

Projet de cryptographie

Blockchain et modèle d'applications



Sheick Ali, SIMPORE
Majeur Réseaux et sécurité

Table des matières

Abstract	2
Introduction	3
I. L'histoire de la blockchain.....	3
II. Comment fonctionne la blockchain.....	4
III. La technologie blockchain	6
1. Blockchain et cryptographie.....	6
2. Démo du fonctionnement d'une blockchain.....	7
IV. Construction d'une blockchain	13
V. Champs d'application de la blockchain.....	14
1. Application de la blockchain dans l'agro-alimentaire.....	15
2. Application de la blockchain dans l'industrie de la finance	16
3. Application de la blockchain dans l'industrie de la santé	16
VI. Blockchain et sécurité	17
VII. Aspects négatifs de la blockchain.....	18
1. Activités illégales.....	18
2. Coût de la technologie	19
Conclusion.....	19
Bibliographie.....	20

Abstract

La blockchain est une infrastructure décentralisée de fichiers interconnectés par des programmes qui génèrent des hashes, ou chaînes de chiffres et de lettres représentant les informations contenues dans les fichiers. Cette architecture garantit la sécurité, la transparence et la fiabilité des transactions.

Les participants du réseau de la blockchain sont des ordinateurs ou des dispositifs qui vérifient continuellement les hashes générés par les programmes. Si un hash correspond exactement au hash généré par le participant, le fichier est accepté et intégré dans la chaîne. En cas d'inconformité, le fichier est rejeté et ne peut pas être ajouté à la blockchain.

Cette approche de vérification répétitive et distribuée rend la blockchain résistante aux fraudes et garantit l'intégrité des données. Les hashes servent également comme références uniques entre les blocs, créant ainsi une chaîne linéaire immuable de transactions.

La blockchain trouve des applications variées, notamment dans le domaine financier avec les cryptomonnaies, mais aussi dans la gestion des documents, l'identité numérique et de nombreux autres secteurs où une transaction sécurisée est nécessaire.

Blockchain

Introduction

La blockchain est une technologie de stockage et de transmission de l'information, réalisée de manière décentralisée. Dans ce projet, nous allons expliquer comment il fonctionne et montrer en quoi la blockchain joue un rôle important dans l'industrie de nos jours.

I. L'histoire de la blockchain

Tout commence en 1982, lorsque David Chaum, pionnier de la cryptographie, imagine un protocole cryptographique préfigurant la blockchain dans sa thèse de doctorat.

Quelques années plus tard, en 1991, la vision de Chaum prend forme avec les travaux de Stuart Haber et Scott Stornetta. Ces chercheurs, conscients des enjeux liés à la sécurité des informations numériques, mettent au point une méthode permettant de sceller des documents horodatés au sein d'une chaîne de blocs, sécurisée par cryptographie.

Ensuite, en 1998, Nick Szabo, un autre pionnier visionnaire, conçoit le **bit gold**, une forme de monnaie numérique décentralisée en s'inspirant des travaux de Stuart Haber et Scott Stornetta.[3] Bien que jamais implémenté, ce projet visionnaire anticipe déjà certains des principes fondamentaux qui animeront plus tard le Bitcoin, notamment l'idée de transactions sans intermédiaire. Szabo introduit alors l'idée de la rareté numérique, essentielle dans l'architecture des monnaies virtuelles actuelles.

L'année 2008 constitue un tournant décisif. C'est à ce moment que Satoshi Nakamoto, un personnage mystérieux (ou un groupe de personnes), bouleverse définitivement le paysage technologique en publiant le célèbre livre blanc du Bitcoin. Ce document décrit un système de monnaie électronique fonctionnant sur un réseau pair-à-pair, sans autorité centrale. Avec la création du Bitcoin, Nakamoto ne se contente pas de proposer une nouvelle monnaie, mais introduit aussi le terme **blockchain** pour désigner l'infrastructure technologique sous-jacente. Cette chaîne de blocs, à la fois publique, sécurisée et transparente, révolutionne la manière dont les transactions sont enregistrées, ouvrant la voie à un système financier décentralisé.

Mais l'histoire ne s'arrête pas là. En 2013, un jeune programmeur, Vitalik Buterin, s'empare de cette technologie naissante et voit plus loin que les simples transactions financières. Il propose alors **Ethereum**, une blockchain qui ne se contente plus d'enregistrer des échanges de valeur, mais permet également d'exécuter des contrats intelligents. Ces programmes autonomes, capables de s'exécuter sans intervention humaine, offrent une flexibilité inédite et marquent l'avènement de la **blockchain 2.0**. Le lancement d'Ethereum en 2015 ouvre une ère d'innovation sans précédent, permettant à des milliers de développeurs de créer des **applications décentralisées (dApps)** et des projets qui bouleversent des secteurs aussi variés que la finance, l'assurance, ou encore la gestion des identités.

Pendant ce temps, les grandes entreprises et les institutions prennent conscience du potentiel de cette technologie. Toujours en 2015, la fondation Linux lance le projet **Hyperledger**, une initiative collaborative visant à développer des blockchains open-source destinées aux entreprises. Contrairement aux blockchains publiques comme Bitcoin ou Ethereum, Hyperledger propose des solutions privées ou permissionnées, spécialement

adaptées aux besoins des industries. Avec cela, la blockchain étend ses applications au-delà du simple monde des cryptomonnaies, en s'immisçant dans des domaines aussi divers que la gestion des chaînes d'approvisionnement, l'automatisation des processus industriels, et même la traçabilité des produits alimentaires.

Ainsi, en quelques décennies seulement, la blockchain a évolué d'une idée théorique à une technologie révolutionnaire, transformant des secteurs entiers de l'économie mondiale. Ce parcours, jalonné d'innovations brillantes, témoigne de la manière dont la blockchain a réussi à redéfinir notre rapport à la sécurité, à la transparence, et à la confiance dans le monde numérique. Aujourd'hui, elle continue de stimuler l'imagination des entrepreneurs et des développeurs du monde entier, posant les bases d'une nouvelle ère de technologies décentralisées.

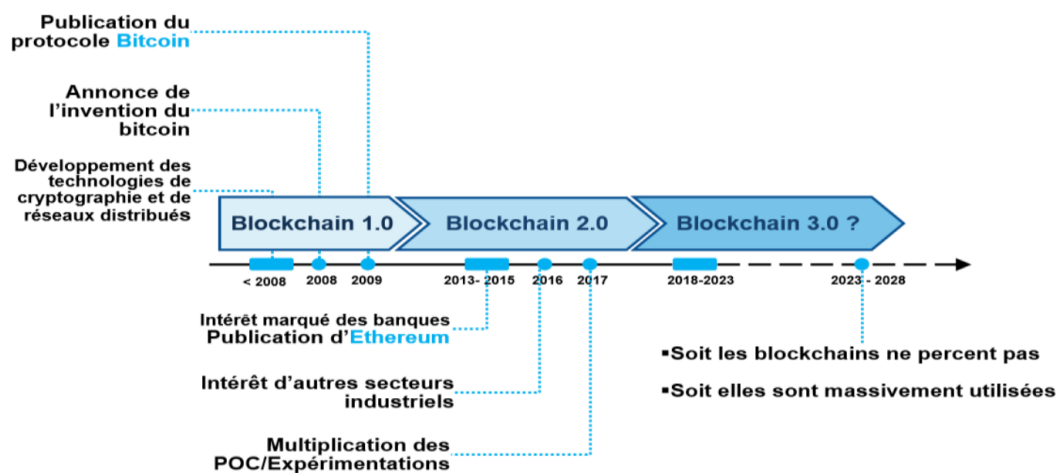


Fig 1 : historique de la blockchain [2]

II. Comment fonctionne la blockchain

Traditionnellement, lorsque vous utilisez une application, qu'il s'agisse d'un site web ou d'un programme qui se connecte à un serveur, vous interagissez avec une entité centralisée. La blockchain élimine l'intermédiaire de cette tierce entité. L'application la plus connue et discutée de la technologie blockchain est le Bitcoin, une monnaie numérique qui peut être utilisée pour échanger des produits et des services, tout comme le dollar américain, l'euro, le yuan chinois et d'autres devises nationales. Nous parlerons plus du bitcoin qui est une technologie blockchain afin de comprendre comment la blockchain fonctionne.

Un bitcoin est une unité unique de la monnaie numérique Bitcoin (BTC). Tout comme un dollar, un bitcoin n'a pas de valeur intrinsèque ; il n'a de valeur que parce que nous acceptons d'échanger des biens et des services pour obtenir davantage de cette monnaie, et nous croyons que les autres feront de même.

Pour suivre la quantité de bitcoins que chacun possède, la blockchain utilise un **registre**, un fichier numérique qui enregistre toutes les transactions en bitcoins.

LEDGER	
Account owner	Value
Mary	4
John	56
Sandra	83
Lisa	16
David	187
Brian	23
...	...

Fig 2 : Ledger (registre)

Le fichier du registre n'est pas stocké sur le serveur d'une entité centrale, comme une banque, ni dans un seul centre de données. Il est distribué à travers le monde via un réseau d'ordinateurs privés qui à la fois stockent les données et exécutent des calculs. Chacun de ces ordinateurs représente un **nœud** du réseau blockchain et possède une copie du fichier du **registre**.

Si David veut envoyer des bitcoins à Sandra, il diffuse un message au réseau indiquant que le montant de bitcoins dans son compte doit diminuer de 5 BTC, et que le montant dans le compte de Sandra doit augmenter de la même quantité. Chaque nœud du réseau recevra ce message et appliquera la transaction demandée à sa copie du registre, mettant ainsi à jour les comptes.

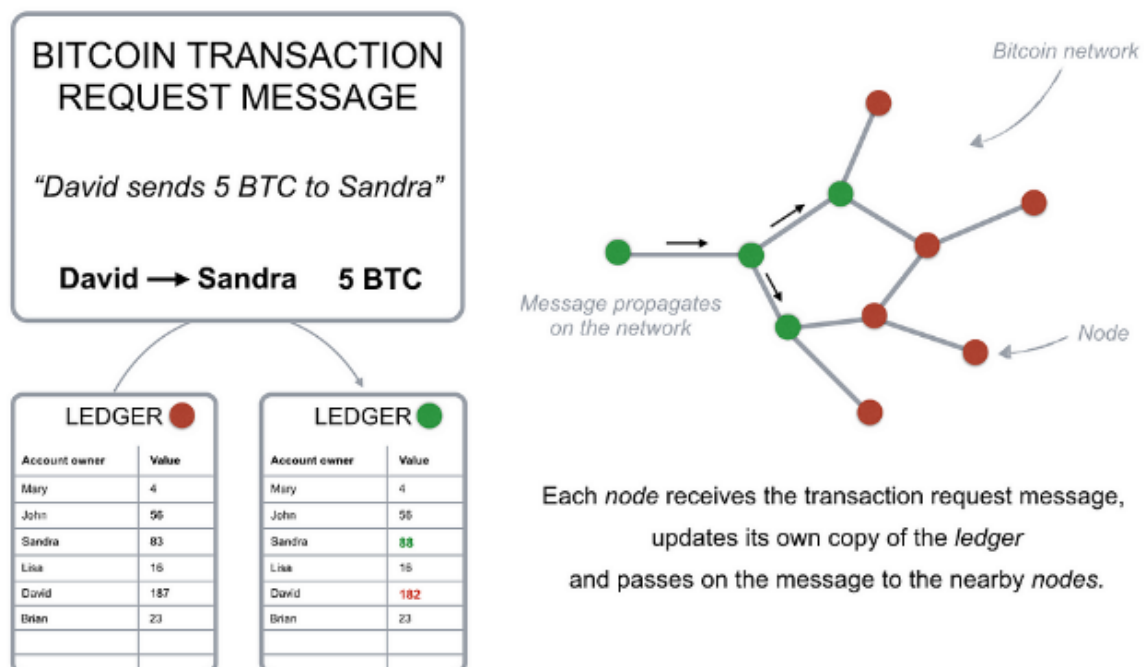


Fig 3 : exemple de transactions [3]

Le fait que le registre soit maintenu par un groupe d'ordinateurs connectés plutôt que par une entité centralisée comme une banque a plusieurs implications.

Dans notre système bancaire, nous ne connaissons que nos propres transactions et soldes de compte ; sur la blockchain, chacun peut voir les transactions de tous les autres. Alors que l'on peut généralement faire confiance à sa banque, le réseau Bitcoin est décentralisé et s'il y a un problème, il n'y a pas de service client à contacter ni personne à poursuivre en justice.

Le système blockchain est conçu de telle manière qu'aucune confiance n'est nécessaire ; la sécurité et la fiabilité sont obtenues grâce à des fonctions mathématiques spéciales et du code informatique.

III. La technologie blockchain

1. Blockchain et cryptographie

La blockchain utilise la cryptographie et la collaboration pour créer une confiance et, par conséquent, élimine le besoin d'une institution centralisée agissant comme intermédiaire. Les informations sur la blockchain sont stockées dans le registre à l'aide de la cryptographie. Pour effectuer des transactions sur la blockchain, vous avez besoin d'un portefeuille, un programme qui vous permet de stocker et d'échanger vos bitcoins. Comme vous seul devez pouvoir dépenser vos bitcoins, chaque portefeuille est protégé par une méthode cryptographique spéciale qui utilise une paire unique de clés distinctes mais connectées : une clé privée et une clé publique.

La blockchain utilise certains éléments de base de la cryptographie, comme suit [4]:

- **Cryptographie à clé publique** : Utilisée pour les signatures numériques et le chiffrement. Elle sert à prouver qu'une transaction a été créée par la bonne personne. Dans la blockchain, la clé privée est conservée dans un portefeuille numérique, soit un portefeuille matériel (un dispositif physique pour stocker la clé privée), soit un portefeuille logiciel (par exemple, une application de portefeuille pour ordinateur, une application de portefeuille mobile ou un portefeuille web).
- **Le ZeroKnowledge proof** : Démontre la connaissance d'un secret sans le révéler. Lorsqu'un utilisateur demande à envoyer de l'argent à un autre utilisateur, la blockchain veut naturellement s'assurer, avant de valider cette transaction, que l'utilisateur qui envoie l'argent en a suffisamment. Cependant, la blockchain n'a pas réellement besoin de savoir ou de se soucier de qui dépense l'argent, ni de combien d'argent il/elle possède au total. Dans ce cas, la blockchain n'a aucune connaissance de la personne à qui l'utilisateur envoie l'argent ni de la somme totale que l'utilisateur possède.
- **Fonctions de hachage** : Fonctions mathématiques pseudo-aléatoires à sens unique.

Si un message est chiffré avec une clé publique spécifique, seul le propriétaire de la clé privée associée peut le déchiffrer et le lire. L'inverse est également vrai : si vous chiffrez un message avec votre clé privée, seule la clé publique associée peut le déchiffrer. Lorsque David veut envoyer des bitcoins, il doit diffuser un message chiffré avec la clé privée de son portefeuille. Comme David est le seul à connaître la clé privée nécessaire pour débloquent son portefeuille, il est le seul à pouvoir dépenser ses bitcoins. Chaque nœud du réseau peut vérifier que la demande de transaction vient bien de David en déchiffrant le message avec la clé publique de son portefeuille.

Lorsque vous chiffrez une demande de transaction avec la clé privée de votre portefeuille, vous générez une signature numérique qui est utilisée par les ordinateurs de la blockchain pour vérifier la source et l'authenticité de la transaction. La signature numérique est une chaîne de texte résultant de votre demande de transaction et de votre clé privée ; elle ne peut donc pas être utilisée pour d'autres transactions. Si vous changez un seul caractère dans le message de demande de transaction, la signature numérique changera, donc aucun attaquant potentiel ne peut modifier vos demandes de transaction ou altérer le montant de bitcoin que vous envoyez.

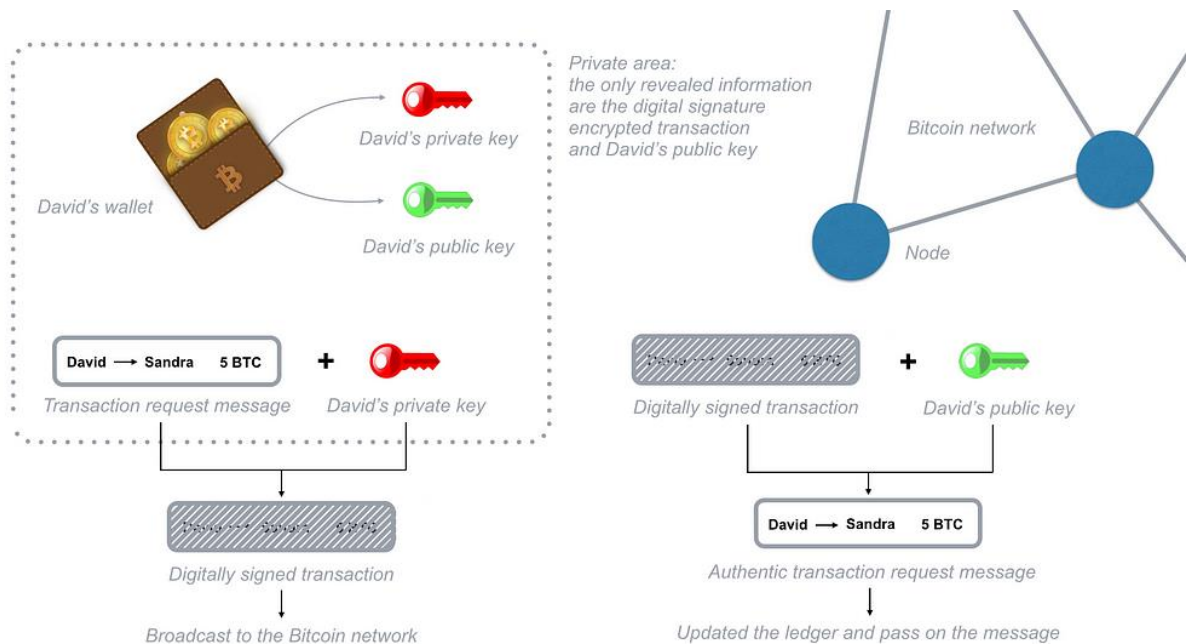


Fig 4 : Illustration d'une transaction [3]

2. D mo du fonctionnement d'une blockchain

La blockchain est une technologie innovante qui utilise une base de donn es distribu e et s curis e pour stocker des informations de mani re d centralis e. Anders Brownworth, un expert en la mati re, nous pr sente une approche visuelle pour comprendre comment fonctionne cette technologie fascinante. Nous nous inspirerons de son travail pour cette d mo [8].

La blockchain repose sur trois concepts fondamentaux :

1. Le hash

2. Le bloc
3. La chaîne de blocs

Ces éléments travaillent ensemble pour former la blockchain.

- Le hash :

L'algorithme de hashage cryptographique spécifique utilisé dans de nombreuses implémentations de blockchain est l'algorithme de Hashage Sécurisé (SHA) avec une taille de sortie de 256 bits (SHA-256). De nombreux ordinateurs supportent cet algorithme matériellement, ce qui le rend rapide à calculer. SHA-256 produit une sortie de 32 octets (1 octet = 8 bits, 32 octets = 256 bits), généralement affichée sous forme de chaîne hexadécimale de 64 caractères. Le hash est comme une empreinte numérique unique pour des données numériques. Des données identiques produisent toujours le même hash, quelle que soit la longueur du texte. Le hash conserve toujours la même taille, ce qui en fait un outil précieux pour l'identification et la vérification des données.

SHA256 Hash

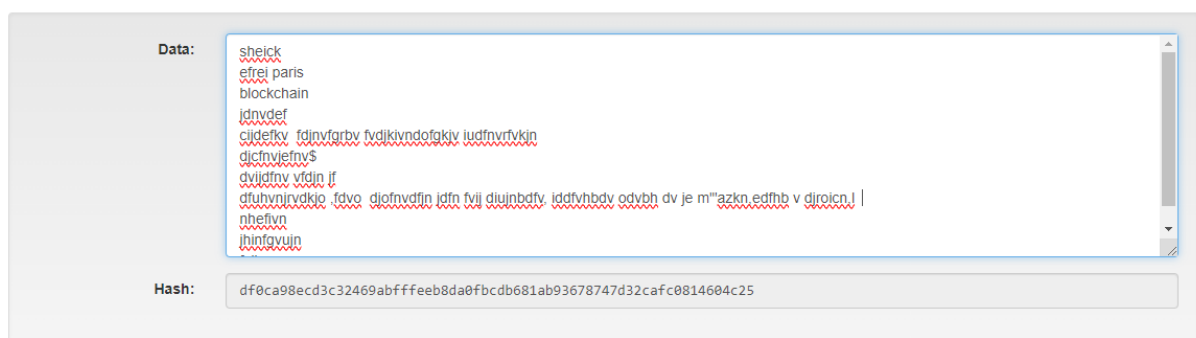


Data: sheick

Hash: c4a3d4f61628ca7c084f1503589a1c3b1370baf67f68a1fd33e9a1cfaf03842

Le hash garde la même taille quel que soit la longueur du texte.

SHA256 Hash



Data: sheick
effrei paris
blockchain
idnvdof
cjdfeikv fdjnvforbv fvdikivndofakiv iudfnvrvtkin
dicfnviefnys
dviidtnv vfdin if
dfuhvnrjvdtkio fdvo djoifnvdfjn idfn fvij diuinbdfv iddfvhbdv odvbn dv je m"azkn edfthb v diroicn. |
nhfefvn
ihinfvujn

Hash: df0ca98ecd3c32469abfffeeb8da0fbcd681ab93678747d32cafc0814604c25

- Le block :

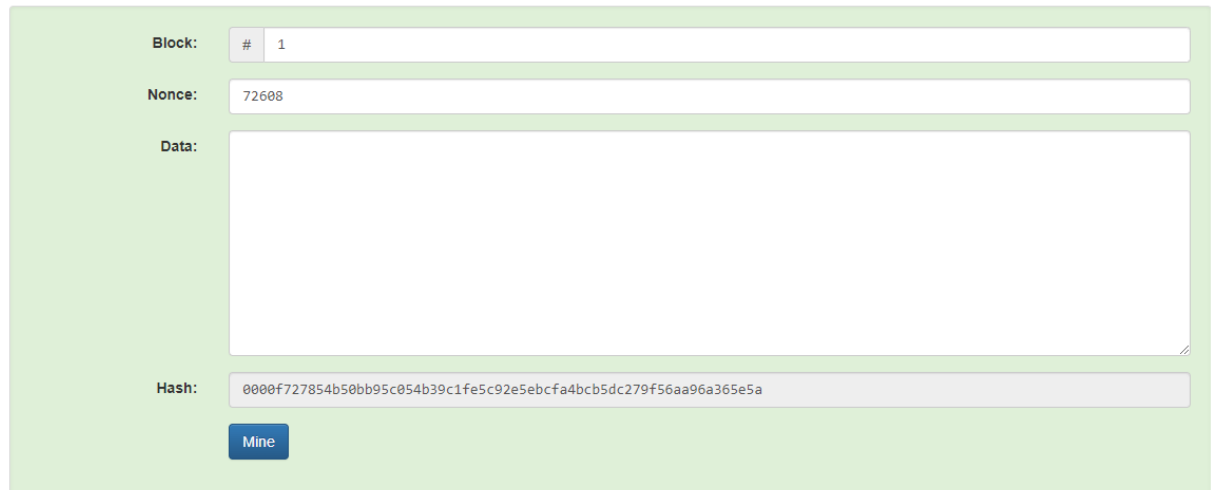
Un bloc est l'unité de base de la blockchain. Il contient :

- Un numéro unique identifiant le bloc
- Un nonce (nombre utilisé une seule fois)
- Les données du bloc
- Le hash du bloc

Le hash prend en compte toutes ces informations. Si seulement une donnée change, le hash devient différent. Pour qu'un bloc soit valide, son hash doit commencer par 4 zéro. Dans ce cas, le bloc est signé et considéré comme valide.

Block valide

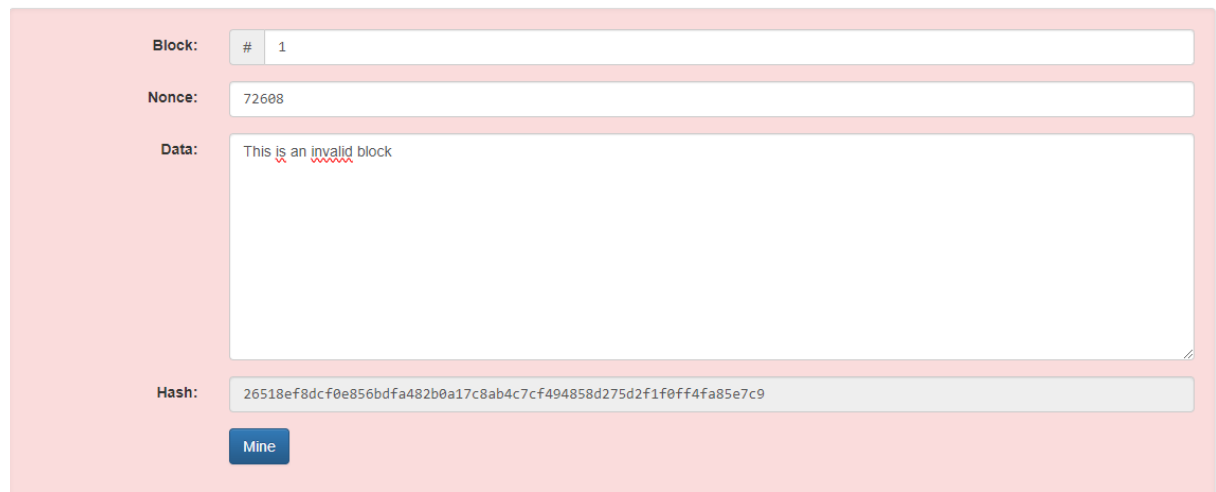
Block



A screenshot of a web interface for mining a valid block. The interface has a light green background. It contains four input fields: 'Block:' with a dropdown set to '# 1', 'Nonce:' with the value '72608', 'Data:' which is an empty text area, and 'Hash:' which displays '0000f727854b50bb95c054b39c1fe5c92e5ebcfa4bcb5dc279f56aa96a365e5a'. Below the hash field is a blue button labeled 'Mine'.

Block invalide :

Block



A screenshot of a web interface for mining an invalid block. The interface has a light red background. It contains four input fields: 'Block:' with a dropdown set to '# 1', 'Nonce:' with the value '72608', 'Data:' which contains the text 'This is an invalid block' with 'invalid' underlined in red, and 'Hash:' which displays '26518ef8dcf0e856bdfa482b0a17c8ab4c7cf494858d275d2f1f0ff4fa85e7c9'. Below the hash field is a blue button labeled 'Mine'.

Ici, les quatre premières valeurs du hash sont 2651. Le block n'est donc pas signé et dans ce cas il est invalide.

Pour rendre un bloc valide, le mineur, le nœud ou l'ordinateur doit trouver un nonce approprié qui permet d'obtenir un hash avec les quatre premières valeurs à zéro. Pour ce faire, voici comment il procède :

1. Initialisation : Le nonce commence à zéro.
2. Calcul du Hash : Le programme de minage calcule le hash du bloc en utilisant le nonce actuel.

3. Vérification : Si le hash commence par 4 zéro, le bloc est considéré comme validé.
4. Incrémentation : Si le hash n'est pas valide, le nonce est incrémenté de 1.
5. Répétition : Les étapes 2 à 4 sont répétées jusqu'à trouver un nonce valide.

Ce processus est appelé **minage** et consiste à résoudre un problème mathématique complexe. Le premier mineur à réussir obtient la récompense et sa marque est ajoutée à la blockchain.

Block

The screenshot shows a mining interface with the following fields:

- Block:** # 1
- Nonce:** 61893
- Data:** This is an invalid block
- Hash:** 000039c507d3cf9095816e3f7a88d95aeae860cab83c68da619961b00b24de1e

A red circle highlights the **Mine** button, which is located below the hash field.

- **La blockchain** : la blockchain est une chaîne de block.

Blockchain

The screenshot shows a blockchain interface with three blocks, each with its own mining controls:

- Block 1:** # 1, Nonce: 11316, Prev: 00, Hash: 000015783b76425d382017091a36d206d0000e2cb3567748f46a33fe9297cf
- Block 2:** # 2, Nonce: 35230, Prev: 000015783b76425d382017091a36d206d0000e2cb3567748f46a33fe9297cf, Hash: 000012fa0b016eb9878f8d98a7864e697ae83ed54f5146bd84452cdf0843c19
- Block 3:** # 3, Nonce: 12937, Prev: 000012fa0b016eb9878f8d98a7864e697ae83ed54f5146bd84452cdf0843c19, Hash: 000009015ce2a08b61216ba5a0778545bf4dd07ce

Each block has a **Mine** button below its hash field.

Dans chaque block on retrouve le hash du block précédent qui pointe alors la transaction précédente formant ainsi une chaîne en fonction du nombre de block.

Si une information est changée dans un block, la blockchain devient invalide du fait que chaque block garde le hash du block précédent qui d'ailleurs avait déjà été validé.

Tentative de modification d'un bloc : Résultante : la chaine de block devient invalide

Blockchain

Block	Block #	Nonce	Data	Prev	Hash
1	1	11316		00	000015783b764259d382017d91a36d286d800e2c3b3567748f46a33fe9297cf
2	2	35230	changed the block	000015783b764259d382017d91a36d286d800e2c3b3567748f46a33fe9297cf	11e60b39831ad00b41a570fa257e93e2e4d1fe0dd9bb799ce4659fecbd83cd
3	3	12937		11e60b39831ad00b41a570fa257e93e2e4d1fe0dd9bb799ce4659fecbd83cd	ef60b49e049cc4780c07ef2353c9c451cc418d78f51849

- Blockchain distribuée :

Dans une blockchain distribuée, chaque pair conserve une copie complète de la blockchain. Lorsqu'un bloc est modifié, on peut le détecter en comparant les copies de la blockchain détenues par les différents pairs. Ce système repose sur un principe de consensus : si la majorité des pairs possèdent la même version de la blockchain tandis qu'une minorité présente une version différente, il est possible d'identifier où se situe l'anomalie.

Distributed Blockchain

Peer	Block	Block #	Nonce	Data	Prev	Hash
Peer A	1	1	11316		00	000015783b764259d382017d91a36d286d800e2c3b3567748f46a33fe9297cf
	2	2	35230	changed the block	000015783b764259d382017d91a36d286d800e2c3b3567748f46a33fe9297cf	11e60b39831ad00b41a570fa257e93e2e4d1fe0dd9bb799ce4659fecbd83cd
	3	3	12937		11e60b39831ad00b41a570fa257e93e2e4d1fe0dd9bb799ce4659fecbd83cd	ef60b49e049cc4780c07ef2353c9c451cc418d78f51849
Peer B	1	1	11316		00	000015783b764259d382017d91a36d286d800e2c3b3567748f46a33fe9297cf
	2	2	35230		000015783b764259d382017d91a36d286d800e2c3b3567748f46a33fe9297cf	000015783b764259d382017d91a36d286d800e2c3b3567748f46a33fe9297cf
	3	3	12937		000015783b764259d382017d91a36d286d800e2c3b3567748f46a33fe9297cf	000015783b764259d382017d91a36d286d800e2c3b3567748f46a33fe9297cf

C'est pourquoi, par exemple, dans le réseau Bitcoin, compromettre la blockchain nécessiterait de corrompre plus de 51 % des blocs. Une attaque de ce type, appelée attaque des 51 %, est extrêmement difficile à réaliser en raison de la puissance de calcul nécessaire, rendant ainsi la falsification de la blockchain pratiquement impossible.

- [illegible]

- **Les signatures :**

La blockchain utilise un système de signature à clé publique/privée et le concept de zero-knowledge [6] pour valider les transactions sans connaître le solde des comptes. L'utilisateur signe sa transaction avec sa clé privée, et le réseau vérifie cette signature avec la clé publique correspondante. Cette approche permet de prouver la validité d'une transaction sans révéler le montant total disponible sur le compte, assurant ainsi la confidentialité des utilisateurs tout en maintenant l'intégrité du système. Le bloc peut donc valider les transactions basées uniquement sur ces preuves cryptographiques, sans avoir

besoin d'accéder à l'historique complet ou au solde actuel de l'utilisateur.

Peer A

Block: # 1
Nonce: 16651
Coinbase: \$ 100.00 → Anders
Tx:
Prev: 00
Hash: 0000438d762508a6f36540d1929975a6d3f7cf9047e56cc587cadd0b0d781
Mine

Block: # 2
Nonce: 215410
Coinbase: \$ 100.00 → Anders
Tx:
\$ 10.00 From Anders → Sophia
\$ 20.00 From Anders → Lucas
\$ 15.00 From Anders → Emily
\$ 15.00 From Anders → Madison
Prev: 0000438d762508a6f36540d1929975a6d3f7cf9047e56cc587cadd0b0d781
Hash: 00
Mine

Block: # 3
Nonce: 140
Coinbase: \$ 100.00 → And
Tx:
\$ 10.00 From Emily
\$ 1.00 From Madison
\$ 20.00 From Lucas
Prev: 00
Hash: 00
Mine

En résumé : La blockchain

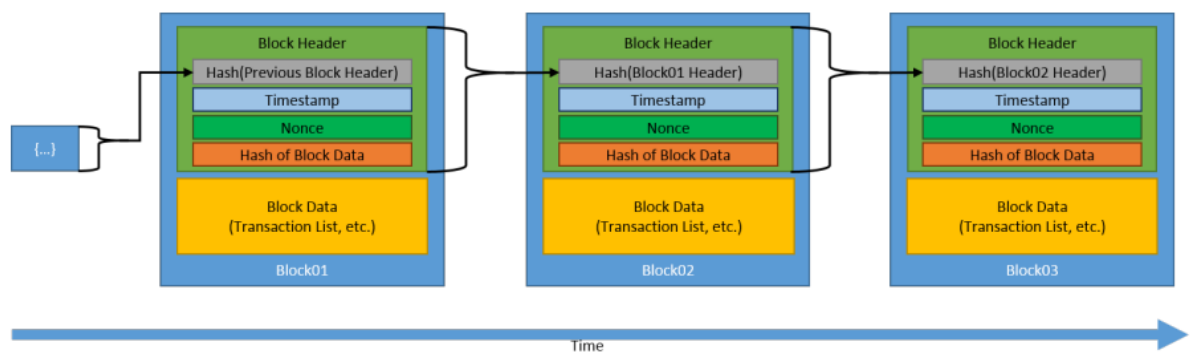


Fig 5 : La blockchain

IV. Construction d'une blockchain

Dans cette partie nous construirons un système de blockchain en utilisant python et flask.

```
C: > Developpement > blockchain > block.py > Blockchain

1  """
2  |   Blockchain Construction
3  |
4  |   """
5
6
7  import hashlib
8  import json
9  from time import time
10 from uuid import uuid4
11 from textwrap import dedent
12 from flask import Flask, jsonify
13 from urllib.parse import urlparse
14
15
16 class Blockchain(object) :
17
18     def __init__(self) :
19         self.chain = []
20         self.current_transactions = []
21         self.new_block(previous_hash=1, proof=100)
22         self.nodes = set()
23
24
25
26     def register_node(self, address) :
27
28         # Adding a new node to the list
29
30         parsed_url = urlparse(address)
31         self.nodes.add(parsed_url.netloc)
32
33
```

Le projet est disponible sur mon github : <https://github.com/sheicky/Blockchain>



V. Champs d'application de la blockchain

La blockchain a plusieurs champs d'applications et peut être adapté dans tous les domaines de l'informatique.

Ce tableau résumé quelques champs d'application de la blockchain en fonction du domaine.

Domaine d'application	Utilités
-----------------------	----------

Finances	<ul style="list-style-type: none"> ❖ Cryptomonnaies : Bitcoin, Ethereum, et des milliers d'autres ❖ Marchés boursiers : négociation plus rapide et transparente ❖ Services financiers décentralisés (DeFi) : prêts, épargne, assurance sans intermédiaires ❖ Financement participatif : plateformes de crowdfunding plus transparentes ❖ Paiements transfrontaliers : transferts d'argent plus rapide et moins coûteux
IoT	<ul style="list-style-type: none"> ❖ Sécurité et confidentialité : protection des données collectées par les appareils connectés ❖ Commerce électronique : traçabilité des produits et lutte contre la contrefaçon ❖ Villes intelligentes : gestion optimisée des infrastructures urbaines
Energie	<ul style="list-style-type: none"> ❖ Marché de l'énergie : échanges peer-to-peer d'énergie renouvelable ❖ Suivi des émissions de carbone
Gouvernance et service public	<ul style="list-style-type: none"> ❖ Vote électronique : systèmes de vote sécurisés et transparents ❖ Administration publique : gestion des registres d'état civil, cadastre ❖ Aide au développement : traçabilité des fonds et lutte contre la corruption
Identité numérique	<ul style="list-style-type: none"> ❖ Gestion d'identité décentralisée : contrôle de ses données personnelles ❖ Protection de la vie privée : partage sélectif et sécurisé d'informations

Nous allons plus nous intéresser à l'industrie agro-alimentaire, à la finance et au secteur de la santé.

1. Application de la blockchain dans l'agro-alimentaire

Dans l'industrie alimentaire, la blockchain peut être utilisée avec les TIC pour assurer la sécurité alimentaire. Par exemple, elle peut être utilisée avec la RFID (identification par radiofréquence) pour construire un système de traçabilité de la chaîne d'approvisionnement agroalimentaire. Un tel système peut fournir des informations fiables grâce à des processus sécurisés de collecte et de communication des données dans la chaîne d'approvisionnement agroalimentaire pour assurer la sécurité des aliments à tous les stades de la production, de la fabrication, de l'entreposage, de la livraison et de la vente. Walmart travaille avec IBM et l'Université Tsinghua de Pékin pour créer des applications de chaîne d'approvisionnement basées sur la blockchain en Chine, avec un accent particulier sur le marché du porc [7]. Ils ont rapporté un résultat encourageant en réduisant le temps nécessaire pour tracer les aliments de plusieurs jours à quelques minutes.

En général, l'utilisation de la blockchain dans l'industrie alimentaire présente de nombreux avantages, notamment l'amélioration de la transparence des systèmes alimentaires,

l'optimisation des flux alimentaires, la réduction du gaspillage alimentaire, l'aide à la dissuasion de la fraude alimentaire et l'offre de nouveaux outils pour accroître la confiance dans les aliments.

2. Application de la blockchain dans l'industrie de la finance

Le succès retentissant de la blockchain dans l'univers des cryptomonnaies a naturellement conduit le secteur financier traditionnel à explorer son potentiel dans d'autres domaines. Jusqu'à présent, l'industrie financière reposait largement sur des intermédiaires de confiance pour assurer le bon déroulement des transactions. Ces tiers assumaient généralement quatre fonctions essentielles :

- Authentifier les transactions
- Prévenir les doublons
- Enregistrer et valider les opérations
- Servir d'intermédiaires entre les parties

La technologie blockchain se révèle particulièrement efficace pour remplir deux de ces rôles cruciaux : la prévention des doublons et la tenue d'un registre fiable des transactions.

L'un des atouts majeurs de la blockchain réside dans sa capacité à empêcher les transactions frauduleuses. Contrairement aux systèmes traditionnels où il est parfois possible de dépenser plus que son solde (comme avec les chèques sans provision), la blockchain impose une vérification collective de chaque transaction avant son exécution. Cette approche élimine pratiquement tout risque de double dépense ou de dépassement de solde.

La blockchain fonctionne également comme un grand livre comptable numérique, immuable et accessible à tous les participants du réseau. Une fois une transaction enregistrée, elle ne peut être modifiée ou effacée, garantissant ainsi l'intégrité et la traçabilité de toutes les opérations. Ce mécanisme de validation collective renforce la confiance entre les parties sans nécessiter l'intervention d'un tiers.

Ces caractéristiques ouvrent la voie à de nombreuses innovations dans le secteur financier, notamment :

- Des systèmes de paiement internationaux plus rapides et moins coûteux
- Des contrats intelligents automatisant certaines opérations financières
- Une gestion plus transparente et efficace des chaînes d'approvisionnement
- Des processus de vérification d'identité (KYC) simplifiés et sécurisés

3. Application de la blockchain dans l'industrie de la santé

La blockchain offre des perspectives prometteuses pour améliorer le partage et la gestion des données de santé. L'un des éléments les plus sensibles et critiques dans le domaine de la santé est constitué par les données des patients. Le dossier médical d'un patient est généralement dispersé entre plusieurs systèmes détenus et gérés par un ou plusieurs prestataires de soins. [6]

L'évolution numérique a permis de digitaliser les informations des patients dans ce qu'on appelle communément le dossier médical électronique (DME). Le partage des DME entre plusieurs prestataires de soins et organisations liées à la santé se heurte à de nombreux obstacles, notamment en matière de sécurité et de confidentialité. La blockchain peut être

utilisée pour permettre un partage sécurisé des DME et d'autres informations de santé entre plusieurs prestataires.

Une startup nommée Gem a développé un réseau basé sur la blockchain pour créer des applications de santé et une infrastructure universelle de données de santé. De plus, une autre startup, Tierion, a mis au point une plateforme de stockage des données de santé. Cette plateforme prend également en charge les processus de vérification et d'audit des dossiers et des procédures de santé. Dans un autre travail de recherche, Health Data Gateway (HDG) est proposé comme une architecture d'application basée sur la blockchain, permettant aux patients de contrôler et de partager en toute sécurité leurs données de santé tout en préservant leur vie privée. Cette architecture garantit que, bien que les patients possèdent et contrôlent l'accès à leurs dossiers de santé, ils ne peuvent ni modifier, ni supprimer, ni ajouter d'informations liées à la santé dans ces dossiers. Dans une telle architecture, des politiques d'accès peuvent être définies à l'aide de services logiciels, tandis que différentes entités peuvent utiliser d'autres services pour accéder aux DME. Comme les DME peuvent être mis à jour par plusieurs entités autorisées, la technologie blockchain peut également être utilisée pour enregistrer toutes ces mises à jour afin de maintenir une piste d'audit fiable qui peut fournir un historique détaillé de toutes les mises à jour des DME.

Le partage sécurisé des DME et des informations de santé connexes peut également faciliter une analyse fine des données des patients, des innovations médicales et des résultats de recherche, en plus des données collectées sur les traitements, les diagnostics et les travaux connexes, de manière sécurisée et anonyme si nécessaire. De plus, la blockchain peut être utilisée pour soutenir d'autres industries liées à la santé, comme l'industrie pharmaceutique. Un exemple est l'utilisation de la blockchain pour améliorer la gestion de la chaîne d'approvisionnement pharmaceutique.

VI. Blockchain et sécurité

L'une des principales préoccupations concernant l'utilisation de la blockchain est la sécurité. Comme les applications blockchain sont connectées et disponibles sur Internet, elles sont vulnérables à diverses cyberattaques, notamment le vol, les tentatives d'espionnage et les attaques par déni de service (DoS), qui peuvent rendre les services blockchain indisponibles. L'une des attaques de vol a été menée contre MtGox, une plateforme d'échange de bitcoins basée à Tokyo, au Japon, en 2014, qui a entraîné une perte de 600 millions de dollars. Un autre exemple concerne la monnaie numérique Ether, pour une valeur d'environ 55 millions de dollars. L'une des attaques qui peut compromettre un réseau de cryptomonnaie est l'attaque des 51%. Elle est également appelée attaque majoritaire ou attaque >50%. Si la majorité des mineurs (ordinateurs traitant les transactions du réseau) dans de tels réseaux sont gérés par une seule entité, ils auraient la capacité de sélectionner les transactions à approuver. Cela leur permet de rejeter d'autres transactions et d'autoriser leurs propres pièces à être dépensées plusieurs fois, ce qu'on appelle une double dépense. Ce type d'attaque s'est produit davantage dans les cryptomonnaies avec de petites communautés de mineurs, tandis que les cryptomonnaies avec de grandes communautés de mineurs, comme Bitcoin, sont plus résistantes à ce type d'attaque. Il a été constaté que plus de 20 millions de dollars de vol de cryptomonnaies ont été réalisés avec cette attaque au cours des 10 premiers mois de 2018. Bien que ce type d'attaques se soit principalement produit pour les applications de cryptomonnaies, il pourrait également se produire pour d'autres applications blockchain avec

de petites communautés de mineurs. Sans mesures de sécurité appropriées pour se protéger contre de telles attaques, elles peuvent paralyser les applications. Malheureusement, la nature même de la blockchain et ses modèles d'utilisation augmentent cette vulnérabilité car elle fonctionne sur plusieurs plateformes, communique en utilisant des réseaux ouverts et implique plusieurs entités. Les mesures de sécurité actuelles offrent certaines réponses, mais il est nécessaire d'aborder les problèmes spécifiquement dans le contexte de la blockchain pour élaborer des modèles de sécurité plus adaptés et efficaces.

Dans de nombreuses applications industrielles comme les applications de santé, où des informations sensibles ou privées sont généralement impliquées, il est important de garantir que toutes les technologies et applications utilisées incluent et maintiennent des niveaux acceptables de mesures de sécurité et de confidentialité. Bien que la blockchain offre de nombreux avantages positifs pour différentes industries, elle pose également plusieurs menaces à leur sécurité, leur sûreté, leur fiabilité et leur confidentialité en s'appuyant fortement sur leurs caractéristiques. De plus, comme les solutions blockchain seront intégrées à d'autres solutions de systèmes industriels, cette intégration doit également être sécurisée. La possibilité d'accès illégal ou d'attaques malveillantes sur de telles infrastructures peut conduire à des résultats catastrophiques affectant les opérations et l'infrastructure de l'industrie, ses clients et ses partenaires.

VII. Aspects négatifs de la blockchain

1. Activités illégales

Bien que la confidentialité sur le réseau blockchain protège les utilisateurs contre les piratages et préserve la vie privée, elle permet également des échanges et des activités illégales. L'exemple le plus souvent cité d'utilisation de la blockchain pour des transactions illicites est probablement Silk Road, une place de marché en ligne du dark web dédiée au trafic de drogue et au blanchiment d'argent. Silk Road a fonctionné de février 2011 à octobre 2013, date à laquelle le FBI l'a fermée.[4]

Le dark web permet aux utilisateurs d'acheter et de vendre des biens illégaux sans être tracés, en utilisant le navigateur Tor, qui masque leur adresse IP. Les paiements sont souvent effectués en Bitcoin ou dans d'autres cryptomonnaies, offrant un niveau d'anonymat supplémentaire. Cela contraste fortement avec les réglementations américaines qui exigent que les fournisseurs de services financiers obtiennent des informations sur leurs clients lors de l'ouverture d'un compte. Ces institutions doivent vérifier l'identité de chaque client et s'assurer qu'ils ne figurent pas sur une liste d'organisations terroristes connues ou suspectées.

Les activités illégales facilitées par la blockchain sont variées. Le trafic de drogue est l'une des plus notables. De plus, d'autres marchés en ligne similaires ont été utilisés pour le commerce illégal d'armes. La blockchain est également exploitée pour le blanchiment d'argent, permettant aux criminels de dissimuler l'origine de fonds illicites et de les intégrer dans l'économie légale. Le financement du terrorisme représente une autre menace, car l'anonymat relatif des transactions peut être utilisé pour soutenir des activités terroristes sans éveiller les soupçons.

2. Coût de la technologie

Même si la technologie blockchain est moins coûteuse pour les utilisateurs ; elle est loin d'être gratuite.

Sur le plan énergétique consommation du Bitcoin est un sujet de préoccupation majeure. Selon diverses estimations, le réseau Bitcoin consomme annuellement entre 91 et 160 térawattheures (TWh) d'électricité. Pour mettre cela en perspective, cette consommation dépasse celle de pays entiers. En effet, dans le monde réel, l'énergie consommée par les millions d'appareils sur le réseau Bitcoin est supérieure à la consommation annuelle du Pakistan [6].

Cette consommation énorme s'explique par le processus de minage du Bitcoin, qui repose sur un mécanisme de consensus appelé **Preuve de travail (Proof of Work)** [1]. Ce processus nécessite une puissance de calcul considérable, ce qui se traduit par une forte demande en électricité. À titre de comparaison, une seule transaction Bitcoin peut consommer jusqu'à 1 200 kWh d'énergie, ce qui équivaut à près de 100 000 transactions par carte VISA [2].

La consommation du réseau Bitcoin représente environ 0,5% de la consommation énergétique mondiale. Elle utilise plus de 7 fois autant d'électricité que toutes les opérations mondiales de Google. En termes d'échelle nationale, le minage de Bitcoin consomme à peu près autant d'électricité que l'État de Washington chaque année, ou encore plus que l'Argentine entière [6].

Cette consommation énergétique a des implications environnementales significatives. On estime que la production de Bitcoin génère entre 22 et 23 millions de tonnes métriques de dioxyde de carbone chaque année [4]. Les émissions totales du réseau Bitcoin sont comparables à celles de la Grèce, ce qui en fait un contributeur important à la pollution atmosphérique mondiale et au changement climatique.

Il est important de noter que la part des énergies renouvelables dans l'alimentation du réseau a diminué, passant de 41,6% à 25,1% suite à la répression du minage en Chine au printemps 2021. Les mineurs, qui avaient auparavant accès à une quantité substantielle d'énergies renouvelables en Chine (notamment l'hydroélectricité pendant la saison des pluies), ont dû se déplacer vers des pays comme les États-Unis et le Kazakhstan, où l'électricité est principalement produite à partir de charbon ou de gaz [2].

Conclusion

Notre projet sur la blockchain a mis en lumière les principaux éléments qui constituent cette technologie innovante et prometteuse. Nous avons exploré les concepts fondamentaux tels que le hash, le bloc et la chaîne de blocs, ainsi que le processus de minage qui rend la blockchain sécurisée et décentralisée.

Les résultats de nos recherches ont confirmé l'efficacité de la blockchain dans la création d'un système de données immuable et fiable. L'utilisation des hashes pour lier les blocs et créer une chaîne linéaire unique a été particulièrement intéressante à observer.

Nous avons également examiné les applications potentielles de la blockchain, notamment dans le domaine financier avec les cryptomonnaies, mais aussi dans la gestion des documents, l'identité numérique et d'autres secteurs où une transaction sécurisée est nécessaire.

Nos découvertes soulignent l'importance de la décentralisation et de la transparence dans la gestion des données. La blockchain offre une alternative prometteuse aux systèmes centralisés traditionnels, offrant une meilleure protection contre les fraudes et une plus grande confiance entre les parties prenantes.

En conclusion, notre projet a non seulement renforcé notre compréhension de la blockchain, mais a également soulevé de nouvelles questions sur son impact futur sur notre économie et notre société.

Bibliographie

- [1] S. Nakamoto, « Bitcoin: A Peer-to-Peer Electronic Cash System ».
- [2] « Blockchain Facts: What Is It, How It Works, and How It Can Be Used », Investopedia. Consulté le: 10 octobre 2024. [En ligne]. Disponible sur: <https://www.investopedia.com/terms/b/blockchain.asp>
- [3] A. M. Shamsan Saleh, « Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review », *Blockchain: Research and Applications*, vol. 5, n° 3, p. 100193, sept. 2024, doi: [10.1016/j.bcr.2024.100193](https://doi.org/10.1016/j.bcr.2024.100193).
- [4] M. Javaid, A. Haleem, R. Pratap Singh, S. Khan, et R. Suman, « Blockchain technology applications for Industry 4.0: A literature-based review », *Blockchain: Research and Applications*, vol. 2, n° 4, p. 100027, déc. 2021, doi: [10.1016/j.bcr.2021.100027](https://doi.org/10.1016/j.bcr.2021.100027).
- [5] D. Yaga, P. Mell, N. Roby, et K. Scarfone, « Blockchain technology overview », National Institute of Standards and Technology, Gaithersburg, MD, NIST IR 8202, oct. 2018. doi: [10.6028/NIST.IR.8202](https://doi.org/10.6028/NIST.IR.8202).
- [6] X. Boyen, C. Carr, et T. Haines, « Blockchain-Free Cryptocurrencies: A Framework for Truly Decentralised Fast Transactions », 2016, 2016/871. Consulté le: 10 octobre 2024. [En ligne]. Disponible sur: <https://eprint.iacr.org/2016/871>
- [7] A. Kamilaris, A. Fonts, et F. X. Prenafeta-Boldu, « The Rise of Blockchain Technology in Agriculture and Food Supply Chains », 18 août 2019, *arXiv*: arXiv:1908.07391. Consulté le: 10 octobre 2024. [En ligne]. Disponible sur: <http://arxiv.org/abs/1908.07391>
- [8] « Blockchain Demo ». Consulté le: 10 octobre 2024. [En ligne]. Disponible sur: <https://andersbrownworth.com/blockchain/>

