BLOCKCHAIN

1 Introduction

Au fil du temps, les technologies de l'information et de la communication ont connu de nombreux développements afin de faciliter, d'améliorer et de sécuriser l'échange et le partage d'informations, de données et de fonds de manière variée. Avec l'émergence d'Internet, les communications numériques ont émergé, permettant toutes les formes d'échange de données grâce aux transactions en ligne. L'évolution d'Internet a soulevé d'importants problèmes et défis de sécurité ainsi que les stratégies correspondantes pour y faire face. Ces problèmes ont un impact croissant sur la confiance qui est la clé de voûte de notre société, car chaque interaction humaine se déroule dans le cadre de la confiance. La société de l'information a également besoin de confiance pour continuer. Il a besoin d'une confiance numérique qui devrait être activée par les technologies de l'information. Dans ce chapitre, nous allons essayer de présenter la technologie nouvelle et innovante de Blockchain. Nous montrerons comment cette technologie peut être utilisée pour partager et contrôler en toute sécurité des informations entre des parties qui ne se font pas nécessairement confiance, et comment elle profite à la façon dont nous traitons les transactions. Dans ce chapitre on va bien expliquer la technologie de la blockchain (concept, architecture, caractéristique ...etc).

2 Concept général de blockchain

La confiance est l'un des éléments les plus fondamentaux de l'existence humaine. En affaires par exemple et jusqu'à récemment, toutes nos transactions étaient basées sur des intermédiaires "de confiance" ou des tiers de confiance (TTP) qui prenaient

la tête et géraient tous les enregistrements des transactions. Aujourd'hui, les banques suivent les soldes de toutes les parties dans un grand livre fermé au public. Nous comptons sur les banques pour confirmer ou rejeter les transactions. La banque vérifie les soldes des parties commerciales dans le grand livre et les met à jour chaque fois qu'une transaction a lieu.

La blockchain est le contraire - essentiellement un système avec une autorité répartie entre les utilisateurs qui leur permet de négocier des actifs numériques[28] . Ceci est très intéressant car dans de nombreuses situations, cette même source de confiance n'est pas elle-même pleinement approuvée par ses utilisateurs. Ce manque de confiance peut conduire à des situations où les entités d'une certaine interaction souhaitée n'ont pas du tout de tels TTP.

La technologie Blockchain a été développée pour répondre à ce besoin. Il introduit une nouvelle architecture de confiance pour remplacer les intermédiaires de confiance hérités. La technologie blockchain a été proposée et déployée pour la première fois par une personne ou un groupe anonyme sous le nom de Satoshi Nakamoto, en 2008[28]. Il a développé un système de trésorerie électronique pair-à-pair décentralisé qui a exploité une nouvelle technologie, plus tard appelée " **Blockchain** ", pour créer Bitcoin, la célèbre et controversée crypto-monnaie. Le système proposé permettrait d'envoyer des paiements en ligne directement d'une partie à une autre sans passer par une institution financière. Bitcoin permet la création d'un environnement décentralisé où les transactions et les données validées cryptographiquement ne sont sous le contrôle d'aucune autorité centrale ou d'intermédiaires.

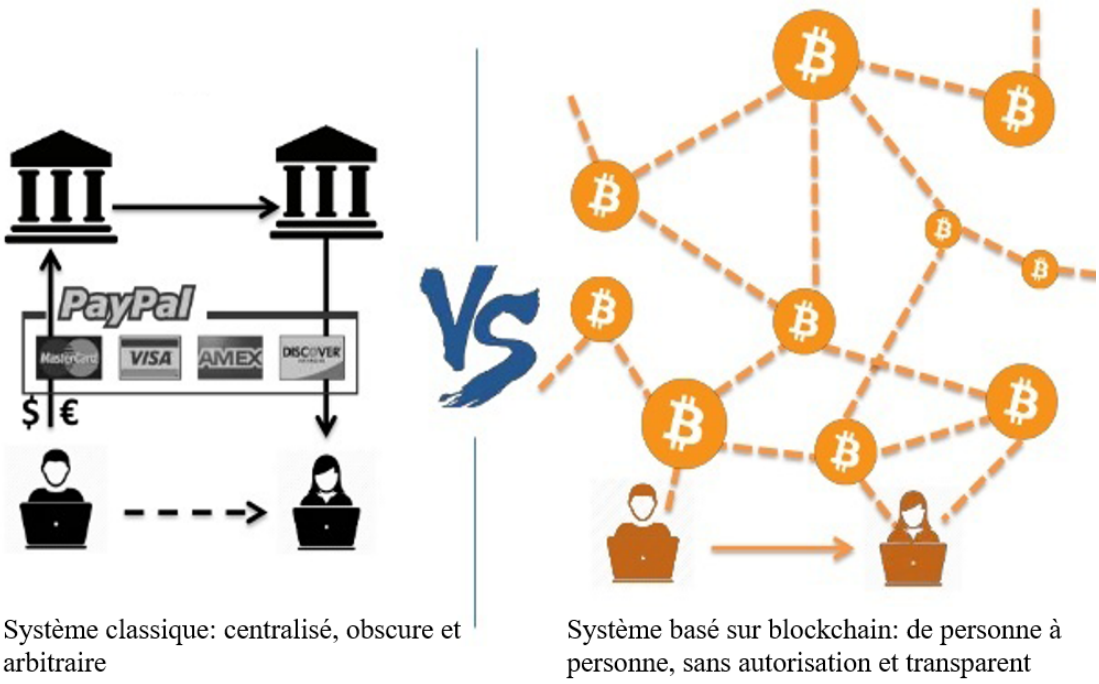

FIGURE 2.1 – Comparaison entre système classique et système basé sur blockchain

Un grand livre numérique inviolable mis en œuvre de manière distribuée (c'est-à-dire sans référentiel central) et généralement sans autorité centrale (c'est-à-dire une banque, une entreprise ou un gouvernement). À leur niveau de base, ils permettent à une communauté d'utilisateurs d'enregistrer des transactions dans un grand livre partagé au sein de cette communauté, de telle sorte qu'en fonctionnement normal du réseau de blockchain, aucune transaction ne peut être modifiée une fois publiée [29].

2.1 Définition de blockchain

La technologie Blockchain est une nouvelle technologie qui intègre la **décentralisation, le calcul distribué, le chiffrement asymétrique, l'horodatage et l'algorithme de consensus** [30]. Il fournit un registre distribué qui simplifie le processus de réconciliation des comptes grâce à des techniques de chiffrement et au protocole de transmission de messages distribués, et conserve une grande quantité de données grâce à la décentralisation. Il est capable d'augmenter l'efficacité du traitement des données et fournit une fonction de partage de données tout en garantissant la sécurité des données. Par conséquent, par rapport aux technologies traditionnelles, la technologie blockchain est dotée des atouts de durabilité, de compatibilité, de partage de données et d'inter-connectivité.

À travers les définitions ci-dessus, nous pouvons définir la blockchain comme un registre, décentralisé et public composé de nombreux pairs (nœuds)[31]. Dans la blockchain simple chaque pair a les mêmes enregistrements de données exactes dans son propre appareil, ces enregistrements distribués sont sauvegardés dans des blocs (groupe de transactions) sous une forme de chaînes immuables et sécurisées. La transparence de la blockchain vient de l'historique de toutes les transactions qui ont été effectuées à l'intérieur de celle-ci,comme toute personne ayant accès à la blockchain pourra voir toutes les transactions qui y ont eu lieu.

Aprés tous ces définitions et explications ce qu'il faut retenir est le suivant :

- La blockchain est une technologie qui permet de stocker et de transmettre les informations de manière sécurisée, fiable et transparente[32].
- Elle garde l'historique de tous les échanges qui ont pu être effectués depuis l'ouverture d'une blockchain.
- On trouve des blockchains publiques, privées et Consortium[33].
- Dans une blockchain, toutes les transactions sont traitées sous la forme de blocs devant être validés par des nœuds de réseau avant d'apparaître dans la blockchain et d'être visible de tous les utilisateurs.
- Sa transparence et sa sécurité permettent à la blockchain de pouvoir être utilisée dans plusieurs applications qui sortent du cadre de la finance.

La blockchain est composée d'un ensemble de blocs reliées entre eux avec une hash(ID) dont chaque bloc contient le hach de bloc précédent de telle manière compose la chaine de blocs [34], le bloc contient d'autres informations comme l'ensemble de transactions, l'horodatage et d'autres informations sera expliquer dans la section 3.1. Une structure de blockchain représentée dans la FIGURE 2.2 suivant.

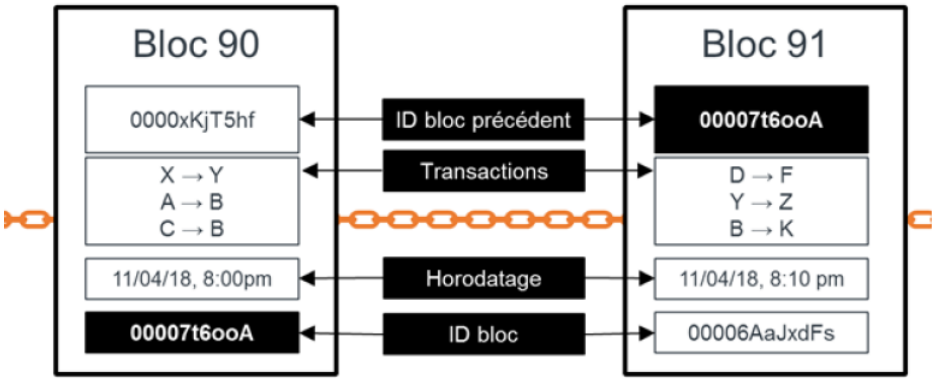

FIGURE 2.2 – Structure d'un blockchain

2.2 Fonctionnement de blockchain

Comme nous l'avons vu, la blockchain a la particularité qu'elle fonctionne sans organe central de contrôle.
Les transactions (achat ou transfert d'argent par exemple) sont distribuées entre tous les membres d'un réseau, au lieu d'être regroupées à un seul endroit ou de passer par un seul intermédiaire. On parle aussi de pair à pair.
Plusieurs étapes interviennent pour ajouter une transaction. Elles diffèrent selon le type de chaînes de blocs. Prenant un exemple d'une transaction sur Bitcoin va comme suit :

— **Étape 1 : création d'un portefeuille Bitcoin**
Un portefeuille Bitcoin doit créer pour qu'une personne puisse envoyer ou recevoir des bitcoins. Un portefeuille bitcoin stocke 2 informations : une **clé privée** et une **clé publique**[32]. La clé privée est un numéro secret(nombre aléatoire entre 0 et 2256-1) qui permet au propriétaire de signer les transactions(fonctionne comme un mot de passe qui doit être gardé secret). La clé publique utilisée pour former une adresse publique personnelle et unique (version hachée de la clé publique) à l'aide d'un algorithme de cryptographie asymétrique appelé ECDSA (Elliptic Curve Digital Signature Algorithm ou algorithme de signature numérique sur courbes elliptiques)[35], peut considérer comme un numéro de compte bancaire, les utilisateurs peuvent créer autant d'adresses publiques.

— **Étape 2 : Création d'une transaction Bitcoin**
Si Alice veut envoyer 1 BTC à Bob, Alice doit se connecter à son portefeuille Bitcoin à l'aide de sa clé privée et créer une transaction qui contient la quantité de bitcoins qu'elle souhaite envoyer et l'adresse à laquelle elle souhaite les envoyer.

— **Étape 3 : Diffusion de transaction sur le réseau de Bitcoin**
Une fois qu'Alice crée la transaction bitcoin, la transaction sera regroupée dans un **bloc** avec d'autres transactions qui attendent d'être incluses dans la Blockchain, ensuite le bloc doit diffuser sur l'ensemble du réseau Bitcoin[32].

— **Étape 4 : confirmation de transaction**
Un mineur écoutant le réseau de Bitcoin authentifie la transaction à l'aide de la clé publique d'Alice, confirme qu'Alice a suffisamment de bitcoins dans son portefeuille (dans ce cas au moins 1 BTC) et ajoute un nouveau bloc à la Blockchain de Bitcoin contenant les détails des transactions[32].

— **Étape 5 : Diffusion de changement de blockchain à tous les mineurs**
Une fois la transaction confirmée, le mineur doit diffuser la modification de la chaîne de blocs à tous les mineurs pour s'assurer que leurs copies de la chaîne de blocs sont toutes synchronisées.

Dans la blockchain, toutes les transactions sont regroupées sous la forme de blocs. Chaque bloc doit ensuite être validé par les nœuds du réseau en utilisant une méthode algorithmique. Une fois que le bloc est validé, il est ajouté à la chaîne de blocs et devient donc visible de tous les utilisateurs. Voici un schéma qui permettra d'illustrer cette définition.

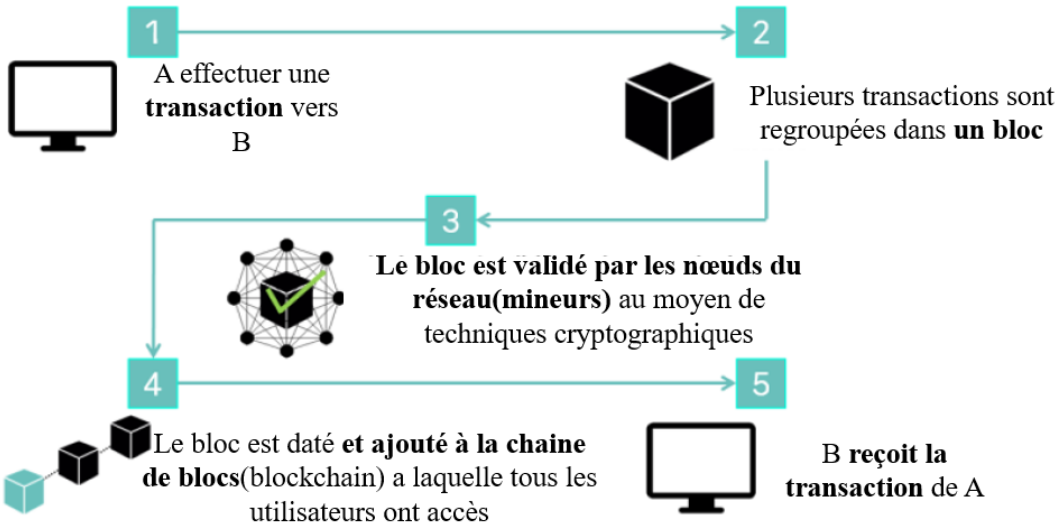

FIGURE 2.3 – Fonctionnement d'un blockchain(Blockchain france 2016)

2.3 Minage et mineurs

Le **minage** est un terme utilisé pour décrire le processus consistant à la validation d'un bloc (transactions qui attendent d'être incluses dans la Blockchain) par un des membres(nœuds) du réseau qui s'appelle **mineur**[36]. C'est donc considéré comme l'opération fondamentale d'une chaîne de blocs[37], quelle qu'elle soit, et qui la distingue d'un système centralisé classique.

Le minage consiste à contribuer à la sécurisation d'une blockchain publique en apportant une contribution en terme de puissance de calcul, dont pour qu'un mineur pouvoir créer un bloc valide dans une blockchain prenant l'exemple de Bitcoin , il est nécessaire de résoudre un problème mathématique très complexe(**preuve de travail**) , dont la solution ne peut être trouvée que par force brute, c'est-à-dire en testant au hasard des solutions jusqu'à tomber sur la bonne.
Pour cela des sociétés spécifiées des fermes de minage qui regroupent des machines dédiées pour le minage ont grande capacité de calcul (de processeurs, d'ordinateurs ou de cartes graphiques utilisées pour les jeux vidéo), alors une grande consommation d'électricité et très coûteux. Les mineurs les plus performants sont récompensés s'ils

FIGURE 2.4 – ferme-minage-bitcoin

ajoutent avec succès un nouveau bloc à la blockchain en bitcoins par exemple ils récompensent des nouveaux Bitcoins. Les mineurs ont été initialement récompensés avec 50 Bitcoins, la récompense est divisée par deux environ tous les quatre ans(6.25 BTC à partir de mai 2020).

Notez que dans la blockchain publique, chaque nœud pourrait participer au processus

de minage, et seul un ensemble sélectionné de nœuds est responsable de la validation du bloc dans la blockchain du consortium [38].

2.4 Caractéristiques de blockchain

— **Décentralisation** : parmi les aspects principaux de la blockchain est qu'il s'agit d'un registre décentralisé, ce qui signifie que les données sont conservées par tous les nœuds du réseau. Aucune autorité centrale ne tient ou ne met à jour le grand livre. Les algorithmes de consensus de plus, chaque homologue du système a le pouvoir d'ajouter de nouvelles transactions. Chaque transaction qui passe la phase de consensus sera enregistrée dans le grand livre[38].

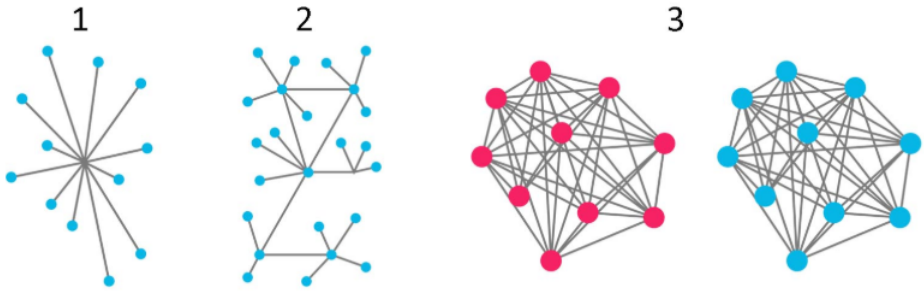

FIGURE 2.5 – Différence entre un système centralisé (1) et décentralisé (2) et (3).

— **Immuable** :une fois qu'une transaction est ajoutée à une blockchain, elle ne peut pas être supprimée ou modifiée. Cette immuabilité est l'un des principaux aspects qui contribuent à la fiabilité du système de blockchain. Le mécanisme de consensus est fait de telle sorte qu'il deviendra impossible de tromper le système et le rendra très fiable. Le grand livre distribué peut être considéré comme un enregistrement permanent irréversible[38].

— **Sécurisé** : les chaînes de blocs sont cryptographiquement sécurisées, les signatures numériques garantissant que les données contenues dans les blocs n'ont pas été modifiées.

— **Transparent** : le grand livre est partagé entre plusieurs pairs du réseau, ce qui signifie que tout utilisateur du réseau peut voir toutes les transactions depuis la création de la blockchain jusqu'au dernier bloc enregistré.

— **Persistance** : Les transactions peuvent être validées rapidement et les transactions invalides ne seraient pas admises par les mineurs. Des blocs contenant des transactions non valides ont pu être découverts immédiatement.

— **Anonymat** : Chaque utilisateur peut interagir avec la blockchain avec une adresse générée, qui ne révèle pas la véritable identité de l'utilisateur. Notez que la blockchain ne peut pas garantir la parfaite préservation de la vie privée grâce à la contrainte intrinsèque [38].

3 Architecture de blockchain

La technologie blockchaine se compose de plusieurs composants dont ils présentés dans cette section.

3.1 Bloc

Les blocs sont une structure de données fondamentale (fichier) dans la blockchain, ils sont liés entre eux pour former une chaîne de blocs. Chaque bloc peut être considéré comme une page dans le grand livre. Un bloc est un enregistrement de certaines transactions valides qui n'ont pas encore été enregistrées dans les blocs déjà chaînés. Les blocs individuels sont composés de plusieurs composants ; presque ceux-ci peuvent être différenciés dans la tête du bloc (en-tête de bloc) qui contient les métadonnées et son corps (corps de bloc)[38].

A) **En-tête de bloc**

Contient les éléments suivants (voir figure 2.6) :

- **Version de bloc** : indique quel ensemble de règles de validation de bloc à suivre, ceci est utilisé pour que les ordinateurs puissent lire correctement le contenu de chaque bloc[38].
- **Hachage de la racine de l'arbre Merkle** : la valeur de hachage de toutes les transactions dans le bloc[38].
- **Horodatage** : heure actuelle en secondes dans le temps universel depuis le 1er janvier 1970[38].
- **Nonce** : le hash que le mineur va devoir faire varier et trouver pour résoudre la preuve de travail, un champ de 4 octets, qui commence généralement par 0 et augmente pour chaque calcul de hachage[38].
- **ParentHash** : une valeur de hachage de 256 bits qui pointe vers le bloc précédent. S'il s'agit du premier bloc(bloc genèse), ce hash vaut 0.
- **Données supplémentaires** : il peut s'agir par exemple de l'index (hauteur) qui indique l'emplacement du bloc à l'intérieur de la blockchain. Le premier bloc est indexé « 0 » ; cela s'appelle le bloc de genèse, le prochain "1", et ainsi de suite[38].

B) Corps de bloc

Le corps de bloc est composé d'un compteur de transactions et transactions. Le nombre maximal de transactions qu'un bloc peut contenir dépend de la taille du bloc et de la taille de chaque transaction[38].

Dans le contexte d'une blockchain, il existe différents types de blocs :

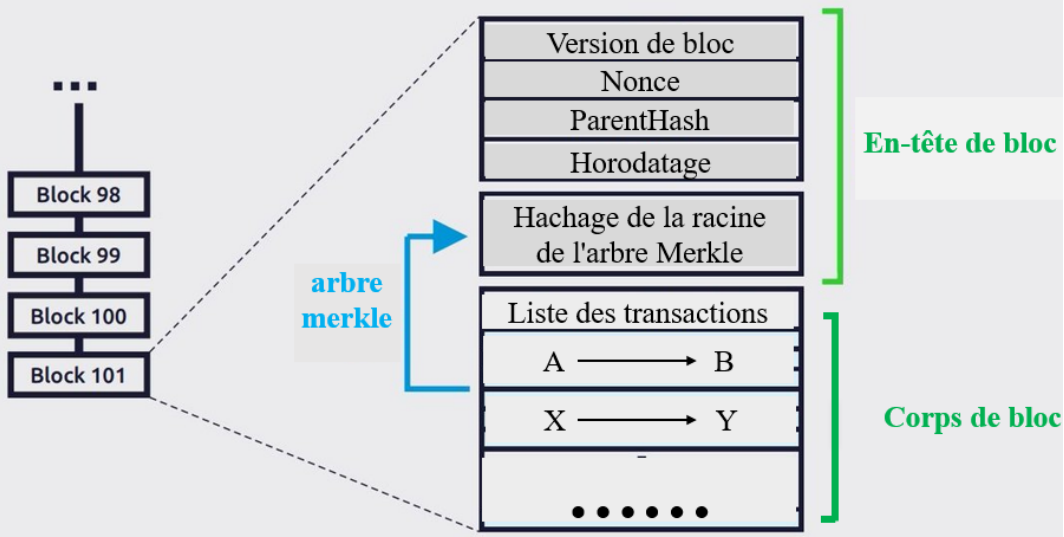

FIGURE 2.6 – Structure simplifié d'un bloc
[38]

— **Bloc genèse** : c'est le premier bloc de toute blockchain (hauteur = 0). Il fournit la base sur laquelle une blockchain entière est construite. En termes de Bitcoin, le bloc genèse a été créé le 3 janvier 2009 et contient 50 BTC.

— **Blocs de branche principale** : les blocs de branche principale font référence aux blocs qui se trouvent dans la chaîne la plus haute.

— **Blocs orphelins** : les blocs orphelins sont les blocs qui ont la même hauteur, ils se produisent lorsque deux mineurs produisent un bloc à des moments similaires. Les blocs orphelins sont considérés comme des blocs valides pour la première fois mais ils ne font pas partie de la chaîne principale.

3.2 Réseau décentralisé

Le réseau de blockchain est composé de nombreux nœuds situés dans le monde entier, chacun d'entre eux conserve une copie locale de la blockchain qui contient un enregistrement complet de toutes les transactions. Il s'agit d'un réseau pair à pair distribué où tous les deux nœuds sont autorisés à communiquer entre eux sans avoir besoin d'une autorité centrale.
Un **nœud** est un ordinateur lié au réseau de la blockchain, il représente un utilisateur particulier. On peut distinguer deux types de noeuds : les noeuds complets et les noeuds légers[39].

— **Noeuds complets** : contiennent une copie complète de la blockchain(l'historique complet de toutes les transactions), généralement suivent toutes les règles de l'algorithme de consensus pour ajouter des blocs au réseau. Parmi les tâches principales de ceux nœuds la vérification de toutes les transactions et le maintien du consensus entre les autres nœuds, peuvent considérer comme un serveur [40].

— **Noeuds légères** : ne contiennent pas la copie complète de la blockchain, mais uniquement les en-têtes de bloc. Également appelés clients VPS (Vérification de Paiement Simplifiée) qui consiste à un utilisateur peut vérifier si certaines transactions ont été incluses ou non dans un bloc. Les nœuds légers dépendent entièrement de nœuds complets et ne peuvent exister sans un nœud complet, généralement ne disposant pas de capacités matérielles suffisantes[40].

Ils considèrent toujours que la chaîne la plus longue est la branche principale et continuent de l'étendre. Lors d'une transaction, elle doit d'abord être validée puis diffusée à chaque autre nœud connecté. De cette façon, les données se propagent d'un nœud à l'autre pair-à-pair (c'est à dire sans intermédiaire) et atteignent l'ensemble du réseau. Un nœud dans un réseau blockchain remplit diverses fonctions selon le rôle qu'il prend.

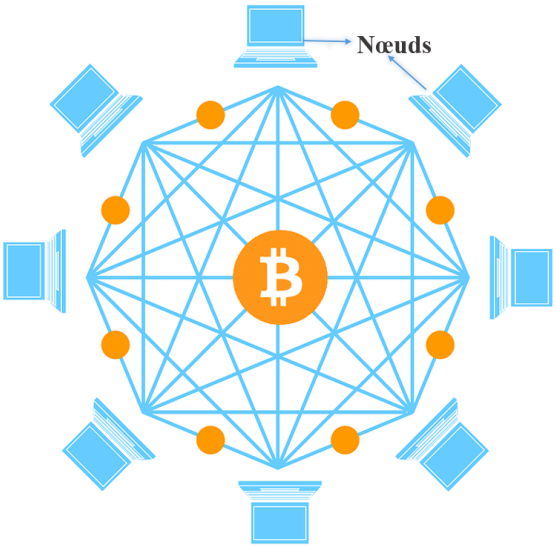

FIGURE 2.7 – Un réseau pair à pair (décentralisé)

Un nœud peut proposer et valider des transactions et effectuer du minage pour faciliter le consensus et sécuriser la blockchain. Cela se fait en suivant un protocole consensuel. (Le plus souvent, c'est la preuve de travail PoW). Les nœuds peuvent également effectuer d'autres fonctions telles que la vérification de paiement simple (nœuds légers), les valideurs et de nombreuses autres fonctions selon le type de la chaîne de blocs utilisée et le rôle attribué au nœud.

3.3 Transactions

Une transaction est l'unité fondamentale d'une blockchain. Elle représente un transfert de valeur d'un compte (adresse) à un autre compte, ce transfert est diffusé sur le réseau, collecté par les mineurs et inclus en blocs. Il est d'abord envoyé à tous les nœuds de connexion, pour augmenter les chances d'être ajouté à un bloc. Pour faire face à un problème de double dépenses, on ne peut transférer que des transactions

non dépensées. Pour éviter que chaque nœud ne doive vérifier l'historique complet de la blockchain pour les transactions partiellement non dépensées, par conception, les transactions sont soit complètement dépensées, soit non dépensées, ce qui signifie qu'il n'est pas possible de dépenser seulement une partie d'une transaction. La quantité restante peut être retransférée dans son propre « portefeuille », créant ainsi une nouvelle transaction non dépensée. Nakamoto définit une pièce comme une chaîne de signatures numériques. Pendant le transfert, le propriétaire de la pièce signe un hachage des transactions précédentes et la clé publique du récepteur et l'ajoute à la fin de cette chaîne de signatures numériques[28]. La clé privée est utilisée pour signer la transaction, et la clé publique est utilisée pour la vérification de la transaction[41], comme le montre la FIGURE 2.8. Avant la blockchain, le problème de la double dépense a été résolu en s'appuyant sur un tiers de confiance.

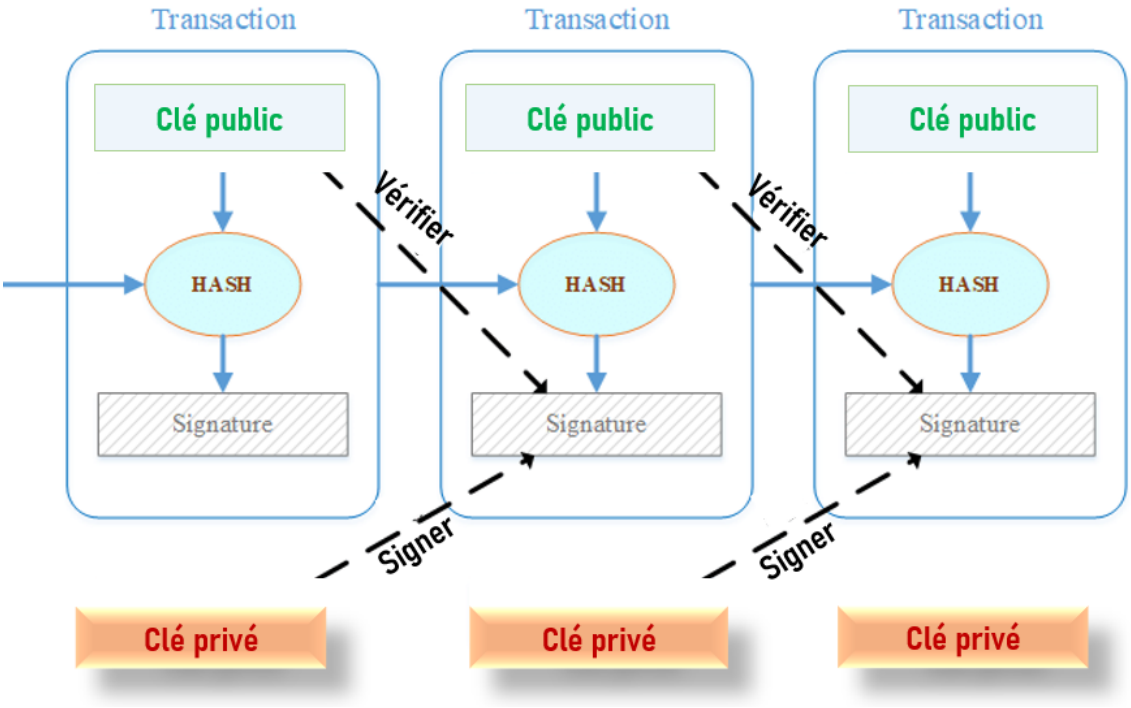

FIGURE 2.8 – Structure de transaction dans une blockchain Bitcoin [42]

3.4 Consensus

Le consensus est un grand problème dans les réseaux distribués comme la blockchain, puisqu'il n'y a pas d'entité centrale pour décider quels nouveaux blocs sont valides, chaque noeud doit décider s'il accepte ou non un nouveau bloc reçu[33]. On peut définir le consensus comme l'épine dorsale de la blockchain (système de grand livre distribué), car la sûreté et la sécurité de la blockchain sont assurées dans cette couche, généralement c'est la couche de base de la plupart des systèmes de blockchain.

Le but principal de cette couche est de faire en sorte que tous les nœuds se mettent d'accord sur un état cohérent du registre, tous suivant des règles simples[28]. Dans un réseau blockchain (Bitcoin par exemple), le consensus sert à la vérification des transactions (simple) + algorithme de consensus(PoW,Pos.....) (compliqué). Il existe de nombreuses variantes différentes de protocoles de consensus tels que la preuve de participation (PoS), PoS délégué (dPoS)....

A) **Preuve de travail (Proof of Work (poW))**

Le mécanisme de preuve de travail est considéré comme le mécanisme de consensus le plus célèbre dans la blockchain car il a été utilisé avec la première crypto-monnaie qui n'ait jamais existé. La preuve de travail est une exigence pour définir un calcul informatique coûteux, également appelé exploration, qui doit être effectué afin de créer un nouveau groupe de transactions sans confiance (bloc) sur un registre distribué de blockchain. Le processus d'extraction vérifie la légitimité d'une transaction, ou évite les soi-disant doubles dépenses et aussi pour créer une nouvelle monnaie numérique en récompensant les mineurs pour effectuer la tâche précédente. Chaque fois qu'une transaction est défini en utilisant l'algorithme POW , les événements suivants se produisent dans les coulisses :

- Les transactions sont regroupées dans un bloc.
- Les mineurs vérifient que les transactions dans chaque bloc sont légitimes.
- Pour ce faire, les mineurs devraient résoudre un casse-tête mathématique appelé problème de preuve de travail (trouver un hash qui répond à certains critères par exemple commenér par un certain nombre de zéros.) qui ne peut se résoudre qu'aléatoirement (force brute), par exemple les calculs successifs d'un hash en ajoutant une chaîne alphanumérique aléatoire (Nonce) pour obtenir différents hashs jusqu'à l'obtient d'un hash inférieur à un seuil (cible) [43]. Une récompense est donnée au premier mineur qui résout chaque problème de bloc.
- Les transactions vérifiées sont stockées dans la blockchain publique.

L'inconvénient majeur du pow est la consommation d'énergie, dont les mineurs ont pour objectif des ordinateurs puissants pour plus de puissance de calcul.

B) **Preuve d'enjeu (Proof-of- stake)**

La preuve d'enjeu ou preuve de mise est un algorithme consensuel proposé en 2012 [44] comme algorithme alternatif à la preuve de travail. Il est utilisé pour valider un bloc de transactions dans le réseau blockchain et dispose d'un mécanisme pour punir les nœuds qui ne suivent pas le protocole de consensus.

Un mineur doit miser des montants d'actifs numériques prédéfinis pour obtenir

un consensus. Contrairement à la preuve de travail, cet algorithme choisit au hasard un mineur dans le pool de minage et le mineur choisi est requis pour résoudre un problème mathématique simple. Ensuite, si le mineur résout le problème avec succès, un intérêt ou un bonus est accordé sur sa mise. Sinon, le mineur suivant est choisi au hasard. Par conséquent, il n'y a pas de course pour résoudre le problème mathématique pour obtenir une incitation économique.

Les principaux avantages de la preuve de mise sur la preuve de travail sont :

— Réduits la consommation d'énergie

— Plus de décentralisation entraînant une diminution des chances d'attaque de 51%[44].

Étant donné que la preuve de participation n'a qu'un problème mathématique simple à résoudre, les mineurs n'ont pas besoin d'ordinateurs haut de gamme pour participer à l'exploitation minière. Un ordinateur moins puissant suffit. Ainsi, beaucoup moins d'énergie est gaspillée et il n'y a pas de concurrence féroce sur la construction de nœuds à haute puissance de calcul pour obtenir une incitation économique. De plus, presque tous les nœuds peuvent participer à l'exploitation minière. Ainsi, la preuve de participation motive une participation plus large à l'exploitation minière, ce qui augmente la décentralisation de la blockchain.

C) **Preuve de mise déléguée (Delegated proof of stake DPOS)**

Le consensus du DPoS est divisé en deux processus : le premier consiste à élire les **témoins** (c'est-à-dire les producteurs de blocs) par les utilisateurs de réseau, ces témoins sont chargés de valider les transactions et de créer des blocs, ils génèrent un bloc toutes les 3s à tour de rôle, et si un témoin n'a pas terminé la tâche à l'heure spécifiée il sera ignoré et remplacé par un autre [45]. Avec DPoS beaucoup moins de nœuds sont nécessaires pour valider un bloc, prenant l'exemple de EOS (l'une des blockchains DPOS les plus populaires), n'a que 21 témoins[46], le bloc peut être confirmé rapidement, ce qui signifie que la transaction peut être confirmée rapidement.

Le second processus sert à générer des blocs. Les utilisateurs des systèmes DPoS votent également pour un groupe de «**délégués**» (parties de confiance responsables de la maintenance du réseau). Les délégués supervisent la gouvernance et les performances de l'ensemble du protocole blockchain, mais ne jouent aucun rôle dans la validation des transactions et la production de blocs. Parmi les rôles des délégués la proposition de changer la taille d'un bloc, ou le montant qu'un témoin devrait être payé en échange de la validation d'un bloc. Mis en œuvre pour la première fois dans son projet BitShares par Dan Larimer.

D) **Preuve d'autorité (PoA)**

Fonctionne selon l'idée suivante, seuls les validateurs ont le droit d'approuver

les transactions et les nouveaux blocs. Un nœud participant gagne une réputation à son identité et ce n'est que lorsque cette réputation est accumulée à un score élevé que le nœud peut devenir un validateur. Le PoA est considéré comme plus robuste que le PoS pour deux raisons. D'une part, les validateurs sont incités à vérifier honnêtement les transactions et les blocs, sinon leur identité sera associée à une réputation négative. D'autre part, un validateur ne peut pas approuver deux blocs consécutifs. Cela empêche la centralisation de la confiance.

E) **Tolérance aux pannes byzantines (BFT)**

L'algorithme pratique de tolérance aux pannes byzantine proposé par Miguel Castro et Barbara Liskov a été la première solution pratique pour parvenir à un consensus face au problème d'échecs byzantins[47]. Le problème a été expliqué de façon pertinente dans un article comme le suivant :

Imaginez que plusieurs divisions de l'armée byzantine campent à l'extérieur d'une ville ennemie, chaque division était commandée par son propre général. Les généraux ne peuvent communiquer entre eux que par messager. Après avoir observé l'ennemi, ils doivent décider d'un plan d'action commun. Cependant, certains des généraux peuvent être des traîtres, essayant d'empêcher les généraux loyaux de parvenir à un accord. Les généraux doivent décider quand attaquer la ville, mais ils ont besoin d'une forte majorité de leur armée pour attaquer en même temps. Les généraux doivent disposer d'un algorithme pour garantir que (a) tous les généraux loyaux décident du même plan d'action, et (b) qu'un petit nombre de traîtres ne puissent pas amener les généraux loyaux à adopter un mauvais plan. Les généraux loyaux feront tout ce que l'algorithme dit qu'ils doivent faire, mais les traîtres peuvent faire ce qu'ils veulent. L'algorithme doit garantir la condition (a) indépendamment de ce que font les traîtres. Les généraux loyaux doivent non seulement se mettre d'accord, mais aussi s'entendre sur un plan raisonnable[47].

Terme informatique désignant une situation où les parties concernées doivent s'entendre sur une stratégie unique pour éviter un échec complet. Toutefois, il suppose que certaines des parties concernées peuvent être corrompues ou peu fiables. L'objectif de la BFT est de pouvoir se défendre contre les défaillances byzantines, dans lesquelles les composants d'un système tombent en panne avec des symptômes qui empêchent certains composants du système de se mettre d'accord entre eux, lorsque cet accord est nécessaire pour le bon fonctionnement du système[48].

Il utilise le concept de machine d'état répliquée et de vote par répliques pour les changements d'état. Il fournit également plusieurs optimisations importantes, telles que la signature et le chiffrement des messages échangés entre les répliques

et les clients, réduisant la taille et le nombre de messages échangés, pour que le système soit pratique face aux pannes byzantines. Cet algorithme nécessite des répliques «3f + 1 » pour pouvoir tolérer les nœuds défaillants « f ». Cette approche impose une faible surcharge sur les performances du service répliqué. Les auteurs signalent un surcoût de 3% pour un service de système de fichiers réseau (NFS) sur lequel ils ont mené leurs expériences. PBFT n'a cependant été mis à l'échelle et étudié qu'à 20 répliques. C'est les frais généraux de la messagerie augmentent considérablement à mesure que le nombre de répliques augmente [38].une comparaison entre ces méthodes de consensus en terme de plusieurs critères est présentée dans le tableau 2.1.

Propriétés	PoW	PoS	DPoS	PBFT
Consommation énergétique	oui	Non	Non	Non
Type de blockchain	Publique	Publique et privée	Publique	Privée
Tolérance au fautes byzantines et à la compromission	<= 25	Dépend de l'algorithme spécifique utilisé	Dépend de l'algorithme spécifique utilisé	<=33
Niveau de sécurité	Très élevé	faible	Élevé	Faible
Niveau de décentralisation	Moyen	Élevé	Très élevé	faible
Exemple	Bitcoin	Peercoin	Bitshares	Hyperledger Fabric

TABLEAU 2.1 – Comparaison entre les algorithmes de consensus PoW,PoS,DPoS,PBFT [38]

3.5 Contrats intelligents (Smart contracts)

Les contrats intelligents sont des programmes informatiques autonomes auto-exécutables qui sont exécutés en fonction d'une condition définie par le programmeur [49]. Ces contrats sont capables de faciliter, de faire respecter et d'exécuter des accords entre deux parties en utilisant la blockchain. Contrairement aux contrats traditionnels, où un tiers (banque, notaire) est requis, les contrats intelligents permettent une entreprise indépendante entre des parties anonymes avec des frais moins chers.

Les contrats intelligents ont diverses applications possibles telles que :

— **Vote numérique** : les contrats intelligents reposant sur la blockchain peuvent améliorer la sécurité des systèmes de vote, par exemple des applications utilisent les contras intelligents et la blockchain pour protéger les votes de la fraude. Quand

une transaction de vote est enregistré sur la blockchain alors elle est protégée.Une fois le vote terminé, le contrat intelligent enverra un jeton à une adresse représentant le résultat de vote (gagnant du vote)[50].

— **Gestion d'entreprise** : les entreprises peuvent bénéficier des contrats intelligents et économiser beaucoup de temps et d'argent, ils peuvent établir un contrat intelligent simplement indiquant quand la date est telle date les salaires seront envoyés automatiquement aux employeurs.

— **Paiement** : par exemple, on peut payer le loyer de la chambre automatiquement à la fin du mois sans impliquer une banque entre les deux, un développeur écrit un programme informatique system (contrat intelligent). Ce programme définit l'intégralité des règles telles qu'elles ont été définies au début du projet : un mois de souscription, à qui les fonds seront envoyés, quel montant minimum sera récolté, quand les conditions (règles) les conditions sont remplies, telles que la date de paiement, le code sera exécuté et le paiement est effectué automatiquement

Il y'a d'autres utilisations des contrats intelligents comme le trading ou prêt de propriété, commerce d'actions ou d'obligations sur des marchés distribués [49]. En outre, il peut également être utilisé pour un système de contrat de notaire numérique autonome.

4 Quelques applications de blockchain

L'importance de la blockchain vient du fait qu'elle nous a permis pour la première fois à transférer de la valeur plutôt que de simples copies de données. En effet, la blockchain est venue empêcher les doubles dépenses et établir la confiance entre les participants anonymes dans les transactions plutôt que d'utiliser des intermédiaires de confiance. La blockchain peut être utilisée dans différents domaines d'application tels que financiers, non financiers, assurances, Internet des objets (IOT), soins de santé, Internet, crypto-monnaie, parmi les différentes utilisations on peut compter quelques exemples.

4.1 Bitcoin

En 2008, Satoshi Nakamoto a expliqué l'idée principale de son invention dans son livre blanc intitulé « Bitcoin : un système de paiement électronique pair à pair », il a déclaré : « Ce dont nous avons besoin, c'est d'un système de paiement électronique basé sur une preuve cryptographique plutôt que sur la confiance permettant à deux parties de traiter directement entre elles sans avoir besoin d'un tiers de confiance [28]. Chaque transaction est stockée dans la blockchain. Il s'agit donc d'un fonctionnement décentralisé, s'appuyant sur un système de nœuds. Chaque nouveau bloc ajouté à

la chaîne doit être vérifié, sécurisé puis enregistré. Les utilisateurs qui effectuent ces contrôles, les mineurs, sont ensuite rémunérés pour chaque nouveau bloc enregistré.

4.2 Ethereum

Ethereum est une plate-forme informatique conçue pour faciliter les contrats intelligents dans lesquels Ether est la crypto-monnaie utilisée[32]. Son prix a légèrement augmenté au fil des ans, mais il reste assez précieux. Ethereum, en tant que plate-forme, utilise le même système de blockchain que Bitcoin mais ne se limite pas aux transactions pair-à-pair et va plus loin pour prendre en charge les contrats intelligents. Étant donné la variété des applications qu'Ethereum facilite, Ether a de nombreuses utilisations immédiates.

4.3 Litecoin

Lancé en 2011 [51], Litecoin était basé sur Bitcoin mais avec plusieurs améliorations. Il a été conçu pour être plus difficile à produire, avoir une vitesse de transaction plus rapide et consommer moins de mémoire lors de son traitement.

4.4 Blockchain et l'écosystème de la santé

La blockchain a le pouvoir de faire une percée massive dans l'écosystème de la santé car elle peut facilement apporter des changements spécifiques dans la gestion des soins de santé du patient. Grâce à cette technologie, le pouvoir reviendra aux mains des gens. Cela signifie que les individus seront ainsi responsables de gérer leurs propres enregistrements, obtenant ainsi le contrôle global de leurs propres donnés.

4.5 Vote

Le système de vote traditionnel(sur les papiers) a beaucoup d'inconvénients tels que la perte de registres et la fraude électorale. Blockchain peut changer le système de vote traditionnel par un système de vote numérisé avec une plate-forme sécurisée servant de support à tout le processus(voter, dépister et compter les votes). Les résultats d'un système de vote basé sur la technologie de la blockchain sont transparents parce que les votes peuvent compter et vérifier qu'aucun vote n'avait été supprimé, modifié ou adaptée par l'être humain.

5 Taxonomie des systèmes de blockchain

La diversité de la recherche et du développement de la blockchain offre la possibilité de classer la blockchain en catégories selon un ensemble de critères comme la

décentralisation,l'immuabilité, processus de consensus...

5.1 Blockchain publique

Dans la blockchain publique(sans permission), tous les enregistrements sont visibles pour le public et comme tout le monde pourrait participer au processus de consensus(n'importe qui peut en devenir un nœud)[38] on peut s'attendre à voir une topologie très décentralisée sur un réseau établi. Étant donné que les transactions sont stockées dans différents nœuds du réseau distribué, il est presque impossible de falsifier la blockchain publique. De coté de rapidité car il existe un grand nombre de nœuds sur le réseau public de blockchain la propagation des transactions et des blocs prend beaucoup de temps car le processus de consensus prend beaucoup de temps par rapport au blockchain privé ou consortium[38].

5.2 Blockchain privée

Considérée comme un réseau centralisé car il est entièrement contrôlé par une seule organisation[38] où tous les nœuds du système sont identifiés et connus. Comme seuls les utilisateurs autorisés gèrent la blockchain, il est possible de restreindre l'accès en lecture et de restreindre les personnes qui peuvent émettre des transactions.
Les réseaux blockchain autorisés peuvent ainsi permettre à quiconque de lire la blockchain ou restreindre l'accès en lecture aux personnes autorisées. Ils peuvent également permettre à quiconque de soumettre des transactions à inclure dans la blockchain ou, encore une fois, ils peuvent restreindre cet accès uniquement aux personnes autorisées. Les réseaux blockchain autorisés peuvent être instanciés et maintenus en utilisant un logiciel open source ou fermé [29]. Plus efficace Avec moins de validateurs.

5.3 Blockchain de consortium

Également connu sous le nom d'hybride. Ce type n'est pas contrôlé par une seule autorité mais par un groupe spécifié créé pour contrôler le processus de consensus. La blockchain du consortium est un système «semi-privé» et a un groupe d'utilisateurs contrôlé, mais fonctionne à travers différentes organisations. Ils sont souvent associés à une utilisation en entreprise, avec un groupe d'entreprises collaborant pour tirer parti de la technologie de la chaîne de blocs pour améliorer les processus métier. Comme la blockchain privée il est plus efficace que la blockchain publique.
Une comparaison entre les trois types de blockchain est répertoriée dans le tableau 2.2.

Type de blockchain / Propriété	Blockchain public	Blockchain privé	Blockchain à Consortium
Qui peut la consulter ?	Tout le monde	Seulement les utilisateurs invités	Cela varie
Centralisé	Non	Oui	Partiel
Vitesse de transaction	Lente	Rapide	Rapide
Immutabilité	Presque impossible à falsifier	Pourrait être falsifié	Pourrait être falsifié
Anonymat des utiisateurs	Oui	Non	Non
Détermination du consensus	Tous les noeuds	Une organisation	ensemble de nœuds sélectionné
Permission	Sans autorisation	autorisé	autorisé

TABLEAU 2.2 – Comparaison entre les 3 types de blockchain public, privé, consortieum [38]

6 Conclusion

La technologie Blockchain est un grand registre distribué qui enregistre une liste ordonnée d'enregistrements de transactions (ou de faits) immuables reliées entre elles par une chaîne, sur des blocs, les blocs sont référencés par leur hachage et chaque bloc spécifie explicitement le bloc (hachage) sur lequel il est construit. Dans ce chapitre, nous avons présenté la blockchain et ses concepts qui est une nouvelle technologie révolutionnaire qui a captivé l'attention des chercheurs et des innovateurs dans le monde de la technologie, ainsi que leur fonctionnement. Les différents types de blockchain, et quelques applications de cette technologie dans la vie humaine sont aussi présentés dans ce chapitre.

Dans le chapitre suivant, on va expliquer comment combiner entre les deux technologies blockchain et la biométrie pour la gestion des identités.