Projet M1
Année scolaire 2020/2021

Institut Supérieur de l'Électronique et du Numérique
Tél. : +33 (0)2.98.03.84.00
Fax : +33 (0)2.98.03.84.10
20, rue Cuirassé Bretagne
CS 42807 - 29228 BREST Cedex 2 - FRANCE

Création d'une application utilisant une blockchain « Safe On Chain »

Proposé par : Marc Lacourt

Thématique : Cybersécurité et réseaux

Jérémy Beaugeard — Domaine professionnel : Cybersécurité et réseaux
Quentin Sauvêtre — Domaine professionnel : Cybersécurité et réseaux

Remerciements

Nous tenons à remercier Monsieur Marc Lacourt professeur référant du projet. Sa disponibilité et sa franchise nous ont permis d'avancer efficacement et sereinement tout au long de ce travail de fin d'année. De plus, bien que le projet se soit déroulé exclusivement à distance, Monsieur Lacourt a su, répondre à tous nos problèmes, donner une solution adéquate dans les plus brefs délais établissant ainsi une relation de confiance et facilitant la communication entre nous. Nous tenons également à remercier Monsieur Montero pour l'aide apportée dans la compréhension de certains concepts et pour avoir partagé son expérience sur la blockchain.

TABLE DES MATIERES

Table des figures

Glossaire

Jeton : est une dénomination d'une crypto-monnaie, il représente un actif qui réside sur sa propre blockchain et permet à son détenteur de l'utiliser à des fins d'investissements ou économiques.

NFT : est un jeton non fongible qui certifie qu'un actif numérique est unique et donc non interchangeable. Les NFT peuvent être utilisés pour représenter des éléments tels que des photos, des vidéos, de l'audio et d'autres types de fichiers numériques.

Metadata : sont des données supplémentaires qui définissent un NFT tels qu'une image, un nom, une description ou des propriétés

MD5 / SHA1 / SHA-256 : algorithmes de chiffrement

Hash : est la sortie d'un algorithme de hachage tel que SHA-256

KYC : Know Your Customer, est une procédure qui s'inscrit dans le cadre de la politique de lutte contre le blanchiment d'argent

Bloc genesis : est le premier bloc d'une transaction sur une blockchain

Modèle OSI : Open Systems Interconnection, est une norme de communication en réseau de tous les systèmes informatiques.

CAPTCHA : est une test défi-réponse utilisé en informatique pour déterminer si l'utilisateur est humain ou non

DeFi : est l'acronyme de finance décentralisée

LVMH : est l'acronyme du groupe français Moët Hennessy Louis Vuitton

IBM : est l'acronyme de International Business Machines qui est une entreprise américaine

Introduction

Ce projet est divisé en trois grands axes. Pour commencer, faire un tour d'horizon des blockchains, de comprendre leurs conceptions et leurs différentes utilisations. Ensuite, présenter de manière précise et technique le fonctionnement de la blockchain. Enfin, le troisième axe consiste à rechercher et concevoir une application utilisant une blockchain. Ce rapport commencera donc par expliquer ce qu'est une blockchain et décrira son fonctionnement. Dans un second temps, le rapport traitera du cahier des charges, de la gestion de projet et des solutions techniques utilisés pour créer l'application « Safe On Chain ».

Le concept de blockchain est apparu pour la première fois en 2008. La blockchain est une technologie récente, principalement utilisée par les informaticiens et mathématiciens dont l'objectif était de développer une solution alternative au système monétaire actuel.

Comme toutes les technologies majeures elle mettra dix ans avant de se populariser avec l'apparition et la médiatisation de la crypto-monnaie Bitcoin. La blockchain repose sur un argument simple, elle permet de concevoir le stockage d'informations sans avoir besoin d'un tiers de confiance. En effet, avec ce système, la blockchain peut être représentée comme une grande base de données accessible à tous, contrôlée par les utilisateurs et non par une organisation.

Pour rendre possible la création d'une monnaie virtuelle (crypto-monnaie), la blockchain a su résoudre un problème qui avait résisté jusqu'alors aux informaticiens : le transfert de titres de propriété sans l'intervention d'un tiers de confiance. Elle le fait en permettant à un réseau d'ordinateurs de s'accorder sur un livre de compte commun sans qu'aucun des participants n'ait à se faire confiance.

Vue par certains comme une révolution majeure au même titre qu'internet, la blockchain prend de plus en plus d'ampleur dans les industries de recherche technologique avec plus de 4 milliards de dollars investis en 2019. Son utilisation versatile et le faible montant d'investissement à mettre en place pour créer une blockchain permet de laisser place à de nombreux projets ambitieux dans de multiples domaines.

La blockchain suit une politique libérale qui vise à privilégier les libertés individuelles. Si on prend l'exemple des banques, elles représentent en France la gestion des transactions et des comptes, dans le cas d'une monnaie virtuelle basée sur une blockchain la présence des banques devient négligeable. Le même principe est repris pour toutes les utilisations de blockchain rendant obsolète la présence d'organismes intermédiaires entre les clients.

1. Présentation de la blockchain

1.1. Historique

La technologie blockchain n'est pas apparue du jour au lendemain ; elle découle de nombreuses années de recherche sur des concepts sur lesquels se base la blockchain. Les techniques de cryptage et leur informatisation ont fortement inspiré la première création de blockchain.

Le Bitcoin marque l'histoire de la blockchain. Après sa création en 2009 le monde prend connaissance des possibilités qu'offre la blockchain entraînant une multiplication du nombre de projets de monnaies digitales.

L'ère post Bitcoin est dédiée aux programmeurs et entrepreneurs cherchant à élargir l'utilisation de la blockchain dans d'autres domaines que la crypto-monnaie. Dans un monde où la confiance et la sécurisation de l'information sont la base des relations sociales, la blockchain n'a plus qu'à s'installer et remplacer les organismes tiers en qui nous n'avons pas d'autres choix que de leur faire confiance pour le moment.

1.1.1. La cryptologie

La cryptologie est une science clé de la blockchain. Elle se divise en deux parties nettement différenciées. D'une part la cryptographie à clef secrète appelée symétrique ou bien classique et d'autre part la cryptographie à clef publique dite asymétrique ou moderne.

Les premières preuves d'utilisation de la cryptologie remontent au XVIème siècle av. J. -C. Le premier document chiffré retrouvé en Irak datant de cette époque est une tablette, elle a été créée dans le but d'assurer la confidentialité de l'information en utilisant une clé symétrique. La clé symétrique doit être connue des deux partis elle est nécessaire au chiffrement ainsi qu'au déchiffrement du message. Une des premières techniques de chiffrement appelée "chiffre de César".

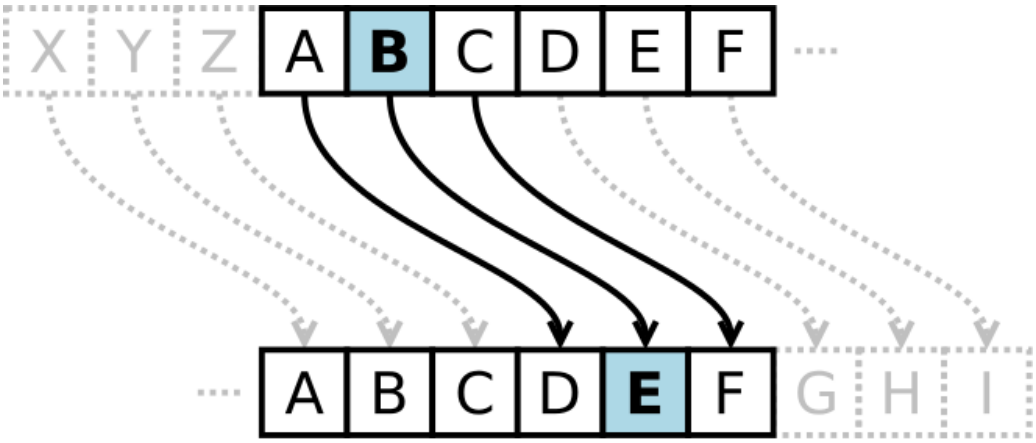


Figure 1 - Fonctionnement du chiffre de César avec la clé 3

Le chiffre de César est une technique simple qui consiste à remplacer chaque lettre d'un texte clair original par une lettre à distance fixe. Sur la figure ci-dessus la lettre B avec une clé 3 donne la lettre E. Mais la cryptographie symétrique nécessite l'échange d'une clé secrète ce qui rend nulle la confidentialité d'un message si celle-ci est interceptée.

A l'opposé de la cryptographie à clé secrète, la cryptographie à clé publique consiste à donner à chacune des parties une clé privée utile pour le déchiffrement du message et une clé publique utilisée pour le chiffrement du message.

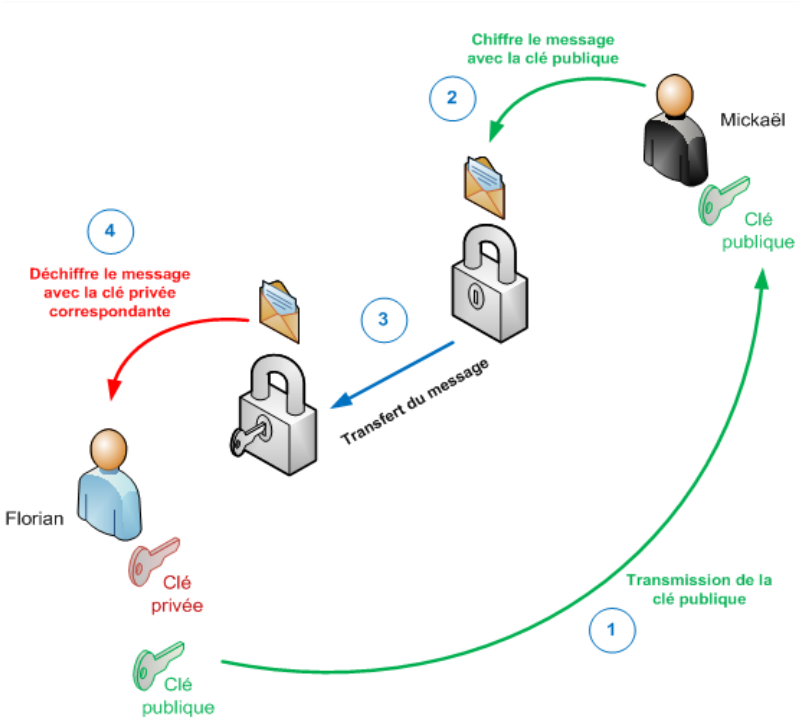


Figure 2 - Fonctionnement de la cryptographie à clé publique

Sur la figure ci-dessus on peut voir que Florian commence par fournir sa clé publique à Mickaël qui l'utilise pour chiffrer le message. Il envoie ensuite ce message à Florian qui sera le seul en capacité de déchiffrer ce message grâce à sa clé privée.

Le chiffrement RSA créé en 1977 est la première utilisation du chiffrement asymétrique. Permettant d'assurer la confidentialité d'une communication entre deux interlocuteurs et d'assurer l'authenticité de l'expéditeur du message, le chiffrement asymétrique est très vite utilisé pour le commerce et l'échange de données.

Avec la méthode du RSA, les clés de chiffrement et de déchiffrement se calculent grâce à un module de chiffrement, un exposant de chiffrement et un exposant de déchiffrement.

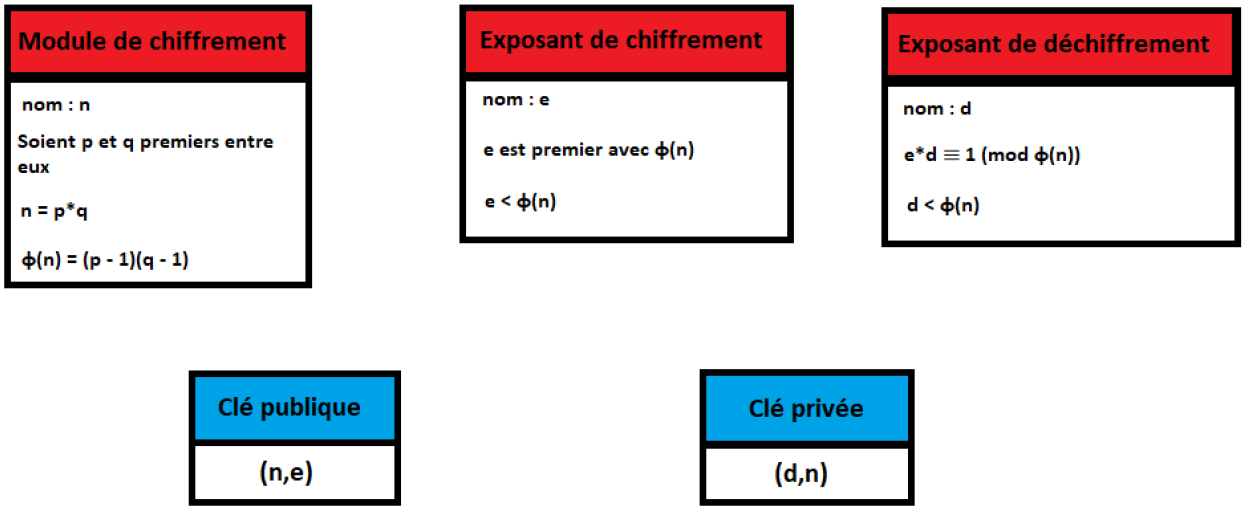


Figure 3 - Chiffrement RSA

Le chiffré du message s'obtient en calculant le module du message exposant e.

$$M^e \equiv C \pmod{n}$$

On déchiffre le message en effectuant l'opération inverse avec l'exposant de déchiffrement d.

$$M \equiv C^d \pmod{n}$$

Pour déchiffrer le message sans avoir l'exposant d il faut réussir à factoriser n pour trouver les valeurs de p et q en sachant qu'ils sont premiers entre eux. Tout l'algorithme RSA est basé sur le fait qu'il est facile de multiplier deux grands nombres premiers mais il est beaucoup plus difficile de trouver leur factorisation. En pratique, la taille du module choisi est de 1024 ou 2048 bits. A ce jour, il n'existe pas de résolution dont la complexité est meilleure que sous-exponentielle. Le plus grand module RSA factorisé est long de 768 bits. Avec l'amélioration de la puissance de calcul des machines, il est préférable de choisir une clé de 2048 bits même si en théorie une clé de 1024 bits reste incassable dans un temps restreint.

1.1.2. Les premières blockchains

En 1983, la première monnaie virtuelle Ecash est créée par David Chaum. Cette monnaie garantit une anonymisation des paiements basée sur un protocole cryptographique appelé la signature à l'aveugle.

C'est en 1991 qu'une première notion de blockchain apparaît avec la mention de confiance distribuée. Les chercheurs Stuart Haber et W. Scott Stornetta présente la possibilité d'horodater un document digital et de le rendre inaltérable. Pour la première fois, il est proposé de lier les données les unes aux autres de manière chronologique pour créer un système où il est impossible de revenir en arrière. Ce concept est une notion fondamentale du concept de blockchain.

Une autre notion fondamentale de la blockchain est la preuve de travail. En 1997 Adam Black propose un système de preuve de travail HashCash qui permet de faire face aux attaques par déni de service. Le principe est de devoir résoudre un problème mathématique demandant de la puissance de calcul et du temps pour pouvoir faire une interaction ce qui empêche de créer massivement des interactions.

Grâce à ces deux concepts, l'immuabilité de données et la preuve de travail, le Bit gold est conçu en 1998 par Nick Szabo. Dans le principe du Bit gold, les participants consacrent la puissance de leur ordinateur à la résolution d'énigmes cryptographiques. Chaque solution est intégrée au problème suivant créant des chaînes de plus en plus longues. Il faut attendre que la solution à l'énigme en cours soit trouvée pour que la prochaine résolution commence. Une faille de sécurité de taille à fait échouer le projet, le problème de double dépense qui permet de dépenser deux fois une somme même si on ne possède pas le montant nécessaire.

Cette approche avec un système monétaire décentralisé a séduit dans les années 90 un groupe de quelques milliers de personnes appelés Cypherpunks. Les membres composant ce groupe sont principalement des mathématiciens, des cryptographes et des informaticiens. Ils suivent une politique libérale visant à privilégier la liberté individuelle et principalement protéger la vie privée sur internet. Pour les Cypherpunks, dans la mesure où on ne peut pas faire confiance à un état central pour respecter, entre autres, la vie privée des citoyens, les garanties ne doivent pas venir des lois mais des logiciels eux-mêmes. C'est dans ce groupe de personnes qu'est diffusé en 2008 par Satoshi Nakamoto le document renseignant la méthode pour utiliser le Bitcoin.

1.1.3. La démocratisation de la blockchain

La monnaie virtuelle Bitcoin inventée par un individu anonyme sous le surnom de Satoshi Nakamoto présente les cinq techniques permettant d'assurer son fonctionnement : les doubles dépenses sont évitées grâce à un réseau pair à pair, aucun organisme n'a la charge d'éditer la monnaie, les participants peuvent être anonymes, les nouvelles unités de

monnaie sont fabriquées à partir de preuves de travail (HashCash), et enfin, la preuve de travail pour la génération de nouvelles pièces alimente aussi le réseau pour éviter les doubles dépenses. En 2013, donc cinq ans après sa création, la valeur du Bitcoin dépasse les 800 dollars et certaines banques ou commerces commencent à autoriser le paiement en Bitcoin. Sa valeur a dépassé les 50 000 dollars en 2021.

La popularisation du Bitcoin marque le début d'une nouvelle ère pour la blockchain. En effet, le Bitcoin démontre par ses propriétés les pleines capacités de la technologie blockchain. Cette technologie a permis de créer pour la première fois une monnaie électronique complètement décentralisée, sans organisation pour la gérer et avec un niveau de sécurité suffisant pour démarrer son utilisation.

Le phénomène Bitcoin a déclenché l'apparition d'une multitude de projets ambitieux utilisant la blockchain. Pour commencer, de nombreuses crypto-monnaies ont vu le jour, toutes pour des utilisations différentes comme le Litecoin qui propose de traiter les transactions en deux minutes contre environ dix minutes pour le Bitcoin ou encore Monero qui empêche les tiers d'accéder aux transactions.

Les inventeurs et programmeurs ont trouvé de nouvelles utilisations à ce système permettant de stocker de manière décentralisée et sécurisée. Il existe un large panel d'applications et pour montrer la versatilité de cette technologie, trois applications bien différentes nous serviront d'exemple.

Pour commencer, dès 2012, la startup "Follow my vote" propose un système de vote enregistré sur une blockchain. Chacun des votes formerait alors un bloc de la chaîne et serait consultable par tous. Aucun vote ne peut être modifié après sa validation. En vue du déroulement des dernières élections présidentielles américaines de 2020, cette nouvelle procédure de vote semble plus adaptée à la situation.

Ensuite le projet Enigma du MIT Media Lab a pour but de créer une blockchain permettant à ses utilisateurs de stocker des données dans un environnement entièrement sécurisé. Les données des utilisateurs seront fractionnées dans plusieurs blocs et seul l'utilisateur à qui appartient la donnée possède la clé rassemblant ces blocs qui regroupent ses données. Le projet Enigma rencontre un problème de taille face à la loi RGPD (règlement général de protection des données) qui stipule que les données des utilisateurs sur internet doivent pouvoir être supprimées si celui-ci le désire. Or la suppression de données va à l'encontre du principe d'utilisation d'une blockchain.

Enfin, l'entreprise SkuChain offre une blockchain permettant de retracer l'origine d'un produit à l'aide d'un QR code. Ainsi on pourrait prendre un produit sur le marché et savoir de manière sûre et non modifiable par les acheteurs/revendeurs la chaîne de production et la provenance du produit.

1.2. Fonctionnement de la blockchain

La blockchain est une technologie permettant de partager une base de données capable de stocker tout type d'informations (texte, pdf, images, etc.) et qui contient l'historique de toutes les transactions effectuées par les utilisateurs, nous pourrions la comparer à un grand livre en comptabilité.

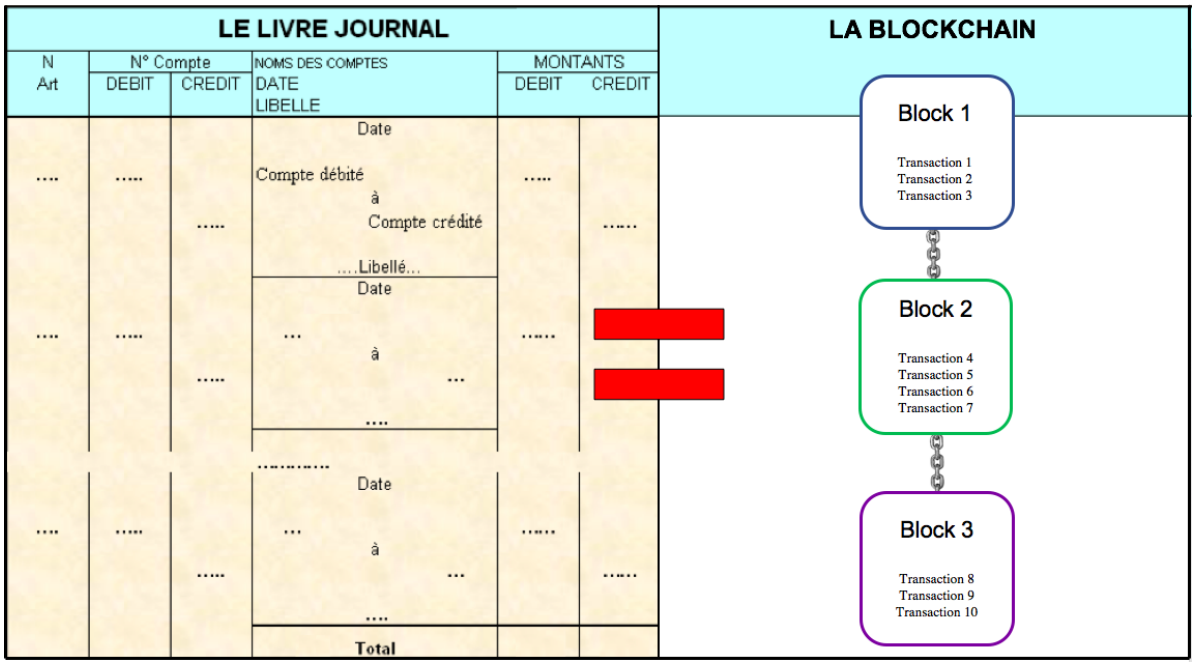


Figure 4 - Comparaison d'un grand livre comptable et de la blockchain

Concrètement comment fonctionne un transfert de crypto-monnaie sur une blockchain ?

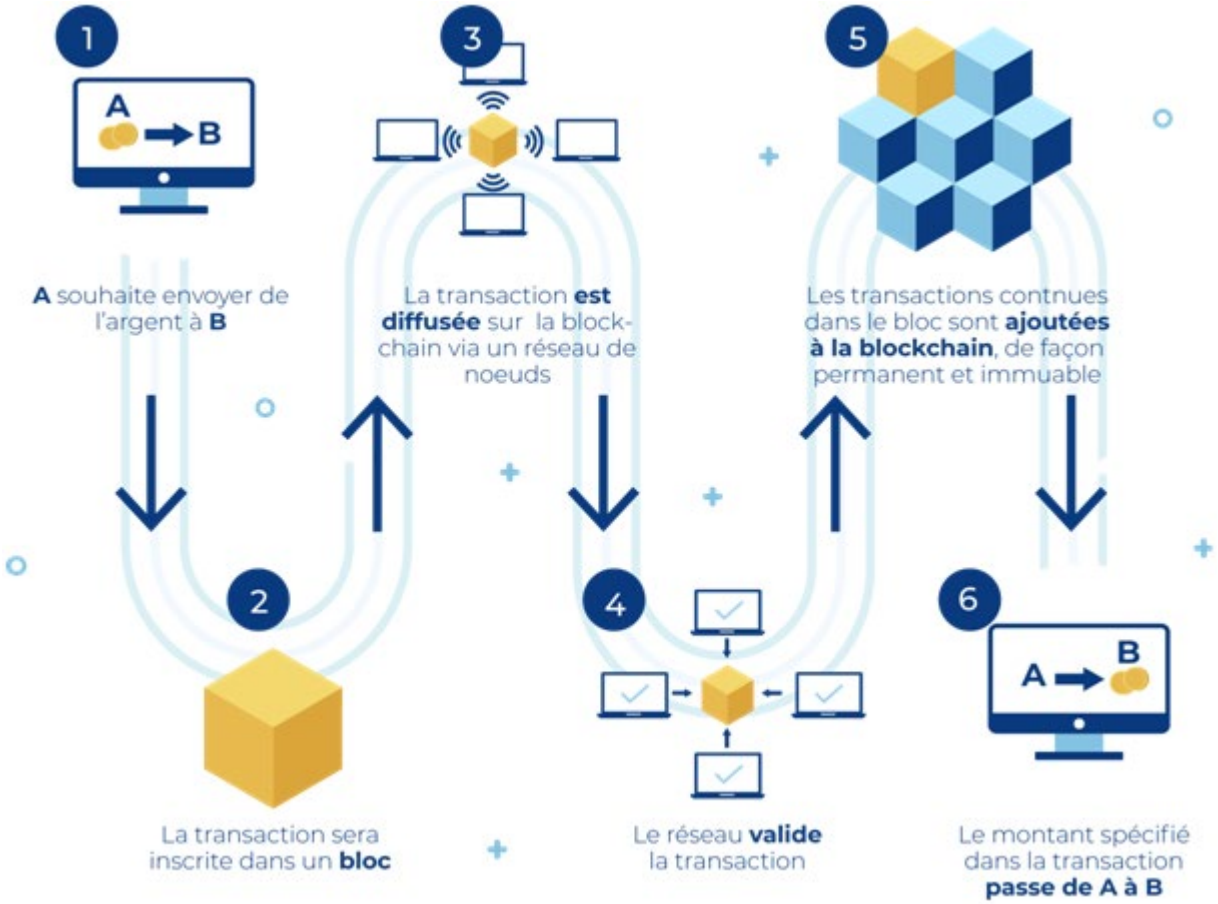


Figure 5 - fonctionnement d'une transaction sur une blockchain

L'aspect révolutionnaire de la blockchain réside dans ses trois principales caractéristiques : immuable, décentralisée et sécurisée. Comme on peut le voir sur la figure ci-dessus, lorsqu'une transaction est proposée, une partie du réseau est sollicitée pour valider cette transaction. La transaction est ensuite ajoutée à la blockchain. L'ajout du bloc est alors copié par tous les détenteurs d'un exemplaire de la blockchain ce qui assure l'immuabilité des données.

1.2.1. Décentralisée

La blockchain permet le partage de ces données de manière décentralisée, c'est-à-dire entre acteurs ne se faisant pas nécessairement confiance et sans entité centrale de contrôle (ex : une banque ou une institution). Comme dans tout système de paiement, il est nécessaire de tenir à jour un registre des comptes pour pouvoir connaître la balance

financière de chaque utilisateur. Dans le système de notre société actuelle, ce sont les banques qui tiennent ce registre.

Le principe fondamental de la blockchain est relativement simple : au lieu que le registre soit maintenu par un seul organisme privé, il l'est de manière décentralisée. En clair, chaque ordinateur (appelé nœud) du réseau contient une copie du registre et aide à le maintenir à jour, cette architecture est appelée pair à pair(P2P). Le registre est protégé par cette décentralisation.

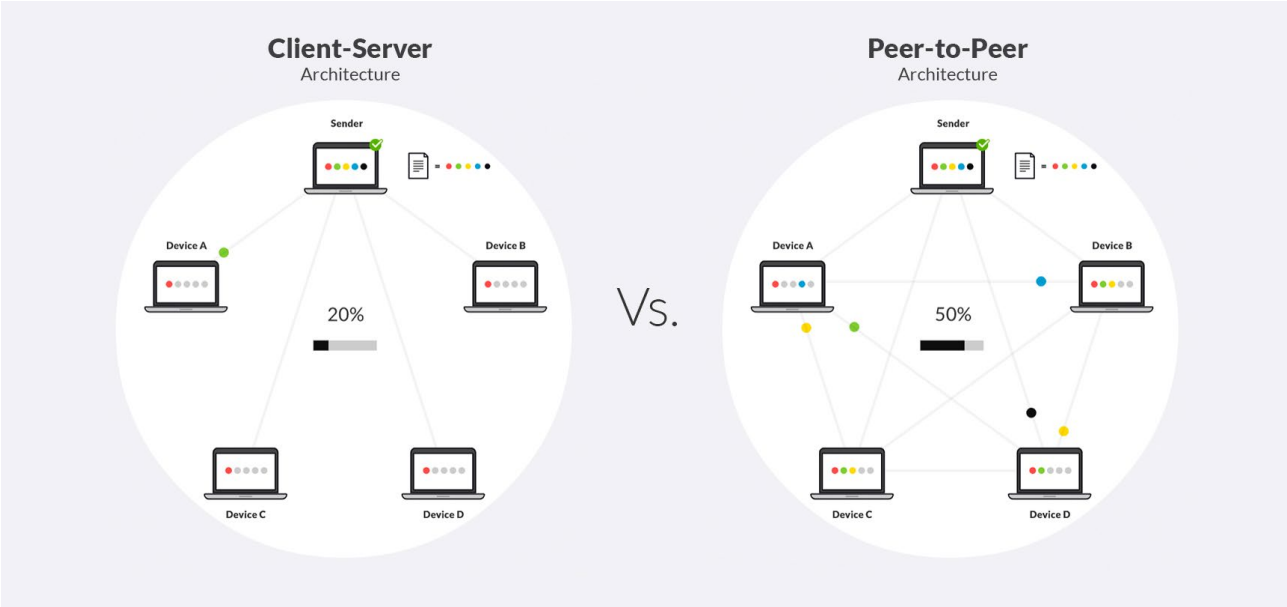


Figure 6 - Différence entre une architecture client-serveur et pair et à pair

D'après le site web https://bitnodes.io il y aurait 10457 nœuds participant à la décentralisation de la blockchain Bitcoin (à l'écriture de ce rapport - 15 mars 2021).

1.2.2. Immuable

Les transactions effectuées entre les utilisateurs sont regroupées dans des blocs, d'où le terme de blockchain.

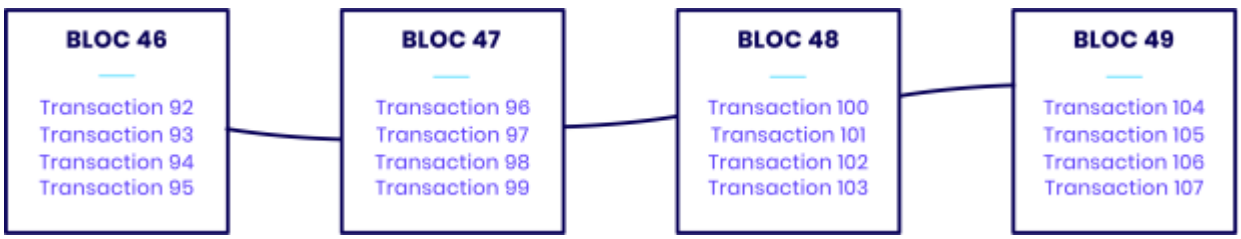


Figure 6 - Représentation d'une chaîne de blocs

Une de ses caractéristiques principales est qu'elle ne peut pas être modifiée. Les blocs sont protégés par plusieurs procédés cryptographiques innovants qui rendent la modification impossible à posteriori car chaque bloc est relié au précédent ; ainsi pour modifier un bloc il faudrait modifier son précédent et ainsi de suite... Après avoir enregistré les transactions récentes, un nouveau bloc est créé et les transactions vont être vérifiées par les validateurs du réseau (généralement appelé mineur). Si le bloc est validé il est horodaté et ajouté à la chaîne de blocs, les transactions seront alors visibles à l'ensemble du réseau.

Si un individu mal intentionné essayait de modifier frauduleusement un bloc précédent il faudrait qu'il modifie l'empreinte de ce dernier, donc recalculer l'empreinte du bloc suivant pour que celui-ci soit valable, ainsi de suite. Ce type d'attaque est quasiment infaisable car le réseau continue de valider les nouveaux blocs donc la liste des empreintes à revérifier serait infinie. Pour la blockchain du Bitcoin où pour retrouver un bloc il faut dix minutes, on vous laisse imaginer le temps nécessaire pour recalculer tous les blocs après avoir falsifié un élément de la chaine.

Pour qu'un mineur puisse modifier la blockchain il faudrait qu'il dispose de plus de la moitié de la puissance de calcul totale ; on appelle ça une attaque des 51%. Ce type d'attaque est pratiquement impossible sur un réseau extrêmement décentralisé et demande une quantité de calcul considérable.

1.2.3. Sécurisée

L'hébergement décentralisé rend la technologie blockchain sûre : elle rend quasiment impossible la suppression de toutes les copies d'un document dupliquées sur une multitude de serveurs à travers le monde. En effet, si un élément de la blockchain est supprimé ou modifié, la modification doit être validée et appliquée par tous les possesseurs de cette blockchain.

Cette architecture rend la blockchain très résistante aux cyber-attaques ou au contrôle d'une organisation comme un État, ainsi cette dernière peut être considérée comme inviolable. Comme exemple concret nous pouvons citer l'affaire WikiLeaks du lanceur d'alerte Julien Assange qui a demandé aux défenseurs de la liberté d'expression de partager leur serveur avec une copie complète des nombreux documents ayant fuité.

1.2.4. Transparente

Nous avons pu voir qu'une fois un document inscrit sur la blockchain il est très facile de prouver son authenticité à un instant T. La blockchain est qualifiée de transparente car tout individu peut la télécharger intégralement et ainsi voir les transactions passées.

Si un bloc est cassé au sein de la chaîne, la cassure est exposée aux yeux de tous ce qui implique que tous les utilisateurs doivent valider cette modification.

1.3. Différents types de blockchain

1.3.1. Les blockchains publiques

Dans une blockchain publique tout le monde peut interagir et voir les transactions effectuées. Il n'y a également aucune permission, quiconque peut décider de devenir validateur et de se soumettre au mécanisme de consensus que nous expliquerons plus tard.

La blockchain publique la plus connue est évidemment la blockchain Bitcoin, ensuite nous pouvons citer Ethereum ou Avalanche.

Nous pouvons citer le cas du groupe LVMH qui travaille sur un projet de blockchain pour sécuriser la provenance de ses articles par exemple en identifiant le parcours complet d'un sac à un main.

1.3.2. Les blockchains privées

Dans une blockchain privée les validateurs sont sélectionnés et soumis à des régulations, de plus la lecture et/ou l'écriture du registre peuvent être restreintes ; ce ne sont pas des systèmes décentralisés. Les chaînes privées sont mieux adaptées aux environnements d'entreprise, où une organisation souhaite profiter des propriétés de la blockchain sans rendre son réseau accessible de l'extérieur, les cas d'usage peuvent être de la traçabilité dans la chaîne logistique.

En 2018 Carrefour a annoncé avoir rejoint la « blockchain alimentaire » de l'américain IBM afin de garantir à terme la traçabilité de ses produits. Cette blockchain, IBM Food Trust, repose sur la technologie HyperLedger qui permet aux entreprises de créer des blockchains privées.

1.3.3. Les blockchains consortiums

La blockchain du consortium se situe entre les blockchain publiques et privées, combinant des éléments des deux. La différence la plus notable entre les deux systèmes peut être observée au niveau du consensus. Au lieu d'un système ouvert où tout le monde peut valider des blocs ou d'un système fermé où une seule entité nomme les validateurs, une blockchain de consortium voit une poignée de parties tout aussi puissantes fonctionner comme validateurs.

A partir de là, les règles du système sont flexibles : la visibilité de la chaîne peut être limitée aux validateurs, visible par les personnes autorisées, ou par tous. À condition que les validateurs parviennent à un consensus, les changements peuvent être facilement mis en œuvre. Quant au fonctionnement de la blockchain, si un certain seuil de ces parties se comporte honnêtement le système ne rencontrera aucun problème.

Une blockchain de consortium serait plus avantageuse dans un contexte où plusieurs organisations opèrent dans le même secteur et nécessitent un terrain d'entente sur lequel effectuer des transactions ou relayer des informations. Rejoindre un consortium de ce type pourrait être bénéfique pour une organisation, car cela lui permettrait de partager des informations sur son secteur avec d'autres acteurs.

Récapitulatif :

	Publique	**Privée**	**Consortium**
Sans permission	oui	non	non
Droit de lecture	tout le monde	certains individus sélectionnés	ça dépend
Droit d'écriture	tout le monde	participants approuvés	participants approuvés
Possession	personne	une entité	plusieurs entités
Participants connus	non	oui	oui

2. Description technique de la blockchain

2.1. Fonctions de hachage

2.1.1. Principes de fonctionnement

Dans une blockchain, l'identité de chaque bloc est déterminée par des codes de hachage. Ces codes sont générés par des algorithmes de hachage, les plus connus étant le MD5 et le SHA1 (Secure Hash Algorithm 1). Ces codes de hachage sont utilisés pour sécuriser les mots de passe, les navigateurs internet, les certificats SSL, etc…

Une fonction de hachage cryptographique est une fonction qui, lorsqu'on lui donne une valeur en entrée, donne une empreinte de hachage aussi appelée signature. Cette empreinte est de taille fixe, la taille dépend de l'algorithme choisi.

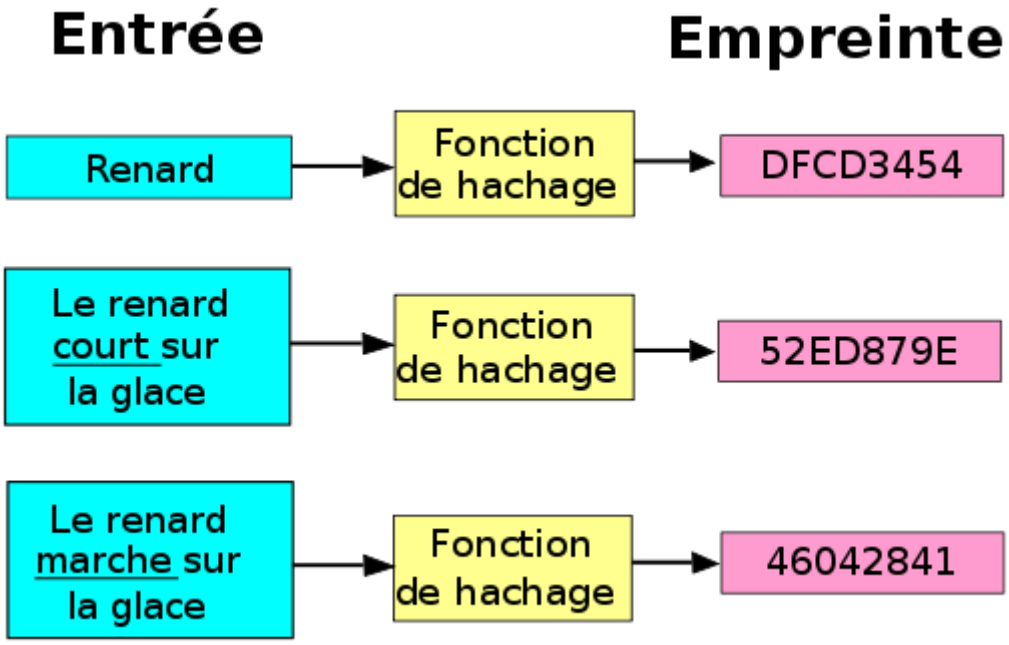


Figure 7 - Principe d'une fonction de hachage

Les fonctions de hachage vont d'abord ajouter des éléments à l'entrée de sorte que sa taille soit un multiple d'un nombre qui dépend de l'algorithme utilisé. La fonction va ensuite découper la donnée mise en entrée pour mélanger et modifier les morceaux de données en suivant des règles propres à chaque fonction de hachage pour enfin donner en sortie une empreinte de taille fixe. Généralement, le temps de traitement nécessaire pour obtenir une empreinte est de l'ordre de la milliseconde.

2.1.2. Propriétés d'une fonction de hachage

Les fonctions de hachage sont conçues pour être cryptographiques, uniformes, non inversibles et déterministes.

Pour commencer, une fonction est dite cryptographique s'il n'est pas possible de prédire l'empreinte générée. Si on utilise la fonction de hachage sur deux entrées très similaires, les empreintes ne doivent avoir aucun lien, aucune ressemblance entre elles. Sur la figure ci-dessus, l'empreinte de "Renard" est "DFCD3454", si je passe dans la fonction la valeur "Renar", l'empreinte pourrait être "85HJ2148".

Ensuite, une bonne fonction de hachage doit répartir équitablement les empreintes pour les éléments en entrée. Autrement dit, si la taille d'empreinte de l'algorithme est de quatre bits, alors l'empreinte pourra prendre 2^4 valeurs différentes soit seize valeurs différentes. Pour que cette fonction devienne uniforme, chacune des empreintes doit coder un élément sur seize. On appelle cela l'uniformité de la distribution.

La fonction doit également être non-inversible. Il doit être impossible de retrouver la valeur d'entrée si on possède la valeur de sortie.

Enfin, les fonctions de hachage doivent être déterministes. Pour une entrée identique, l'empreinte obtenue doit être la même. Dans notre cas, si je donne en entrée de ma fonction "Renard" dix fois sur des machines différentes à des heures différentes, l'empreinte obtenue devra toujours être "DFCD3454".

2.1.3. Le hachage dans une blockchain

Les blockchains utilisent les fonctions de hachage de différentes manières, on présentera ici les configurations les plus utilisées.

La taille fixe des empreintes en sortie de l'algorithme est plus grande que dans nos exemples. Pour l'algorithme SHA-256, la taille des empreintes est de 64 caractères hexadécimaux soit 256 bits.

Si on prenait une taille d'empreinte plus petite, deux entrées différentes auraient plus de chances d'avoir la même empreinte. Dans notre exemple précédent, avec une taille d'empreinte de 16 bits, on a obligatoirement au moins deux empreintes identiques si on lance la fonction de hachage avec 17 entrées différentes.

Pour les empreintes de SHA-256 on peut calculer la probabilité de collision de façon intuitive. On a 256 bits donc 2^{256} valeurs différentes possible (1 bits peut valoir 0 ou 1), on peut donc facilement conclure qu'il faut créer $2^{256} + 1$ empreintes pour être sûr d'obtenir une collision soit environ 10^{77} empreintes. En réalité, si on fait le calcul avec la généralisation du paradoxe d'anniversaire, on obtient un résultat inférieur.

$$p(n) = 1 - \frac{N!}{(N-n)!} \cdot \frac{1}{N^n}.$$

L'ordre de grandeur de la probabilité d'obtenir deux empreintes identiques reste extrêmement grand. A titre de comparaison, la probabilité de gagner dix fois d'affilée au loto est d'environ 10^{-60}.

Une blockchain est une suite de blocs chaînés. Un bloc est composé de trois éléments, son adresse, la donnée et l'adresse du bloc suivant.

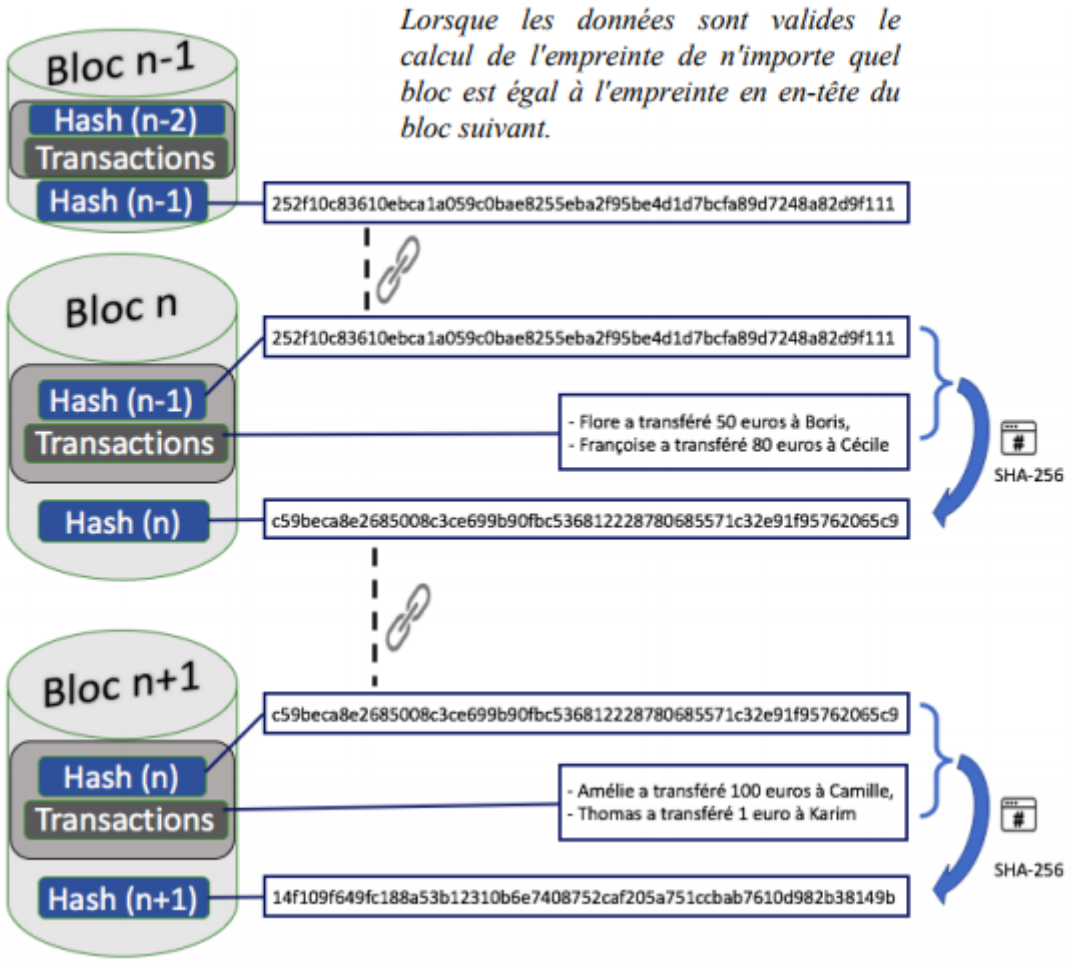


Figure 8 - Structure des blocs et formation de leurs adresses

Les adresses du bloc actuel et du bloc suivant sont des empreintes générées par une fonction de hachage (ici SHA-256). On utilise la combinaison de l'adresse du dernier bloc de la chaîne et de son contenu pour obtenir l'empreinte de l'adresse du nouveau bloc. Par conséquent, modifier un seul caractère dans les données contenues par le bloc va entièrement changer son empreinte. De plus, changer l'empreinte d'un bloc de la chaîne modifiera l'adresse du bloc suivant et ainsi de suite.

En conclusion, si un individu souhaite changer le contenu d'un bloc, il doit impérativement recréer l'intégralité de la blockchain et la faire valider par la majorité des possesseurs de celle-ci. On peut donc considérer, pour une blockchain publique, qu'il est impossible de modifier une blockchain.

2.2. Algorithmes et protocoles de consensus

Les algorithmes et les protocoles de consensus sont deux étapes très importantes et entièrement différentes qui permettent à un système décentralisé d'être viable. L'algorithme consiste à décider quel nœud doit générer le bloc suivant, et le protocole se concentre sur l'acceptation ou non d'un nouveau bloc dans la blockchain.

2.2.1. Algorithmes de consensus

Les blockchains, pour une très large majorité, sont conçues pour être décentralisées. Cependant comment un réseau distribué peut-il se mettre d'accord sur une décision, si certains des nœuds sont susceptibles de tomber en panne ou d'agir de manière malhonnête ? Il s'agit de la question fondamentale du problème dit des généraux byzantins, qui a donné naissance au concept de tolérance aux pannes byzantines.

Imaginons qu'un général représente un nœud d'une blockchain. Le problème des généraux byzantins fait référence à une situation de siège d'une cité entourée de groupes de soldats. Chacun des groupes est dirigé par un général. Le général doit faire circuler l'information si l'attaque doit avoir lieu ou non, le but étant de faire attaquer tous les soldats simultanément pour mener à bien l'attaque. Seulement, certains généraux sont des traîtres, il faut donc élaborer une méthode assurant la victoire à l'empire byzantin.

Les généraux communiquent par le biais de messagers, impliquant le fait que les messages peuvent être détruits ou retardés. De plus, un général (ou plusieurs) peut décider d'envoyer un message frauduleux. Par conséquent, la seule manière de parvenir à un consensus est d'avoir au moins ⅔ des généraux fiables et honnêtes ; si la majorité décide d'agir de manière frauduleuse le réseau n'est plus fiable et sujet aux attaques (comme l'attaque dite des 51%).

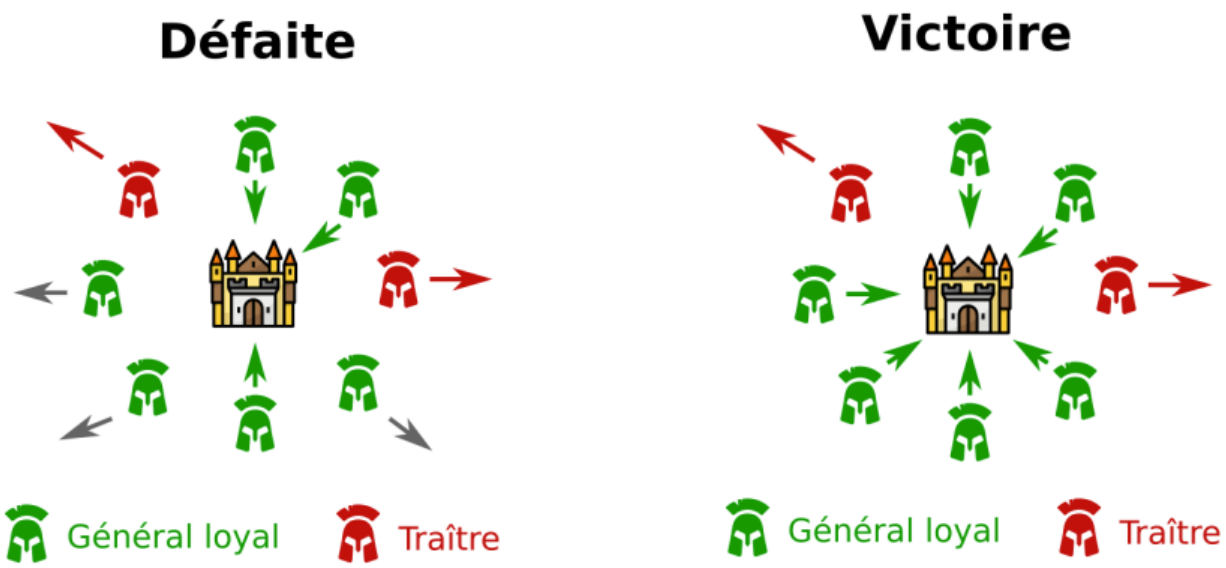


Figure 9 - Scénarios d'attaque des généraux byzantins

Il existe différentes manières permettant à un réseau décentralisé d'attendre la tolérance byzantine grâce aux algorithmes de consensus.

Les algorithmes de consensus sont des protocoles de défenses contre les attaques Sybil qui permettent de sélectionner le prochain bloc à soumettre au consensus. Une majorité des blockchains, grâce au processus de validation décentralisé, c'est à dire géré par tous les validateurs, si un individu tente de proposer des blocs non valides, il subira alors une punition variant en fonction de l'algorithme utilisé. Ces méthodes de validations rendent inefficaces toute tentative de falsification de bloc. Pour la preuve de travail (Bitcoin), la punition sont les calculs effectués pour trouver les blocs, pour la preuve d'enjeu, la punition sont les jetons mis en jeu pour obtenir la recherche du bloc.

Lors de l'attaque Sybil, l'attaquant contourne le système de réputation du réseau en créant un grand nombre d'identités et en les utilisant pour exercer une influence disproportionnée. Réaliser (et réussir) une attaque Sybil lors des élections présidentielles reviendrait à faire voter des millions de fois une personne pour obtenir plus de 50% des votes. Dans notre cas de la blockchain ou plus largement des registres distribués (DLT), une attaque Sybil serait la création de nombreux nœuds propageant les mêmes transactions erronées et réussir à intégrer ces transactions à la blockchain.

2.2.1.1. Preuve de travail

Pour le réseau Bitcoin, Satoshi Nakamoto a eu l'idée d'utiliser la preuve de travail (PoW - Proof of Work) originalement implémenté par Adam Back en 1997 pour Hashcash afin de combattre le courrier indésirable. Le principe étant de demander à l'expéditeur d'effectuer une tâche plus ou moins simple pour valider l'envoi du courrier.

Pour le Bitcoin, on demande au mineur de trouver un "nonce" validant certaines conditions.

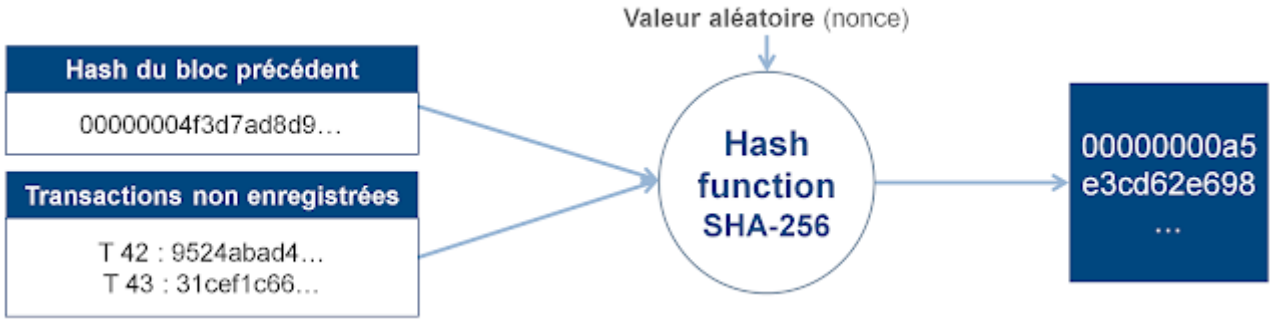


Figure 10 - Principe de recherche du hash du bloc suivant

Par exemple, si le hash du bloc actuel est "42" et le contenu du bloc est Bonjour (contenu = transaction sur la figure) alors on recherche un nonce N tel que "42bonjourN" génère un hash validant la condition fixée. Dans le cas du bitcoin un seuil est fixé et le mineur doit trouver un hash d'une valeur inférieure au seuil.

Le poids d'un hash est calculé de la manière suivante :

Hash : "a7c3"

Ici le hash est en valeurs hexadécimales, ce qui signifie que les chiffres qui le composent sont dans l'ensemble {0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f}, où (a,b,c,d,e,f) correspond à (10,11,12,13,14,15).

$a7c3 = 10*16^3 + 7*16^2 + 12*16^1 + 3*16^0 = 40\,960 + 1792 + 3 = 42\,753.$

On observe que les premiers éléments du hash sont les plus lourds, par conséquent, plus le seuil est bas, plus on recherche de zéro en début de hash. Un mineur de Bitcoin va donc tester des nonces différents jusqu'à trouver un hash suffisamment léger. Le seuil est fixé de sorte que l'ensemble des mineurs cherchant un nouveau bloc mettent dix minutes à le trouver. Si un mineur trouve le hash en neuf minutes, alors le seuil est abaissé et inversement.

Difficulté	Changement	Bits	Bloc moyen
21,448,277,761,059 - 21.45 T	- 1.27 %	0x170d1f8c	10 min 08 s
21,724,134,900,047 - 21.72 T	+ 1.35 %	0x170cf4e3	09 min 52 s
21,434,395,961,348 - 21.43 T	+ 2.93 %	0x170d21b9	09 min 43 s
20,823,531,150,111 - 20.82 T	+ 1.05 %	0x170d8457	09 min 54 s
20,607,418,304,385 - 20.61 T	+ 10.79 %	0x170da8a1	09 min 02 s
18,599,593,048,299 - 18.60 T	- 0.38 %	0x170f2217	10 min 02 s
18,670,168,558,399 - 18.67 T	- 2.54 %	0x170f1372	10 min 16 s
19,157,154,724,710 - 19.16 T	+ 8.87 %	0x170eb156	09 min 11 s
17,596,801,059,571 - 17.60 T	+ 4.82 %	0x170ffedd	09 min 32 s
16,787,779,609,932 - 16.79 T	- 16.05 %	0x1710c433	11 min 55 s
19,997,335,994,446 - 20.00 T	+ 3.62 %	0x170e134e	09 min 40 s

Figure 11 - Exemples de temps nécessaire pour trouver un nouveau block

Les mineurs investissent du temps de calcul et consomment beaucoup d'énergie pour résoudre un problème mathématique complexe ; la difficulté est ajustée afin que la résolution se fasse tous les 2016 blocs (dix minutes environ). Une fois le hash calculé et le bloc validé par le réseau, les mineurs sont récompensés ; ainsi il est très peu intéressant voir pas du tout d'être malhonnête puisqu'il faudrait déployer une immense puissance de calcul très coûteuse qui augmente exponentiellement dans le monde.

Le mining sur le réseau Bitcoin consomme actuellement plus de 79 TWh par an ce qui correspond à la consommation d'électricité du Chili et une seule transaction à la même empreinte carbone qu'environ 700 000 transactions Visa soit 338.94 kgCO2.

2.2.1.2. Preuve d’enjeu

Il existe plusieurs autres formes de preuve qui concurrence la preuve de travail peu écologique et généralement lente. La preuve d’enjeu utilise un processus différent, le système utilise toujours un algorithme cryptographique mais l’objectif du mécanisme est différent ; dans ce système l’enjeu est basé sur le nombre de jetons que possède un validateur. De plus, dans une majorité de blockchain utilisant la preuve d’enjeu, si un individu crée des blocs frauduleux il sera puni et une partie de ses jetons lui sera retirée, réduisant son impact sur le réseau. Ainsi au lieu d’investir dans du matériel et de l'électricité coûteux, les participants investissent directement dans le jeton lui-même.

Imaginons le cas d’une blockchain avec 1000 jetons en circulation, vous achetez et mettez en jeu 100 jetons ; vous avez donc mis en jeu 10% des jetons en circulation donc vous avez 10% de chance d’être sélectionné pour valider la transaction et gagner une récompense. Ainsi un attaquant devra acheter des jetons pour faire des attaques et selon la blockchain risque des pénalités en cas de comportements malveillants. La bonne mise en place de la preuve d’enjeu repose sur la distribution équitable des jetons au départ pour assurer la décentralisation de la chaîne et empêcher un monopole.

2.2.1.3. Preuve d’enjeu délégué

Dans le processus de preuve d’enjeu délégué, le principe est dérivé de la preuve d’enjeu : les utilisateurs peuvent mettre leurs jetons en jeu et voter pour un nombre particulier de délégués. Le poids du vote d'un utilisateur est basé sur son enjeu.

Par exemple, si un utilisateur Bob mise 20 jetons pour un délégué et qu'une autre utilisatrice Alice en place 2, le vote de X aura plus de poids que celui de Y. Ainsi le délégué qui reçoit le plus grand nombre de votes aura plus de probabilité de produire de nouveaux blocs et d’être récompensé.

2.2.1.4. Preuve de personne ou d’humanité

Idena est la première blockchain de preuve de personne où chaque nœud est lié à une crypto-identité - une seule personne avec un pouvoir de vote égal. Pour devenir utilisateur, vous devez prouver que vous êtes un humain unique sans exiger la divulgation d'aucune donnée personnelle (pas de KYC). Pour cela vous devez participer régulièrement (au moment de la rédaction de ce rapport toutes les deux semaines) à une cérémonie où vous devrez résoudre une série de “flips” (CAPTCHA). Après chaque validation si votre score dépasse 75% vous serez récompensé sinon votre compte sera supprimé.

2.2.1.5. Preuve de capacité

La preuve de capacité est un mélange de la preuve de travail et d’enjeu, elle permet aux mineurs d’utiliser l’espace vide de leur disque dur pour miner des cryptomonnaies et participer à la sécurité du réseau.

Au lieu de modifier à plusieurs reprises les chiffres de l'en-tête du bloc et de procéder à un hachage répété pour obtenir la valeur de la solution, l’algorithme fonctionne en stockant une liste de solutions possibles sur le disque dur du dispositif de minage avant même que l'activité de minage ne commence. Ainsi plus le disque dur est grand, plus on peut y stocker de valeurs de solutions possibles, et plus le mineur a de chances de faire correspondre la valeur de hachage requise de sa liste, ce qui augmente ses chances de gagner la récompense.

L’objectif final est simple : Il s'agit de récompenser les participants du réseau pour leur comportement honnête tout en rendant les comportements malveillants compliqués et coûteux.

2.2.2. Protocoles de consensus

Depuis la création des réseaux distribués (dans les années 1980-1990) il n'y a eu que trois approches aux problèmes du consensus : Classique, Nakamoto et plus récemment Avalanche.

Les protocoles de consensus dits classiques ont émergé bien avant l'avènement de la blockchain dans les années 1980-1990 et sont utilisés principalement dans les bases de données distribuées à divers degrés de décentralisation. Chaque validateur a besoin d'entendre un vaste ensemble de nœuds avant de prendre une décision. Ce consensus possède deux problèmes majeurs, ce protocole est fragile car tous les validateurs se connaissent et un attaquant n'a besoin que de 33% du réseau pour le contrôler. De plus, il est très peu scalable et les performances sont très altérées à partir d'une centaine de validateurs.

Le protocole Nakamoto créé par Satoshi Nakamoto a été le premier consensus capable de résister à un adversaire et de fonctionner à l'échelle mondiale. C'est une révolution mais qui comporte plusieurs inconvénients : ce protocole est lent, consomme beaucoup d'énergie.

Publiée en mai 2018 dans un article, la team Rocket propose un troisième consensus appelé Avalanche. L'objectif du protocole Avalanche est de combiner les avantages du consensus classique (vitesse, finalité rapide, écologique) et ceux de Nakamoto (robustesse et décentralisation).

Voici un tableau récapitulatif des avantages et désavantages de chacun :

	Classique	Nakamoto	Avalanche
Scalable	non	non	oui
Robuste	non	oui	oui
Hautement décentralisée	non	oui	oui
Faible latence	oui	non	oui
Haut débit	oui	non	oui
Léger	oui	non	oui
Écologique	oui	non	oui
Résilient aux attaques 51%	non	non	oui

2.3. Conception

On cherchera dans cette partie à présenter un moyen, parmi ceux existants, de construire une blockchain basique et fonctionnelle. Les méthodes d'implémentations seront très simplifiées.

2.3.1. Structure de base

L'élément indispensable dans une blockchain sont les blocs eux-mêmes. Leurs propriétés définissent le principe de fonctionnement des méthodes. Il faut donc commencer par définir les informations que contiennent les blocs.

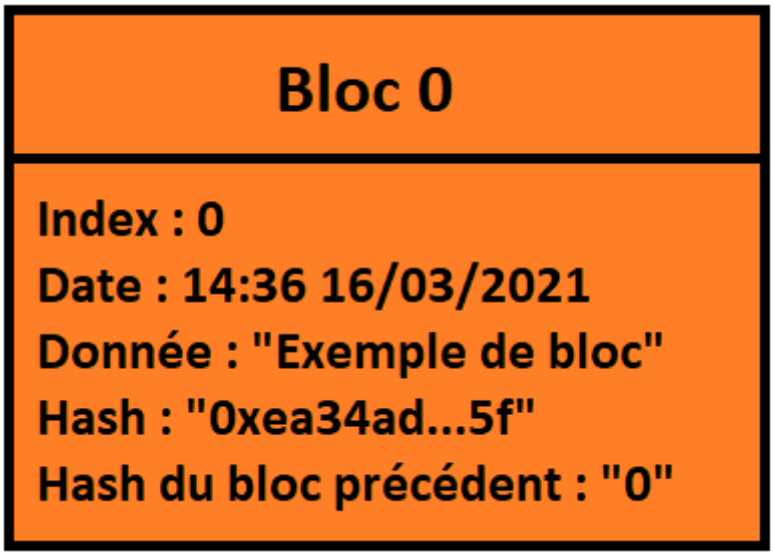


Figure 12 - Exemple de structure d'un bloc

Tous les blocs contiendront les informations définies au départ. Ici on utilisera l'index du bloc pour connaître sa hauteur dans la chaîne, la date à laquelle il a été ajouté, la donnée stockée dans ce bloc et enfin le hash du bloc ainsi que celui du bloc précédent pour pouvoir chaîner les blocs entre eux.

Une fois la structure mise en place, on rajoute quelques éléments de base. Pour commencer on crée le premier bloc de la chaîne, on l'appelle bloc genesis, c'est le seul bloc qui ne possède pas de hash précédent et le bloc suivant va générer son hash grâce au hash du premier bloc ce qui permettra à la chaîne de continuer son développement de façon indépendante. Ensuite on ajoute les méthodes d'ajout et de validation de bloc. On contrôle également les chaînes proposées en vérifiant si le premier bloc correspond au bloc genesis puis on parcourt les blocs de la chaîne. Si la chaîne est valide et plus grande que la précédente, on stocke alors la nouvelle chaîne.

2.3.2. Ajout de la preuve

La structure étant en place, on ajoute à la méthode de création de bloc une condition que devra remplir l'utilisateur souhaitant trouver le bloc suivant. Il existe plusieurs concepts de preuves comme on a pu le voir dans les parties précédentes. On présentera succinctement l'ajout de la preuve d'enjeu et de travail.

Pour implémenter la preuve de travail il faut fixer une difficulté, la difficulté va imposer au créateur d'un nouveau bloc de trouver un hash spécifique. Dans la fonction contrôlant la validité d'un bloc on ajoute la valeur de cette difficulté pour vérifier si le hash proposer en bon ou non. Maintenant que la notion de difficulté est ajoutée à cette blockchain, on peut désormais choisir la blockchain non en fonction de sa longueur mais en fonction de sa difficulté cumulée, on calcule la valeur totale de la difficulté utilisée pour chaque bloc et la chaîne possédant la plus haute somme est choisie.

La preuve d'enjeu se présente comme un système de loterie. Pour participer il faut soumettre un bloc et une valeur d'enjeu. La fonction va prendre la liste de tous les participants et choisir aléatoirement un gagnant. Chaque participant à une chance proportionnelle à la taille de la valeur mise en jeu de se faire choisir. Une fois le gagnant choisi, le bloc qu'il propose passe le test de validation, si celui-ci est invalide le gagnant perd la valeur mise en jeu et la loterie recommence.

2.3.3. Transactions

Pour introduire le concept de transaction dans la blockchain il faut utiliser les signatures. En effet, pour savoir de qui provient et à qui est destiné une transaction on utilise sa signature. Le système de signature est implémenté grâce à une paire de clés attribuée à chaque utilisateur.

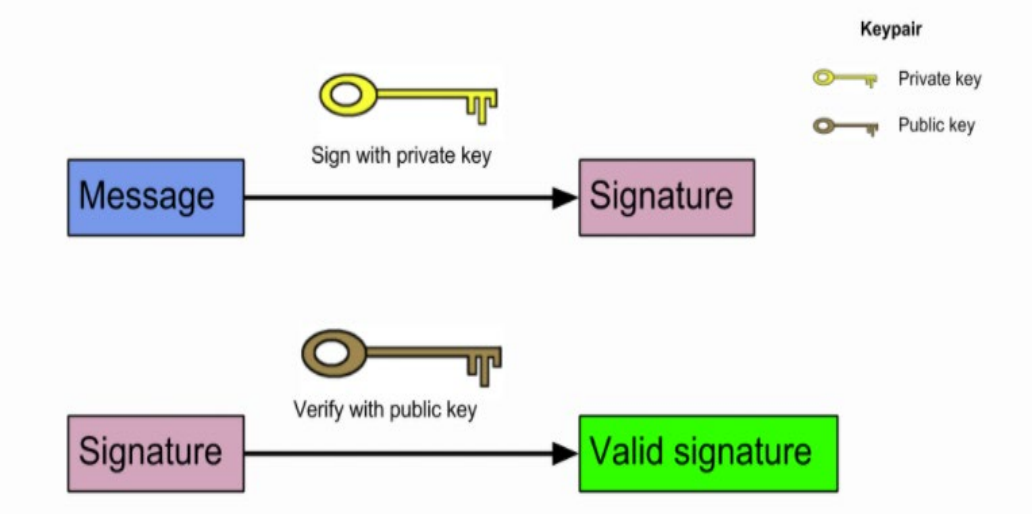


Figure 13 - Fonctionnement des clés de signature

Une clé de la paire est la clé privée que seul le propriétaire doit connaître, cette clé va servir à générer la signature. La seconde clé est publique et donc disponible pour tout le monde. La clé publique est la seule clé déchiffrant la signature faite avec la clé privée ce qui prouve l'authenticité de la transaction si celle-ci déchiffre la signature.

Une transaction est matérialisée en deux parties possédant chacune une adresse publique (clé publique) et de l'objet de la transaction (argent, contrat, etc…).

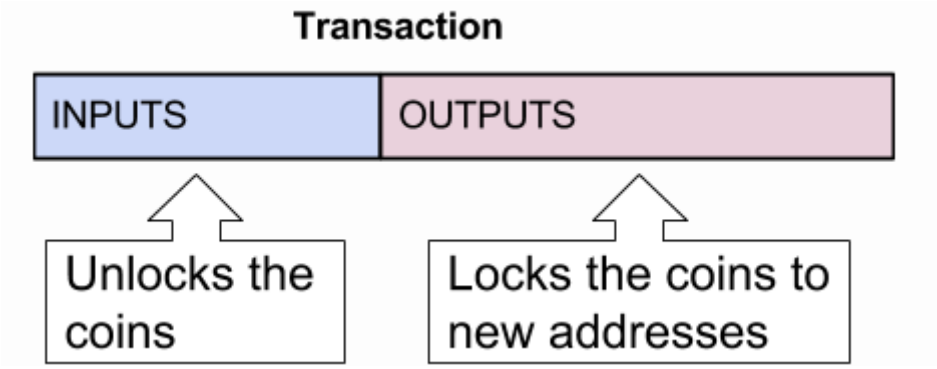


Figure 14 - Contenu d'une transaction

La première partie de la transaction contient d'où provient le contenu de la transaction et débloque l'accès à l'offre grâce à la signature de l'auteur. La deuxième partie donne le contenu de l'offre au destinataire à qui appartient la clé publique dans la transaction. Seule la personne possédant la clé privée correspondant à la clé publique sera capable d'accéder au contenu de la transaction.

2.3.4. Explorateur de la blockchain

Il ne reste plus qu'à rendre la blockchain utilisable en créant un explorateur de blockchain. Son rôle est de trouver le bloc correspondant aux transactions que l'on souhaite consulter ou encore trouver toutes les transactions effectuées par une adresse (utilisateur). Il existe aujourd'hui des explorateurs pour les blockchains les plus populaires, le site Blockchain.com propose des recherches sur la blockchain du Bitcoin et de l'Ethereum par exemple.

3. Projets existants sur la blockchain

3.1. Blockchains existantes

Il existe de nombreux projets basés sur la blockchain tous différents les uns des autres cependant tous tournent autour de trois concepts fondamentaux : la décentralisation, l'évolutivité et la sécurité. Le trilemme des blockchains définies par Vitalik Buterin, créateur de la blockchain Ethereum, pose un défi aux développeurs : créer la blockchain parfaite, évolutive, décentralisée et sécurisée ; sans faire de compromis sur aucun aspect.

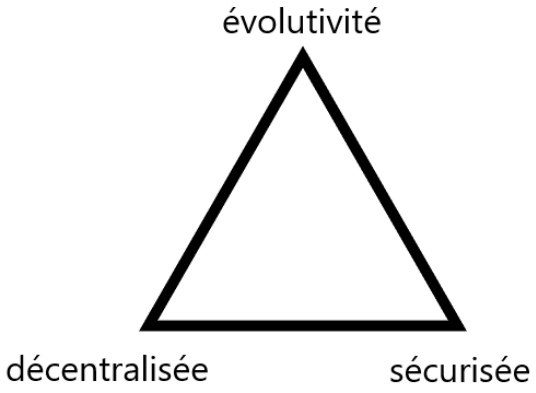


Figure 15 - Trilemme des blockchains

3.1.1. Bitcoin

Bitcoin est la première blockchain à être créée en 2009, une dizaine d'années après elle a réussi à imposer cette technologie comme révolutionnaire. Malgré ses nombreux désavantages (preuve de travail qui pollue, lenteur et coût des transactions) sa crypto-monnaie native le bitcoin tend à devenir une valeur refuge tel l'or face au dollar.

Il existe de nombreux projets utilisant la blockchain Bitcoin comme le lightning Network qui est un protocole de paiement de couche 2 (surcouche comme le modèle OSI). Il existe plusieurs solutions présentes sur la couche 2, l'une d'entre elles est le canal d'état utilisé par le lightning Network. C'est un canal de communication bidirectionnel entre les participants qui leur permet de mener des interactions, qui se produiraient normalement sur la blockchain, hors de la blockchain. Cela permet de réduire le temps d'attente puisque vous n'êtes plus dépendant d'un tiers comme un mineur. Un contrat est signé entre les participants qui interagissent directement les uns avec les autres, puis lorsque l'ensemble des transactions est terminé, l'état final de la chaîne est rajouté à la blockchain.

Malgré sa faible adoption, il est destiné à permettre des transactions rapides et a été proposé comme une solution au problème de l'évolutivité du bitcoin.

3.1.2. Ethereum

Ethereum est une blockchain décentralisée et open-source dotée de fonctionnalités de contrats intelligents (smart contracts). Un smart contract est un programme informatique déployé sur une blockchain et qui est irrévocable ; ce type de fonctionnalité dispose de nombreux avantages comme sécuriser un paiement entre deux parties (ou plus) ou plus simplement automatiser des paiements. Le financement participatif est un bon exemple : si une certaine quantité de crypto-monnaies est déposée dans un contrat intelligent à une certaine date, le paiement sera versé à la collecte de fonds - si ce n'est pas le cas, le paiement sera retourné aux donateurs. Étant donné que les contrats intelligents existent sur une blockchain, ils sont immuables et vérifiables (“code is law” - Lawrence Lessig), garantissant un niveau élevé de confiance entre les parties afin qu'ils reflètent fidèlement les paramètres énoncés de l'accord et s'exécutent si, et seulement si, ces paramètres sont respectés.

Sa crypto-monnaie native s’appelle Eth et est la deuxième plus grande crypto-monnaie en termes de capitalisation boursière, après le Bitcoin. Ethereum est la blockchain la plus activement utilisée notamment par les développeurs.

Récemment la popularité de la DeFi (Decentralized Finance) a explosé, ses acteurs proposent de créer un système financier alternatif au système actuel contrôlé par les institutions. Les services de la DeFi sont uniquement accessibles sur le Web 3.0 (celui des systèmes décentralisés comme la blockchain) et ses objectifs sont multiples au-delà de l’aspect financier très présent : la création de valeurs financières accessibles de manière décentralisée, transparente et sans intermédiaire.

En 2020 la valeur totale bloquée a fait un bond de plus de 9000% passant de moins de 500 millions de dollars à 45 milliards de dollars (chiffre datant du 15 mars 2021).

Le principal inconvénient actuel à la blockchain Ethereum sont les frais de transactions, pour une simple transaction les frais oscillent entre 15 et 25 dollars.

3.1.3. Chainlink

La principale limite dans les contrats intelligents est la difficulté à connecter des sources d’informations extérieures aux contrats sur la blockchain, c’est à ce moment qu'interviennent les oracles.

Chainlink est un réseau décentralisé qui fournit des données et des informations à partir de sources hors blockchain (off-chain) à travers des contrats intelligents.

Un contrat émet une demande d’informations, le protocole Chainlink l’enregistre et crée un nouveau contrat intelligent appelé SLA (Chainlink Service Level Agreement) pour

obtenir ces informations hors chaîne. Ce contrat SLA génère trois sous contrats : un contrat de réputation, de correspondance des commandes et d'agrégation.

Le contrat de réputation va vérifier les antécédents d'un fournisseur d'oracle, évalue et supprime les nœuds peu fiables ; le contrat de correspondance des commandes délivre la demande du contrat, prends leurs offres et choisi le type et nombre de nœuds pour répondre à la demande ; enfin le contrat d'agrégation recueille les données, les valide et les concilie pour obtenir un résultat précis. Les données sont ensuite traduites sur la blockchain.

3.2. Projets utilisant la technologie blockchain

3.2.1. UjoMusic

Lorsqu'une production crée une nouvelle musique, elle est majoritairement distribuée sur les plateformes de streaming comme spotify, deezer ou encore youtube. La rémunération des artistes s'effectue en fonction du nombre d'écoutes et est directement reversée aux plateformes qui distribuent ensuite aux artistes les bénéfices.

La startup UjoMusic propose un système utilisant la blockchain ethereum pour assurer la traçabilité et la rémunération d'une œuvre. L'œuvre serait stockée sur la blockchain ce qui assure qu'aucune modification n'a été apportée à la musique. Pour y accéder, l'utilisateur doit payer une somme en Éther fixée par l'auteur. Cette méthode de rémunération crée un lien direct entre les utilisateurs et le créateur sans passer par les plateformes de streaming et les systèmes bancaires.

3.2.2. ThinngChain

De nos jours, la consommation responsable n'est plus une pratique de niche. De plus en plus de français prêtent attention aux labels bio ou éco responsables. Malheureusement certains de ces labels sont créés par l'entreprise qui vend le produit, d'autres sont appliqués contre de l'argent et non un contrôle du respect des règles du label. De plus, les pays européens montrent déjà des difficultés à conserver la traçabilité des aliments arrivant dans nos magasins, le scandale des lasagnes à la viande de cheval de Findus en est un exemple.

La startup ThingChain met en action l'inviolabilité des informations inscrites dans une blockchain pour donner la possibilité à l'utilisateur et aux organismes de contrôle de consulter la chaîne de production des produits qu'il achète. A l'aide de PopCodes (Proof-Of-Provenance) servant d'identifiant digital unique inscrit dans la blockchain Bitcoin. Ce PopCode permet de remonter toutes les étapes de la chaîne de production du produit. Pour une part de lasagnes on peut donc retrouver d'où viennent les tomates, les pâtes et même le blé, les œufs utilisés pour faire l'intégralité de la recette.

3.2.3. Enigma

L'utilisation des données personnelles n'est plus un sujet ignoré des utilisateurs d'internet depuis les accusations de divulgation des données sur les grosses multinationales Facebook, Google, Twitter, … Les utilisateurs sont aujourd'hui traqués dans leurs activités en ligne avec peu de moyens de contrôler où vont leurs données personnelles. S'ajoutent à ces problématiques, le vol de données lors des cyber-attaques.

Enigma est une création du MIT Media Lab, son but est simple, ne plus donner la responsabilité du cryptage et du stockage des données à un organisme tiers. Les données d'un utilisateur sont stockées dans un ou plusieurs blocs d'une blockchain et organisées selon leur sensibilité. Les données sont cryptées avec plusieurs clés de cryptage que l'utilisateur détient. Il peut donc choisir de donner l'accès ou non à des informations que lui seul peut gérer.

3.3. Smart contracts

Les smart contracts, ou contrats intelligents, sont des programmes informatiques irrévocables. Ils sont de plus en plus déployés sur des blockchains et exécutent un ensemble d'instruction prédéfinies.

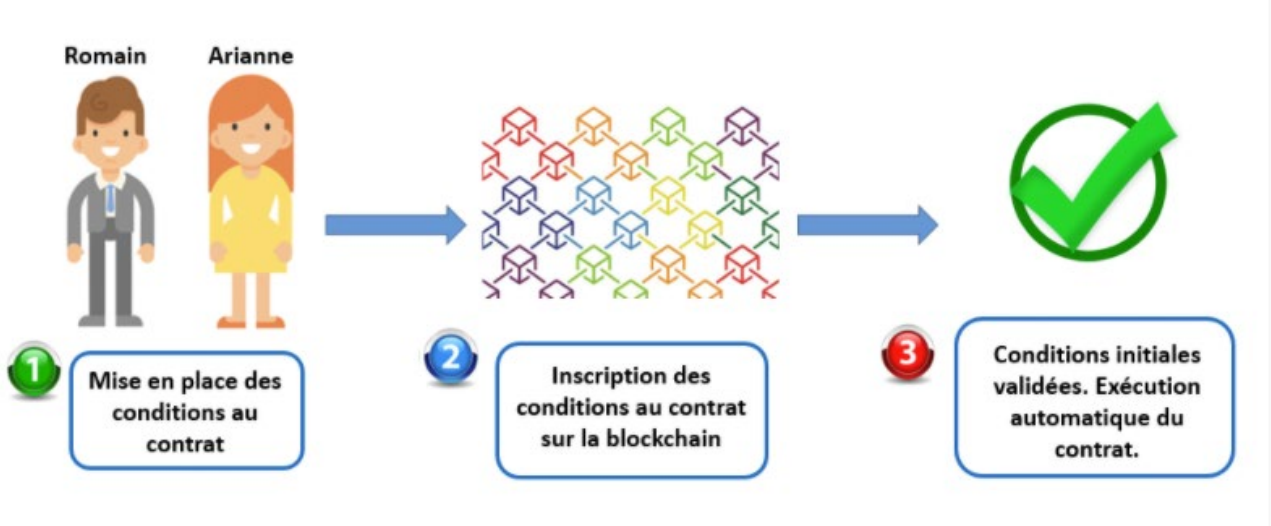


Figure 16 – Schéma explicatif du fonctionnement d'un smart contract

Pour un contrat classique, écrit et signé par deux acteurs, c'est la loi qui assure le respect des clauses du contrat. Dans le cas d'un contrat intelligent déployé sur la blockchain, la force obligatoire des contrats n'est plus garantie par la loi, mais par le code informatique (code is law). Les propriétés de la blockchain permettent, contrairement aux contrats classiques, de les rendre inchangeables et visibles de tous, tout en garantissant le

respect des conditions. Les smart contracts peuvent être très basiques avec la livraison d'une donnée si un paiement est enregistré, mais les smart contracts sont très puissants et peuvent aller jusqu'à répliquer toutes les clauses et les règles permettant à des sociétés de fonctionner.

La plus grande majorité des smart contracts utilisé de nos jours servent pour automatiser des échanges de cryptomonnaies. Toutes les informations de ces échanges de valeurs sont automatiquement inscrites dans la blockchain. Par conséquent, les transferts utilisant des smart contracts sont publics, prévisibles et irrévocables. On peut alors tracer le chemin de la monnaie et déterminer qui la détient. Les smart contracts peuvent contenir autant de conditions d'exécution que nécessaire, ces propriétés ne laissent normalement pas de place au doute. Pas besoins de faire confiance à qui que ce ne soit ni à se soucier du non-respect des règles du contrat.

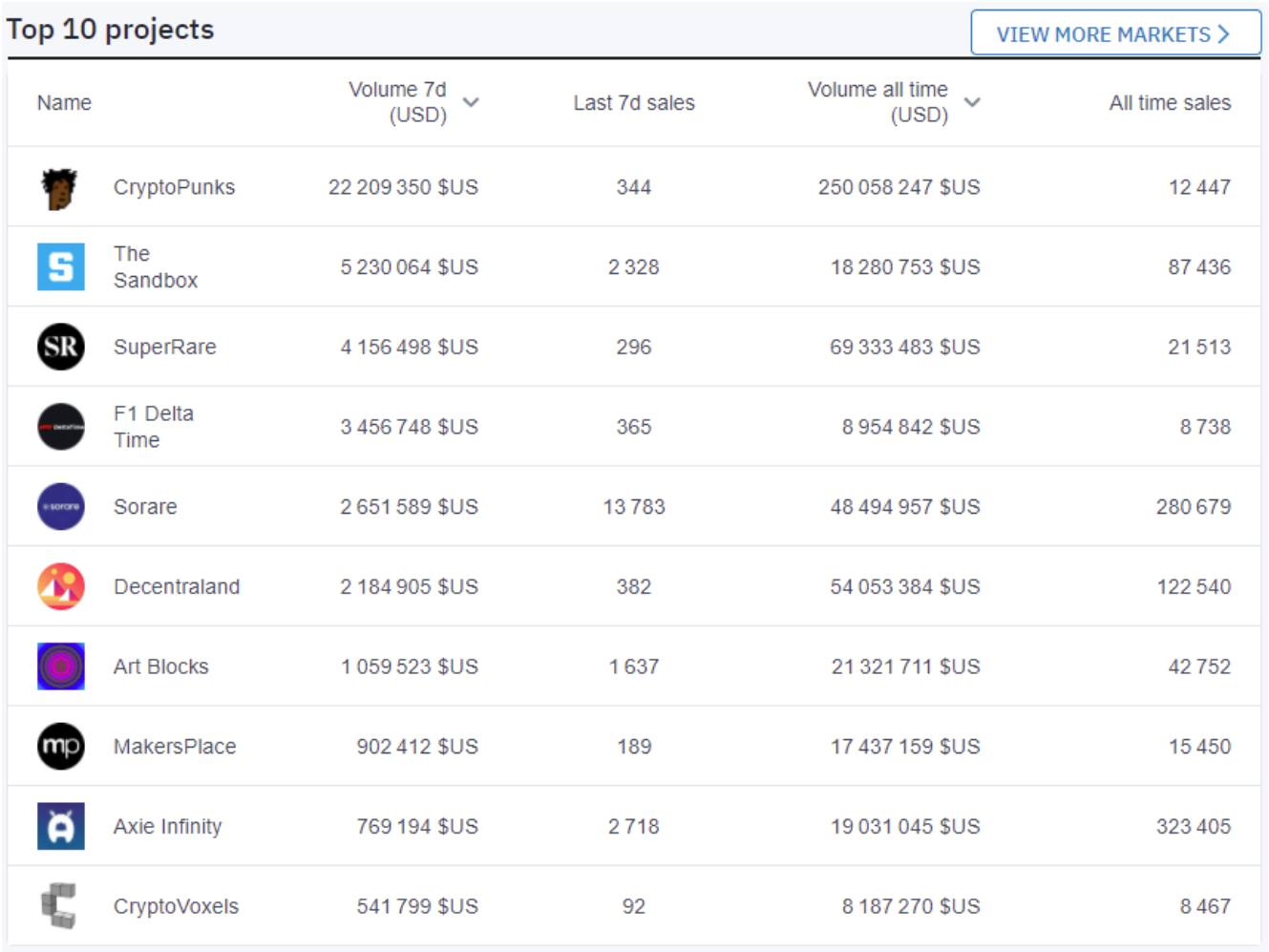
Des standards ont été établi pour la création des smart contracts. Le plus utilisé est le standard ERC-20 pour créer des jetons. Le standard ERC-223 est une version plus complexe du ERC-20 mais permet d'éviter la perte de jetons s'ils sont utilisés dans des smart contracts pas adapter à leur type.

Récemment, le standard ERC-721 a vu son utilisation décuplée. Son principal objectif est de créé des jetons non-fongibles (NFT). Un jeton non-fongible désigne un jeton unique et non divisible. Si on prend l'exemple du Bitcoin, un Bitcoin est équivalent à n'importe quel autre Bitcoin. Il est aussi divisible et un individu peut envoyer 0.1 Bitcoin à dix personnes différentes. Un NFT peut être comparé à une œuvre d'art comme la Joconde, elle n'existe qu'en un seul exemplaire, on peut en prendre une photo mais qu'une seule personne détient l'original.

La démocratisation de l'utilisation des NFT est fortement liée à plusieurs mouvements de mode avec notamment les Cryptokitties créés en 2017 par Dapper Labs. Les Crytpokitties sont des chats à collectionner. Chaque chat est un NFT et possède des caractéristiques génétiques unique définissant sa rareté et donc son prix.

Figure 17 – Exemple de Cryptokitties

Maintenant tout objet virtuel est susceptible d'être tokenisé, des pistes audios, des images, des GIF ou encore des tweets. Leur donnés seront conservés est resteront inchangées sur la blockchain. On estime d'après le site NonFungible.com une capitalisation globale de plus de 300 millions de dollars en 2020.



Top 10 projects

VIEW MORE MARKETS >

Name	Volume 7d (USD)	Last 7d sales	Volume all time (USD)	All time sales
CryptoPunks	22 209 350 $US	344	250 058 247 $US	12 447
The Sandbox	5 230 064 $US	2 328	18 280 753 $US	87 436
SuperRare	4 156 498 $US	296	69 333 483 $US	21 513
F1 Delta Time	3 456 748 $US	365	8 954 842 $US	8 738
Sorare	2 651 589 $US	13 783	48 494 957 $US	280 679
Decentraland	2 184 905 $US	382	54 053 384 $US	122 540
Art Blocks	1 059 523 $US	1 637	21 321 711 $US	42 752
MakersPlace	902 412 $US	189	17 437 159 $US	15 450
Axie Infinity	769 194 $US	2 718	19 031 045 $US	323 405
CryptoVoxels	541 799 $US	92	8 187 270 $US	8 467

Figure 18 – Liste des 10 plus gros projets sur le site NonFungible.com

4. Notre application

Le code de « Safe On Chain » est disponible en open source ici.

4.1. Cahier des charges

Le projet « Safe On Chain » est une application destinée à servir aux écoles délivrant un diplôme et aux futurs diplômés. Le but est de fournir un moyen virtuel sûr et durable pour conserver les diplômes et certifier leur provenance.

Le produit final doit donc répondre aux besoins des écoles et de leur futur diplômé. La réalisation du projet est contrainte à une restriction temporelle. Le projet doit être prêt en 8 semaines. Dans ces 8 semaines sont aussi comptés le temps de recherche et de présentations de la blockchain ainsi que le temps de recherche de l'application. Ces contraintes ne permettent de réaliser qu'une version fonctionnelle mais imparfaite de l'application.

Ci-dessous le QQOQCP récapitulant les informations précédentes :

QUOI	Virtualiser les diplômes
QUI	ISEN
OU	Sur un site web
QUAND	Le 26 avril
COMMENT	En utilisant une Blockchain
POURQUOI	Pour certifier et sauvegarder les diplômes
COMBIEN	Non défini

Le client a donné, au début du développement de l'application, son cahier des charges. Le produit doit :

- Permettre aux écoles de créer des diplômes
- Stocker les diplômes des étudiants sur une longue durée
- Certifier l'intégrité et la provenance d'un diplôme
- Permettre aux diplômés de consulter leur diplôme
- Utiliser une blockchain
- Respecter les lois en vigueur concernant la conservation des données personnelles
- Être sécurisé

Tableau récapitulatif des fonctions principales (Fp) et des fonctions contraintes (Fc).

Situation	Fonction	Mot clé	Caractéristiques
Utilisation	Fp1	Créer	Insertion des données nécessaires
	Fp2	Stocker	Longue durée
	Fp3	Retrouver	Méthode simple et rapide
	Fp4	Prouver	Provenance et détenteur
	Fc1	Blockchain	Adaptée au besoin
	Fc2	Lois	RGPD
	Fc3	Sécurité	Non falsifiable ou destructible

4.2. Gestion de projet

Le projet s'est déroulé sur plusieurs mois, en distanciel et en équipe. Dans ces conditions il est nécessaire de mettre en place une organisation claire et précise des systèmes de communication et du temps.

4.2.1. Gestion du temps

Pour prendre conscience de l'avancée du projet et prendre les bonnes décisions en fonction de l'avancement de celui-ci, un planning sous forme de diagramme de GANTT a été mis en place une fois que le cahier des charges de l'application fut déterminé. Ce planning donne des dates limites pour chaque tâche permettant d'adapter le développement de l'application au fur et à mesure de sa conception. Le diagramme de GANTT fut modifié à plusieurs reprises tout au long du projet pour toujours garder une idée précise et réaliste l'avancement du projet afin de le réaliser dans le délai imparti.

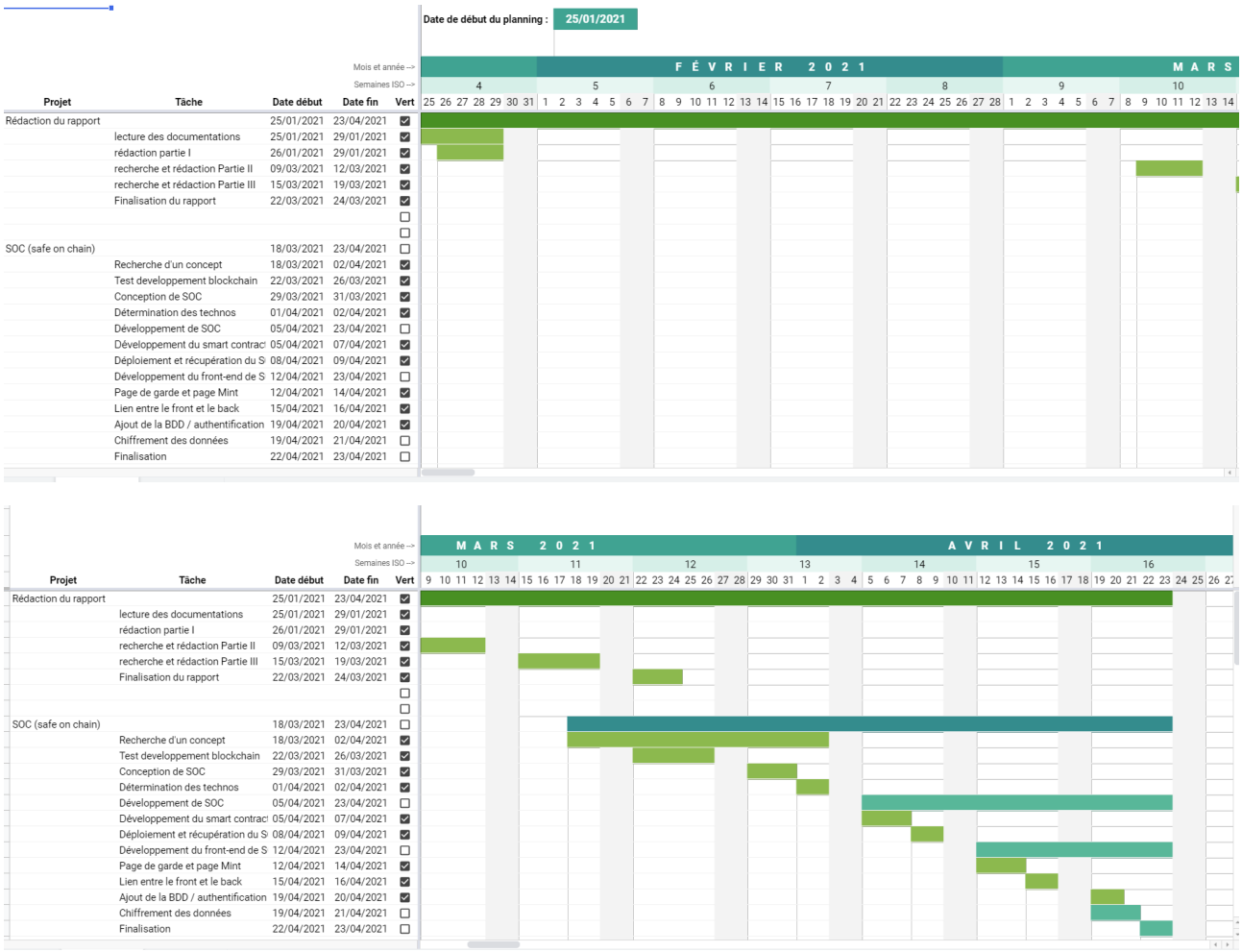


Figure 19 – Diagramme de GANTT final

4.2.2. Gestion de la communication

Le projet s'est déroulé pendant la période de confinement de la COVID-19, l'intégralité de la partie recherche et développement du projet s'est faite en distanciel. Ce fonctionnement impose de mettre en place une méthode de communication efficace et organisée.

Des réunions journalières de l'équipe furent imposées. Ces réunions ont permis de prendre en compte les difficultés de chacun rapidement et de trouver des solutions convenant aux besoins du client. Se sont ajoutés à ces réunions, des rendez-vous réguliers avec le professeur référent de ce projet pour présenter l'avancement du projet, résoudre les problèmes de conception et fournir des informations impossibles d'accès (ex : organisation interne de l'entreprise cliente, méthode de remise des diplômes…).

L'outil Google Drive a facilité le partage des fichiers et la rédaction du rapport. L'organisation des fichiers au sein de ce stockage sur le Cloud est facile à gérer et supporte tous les types de fichiers. De plus, les modifications apportées sur un document sont prises

en comptes dynamiquement par les autres utilisateurs ce qui facilite la mise en commun des modifications.

L'outil Github a été utilisé dès le début du développement de l'application pour stocker et partager le code produit entre les membres de l'équipe. Chaque modification du code est ainsi stockée sur Github, rendant possible de suivre pas à pas chaque étape de développement d'un programme.

4.3. Phase de recherche

Le temps dédié à la recherche de l'application était initialement fixé à deux jours, cependant cette phase de recherche s'est avérée plus longue que prévu et a pris finalement cinq jours, c'est l'élément qui a le plus bouleversé le déroulement du projet. Les trois idées d'applications considérées pendant la phase de recherche sont décrites plus loin.

4.3.1. Création d'une blockchain pour les écoles

La première idée était de créer une blockchain. Cette blockchain a pour but de contenir tous les types d'informations que les écoles ont besoins de conserver sur une longue durée, le tout dans un environnement fiable et durable.

Les écoles participant au projet possèdent des nœuds et sont ainsi validateurs du réseau ; le processus de validation se fait par la preuve d'enjeu donc des jetons sont délivrés aux écoles.

Des squelettes de blockchain sont disponibles en open source mais il fallait implémenter entièrement la validation des blocs, le système de distribution des jetons, la communication entre les nœuds et créer un livrable pour installer et utiliser la blockchain. Après avoir consulté un expert de la blockchain, nous avons eu la confirmation que cette idée semblait irréalisable dans le temps imparti.

4.3.2. Plateforme de pari sans organisme tiers

À la suite de l'explosion de l'utilisation des NFTs, l'idée de créer une plateforme où l'on met en jeu des NFTs plus ou moins rare ne demandant pas de reposer sa confiance sur un organisme tiers comme certaines entreprises le font pour les paris sportifs.

L'objectif étant de créer des NFTs avec un système de rareté ajoutant de valeur qui a pour but de rajouter un enjeu à chaque pari. Chacun des participants met en jeu un NFT et le match se déroule via un smart contract, le code est donc public et personne ne peux

intervenir sur l'issue du match. Les récompenses sont automatiquement reversées une fois le match terminé.

Aucune solution n'a été trouvée pour « forcer » le paiement à la fin du match. Le seul moyen est de valider la transaction à un compte neutre avant le match mais cela revient à placer sa confiance dans un système tiers. De plus, cela multiplie les transactions et donc le prix de participation au match.

4.3.3. Safe On Chain

« Safe On Chain » reprend l'utilisation des NFT de la plateforme de pari. Cette fois, les NFTs sont des diplômes qu'une école délivre à ses étudiants. Le but de cette application est de permettre aux écoles de virtualiser la remise des diplômes et de certifier sur une longue durée leur authenticité.

L'application est matérialisée par une application web constituant l'interface utilisateur pour créer un diplôme, un diplômé peut ensuite consulter son diplôme directement sur un autre site web. Son diplôme est un NFT déployé sur la blockchain à l'aide d'un smart contract. L'école doit connecter son portefeuille virtuel pour payer les transactions lors du déploiement d'un diplôme.

4.4. Choix techniques

4.4.1. Choix de la blockchain

Une fois que l'application sera déployée, tous les nouveaux diplômes seront émis sur la blockchain pour être conservés *ad vitam aeternam*. Chaque nouveau diplôme créé nécessite une transaction pour créer le NFT. Cette transaction a un coût et cela peut devenir un frein à l'adoption de l'application si ce coût est trop élevé. De plus, la création du NFT se fait par des smart contracts, la blockchain doit donc supporter le déploiement d'un smart contract et son utilisation. Enfin, le but est de créer un système utilisable par un nombre indéfini d'écoles, il faut donc une blockchain qui permet d'accueillir autant d'utilisateurs que possible.

Avalanche est une plateforme open-source pour le lancement d'applications décentralisées et hautement évolutives créée par Emin Gün Sirer et développée par la société Ava Labs. La différence clé entre Avalanche et d'autres réseaux décentralisés est son nouveau protocole de consensus. Le protocole Avalanche utilise une nouvelle approche du consensus pour atteindre ses solides garanties de sécurité, sa finalité rapide et son haut débit, sans compromettre la décentralisation.

Avalanche est une plateforme « durable ». En effet, son consensus fonctionne sur le principe de la preuve d'enjeu, moins énergivore et plus scalable que les protocoles basés sur la preuve de travail.

Avalanche est composée de trois blockchains intégrées : la chaine d'échange (X-Chain), la chaine de plateforme (P-Chain) et la chaine de contrat (C-Chain). C'est cette dernière que nous utiliserons car c'est une instance de la machine virtuelle Ethereum qui permet ainsi de développer et de déployer des smart contracts en Solidity avec l'utilisation de frameworks tels que Remix, Metamask et Truffle. Solidity++ a pour but d'être implémenté sur Avalanche pour supporter le versionnage et améliorer le système de saisie.

Les frais sont plus faibles que ceux de la blockchain Ethereum, depuis une mise à jour du réseau les frais ont été diminués par 50%. De plus avec l'implémentation de l'EIP-3298 par Ethereum et la mise à jour Apricot sur le réseau Avalanche ces frais deviendront dynamiques et extrêmement faible.

4.4.2. Smart contract et NFT

Les jetons ERC-721 sont une catégorie de jetons élaborés par le réseau Ethereum en 2017. Ce standard a été mis au point de façon à créer des jetons non fongibles. Ces jetons sont uniques, des données et une image sont liés aux jetons.

Le standard ERC-721 est disponible en open source et utilise le langage programmation Solidity qui est un langage orienté objet, tout comme peuvent l'être le Javascript, le Python ou le C++. Ce langage emprunte beaucoup à d'autres langages de programmation comme le JS, C++ ou C# pour permettre à n'importe quel développeur de travailler rapidement avec ce nouveau langage.

Le langage Solidity et le standard ERC-721 sont donc des technologies adaptées à la création de jetons uniques représentés par les diplômes délivrés par les écoles.

4.4.3. Front-end

Le but du front-end de l'application est de donner une interface visuelle aux écoles pour générer simplement de nouveaux diplômes et permettre aux diplômés de consulter leur diplôme.

Le déploiement de NFT sur la blockchain nécessite de payer des frais de transaction. Metamask est une extension des navigateurs web pour interagir avec la blockchain. Metamask est un fournisseur de portefeuille qui peut être utilisé pour toutes les blockchains et intègre l'EVM (Ethereum Virtual Machine). La clé privée du portefeuille Metamask est stockée sur le navigateur de l'utilisateur, et non pas sur des serveurs distants ; cela donne à l'utilisateur plus de contrôle sur ses clés publiques et privées. De plus, une fois configuré,

Metamask est très simple à utiliser, toutes ses fonctionnalités sont claires afin d'envoyer et de recevoir de la monnaie facilement.

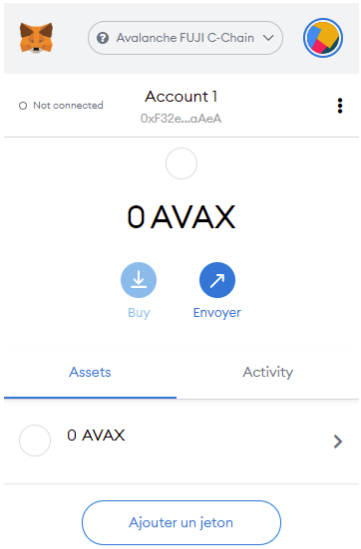


Figure 20 – Interface Metamask

Pour communiquer avec Metamask et la blockchain il est nécessaire d'utiliser la librairie web3 créée par les développeurs d'Ethereum.

La partie administrateur de notre application utilise la libraire React qui facilite la création d'interfaces utilisateurs interactives avec la conception de vues simples pour chaque état d'une application et est facilement utilisable avec la bibliothèque web3.

Étant donné du peu de données à afficher et de la simplicité du code, il a été décidé d'utiliser uniquement du HTML et du Javascript pour la partie utilisateur vérification et affichage du diplôme.

4.4.4. Backend

Lors de l'utilisation d'une application web où le traitement se fait chez le client, comme dans le cas de notre application, il est nécessaire d'avoir un backend et une API (interface de programmation d'application) pour notamment communiquer avec une base de données ou utiliser des services nécessitant des mots de passe qui ne peuvent pas être en clair sur le site web. Le choix s'est porté sur NodeJS et Express qui permet de combiner backend et API très simplement, l'avantage est qu'une très large majorité de notre application n'est codé qu'avec un seul langage : le JavaScript.

Les données sur la blockchain étant immuables, il était nécessaire de trouver une parade afin de respecter les lois du RGPD (règlement général sur la protection des données) ; notamment si un étudiant fait une requête pour supprimer ses données.

C’est à ce moment que le backend intervient : il permet de chiffrer les données personnelles des étudiants. Lors de la création d’un diplôme, les données sont envoyées en clair sur le serveur puis sont chiffrées avec l’algorithme aes-256-ctr et sont renvoyées sur l’application web pour être ajoutées sur la blockchain. Le mode CTR est utilisé pour avoir une bonne parallélisation.

4.5. Réalisation de l’application

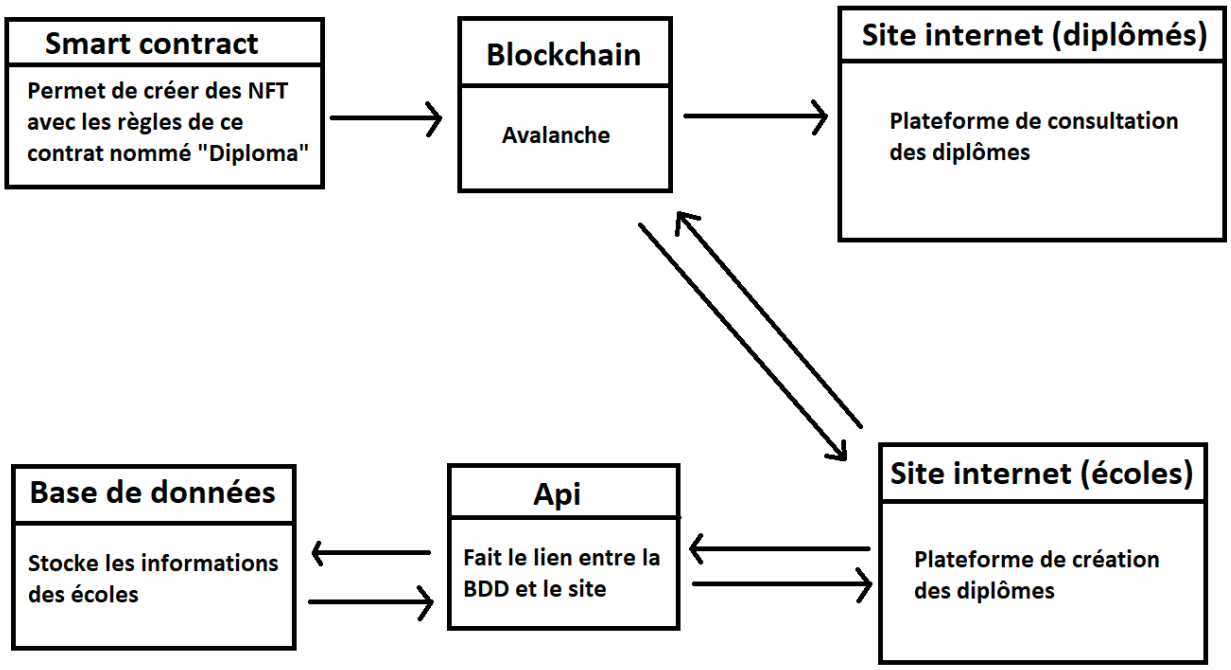


Figure 21 – Schéma de la structure de l’application

4.5.1. Conception et déploiement du smart contract

Pour créer le smart contract « Diploma », on utilise la classe mère ERC721 pour implémenter les fonctionnalités du standard de création de NFT. Il existe des extensions optionnelles à ce standard, ces extensions sont des classes abstraites. La classe abstraite ERC721Ennumerable ajoute une fonction qui donne un numéro d’index unique à chaque NFT créé. La classe abstraite ERC721URIStorage donne la possibilité d’ajouter des données au NFT, appelée metadata.

Une classe abstraite nécessite d’implémenter ces fonctions dans le smart contract. Les fonctions « _burn » et « tokenURI » proviennent de la classe ERC721Storage. « _burn » envoie le NFT en argument de cette fonction à l’adresse 0x000…0dEaD. Cette adresse n’appartient à aucune entité. Il est impossible de supprimer un élément déployé sur

la blockchain, cependant, tout jeton envoyé à cette adresse est considéré comme supprimé ou brulé. La fonction « tokenURI » renvoie la metadata stockée dans le NFT.

Les fonctions « _beforeTokenTransfer » et « supportsInterface » appartiennent à la classe abstraite ERC721Enumerable. La fonction « _beforeTokenTransfer » envoie le jeton à l'adresse 0x000…000 si l'adresse de destination est manquante ou invalide. « supportsInterface » vérifie si le contrat est conforme aux normes du standard ERC721.

Ensuite, la fonction « mint » est la plus importante du contrat. Elle permet de créer le NFT ; cette la fonction va attribuer un ID au jeton, ajouter la metadata puis déploier le jeton sur la blockchain.

Enfin, Truffle est un environnement de développement qui permet d'implémenter, de tester et de déployer un smart contract sur une blockchain supportant l'EVM (Ethereum Virtual Machine). Il est facile de configurer la blockchain sur laquelle le smart contract doit-être déployé. Il suffit de renseigner l'ID de la blockchain et l'URL qui permet de s'y connecter.

4.5.2. Interface utilisateur et création de NFT

L'objectif de l'interface utilisateur est de fournir un moyen simple pour les écoles de créer et déployer les diplômes sur la blockchain. Cette interface n'est donc destinée qu'aux écoles et aux administrateurs du site.

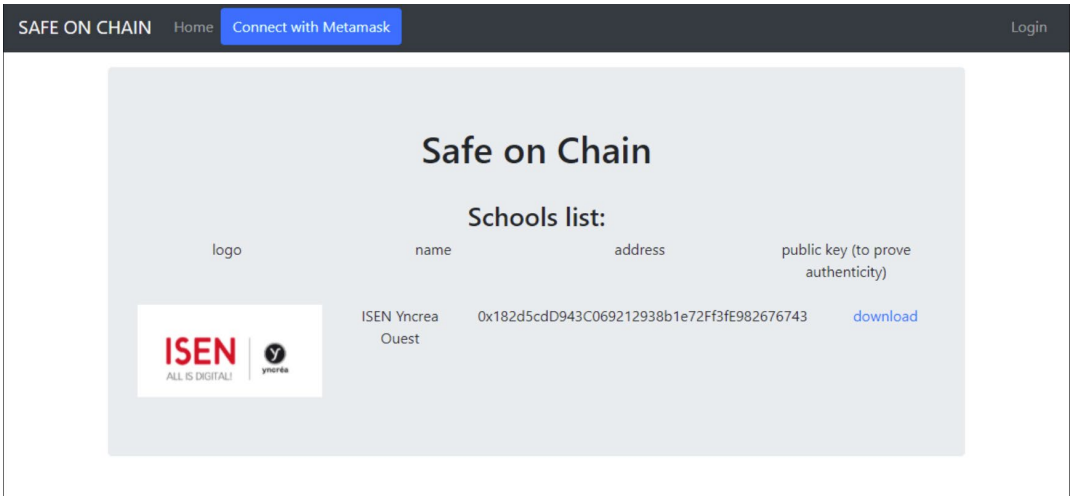


Figure 22 – Page d'accueil de l'interface utilisateur (école)

La page d'accueil affiche la liste des écoles enregistrées. Pour chaque école, son logo, son nom et l'adresse de son portefeuille virtuel sont affichés. Le bouton en haut à droite « login » permet à un administrateur de se connecter et d'avoir accès à l'interface pour ajouter une nouvelle école au site.

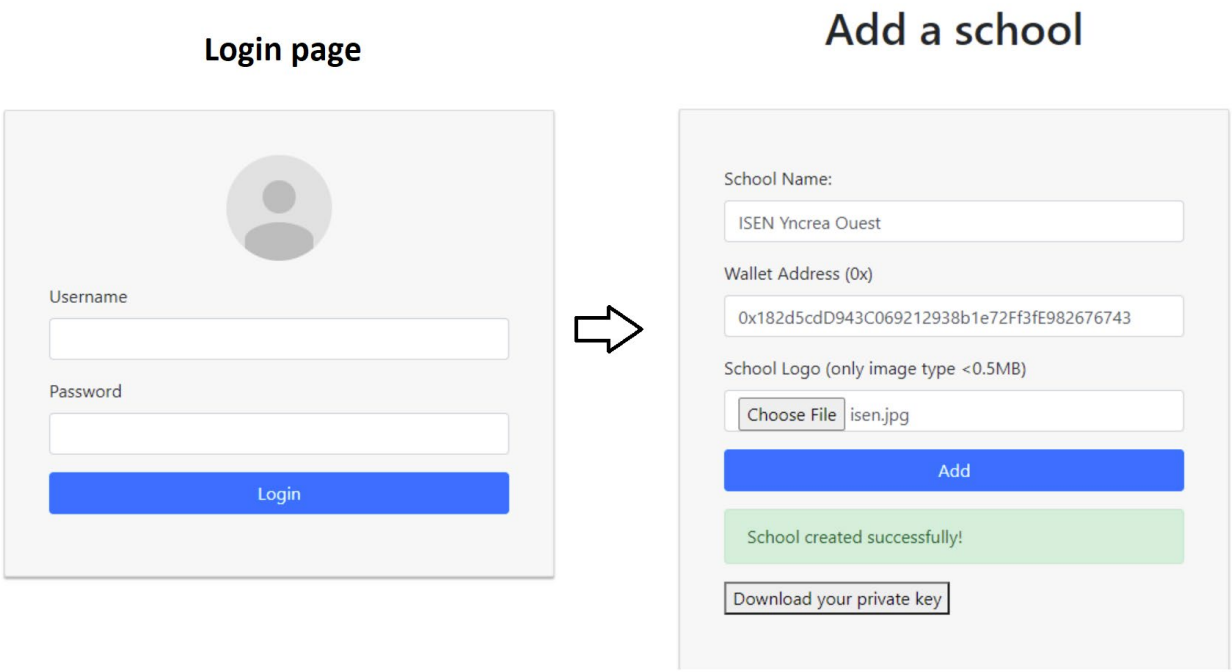


Figure 23 – Fonctionnalités admin

L'adresse du portefeuille virtuel de l'école sert à identifier celle-ci sur le site. Dans le header de la page d'accueil, le bouton « connect with Metamask » lie le portefeuille utilisé avec l'extension de navigateur Metamask avec le site web. L'authentification ne passe donc pas par l'ajout d'un mot de passe mais par la connexion à son portefeuille virtuel car toutes les adresses sont uniques. Une fois l'école créée, une paire de clés privée et publique est générée ; la clé publique est sauvegardée dans la base de données et la clé privée sera téléchargée et utilisée lors de la création de diplômes pour signer celui-ci et certifier sa provenance.

Si une école enregistrée sur le site se connecte avec Metamask, un bouton « Create diploma » apparaît.

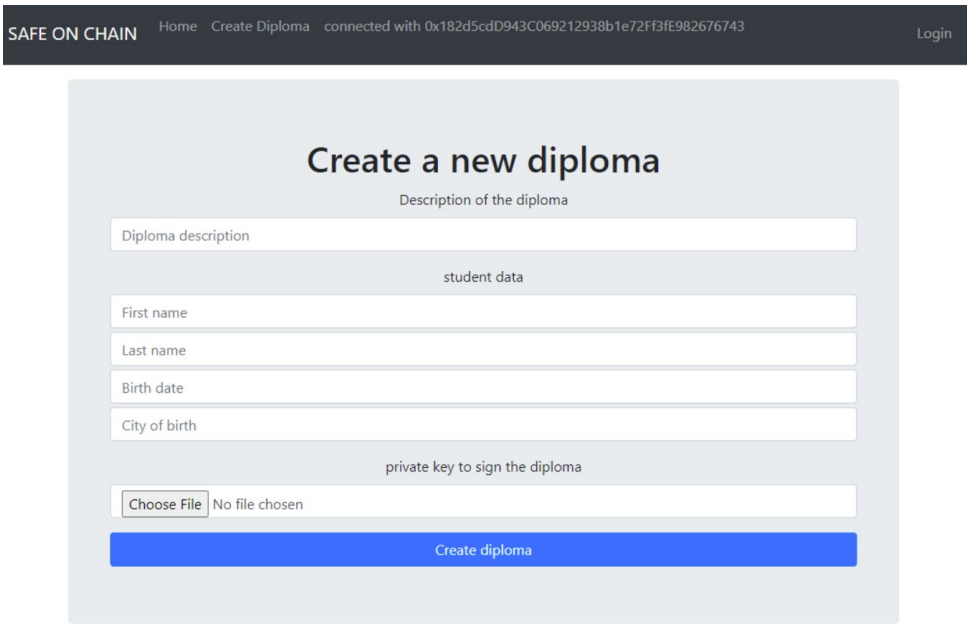


Figure 24 – Formulaire de création de diplôme

L'école peut ensuite renseigner les différents champs qui seront insérés dans le NFT. La clé privée générée lors de la création de l'école est également ajoutée pour signer le diplôme. Quand l'école clique sur le bouton « Create diploma », le NFT est créé et déployé sur la blockchain.

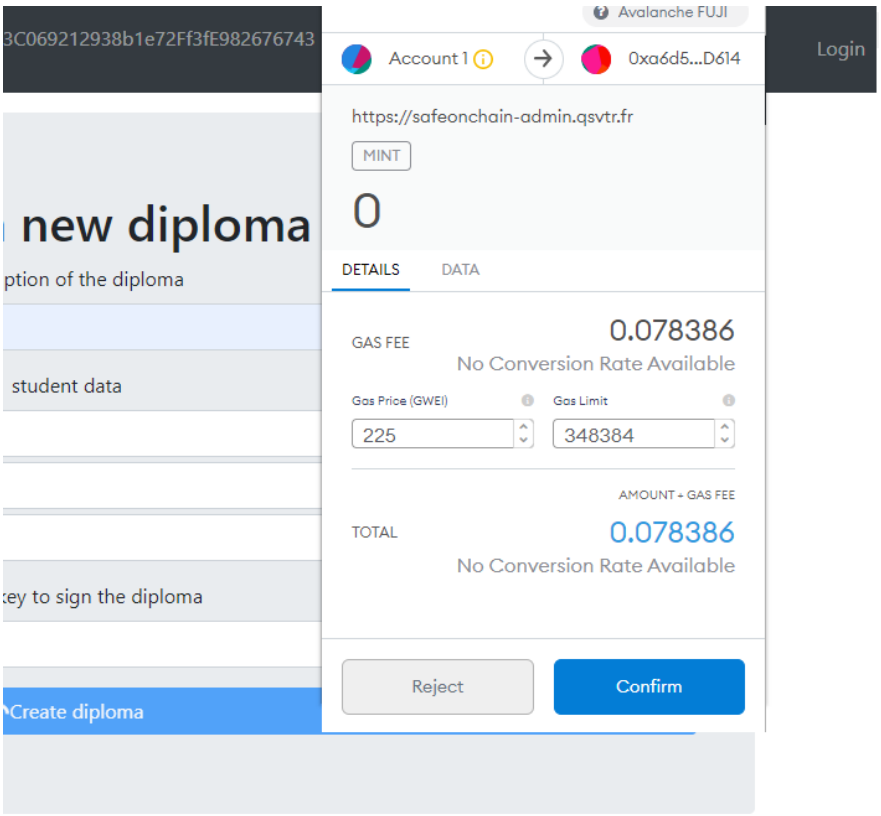


Figure 25 – Validation de transaction avec Metamas

Pour déployer le diplôme sur la blockchain, il faut payer des frais de transaction. C'est le portefeuille virtuel de l'école qui est utilisé pour payer la transaction. L'interface de paiement de l'extension Metamask s'ouvre sur la droite, elle affiche le prix de la transaction, il suffit d'appuyer sur « Confirm » pour que l'opération soit validée.

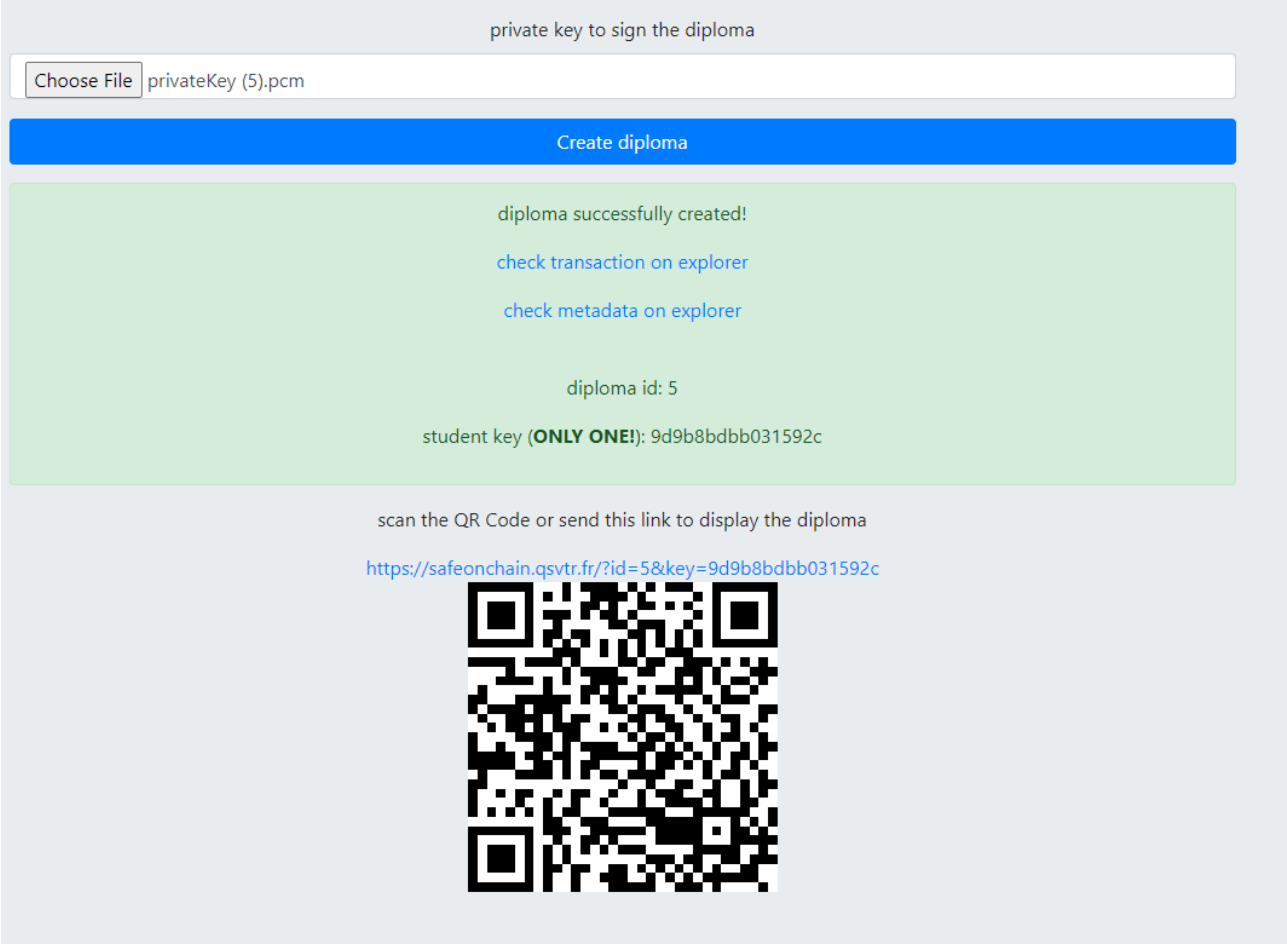


Figure 26 – Résultat de la création d'u diplôme

Lorsque la transaction est validée (environ une seconde), l'ID du diplôme et la clé de déchiffrement de l'étudiant s'affichent. Des liens pour visualiser le NFT sur la blockchain sont également disponibles. Un lien vers le site d'affichage du diplôme est affiché en bas et un QR code mène également au site.

4.5.3. Affichage du diplôme

Une page html indépendante du site est chargée de l'affichage des diplômes. Il faut utiliser l'ID du diplôme pour le retrouver sur la blockchain. Il est possible d'accéder au site d'affiche par deux moyens différents. Le diplômé peut choisir d'utiliser l'URL de base du site, un formulaire basique s'affiche.

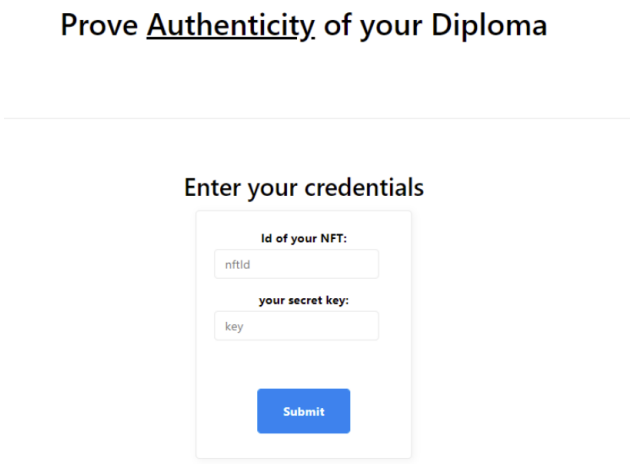


Figure 27 – Formulaire de recherche de diplôme

Le deuxième moyen d'accéder à son diplôme est de scanner le QR code fourni lors de la création du diplôme. Il redirige automatiquement vers le site d'affichage, les informations nécessaires pour retrouver et afficher le diplôme sont renseignées dans l'URL.

safeonchain.qsvtr.fr/?id=58&key=c76e408dd5b9b21a

Une fois les informations ajoutées, le NFT est retrouvé sur la blockchain, la clé de déchiffrement est appliquée sur les données. C'est aussi ici que la signature de l'école est vérifiée. Si celle-ci est valide, une alerte verte indique que le diplôme est authentique et toute la metadata est affichée.

Figure 28 – Affichage du diplôme déchiffré

4.5.4. API

L'API est utilisée pour faire un lien entre le frontend en React et la base de données. La base de données sert à stocker les informations d'authentification, plus précisément l'identifiant et le mot de passe des administrateurs. Elle stocke également la liste des écoles enregistrées sur le site, leur logo, leur nom, leur adresse et leur clé publique qui permet de déchiffrer la signature.

La discussion entre l'API et le frontend s'effectue par des requêtes HTTP. La libraire Express est configurée de telle sorte que seules les adresses du site puissent effectuer des requêtes sur l'API.

4.5.5. Chiffrement des données et signature

Le chiffrement des données personnelles du diplômé et la génération d'une paire de clés pour la signature de l'école ont nécessité l'ajout d'un backend. Le backend est un programme qui fonctionne automatiquement sur le serveur.

Pour le chiffrement des données du diplôme, la fonction « encrypt » utilise la donnée à chiffrer, une clé de chiffrement stockée sur le serveur ainsi qu'un IV. L'IV est une valeur déterminée aléatoirement qui permet de générer un hash différent pour une même valeur chiffrée. C'est l'IV que l'on fournit au diplômé lors de la création de son diplôme pour déchiffrer les données.

La partie vérification de la signature de l'école est également gérée par la fonction « verifyAuthenticityNFT » dans le backend. Elle prend en argument la clé publique, la signature, la donnée signée et l'algorithme utilisé pour générer la signature.

4.6. Ouverture

L'étude du projet a pris en compte la totalité de celui-ci, de la conception à la mise en application. Or, la réalisation technique s'est focalisée sur la production d'un outil fonctionnel. De ce fait, le projet reste encore améliorable sur plusieurs points.

Pour commencer, les diplômes se créent manuellement un par un. Pour chaque nouvelle création il faut rentrer les informations personnelles et la clé privée pour signer le diplôme. On imagine difficilement la viabilité de ce système pour des clients avec des effectifs plus importants. Il serait beaucoup plus ergonomique de récupérer un fichier sous le format csv contenant toutes les informations nécessaires. La clé privée pour signer les diplômes peut également être liée à la session et non à la création d'un diplôme ce qui n'obligerait pas l'école à devoir la rentrer pour chaque diplôme mais seulement une fois à la connexion.

Ensuite, l'aspect visuel des interfaces utilisateurs reste assez basique et peut intuitive. Une page de description du site et une revue du style de la page sont des éléments à régler avant d'utiliser cette application pour un plus grand nombre de clients.

Enfin, l'application a été développée dans le but de certifier des diplômes. Même si les données ne sont pas formatées pour les utiliser dans d'autres situations, on peut facilement modifier la structure de ces données pour l'adapter à d'autres types de documents. Selon les besoins de l'école, d'autres documents peuvent être conservés avec la même méthode (Certificat de scolarité, bulletin de semestre…).

5. Conclusion

Mener à bien un projet complexe divisé en plusieurs parties en binôme sur une durée d'environ deux mois est très enrichissant. Des recherches précises et organisées ont constitué une solide base pour appréhender la suite du projet. Avec une bonne connaissance du sujet, il a été possible de concevoir et de réaliser, à temps, une application utilisant une blockchain.

La création de l'application « Safe On Chain » est une véritable expérience. La conception de l'application est complexe et demande d'utiliser en harmonie des langages et des frameworks différents. Une bonne communication est primordiale au sein du groupe lors du développement des différents composants pour assurer une mise en commun efficace. En effet, on peut aisément déterminer l'origine des problèmes quand les membres de l'équipe sont au courant du travail des autres.

Une présentation de la technologie blockchain et l'application « Safe On Chain » mise en ligne et disponible en open source sur Github représente le produit final de ce projet. L'application « Safe On Chain » est fonctionnelle et considérée comme aboutie pour le temps accordé à sa réalisation.

Il reste des points à améliorer pour utiliser « Safe On Chain » au grand public. Dans l'hypothèse d'une reprise du projet, des indications sur des éléments à améliorer sont disponibles dans ce rapport et le code a été développé en suivant une organisation des fichiers stricte facilitant sa reprise et sa modification.

Bibliographie

PARES, Pascal, 2016. Introduction à la blockchain. Creative commons. P. 18.

PIGNEL, Marion, 2019. LA TECHNOLOGIE BLOCKCHAIN. P. 31.

BUFFET, Guillaume, 2016. Comprendre la blockchain : anticiper le potentiel de disruption de la blockchain sur les organisations, U. P. 56.

ISMAIL, Lotmani Zakaria, YOUCEF, Elhomr et BENTAOUZA, Chahinez Mérièm, sans date. SIMULATION D'UNE ATTAQUE SUR LE CRYPTOSYSTEME RSA. P. 52.

TESSIER, Sylvain, 2019. Fonctionnement de la blockchain et son intérêt pour le monde pharmaceutique. P. 264.

À la découverte du mouvement cypherpunk à l'origine du Bitcoin, 2020. *Cryptoast* [en ligne]. [Consulté le 10 mars 2021]. Consulté à l'adresse : https://cryptoast.fr/decouverte-mouvement-cypherpunk-origine-bitcoin/

Chiffrement par décalage, 2020. *Wikipédia* [en ligne]. [Consulté le 11 mars 2021]. Consulté à l'adresse : https://fr.wikipedia.org/w/index.php?title=Chiffrement_par_d%C3%A9calage&oldid=176276364

Chiffrement RSA, 2021. *Wikipédia* [en ligne]. [Consulté le 11 mars 2021]. Consulté à l'adresse : https://fr.wikipedia.org/w/index.php?title=Chiffrement_RSA&oldid=180659245

Cryptographie asymétrique, 2020. *Wikipédia* [en ligne]. [Consulté le 12 mars 2021]. Consulté à l'adresse : https://fr.wikipedia.org/w/index.php?title=Cryptographie_asym%C3%A9trique&oldid=176342854

Cryptologie, 2020. *Wikipédia* [en ligne]. [Consulté le 12 mars 2021]. Consulté à l'adresse : https://fr.wikipedia.org/w/index.php?title=Cryptologie&oldid=177116117

Hash function, 2021. *Wikipedia* [en ligne]. [Consulté le 15 mars 2021]. Consulté à l'adresse : https://en.wikipedia.org/w/index.php?title=Hash_function&oldid=1019270146

Birthday problem, 2021. *Wikipedia* [en ligne]. [Consulté le 15 mars 2021]. Consulté à l'adresse : https://en.wikipedia.org/w/index.php?title=Birthday_problem&oldid=1017399203

Nick Szabo, 2020. *Wikipédia* [en ligne]. [Consulté le 16 mars 2021]. Consulté à l'adresse : https://fr.wikipedia.org/w/index.php?title=Nick_Szabo&oldid=175576615

Enigma, le système de cryptage de données basé sur la blockchain du MIT Media Lab, sans date. *usine-digitale.fr* [en ligne]. [Consulté le 18 mars 2021]. Consulté à l'adresse : https://www.usine-digitale.fr/article/enigma-le-systeme-de-cryptage-de-donnees-base-sur-la-blockchain-du-mit-media-lab.N372044

Qu'est-ce que Enigma? Guide d'initiation aux contrats secrets, sans date. *Acheter Bitcoin* [en ligne]. [Consulté le 18 mars 2021]. Consulté à l'adresse : https://acheterbitcoin.pro/altcoins/enigma-eng-avis/

startup Archives, sans date. *Follow My Vote* [en ligne]. [Consulté le 18 mars 2021]. Consulté à l'adresse : https://followmyvote.com/tag/startup/

Bitcoin Energy Consumption Index, sans date. *Digiconomist* [en ligne]. [Consulté le 18 mars 2021]. Consulté à l'adresse : https://digiconomist.net/bitcoin-energy-consumption/

Comprendre la blockchain Ethereum – Article 1 : Bitcoin, première implémentation de la blockchain (2/2) | Ethereum France, 2016. [en ligne]. [Consulté le 19 mars 2021]. Consulté à l'adresse : https://www.ethereum-france.com/comprendre-la-blockchain-ethereum-article-1-bitcoin-premiere-implementation-de-la-blockchain-22/

How to time-stamp a digital document | SpringerLink, sans date. [en ligne]. [Consulté le 19 mars 2021]. Consulté à l'adresse : https://link.springer.com/article/10.1007/BF00196791

Private, Public, and Consortium Blockchains - What's the Difference?, sans date. *Binance Academy* [en ligne]. [Consulté le 22 mars 2021]. Consulté à l'adresse : https://academy.binance.com/en/articles/private-public-and-consortium-blockchains-whats-the-difference

Smart Contract : Qu'est-ce qu'un contrat intelligent ? • BitConseil, sans date. [en ligne]. [Consulté le 22 mars 2021]. Consulté à l'adresse : https://bitconseil.fr/smart-contract-contrat-intelligent/