INSTITUT BURKINABE DES ARTS ET METIERS

MIAGE
Licence 3
2022-2023

Introduction à la Technologie Blockchain

Chapitre 3 : Le fonctionnement de la blockchain

Enseignant: OUEDRAOGO Ablassé oued.ablasse@gmail.com **+226 70 47 04 18 /76 59 13 72** Profil LinkedIn

Objectifs

- Maîtriser le processus de gestion des transaction
- Maitriser le processus de fabrication des blocs (minage)
- Maitriser les concepts de wallet, de smart contract et de DApp.
- Connaitre les défis liés a la sécurité sur la blockchain

Prérequis

- Chapitre 1: Fondamentaux de la blockchain
- Chapitre 2: Cryptographie appliqué à la blockchain

Plan

SD

Introduction

La cryptographie est une discipline clé pour comprendre le fonctionnement de la Blockchain . Nous utiliserons les connaissance acquise dans le chapitre précèdent pour expliquer le fonctionnement de la blockchain Bitcoin.

En effet La Blockchain se fonde sur deux **outils cryptographiques** :

- La ***signature électronique*** fondée sur des **algorithmes asymétriques;**
- ***les algorithmes de hachage***.

Dans le cas du Bitcoin, c'est l'algorithme à courbes elliptiques ***ECDAS*** qui est utilisé.

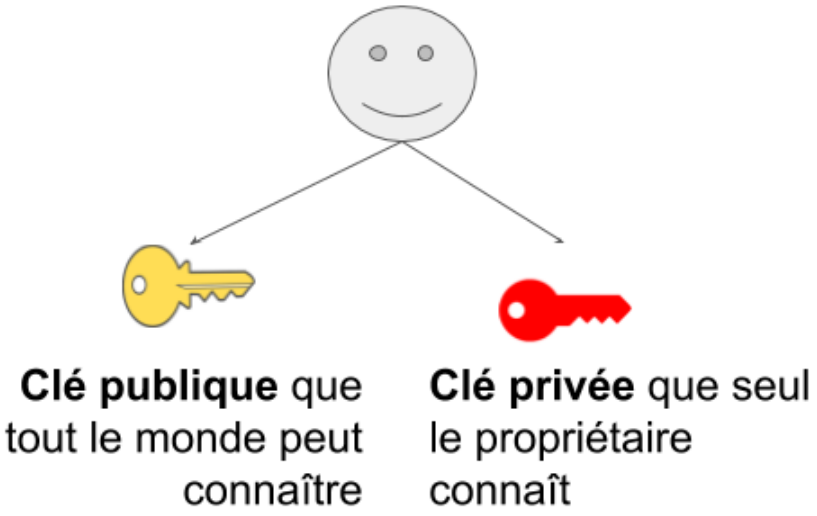
I. Gestion des transactions

1. Génération des clés cryptographique
2. Emission d'une transaction
3. Signature de la transaction

I. Gestion des transactions

1. Génération des clés cryptographiques

Dans un réseau Blockchain, chaque utilisateur crée une suite aléatoire de chiffres, appelée **clé privée**. À partir de celle-ci un algorithme permet de produire une seconde clé appelée **clé publique.**



I. Gestion des transactions

2. Emission d'une transaction

lors d'une transaction sur le réseau, l'émetteur va utiliser la clé publique du récepteur pour lui transférer un certain nombre de satoshis. Ces derniers représentent la plus petite fraction de bitcoin , ***un satoshi équivalent à 0,00000001 bitcoin***.

Une transaction comprends entre autres les champs suivants :

a) **Version** : Il s'agit d'un entier signé de 32 bits qui précise la version du protocole (logiciel) Bitcoin utilisé.

I. Gestion des transactions

2. Emission d'une transaction

b) **Entrées (inputs) :** Les entrées de la transaction font référence aux sorties de transactions précédentes qui seront utilisées comme sources de fonds. Chaque entrée inclut généralement :

- **Identifiant de transaction (TXID)** : Il s'agit de l'identifiant unique de la transaction précédente dont vous souhaitez utiliser la sortie. Le TXID est un hash qui identifie de manière unique une transaction dans la blockchain.
- **Indice de sortie (vout) :** Une transaction précédente peut avoir plusieurs sorties (outputs), et l'indice de sortie indique quelle sortie de transaction spécifique utilisée comme source de fonds dans la transaction en cours. L'indice de sortie commence généralement à zéro pour la première sortie et est incrémenté pour chaque sortie supplémentaire.

I. Gestion des transactions

2. Emission d'une transaction

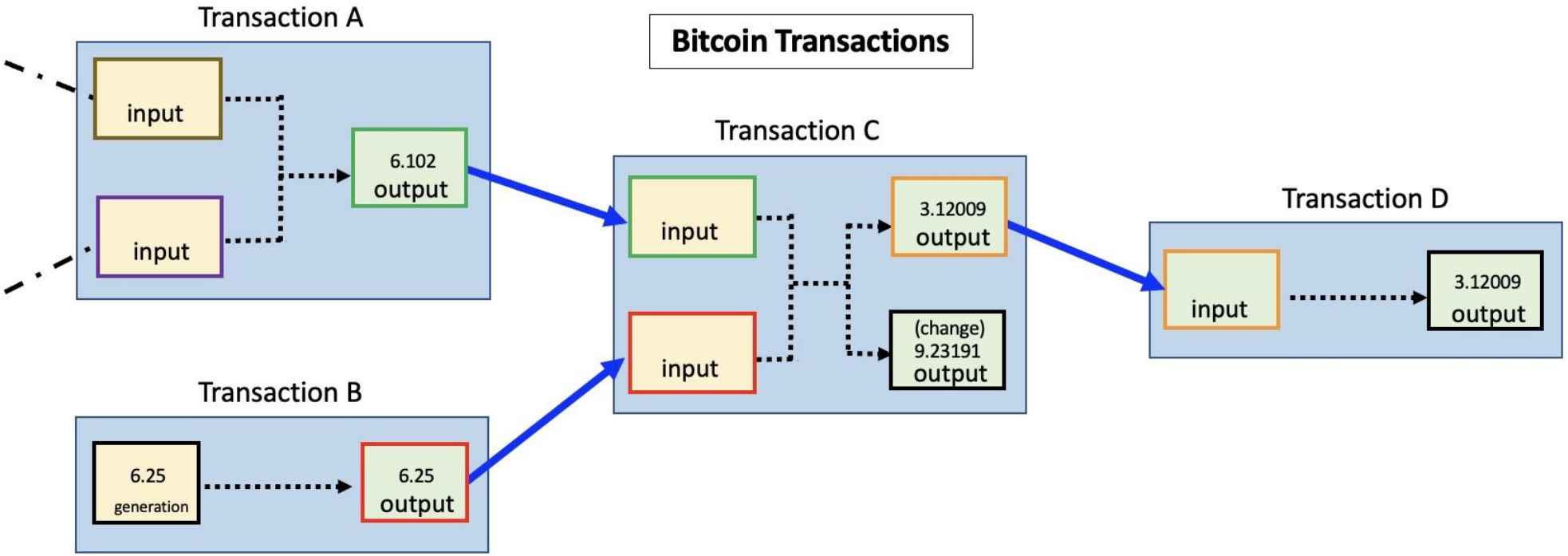
b) **Sorties (outputs)** : Les sorties de la transaction définissent les destinataires et les montants des fonds ou des bitcoins à transférer. Chaque sortie indique l'adresse du destinataire et la quantité de bitcoins qui lui est attribuée.

c) **Montants des frais de transaction** : Il s'agit du montant en bitcoins que l'émetteur de la transaction est prêt à payer en frais de transaction. Ces frais sont généralement destinés aux mineurs de la blockchain Bitcoin comme incitation à inclure la transaction dans un bloc.

d) **Horodatage** : Il s'agit de la date et l'heure à laquelle la transaction est créée.

I. Gestion des transactions

2. Emission d'une transaction



I. Gestion des transactions

3. Signature d'une transaction

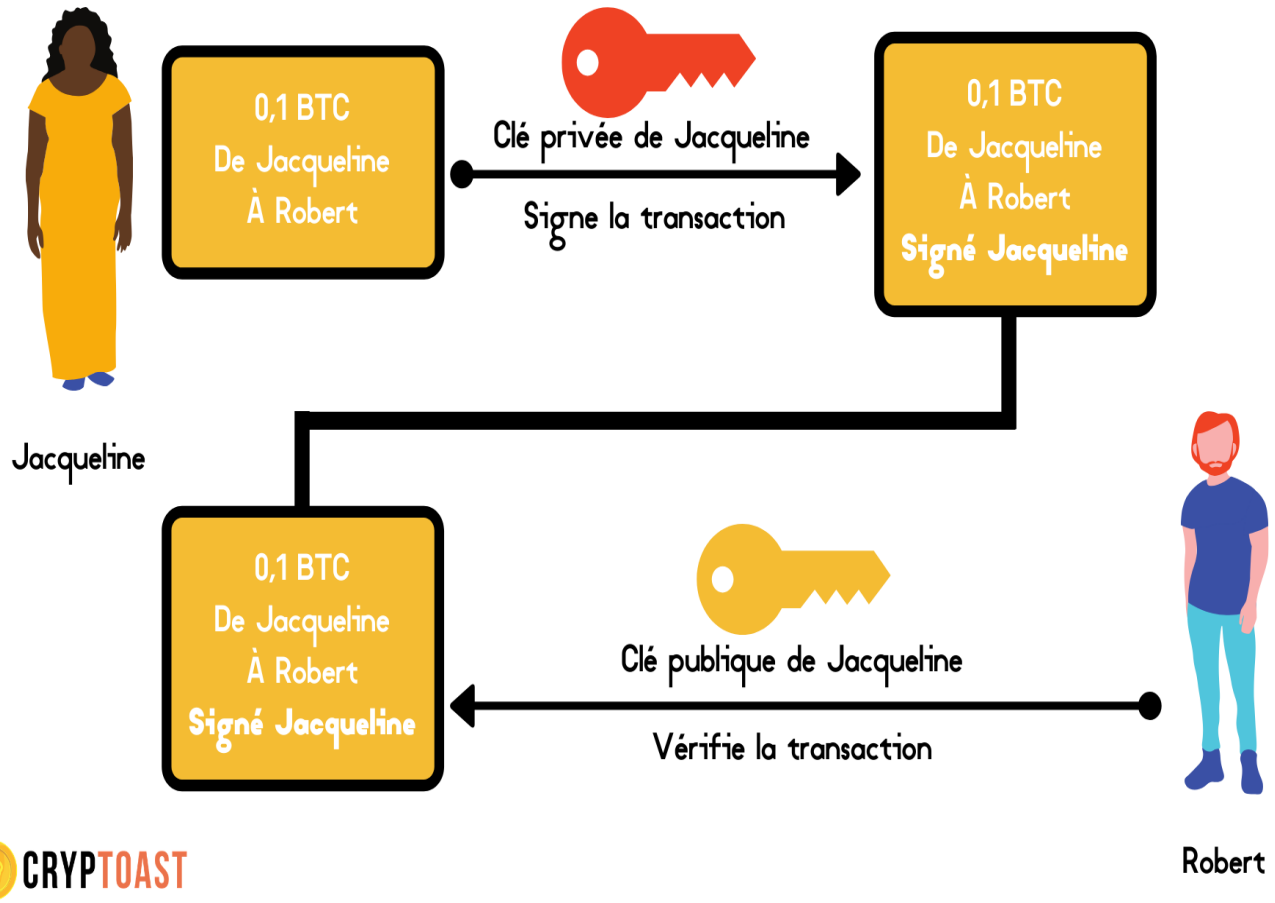
Une fois la transaction constitué:

a) L'émetteur la signe avec sa ***clé privée.*** Le hash chiffré avec sa clé privée est appelé ***scripts de déverrouillage (Unlocking scripts)*** et est ajouté à la transaction. Ainsi les autres membres du réseau peuvent vérifier l'auteur de la transaction en utilisant la ***clé publique*** de l'émetteur.

b) et il chiffre le hash de cette mêmes transaction avec la ***clé publique*** du récepteur (ou destinataire). Ce hash chiffré appelé ***scripts de verrouillage (Locking scripts)*** est ajouter à la transaction. Le destinataire seul peut alors la déchiffrer avec sa ***clé privée*** et dépenser le montant de la transaction.

I. Gestion des transactions

3. Signature d'une transaction



II. Fabrication des blocs (minage)

1. La désignation du fabricant
2. Emission d'une transaction
3. Signature de la transaction

II. Fabrication des blocs (minage)

1. La désignation du fabricant

Dans le cadre de la Blockchain Bitcoin, chaque 10 minutes, les nœud du réseau (ou mineurs) compétissent pour trouver le résultat d'un calcul complexe proposé par la Blockchain. Le premier mineur a trouver le résultat obtient le droit de créer un bloc et sera rémunéré pour ce travail: C'est le ***minage Proof of Work***.

II. Fabrication des blocs (minage)

2. La création de bloc

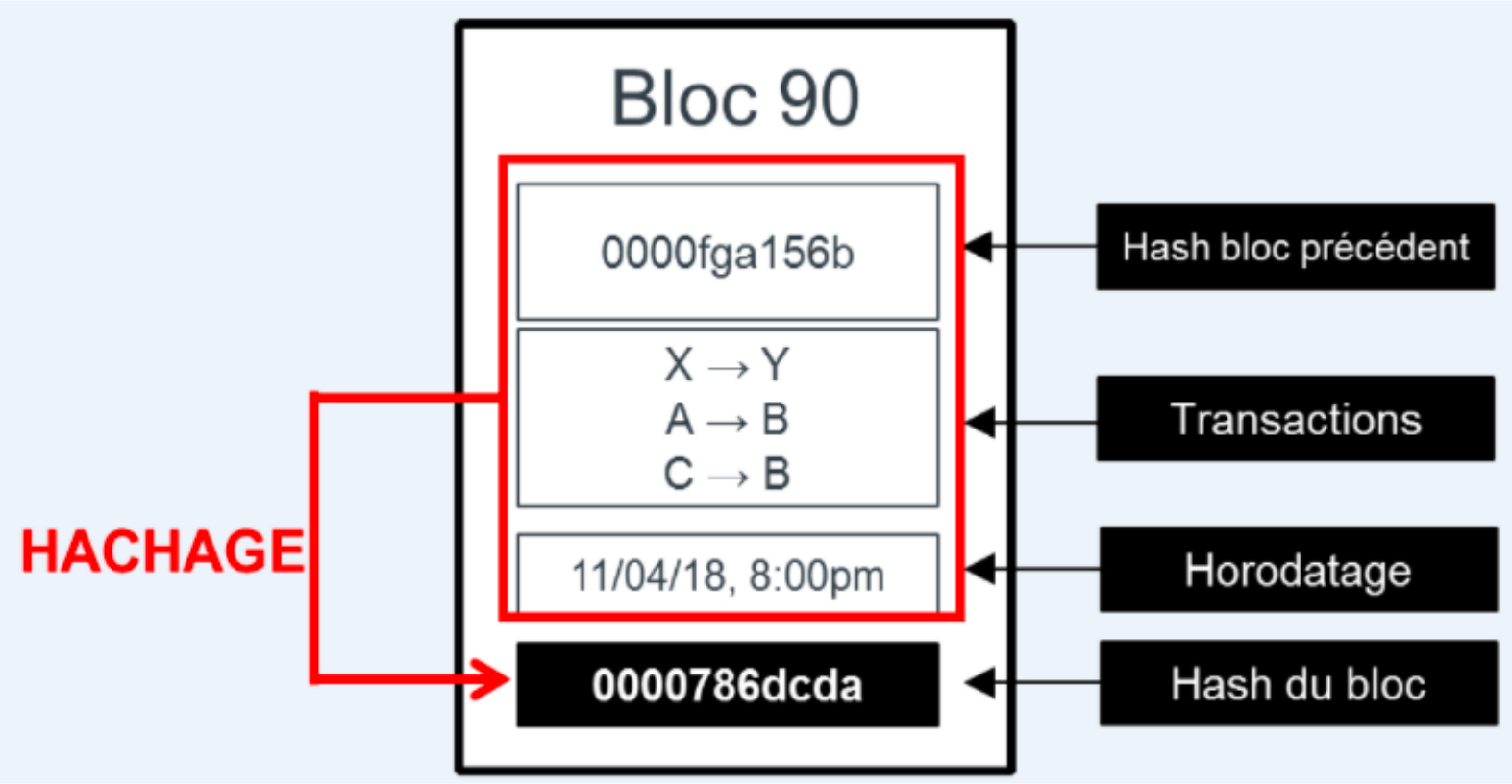
La création de bloc consiste, pour un mineur de :

1. rassembler les transactions vérifiées (valides) dans un même fichier;
2. y ajouter la date et l'heure de création;
3. y ajouter le hash du bloc précèdent ;
4. Hacher le fichier obtenu et y intégrer son hash (empreinte). C'est le calcul de ce hash qui est mis en compétition entre les mineur pour designer le fabricant du bloc.

II. Fabrication des blocs (minage)

2. La création de bloc

Le rôle des hashs dans les blocs



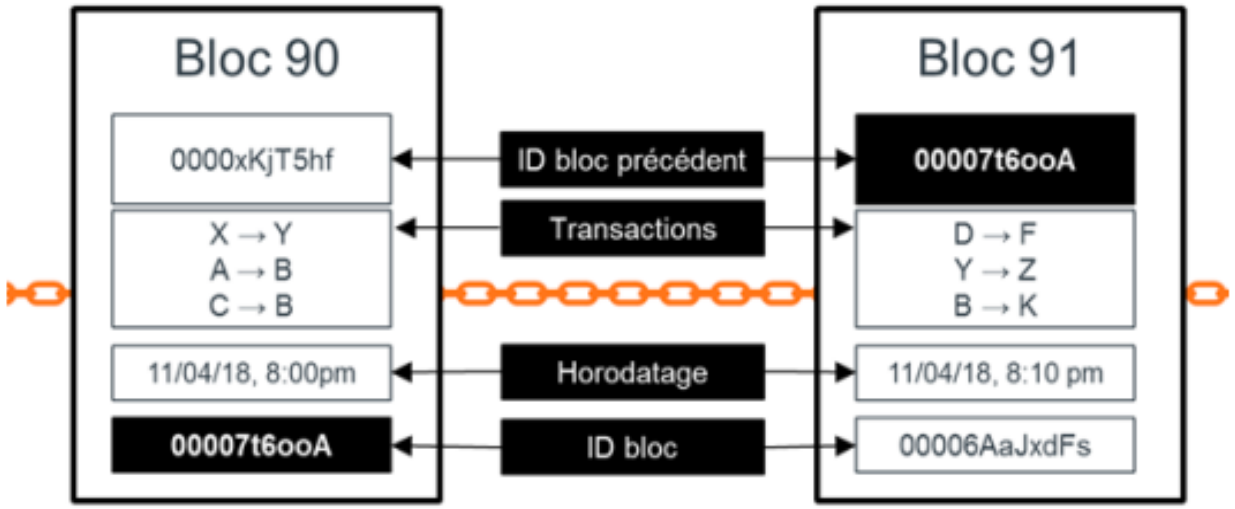
Source : OPECST

II. Fabrication des blocs (minage)

3. La liaison avec le bloc précèdent

Le hach du bloc précèdent utilisé dans le bloc actuel permet de les relier de façon **immuable** et ainsi constituer la chaine de blocs ou blockchain.

La structure d'une *blockchain* et le rôle des hashs



Source : Blockchain France

TP: Fabrication de blocs

A l'aide de fichiers texte (.txt) de l'algorithme RSA et de la fonction de hachage SHA-256 :

1. Créez et envoyez une transaction signée à votre binôme;
2. créez trois bloc liés et immuables.

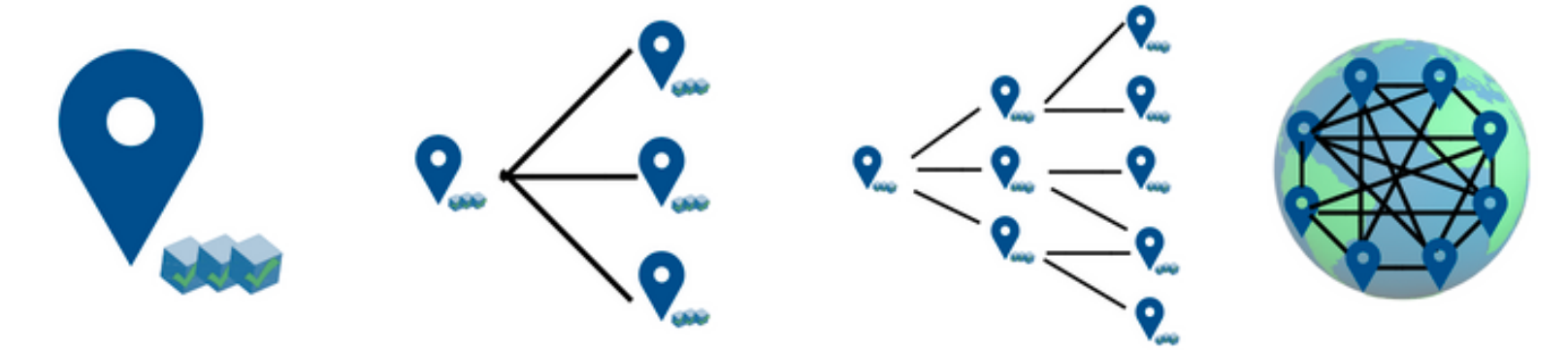
III. Le réseau Blockchain (Web3)

1. Intégration au réseau
2. Validation du bloc candidat
3. Diffusion du bloc et récompense

III. Le réseau Blockchain (Web3)

1. Intégration au réseau

Dans les blockchains dites publique (permissionless), comme celle du bitcoin, n'importe quel utilisateur de l'internet peut ainsi devenir un noeud du réseau en téléchargeant le registre auprès d'un noeud existant. Chaque noeud est connecté à plusieurs autres, appelés pairs , eux-mêmes ayant leurs propres pairs, ce qui forme un ***réseau pair à pair***.



Un **nœud** est un détenteur du registre

Chaque nœud est connecté à plusieurs **pairs**

Ils forment ainsi un **réseau pair à pair**

Ce réseau peut mailler l'ensemble du globe

Source : OPECST

III. Le réseau Blockchain (Web3)

2. Validation du bloc candidat

Trouver un hash satisfaisant : Lorsqu'un mineur trouve un hash qui répond aux critères de la difficulté, il annonce le bloc nouvellement créé aux autres participants du réseau.

Validation par le réseau : Les autres nœuds du réseau vérifient la validité du bloc en vérifiant que toutes les transactions incluses dans le bloc sont correctes et conformes aux règles du protocole Bitcoin. Ils vérifient également que le hash du bloc satisfait à la difficulté requise.

III. Le réseau Blockchain (Web3)

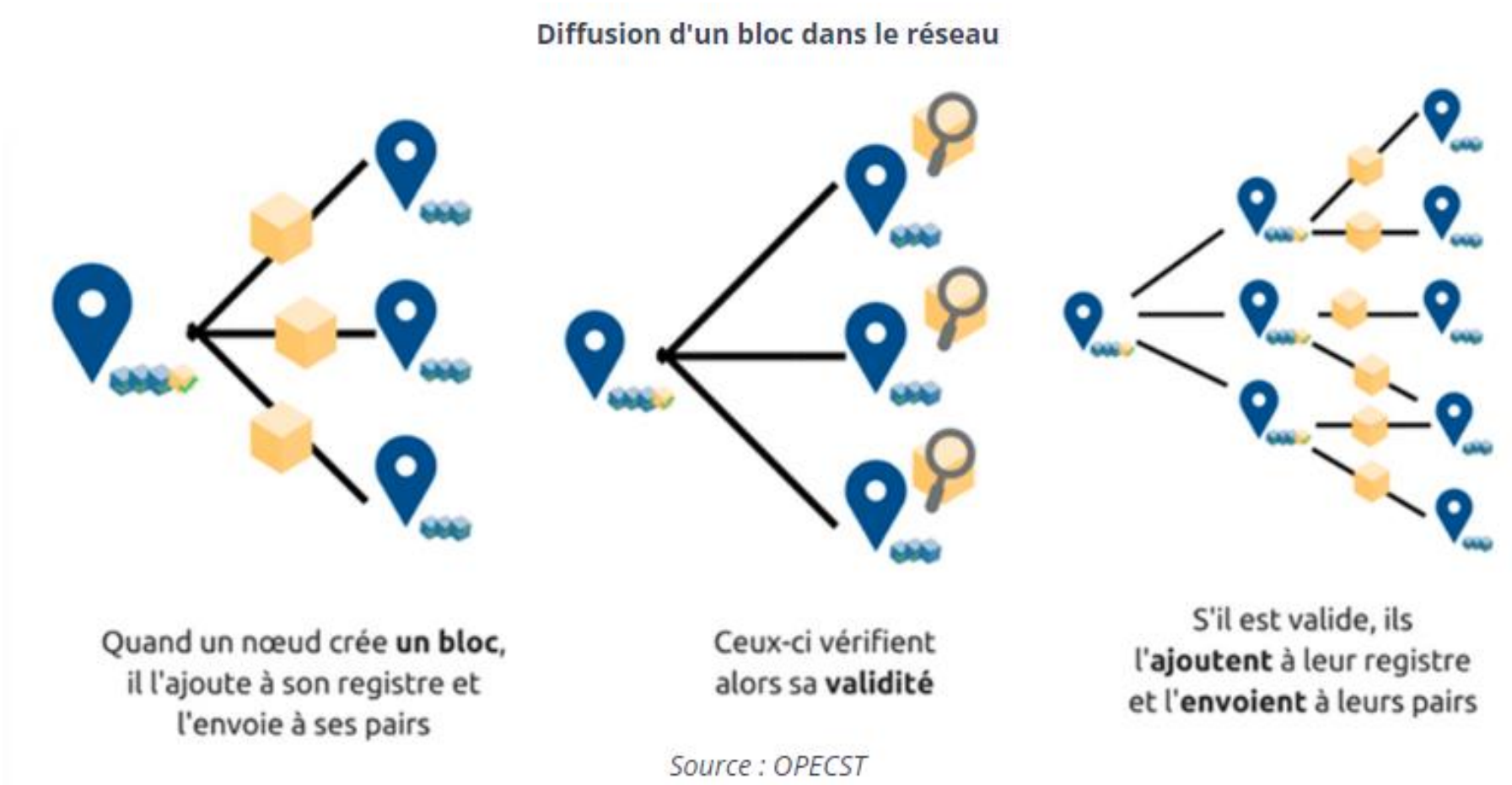
3. Diffusion du bloc et récompense

Diffusion et ajout à la blockchain : Si le bloc est validé avec succès par le réseau, il est diffusé à l'ensemble du réseau Bitcoin. Les mineurs l'ajoutent ensuite à leur copie locale de la blockchain en l'incorporant à la chaîne existante.

Récompense et frais de transaction : Le mineur qui réussit à miner un bloc valide reçoit une récompense en bitcoins nouvellement créés, ainsi que les frais de transaction associés aux transactions incluses dans le bloc. Ces récompenses constituent l'incitation économique pour les mineurs à participer au processus de minage.

III. Le réseau Blockchain (Web3)

3. Diffusion du bloc et récompense



III. Le réseau Blockchain (Web3)

3. Diffusion du bloc et récompense

Introduction d'un bloc invalide

Si un nœud crée un **bloc invalide**

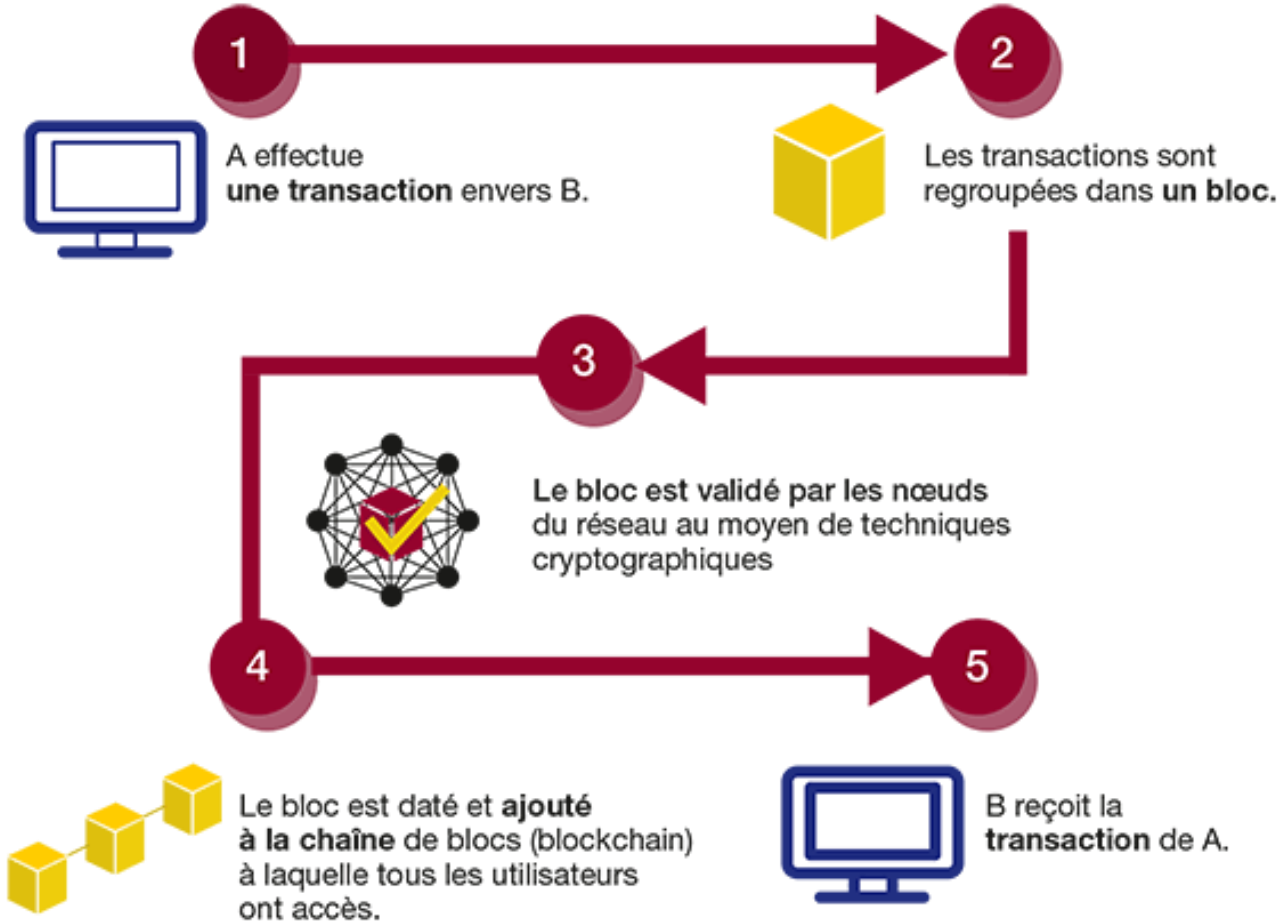
Les nœuds identifient la fraude

Ils ne l'ajoutent pas à leur registre et ne le diffusent pas

Source : OPECST

III. Le réseau Blockchain (Web3)

En résume



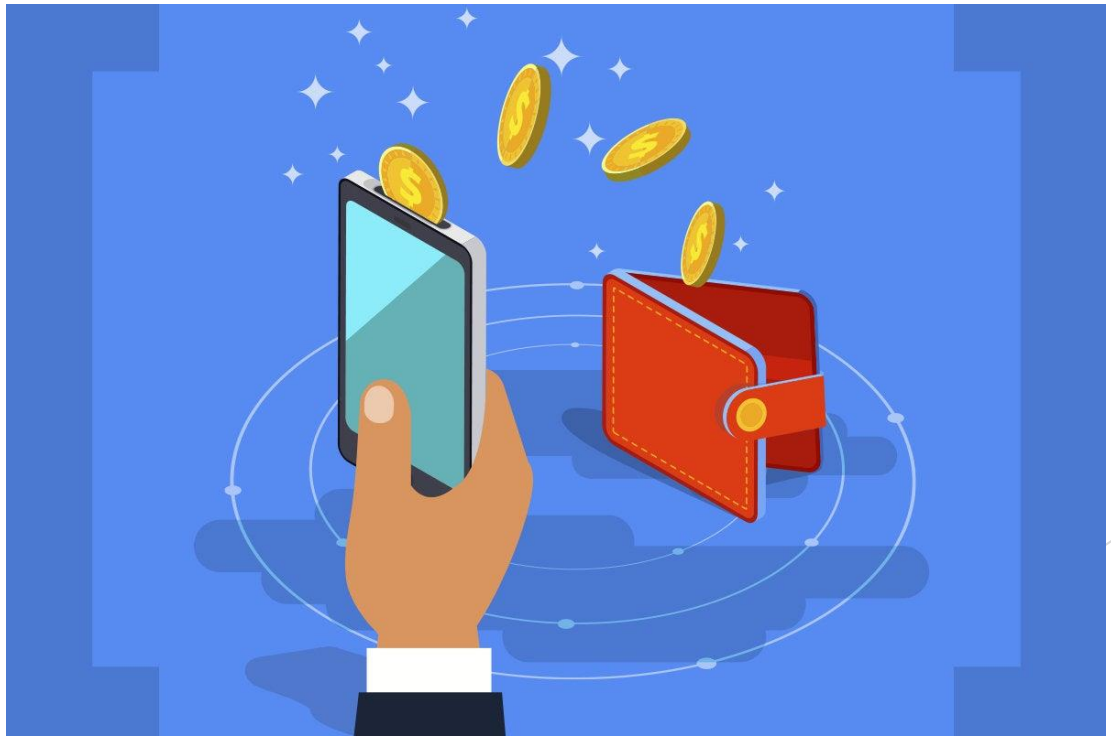
IV. Wallet, smart contract et Dapp

1. Wallet
2. Smart contract
3. Dapp

IV. Wallet, smart contract et Dapp

1. Wallet

Un wallet blockchain, également connu sous le nom de portefeuille blockchain, est une application ou un dispositif utilisé pour stocker, gérer et interagir avec des actifs numériques basés sur la technologie de la blockchain, tels que les cryptomonnaies (Bitcoin, Ethereum, etc.) ou les jetons (tokens) émis sur une blockchain spécifique.



IV. Wallet, smart contract et Dapp

1. Wallet

Un wallet blockchain permet généralement à un utilisateur de réaliser les opérations suivantes :

1. **Stockage sécurisé des clés privées :** Un wallet blockchain stocke les clés privées nécessaires pour accéder et contrôler les actifs numériques. Les wallets sécurisent ces clés privées en les stockant de manière cryptée et en utilisant des mécanismes de sécurité tels que les mots de passe, les codes PIN ou les dispositifs matériels.
2. **Gestion des adresses :** Un wallet blockchain génère des adresses publiques associées aux clés privées. Ces adresses sont utilisées pour recevoir des fonds ou des jetons sur la blockchain. Le wallet permet également de visualiser l'historique des transactions associées à chaque adresse.

IV. Wallet, smart contract et Dapp

1. Wallet

3. Envoi et réception de fonds : Un wallet blockchain permet d'envoyer et de recevoir des fonds en créant et en signant des transactions. L'utilisateur peut spécifier l'adresse de destination, le montant à transférer et éventuellement les frais de transaction.

4. Suivi du solde et de l'historique des transactions : Un wallet blockchain fournit des informations sur le solde des actifs détenus par l'utilisateur, ainsi que l'historique complet des transactions effectuées. Cela permet à l'utilisateur de vérifier les soldes, de suivre les dépenses et les réceptions, et de générer des rapports.

IV. Wallet, smart contract et Dapp

1. Wallet

Les wallets blockchain peuvent exister sous différentes formes :

Wallets logiciels : Ce sont des applications installées sur un ordinateur, un smartphone ou une tablette. Ils offrent une facilité d'utilisation et une mobilité, mais nécessitent une attention particulière à la sécurité du dispositif sur lequel ils sont installés.

Wallets matériels : Il s'agit de dispositifs physiques dédiés à la sécurisation des clés privées. Ils offrent une sécurité supplémentaire en isolant les clés privées des connexions Internet et des logiciels malveillants.

Wallets en ligne : Aussi appelés wallets web, ils sont hébergés sur des serveurs distants et accessibles via un navigateur web. Bien qu'ils offrent une facilité d'utilisation, ils nécessitent de faire confiance au fournisseur du service en ligne pour la sécurité et la protection des actifs.

IV. Wallet, smart contract et Dapp

1. Wallet

TP: Installation de Metamask

tutoriel metamask

IV. Wallet, smart contract et Dapp

2. Smart contract

Les wallets blockchain peuvent exister sous différentes formes :