

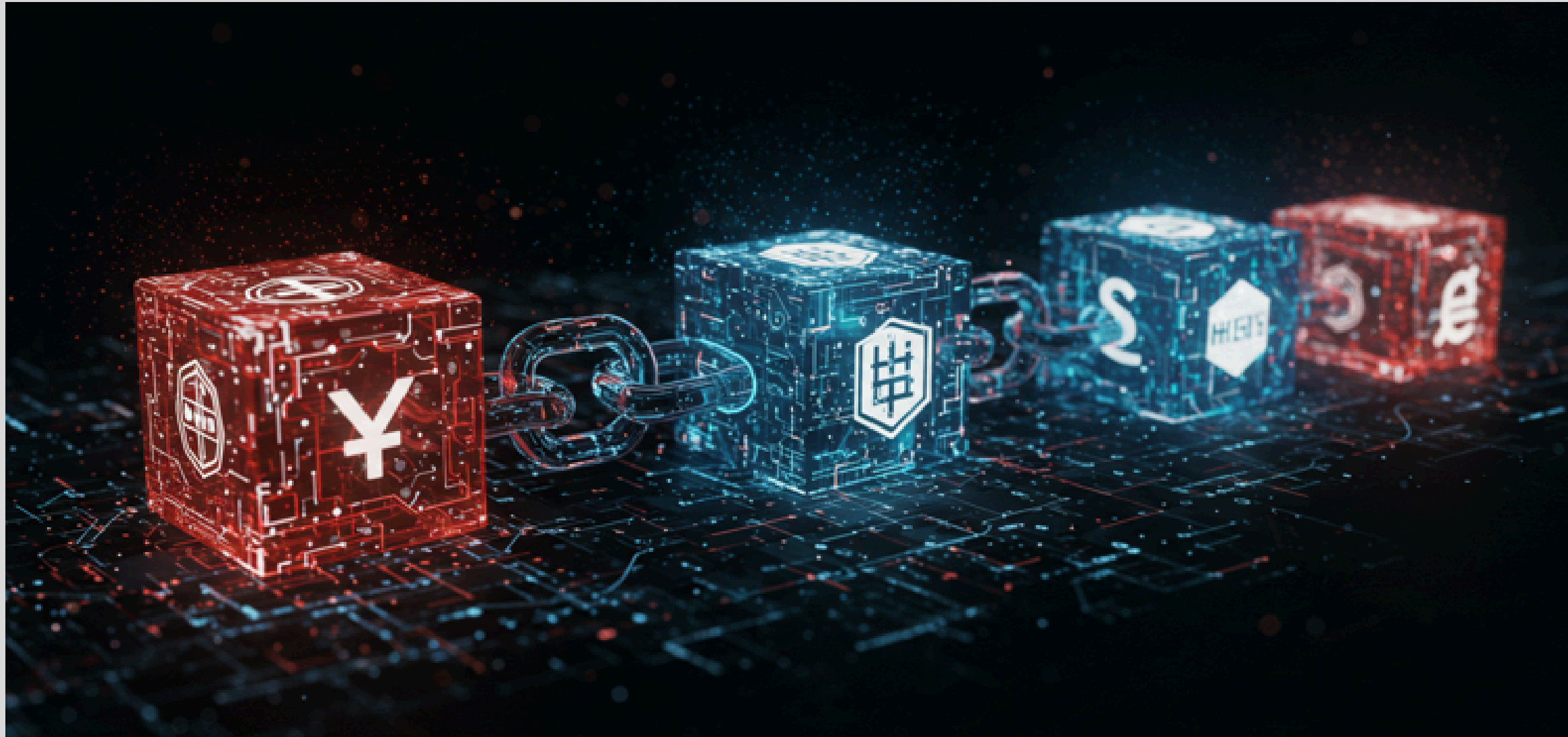
projet de fin d'étude:

Stockage et vérification des certificats utilisant la blockchain



1

1. Qu'est-ce que la Blockchain ?



Introduction :

1. Qu'est-ce que la Blockchain ?

La blockchain est une technologie qui permet de stocker et vérifier des informations de manière sécurisée et décentralisée, sans passer par une autorité centrale.

Les données sont enregistrées dans des blocs qui sont liés entre eux, garantissant ainsi leur intégrité et leur immutabilité. Dans notre projet, nous utilisons cette technologie pour le stockage des certificats scolaires, assurant ainsi leur authenticité, les rendant infalsifiables et facilement vérifiables.

Dans notre projet, nous l'utilisons pour garantir l'authenticité des certificats scolaires, afin qu'ils soient infalsifiables et facilement vérifiables.

La blockchain enregistre les transactions dans des blocs, qui sont validés par un réseau décentralisé de participants.

Chaque bloc

contient un hash unique et le hash du bloc précédent, garantissant l'intégrité des données. Une fois validée, la transaction est ajoutée à la chaîne et devient immuable.

La blockchain enregistre les transactions dans des blocs.

Chaque bloc contient :

- **Des données de transaction**
- **Un hash unique (empreinte numérique)**
- **Le hash du bloc précédent (qui relie les blocs entre eux)**
- **Un réseau décentralisé de participants valide chaque bloc par consensus.**

Une fois validé, le bloc est ajouté à la chaîne et devient immuable (ne peut pas être modifié).

Décentralisation :

La blockchain fonctionne sans un contrôle central. Le réseau est réparti entre tous les participants, ce qui permet une gouvernance décentralisée où aucune autorité unique ne peut imposer de modifications sur les transactions.

Transparence :

Toutes les transactions sont visibles par les membres du réseau. Cela assure que tout le monde peut vérifier et auditer les transactions, ce qui renforce la confiance dans le système.

Les caractéristiques de la Blockchain:

Sécurité :

Les données sont protégées par des méthodes cryptographiques complexes. Cela rend les transactions pratiquement impossibles à falsifier, garantissant leur authenticité et leur sécurité contre toute manipulation.

Immuabilité :

Une fois qu'une transaction est inscrite dans la blockchain, elle ne peut plus être modifiée. Cela empêche toute modification rétroactive des données et assure leur intégrité sur le long terme.

Consensus :

Les transactions doivent être validées par un mécanisme de consensus entre les participants du réseau (par exemple, Proof of Work ou Proof of Stake). Cela garantit que seules les transactions valides sont ajoutées à la blockchain.

Divisibilité :

Les actifs peuvent être divisés en petites unités (par exemple, un Bitcoin peut être divisé en 100 millions de satoshis), permettant ainsi des transactions de toute taille. Cette divisibilité facilite les micro-transactions et la flexibilité du système.

Permanence :

Les enregistrements dans la blockchain sont permanents et restent accessibles à tout moment. Cela assure une traçabilité complète des informations stockées, ce qui est crucial pour des applications comme la vérification des certificats ou des transactions.

4.1 .Les types de Blockchain :

Blockchain Publique :

Exemples : Bitcoin, Ethereum.

Accessible à tous, chacun peut participer à la validation.

Blockchain Privée :

Exemple : Hyperledger.

Accès restreint à certains participants autorisés (entreprises).

Blockchain Hybride :

Combine blockchain publique et privée.

Certaines données sont publiques, d'autres privées.

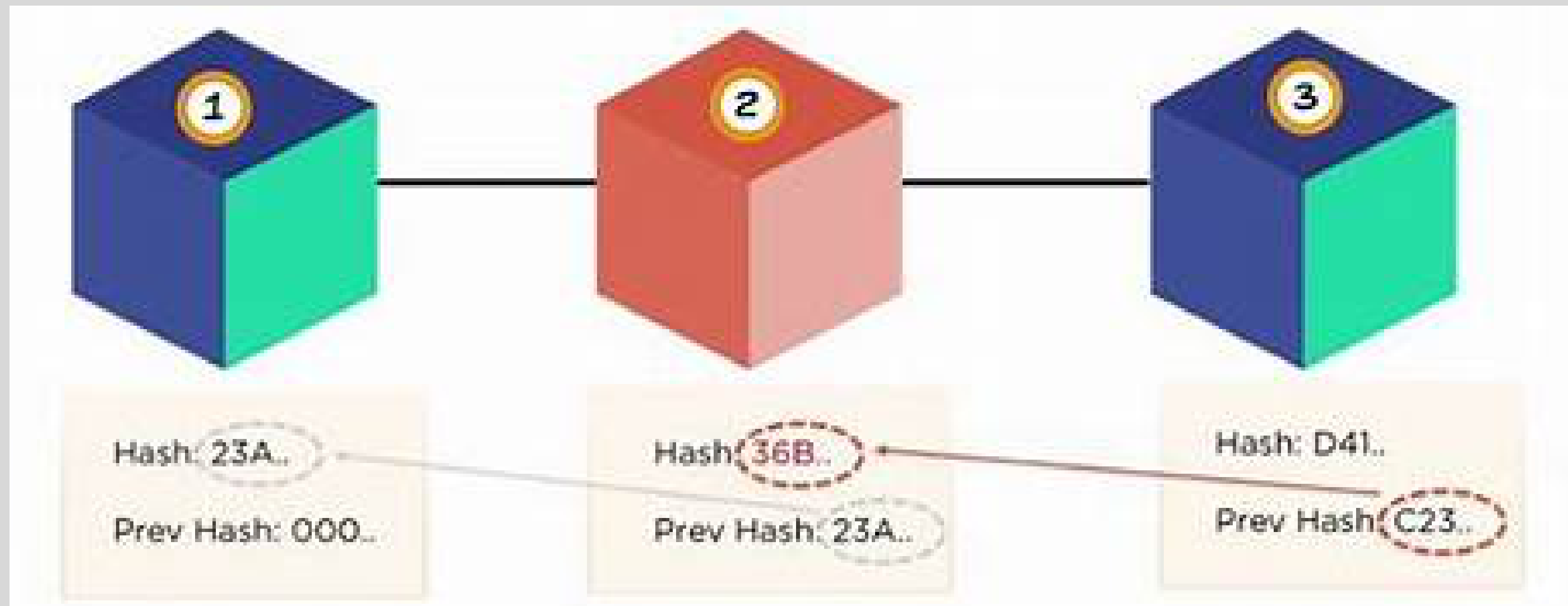
Blockchain de Consortium :

Contrôlée par un groupe d'organisations qui valident les transactions ensemble.

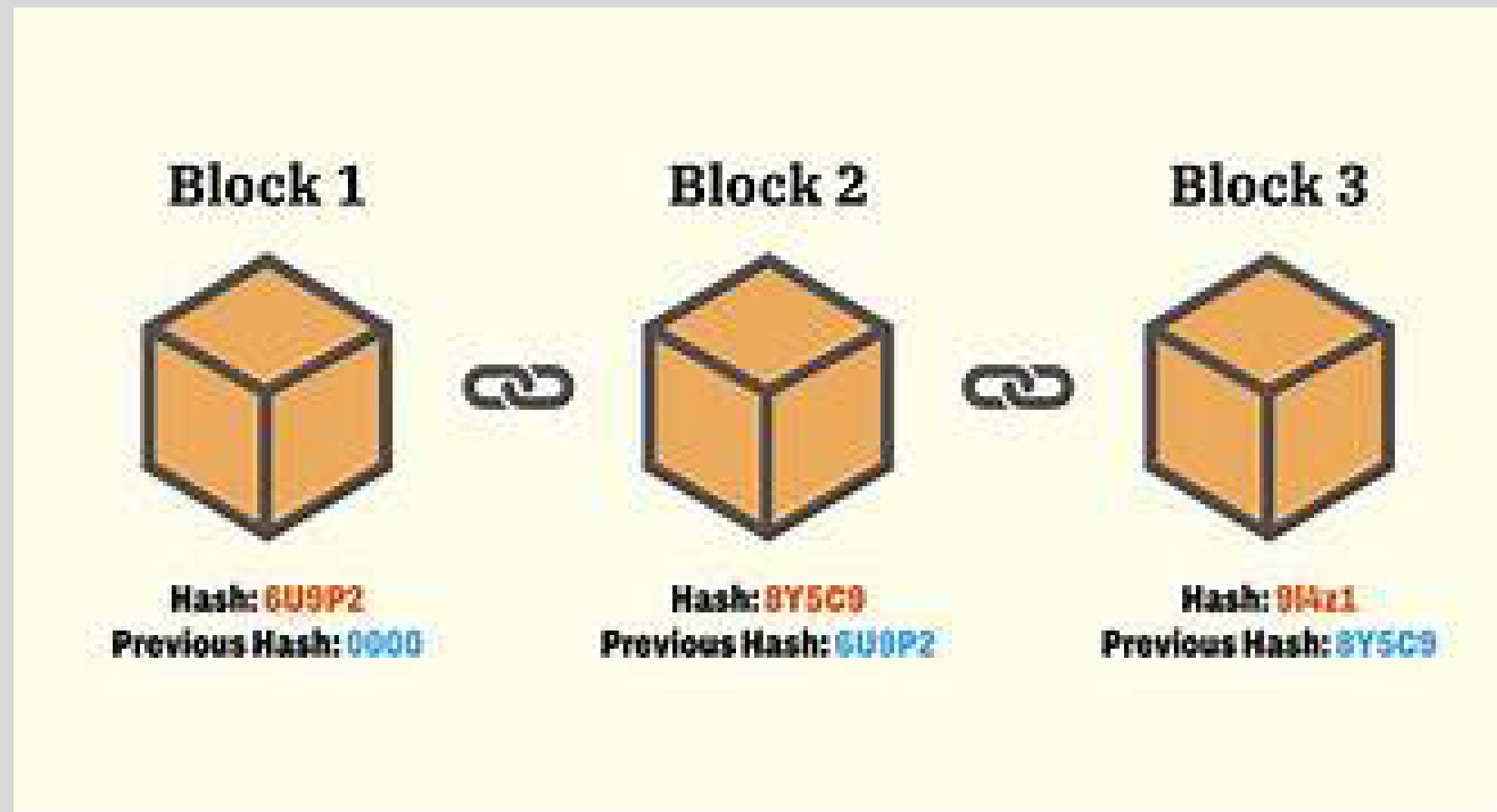
- **Clé privée:**

- Utilisée pour signer une transaction et prouver que le détenteur de la clé est bien l'auteur de la transaction. Elle doit rester secrète.
- Garantit le contrôle total des fonds et permet de signer les transactions
- Exemple d'utilisation : Lorsqu'Alice envoie 1 Bitcoin à Bob, elle utilise sa clé privée pour signer la transaction et prouver qu'elle en est l'expéditrice légitime.

- **Clé publique :**
- Elle est dérivée de la clé privée et est utilisée pour recevoir des fonds ou des informations. Elle est partagée publiquement.
- Garantit l'authenticité des transactions et permet de vérifier les signatures.
- Exemple d'utilisation : Bob partage sa clé publique avec Alice pour qu'elle puisse lui envoyer 1 Bitcoin.



Le hashage est un processus cryptographique qui transforme des données (comme une transaction) en une chaîne de caractères de taille fixe (appelée hash). Ce processus est essentiel dans la blockchain pour plusieurs raisons :



- Vérification de l'intégrité des données :

Un hash garantit qu'aucune donnée n'a été modifiée. Si une seule lettre d'un bloc change, son hash sera complètement différent, ce qui rendra la modification évidente pour tous les participants du réseau.

- Chaînage des blocs :

Chaque bloc de la blockchain contient un hash du bloc précédent. Cela lie les blocs entre eux de manière sécurisée et rend difficile la modification des transactions passées.

Chaque bloc contient plusieurs éléments :

- **Données de la transaction :** La liste de toutes les transactions validées dans ce bloc.
- **Hash du bloc précédent:** Chaque bloc contient l'identifiant (hash) du bloc précédent, ce qui lie les blocs entre eux.
- **Hash du bloc actuel :** Chaque bloc contient son propre hash, généré à partir des données du bloc.
- **Le Nonce:** Un nombre aléatoire utilisé dans le processus de validation (Proof of Work) pour créer un hash spécifique.

