L’application de la blockchain dans le monde du Jeu Vidéo

Par Codelupi Quentin & Perez Alexander

Introduction

D’un côté, la blockchain, une technologie de stockage et de transmission d’informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle. Une technologie prometteuse et très “à la mode” mais encore sous exploité et utilisé que dans très peu de domaines.

De l’autre côté, l’industrie du Jeu Vidéo, une industrie présente depuis un moment maintenant et qui est toujours en pleine évolution. Une industrie en pleine évolution certe, mais qui commence à se heurté a des problématiques qui deviennent de plus en plus complexe a résoudre avec les technologies qu’elle utilise actuellement.

Dans ce topic, nous allons expliquer comment la blockchain, dans son évolution future, pourrait apporter un grand nombre de solutions et de nouveautées au monde du Jeu Vidéo.

Blockchain

Définition

La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle
(définition de Blockchain France).

Par extension, une blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne.

Les avantages

La blockchain peut avoir plusieurs avantages en fonction du contexte de son utilisation, ici on va en citer les 4 principales:

- Créer de la confiance entre deux parties sans intermédiaire
- Réduire drastiquement les coûts de transaction
- Permettre l'automatisation de contrats immuables
- Offrir la perspective d'un nouveau mode de gouvernance

La création de confiance entre deux parties sans intermédiaire

La transmission de valeur entre utilisateurs du réseau repose sur la cryptographie asymétrique. Le registre public n'est pas tenu par une institution centrale : chaque nœud en possède une copie. Les utilisateurs du réseau connaissent les modalités de son fonctionnement et la blockchain repose sur l'acceptation d'un consensus commun.

La réduction des coûts de transaction

C'est dans le secteur de la finance que le bouleversement peut être l'un des plus importants. La mise en concurrence des mineurs provoque mécaniquement une baisse des frais de fonctionnement du réseau. Les banques s'en inspirent naturellement pour l'implémenter dans leurs services.

Une automatisation de contrats immuables

Le registre d'une blockchain permet la mise en place de "contrats intelligents" dont les conditions sont fixées à l'avance entre deux tiers. Lorsqu'un événement se produit, le déclenchement de la clause associée est immédiate et transparente. L'instantanéité du réseau peut assurer le versement d'un paiement dans la foulée : on notera l'intérêt de la technologie pour le secteur de l'assurance par exemple.

Un nouveau mode de gouvernance

La mise en place d'un système de vote infalsifiable et ergonomique apparaît comme une application évidente de la blockchain. On peut imaginer une votation sur un projet dont l'allocation des fonds est automatisée lorsqu'un certain seuil est obtenu dans les suffrages (la blockchain permet l'anonymisation de l'individu bien-entendu). Le registre étant public, la corruption est rendu quasiment impossible.

Comment ça marche?

Il est difficile aujourd'hui de trouver une explication claire du fonctionnement de la blockchain sans qu'elle soit mise dans le contexte de la cryptomonnaie, nous pouvons tout de même se baser sur les explications de quantmetry.com pour comprendre le fonctionnement et les parties techniques concernant la blockchain:

Blockchain : fonctionnement du protocole

Ceci est le premier d'une série d'articles sur la technologie blockchain. L'objectif ici est de comprendre dans quelle mesure la technologie blockchain constitue une solution naturelle au problème de transfert d'actifs entre deux agents sans tiers de confiance.

Le Bitcoin, projet d'échange décentralisé et sécurisé d'argent virtuel, est né suite à la crise de confiance de 2008 envers les institutions financières. Son objectif affiché était de se passer des intermédiaires de confiance dont le rôle est de certifier et d'enregistrer l'historique des transactions monétaires, à savoir les banques.

Ce système décentralisé, constitué de milliers d'ordinateurs à travers le monde, représente en quelque sorte un registre public, anonyme et distribué :

- Public car tout le monde peut accéder au contenu du registre sans demande de permission
- Anonyme car chaque utilisateur n'est associé à rien d'autre qu'un ensemble d'adresses alphanumériques contenant des Bitcoins

- Distribué car il n'existe pas d'autorité centrale de certification des transactions.

Le protocole blockchain

Pour comprendre techniquement comment ces trois propriétés s'articulent pour certifier les échanges, considérons deux personnes. Alice et Bob veulent effectuer une double transaction : un transfert d'un actif monétaire (paiement) qui déclenche ensuite un transfert d'un autre type d'actif (envoi par courrier d'un bien, réalisation d'un service, etc.). Nous allons progressivement construire une monnaie digitale dénommée « Infocoin » permettant un échange sécurisé entre les deux agents. Les solutions aux différents obstacles rencontrés nous permettront de montrer en quoi le protocole blockchain constitue une solution « naturelle » au problème de transfert sécurisé de valeur.

Étape 1 : La notion de signature numérique

Alice, qui cherche à transférer un Infocoin à Bob, peut envoyer un fichier texte où elle inscrit « Alice transfère un Infocoin à Bob ». La fragilité d'un tel système est évidente : un tiers autre qu'Alice peut très bien générer un tel fichier, ou bien falsifier le message.
La solution à ce problème passe par l'utilisation d'une signature numérique : Alice hash le texte de départ, le crypte avec la partie privée d'une clef RSA dont elle transfère la partie publique à Bob, ainsi que le message original. Bob, en utilisant la clef publique, décryptera le message, qu'il comparera au message original reçu. Si les deux messages coïncident, alors Bob peut être certain que c'est bien Alice qui a envoyé le message (par principe, seule Alice possède la partie privée de la clef) et que ce dernier n'a pas été falsifié en cours de route (voir Fig. 1).

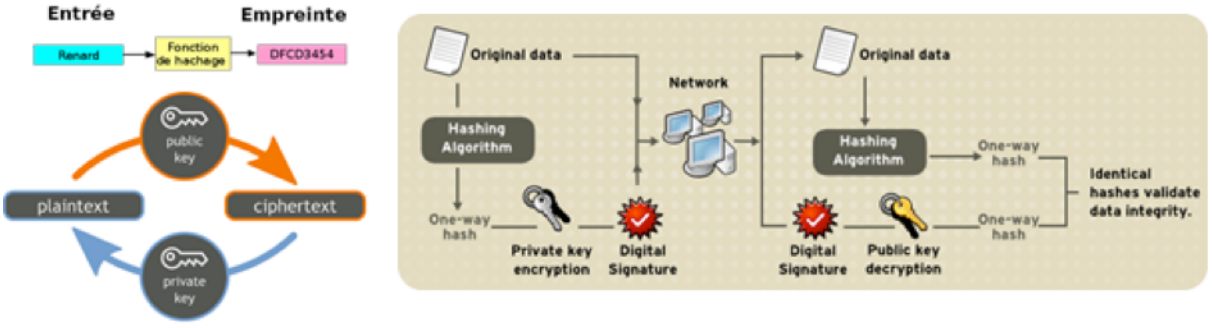

Figure 1 : La notion de signature numérique

Étape 2 : La sérialisation et le registre public

Maintenant que l'identité d'Alice est certifiée, comment éviter qu'elle ne génère abusivement 10 fois le même message, dépensant ainsi des Infocoins qu'elle ne
possède pas ?

- Première solution : on associe un numéro de série à chaque Infocoin pour le rendre unique, un peu comme un billet de banque. Néanmoins, dans le cas de la banque, il

existe une autorité centrale qui certifie les numéros de série et garantit leur unicité, exactement ce que l'on cherche à éviter !

- Deuxième solution : tenir un registre public distribué de la propriété des Infocoins sérialisés. Ainsi, Bob peut vérifier sur sa copie locale du registre que l'Infocoin n°56 appartient bien à Alice. Il diffuse ensuite un message d'acceptation de l'envoi par Alice de cet Infocoin, amenant tous les autres participants à mettre à jour leur copie locale du registre. Le nouvel état du registre, partagé par tous, indiquera donc bien que l'unique Infocoin n°56 du réseau a été transféré d'Alice à Bob.
-

Malheureusement, la vérification de l'unicité de l'Infocoin dépensé par Bob via le registre public s'avère insuffisante si un utilisateur malintentionné exploite la latence du réseau de communication entre les différents participants au système de monnaie digitale pour effectuer des doubles dépenses. En effet, Alice peut diffuser son message deux fois avec deux destinataires différents pour l'Infocoin, Bob et Charlie. Bob, ayant reçu l'Infocoin n°56 d'Alice, vérifiera sur son registre local qu'elle en est bien la propriétaire et diffusera un message de validation de la transaction au reste du réseau. Charlie en fera de même, son message de validation de la transaction étant accepté s'il arrive en premier, et refusé s'il arrive après celui de Bob. Du coup deux versions incompatibles du registre public seront présentes au sein du réseau : une partie des nœuds, qui a reçu la validation de Bob en premier considérera que c'est lui le propriétaire de l'Infocoin n° 56, l'autre partie considérera que c'est Charlie. Le système créé n'est donc pas encore un système viable.
La résolution du problème de la double dépense constitue la challenge le plus important dans la construction d'une monnaie digitale, et nécessite trois étapes supplémentaires qui nous mèneront vers l'architecture technique d'une blockchain.

Étape 3 : La vérification collective

Un premier pas dans la résolution du problème de la double dépense passe par le fait que Bob attende une vérification collective de la propriété de l'Infocoin avant d'envoyer son message de validation de la transaction, qui entraîne une mise à jour des registres. Ainsi, l'envoi de deux messages contradictoires de la part d'Alice entraînera des retours contradictoires à Bob de la part du réseau, d'où une annulation de la transaction.

La question qui se pose avec ce système de validation par 100% des nœuds du réseau est celle de la présence d'agents non-coopératifs, qui peuvent volontairement fausser la validation des transactions de leurs concurrents. Si l'on accorde le privilège de la validation à quelques nœuds uniquement, on abandonne l'objectif d'un système complètement décentralisé, tandis qu'un système basé sur le vote peut facilement être piraté en générant des fausses identités pour les nœuds du réseau.

Étape 4 : La preuve de travail

Imaginons que l'on force les nœuds du réseau à « travailler » et à donner une preuve de leur travail avant de considérer leur retour comme valable. Ce travail peut prendre la forme de la résolution d'un problème mathématique : les nœuds devront fournir la solution à un problème dont la vérification de la validité est simple, comme la résolution d'une équation h(T + N) = 0000…123, avec h une fonction de hachage, T le message de la transaction, N un message aléatoire dénommé « nonce » en anglais, et m 0 au début du membre de droite de l'équation qui est encodé dans un format 16 bits. La recherche d'une solution par force brute nécessiterait de tester 16^m combinaisons pour trouver le N qui convient, tandis que la vérification de la solution N trouvée est très rapide.

Dès qu'un nœud a trouvé une solution N valide, il la diffuse au reste du réseau qui vérifie quasi-instantanément si elle convient ou non en calculant la valeur h(T + N), avec mise à jour de la copie locale du registre si la solution est acceptée. Sachant qu'un calcul coûte de l'argent (possession d'un ordinateur, consommation d'électricité, etc.), on peut inciter les agents à effectuer les calculs en les rémunérant pour chaque transaction validée. Avec quel argent ? C'est là toute la beauté du système Bitcoin ou de ses avatars : on génère un Bitcoin ex nihilo pour justement récompenser le travail de validation d'une transaction.
Ainsi, hormis la masse d'argent initiale créée en même temps que le protocole, la seule façon d'augmenter la masse monétaire en Bitcoins ou en Infocoins est d'effectuer des calculs de validation des transactions. Les travailleurs du réseau sont dénommés les « mineurs », tandis que leur travail est connu sous le nom de « minage ».

Étape 5 : Ordre temporel des blocs

Pour des raisons d'optimisation, on regroupe les transactions dans des blocs à valider, constitués chacun de :

- Un hash de la liste de transactions via une fonction qui fait partie du protocole
- Un timestamp de création du bloc
- Le nonce trouvé par le mineur ayant validé le bloc de transactions
- Le hash du bloc précédent, ce qui constitue une convention de pointage instaurant un ordre temporel entre les blocs

Des techniques d'optimisation du hashage des transactions à regrouper dans le bloc existent, mais nous n'allons pas entrer dans ces détails dans cet article (voir Fig. 2). Le système composé de blocs et de pointages constitue une chaîne ordonnée de transactions, d'où la dénomination « blockchain ».

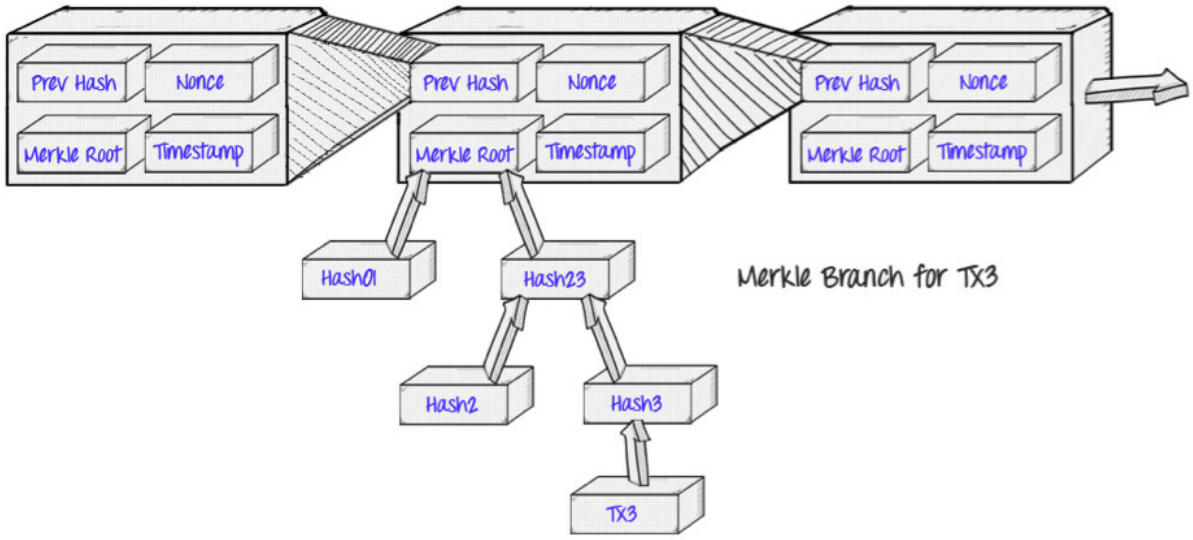

Figure 2 : Ordre temporel des blocs par pointage

Étape 6 : Gestion des bifurcations

Plusieurs blocs étant minés en même temps, une règle d'or est instaurée pour réguler le travail des mineurs : « la branche valide est la branche la plus longue ». Ainsi, des mineurs travaillant sur deux blocs en concurrence doivent cesser leur travail sur le bloc perdant aussitôt qu'un bloc a été validé. Après vérification de la validité du contenu du bloc, ils mettent à jour leur copie locale du registre, avec un pointage qui tient compte de l'arrivée du nouveau bloc.

Que se passe-t-il lorsque deux mineurs finissent en même temps de miner un bloc de transactions ? Il se crée alors ce que l'on nomme une bifurcation : les mineurs continuent à miner le long des deux branches, avec potentiellement des nouvelles sous-branches qui apparaissent dès lors que des nouveaux blocs sont terminés simultanément. Cependant, dès qu'un bloc est terminé avant les autres le long d'une branche qui devient la plus longue,

tous les mineurs vérifient le contenu du bloc puis doivent mettre à jour leur registre local et basculer sur cette nouvelle branche légitime (voir Fig. 3).

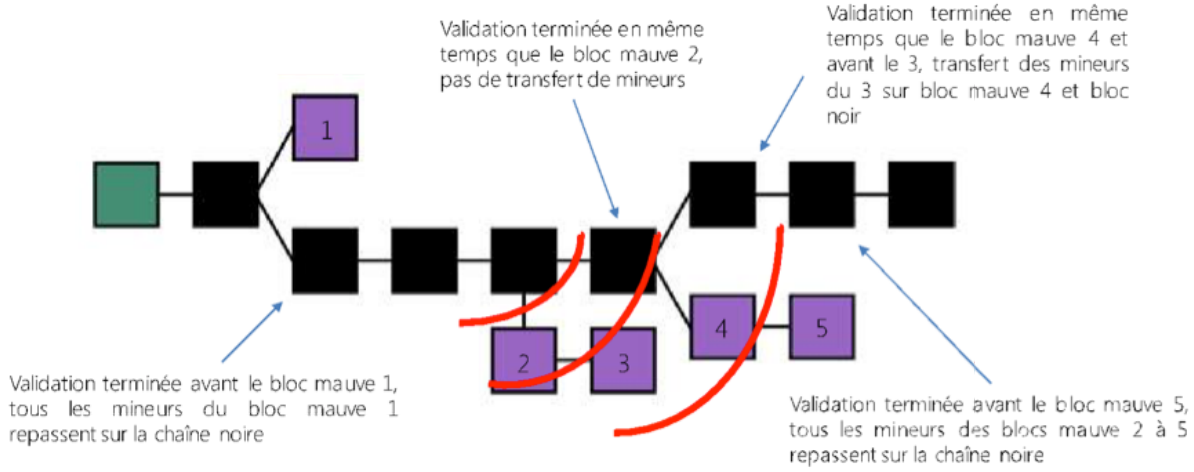

Figure 3 : La gestion des bifurcations dans une blockchain

Vérification de la robustesse du protocole

Analysons maintenant la robustesse de ce protocole.

Imaginons un premier type d'attaque où Alice insère dans un même bloc deux transactions incompatibles, l'une envoyant un Infocoin à Bob, l'autre envoyant le même Infocoin à Charlie. Alice peut alors miner le bloc, avec une vitesse proportionnelle aux capacités de calcul qu'elle possède. Elle peut diffuser ensuite le message de validation au reste du réseau. Néanmoins, ce type d'attaque basique est voué à l'échec car la lecture du bloc par les autres acteurs du réseau montrera clairement qu'il contient deux transactions incompatibles, entraînant ainsi son invalidation.

Deuxième type d'attaque, Alice diffuse deux messages distincts portant sur des transactions incompatibles entre elles à destination de Bob et Charlie. Une bifurcation de minage se crée dans le réseau, mais à terme seule l'une des deux branches sera validée car considérée la plus longue, généralement celle ayant bénéficié des ressources de calcul les plus importantes. Ainsi, Bob ou Charlie saura que sa transaction n'a pas été validée, et l'échange n'aura pas lieu. Attention à un envoi prématuré de la contrepartie : la validation des blocs et les bifurcations étant une information locale, il ne faut pas considérer une transaction fraîchement validée comme fiable, au risque d'être trompé si la branche ayant validé la transaction s'avère non-légitime par la suite car plus courte qu'une autre. D'où une recommandation d'attendre 6 blocs validés suite à celui contenant la transaction lancée avant d'envoyer en toute confiance la contrepartie. En effet, on peut démontrer mathématiquement que la probabilité que plusieurs blocs suite à la bifurcation soit validés simultanément diminue exponentiellement avec le nombre de blocs, tant qu'aucun nœud ne possède plus de 50% de la capacité de calcul du réseau. À titre d'exemple, un bloc nécessite en moyenne 10 minutes pour être validé sur la blockchain Bitcoin, il faut donc généralement attendre une heure après le paiement avant l'envoi de la contrepartie.

Pourquoi la condition sur l'absence d'un nœud avec plus de 50% de la capacité de calcul du réseau ? Ceci nous amène à considérer une dernière attaque, la plus sournoise. Alice émet deux transactions sur le même Infocoin, l'une à destination de Bob, et l'autre à destination d'elle-même. Elle attend que le réseau confirme la transaction avec Bob, et se met à miner une branche qui démarre juste avant le bloc nouvellement validé. La légitimation de sa branche annulerait dans les registres locaux la transaction avec Bob, et si ce dernier a déjà envoyé la contrepartie à la transaction monétaire, il sera arnaqué. Comment Alice peut-elle légitimer la branche qu'elle crée ? Selon la règle d'or, cette branche doit devenir la plus longue. Alice doit donc miner seule sa branche (tous les mineurs honnêtes ont basculé sur la branche contenant le bloc de la transaction avec Bob), et en faire à un moment donné la branche la plus longue. Par définition, elle doit donc posséder strictement plus que 50% de la capacité de calcul du réseau (voir Fig. 4).

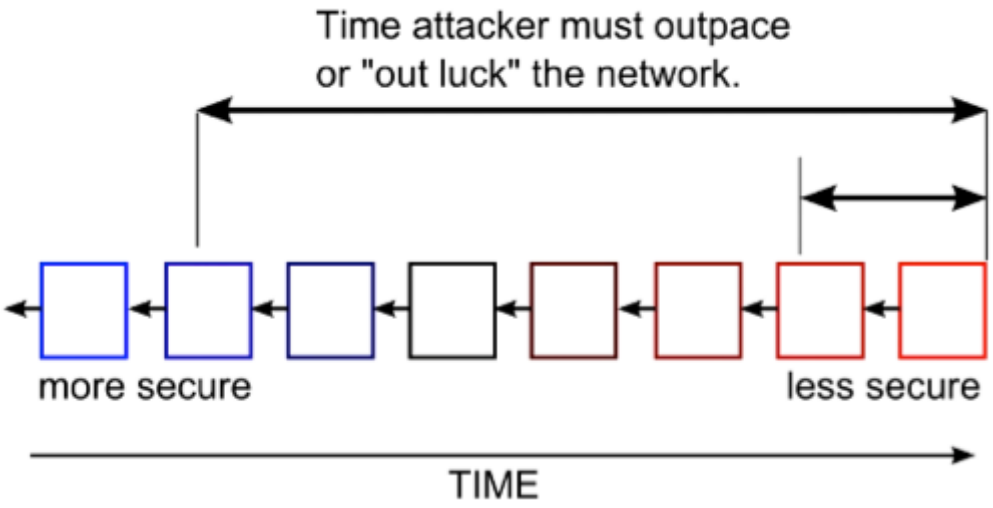

Figure 4 : La course contre-la-montre des fraudeurs

Plus le réseau est grand, plus ce type d'attaque devient difficile à réaliser si les utilisateurs attendent d'obtenir suffisamment de confirmations du réseau pour conclure leurs transactions. Mais difficile ne veut pas dire impossible : un réseau de mineurs a récemment réussi plusieurs dépassements ponctuels de 51% de la capacité de calcul du réseau Bitcoin.
Et voilà ! Nous avons construit étape par étape une monnaie digitale, en montrant en quoi chaque ajout de brique technique constituait une réponse à un type d'attaque spécifique. En conclusion, le protocole blockchain est intéressant en cela qu'il constitue une solution naturelle (chaque brique est nécessaire) et élégante (d'un point de vue algorithmique) au problème de l'échange de valeur sans intermédiaire de confiance.

Le Monde du Jeu Vidéo

Description

Depuis les années 1970 et l'arrivé du jeu vidéo grand public, l'industrie vidéo connaît une forte évolution. En effet, en 2018, 8 générations de consoles se sont déjà succédé apportant toutes plus de performances, de nouveaux concepts et modes de jeu a chaque génération.

Plus que juste un outil de loisir, le jeu vidéo fait maintenant partie intégrante de notre société entraînant l'apparition de nouvelles problématiques sociales, juridiques et culturelles en plus de celles déjà présente dans le domaine.

Les problématiques actuelles

Dans le monde du jeu vidéo, certaines problématiques ont toujours été présentes et demandent une concentration permanente des éditeurs de jeu vidéo pour trouver des solutions à celles-ci.

En effet, avec l'apparition des jeux en lignes, le souci de l'hébergement, de la mise en réseau des joueurs et de réussir à maintenir une certaine stabilité du jeu est au centre des préoccupations. De plus, avec l'évolution des supports, des types de jeu et des moteurs de jeux, la quantité de données a échanger à travers ces réseaux devient de plus en plus grande et ne cesse de grossir de jour en jour. Ce qui implique d'adapter constamment les outils et modes d'hébergement et mise en réseau.

D'autre part, depuis la "démocratisation" des jeux vidéo, les comportements malveillants tels que la fraude, la triche ou le téléchargement illégale de jeux n'ont cessé de se multiplier obligeant les développeurs de jeu vidéo à mettre des moyens en place pour les contrer. L'évolution permanente des méthodes et systèmes de triches et le manque de solution évolutives fiable force les éditeurs de jeux à allouer constamment de nouvelles ressources sur cette problématique.

Avec l'arrivée des système de "microtransaction", "lootbox" ou "in game currency", c'est à dire la possibilité, pour les utilisateurs (joueurs), de dépenser de l'argent pour obtenir des "biens digitaux" dans le jeu (par exemple : de la monnaie, des assets graphiques, un item de jeu aléatoire); on a pu voir apparaître de nouvelles questions juridiques concernant ces "biens digitaux". Par exemple :

- A qui appartient l'item que je viens d'acheter ?
- La lootBox donne un item aléatoire, peut-on considérer ça comme du paris ?
- Doit-on accepter les mineurs dans les jeux vidéo à microtransaction ou lootbox ?
- …

Ces questions étant des problématiques auxquelles les développeurs de jeux vidéo devront avoir la solution dans un futur très proches.

Et enfin, la dernière problématique que nous citerons, et pas des moindres, celle des dépenses des éditeurs de jeux. Puisque depuis l'énorme gain de popularité des jeux vidéo, des plateformes de ventes, hébergement, partage, marché de microstransactions … ont commencé à apparaître et à prendre de l'ampleur, taxant les développeurs de jeux sur toutes les transactions passant par ces plateformes de l'ordre de 1% a parfois plus de 40%. A ces nouvelles dépenses, il ne faut pas oublier la taxation des différents états ou sont vendu les jeux ainsi que les infrastructures à mettre en place et maintenir pour faire fonctionner le système de jeu. Toutes ces dépenses rendent de plus en plus complexe la création de jeu et surtout de pouvoir assurer la rentabilité des structures de développement.

Il y a des nombreuses autres problématiques dans le domaine du jeu vidéo que nous choisissons de ne pas citer puisque nous les trouvons moins pertinentes dans le parallèle avec la blockchain.

Les solutions de la Blockchain

Comme nous l'avons vu précédemment, de nombreuses problématiques du monde du jeu vidéo sont complexes et demande un investissement constant de la part des développeurs de jeux vidéo. Mais, la blockchain, grâce à ses propriétés et son fonctionnement, peut apporter une solution concrète et évolutive aux différentes problématiques que nous avons citées plus tôt.

Idées

Le Real OwnerShip

Ou plus concrètement : posséder "pour de vrai" les biens digitaux achetés dans un jeu, les avatars créés, les objets gagnés ou encore la version digitale du jeu lui-même. Ces informations seraient stockées sur la blockchain, dans le portefeuille (Wallet) du joueur plutôt que sur les bases de données des développeurs de jeu.
Ceci permettrait l'échange, l'achat/vente entre joueur, sans passer par les serveurs du jeu mais aussi de résoudre beaucoup de questionnements juridique à propos de ces "biens digitaux", ou encore de permettre le transfert d'item entre des jeux différents et bien d'autres concepts auxquels nous n'avons pas encore pensé.

Moins de frais

La blockchain étant un système indépendant des états ou d'entreprises et plateformes, si les développeurs décident de passer leurs systèmes d'acquisition uniquement sur la blockchain, ceci réduirait voir supprimerait les taxes appliqué sur leurs contenus et permettrait de rediriger plus de bénéfice directement vers les développeurs.
On peut ajouter à ça la possibilité de réduire ou supprimer les bases de données et serveurs afin de passer uniquement par la blockchain ce qui réduirait de fait les coûts liés aux infrastructures.

Sûreté des données

La blockchain permet de stocker et échanger les données de manière sûre, sans possibilité d'altération, authentifier. Cette sûreté qu'apporte la blockchain pourrait permettre au monde du jeu vidéo de résoudre ses problèmes de fraudes et triches en plus de renforcer la confiance des joueurs vis à vis des développeurs. En effet, sans possibilité d'altération et avec les vérifications effectuées sur la blockchain, la fraude ou la triche seraient impossibles

à réaliser; et , dans le cas ou une tentative réussirait, la partie authentifier de la blockchain permettrait de connaître automatiquement l'auteur des faits afin de corriger et sanctionner instantanément.

Décentralisation

Le système de base de la blockchain fonctionne sur un réseau pair to pair (P2P). Ceci étant, l'idée de faire reposer un jeu vidéo sur la blockchain et donc sur ce réseau P2P n'est pas impossible. Cette idée permettrait la décentralisation des jeux en réseaux et la disparition des serveurs de jeu pour reposer entièrement sur le réseau de la blockchain. Ceci permettrait d'une part une réduction des coûts comme mentionnée précédemment; mais aussi l'amélioration de la qualité de vie des joueurs puisque cela supprimerait les fermetures de serveurs pour maintenance, les problèmes de surcharges et tout autre soucis liés aux limites des serveurs.

De nombreuses possibilités

On peut imaginer dans quelques années de nouvelles possibilités apporté par la blockchain au monde du jeu vidéo. Par exemple de nouveaux concept de gameplay basé sur les caractéristiques que permet la blockchain (exemple : l'unicité des items permet de les faire évoluer en fonction des joueurs qui l'utilisent et des action qu'ils font avec). Ou même de nouveaux genre de jeu, de nouveaux genre de joueurs …
Tout ceci dépendra de l'utilisation qu'en feront les futurs développeurs de jeux.

Exemples

La blockchain commence déjà à faire son apparition dans le monde du jeu vidéo, au travers de petits jeux simples basé sur la technologie, de groupes d'éditeur et de développeur qui se rassemble pour faire avancer le concept ou encore de technologies qui se préparent à cette possible utilisation dans le jeu vidéo.

Des jeux

Des groupes

Conclusion

Comme nous avons pu le voir, l'utilisation de la blockchain dans le monde du jeu vidéo pourrait permettre d'avancer énormément et de résoudre de manière définitive certaines problématiques de ce domaine et lui serait bénéfique.

Mais, bien que l'utilisation de la blockchain commence à apparaître dans le monde du jeu vidéo, son utilisation n'est pas encore totalement possible et la plupart des applications possible ne sont pas encore applicable dans des conditions réelles. Principalement parce que la blockchain n'a pas été faite de base pour le jeu vidéo et est de fait, en l'état, trop lente (dans l'exécution) et trop lourde à mettre en place pour créer un jeu complet entièrement basé sur la blockchain.

A ces contraintes technique s'ajoute les "envies" et "frayeurs" des deux mondes. Le monde du jeu vidéo n'a pas envie de s'engager entièrement dans la blockchain sans certitude que cela va vraiment fonctionner. Et de l'autre côté les développeurs de technologies blockchain ne veulent pas commencer à développer leurs technologies pour qu'elles correspondent aux attentes du monde du jeu vidéo sans la certitude qu'elles auront du succès auprès d'eux.

Malgré ces freins, l'idée se développe de petit à petit et de plus en plus de contenu sont créés autour de ce concept. Les idées sont donc en train d'évoluer et on pourrait peut être observer d'ici quelques années un changement de tendance et l'apparition de gros studios de jeux vidéo travaillant avec la blockchain.