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

Quel est l'impact de la blockchain dans les finances, la démocratie et la traçabilité alimentaire

ARJOCA Adrian
VAN KERCKVOORDE Clément

Projet d'étude 2024/2025

SUP DE VINCI
INGÉNIERIE DES SYSTÈMES D'INFORMATION

SOMMAIRE

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 grâce à 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 évolué 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 (c'est d'ailleurs de là que vient son nom). 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 (euro, dollar...). 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. Cela 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 inégalités 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€ à 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.

Il est également bon à 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 nuls. 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 éco-no-mique 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 ?

Les avancées numériques ont bouleversé de nombreux métiers, y compris celui de l'élection. Ainsi, le vote électronique a émergé comme une alternative moderne au système traditionnel, qui reste pratique et rapide, malgré les réticences à son adoption, notamment liées à la sécurité, la transparence et la confiance. La fraude et la manipulation des résultats, souvent évoquées, rendent la transition vers le vote électronique compliquée. La blockchain, en raison de ses propriétés d'immuabilité, de traçabilité et d'anonymat, pourrait apporter des

solutions pouvant sécuriser ce process et rassurer les électeurs sur l'intégrité du vote. Dès lors, que pourrait entraîner une telle transformation du vote électronique par la blockchain ?

4.1 - ENJEUX AU NIVEAU DE LA TRANSPARENCE

Le vote électronique offre indéniablement plusieurs avantages qu'il convient d'apprécier pour la simplification ou l'efficacité du processus électoral, mais suscite des inquiétudes légitimes qui touchent notamment à la transparence du processus électoral. Les risques de fraude, de manipulation des résultats, de violation de la sécurité des données électorales sont des défis particulièrement préoccupants. Ces menaces, si elles se réalisent, risquent à terme non seulement d'altérer les résultats des élections, mais également de détruire la confiance des citoyens dans la probité du processus électoral et, par conséquent, de fragiliser la légitimité des gouvernements issus des urnes.
Un des principaux objets d'inquiétude concerne l'absence de visibilité sur le traitement et l'examen des voix. Dans les systèmes de vote classique, les voix sont correctement comptées dans un bureau de vote visible, surveillé et se déroulant dans la bonne proximité de tous les électeurs tandis que le vote électronique a lieu dans un environnement purement numérique, peu ou non transparent tant pour les électeurs que pour les observateurs indépendants, qui ne perçoivent pas toujours clairement, ni ne peuvent contrôler ni vérifier chacune des étapes de l'exécution du processus électoral. Les doutes se nourrissent alors sur la sécurité des systèmes informatiques susceptibles d'être attaqués par un agent extérieur à l'insu de tous afin de falsifier les résultats ou de bloquer, de discrètement de manipuler, le processus électoral, qu'il s'agisse d'éventuelles erreurs de traitement, de validation ou de consultation et bien davantage encore dans un système non transparent. Autre source de tension, s'infiltre-t-on des votes truqués au sein des voix en cours de traitement ou manipule-t-on de façon insidieuse, à l'insu de tous, les données, et si bien, dès lors, qu'elles ne seraient jamais détectées ? Dans une telle situation de dissimulation, la capacité de manipulation en vue d'un succès d'un scrutin falsifié des résultats pourrait avoir pour effet une rupture de la confiance des citoyens envers le système démocratique.

Cela devient d'autant plus préoccupant dans les contextes où des acteurs malveillants, qu'ils soient internes ou externes, s'immiscent dans le processus électoral à des fins politiques, économiques ou géopolitiques. Par ailleurs, le manque de transparence dans le fonctionnement algébrique des systèmes de calcul des votes accroit la méfiance. Si ces systèmes ne font pas l'objet d'explications claires, voire d'audits sur le plan de la vérification indépendante, il devient difficile pour les électeurs de s'assurer que leur vote est correctement considéré et que le processus est juste. Cela produit une atmosphère de méfiance et, in fine, aboutit à une baisse de la participation électorale, en raison du doute que les électeurs auront sur l'utilité de leur vote et la vérité du résultat. Pour garantir la confiance dans le vote électronique, il convient de prévoir des dispositifs de transparence et de sécurité. Les systèmes de vérification indépendants des résultats, la traçabilité dans le vote, le renforcement des protocoles de sécurité constituent de bons moyens de tranquilliser les citoyens. En outre, l'information claire des électeurs sur le fonctionnement du système et les mesures de sécurité est essentielle pour apaiser les craintes et maintenir la légitimité du processus électoral.

4.2 - CONTRIBUTION DE LA BLOCKCHAIN

La technologie blockchain pourrait être une solution pour mieux assurer la transparence, la fiabilité, la sécurisation des applications de vote électronique. Celles-ci disposent notamment de plusieurs aspects utiles : vérification et traçabilité des votes, lutte contre la fraude électorale.

Vérification et traçabilité des votes :

Un des enjeux du vote dématérialisé est de s'assurer que tous les votes exprimés soient bien enregistrés et, dans la mesure où la blockchain est immuable et décentralisée, et que la date de leur émission initiale soit bien respectée. Mais, un vote émis est une transaction et donc visible même après son enregistrement dans la blockchain, assurant la transparence, en cas d'absence de fraude, des électeurs et garantissant la confiance dans le bon fonctionnement du processus électoral, elle assure donc sa crédibilité.

Minimisation des fraudes :

Le système blockchain réduit les fraudes comme les votes multiples puisque chaque vote est indivisible et attaché à l'électeur par des méthodes d'identification fiables ; par ailleurs, une tentative de changement du résultat serait immédiatement décelée puisqu'il faudrait modifier toutes les copies de la blockchain ce qui serait quasiment impossible. De plus, dans ce cadre décentralisé, aucune entité centralisée ne pourrait truquer les résultats.

Sécurisation des données :

C'est grâce à des méthodes cryptographiques très innovantes que la blockchain permet la protection des données personnelles des électeurs. De plus, la décentralisation des données réduit les dangers des cyberattaques permettant une meilleure protection des données personnelles.

Confiance et participation démocratique :

En améliorant sécurité, transparence, traçabilité, la blockchain pourrait renforcer la confiance des citoyens au système électoral. Si les électeurs sont certains que leur vote est sécurisé et impossible à manipuler, cela pourrait susciter une participation renforcée qui augmenterait la légitimité des élections.

À ce titre, la technologie blockchain représente bel et bien un véritable progrès pour les enjeux de fiabilité et de sécurité du vote par Internet. Grâce à ses propriétés de décentralisation, d'immuabilité ou encore de transparence, elle permet d'assurer l'intégrité du vote, de prévenir la fraude et d'assurer la traçabilité des votes. Toutefois, la nécessité de continuer à tester les outils dans des contextes réels afin qu'ils puissent faire l'objet de mises à l'épreuve et d'analyses, pour permettre la détection d'éventuelles faiblesses et évaluer les conditions d'une mise en œuvre efficace à l'échelle nationale.

4.3 - ANONYMAT ET INTÉGRITÉ

La technologie blockchain permet de garantir la sécurité et la transparence du processus électoral au même titre que l'anonymat des électeurs tout comme l'intégrité des votes. En effet, dans les systèmes de vote traditionnels, l'anonymat des votants peut faire obstacle à la vérification, à la sécurité. La blockchain permet de préserver la confidentialité des électeurs tout en préservant l'authenticité du vote.

Confidentialité des électeurs : Contrairement aux systèmes centralisés où la protection des données personnelles des électeurs est compromise, la blockchain permet d'assurer l'anonymat des votants par un login unique attribué à chaque électeur, sous forme de hash alphanumérique, généré à partir de ses données d'identification, ainsi qu'un hash sécurisé et irréversibles , permettant de le représenter par son hash alphanumérique, sans conserver aucune donnée personnelle sur la blockchain. En effet, l'identifiant ne peut plus être mis en relation avec une personne physique, sauf par sa clé privée qui protège la confidentialité des électeurs tout le long de l'opération électorale.

Dissociation du vote et de l'identité de l'électeur :

La technologie blockchain permet de dissocier le vote de l'identité électorale. Dès lors, si on lui remettait un enregistrement du vote, l'individu ne saurait à qui fait référence ce choix de vote. Ce point est essentiel pour la confiance dans le processus électoral.

La sécurité et la transparence :

En plus de son aspect anonyme, la blockchain garantit la sécurité et la fiabilité du vote grâce à l'immuabilité des transactions. Un vote une fois exprimé ne peut être ni substitué ni falsifié. Par ailleurs, la blockchain décentralisée joue un rôle de deuxième niveau de sécurité en écartant les malversations d'un serveur central mal sécurisé

L'équilibre entre confidentialité et transparence :

Avec la blockchain, pourrait-on dire que le couple incognito/transparence est enfin parachevé ? D'une part, le processus électoral est totalement transparent, chaque vote est traçable et pourra être fait être vérifiable au public voire au votant. D'autre part, il préserve le secret de vote et donc la liberté électorale des individus.

De cette manière, la blockchain résout l'énigme difficile (mais pas seulement) de l'urne électronique en rendant paradoxalement possible l'anonymat de l'électeur tout en préservant le secret (démocratique) du vote en recourant à des identifiants cryptographiques (qu'il est ici possible d'assurer de façon sécurisée et transparente). C'est l'une des avancées notables de la mise à jour des systèmes électoraux aux fins de rassurer les citoyens sur la démocratie et le processus électoral.

4.4 AUTHENTIFICATION SÉCURISÉE

La sécurité de l'authentification est un prérequis indispensable à la pérennité et à l'authenticité des élections électroniques. On ne doit permettre à voter que les citoyens dûment autorisés en dotant le système de moyens d'identification et de vérification des électeurs. Sans la mise en œuvre d'une identification appropriée, les dispositifs de vote électronique sont exposés à des menaces telles que le vol d'identité et l'usurpation de vote, qui précisent la validité des résultats.

Les technologies modernes de l'authentification :

Les technologies modernes présentent différentes solutions techniques pour assurer une bonne authentification des électeurs. Les systèmes biométriques et les clés de cryptage se révèlent les plus appropriés aux impératifs de sécurité des élections électroniques.

En matière d'authentification biologique, celle-ci repose sur des caractéristiques physiques, elles-mêmes originales et uniques, que n'ont pas d'autres individus ; de ce fait, on peut recourir à l'empreinte digitale, à la reconnaissance faciale, à l'iris, à la voix… Ces caractéristiques sont impossibles à reproduire, et pour cette raison, cette méthode d'identification n'est pas du tout problématique. Pour s'identifier lors de la connexion au vote, l'électeur pourra ainsi être invité à fournir l'une de ces données, respectivement comparées à celles mises dans la base de données sécurisée, pour valider son identité en un rien de temps et de manière fiable. L'un des atouts majeurs de la biométrie est de ne pas s'appuyer sur un couple mot de passe / identifiant, ce qui pose un problème en cas d'oubli ou de transfert de données.

Les clés cryptographiques constituent un autre puissant moyen d'authentification des électeurs. Ce système repose sur l'utilisation de clés publiques et privées, chaque électeur se voit attribuer, de manière unique, l'une des paires de clés. Au moment d'inscrire l'électeur, ce dernier reçoit une clé privée sécurisée, qui lui permettra d'entrer dans le système et de voter de façon anonyme tout en étant vérifiable. La clé publique s'utilise sans identifier l'électeur. Ainsi, la sécurité est renforcée contre toute fraude car même si les données étaient interceptées par un attaquant, il ne pourrait les modifier sans la clé privée correspondante.

Prévention du risque de fraude et d'usurpation

Avec la biométrie, ou les clés cryptographiques, le risque de fraude, comme le vol d'identité ou usurpation du vote est plus faible. En effet, dans un système traditionnel, un individu malveillant pouvait usurper l'identité d'un autre, mais à l'aide de la biométrie, et de la cryptographie, chaque électeur est authentifié de façon unique et fiable, rendant ces fraudes quasiment impossibles ; ces moyens technologiques permettent également d'éviter les votes multiples. En effet, dès l'instant où l'identité a été validée, le système empêche toute autre tentative de vote.

Préservation de la vie privée et protection des informations personnelles des électeurs

Un des principaux défis de l'identification sécurisée à l'électorat lors de l'élection électronique est de garantir que les informations personnelles des électeurs soient préservées. Les systèmes de biométrie et de cryptographie, une fois correctement mis en œuvre, répondent à cette exigence puisqu'ils préservent la confidentialité des données sensibles (empreintes digitales, photos faciales, etc.). La cryptographie permet de traiter les données de façon que même les administrateurs du système ne soient pas informés du contenu du vote ou de l'identité des électeurs. L'authentification sécurisée constitue donc un des objectifs fondamentaux, sur lequel repose la sécurité du vote électronique et garantir son intégrité. Grâce à la biométrie et aux clés cryptographiques, il est possible d'authentifier les électeurs tout en préservant leur confidentialité, de réduire le risque de fraude et d'atteinte aux personnes, de vol d'identité et d'usurpation. Ainsi, seul l'électeur disposant d'une ou plusieurs clés - ou utilisant un élément de biométrie en possession de l'électeur, de son vivant - pourra se faire enregistrer. Ces dispositifs sont devenus des outils indispensables à la préservation de la confiance des citoyens dans le déroulement de l'élection électronique et des résultats qui en découlent.

4.5 - CAS CONCRETS

Un certain nombre de pays ont déjà exploré ou mis en œuvre des systèmes électoraux reposant sur un vote issu d'un mécanisme de vote basé sur la blockchain.
Estonie : pays innovant sur le plan numérique, l'Estonie a donc mis en œuvre des solutions blockchain pour assurer la sécurité mais aussi la transparence de son système de vote électronique.

En Suisse, plusieurs cantons ont émergé en test à l'urne de vote électronique avec un processus reposant sur la blockchain pour obtenir, d'une part, l'assurance de la confidentialité mais aussi, d'autre part, celle de l'intégrité des résultats. En Russie, à l'occasion de quelques élections locales, la blockchain a été mise en œuvre dans le cadre de l'enregistrement des votes effectués par voie électronique avec une transparence promise mais, il faut le dire, pas encore totalement vérifiée.

Etats-Unis : dans certains de leurs états, aux USA, des expérimentations ont été faites sur l'éventuel usage de la blockchain pour les élections locales et pour les votes des citoyens en situation d'éloignement (notamment des militaires sur zone).
Ces expériences reconnaissent le potentiel élevé que les technologies blockchain permettent d'offrir pour améliorer la mise en place du vote électronique dans un futur proche mais de nombreux défis techniques, éthiques et juridiques devront préalablement être résolus avant d'affirmer atteindre une généralisation.

V. L'IMPACT DE LA BLOCKCHAIN SUR LA TRAÇABILITÉ ALIMENTAIRE

À l'heure actuelle, dans le secteur de l'agroalimentaire, la traçabilité alimentaire est devenue un enjeu de taille pour le consommateur en quête de sécurité alimentaire. Il demande donc à la fois qualité, traçabilité et origine des produits, mais aussi l'engagement des distributeurs. Les crises alimentaires émaillent l'actualité, tout comme la mondialisation des circuits de distribution, constituent des attachements au client. La blockchain, atout technologique misant sur un registre unique, distribué et non modifiable, permet de garantir la traçabilité des aliments et de l'information fournis par l'ensemble des acteurs de la chaîne des approvisionnements, du producteur au consommateur.

5.1 - LES ENJEUX DE LA TRAÇABILITÉ ALIMENTAIRE

Un besoin croissant de transparence

Diverses crises sanitaires et scandales alimentaires ont miné la confiance des consommateurs envers l'alimentation. Aujourd'hui les consommateurs ont besoin d'être rassurés et de disposer d'éléments d'information fiables au sujet de :
La provenance des ingrédients
Les conditions de production et de transformation
L'empreinte écologique du produit
Le manque de transparence peut déboucher sur une méfiance généralisée qui va nuire aux marques/distributeurs. En responsabilisant la traçabilité des produits, les consommateurs peuvent être rassurés et les producteurs peuvent en bénéficier par une valorisation de leurs démarches responsables.

Des défis logistiques et technologiques

Assurer une traçabilité exhaustive des produits d'alimentation s'avère un défi d'ampleur, car il faut tenir compte de multiples acteurs comme les agriculteurs, les transporteurs, les transformateurs, les distributeurs, etc. Tout intervenant doit pouvoir renseigner, communiquer, des informations précises dans les formats adéquats de façon sûre. En revanche, il est fréquent que les systèmes de suivi soient bâtis sur une base de données centralisée exposée aux erreurs, fraudes et manipulations de toute sorte. Des règlements et normes qui varient d'un pays à l'autre n'aident pas non plus à l'unification des pratiques de traçabilité. Un système solide et accessible à tous les acteurs devient donc indispensable.

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

La blockchain se spécifie comme une technique de conservation et de transmission de l'information sous forme de blocs sécurisés et chaînés chronologiquement. Elle repose sur trois principes fondamentaux :

Décentralisation : les informations ne sont pas centralisées sur un serveur, mais sont dispersées entre plusieurs acteurs, ce qui leur garantit une sécurité.

Immutabilité c'est-à-dire que les données sont authentifiées à la date et de leur inscription dans la blockchain. Les données inscrites ne peuvent être altérées ou détruites, ce qui empêche toute possibilité de falsification.

Transparence parce que les différents acteurs de la chaîne peuvent consulter les données inscrites dans la blockchain, ce qui renforce la relation de confiance nécessaire à la coopération entre les acteurs de la chaîne.

Les bénéfices présentés par la blockchain dans le secteur agroalimentaire

Les atouts notables de la blockchain pour le secteur agroalimentaire se déclinent comme suit :

Une meilleure confiance des données : Chaque transaction et chaque information sont sécurisées pour en garantir l'inaltérabilité.

Une traçabilité renforcée sur les produits : On peut suivre, en temps réel, l'ensemble du cycle de vie d'un produit, depuis la ferme jusqu'au rayon d'un supermarché

Le gain de confiance des consommateurs : En scannant un QR code ou en utilisant une application, les consommateurs peuvent disposer, en temps réel, de données concernant le produit (provenance, date de récolte, méthode de production, certifications, etc.).

Dans le cadre de la gestion des rappels de produits : En cas de contamination ou problème sanitaire, le repérage immédiat des lots améliore les réponses appropriées et donc les risques pour la santé publique.

5.3 - DES INITIATIVES MISES EN PLACE PAR LES GRANDES ENTREPRISES

Au sein d'une sélection privilégiée de grands acteurs du secteur agro-alimentaire, certains ont commencé à mettre en place la blockchain en vue d'améliorer la traçabilité de certains produits :

Carrefour : le groupe a intégré la blockchain au sein de leur groupe de grande distribution pour garantir la traçabilité de certains produits (poulet, lait, tomates, etc.). En scannant un QR code sur l'emballage, le consommateur peut connaître les modalités de l'acheminement du produit. **[Voir annexe 3]**

IBM Food Trust : Ce réseau basé sur la blockchain permet aux distributeurs et producteurs une gestion en temps réel des flux alimentaires pour une optimisation logistique.

Il ne s'agit là que d'une avancée technologique et ne répond pas seulement à des enjeux de transparence, de sécurité alimentaire.

5.4 - IMPACTS ET BÉNÉFICES POUR LES CONSOMMATEURS

L'intégration de la blockchain au monde agro-alimentaire peut s'avérer bénéfique à court terme pour les consommateurs concernés :

- **Une information lisible et accessible** : Lucrativement armé, chacun peut en un clic garantir l'authenticité et la qualité des produits qu'il consomme.

- **Une mise en avant des producteurs respectueux** : Les producteurs garantissant un certain respect des normes environnementales et éthiques peuvent communiquer sur leur engagement.
- **Une sécurité sanitaire** : Dans le cadre d'une crise sanitaire, cela permettrait de retracer l'itinéraire des produits et identifier rapidement les produits contaminés afin d'en limiter la distribution.

La blockchain constitue une avancée dans le domaine qu'est la traçabilité alimentaire, son adoption croissante par les industriels, et de distributeurs en témoigne, elle répond à une attente des consommateurs pour davantage de transparence et de sécurité.
En ramenant une visibilité complète sur le parcours des produits, cette technologie pourrait permettre de restaurer la confiance entre les acteurs devant.

retourner vers la consommation de produits, nourrir la « confiance » des acteurs au sein de sa chaîne logistique alimentaire, etc. Le développement durable pourrait par la suite connaître un effet d'entraînement s'engageant dans la voie du culte de la transparence, ou de la confiance considérée à terme comme nécessaire à la consommation, lorsqu 'existerait un pas de tombe fait dans la dignité humaine.

CONCLUSION

A travers ce projet, nous avons exploré les multiples facettes de la blockchain, cette technologie novatrice qui promet transparence, sécurité et décentralisation dans divers secteurs. Nous avons d'abord retracé son histoire, née de la volonté de sécuriser les échanges numériques dès les années 1980, jusqu'à son application concrète avec le Bitcoin en 2008. Cette genèse met en lumière les fondements cryptographiques et les ambitions de rupture avec les systèmes centralisés traditionnels.

Dans le domaine des **finances**, la blockchain bouleverse les modèles établis en offrant une alternative décentralisée aux monnaies FIAT. Elle permet non seulement de sécuriser les transactions grâce à des mécanismes comme le *Proof of Work*, mais elle ouvre aussi la voie à de nouveaux modèles économiques avec les *smart contracts* et la *tokenisation des actifs*. Malgré ses promesses, des défis tels que la concentration de la richesse ou la volatilité des cryptomonnaies demeurent.

En matière de **vote électronique**, la blockchain apparaît comme une réponse crédible aux enjeux de transparence, de sécurité et d'intégrité du processus démocratique. Grâce à l'immuabilité de ses registres, la traçabilité des votes et l'anonymat des électeurs sont garantis, renforçant ainsi la confiance des citoyens. Cependant, la mise en œuvre à grande échelle nécessite encore des tests rigoureux, notamment sur les plans juridique, technique et éthique.

Enfin, dans le secteur de la **traçabilité alimentaire**, la blockchain répond aux attentes croissantes des consommateurs en matière de transparence, de qualité et de sécurité. En permettant de suivre un produit depuis sa production jusqu'à sa consommation finale, elle valorise les démarches responsables des producteurs et redonne confiance au consommateur, tout en facilitant la gestion des crises sanitaires.

En somme, la blockchain ne se limite pas à un simple effet de mode technologique. Elle représente une révolution structurelle qui, si elle est encadrée et utilisée à bon escient, pourrait transformer en profondeur notre manière d’échanger, de votre et de consommer. Son développement futur dépendra de la capacité des sociétés à concilier innovation technologique, cadre réglementaire et inclusion sociale.

Nous remercions l'école Sup de Vinci de Paris de nous avoir attribué ce sujet. Travailler dessus nous a permis d’en apprendre beaucoup sur les technologies de la blockchain, de son impact aujourd’hui et avenir.

QUI A FAIT QUOI ?

- **ARJOCA Adrian**
  - Style global et page de garde
  - Introduction
  - Glossaire
  - Chapitre III (finances)
- **VAN KERCKVOORDE Clément**
  - Chapitre IV (démocratie / vote électronique)
  - Chapitre V (traçabilité alimentaire)
  - Conclusion
- **Ensemble**
  - Sommaire
  - Références
  - Annexes

BIBLIOGRAPGIE

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 sujets 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 électronique
https://www.netservice.eu/fr/produits-et-solutions/b-voting

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

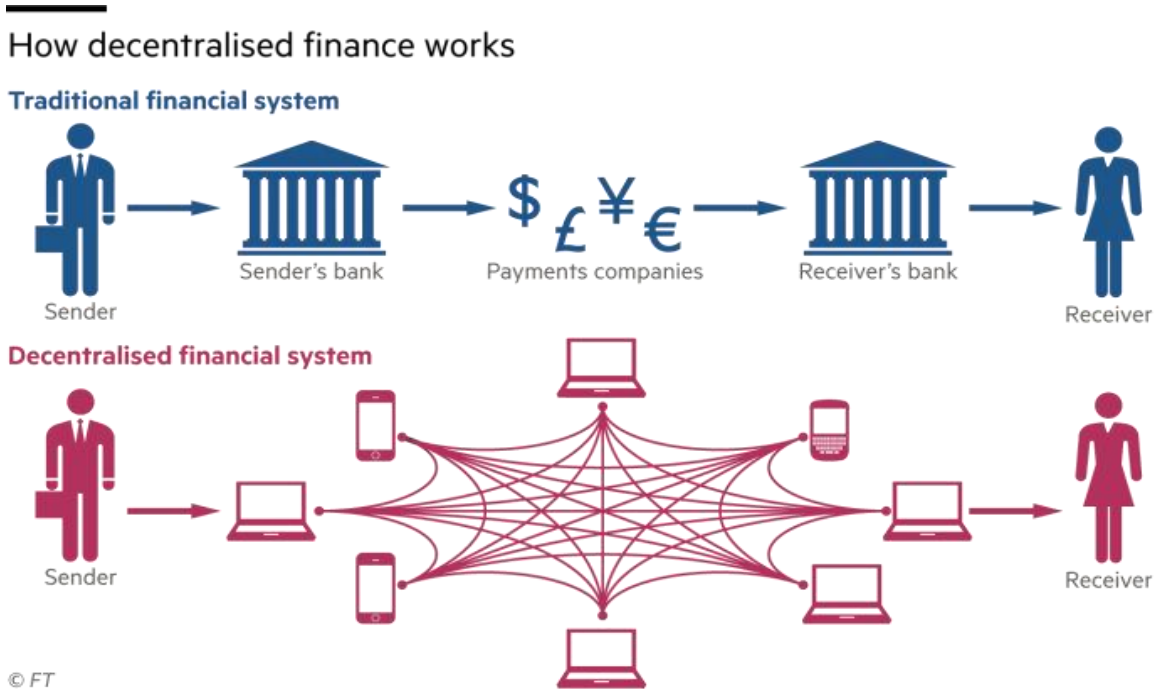
Cas d’usage de la blockchain dans des entreprise de l’agroalimentaire
https://www.alcimed.com/fr/insights/5-cas-usage-cryptomonnaies-agroalimentaire/

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

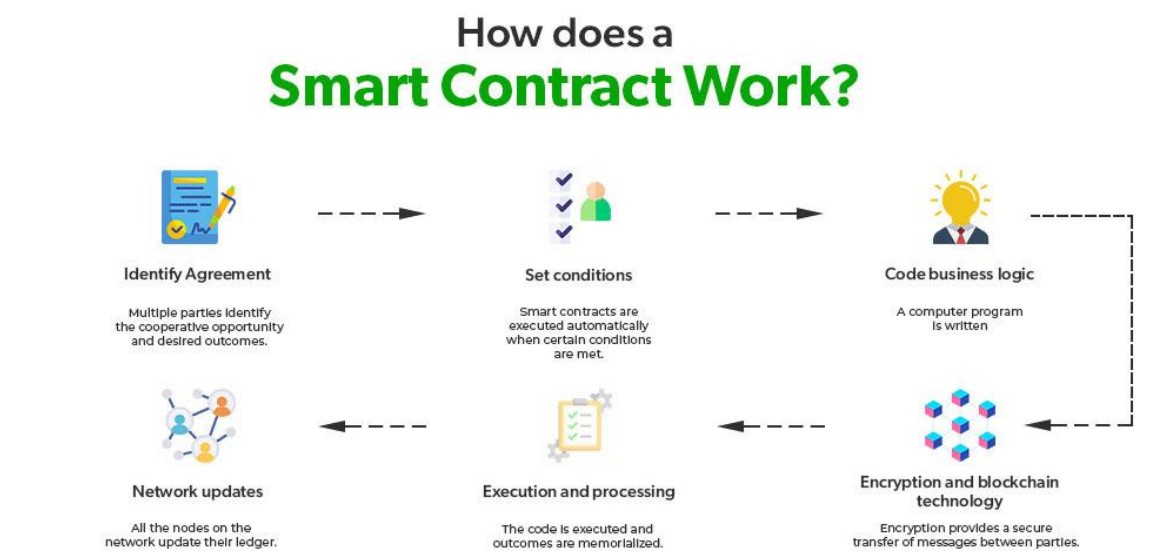
ANNEXES

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



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

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

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