La blockchain: au service de la transparence et de la confiance.

ARJOCA Adrian
VAN KERCKVOORDE Clément

Projet d'étude

Glossaire

BLOCKCHAIN *(n.f.)***:** Technologie de stockage et de transmission d'informations, sécurisée transparente* et fonctionnant sans organe central de contrôle. Une blockchain est une base de données décentralisée* composée de blocs liés entre eux de manière chronologique et sécurisée par la cryptographie*. Chaque bloc contient un ensemble de transactions validées par un réseau de participants (appelés nœuds) via un protocole de consensus*. Initialement popularisé par le Bitcoin, cette technologie est utilisée dans divers domaines tels que la finance, la logistique, les contrats intelligents (smart contracts) et la gestion d'identité numérique.

DÉMOCRATIE *(n.f.)***:** Système politique dans lequel le pouvoir est exercé par le peuple, directement ou par l'intermédiaire de représentants élus. Fondée sur les principes tels que la liberté d'expression, le pluralisme politique, la séparation des pouvoirs et le respect des droits fondamentaux, la démocratie vise à garantir l'égalité des citoyens devant la loi et leur participation active aux décisions publiques. Elle peut prendre plusieurs formes, notamment la démocratie directe (où les citoyens votent directement les lois) et la démocratie représentative (ou les représentants sont élus pour prendre des décisions au nom du peuple).

FINANCES *(n.f. pl.)*: Ensemble des activités liées à la gestion de l'argent, des capitaux et des ressources financières, qu'il s'agisse d'individus, d'entreprises ou d'états. Les finances englobent plusieurs domaines tels que la finance personnelle (gestion du budget, épargne, investissements individuels), la finance d'entreprise (optimisation des ressources, analyse des coûts, investissements stratégiques) et la finance publique (gestion des budgets et des dépenses d'un état). Leur objectif principal est d'assurer une utilisation efficace des ressources financières pour maximiser les rendements tout en minimisant les risques.

DÉCENTRALISATION *(n.f.)*: Processus par lequel une autorité centrale transfère une partie de ses pouvoirs de décision, de gestion ou d'administration à des entités locales ou autonomes. En politique, la décentralisation permet aux collectivités de gérer elles- mêmes certaines compétences, favorisant ainsi une gouvernance plus proche des citoyens. En technologie, notamment avec la Blockchain*, la décentralisation désigne un système ou les données ou le pouvoir de contrôle ne sont pas centralisés mais répartis entre plusieurs acteurs, garantissant une plus grande transparence, résilience et indépendance vis-à- vis d'une autorité unique.

TRANSPARENCE *(n.f.)*: Principe selon lequel les actions, décisions ou informations d'une organisation, d'une institution ou d'un individu sont accessibles, claires et compréhensibles pour les parties concernées. En politique, la transparence vise à lutter contre la corruption et à renforcer la confiance des citoyens envers leurs représentants. Dans le domaine des affaires, elle garantit une communication honnête sur les pratiques financières et opérationnelles. En technologie, notamment dans la Blockchain*, la transparence se traduit par la possibilité pour tous les participants du réseau de vérifier les transactions et les données enregistrées, assurant ainsi une meilleure responsabilité et traçabilité.

CRYPTOGRAPHIE *(n.f.)*: Science et ensemble de techniques visant à sécuriser des informations en les rendant inaccessibles à toutes personnes non autorisées. Elle repose sur des méthodes mathématiques complexes pour chiffrer (encoder) et déchiffrer (décoder) des messages ou des données. Utilisée depuis l'antiquité pour protéger des communications secrètes, la cryptographie moderne joue aujourd'hui un rôle essentiel dans la sécurité informatique, le commerce en ligne, les cryptomonnaies* et la protection des données personnelles. Ses principaux objectifs incluent la confidentialité (rendre les

données illisibles sans clé), l'intégrité (assurer que les données n'ont pas été modifiées depuis l'envoi) et l'authentification (vérifier l'identité des utilisateurs).

CONSENSUS *(n.f.)*: Accord général obtenu parmi les membres d'un groupe, souvent après des discussions ou négociations, sans opposition forte. Dans un contexte social ou politique, le consensus vise à trouver une solution acceptable pour tous, même si elle n'est pas parfaitement idéale pour chacun. En Technologie, notamment dans les systèmes décentralisés comme la blockchain, le consensus désigne un mécanisme permettant aux différents participants d'un réseau distribué de s'accorder sur l'état actuel des données (comme la validité d'une transaction). Les algorithmes de consensus les plus connus incluent le Proof of Work (PoW) et le Proof of Stake (PoS), assurant ainsi la sécurité, l'intégrité et fiabilité du système.

I. INTRODUCTION

Le monde évolue, tandis que les crimes demeurent. Le monde politique n'est pas sans risque à cette époque ou les fraudes et manque de confiance sont de plus en plus présents. L'économie mondiale centralisée est une source d'incertitude et manque de traçabilité. La démocratie est en danger face à la croissance des fraudes dans les votes traditionnels. Cependant, une solution existe. La Blockchain*. Elle peut réduire les fraudes grâce à sa transparence, elle peut être une source de confiance grace a sa décentralisation*, et elle peut en faire bien plus.

Ainsi, une question demeure: dans quelle mesure la blockchain peut-elle être utilisée pour améliorer la transparence* dans les secteurs comme les finances, le vote électronique ou la traçabilité alimentaire ?

Ce projet d'étude aura pour objectif de répondre à cette question dans les moindres détails. Pour cela, explorerons d'abord l'histoire de la blockchain* avant d'analyser son impact sur la finance* et la démocratie*.

II. HISTOIRE DE LA BLOCKCHAIN

Pour comprendre l'origine de la blockchain*, il faut remonter au début des années 1980. Ce concept novateur a été introduit par David Chaum, un informaticien américain désireux de permettre des transactions anonymes en s'appuyant sur des technologies cryptographiques. Dans les années 1990, son idée a été approfondie par Stuart Haber et Scott Stornetta, deux ingénieurs qui ont concentré leurs recherches sur la blockchain*. Leur objectif était de concevoir un système garantissant la sécurité des documents horodatés (qui comprend l'indication du moment précis). C'est toutefois en 2008 que Satoshi Nakamoto propose la première véritable application de la blockchain*. Avec le lancement du Bitcoin, basé sur les travaux cryptographiques antérieurs de David Chaum, le tout premier système monétaire numérique décentralisé* voit le jour.

La blockchain* devient alors le premier registre public, infalsifiable et accessible à tous. Cette technologie présente un potentiel extraordinaire, non seulement grâce aux innovations qu'elle apporte à la finance décentralisée, mais également en raison des transformations qu'elle engendre dans divers secteurs comme la finance, le voyage, la santé, et bien d'autres.

III. LA BLOCKCHAIN: QUEL IMPACT DANS LES FINANCES ?

Depuis la préhistoire, l'homme marchandait. Tout a commencé avec le troc (l'échange d'objets), étant la première forme d'économie. Puis, cette économie a évolué. Les objets sont devenus des animaux, puis les animaux sont devenus des pièces de métal: la première devise. Cette devise a évoluée durant des milliers d'années, jusqu'à la monnaie que l'on connait: les pièces et les billets. Par la suite, une nouvelle ère est arrivée dans l'économie: la monnaie électronique, que l'on garde sur son compte en banque. Aujourd'hui, les monnaies cryptographiques (crypto monnaies) progressent à grand pas dans le monde de l'économie, et sera certainement la prochaine devise officielle. Mais sur quoi repose cette monnaie, et comment fonctionne t elle ? Et plus important encore, quel est et quel sera son impact sur les finances mondiales ?

3.1 - LA MONNAIE DÉCENTRALISÉE ET SÉCURISÉE

Parlons des monnaies traditionnelles. À la fin des accords de Bretton Woods en 1971, les états unis ont décidé que leur monnaie, le dollar, ne serait plus adossé à l'or mais déterminée par décret, c'est à dire par l'autorité centrale de l'état. C'est ce qu'on appelle une monnaie FIAT. La confiance et la valeur de la monnaie repose donc sur la confiance que l'on donne aux différentes autorités centrales, autrement dit, les États souverains. Aujourd'hui, lorsque l'on effectue une transaction par carte ou en virement, nous faisons appel à un tiers de confiance pour valider la transaction. Pour s'assurer que la transaction est bien validée dans un monde digital, ce registre est centralisé au sein des banques et il garantit que les transactions ont bien eu lieu. Sans ce registre, un vendeur pourrait dire qu'il n'a jamais reçu son argent, même si la transaction a bien eu lieu, et inversement, un acheteur pourrait dire avoir payé sans l'avoir fait. Ce problème se nomme "Double Dépense". Les cryptomonnaies et la technologie de la blockchain se passent de ce tiers de confiance, ou l'ensemble du réseau a une copie de ce registre et garantit l'authenticité des transactions. Ce qui induit, que plus le réseau Bitcoin est décentralisé, plus il devient sûr, car il devient quasiment impossible de contrôler 51% du réseau du minage, afin de corrompre le système par un mauvais registre.

[Voir Annexe 1]

Lorsqu'un mineur n'a pas le même registre, il doit refaire les calculs pour s'aligner sur le registre commun et se débarrasser de sa donnée corrompue. Au bout d'un certain nombre de transactions, cela crée un bloc ou de nouveaux calculs sont effectués et vient s'ajouter aux autres blocs pour continuer ainsi à former la Blockchain. Ces différents calculs pour garantir le bon fonctionnement du réseau, c'est ce qu'on appelle le Proof of Work (PoW) ou en français, la preuve de travail. Les mineurs sont rémunérés en Bitcoin pour le travail effectué. Ces bitcoins proviennent des frais de transactions mais aussi de la découverte de nouveaux bitcoins. Le registre de transactions Bitcoin est publique et offre un semi anonymat, c'est-à-dire que l'on peut voir l'ensemble des transactions qui s'opèrent sur la blockchain entre différents portefeuilles, mais nous ne pouvons pas savoir à qui ces portefeuilles appartiennent.

3.2 - LES ENJEUX DE LA DISTRIBUTIVITÉ MONÉTAIRE

Les monnaies FIAT sont des monnaies émises et régulées par des banques centrales. Elles contrôlent la masse monétaire en circulation via des politiques monétaires comme la fixation des taux d'intérêts ou l'émission de nouvelle devise. La distribution passe par les banques commerciales qui jouent un rôle d'intermédiaire dans l'économie. Les banques prêtent de l'argent et permettent de gérer les transactions via des comptes bancaires. Ceci dit, il est important de savoir que la distribution de monnaies FIAT est souvent liée à des facteurs économiques et sociaux, ce qui signifie qu'une grande partie de la richesse peut être concentrée entre les mains de quelques acteurs. Pour les crypto-monnaies, comme dit précédemment, elles ne dépendent pas d'une autorité centrale. La distribution initiale repose sur des mécanismes comme le minage (Proof of Work) ou le staking (Proof of Stake), où les participants reçoivent des récompenses en fonction de leurs efforts ou de leur contribution. N'importe qui ayant accès à Internet peut participer au réseau, détenir des cryptomonnaies ou contribuer à leur minage. Cela favorise une distribution plus ouverte, bien qu'elle reste influencée par l'accès aux ressources technologiques (plus un équipement est puissant, plus il a un meilleur rendement de minage). Cependant, même si la blockchain est décentralisée, des études (voir les références) montrent qu'une grande partie des cryptomonnaies est détenue par une petite fraction d'utilisateurs appelés "baleines" (whales). Cela pose des questions sur la véritable décentralisation économique. Cette inégalité peut être due aux inégalitées techniques (Le minage nécessite des ressources coûteuses ce qui favorise les régions où l'énergie est bon marché ou les grands groupes possédant un avantage technologique) ou une meilleure situation financière initiale.

3.3 - LA TRANSPARENCE DANS LES TRANSACTIONS

La transparence est très importante dans l'efficacité de la blockchain. Chaque transaction effectuée est enregistrée de manière permanente. Elle est immuable et accessible à tous les participants du réseau, offrant un niveau inédit de vérifiabilité. Cela permet de garantir l'intégrité des données et de prévenir les fraudes ou altérations intentionnelles. Dans le domaine de la finance, cette transparence renforce la confiance des utilisateurs et des institutions en offrant une vue claire sur les flux financiers, éliminant les zones d'ombre qui pourraient favoriser les malversations.

3.4 - LES CONTRATS INTELLIGENTS

Cela fait quelque temps que l'on parle des "smart contrats" ou "contrats intelligents". Pourtant, même si ce terme est de plus en plus fréquent, il est difficile de comprendre vraiment ce que c'est. L'idée même des smart contracts remonte aux années 90. En effet, à cette époque, Nyxabo, un des précurseurs de la blockchain et du bitcoin décrivait déjà le recours à des contrats informatiques qui seraient automatiques et sécurisés sur un réseau public. Concrètement, les smart contracts ont pour but la conclusion de contrats, comme on le fait aujourd'hui, à la différence que cette fois-ci, le contrat est totalement dématérialisé, automatique et sans intermédiaire. Par exemple, si quelqu'un souhaite acheter une maison, le smart contract me permettra de conclure le contrat avec le vendeur sans qu'il y ait besoin de recourir à une banque, un notaire etc. La transaction se fera en direct entre le vendeur et le client **[Voir Annexe 2]**.

À noter également que les smart contracts sont des contrats qui utilisent une blockchain (celle de l'Ethereum) pour s'exécuter. Ils ne peuvent être exécutés sur d'autres blockchains comme le Bitcoin ou le Solana. Un autre point important et intéressant sur les smart contracts est sa sécurité. Une fois qu'il est signé, il devient immuable, c'est-à-dire qu'il ne peut plus être modifié et il devient alors impossible de revenir dessus. Cette technologie paraît révolutionnaire, mais elle a des limites. La première est liée à la transaction elle-même. Prenons un exemple: A signé un contrat de xxx€ a B pour que B lui donne un bien dématérialisé. Cela marche bien. Maintenant, reprenons l'exemple précédent. Si B vend sa maison, qui est elle-même matérielle, on ne peut l'intégrer dans la blockchain. Une fois le contrat signé, l'argent est envoyé mais on ne sait pas si B a vraiment cédé sa maison. Pour résoudre ce problème, on va faire appel à un tiers de confiance, que l'on appelle un Oracle. Cela est contradictoire au principe même du smart contrat qui devait se dérouler sans intermédiaire. Mais l'oracle n'est pas n'importe quel tiers de confiance. C'est un tiers de confiance qui aura été nommément cité par le smart contrat et qui devra intégrer dans la blockchain, et donc dans le contrat, selon laquelle la maison de B a bien été cédée, de sorte que A devient automatiquement propriétaire du bien.

A savoir qu'il existe des mécanismes prévus pour pouvoir contrôler l'oracle et s'assurer de son indépendance. La deuxième limite est liée à une des caractéristiques du contrat, son immuabilité. C'est généralement vu comme un avantage, mais c'est aussi une faiblesse. En effet, si le développeur qui a créé le contrat a malencontreusement mal codé celui ci et que ce dernier comporte des bugs, alors ces bugs peuvent être exploités, comme ce qui s'est passé pour le projet DAO qui pour rappel permettait à des utilisateurs anonymes d'accorder ou non des financements à des projets via des smart contracts. Hélas, une faille dans le code de ces contrats a permis à un pirate de récupérer 3 millions de Ethereum, ce qui ferait aujourd'hui 9 300 786 224€ soit plus de 9 millions d'euros. Enfin, la troisième limite est que le smart contrat se base sur l'ethereum. Cependant, l'ETH est une monnaie donc le cours est très volatile puisque c'est une monnaie décentralisée. Toutefois, il n'est jamais prudent de conclure un contrat se basant sur une monnaie qui est volatile. Pour remédier à ce problème, il est maintenant possible d'utiliser non pas l'ethereum mais des Stable Coins, étant des crypto-monnaies dont le cours ne varie pas.

3.5 - LA TOKENISATION DES ACTIFS: UNE RÉVOLUTION ?

La tokenisation des actifs est un processus qui consiste à convertir des actifs physiques ou financiers en jetons numériques (crypto-monnaies ou NFT) sur une blockchain. Cette technologie offre plusieurs avantages significatifs. Tout d'abord, l'un des avantages de ce processus se trouve dans la liquidité des actifs. La tokenisation permet de fractionner des actifs comme les biens immobiliers, les actions non cotées ou les œuvres d'art, en jetons plus petits et plus facilement échangeables. Par exemple, si je veux vendre une maison d'une valeur de plusieurs millions d'euros, je peux la diviser en milliers de jetons, chacun représentant une fraction de la propriété. Cela permet à tous les intéressés d'accéder à des actifs autrement inaccessibles, augmentant ainsi la liquidité du marché. Les jetons peuvent être échangés sur des plateformes de trading décentralisées, permettant des transactions plus rapides et moins coûteuses que les méthodes traditionnelles. Le deuxième avantage réside dans l'accessibilité de ce processus. La tokenisation démocratise l'investissement en rendant des actifs coûteux accessibles à un plus grand nombre de personnes. Par exemple, au lieu d'avoir besoin de millions d'euros pour acheter ma maison (en référence à l'exemple précédent), un investisseur peut acheter des jetons représentant une fraction de cet actif pour quelques centaines ou milliers d'euros. Cela ouvre de nouvelles opportunités d'investissement pour les petits investisseurs et diversifié le marché. De plus, la nature numérique des jetons permet des transactions transfrontalières plus faciles, élargissant encore l'accès international. Comme abordé précédemment, la transparence est un élément clé de la blockchain, et la tokenisation rentre très bien dans ce sujet. Puisque toutes les transactions sont enregistrées de manière immuable et accessible au public, les risques de fraude et de manipulation sont presque nulles. Les investisseurs peuvent suivre l'historique complet des transactions d'un actif tokenisé, ce qui augmente la confiance dans le marché. De plus, les smart contracts (étudiés précédemment) peuvent automatiser certaines parties du processus de transaction, comme le transfert de propriété et le paiement des dividendes, réduisant ainsi les besoins en intermédiaires et les coûts associés. La tokenisation des actifs représente donc une avancée majeure dans le domaine de la finance, offrant des avantages significatifs en termes de liquidité, d'accessibilité et de transparence.

3.6 - LA BLOCKCHAIN DANS LES FINANCES: CONCLUSION

La blockchain est déjà en train de réinventer la finance mondiale, mais elle n'offre pas seulement une alternative aux modèles traditionnels fondés sur la centralisation. Sa promesse de transparence, de sécurité et de décentralisation semble même ouvrir la voie à un modèle économique plus juste et plus accessible.
Pourtant, la vérité est plus complexe. Les cryptomonnaies et la finance décentralisée convainquent certes de plus en plus d'investisseurs et d'entreprises mais se heurtent cependant à des difficultés notables telles que la volatilité des marchés, la concentration de la richesse entre les mains d'un petit nombre d'acteurs, et surtout une réglementation encore floue et peu adaptable qui risque bien de bloquer ou retarder leur adoption massive.
En conclusion, la blockchain, ni miracle ni menace absolue pour la finance traditionnelle, se développera en fonction de la capacité des États, des acteurs financiers et des innovateurs à trouver un juste milieu entre régulation et liberté technologique. L'avenir nous dira si elle sera en mesure de s'installer en tant que nouvelle norme ou si elle restera un simple complément au système existant.

IV. LA BLOCKCHAIN: QUEL IMPACT DANS LE VOTE ÉLECTRONIQUE ?

L'essor des technologies numériques a transformé de nombreux secteurs, y compris le processus électoral. Le vote électronique est devenu une alternative moderne aux systèmes

traditionnels, offrant praticité et rapidité. Toutefois, des préoccupations demeurent, notamment concernant la sécurité, la transparence et la confiance des citoyens. Les risques de fraude et de manipulation des résultats freinent son adoption. La blockchain, avec ses caractéristiques d'immuabilité, de traçabilité et d'anonymat, offre des solutions pour renforcer la confiance des électeurs et garantir l'intégrité du processus. Il est essentiel de comprendre comment la blockchain pourrait transformer le vote électronique et répondre à ces défis.

4.1 - ENJEUX AU NIVEAU DE LA TRANSPARENCE

Le vote électronique présente de nombreux avantages en termes de praticité et d'efficacité, mais il suscite également de vives préoccupations, en particulier concernant la transparence du processus électoral. Les risques de fraude, de manipulation des résultats et de violation de la sécurité des données des électeurs sont des enjeux majeurs. Ces menaces, si elles se concrétisent, peuvent non seulement affecter les résultats des élections, mais aussi nuire à la confiance du public dans l'intégrité du processus électoral, et par extension, remettre en question la légitimité des gouvernements élus.

L'une des principales inquiétudes réside dans le manque de visibilité sur la manière dont les votes sont comptabilisés et vérifiés. Contrairement aux systèmes traditionnels où les bulletins sont comptés de manière transparente dans des bureaux de vote supervisés, le vote électronique se déroule dans un environnement numérique où il est difficile pour les électeurs et les observateurs indépendants de suivre et de vérifier les étapes du processus. Cela suscite des préoccupations sur la sécurité des systèmes informatiques, qui pourraient être la cible de cyberattaques visant à manipuler les résultats ou interférer de manière discrète avec le processus électoral.

Une autre source de tension est le risque de manipulation subtile, comme l'insertion de votes frauduleux dans les systèmes ou l'altération des données sans détection immédiate. Ces manipulations, si elles restent invisibles, peuvent grandement affecter la confiance du public dans le système démocratique. Ce problème devient d'autant plus préoccupant dans des contextes où des acteurs malveillants, qu'ils soient internes ou externes, cherchent à influencer les élections pour des raisons politiques, économiques ou géopolitiques.

De plus, le manque de transparence sur le fonctionnement des algorithmes utilisés pour comptabiliser les votes aggrave la méfiance. Si ces systèmes ne sont pas expliqués clairement et audités de manière indépendante, il devient difficile pour les électeurs d'être sûrs que leur vote est pris en compte correctement et que le processus est équitable. Cela peut entraîner un climat de méfiance et, à terme, une diminution de la participation électorale, car les électeurs douteront de l'efficacité de leur vote et de la sincérité des résultats.

Pour garantir la confiance dans le vote électronique, il est essentiel d'intégrer des mécanismes de transparence et de sécurité robustes. Les systèmes de vérification indépendants des résultats, la traçabilité des votes et des protocoles de sécurité renforcés sont des éléments clés pour rassurer les citoyens. Par ailleurs, une communication claire sur le fonctionnement du système et les mesures de sécurité mises en place est cruciale pour apaiser les inquiétudes et préserver la légitimité du processus électoral.

4.2 - CONTRIBUTION DE LA BLOCKCHAIN

La blockchain offre une solution innovante pour améliorer la transparence, la fiabilité et la sécurité des systèmes de vote électronique. Elle présente plusieurs avantages majeurs, notamment la vérification et la traçabilité des votes, ainsi que la réduction des fraudes électorales.

Vérification et traçabilité des votes :
L'un des défis du vote électronique est d'assurer que chaque vote soit enregistré correctement et ne puisse être modifié après son inscription. Grâce à son principe de décentralisation et d'immuabilité, la blockchain garantit que chaque vote est une transaction transparente et infalsifiable. Une fois inscrit, le vote devient accessible à tout moment pour être vérifié, ce qui renforce la confiance des électeurs et assure la transparence du processus électoral.

Réduction des fraudes :
La blockchain réduit les risques de fraude, notamment les votes multiples. Chaque vote est unique et lié à un électeur grâce à des méthodes d'identification sécurisées. De plus, toute tentative de modification des résultats serait immédiatement détectée, car chaque changement nécessiterait de modifier toutes les copies de la blockchain, ce qui est pratiquement impossible. La décentralisation de la blockchain empêche également la manipulation des résultats par une entité centralisée.

Sécurisation des données :
La blockchain protège les données personnelles des électeurs par des techniques de cryptographie avancées. Les informations sont décentralisées, ce qui réduit les risques de cyberattaques et garantit une meilleure confidentialité.

Confiance et participation démocratique :
En améliorant la sécurité, la transparence et la traçabilité, la blockchain peut renforcer la confiance des citoyens dans le système électoral. Si les électeurs ont l'assurance que leur vote est sécurisé et non manipulable, cela pourrait encourager une participation plus large et augmenter la légitimité des élections.

En conclusion, la blockchain représente une avancée majeure pour la fiabilité et la sécurité du vote électronique. Ses caractéristiques de décentralisation, d'immuabilité et de transparence permettent de garantir l'intégrité des élections, de réduire les fraudes et d'assurer une traçabilité complète des votes. Cependant, il est essentiel de continuer à tester ces systèmes dans des contextes réels pour identifier d'éventuelles vulnérabilités et assurer leur efficacité à grande échelle.

4.3 - ANONYMAT ET INTÉGRITÉ

La blockchain, tout en garantissant la transparence et la sécurité du processus électoral, permet également de concilier l'anonymat des électeurs et l'intégrité des votes. Dans les systèmes de vote traditionnels, l'anonymat peut entrer en conflit avec les exigences de vérification et de sécurité. La blockchain résout cette problématique en préservant la confidentialité des électeurs tout en assurant la fiabilité du processus de vote.

Anonymat des électeurs :
Contrairement aux systèmes centralisés où les informations personnelles des électeurs peuvent être compromises, la blockchain protège l'anonymat en attribuant à chaque électeur un identifiant cryptographique unique, sous forme de hash alphanumérique. Ce hash est généré à partir des données d'identification, de manière sécurisée et non réversible. Cela permet de représenter un électeur sans stocker ses informations personnelles sur la blockchain. L'identifiant ne peut être associé à une personne sans la clé privée correspondante, assurant ainsi la confidentialité des électeurs pendant toute la procédure.

Dissociation du vote et de l'identité de l'électeur :
La blockchain dissocie le vote de l'identité de l'électeur. Même si un individu accède à un enregistrement de vote, il ne pourra pas savoir qui a exprimé ce choix. Cette séparation

entre l'identité et le vote est essentielle pour maintenir l'intégrité et la confiance dans le processus électoral.

Sécurité et transparence :
En plus de l'anonymat, la blockchain garantit l'intégrité des votes grâce à l'immuabilité des transactions. Une fois un vote soumis, il devient impossible de le modifier ou de le falsifier. Le caractère décentralisé de la blockchain offre également une couche de sécurité supplémentaire, en éliminant les risques liés à un serveur central vulnérable aux attaques.

Équilibre entre confidentialité et transparence :
La blockchain offre un équilibre entre confidentialité et transparence. D'un côté, elle assure une transparence totale du processus, car chaque vote est enregistré de manière publique et vérifiable. De l'autre, elle garantit la confidentialité des électeurs, préservant ainsi la liberté de vote.

Ainsi, la blockchain résout une question complexe du vote électronique : comment garantir l'anonymat des électeurs tout en préservant l'intégrité des votes ? L'utilisation d'identifiants cryptographiques permet de répondre à cette problématique de manière sécurisée et transparente. Cela représente une avancée majeure pour moderniser les systèmes électoraux, renforçant la confiance des citoyens dans la démocratie et le processus électoral.

4.4 AUTHENTIFICATION SÉCURISÉE

L'authentification sécurisée est essentielle pour garantir l'intégrité et la légitimité des élections électroniques. Afin de s'assurer que seuls les citoyens autorisés peuvent participer, il est crucial de mettre en place des mécanismes solides d'identification et de validation des électeurs. Sans une identification adéquate, les systèmes de vote électronique sont vulnérables aux attaques, telles que le vol d'identité ou l'usurpation de vote, compromettant ainsi la validité des résultats.

Technologies modernes pour l'authentification
Les technologies modernes offrent plusieurs solutions efficaces pour garantir une authentification sécurisée des électeurs. Les systèmes biométriques et les clés cryptographiques sont particulièrement adaptés aux exigences de sécurité des élections électroniques.

Authentification biométrique
L'authentification biométrique repose sur des caractéristiques physiques uniques à chaque individu, telles que les empreintes digitales, la reconnaissance faciale, l'iris ou la reconnaissance vocale. Ces caractéristiques sont difficiles à reproduire, ce qui rend cette méthode d'identification extrêmement fiable. Lors de la connexion au système de vote, l'électeur peut être invité à fournir l'une de ces données, qui sera comparée à celles stockées dans une base de données sécurisée, validant ainsi son identité rapidement et de manière fiable. L'un des grands avantages de la biométrie est qu'elle ne repose pas sur des mots de passe ou des identifiants, réduisant ainsi les risques liés à leur oubli ou à leur partage.

Clés cryptographiques
Les clés cryptographiques sont une autre méthode puissante pour l'authentification des électeurs. Ce système repose sur l'utilisation de clés publiques et privées, associées de manière unique à chaque électeur. Lors de l'inscription, l'électeur reçoit une clé privée

sécurisée, lui permettant de se connecter et de voter de manière anonyme mais vérifiable. La clé publique, quant à elle, est utilisée sans révéler l'identité de l'électeur. Cette méthode renforce la sécurité en empêchant toute tentative de falsification des votes. Si un attaquant intercepte les données, il ne pourra pas les modifier sans la clé privée associée.

Réduction des risques de fraude et d'usurpation

L'utilisation de technologies comme la biométrie ou les clés cryptographiques limite les risques de fraude, notamment le vol d'identité ou l'usurpation de vote. Dans un système traditionnel, un individu malveillant pourrait se faire passer pour une autre personne, mais avec la biométrie et la cryptographie, chaque électeur est authentifié de manière unique et fiable, rendant ces fraudes pratiquement impossibles. Ces technologies permettent également d'éviter le vote multiple, car une fois l'identité validée, le système bloque toute autre tentative de participation.

Protection de la vie privée et confidentialité des électeurs

Un défi majeur de l'identification sécurisée dans le vote électronique est de garantir que les informations personnelles des électeurs ne soient pas compromises. Les systèmes de biométrie et de cryptographie, bien implémentés, respectent cette exigence en protégeant les données sensibles, telles que les empreintes digitales ou les photos faciales. La cryptographie chiffre les données de manière à ce que même les administrateurs du système ne puissent pas connaître les détails du vote ou l'identité des électeurs.

L'authentification sécurisée est donc un pilier fondamental pour garantir la sécurité et l'intégrité du vote électronique. Grâce à des technologies comme la biométrie et les clés cryptographiques, il est possible de valider l'identité des électeurs tout en protégeant leur vie privée. Ces solutions minimisent les risques de fraude, de vol d'identité ou d'usurpation, et assurent que seul un électeur autorisé puisse participer. Elles sont essentielles pour maintenir la confiance des citoyens dans les élections électroniques et préserver l'intégrité des résultats.

4.5 - CAS CONCRETS

Plusieurs pays ont déjà expérimenté ou adopté des systèmes de vote basés sur la blockchain.

- Estonie : Pionnière en matière de technologie numérique, l'Estonie utilise des solutions blockchain pour renforcer la sécurité et la transparence de son système de vote en ligne.
- Suisse : Plusieurs cantons suisses ont testé le vote électronique en s'appuyant sur la blockchain pour garantir la confidentialité et l'intégrité des résultats.
- Russie : Lors de certaines élections locales, la Russie a utilisé la blockchain pour enregistrer les votes de manière transparente.
- Etats-Unis : Dans certains états, des pilotes ont été menés pour tester la blockchain comme un outil pour des élections locales et des votes des citoyens éloignés (comme les militaires en déploiement).

Ces initiatives montrent que la blockchain est une technologie prometteuse pour transformer le vote électronique. Cependant, des défis techniques, éthiques et juridiques subsistent avant une adoption généralisée.

V. L'impact de la blockchain sur la traçabilité alimentaire

La traçabilité alimentaire est devenue un enjeu majeur dans l'industrie agroalimentaire. Les consommateurs, de plus en plus soucieux de la qualité et de l'origine des produits qu'ils

consomment, exigent une transparence accrue. Les scandales alimentaires passés et la mondialisation des circuits de distribution ont accentué cette demande.
La blockchain, technologie reposant sur un registre numérique décentralisé et infalsifiable, s'impose comme une solution innovante pour répondre à ces attentes. Elle permet d'assurer une traçabilité fiable des aliments, de leur production à leur commercialisation, en garantissant l'intégrité des informations partagées entre les différents acteurs de la blockchain d'approvisionnement.

5.1 - LES ENJEUX DE LA TRAÇABILITÉ ALIMENTAIRE

Un besoin croissant de transparence

La confiance des consommateurs dans l'industrie agroalimentaire a été mise à mal par de nombreuses crises sanitaires et fraudes alimentaires. Les consommateurs veulent désormais être assurés et de la qualité des produits qu'ils achètent, en disposant d'informations précises et vérifiables sur:

- L'origine des ingrédients
- Les conditions de production et de transformation
- L'empreinte écologique du produit

L'absence de transparence peut entraîner une méfiance généralisée, nuisant aux marques et aux distributeurs. En renforçant la traçabilité des produits, il devient possible de rassurer le consommateur et de valoriser les pratiques responsables des producteurs.

Des défis logistiques et technologiques

Assurer une traçabilité complète des produits alimentaires est un défi complexe, notamment en raison de la multiplicité des acteurs impliqués : agriculteurs, transporteurs, transformateurs, distributeurs, etc.. Chaque intervenant doit être capable d'enregistrer et de transmettre des informations précises de manière fiable et sécurisée. Or, les systèmes suivi
Les Actuels reposent souvent sur des bases de données centralisées, vulnérables aux erreurs, fraudes et manipulations.
De plus, la diversité des normes et réglementations entre les pays compliqué encore davantage l'harmonisation des pratiques de traçabilité. Une technologie robuste et universellement accessible est donc nécessaire pour relever ces défis.

VERS UNE TRAÇABILITÉ ALIMENTAIRE RENFORCÉE GRÂCE A LA BLOCKCHAIN : ARCHITECTURE ET MÉCANISMES

La blockchain est une technologie de stockage et de transmission d'information sous forme de blocs sécurisés et reliés entre eux de manière chronologique.Elle repose sur trois principes fondamentaux:

- **Décentralisation :** Les données ne sont pas stockées sur un serveur central, mais réparties entre plusieurs participants, garantissant ainsi leur sécurité.
- **Immuabilité :** Une fois enregistrées, les informations ne peuvent pas être modifiées ou supprimées, ce qui empêche la falsification.
- **Transparence :** Tous les acteurs de la chaîne ont accès aux informations inscrites dans la blockchain, favorisant ainsi la confiance mutuelle.

Les avantages pour l'industrie agroalimentaire

L'intégration de la blockchain dans le secteur agroalimentaire présente plusieurs bénéfices majeurs :

- Fiabilité accrue des données : Chaque transaction et chaque information enregistrée sont sécurisées et infalsifiables.
- Meilleure traçabilité des produits : L'ensemble du cycle de vie d'un produit peut être suivi en temps réel, depuis la ferme jusqu'au rayon du supermarché
- Gain de confiance des consommateurs : Grâce à des QR codes ou applications mobiles, les consommateurs peuvent accéder instantanément aux informations relatives à un produit (origines, date de récolte, méthode de production, certifications, etc).
- Optimisation de la gestion des rappels de produits : En cas de contamination ou de problème sanitaire, l'identification rapide des lots concernés permet d'agir efficacement et de limiter les risques pour la santé publique.

5.4 - DES INITIATIVES MISES EN PLACE PAR LES GRANDES ENTREPRISES

Plus acteurs majeurs du secteurs agroalimentaire ont déjà adopté la blockchain pour améliorer la traçabilité de leurs produits :

- Carrefour : Le groupe a intégré la blockchain pour garantir la traçabilité de certains produits (poulet, lait, tomates, etc) en scannant un QR code sur l'emballage, le consommateur peut accéder aux détails du parcours du produit. [VOIR ANNEXE 3]
- IBM Food Trust : Ce réseau basé sur la blockchain permet aux distributeurs et producteurs de suivre en temps réel les flux alimentaires et d'améliorer leur gestion logistique.

Ces initiatives ne se limitent pas à une simple innovation technologique, mais constituent une véritable réponse aux enjeux de transparence et de sécurité alimentaire.

5.5 - IMPACTS ET BÉNÉFICES POUR LES CONSOMMATEURS

L'implémentation de blockchain dans l'agroalimentaire présente des avantages directs pour les consommateurs :

- Une information claire et accessible : Grâce à des outils numériques, chacun peut vérifier en un instant l'authenticité et la qualité des produits qu'il consomme.
- Une meilleure valorisation des producteurs responsables : Les producteurs qui respectent des normes environnementales et éthiques peuvent mettre en avant leur engagement.
- Une sécurité sanitaire renforcée : En cas de crise alimentaire, la blockchain permet d'identifier rapidement les produits contaminés et de limiter leur distribution.

La blockchain représente une avancée majeure dans le domaine de la traçabilité alimentaire. Son adoption croissante par les industriels et de distributeurs témoigne de son efficacité pour répondre aux attentes des consommateurs en matière de transparence et de sécurité.

En offrant une visibilité complète sur le parcours des produits, cette technologie contribue à restaurer la confiance entre les différents acteurs de la chaîne agroalimentaire. A terme la confiance pourrait devenir un standard incontournable en favorisant la consommation plus responsable et éthique.

REFERENCES

Lexique du monde des crypto monnaies et de la blockchain
https://cryptoast.fr/lexique

La répartition des richesses dans les cryptomonnaies, 15 mai 2020 à 11:14 par Alex Griest
https://cryptoast.fr/repartition-richesses-cryptomonnaies/

Comment les grandes banques deviennent des "baleines à bitcoins", BBC News, 8 mars 2024
https://www.bbc.com/afrique/articles/c90eqkxkpezo

Observation des baleines : qui sont les plus gros détenteurs de Bitcoin ?, 27 décembre 2024 par Kala Philo sur Zenledger
https://zenledger.io/fr/blog/whale-watching-who-are-the-largest-holders-of-bitcoin/

Le BITCOIN pour les NULS, 15 janv. 2022 par Crypto pour les nuls sur Youtube
https://www.youtube.com/watch?v=Ou40HUON

La décentralisation, loin d'être une préoccupation des investisseurs cryptos Français, Le 11/12/2024 à 14:24 par Pauline Armandet sur BFMTV
https://www.bfmtv.com/crypto/la-decentralisation-loin-d-etre-une-preoccupation-des-investisseurs-cryptos-francais_AV-202412110568.html

La Blockchain : explorer les nouvelles frontières de la confiance et de la transparence, École Polytechnique Executive Education, publié le 05/02/2024
https://exed.polytechnique.edu/la-blockchain-explorer-les-nouvelles-frontieres-de-la-confiance-et-de-la-transparence

Un SMART CONTRACT c'est QUOI ? de Enissay le 22 février 2022 sur Youtube
https://www.youtube.com/watch?v=fChbMGRnCf8

Smart Contracts in Blockchain, le 23 Mai 2024 sur Geeksforgeeks
https://www.geeksforgeeks.org/smart-contracts-in-blockchain/

DAO perd 50 millions de dollars lors d'un piratage, de SOPHIE EUSTACHE le 17 juin 2016 sur Usine Digitale
https://www.usine-digitale.fr/article/dao-perd-50-millions-de-dollars-lors-d-un-piratage.N397787

Qu'est-ce que la tokenisation et quels secteurs transforme-t-elle ? De Marius Farashi Tasooji le 24 janvier 2024 sur cryptoast
https://cryptoast.fr/tokenisation-quels-secteurs-transforme/

Tokenisation : Concept et perspectives pour les entreprises, par Amaury Laurendeau le 25/11/2024 sur Le Blog Du Dirigeant.
https://www.leblogdudirigeant.com/quest-ce-que-la-tokenisation/

Divers articles scientifiques sur plusieurs sujet de la blockchain, plusieurs auteurs, dernière mise à jour il y a 3 ans
https://github.com/bellaj/Blockchain

Utilisation de la blockchain dans le vote électronique
https://www.esilv.fr/portfolios/utilisation-de-technologie-blockchain-vote-electronique/

Election, vote et blockchain
https://www.alyra.fr/post/election-vote-et-blockchain

Le système innovant du vote électroniquex
https://www.netservice.eu/fr/produits-et-solutions/b-voting

Explication de la traçabilité alimentaire
https://crystalchain.io/fr/tracabilite-origine-des-produits-blockchain/

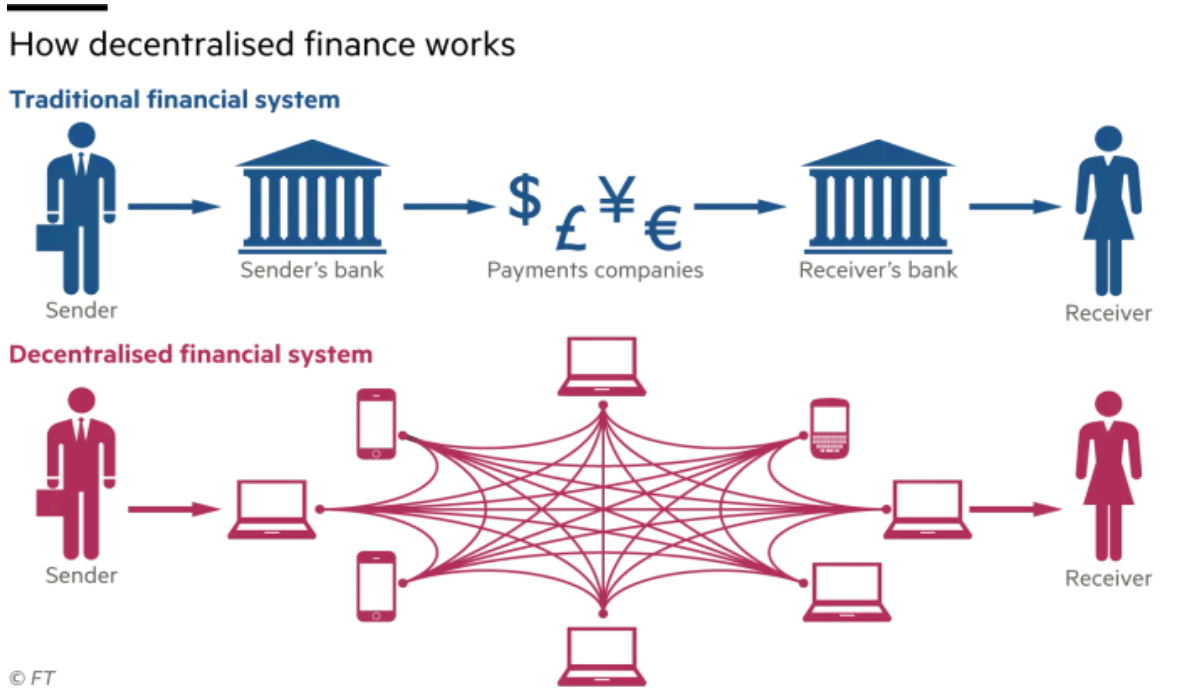
Cas d'usage de la blockchain dans des entreprise de l'agroalimentaire
https://www.alcimed.com/fr/insights/5-cas-usage-cryptomonnaies-agroalimentaire/

Comment marche la traçabilité alimentaire grâce à la solution que propose carrefour
https://www.carrefour.com/fr/groupe/la-transition-alimentaire/la-blockchain-alimentaire

La traçabilité alimentaire via la blockchain comment ça marche ?
https://www.europe1.fr/economie/tracabilite-alimentaire-grace-a-la-blockchain-la-transparence-sinvite-sur-les-emballages-4042081

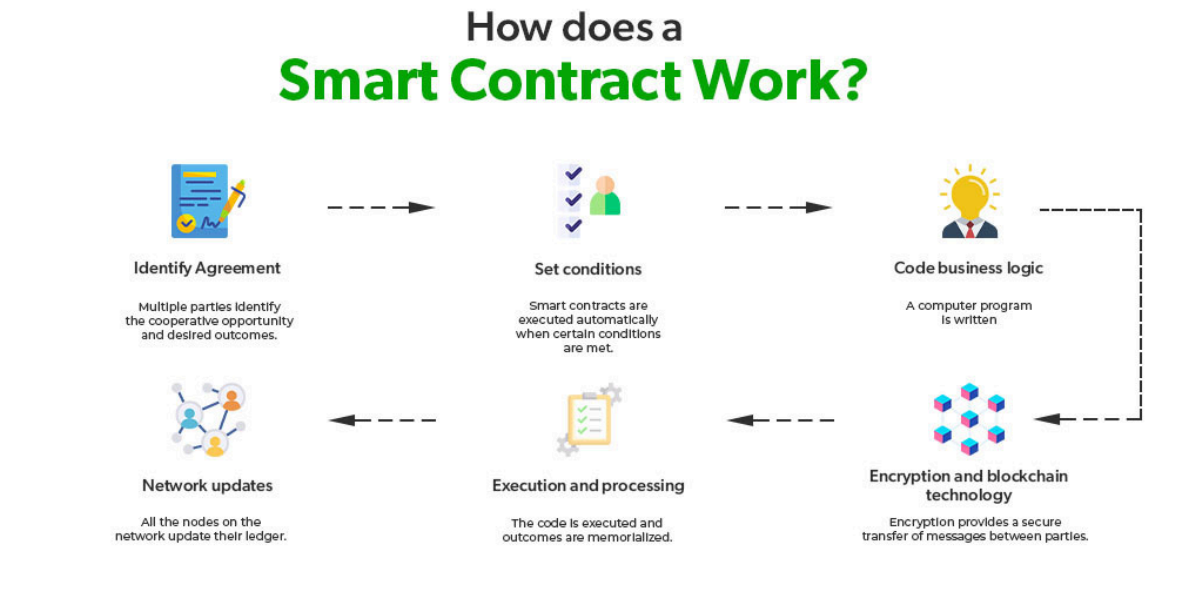
ANNEXES

N° 1: Centralisé ou décentralisé



Source: https://davidgerard.co.uk/blockchain/wp-content/uploads/2020/01/ft-defi.png

N° 2: Fonctionnement des Smart Contracts



https://www.geeksforgeeks.org/smart-contracts-in-blockchain/

N° 3: Exemple d'affichage lié au QR code pour la traçabilité alimentaire

https://www.europe1.fr/economie/tracabilite-alimentaire-grace-a-la-blockchain-la-transparence-sinvite-sur-les-emballages-4042081