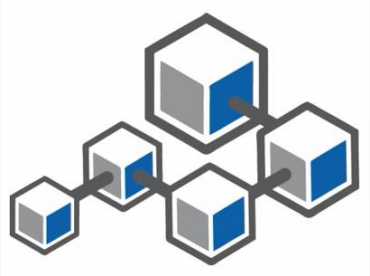
Architecture de la Technologie Blockchain

Notions de Base de la Blockchain : Block, The Hash, Mining, Merkle Trees

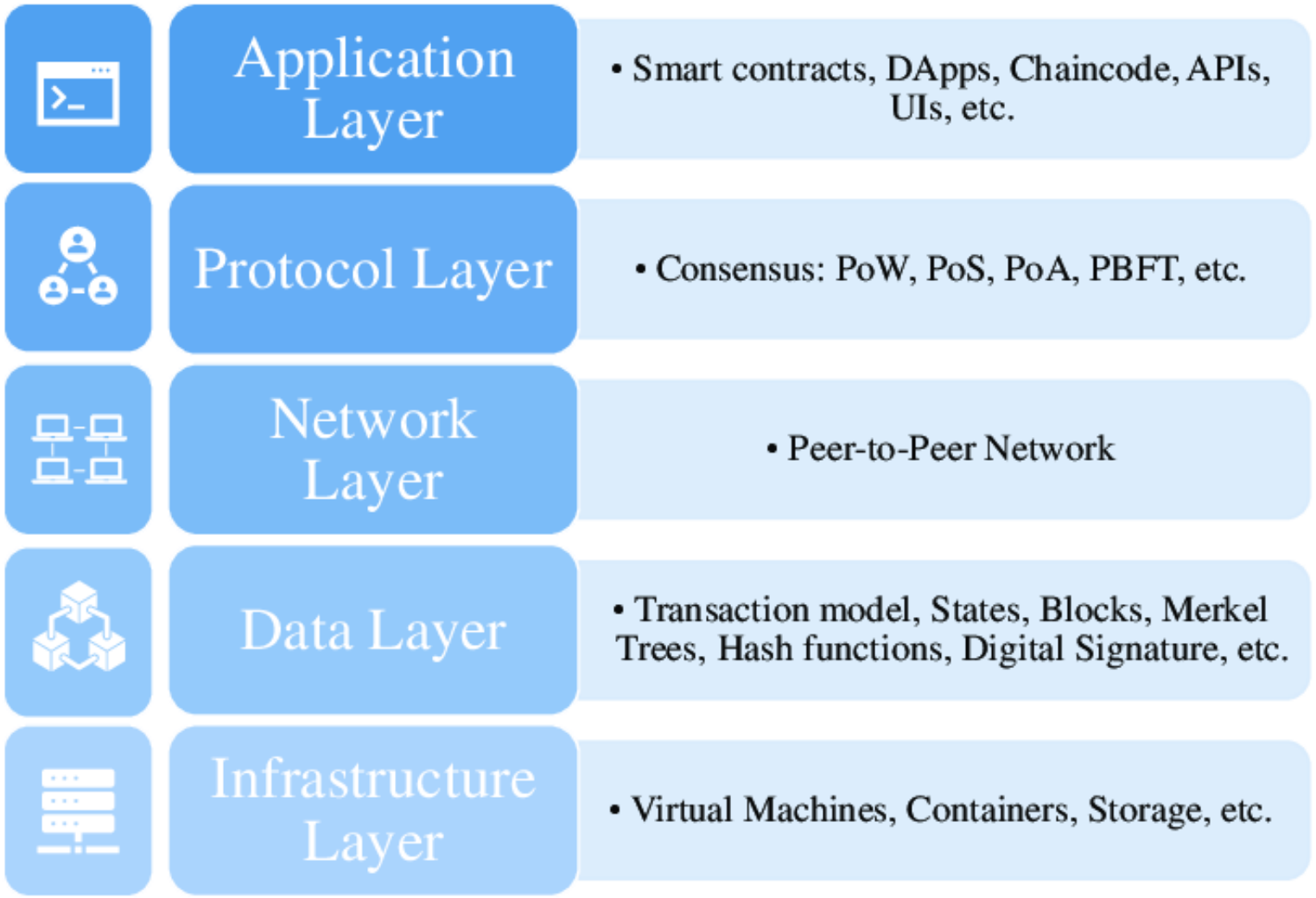


Abdelkader Ouared

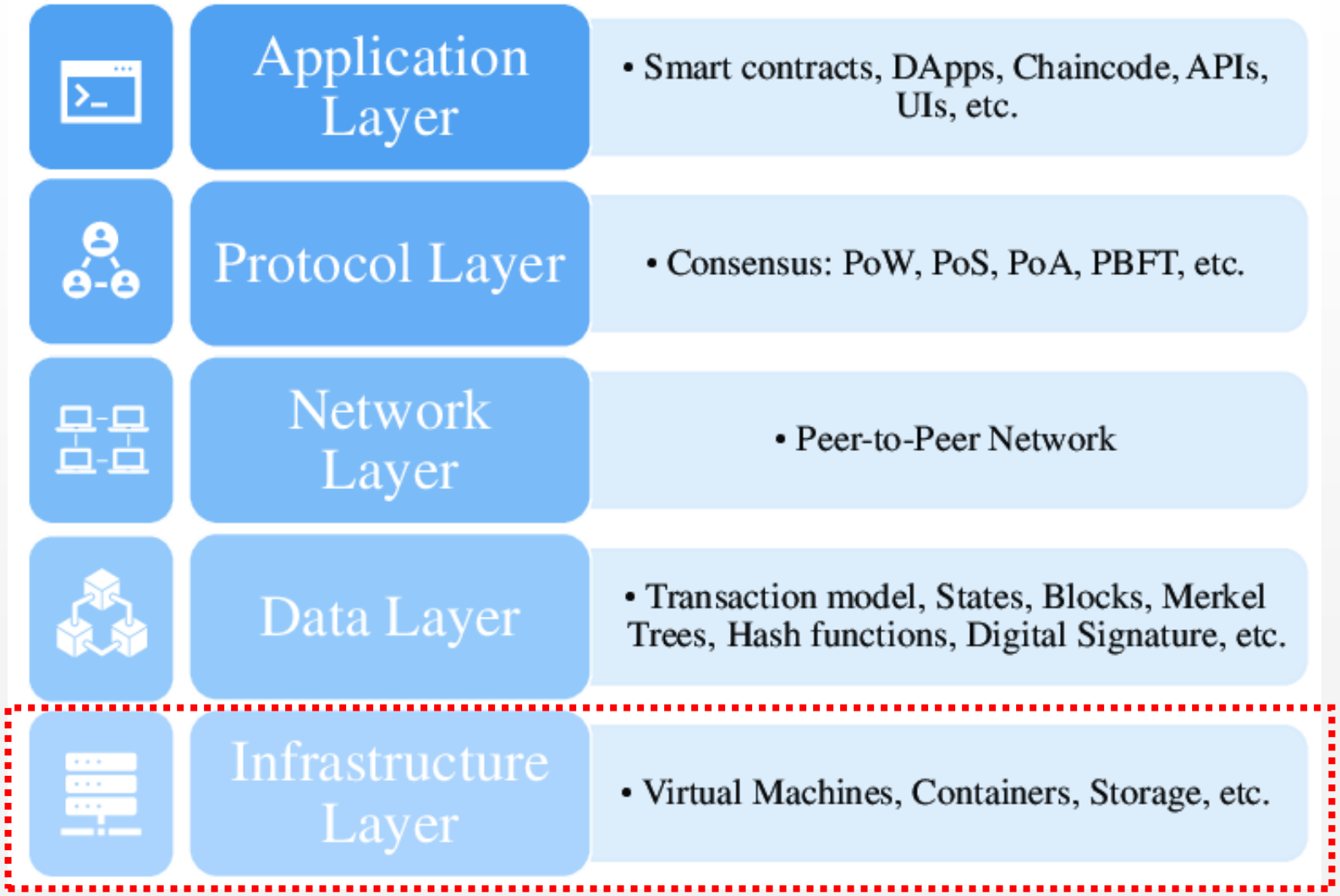
abdelkader.ouared@univ-tiaret.dz

@ouared

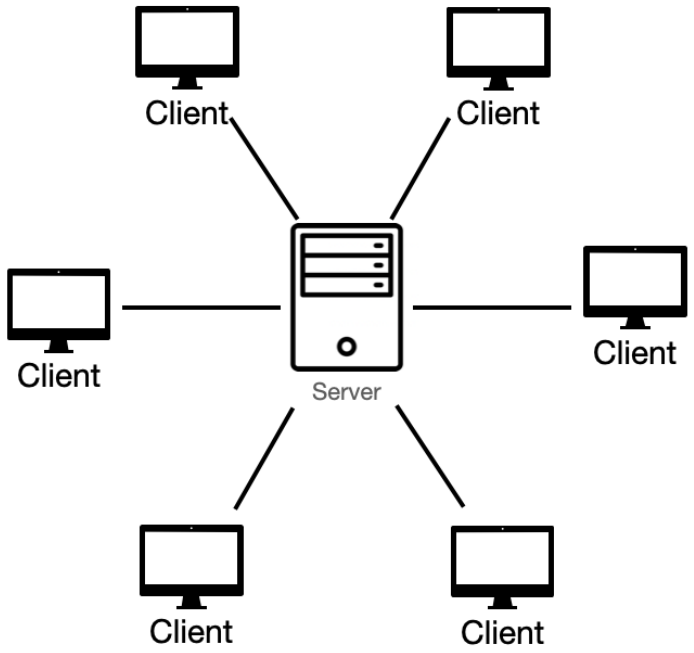
Les couches de blockchain



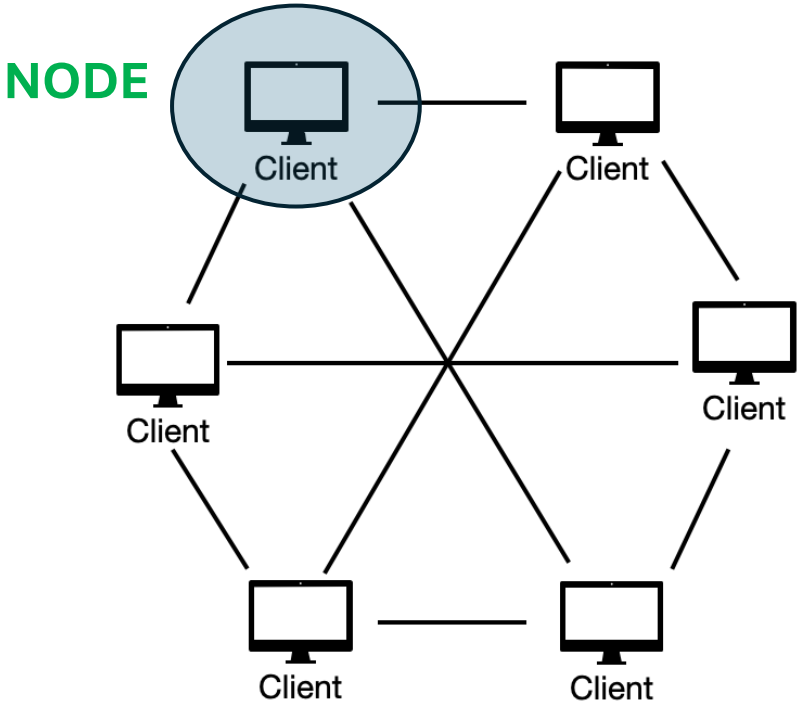
Les couches de blockchain



Couche d'Infrastructure Matérielle



Client Server Architecture



P2P Architecture

Communication entre les nœuds

- Découverte de nœuds
- Création de blocs
- Ajout de blocs
- Propagation

« peer-clients »plus rapide et plus facile

Un consensus sur la validité d'une transaction

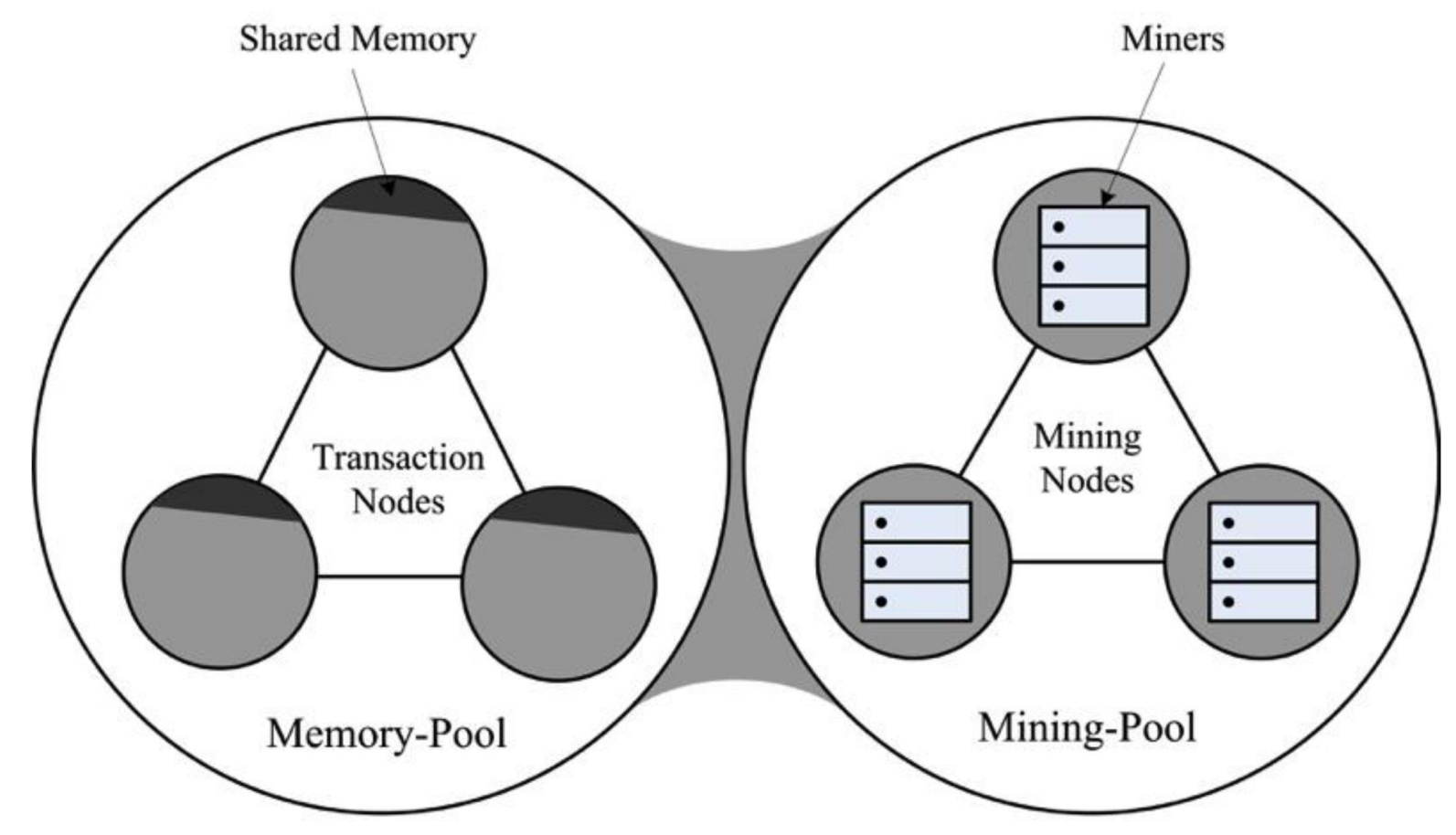
Couche d'Infrastructure Matérielle

Machine virtuelle, conteneurs, services, messagerie

Couche d'Infrastructure Matérielle

Technologie	Fonctionnalité
Machine Virtuelle (VM)	Exécute des smart contracts, garantit l'isolation et l'uniformité des calculs.
Conteneurs	Déploiement léger et rapide de nœuds blockchain, scalable et facile à gérer.
Stockage On-Chain	Données stockées directement dans la blockchain (transactions, contrats).
Stockage Off-Chain	Données volumineuses stockées hors blockchain, avec des références sur la blockchain.

Couche d'Infrastructure Matérielle



Blockchain en tant que service

GCP (Google Cloud Platform) n'a pas encore investi dans ce domaine. Actuellement, ils ne proposent aucun service lié à la **blockchain**. **Microsoft Azure** avait lancé un service appelé Azure Blockchain Service. Cependant, ils ont arrêté ce service en septembre 2021. Alors que **AWS** (Amazon Web Services) offre la solution cloud la plus complète pour ceux qui souhaitent se lancer dans la **blockchain**. AWS propose le service **Amazon Managed Blockchain** qui est un **BaaS** (Blockchain as a Service, ou Blockchain en tant que service).

X

X

Autre acteur de la blockchain sur le cloud

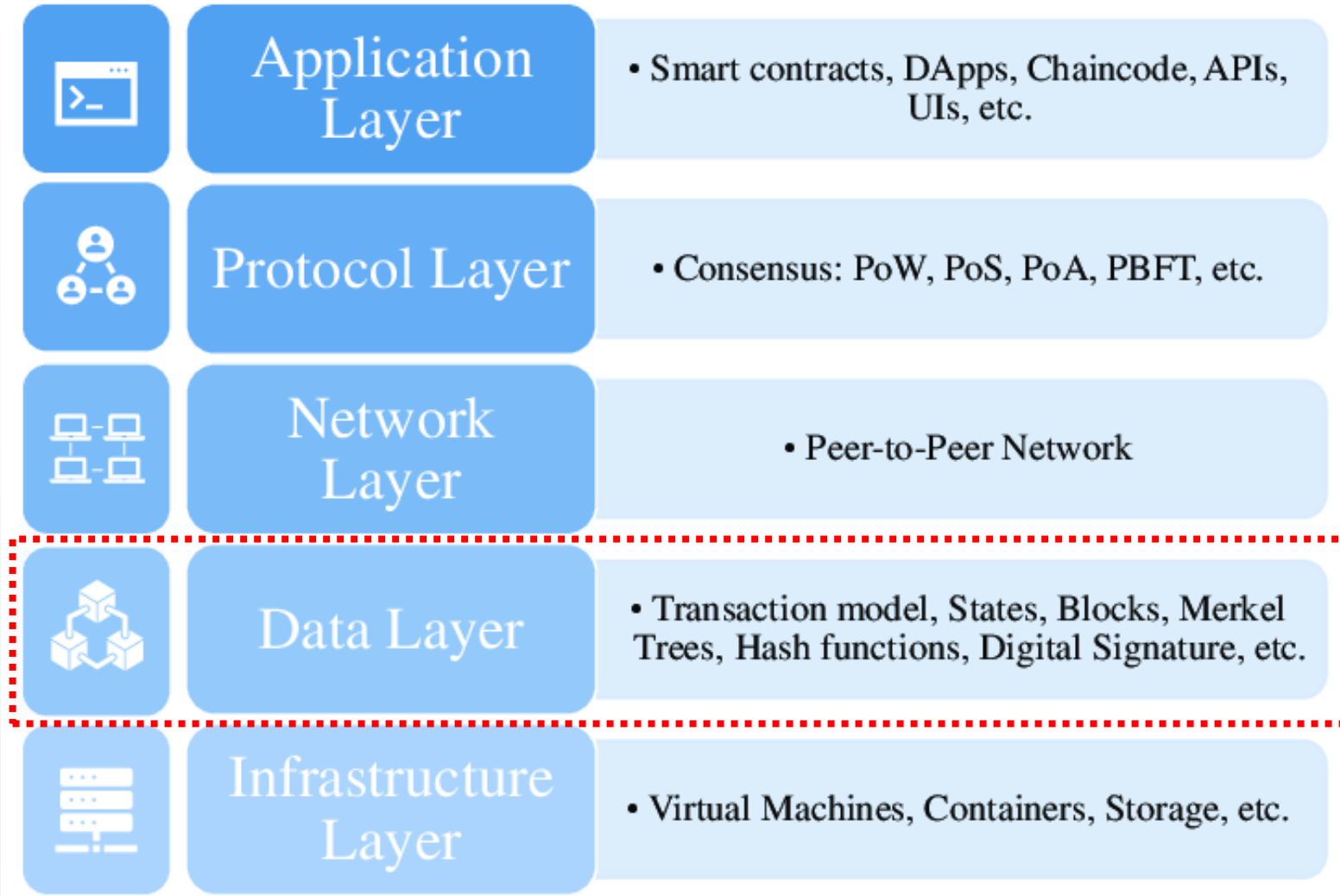
Les étapes clés pour la conception et le développement d'une solution blockchain: **Choix de l'Infrastructure**

1. **Identifier un cas d'utilisation approprié**
2. **Identifier le mécanisme de consensus le plus adapté**
3. **Identifier la plateforme la plus adaptée**
4. **Concevoir les nœuds**
5. **Concevoir l'instance blockchain**
6. **Développer les API**
7. **Concevoir l'interface utilisateur et l'administration**
8. **Ajouter des technologies futures**

Exemple:

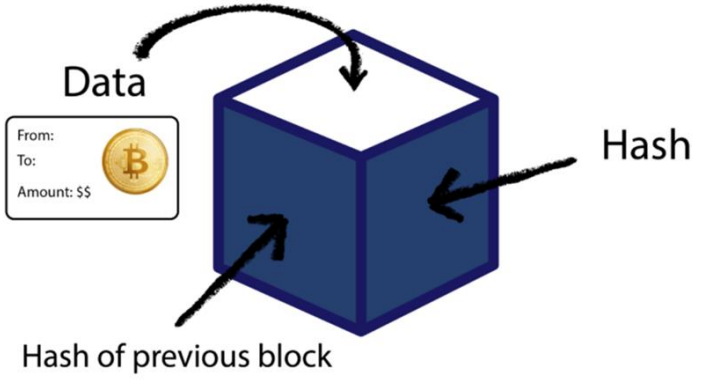
Si la scalabilité et les faibles frais sont essentiels, optez pour **Polygon**.
Pour une solution privée, préférez **Hyperledger Fabric**, et
pour l'interopérabilité, choisissez **Polkadot**.

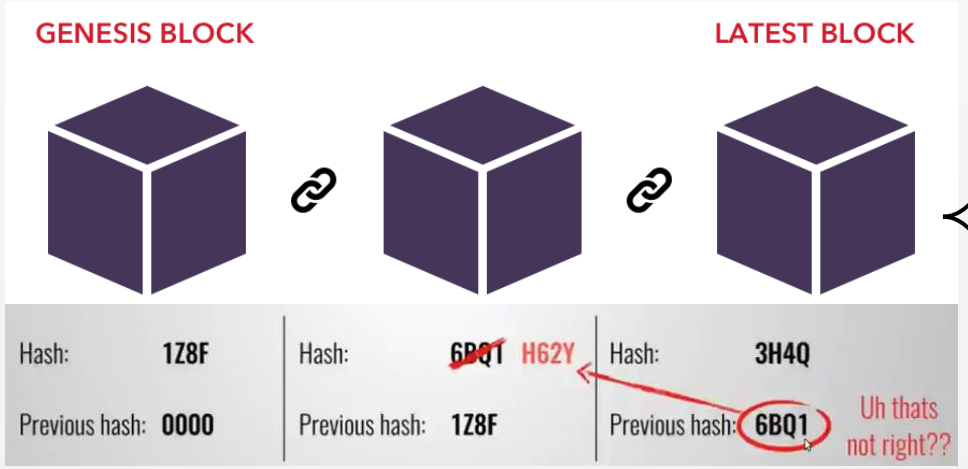
Les couches de blockchain

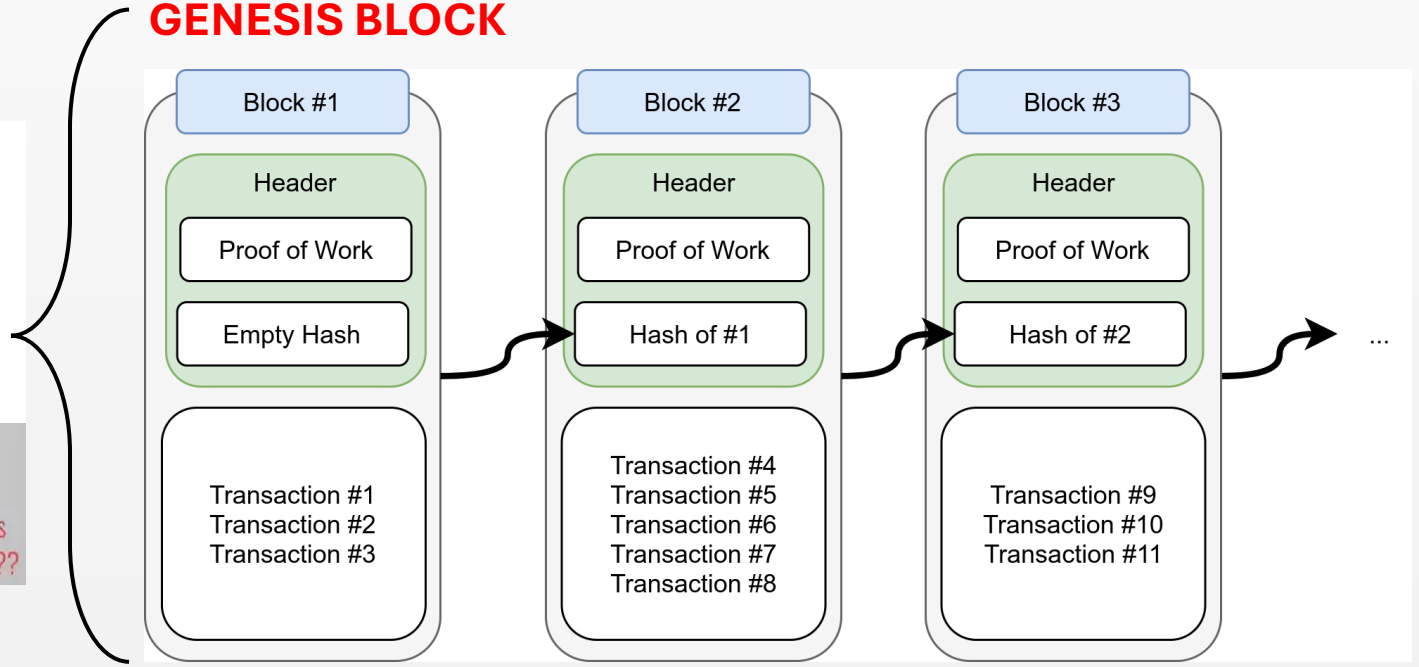


Couche de données: Data Layer

- **Bloc** contenant les données de transaction
- Les données sont traitées dans le bloc => Ajouter à la blockchain => lié au bloc de données précédent
- Le bloc **Genesis** est le premier bloc de la chaîne et ne peut donc pas être lié

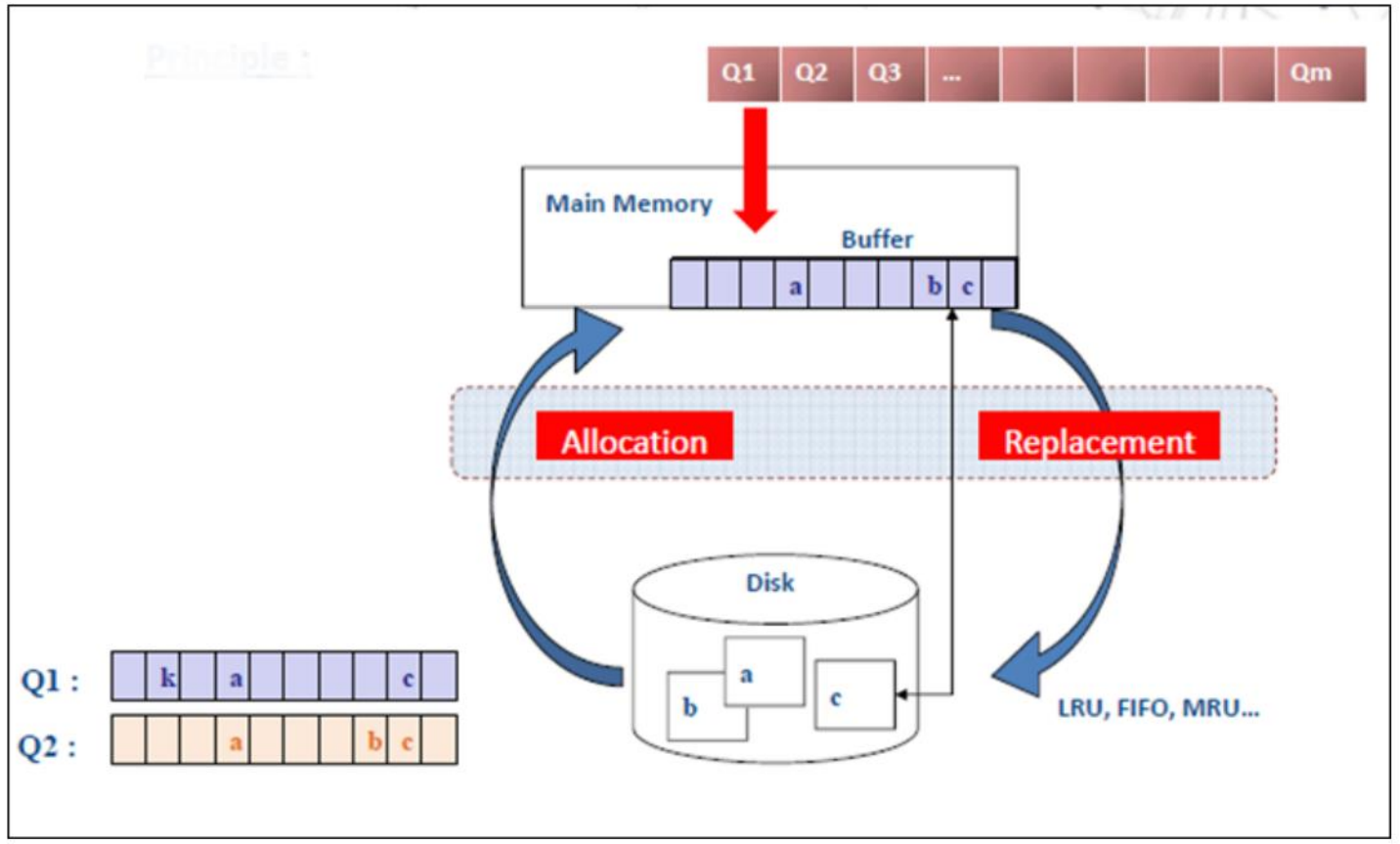






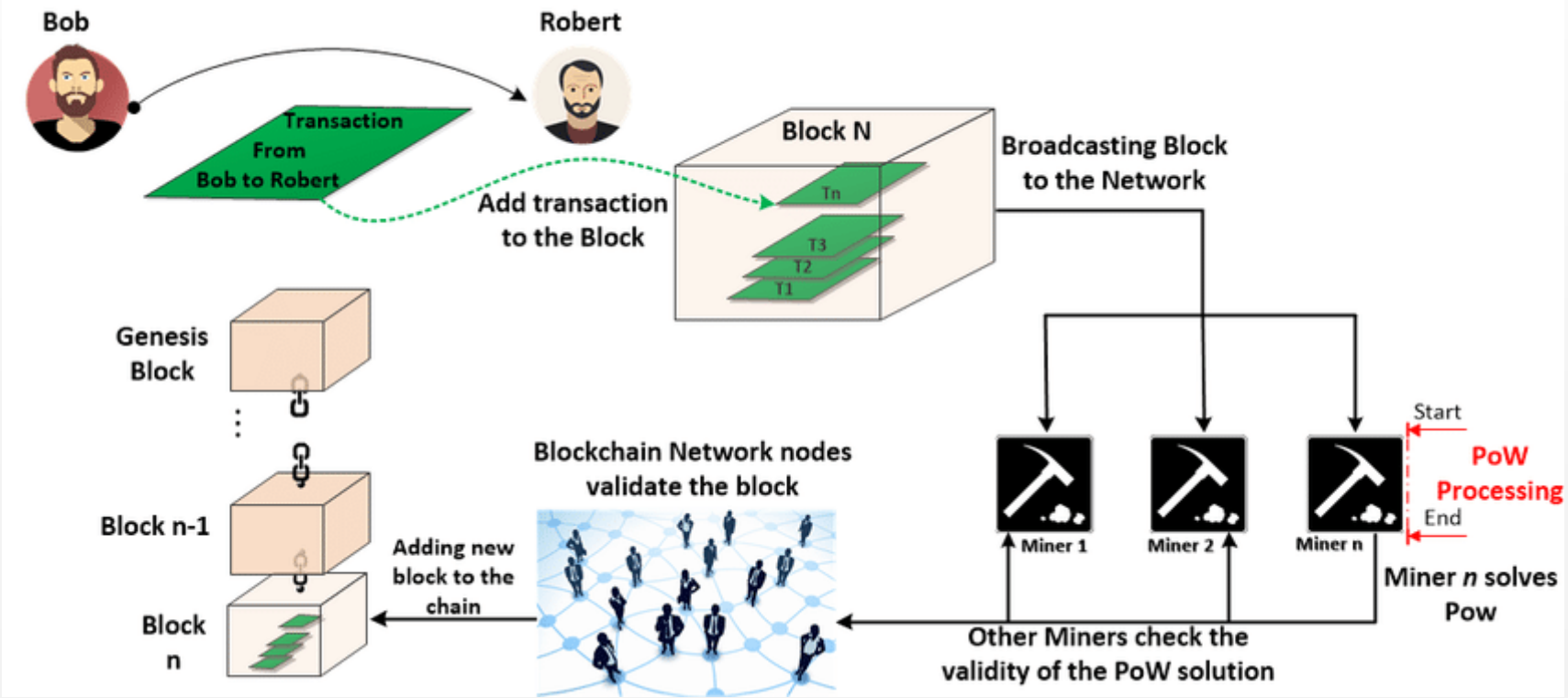
La notion de bloc c'est pas nouveau

- **Base de données structurée :** la base de données est un ensemble de **blocs**
- Un bloc est un ensemble <u>de tuples</u>
- **Facteur de blocage**: Le facteur de blocage désigne le nombre maximal de tuples ou d'enregistrements qu'un bloc peut contenir.

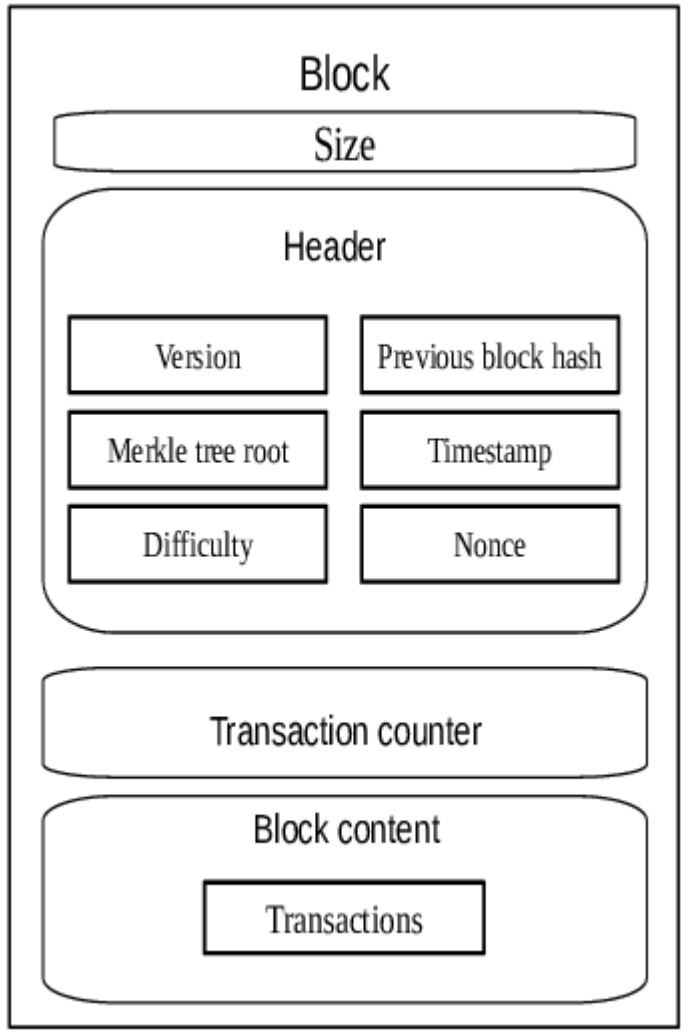


Notion de block

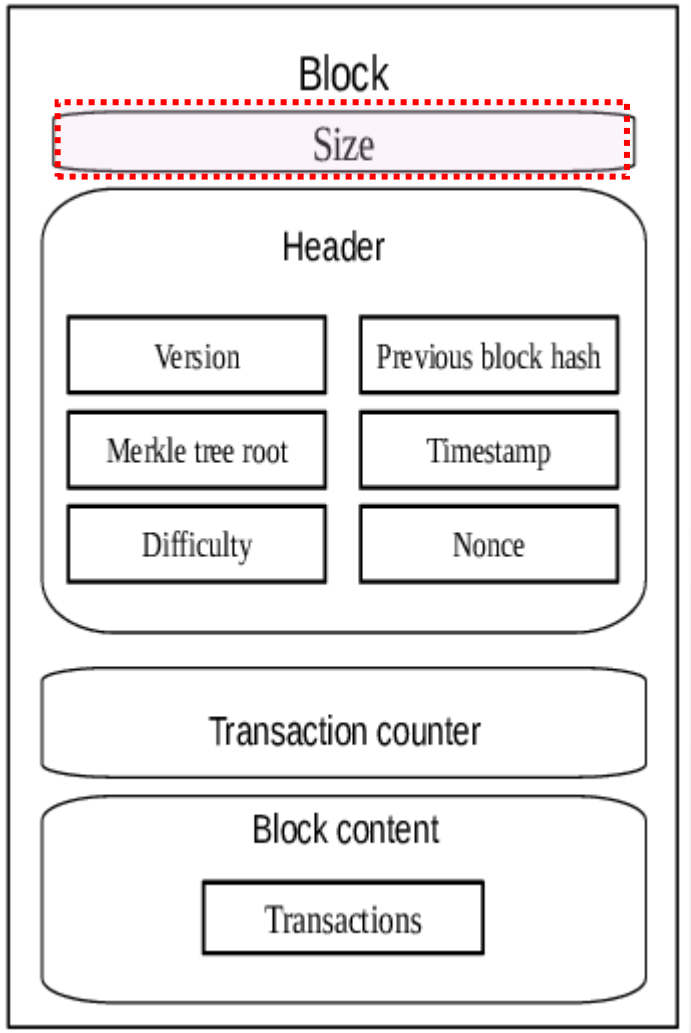
- un bloc peut contenir plusieurs transactions, mais une transaction ne peut **pas être ajoutée** à un bloc déjà existant, car les blocs précédemment validés **sont immuables**.
- Un bloc dans une blockchain ne concerne pas un seul utilisateur. Il peut contenir plusieurs transactions provenant de plusieurs utilisateurs



Que contient chaque bloc ?



Que contient chaque bloc ?



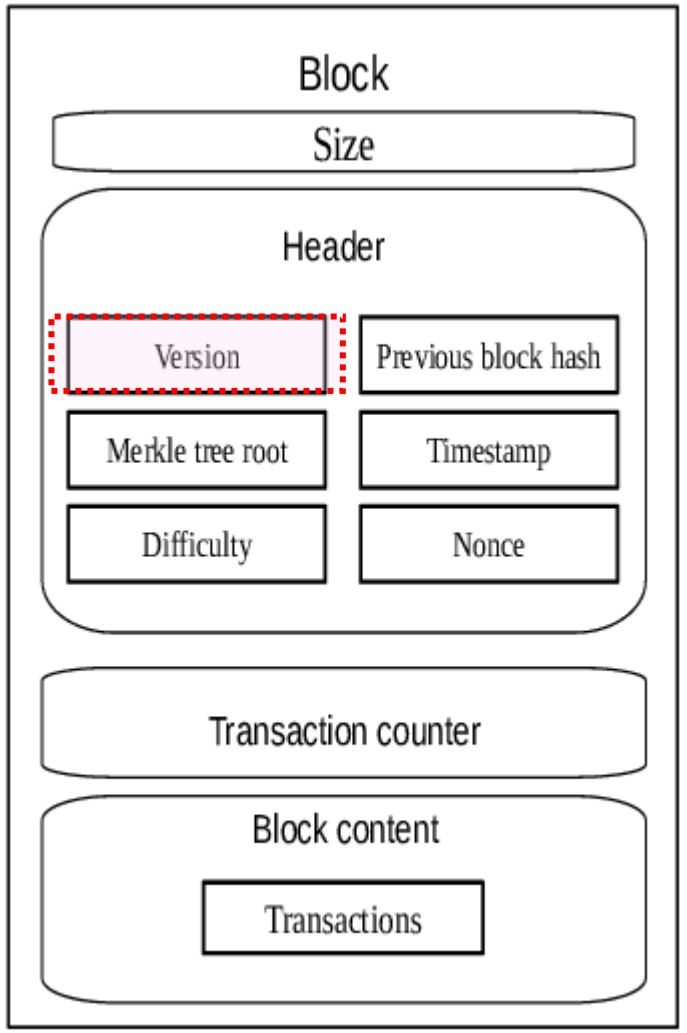
- ***Généralement*** Chaque bloc a une taille maximale définie

  (Exemple: blockchains Bitcoin est fixée à 1 Mo)

- Taille effective d'un bloc peut varier en fonction des données qu'il contient
- D'autres blockchains, comme Ethereum, n'ont pas une taille de bloc fixe mais utilisent plutôt un système pour mesurer la capacité d'exécution des transactions. Cela signifie que le bloc peut avoir une taille variable en fonction de la complexité des transactions

.

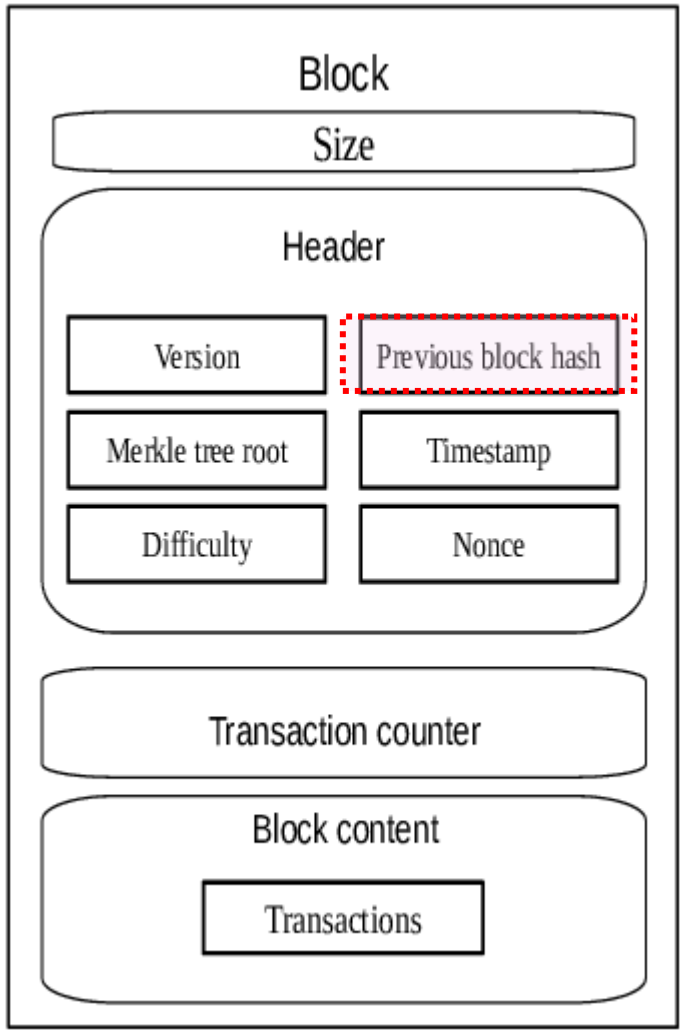
Que contient chaque bloc ?



- **Version:**
  - La version d'un bloc dans une blockchain désigne le numéro qui identifie la version du protocole utilisé pour créer ou valider ce bloc.

- **Pourquoi la Version est Importante ?**
  - **Compatibilité** : Assure que tous les nœuds suivent les mêmes règles.
  - **Évolutivité** : Permet d'introduire de nouvelles fonctionnalités ou corrections de sécurité.
  - **Gestion des mises à jour** : Indique quels types de transactions ou structures sont acceptés selon la version.
- **Exemple :**
  - Version 1.0 : Première version de la blockchain avec des règles de base.
  - Version 2.0 : Amélioration des algorithmes de consensus ou nouvelles fonctionnalités ajoutées.

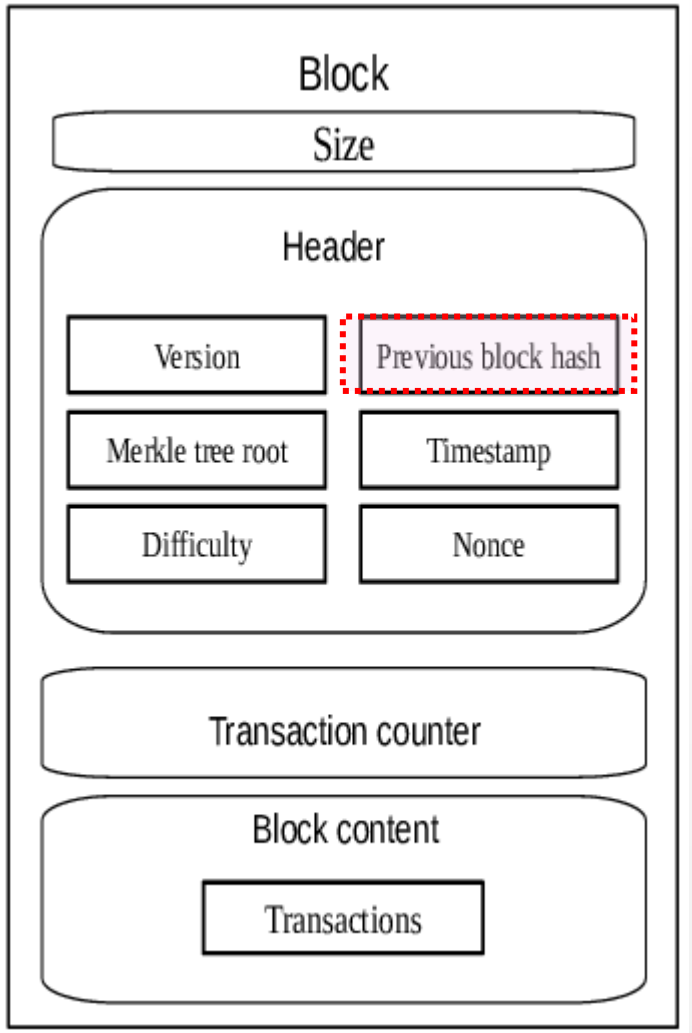
Que contient chaque bloc ?



- **Sécurité:**
  - On ne sait pas prouver **que les fonctions de hachages** utilisées en pratique sont résistantes aux collisions
  - En 2004, une équipe de recherche chinoise a trouvé un moyen de calculer des collisions pour MD5 est une heure. Il est aujourd'hui recommandé de ne plus l'utilisé

  - Le hash d'un fichier est une petite chaine de bits qui caractérise le fichier:
    - Signature du hash
    - Stockage de mot de passe
    - Vérifier l'intégrité
    - **Créer une blockchain**

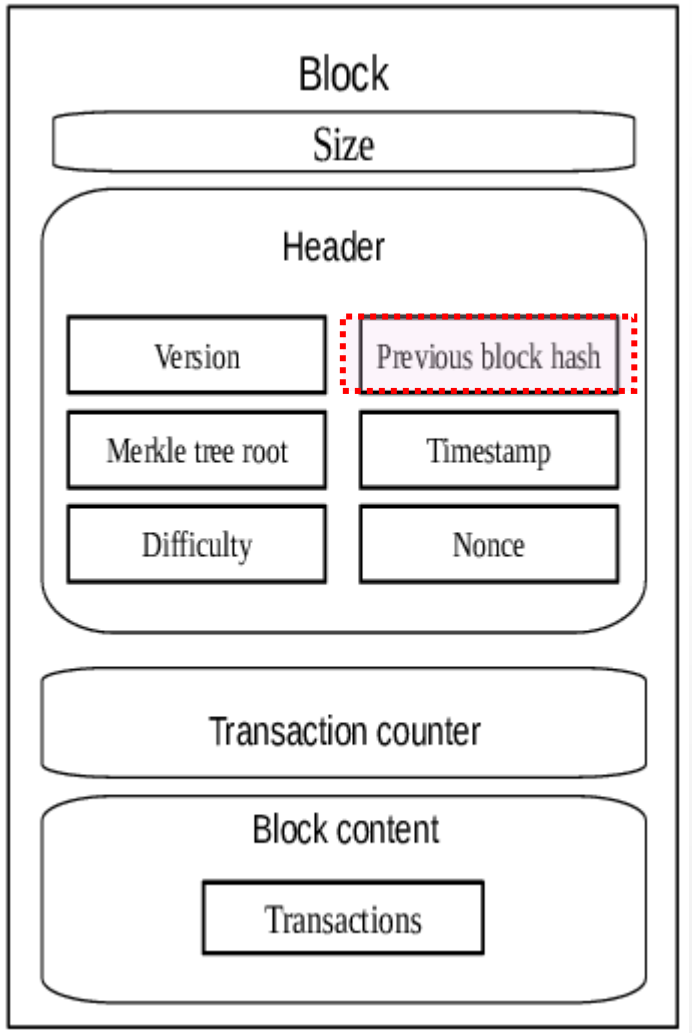
Que contient chaque bloc ?



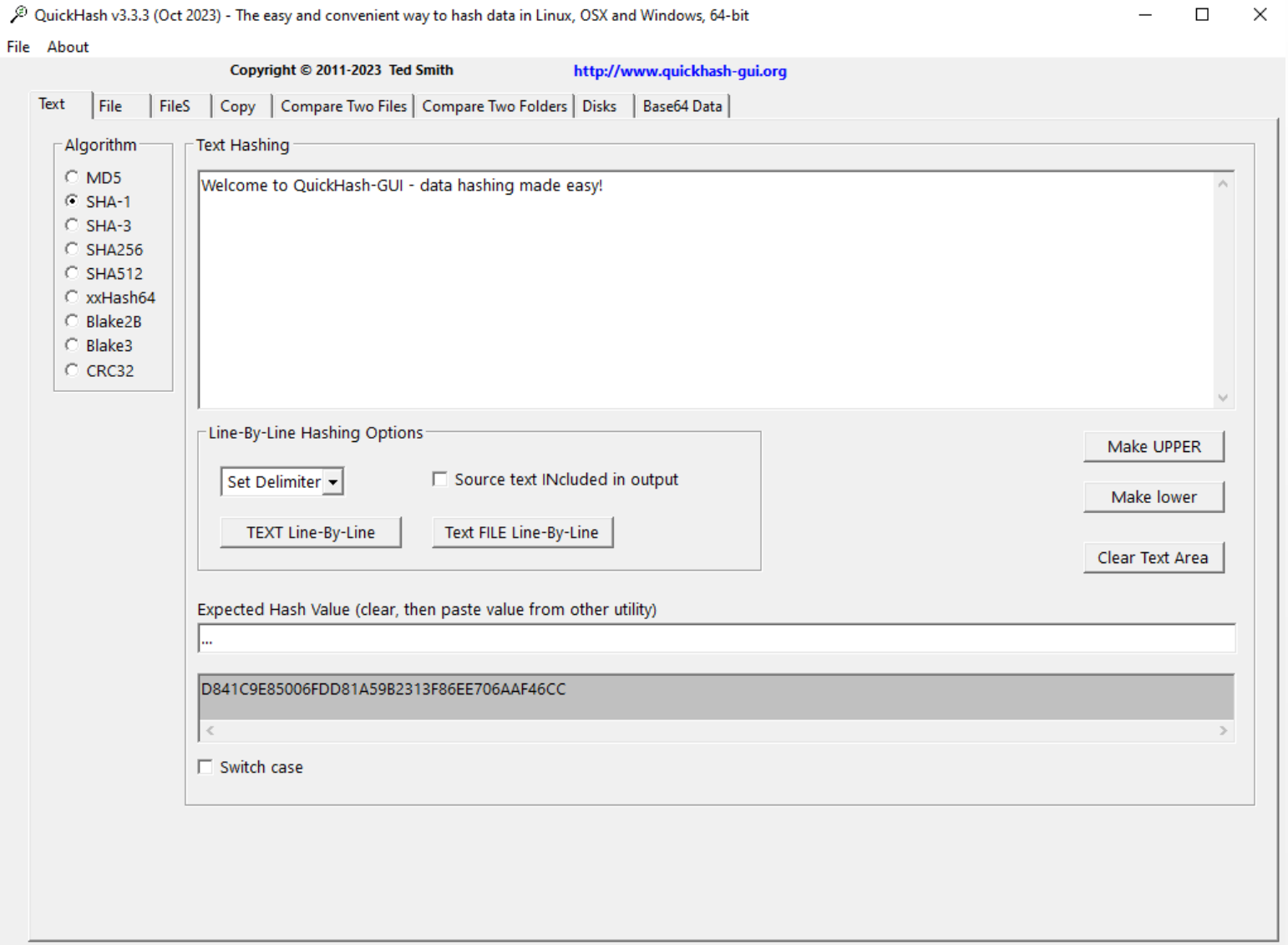
❑ **Sécurité cryptographique**

- **Hachage** : La blockchain utilise des fonctions de hachage cryptographique (par exemple, SHA-256 pour Bitcoin) pour garantir l'intégrité des transactions. Chaque bloc contient le hachage cryptographique du bloc précédent, ce qui rend pratiquement impossible la modification des données sans être détecté.
- **Cryptographie à clé publique/privée** : Les transactions sont sécurisées grâce à un système de cryptographie à clé publique et privée. L'utilisateur signe une transaction avec sa clé privée, et elle peut être vérifiée par n'importe qui avec la clé publique, garantissant l'authenticité sans compromettre la confidentialité.
- **Immutabilité** : Une fois les données enregistrées dans une blockchain, il est extrêmement difficile de les modifier. Cette immutabilité garantit que les données, une fois vérifiées, ne peuvent être altérées, ajoutant ainsi un niveau de sécurité supplémentaire.

Que contient chaque bloc ?

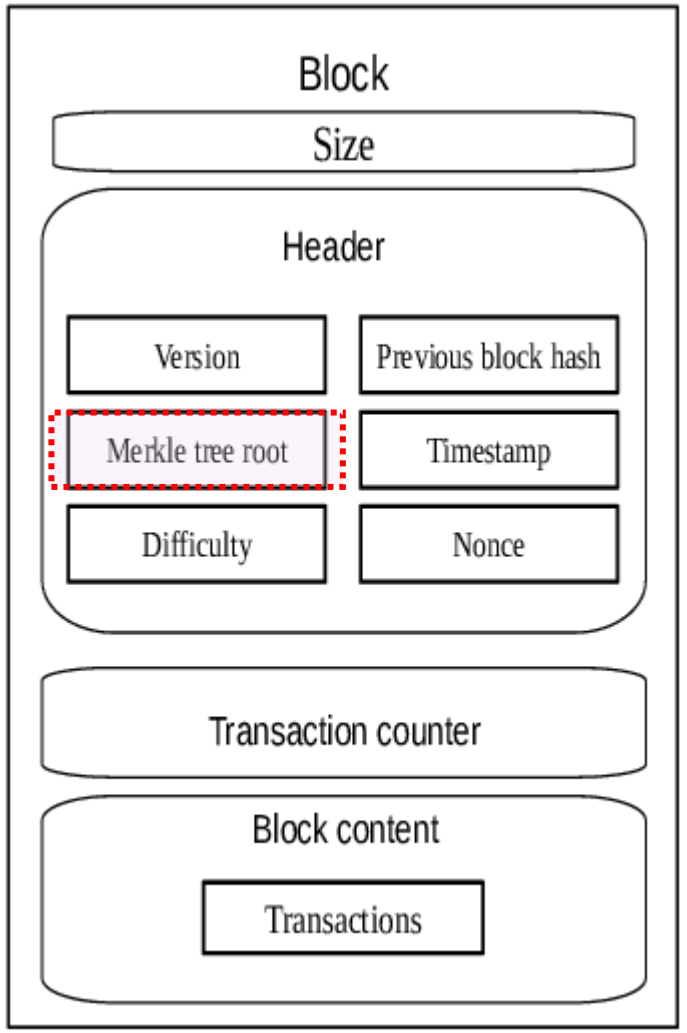


Exemple: **QuickHash-GUI (**)**



https://github.com/tedsmith/quickhash

Que contient chaque bloc ?



BLOCK 1

Transaction #1

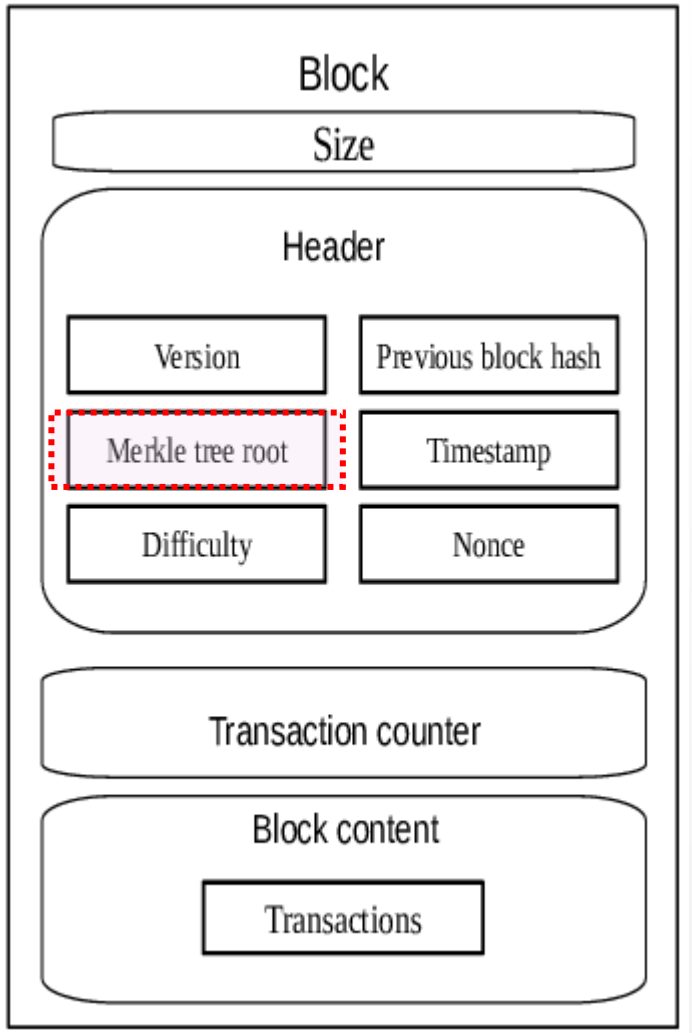
Hachage SHA-256 :
"8a4d7e9a6dcf13b9be1d580f013df47de9c9e12
f8ef4777f4e4dc32b9a2ebde4"

BLOCK 2

Transaction #4
Transaction #5
Transaction #6
Transaction #7
Transaction #8

Hachage SHA-256 :
9c1b80a53ed9e8d8e3b2e3c29f1fa1f3a6b2c08b
374e3d5c1bb5dc0422c60ae6

Que contient chaque bloc ?

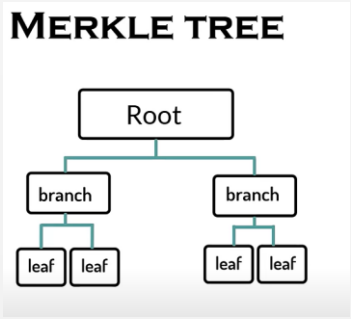


BLOCK 2

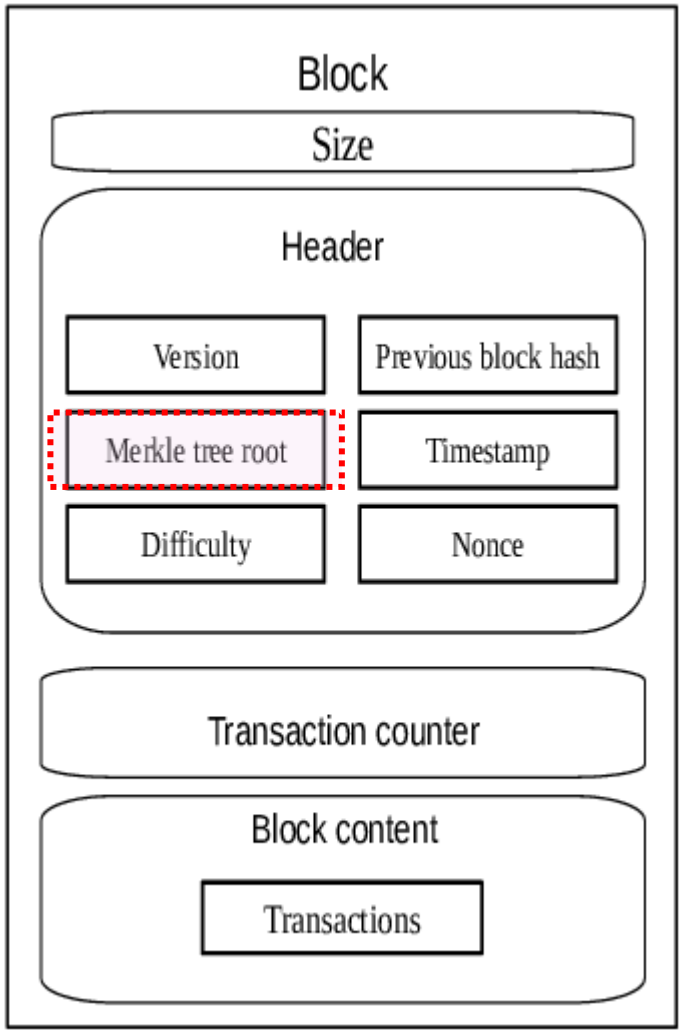
Transaction #4	f10f4737e87879cba3f2722447ab572cf9e4bfcff57180c1e94b0197c72a3c75
Transaction #5	f87a18c1e6a21cc53cd519d6766e38c1e5c5f91f5f5d8c0c5c1b431f76de76db
Transaction #6	ecf72f64bbf456d9995ccf5ee03de87aa47a02bca3ee0c5e6fa4c2e6d6d84726
Transaction #7	7c7ed03317cde545e9d6b8a3d3d11e5ee06d0e2c00d8cb4a9e90fbd17e95d1f9a
Transaction #8	8f5efb33c64458ac0a362eec4ae256d7be9606ae35d06f99aa03d2d61c5a4912

9c1b80a53ed9e8d8e3b2e3c29f1fa1f3a6b2c08b374e3d5c1bb5dc0422c60ae6

- **Comment implémenter cette solution => Merkle tree**



Que contient chaque bloc ?



Ralph Merkle

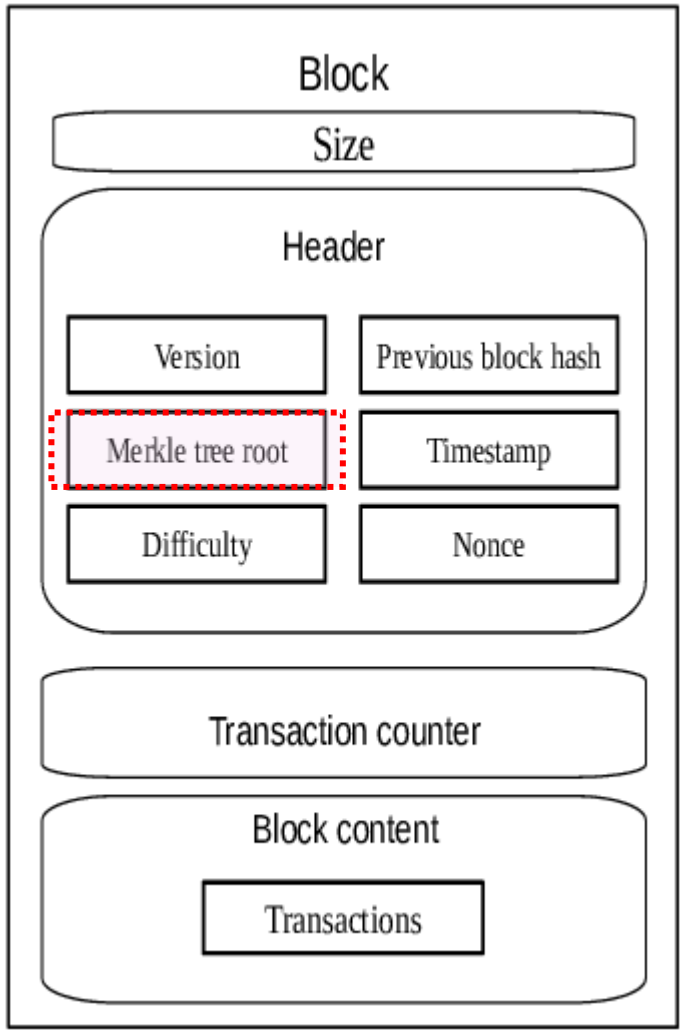
Le **Merkle Root** est une valeur hachée qui résume toutes les transactions contenues dans un bloc de la blockchain. Il est dérivé d'une structure appelée **arbre de Merkle**.

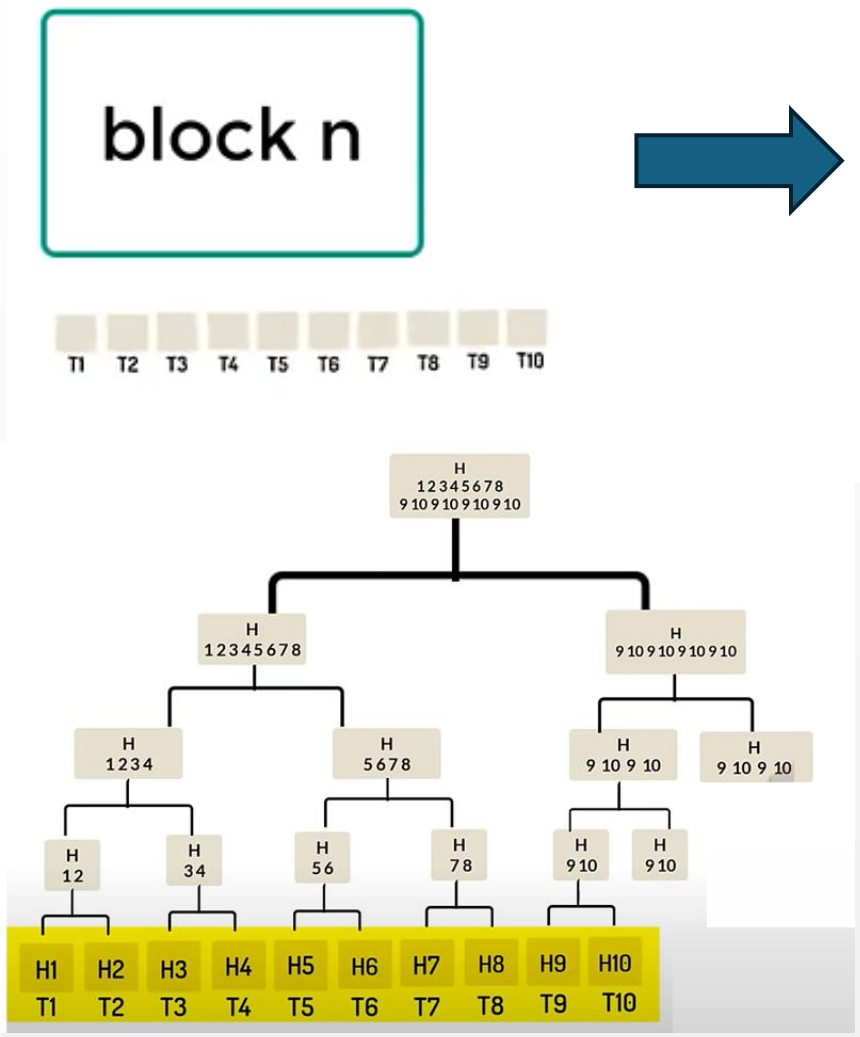
Importance du Merkle Root :

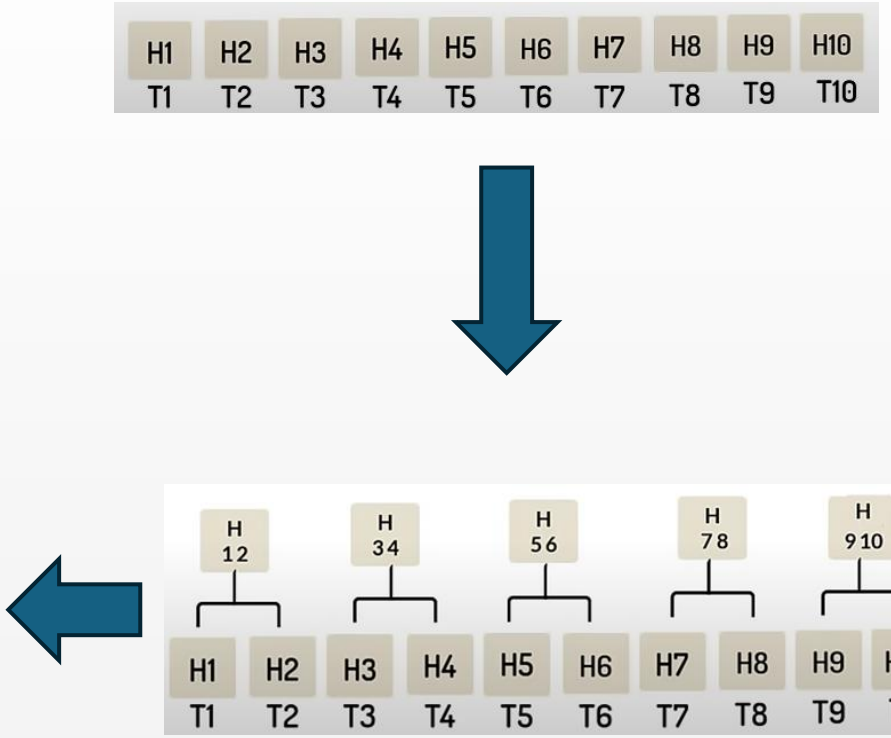
- **Efficacité** : Le Merkle Root permet de vérifier si une transaction particulière fait partie du bloc sans avoir à stocker ou vérifier toutes les transactions.

Ralph C. Merkle (né le 2 février 1952), est un cryptographe américain et chercheur en nanotechnologie

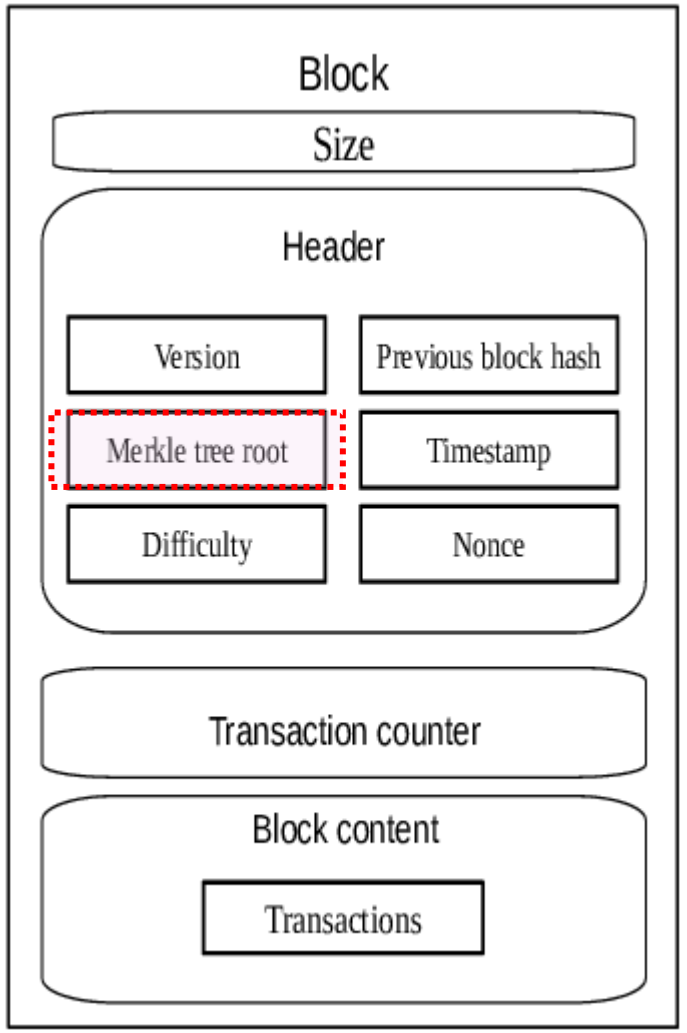
Que contient chaque bloc ?



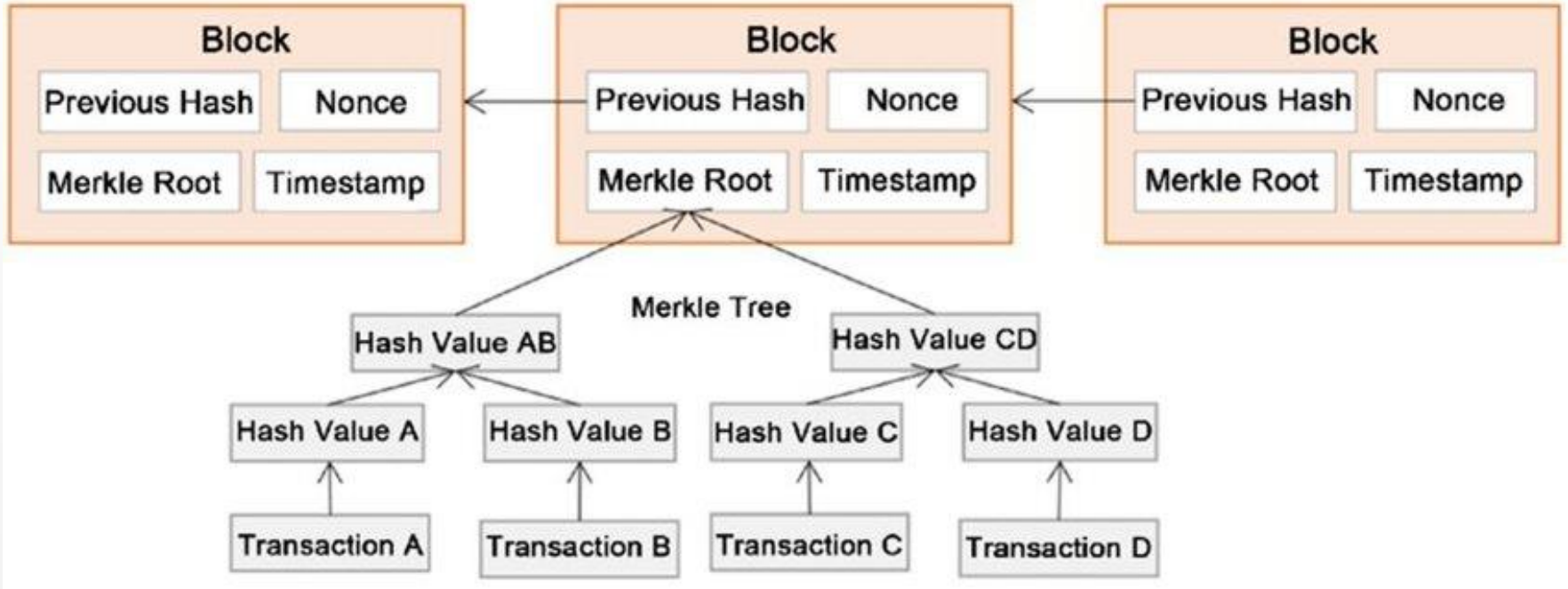




Que contient chaque bloc ?

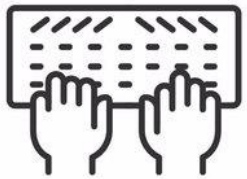


Arbre de Merkle (Merkle Tree)

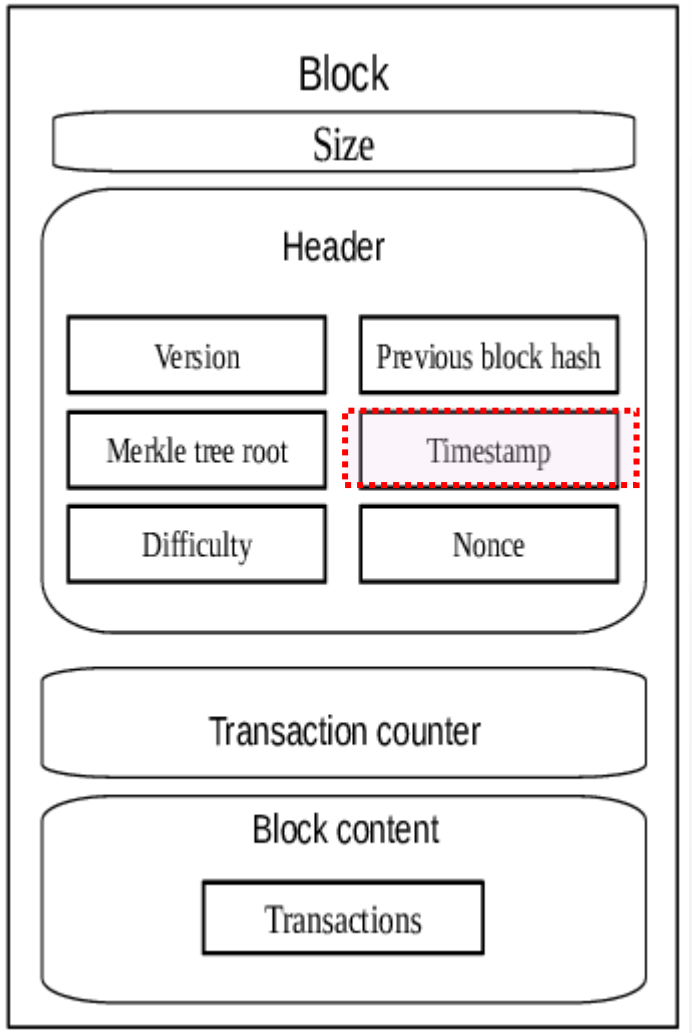


Exercice

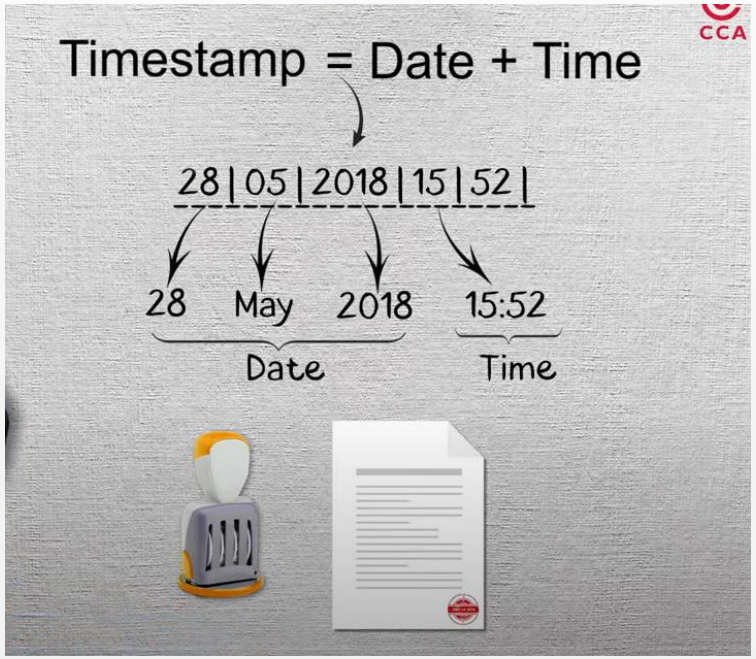
Écrire un programme pour la création d'un arbre de Merkle en Python



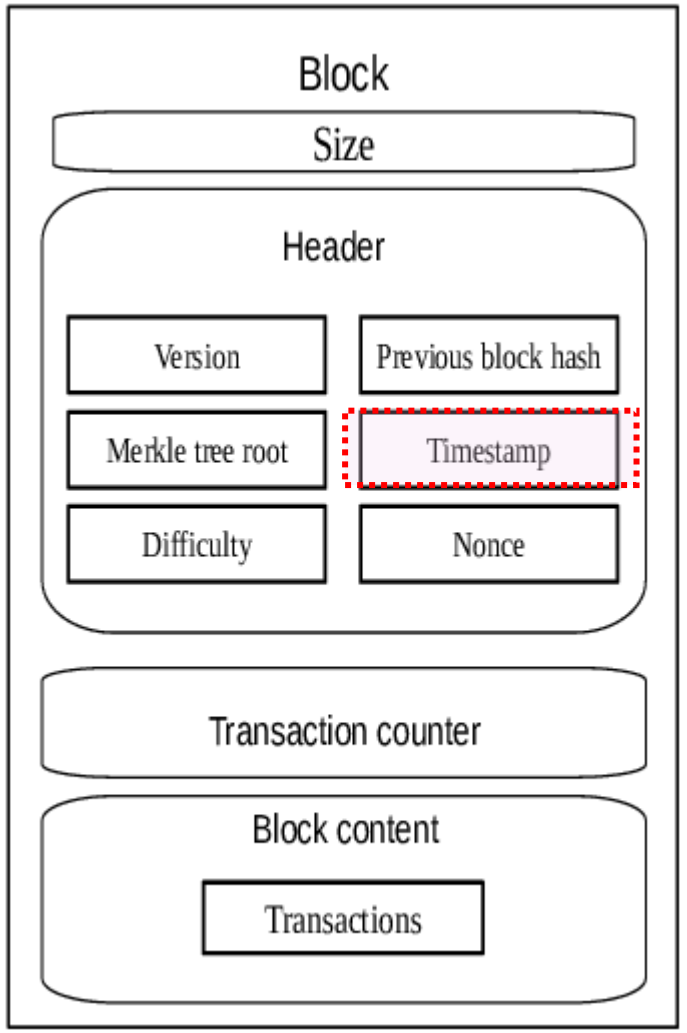
Que contient chaque bloc ?



- Un **timestamp** indiquant la date et l'heure exacte de création d' une transaction ou un événement .
- Ce **timestamp** est un élément clé pour garantir l'ordre des événements dans une blockchain décentralisée.

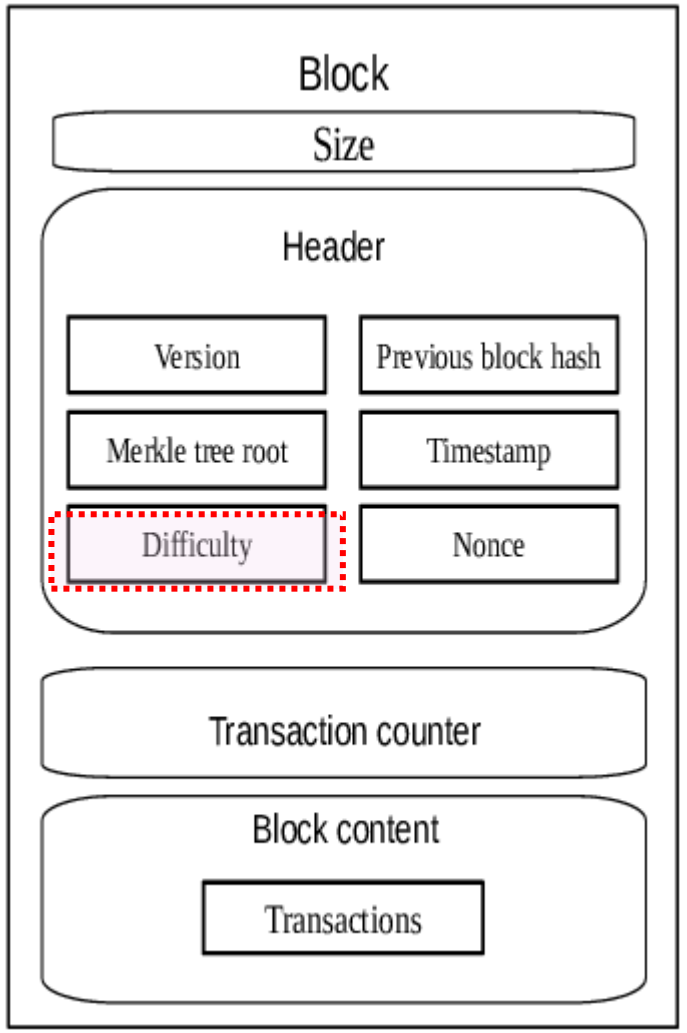


Que contient chaque bloc ?



- **Importance du Timestamp dans la Blockchain**
- Le **timestamp** garantit :
  - **L'ordre des transactions** : Il permet de savoir laquelle des transactions a eu lieu en premier.
  - **La validité des blocs** : Dans un système décentralisé, les nœuds utilisent l'horodatage pour vérifier la cohérence des données partagées.
  - **La sécurité** : Comme les données d'une blockchain sont immuables, un timestamp protège contre la manipulation des transactions.

Que contient chaque bloc ?



Pourquoi?

- **But** : Garder un rythme régulier dans la création de nouveaux blocs, généralement tous les 10 minutes dans le cas de Bitcoin
- **Solution**: Critère de Difficulté

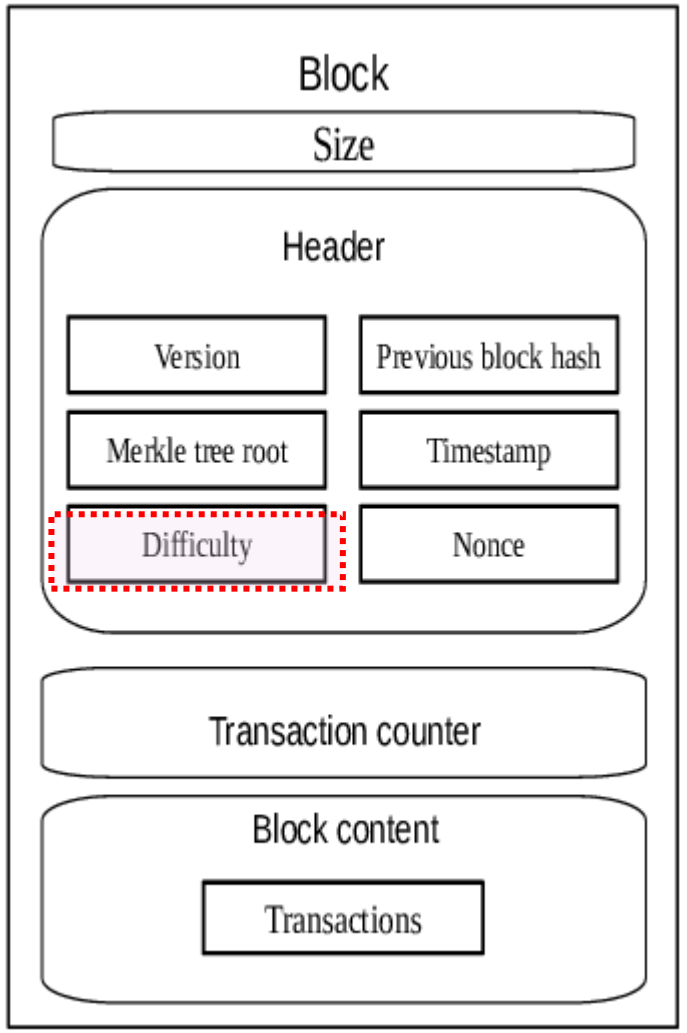
Critère de Difficulté : La difficulté dans une blockchain détermine combien il est difficile de créer un nouveau bloc. Elle est ajustée pour que les blocs soient ajoutés à la chaîne à un rythme régulier

vous lancez un dé (c'est comme générer un hachage

Nombre Secret: 10
Hachage : Pour deviner le nombre

- **Fonctionnement du Critère de Difficulté:**
  - **Difficulté Initiale** : nombre secret est **10**. Vous lancez le dé et essayez de deviner. Supposons que cela prend en moyenne 5 lancers
  - **Ajustement de la Difficulté** :
    - **Si Trop de Gagnants** : Si beaucoup de joueurs devinent rapidement, le nombre secret devient **5** pour rendre le jeu plus difficile (c'est comme augmenter la difficulté).
    - **Si Trop Lents** : Si personne ne trouve un nombre inférieur à 10 après beaucoup de lancers, le nombre secret devient **15** pour faciliter le jeu (c'est comme diminuer la difficulté).

What does each block contains ?

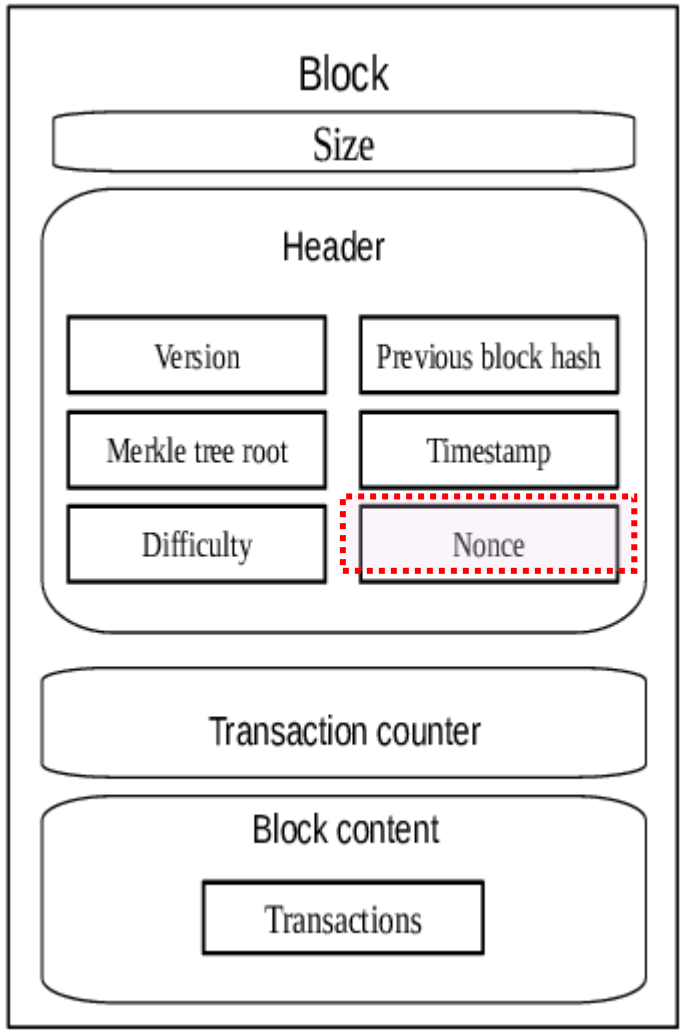


- **Hachage** : Le hachage est une fonction qui prend une entrée (ou un ensemble de données) et produit une sortie fixe, appelée hachage. Pour Bitcoin, la fonction utilisée est SHA-256.
- **Nonce** : Les mineurs ajoutent un nombre arbitraire appelé nonce (number used once) au bloc de données (qui contient les transactions et un lien vers le bloc précédent) pour générer un hachage. Le nonce est modifié pour essayer de trouver un hachage qui répond à des critères spécifiques.
- **Critère de Difficulté :** Le hachage du bloc doit être inférieur à une certaine valeur cible, déterminée par le niveau de difficulté du réseau. Ce critère de difficulté est ajusté environ toutes les deux semaines pour maintenir un temps moyen de création de blocs de 10 minutes.

Équation du puzzle cryptographique

$$\text{Hash}(\text{Bloc\_Header} + \text{Nonce}) < \text{Cible}$$

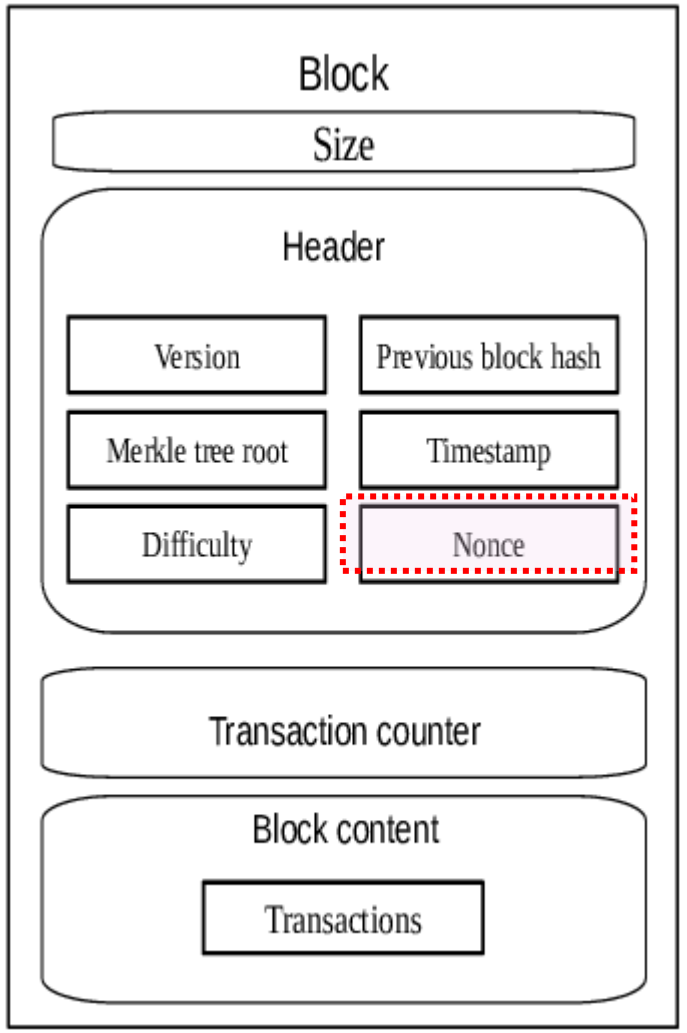
Que contient chaque bloc ?



Le Puzzle Cryptographique

- Les mineurs doivent résoudre un problème mathématique spécifique (appelé un **puzzle cryptographique**). Ce problème implique de trouver un certain nombre, appelé le **nonce**, qui, lorsqu'il est combiné aux transactions du bloc et passé dans une fonction de hachage (SHA-256 pour Bitcoin), donne un résultat qui satisfait certaines conditions (le hachage doit commencer par un certain nombre de zéros).
- **Le problème à résoudre est aléatoire et très difficile**, mais facile à vérifier une fois résolu. Cela demande énormément de **puissance de calcul**, et c'est pourquoi les mineurs utilisent des machines puissantes (des ASICs) pour essayer de deviner le bon nonce le plus rapidement possible.

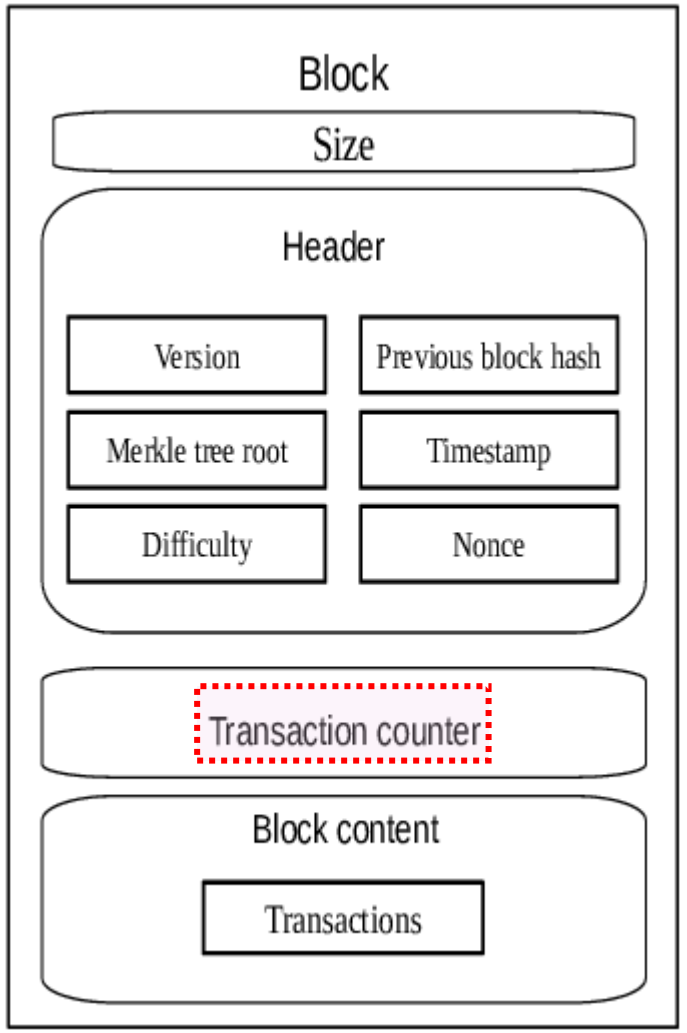
Que contient chaque bloc ?



- Le **mining** est le processus par lequel les transactions sont validées et ajoutées à la blockchain, en particulier dans les systèmes utilisant la preuve de travail (PoW), comme Bitcoin. Ce processus implique plusieurs étapes clés :
  - Calcul Complexe
  - Accéder à un Bloc Spécifique :
  - Hash
  - Approuver les Transactions

Bitcoin Mining Rig 13-GPU READY ULTRA PREMIUM Cryptocurrency Miner BITPUNISHER | eBay

What does each block contains ?



Compteur de Transactions en Blockchain

Un compteur de transactions suit le nombre de transactions associées à un compte ou une adresse blockchain. Ses principaux objectifs sont :

1.Prévention des attaques de répétition :

1. Le compteur garantit l'unicité des transactions. Il s'incrémente à chaque transaction, rendant les doublons invalides.

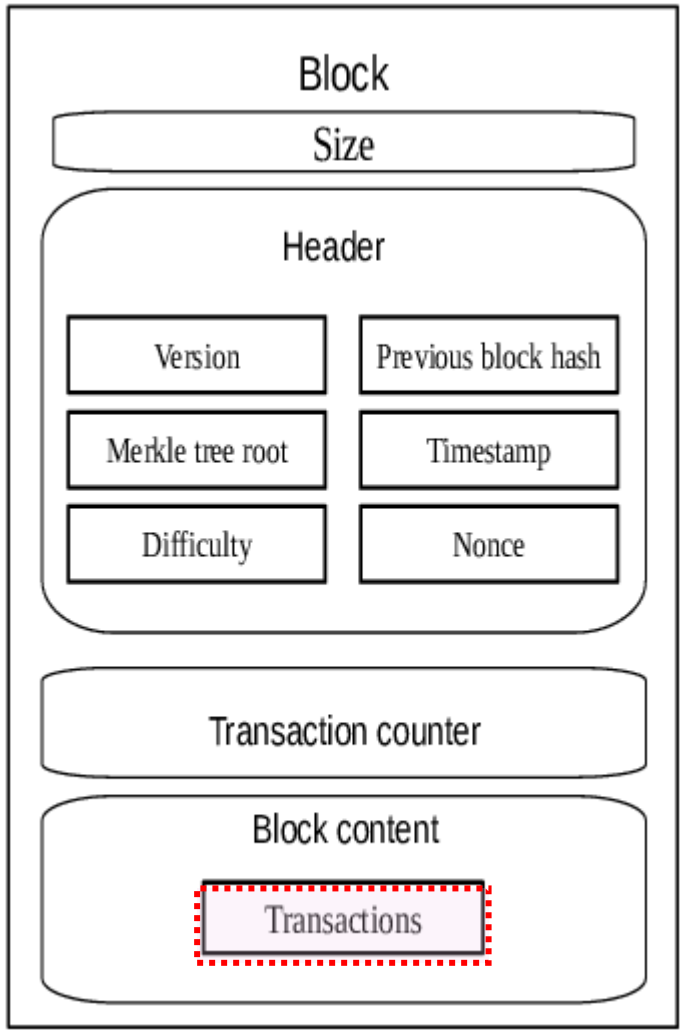
2.Ordonnancement des transactions :

1. Assure que les transactions sont traitées dans l'ordre, les plus anciennes avant les plus récentes.

Exemples :

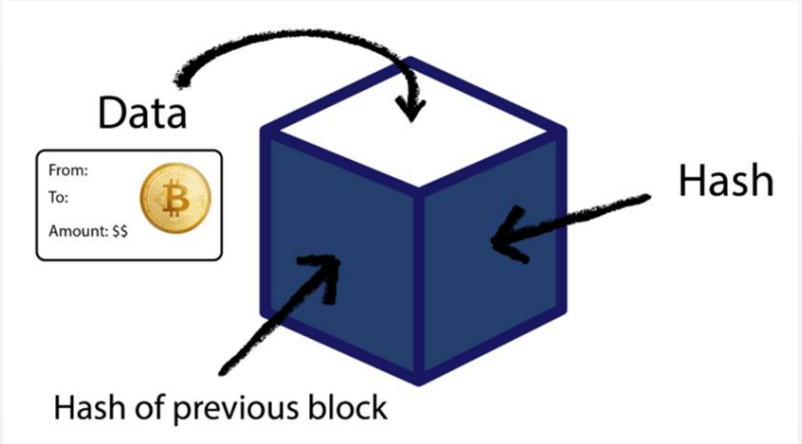
- **Ethereum :** Le compteur s'incrémente avec chaque transaction. Si un compteur est hors séquence, la transaction est invalide.
- **Bitcoin :** Utilise des entrées et des sorties pour garantir l'unicité, évitant la double dépense.

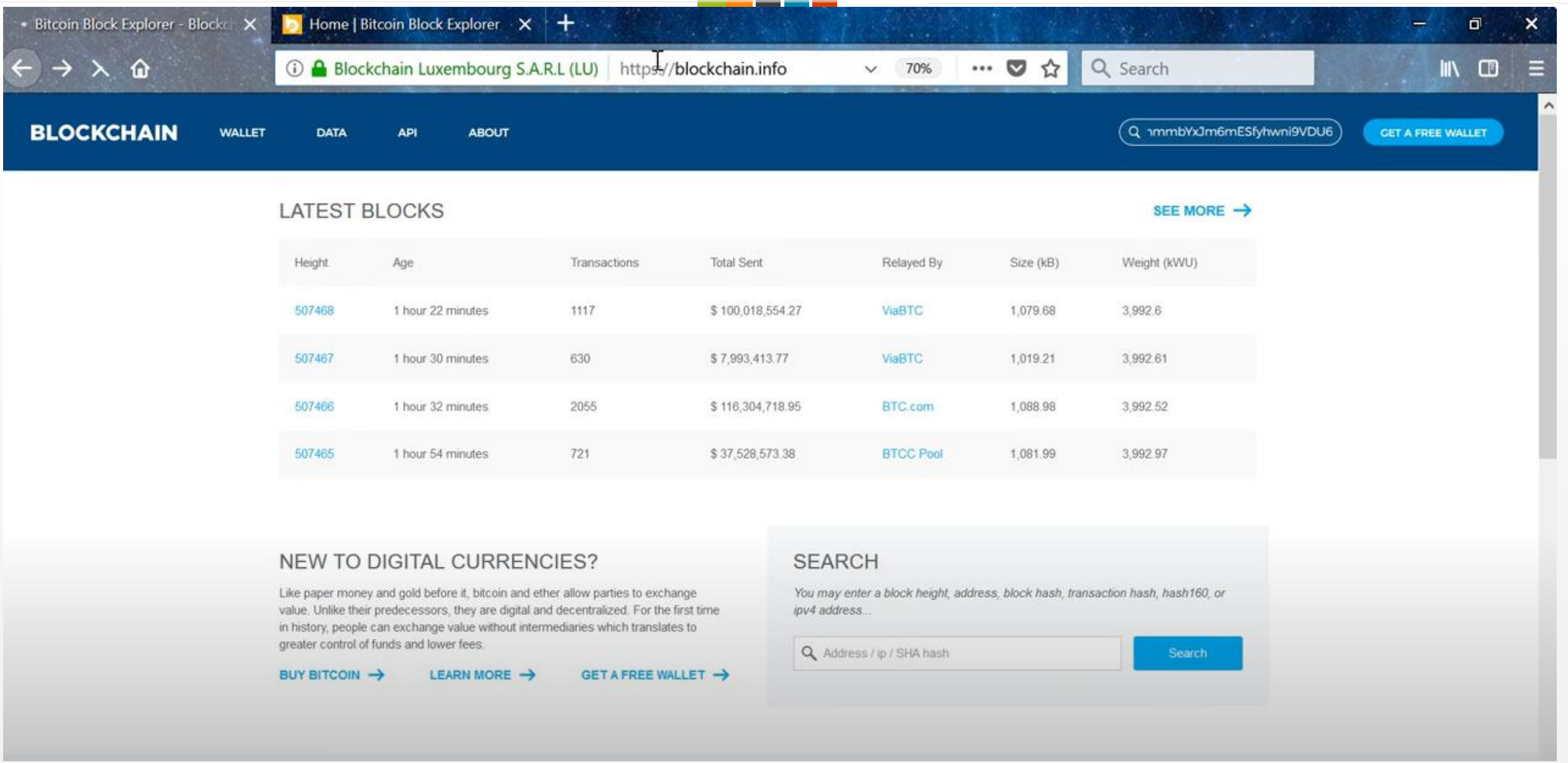
What does each block contains ?

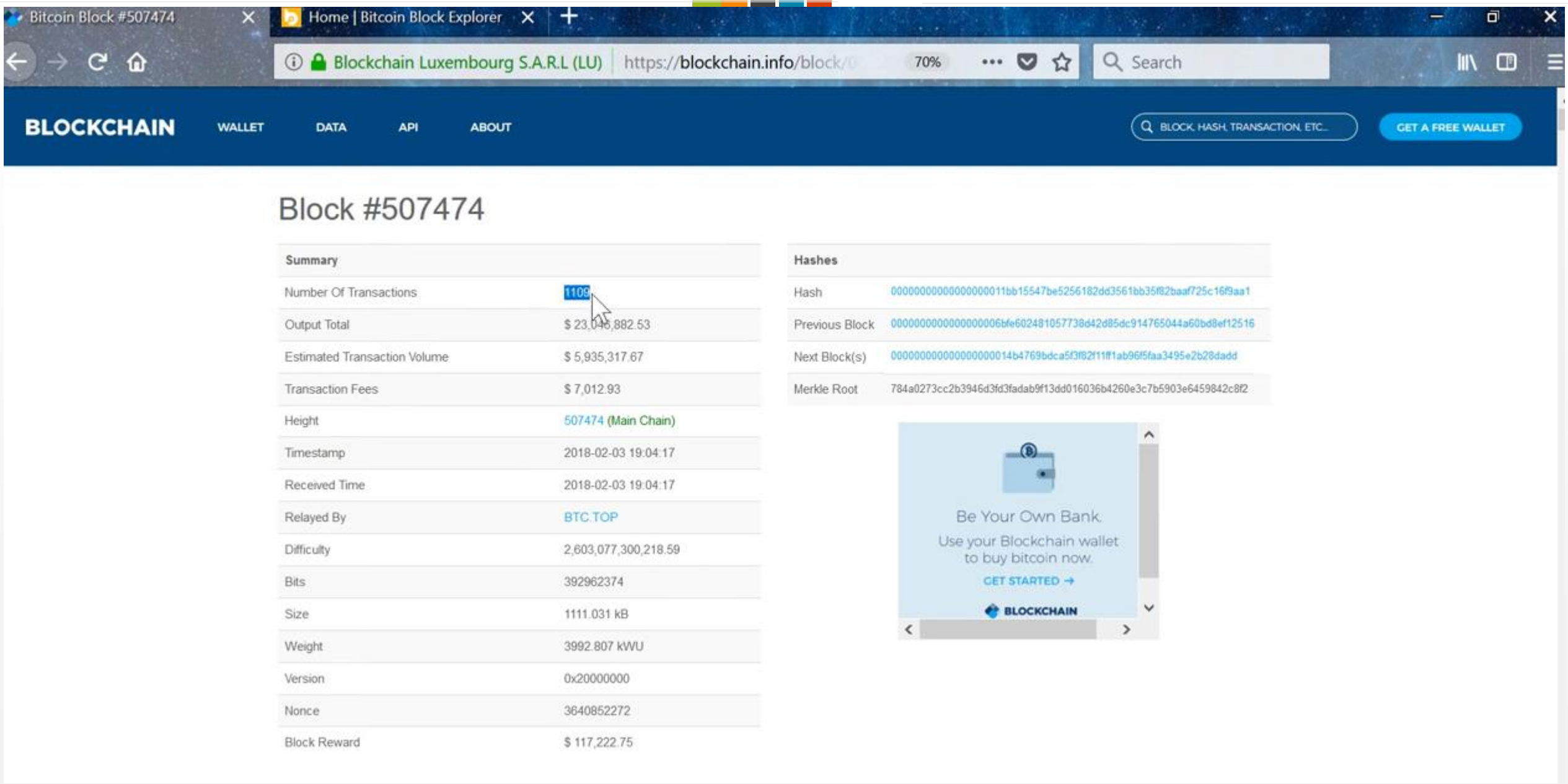


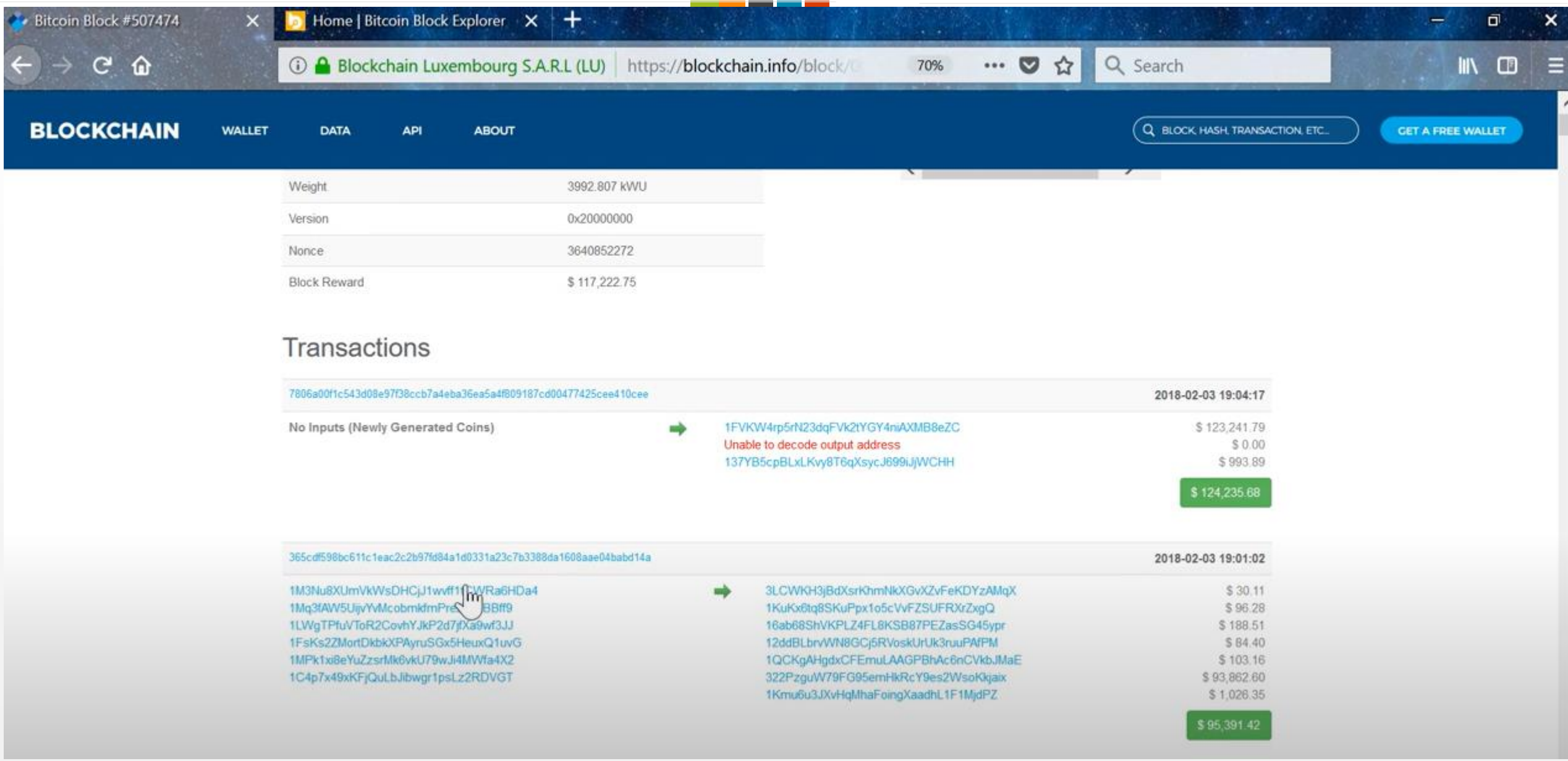
Contenu du Bloc (Block Content)

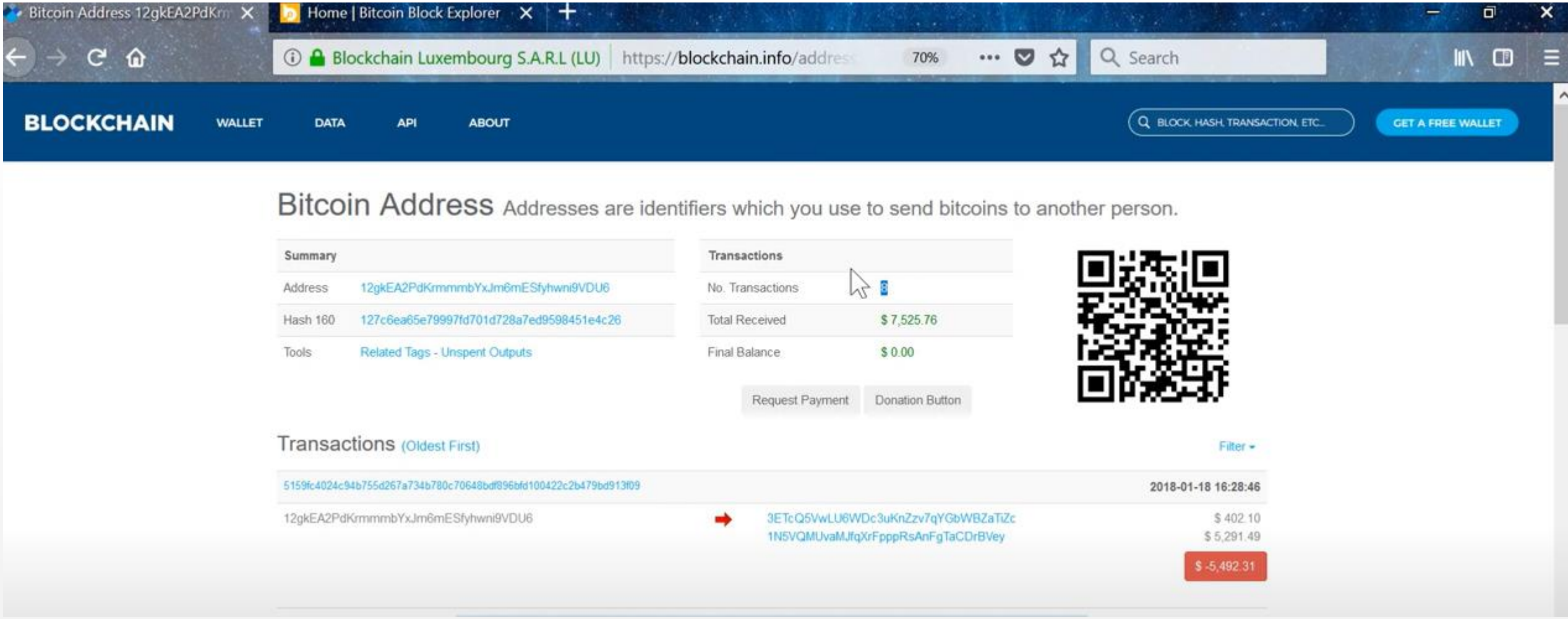
- **Transactions :** Le contenu principal d'un bloc comprend toutes les transactions qui ont été validées et incluses dans ce bloc. Chaque transaction contient des détails tels que l'expéditeur, le destinataire, le montant et les signatures numériques.
- **État :** Certaines blockchains, comme Ethereum, peuvent également inclure des informations sur l'état après l'exécution des transactions, par exemple, l'état des comptes et des smart contracts.




Bitcoin Block Explorer - Blockc
Home | Bitcoin Block Explorer
Blockchain Luxembourg S.A.R.L (LU)
https://blockchain.info
70%
Search
BLOCKCHAIN
WALLET
DATA
API
ABOUT
GET A FREE WALLET
LATEST BLOCKS
SEE MORE
Height
Age
Transactions
Total Sent
Relayed By
Size (kB)
Weight (kWU)
507468
1 hour 22 minutes
1117
$ 100,018,554.27
ViaBTC
1,079.68
3,992.6
507467
1 hour 30 minutes
630
$ 7,993,413.77
ViaBTC
1,019.21
3,992.61
507466
1 hour 32 minutes
2055
$ 116,304,718.95
BTC.com
1,088.98
3,992.52
507465
1 hour 54 minutes
721
$ 37,528,573.38
BTCC Pool
1,081.99
3,992.97
NEW TO DIGITAL CURRENCIES?
Like paper money and gold before it, bitcoin and ether allow parties to exchange value. Unlike their predecessors, they are digital and decentralized. For the first time in history, people can exchange value without intermediaries which translates to greater control of funds and lower fees.
BUY BITCOIN
LEARN MORE
GET A FREE WALLET
SEARCH
You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address...
Address / ip / SHA hash
Search


Bitcoin Block #507474
Home | Bitcoin Block Explorer
Blockchain Luxembourg S.A.R.L (LU)
https://blockchain.info/block/
70%
Search
BLOCKCHAIN
WALLET
DATA
API
ABOUT
BLOCK, HASH, TRANSACTION, ETC...
GET A FREE WALLET
Block #507474
Summary
Number Of Transactions 1109
Output Total $ 23,046,882.53
Estimated Transaction Volume $ 5,935,317.67
Transaction Fees $ 7,012.93
Height 507474 (Main Chain)
Timestamp 2018-02-03 19:04:17
Received Time 2018-02-03 19:04:17
Relayed By BTC.TOP
Difficulty 2,603,077,300,218.59
Bits 392962374
Size 1111.031 kB
Weight 3992.807 kWU
Version 0x20000000
Nonce 3640852272
Block Reward $ 117,222.75
Hashes
Hash 00000000000000000011bb15547be5256182dd3561bb35f82baaf725c16f9aa1
Previous Block 00000000000000000006bfe602481057738d42d85dc914765044a60bd8ef12516
Next Block(s) 00000000000000000014b4769bdca5f3f82f11ff1ab96f5faa3495e2b28dadd
Merkle Root 784a0273cc2b3946d3fd3fadab9f13dd016036b4260e3c7b5903e6459842c8f2
Be Your Own Bank.
Use your Blockchain wallet to buy bitcoin now.
GET STARTED →
BLOCKCHAIN


Bitcoin Block #507474
Home | Bitcoin Block Explorer
Blockchain Luxembourg S.A.R.L (LU)
https://blockchain.info/block/
70%
Search
BLOCKCHAIN
WALLET
DATA
API
ABOUT
BLOCK, HASH, TRANSACTION, ETC...
GET A FREE WALLET
Weight 3992.807 kWU
Version 0x20000000
Nonce 3640852272
Block Reward $ 117,222.75
Transactions
7806a00f1c543d08e97f38ccb7a4eba36ea5a4f809187cd00477425cee410cee
2018-02-03 19:04:17
No Inputs (Newly Generated Coins)
1FVKW4rp5rN23dqFVk2tYGY4niAXMB8eZC $ 123,241.79
Unable to decode output address $ 0.00
137YB5cpBLxLKvy8T6qXsycJ699iJjWCHH $ 993.89
$ 124,235.68
365cdf598bc611c1eac2c2b97fd84a1d0331a23c7b3388da1608aae04babd14a
2018-02-03 19:01:02
1M3Nu8XUmVkWsDHCjJ1wvff1
1Mq3tAW5UjvYvMcobmkfmPre
1LWgTPfuVToR2CovhYJkP2d7jfXa9wf3JJ
1FsKs2ZMortDkbkXPAyruSGx5HeuxQ1uvG
1MPk1xi8eYuZzsrMk6vkU79wJi4MWfa4X2
1C4p7x49xKFjQuLbJibwgr1psLz2RDVGT
3LCWKH3jBdXsrKhmNkXGvXZvFeKDYzAMqX $ 30.11
1KuKx6tq8SKuPpx1o5cVvFZSUFRXrZxgQ $ 96.28
16ab68ShVKPLZ4FL8KSB87PEZasSG45ypr $ 188.51
12ddBLbrvWN8GCj5RVoskUrUk3ruuPAfPM $ 84.40
1QCKgAHgdxCFEmuLAAGPBhAc6nCVkbJMaE $ 103.16
322PzguW79FG95emHkRcY9es2WsoKkjaix $ 93,862.60
1Kmu6u3JXvHqMhaFoingXaadhL1F1MjdPZ $ 1,026.35
$ 95,391.42


Bitcoin Address 12gkEA2PdKm
Home | Bitcoin Block Explorer
Blockchain Luxembourg S.A.R.L (LU)
https://blockchain.info/addres
70%
Search
BLOCKCHAIN
WALLET
DATA
API
ABOUT
BLOCK, HASH, TRANSACTION, ETC...
GET A FREE WALLET
Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.
Summary
Address 12gkEA2PdKrmmmbYxJm6mESfyhwni9VDU6
Hash 160 127c6ea65e79997fd701d728a7ed9598451e4c26
Tools Related Tags - Unspent Outputs
Transactions
No. Transactions 3
Total Received $ 7,525.76
Final Balance $ 0.00
Request Payment
Donation Button
Transactions (Oldest First)
Filter
5159fc4024c94b755d267a734b780c70648bdf896bfd100422c2b479bd913f09
2018-01-18 16:28:46
12gkEA2PdKrmmmbYxJm6mESfyhwni9VDU6
3ETcQ5VwLU6WDc3uKnZzv7qYGbWBZaTiZc
1N5VQMUvaMJfqXrFpppRsAnFgTaCDrBVey
$ 402.10
$ 5,291.49
$ -5,492.31

Questions ?!!