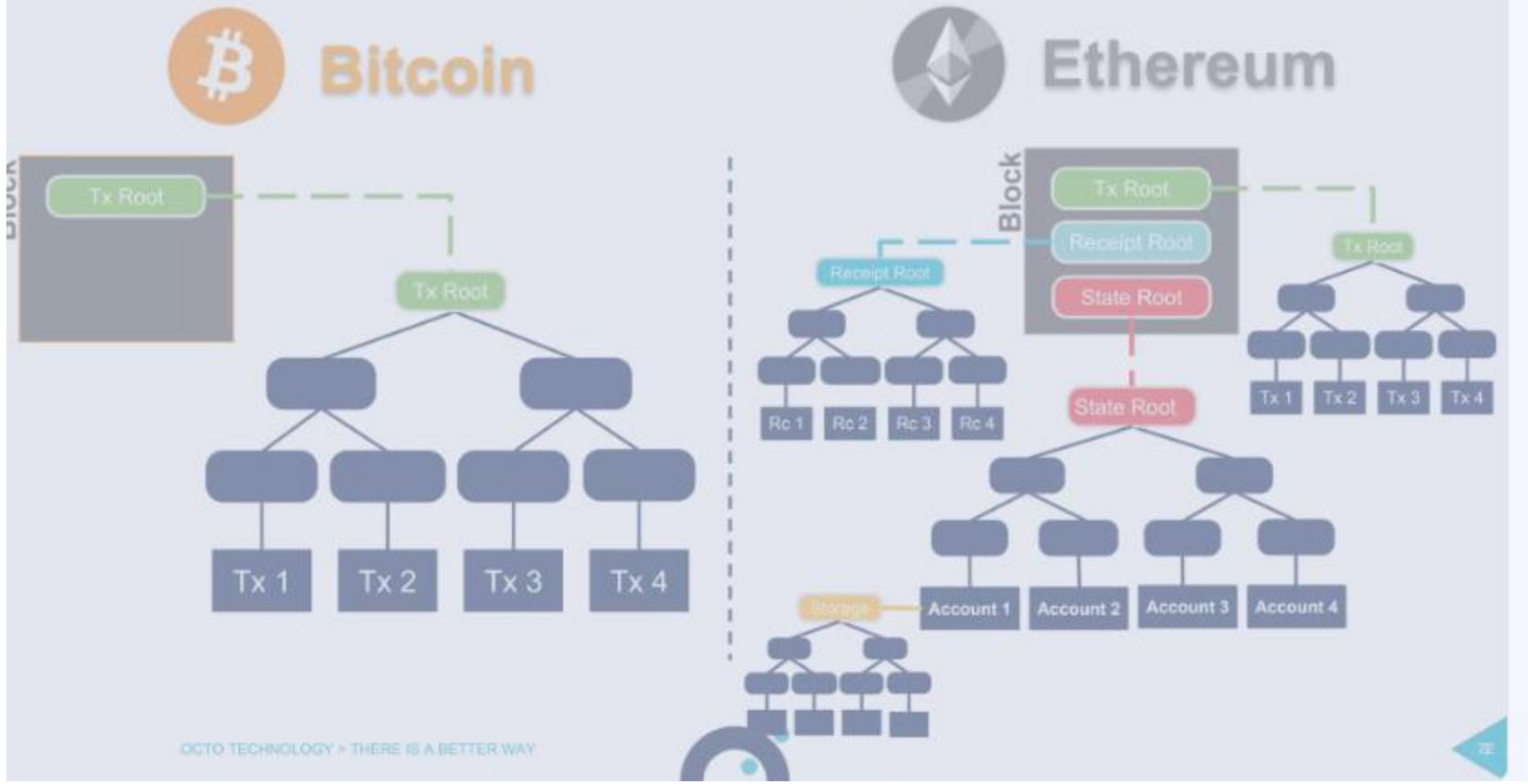
HOW TO BE SURE ABOUT YOUR TRANSACTION

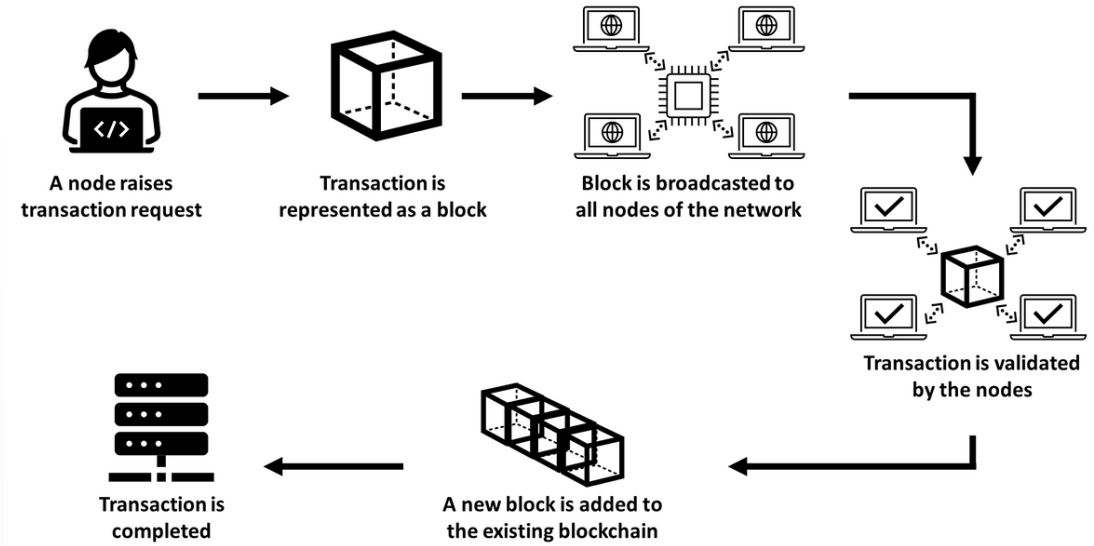
The oldest is a transaction
the less likely a transaction could be reverted

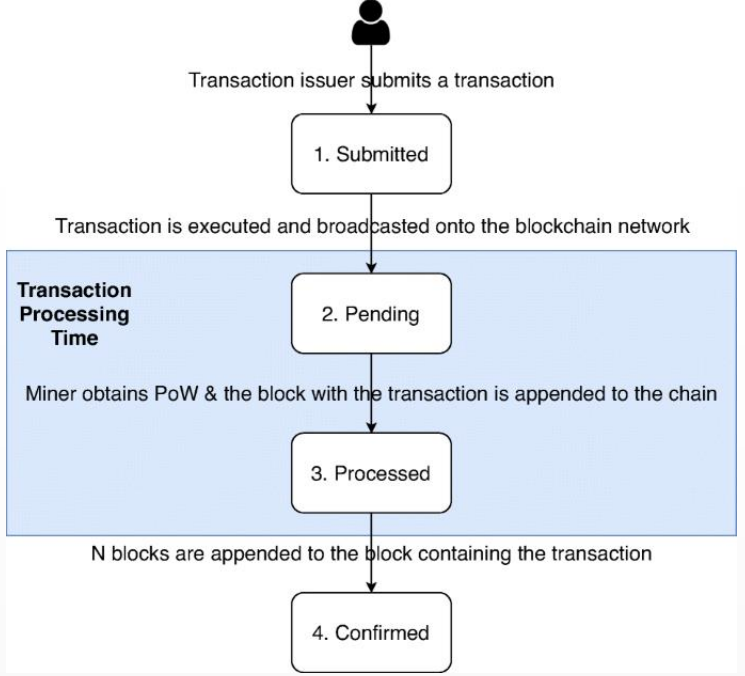


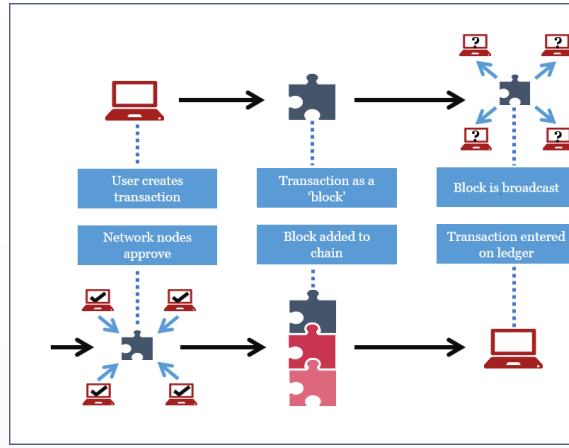
6 blocks-old transactions are considered close to **100% safe**

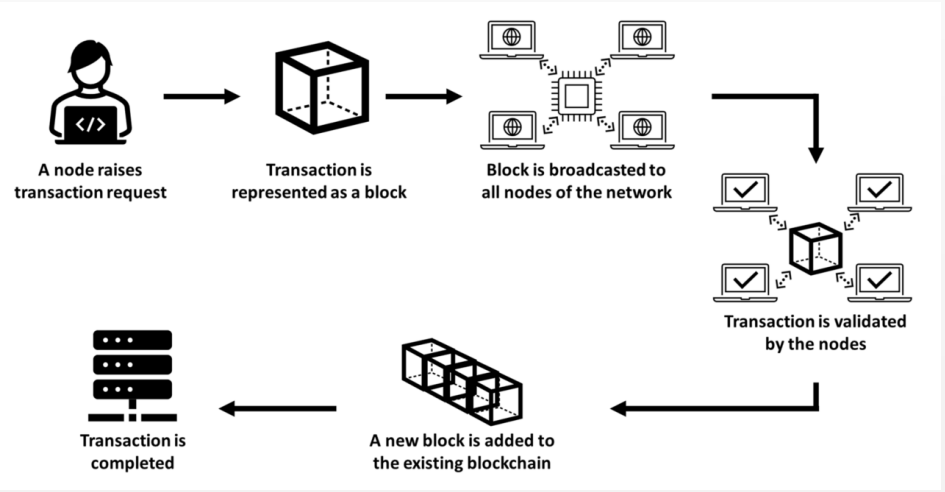
WHERE ARE MERKLE TREES USED?

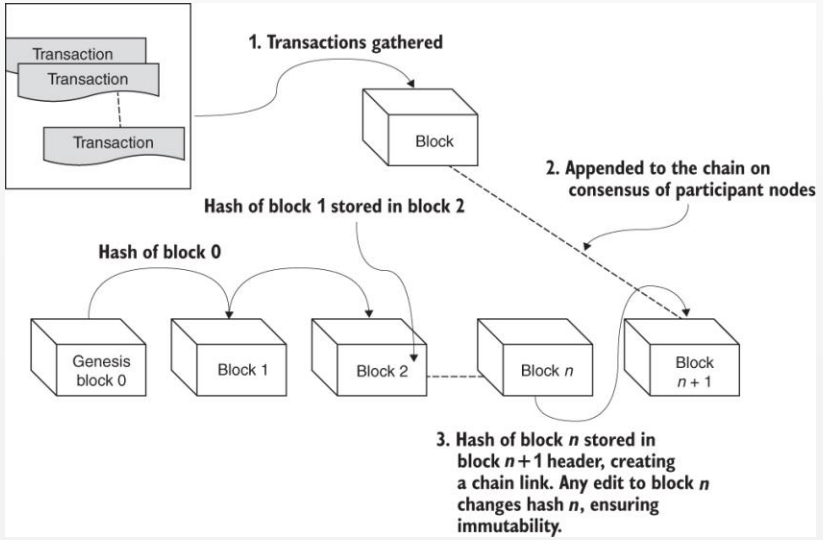


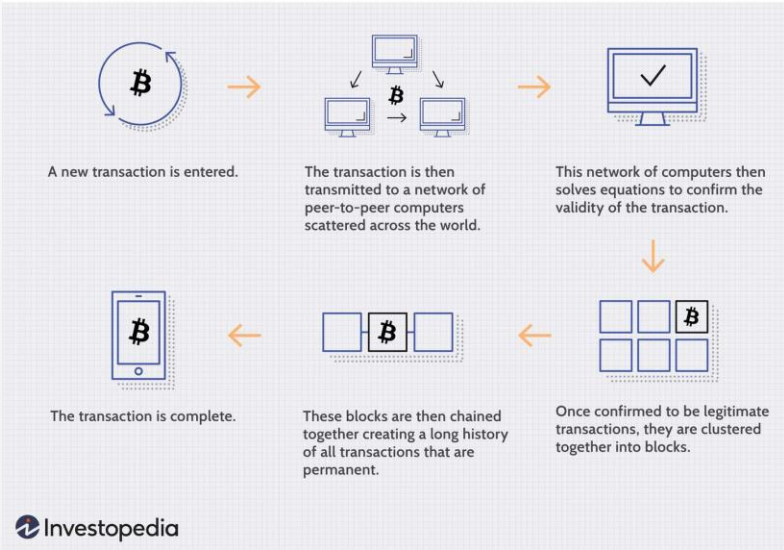

A node raises transaction request
Transaction is represented as a block
Block is broadcasted to all nodes of the network
Transaction is validated by the nodes
A new block is added to the existing blockchain
Transaction is completed


Transaction issuer submits a transaction
1. Submitted
Transaction is executed and broadcasted onto the blockchain network
Transaction Processing Time
2. Pending
Miner obtains PoW & the block with the transaction is appended to the chain
3. Processed
N blocks are appended to the block containing the transaction
4. Confirmed

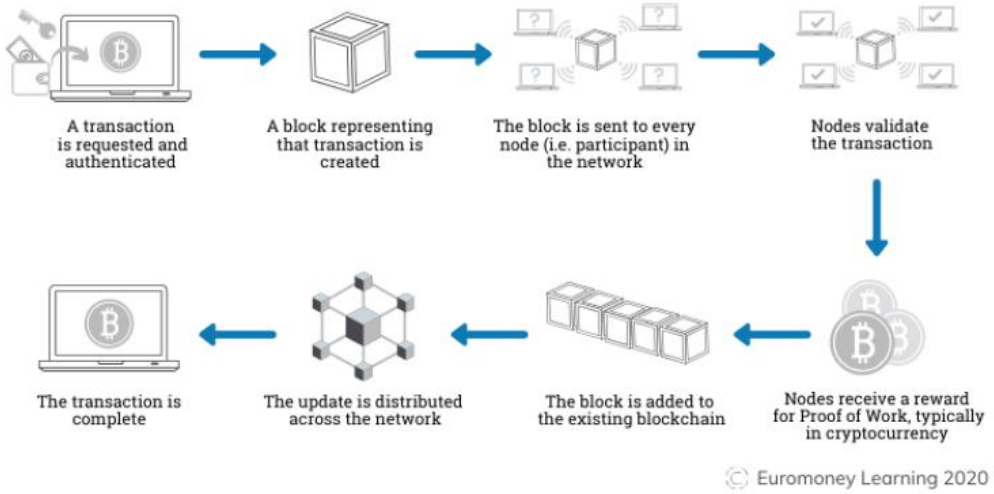

User creates transaction
Transaction as a 'block'
Block is broadcast
Network nodes approve
Block added to chain
Transaction entered on ledger

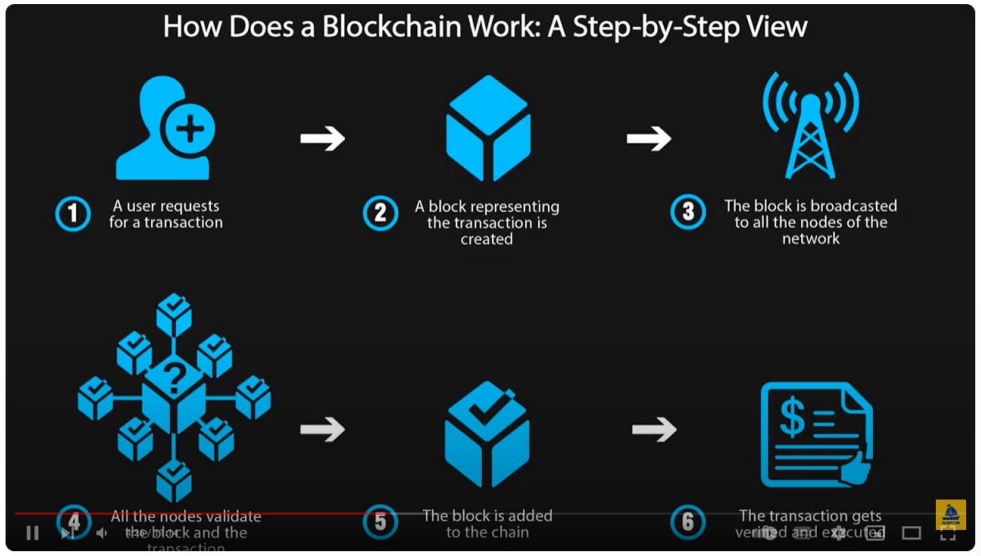

A node raises transaction request
Transaction is represented as a block
Block is broadcasted to all nodes of the network
Transaction is validated by the nodes
A new block is added to the existing blockchain
Transaction is completed


Transaction
Transaction
Transaction
1. Transactions gathered
Block
2. Appended to the chain on consensus of participant nodes
Hash of block 1 stored in block 2
Hash of block 0
Genesis block 0
Block 1
Block 2
Block n
Block n + 1
3. Hash of block n stored in block n + 1 header, creating a chain link. Any edit to block n changes hash n, ensuring immutability.

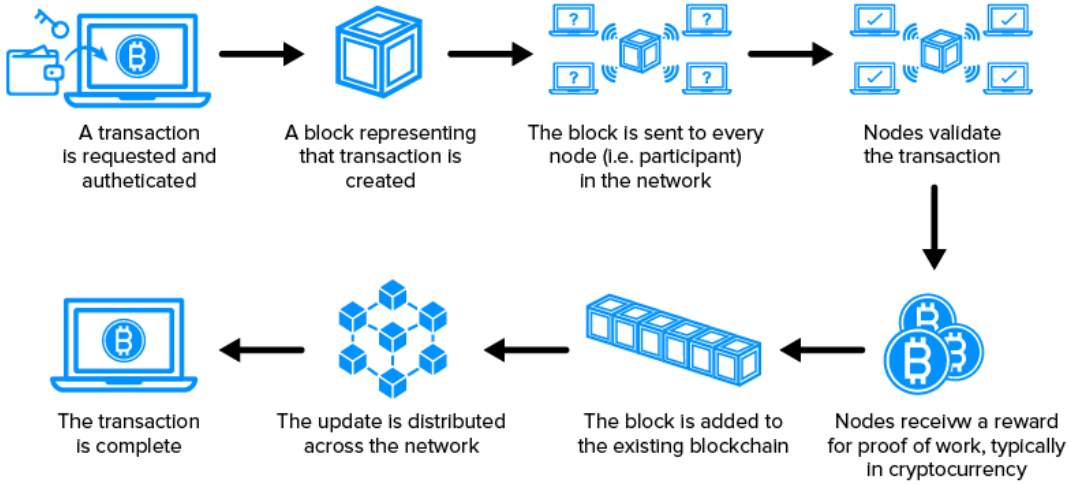

A new transaction is entered.
The transaction is then transmitted to a network of peer-to-peer computers scattered across the world.
This network of computers then solves equations to confirm the validity of the transaction.
Once confirmed to be legitimate transactions, they are clustered together into blocks.
These blocks are then chained together creating a long history of all transactions that are permanent.
The transaction is complete.
Investopedia

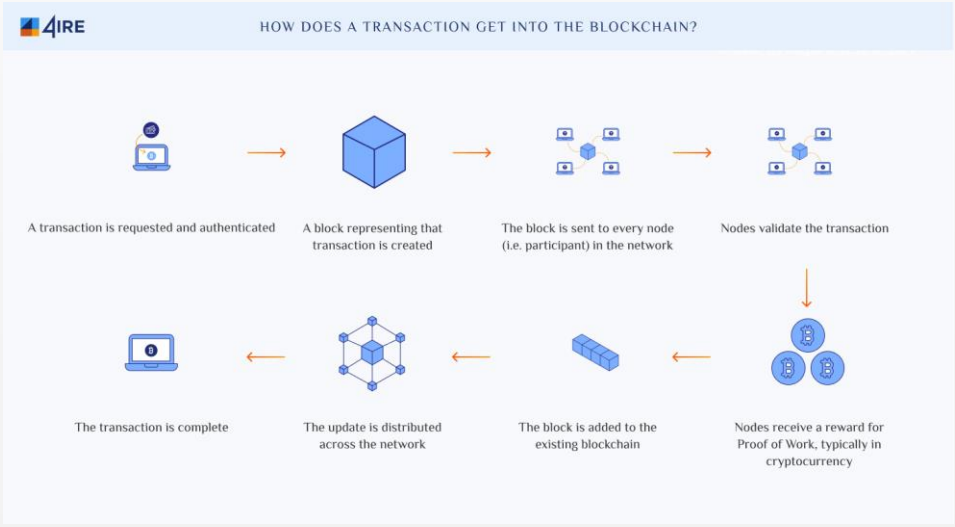
How does a transaction get into the blockchain?



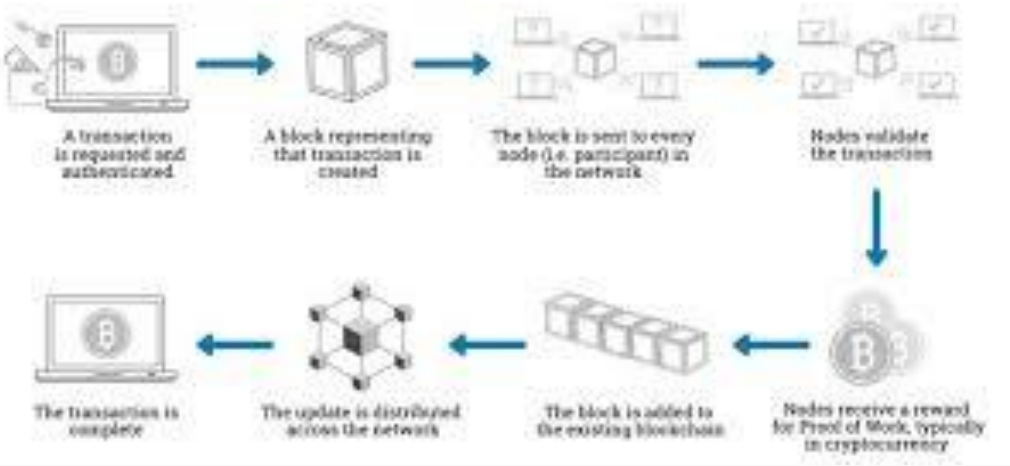


How does a transaction get into the blockchain?

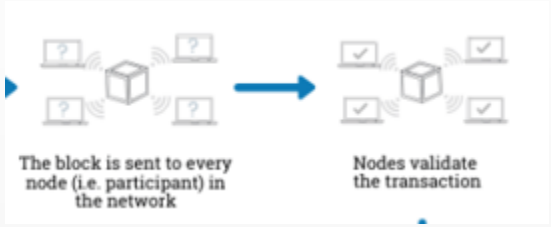


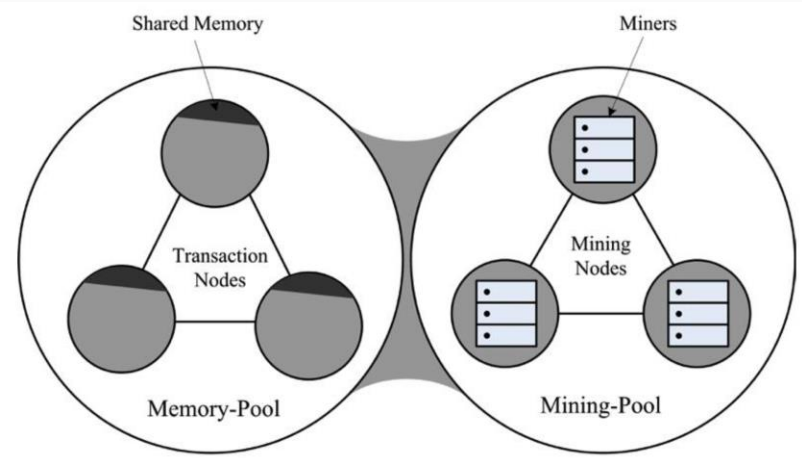


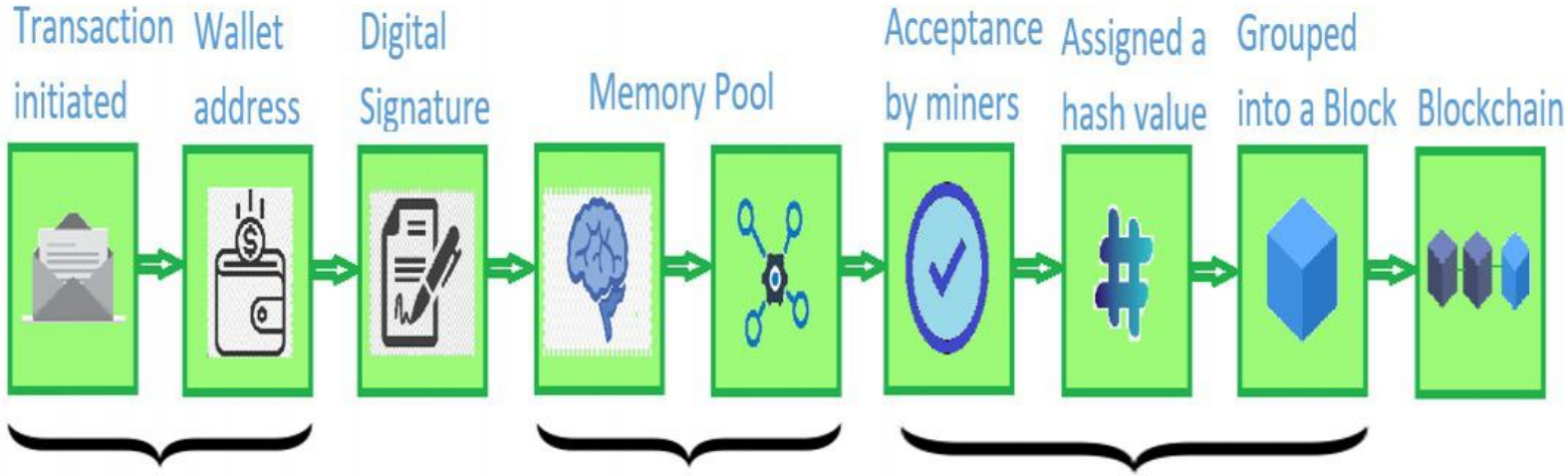
How does a transaction get into the blockchain?



- Transaction Initiated,/Authentification
- Digital Signature,
- Memeory Pool
- Acceptance by miners
- Assigned a hash value
- Gouped in a Block
- Blcok Become part of blockchain







1. A transaction is created by the sender using the wallet address of the receiver
2. Sign a transaction
3. Transaction is sent to the memory pool
4. Transaction is accepted by the miners, grouped into a block and assign a hash value to the block
5. The block now becomes a part of blockchain

Exercice : Concept , coceptual model