

# Jeux video multijoueur en ligne : application basée sur la technologie blockchain

Encadrant : M. Potop-Butucaru,

Etudiants : A. Atsain, I. Boubrik, M. R. Kadri, D. Phan

## Table des matières

<b>1</b>	<b>Cahier des charges</b>	<b>2</b>
1.1	Exigences fonctionnelles et exigences non-fonctionnelles . . . . .	2
1.2	Contraintes Technique . . . . .	3
<b>2</b>	<b>Plan de développement</b>	<b>4</b>
<b>3</b>	<b>Bibliographie</b>	<b>5</b>
<b>4</b>	<b>Analyse</b>	<b>9</b>
4.1	Introduction . . . . .	9
4.2	Architecture des jeux vidéos multijoueurs en ligne . . . . .	9
4.3	Blockchain . . . . .	11
4.3.1	Présentation . . . . .	11
4.3.2	Les jeux vidéos et la Blockchain . . . . .	12
<b>5</b>	<b>Conception</b>	<b>13</b>
<b>6</b>	<b>État d'avancement</b>	<b>16</b>

# 1 Cahier des charges

Le projet a pour objectif de mettre en œuvre un service basé sur l'architecture présentée dans le document [1], permettant la création d'un jeu en ligne utilisant la technologie blockchain. Il est important de noter que le choix du service pourrait être sujet à des modifications après la publication de ce rapport. L'évaluation se concentrera principalement sur les exigences fonctionnelles du service à implémenter.

## 1.1 Exigences fonctionnelles et exigences non-fonctionnelles

Cette section est dédiée aux exigences fonctionnelles :

### 1. En ce qui concerne les données

- La blockchain stocke publiquement et de manière immuable les données échangées entre les services, avec un accès public, une impossibilité de modification, et une structure en blocs numérotés.
- Pour automatiser les communications au sein de la blockchain, il sera nécessaire d'implémenter des smart contract chargés de gérer ces échanges de manière automatique.

### 2. En ce qui concerne la mise en œuvre du service

- Le service doit être en mesure d'établir des communications avec d'autres services spécifiques définis dans l'architecture :
  - Il doit pouvoir approuver ou rejeter un smart contract en fonction des données reçues. Un service sans exigence de signature ne devrait ni approuver ni refuser le contrat (le simple fait de le posséder constitue déjà une anomalie).
  - Il doit seulement traiter des données qui sont attribuées à son service.
  - Il doit être en mesure de transmettre un smart contract au service destiné.
  - Seul le service Vérification, à le droit de valider définitivement une smart contract et d'écrire sur la blockchain
- Les échanges doivent être sécurisés, et pour ce faire, ils seront automatisés à l'aide des smart contracts, une technologie associée à la blockchain.

Dans le cadre de notre projet, les différentes exigences non-fonctionnelles que nous avons identifiées sont les suivantes :

- Performance : Le module doit être capable de traiter efficacement et rapidement plusieurs requêtes provenant d'un service "entrant".
- Sécurité : Il est impératif d'assurer la sécurité des communications entre les divers services existants, car c'est l'objectif fondamental de l'architecture présentée.

## 1.2 Contraintes Technique

La concrétisation de ce projet nécessitera l'utilisation de technologies spécifiques. Nous avons ainsi approfondi nos connaissances sur les blockchains, y compris les smart contracts qui leur sont associés.

## 2 Plan de développement

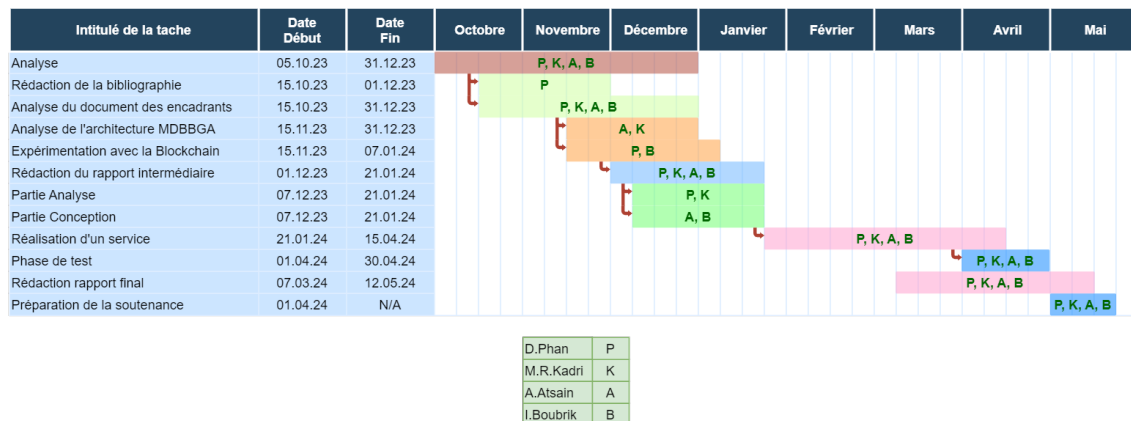


FIGURE 1 : Diagramme de Gantt du projet

Pour pouvoir mener à bien ce projet, il nous était indispensable d'analyser les termes de notre sujet pour pouvoir réaliser une bibliographie adaptée à nos besoins, et mieux comprendre et analyser le document Blockchain-based Massively Multiplayer Online Game framework and Modular decentralized blockchain-based game architecture. Ce document nous a été remis par les encadrants, notre première tâche a été de le comprendre et de présenter ses éléments aux encadrants.

Par la suite, avec les données que nous avons, nous avons effectué des recherches plus approfondies sur l'architecture MDBBGA ainsi que sur des expérimentations sur la blockchain.

Avec toutes ces données, nous avons pu commencer la rédaction de notre rapport intermédiaire. Nous nous sommes donc partagés les tâches pour être plus efficace, tout d'abord Kadri et Phan se sont occupés de la partie bibliographie, analyse pendant que Atsain et Boubrik se sont occupés de la partie conception.

Pour la suite du projet, en ayant choisi un service, il nous faudra donc le réaliser. La réalisation du service s'effectuera, suivie de la phase de test qui nous donnerons assez d'éléments pour rédiger notre rapport final et préparer notre soutenance.

### 3 Bibliographie

Cette partie a pour but de présenter les bibliographies utilisées dans le cadre de notre projet, divisé en trois parties distinctes. La première section explore "l'architecture des jeux en ligne", suivie de "la blockchain" et enfin "la sécurité et les méthodes de triche". L'objectif principal est de fournir des résumés concis de chaque bibliographie, offrant ainsi une compréhension ciblée dans le contexte de notre sujet (jeux vidéos et blockchain).

La bibliographie est une liste organisée des sources documentaires, telles que des livres, articles ou autres références, utilisées ou citées dans le cadre d'un travail académique ou d'une recherche. Elle offre une trace structurée des ressources consultées pour soutenir les informations présentées dans le document. Notez que des modifications peuvent être apportées à cette dernière entre le rendu intermédiaire et le rendu final.

Les références bibliographiques suivantes offrent une réponse préalable aux projets qui nous ont été assignés, à savoir "les jeux vidéo et la blockchain". Elles visent à élaborer une architecture adaptée pour les jeux en ligne intégrant la blockchain en tant que technologie, tout en utilisant les smart contracts pour automatiser divers services. L'objectif est de préciser les raisons justifiant l'utilisation de cette architecture, son applicabilité aux jeux en ligne, ainsi que les avantages et inconvénients associés à cette approche.

La première section vise à analyser les termes du sujet "blockchain et jeux en ligne" et à élaborer une architecture appropriée pour les jeux en ligne. Les articles devront présenter ou orienter vers une architecture adéquate, identifier les éventuels défauts, et proposer des solutions le cas échéant.

Ce premier article introduit une architecture destinée aux jeux MMOG (Massively Multiplayer Online Game). Il propose une initiation au sujet en exposant une architecture de base, tout en explorant les contraintes imposées par le choix d'un jeu en ligne et les diverses contraintes qui en découlent. De plus, l'article aborde des architectures adaptées aux jeux vidéo, ce qui confère une pertinence directe à notre champ d'étude.

[2] ->Architecture pour les jeux MMOG

Le deuxième article expose une architecture intégrant la blockchain en tant que technologie. Il examine les avantages et inconvénients de l'utilisation de cette technologie au sein de l'architecture. Ce document s'inscrit également dans le contexte de notre étude, puisqu'il aborde les jeux en ligne et explore le marché des jeux mobiles.

[3] ->Architecture basée sur la blockchain

Ce document réalise une analyse approfondie de l'architecture peer-to-peer et met en lumière ses avantages et inconvénients dans le contexte des jeux MMOG. Il souligne

également sa nature évolutive. De plus, le document expose les principaux défauts de cette architecture en les classifiant.

[4] ->Architecture P2P pour les jeux MMOG

Ce document expose les lacunes des architectures existantes en les classant selon leurs problèmes pour une analyse approfondie. En complément, le document suivant propose des solutions aux problèmes évoqués précédemment en utilisant les blockchains comme espace de stockage. Cette approche renforce la sécurité des caractéristiques clés d'une architecture P2P traditionnelle, répondant ainsi aux besoins spécifiques des jeux de type MMOG.

[5] ->Solution pour les problèmes d'une architecture P2P

[6] ->Architecture P2P avec espace de stockage en blockchain

Le document à suivre propose des instruments pour définir la portée d'application d'une architecture P2P dans un domaine donné. Cela facilite la délimitation des éléments nécessaires et applicables, distinguant ainsi ceux qui ne le sont pas.

[7] ->Approche pour déterminer un couvrage des types de jeux pour la blockchain

La seconde section a pour objectif d'examiner de manière approfondie la solution proposée, à savoir une architecture Peer-to-Peer intégrant la blockchain en tant qu'espace de stockage. L'analyse se concentrera sur la pertinence de l'utilisation de la blockchain dans le contexte des jeux vidéo, en mettant en lumière les avantages potentiels tels que l'intégration de smart contract. De plus, cette partie abordera les méthodes de triche dans les jeux en ligne, mettant ainsi en évidence les vulnérabilités potentielles de cette architecture..

Le document initial effectue une classification en quatre niveaux et établit un consensus entre le réseau et l'application de la blockchain. L'objectif de cette classification est de mettre en évidence les points faibles tout en fournissant des orientations pour remédier à ces faiblesses.

[8] ->Présentation de la blockchain, de ses domaines d'application, etc...

En utilisant le document suivant, une comparaison est établie entre les différentes blockchains existantes avec leurs algorithmes de consensus. Cela permet de les classer par ordre de préférence en fonction de chaque type de jeu MMOG et d'utiliser cette classification pour réaliser des analyses.

[9] ->Etude des différents types de blockchain et comparatifs

Le document suivant effectue une analyse détaillée des diverses formes de blockchains, classant à la fois leurs performances et les modèles qu'elles établissent. Grâce à cette analyse, il devient possible de développer une technique pour résoudre le problème lié à l'utilisation d'une blockchain spécifique.

[10] ->Analyse des performances des systèmes basés sur la blockchain

Le document suivant présente une architecture et diverses applications de la blockchain dans l'industrie des jeux vidéo. Bien que l'accent principal soit mis sur l'utilisation de la blockchain dans les jeux vidéo, le document explique également en détail l'architecture associée. Ce document sert principalement de complément aux autres document associés à la blockchain ou encore l'architecture du jeu en ligne.

[11] ->Application de la blockchain dans le domaine des jeux vidéos

La section suivante examine et expose diverses vulnérabilités observables liées à l'utilisation des smart contracts. De plus, elle présente un exemple d'attaque dirigée contre les smart contract. Le document propose également une méthode de détection des vulnérabilités des smart contract appelée le modèle SCVSN (Smart Contract Vulnerability Detection Model Based on Siamese Network). Ce modèle définit des étapes pour évaluer la sécurité des smart contract, suivies d'une analyse approfondie de la performance de ce modèle.

[12] ->Vulnérabilité des smart contract

Les deux livres suivants servent de ressources pour la blockchain et les smart contracts. Ils sont des guides pédagogiques pour mettre en œuvre des smart contracts avec la technologie Ethereum, offrant un support tant pour la phase de développement que pour la compréhension de leur implémentation.

[13] ->Implémenter des smart contract avec Ethereum et Solidity

[14] ->Implémenter des smart contract avec Solidity pour un système décentralisé

Le document qui suit effectue la mise en œuvre d'un jeu au tour par tour en utilisant une architecture Peer-to-Peer. Il aborde la recherche de parties, le déroulement d'une partie et la synchronisation entre les utilisateurs du jeu. Le jeu est conçu avec un système anti-triche, et l'ensemble de cette présentation peut servir de support à la blockchain.

[15] ->Exemple d'un jeux de stratégie en ligne utilisant de la blockchain

Ce document examine une nouvelle méthode de consensus sur les blockchains fondée sur le protocole Brlittle (BCP), qui est employé pour soutenir un écosystème de jeux MMOG. Il propose une analyse approfondie du protocole BCP ainsi que des travaux précédents dans ce domaine. Les algorithmes de BCP sont également présentés, accompagnés d'une

simulation permettant d'observer le fonctionnement de cet algorithme.

[16] ->Présentation d'un exemple de support pour les jeux de type MMOG

Le document suivant expose les désavantages associés à l'utilisation d'une architecture Peer-to-Peer et vise à identifier ses vulnérabilités, offrant ainsi des pistes pour résoudre ces problèmes de sécurité. Un document ultérieur aborde spécifiquement ces questions de sécurité dans le contexte d'une architecture Peer-to-Peer. Il présente les aspects sécurisés permettant de défendre cette architecture contre des attaques telles que le DDoS. De plus, il analyse cette nouvelle architecture en restreignant son domaine de détection des fraudes.

[17] ->Sécurisé une architecture P2P

[18] ->Blockchain contre la triche dans les jeux en ligne

Ce document examine en détail les différentes méthodes de triche couramment employées dans les jeux MMOG et les catégorise. Cette classification a pour but de simplifier l'identification des vulnérabilités spécifiques au genre de jeu sélectionné pour l'implémentation, tout en suggérant des solutions potentielles pour contrer ces diverses méthodes de triche.

[19] ->Analyse des méthodes de triche

Le document final propose une nouvelle approche exploitant la blockchain comme technologie pour résoudre les multiples problèmes de sécurité découlant des jeux en ligne et de l'utilisation de l'architecture Peer-to-Peer. Des technologies telles que les contrats intelligents sont employées pour les éléments critiques, et deux méthodes de transfert sont mises en œuvre pour sécuriser les transactions. Ce document met en évidence les solutions élaborées et démontre des performances supérieures à celles d'une architecture classique.

[20] ->Architecture P2P utilisant de la blockchain pour lutter contre la triche dans les jeux en ligne



## 4 Analyse

### 4.1 Introduction

Dans les jeux vidéo modernes, l'aspect multijoueurs et sa fiabilité joue un rôle crucial dans l'expérience des joueurs. Les architectures classiques utilisées pour ce mode sont centralisées et sont donc confrontées à des défis en matière d'évolutivité et de sécurité, en particulier avec la croissance de la base de joueurs et de la complexité des interactions dans le jeu. Dans cette partie Analyse, nous allons examiner le potentiel de la technologie blockchain pour les jeux multijoueurs avec les modèles Peer-to-peer basés sur la blockchain afin de résoudre les problèmes d'évolutivité et à renforcer la sécurité des jeux vidéo et en particulier les MMO (Massively Multiplayer Online).

### 4.2 Architecture des jeux vidéos multijoueurs en ligne

Un jeu vidéo est un jeu électronique qui permet au joueur d'interagir avec un environnement virtuel à travers des interfaces homme-machine (Manette, souris, etc.) et de générer une réponse visuelle, auditive ou haptique sur une interface de sortie adapté (Écran, casque audio, etc.). Il existe différentes catégories de jeux vidéo, chacun offrant des styles de jeu et de narration distincts : action, aventure, jeu de rôle, simulation, sport, stratégie, etc. Chaque catégorie présente des défis et des objectifs uniques, qui définissent l'expérience du joueur dans le monde virtuel.

De nombreux jeux vidéo proposent des modes multijoueurs, permettant la participation simultanée de plusieurs joueurs, qu'ils fassent partie de la même équipe ou de l'équipe adverse, ou qu'ils agissent en solo. Les expériences multijoueurs peuvent être classées en deux styles différents : Joueur contre Joueur ou PvP (De l'anglais "Player vs Player") et Joueur contre l'Environnement ou PvE (De l'anglais "Player vs Environment"). En PvP, les joueurs s'affrontent entre eux, tandis qu'en PvE, ils coopèrent contre les PNJ (Personnages Non-Joueurs) contrôlés par l'IA (Intelligence Artificielle) du jeu.

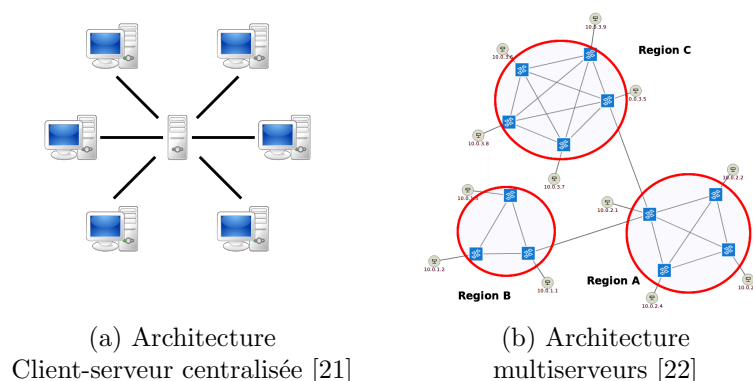


FIGURE 2

Pour l'implémentation du mode multijoueur, l'approche la plus répandue au début était l'architecture client-serveur. Celle-ci consiste à utiliser un seul serveur central chargé d'héberger le monde virtuel du jeu, de gérer les interactions entre les joueurs et les événements du jeu et d'assurer la synchronisation de tous les clients connectés. Bien qu'elle soit efficace pour les jeux dont la population est réduite, ce type d'architecture rencontre des problèmes d'évolutivité à mesure que la popularité du jeu augmente. Le serveur central peine à gérer efficacement la demande croissante, entraînant des problèmes de lag, de latence et une dégradation générale de l'expérience de jeu. En plus, de par sa nature centralisée, ce type d'architecture est vulnérable aux attaques de déni de service (Distributed Denial of Service ou DDoS). Les développeurs de jeux ont donc opté pour des architectures multiserveurs qui consiste à répartir les fonctionnalités du jeu sur plusieurs serveurs, dont chacun s'occupe d'une région ou d'une fonction spécifique. Bien que cela permette de résoudre certains problèmes d'évolutivité, elle introduit des complications telles que le verrouillage géographique (Region lock) des clients et l'augmentation des coûts opérationnels.

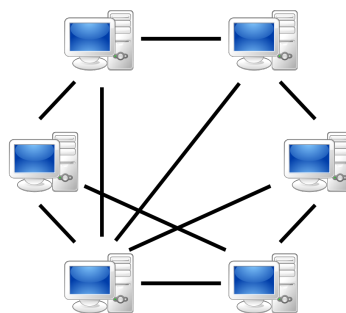


FIGURE 3 : Architecture Peer-to-peer [21]

Pour venir à bout de ces limitations, nous avons enfin l'architecture Peer-to-Peer (P2P). Il s'agit d'un système décentralisé dans lequel les joueurs communiquent directement entre eux plutôt que de dépendre d'un serveur central. Si les architectures P2P offrent des avantages tels qu'une meilleure évolutivité et moins de dépendance à l'infrastructure des serveurs, elles posent également des problèmes, notamment dans le contexte de la sécurité. L'absence d'une autorité centrale pour superviser les événements en jeu rend les systèmes P2P vulnérables à la triche.

En effet, certains joueurs cherchent souvent à obtenir un avantage déloyal ou à manipuler l'environnement du jeu pour influencer les mécanismes du jeu. Les méthodes de triche les plus courantes consistent à utiliser des logiciels tiers, à exploiter des bugs dans le jeu ou à s'engager dans des pratiques contraires aux règles du jeu. Il est possible de

classer ces attaques par type d'attaque comme suggéré par Yahyavi et al.[4] : Interruption de la dissémination de l'information, action illicite en jeu ou accès non autorisé aux informations. Mais aussi, au niveau auquel elles interviennent, comme suggéré par Webb et al. [23] : au niveau du jeu, au niveau du programme (Application), au niveau des protocoles ou au niveau de l'infrastructure.

Une solution pour remédier à ce problème est de combiner l'architecture P2P avec la technologie de la Blockchain. Celle-ci pourrait constituer un registre transparent et inaltérable pour stocker les événements du jeu. En utilisant la blockchain pour stocker les données cruciales du jeu, nous renforçons la sécurité en créant un environnement transparent qui réduit considérablement le risque de Triche.

### 4.3 Blockchain

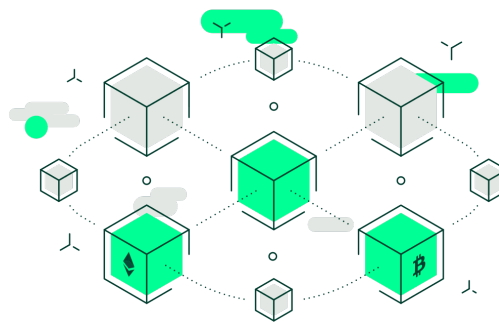


FIGURE 4 : (Illustration à changer)

#### 4.3.1 Présentation

La technologie blockchain est un système de registre décentralisé et distribué qui révolutionne l'enregistrement des transactions à travers un réseau informatique en toute transparence et sécurité. Au-delà du domaine des crypto-monnaies, diverses plateformes de blockchain offrent des caractéristiques uniques. Ethereum, par exemple, facilite les applications décentralisées (DApps) et les contrats intelligents (smart contracts), introduisant de la programmabilité dans la blockchain. Parmi les autres plateformes de blockchain dignes d'intérêt, citons Binance Smart Chain (BSC), conçue pour des applications décentralisées très performantes, et Polygon, qui met l'accent sur l'évolutivité et l'interopérabilité, et qui est compatible avec Ethereum. Les algorithmes de consensus jouent un rôle crucial en garantissant le consensus du réseau sur la validité des transactions. Bitcoin s'appuie sur la preuve de travail (Proof of Work ou PoW), où les nœuds effectuent des calculs complexes pour valider les transactions, tandis qu'Ethereum passe à la preuve d'enjeu (Proof of Stake ou PoS), un modèle basé sur la mise en jeu de crypto-monnaie par les validateurs en guise de garantie.

### 4.3.2 Les jeux vidéos et la Blockchain

L'utilisation la plus populaire de la technologie Blockchain est dans le domaine des finances et des paiements avec des monnaies numériques bien connues comme Bitcoin, Ethereum, Tether, Solana, etc. Et ce, en raison de la transparence, de l'immuabilité et de la décentralisation de son système qui n'est contrôlé par aucune entité centrale, ce qui renforce la confiance parmi les utilisateurs.

Toutefois, une autre utilisation possible de cette technologie serait, comme mentionné précédemment, dans les jeux vidéo en ligne, plus particulièrement les jeux MMO, où certains développeurs ont déjà incorporé la technologie Blockchain dans leurs jeux. Cette technologie peut être employée pour sécuriser la propriété et les transactions des ressources dans le jeu, empêcher la fraude et la triche et garantir la transparence. De plus, la blockchain facilite les échanges et la monétisation des biens virtuels entre les différentes plateformes de jeu pour les utilisateurs.

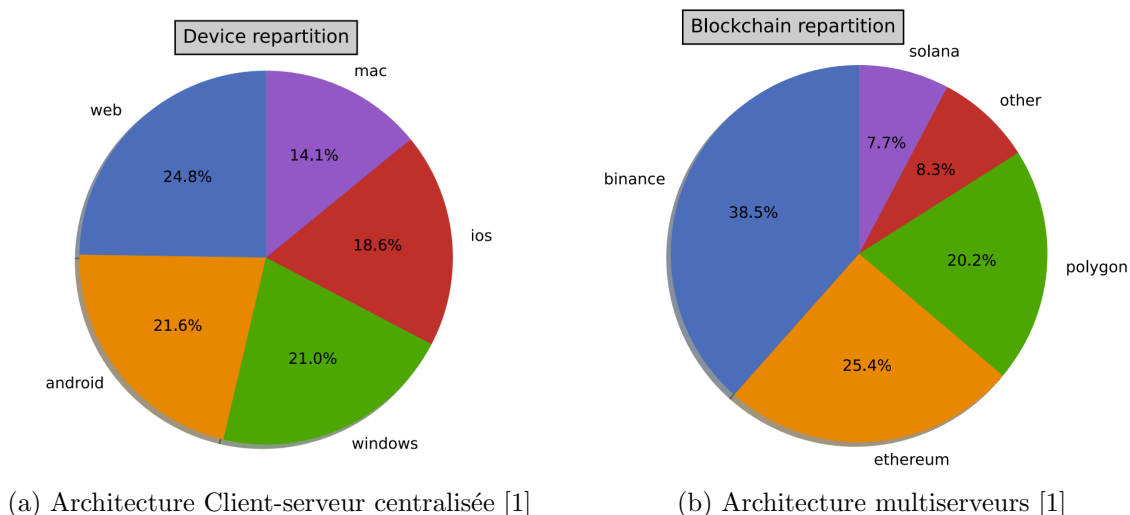


FIGURE 5

Les jeux basés sur la blockchain occupent un espace considérable sur diverses plateformes; les plateformes Web, Windows et Android étant les plateformes privilégiées pour ce type de jeux comme l'illustre la figure 4(a). En ce qui concerne les blockchains les plus utilisées, Binance arrive en tête de file, suivie par Ethereum, Polygon et solana, comme le montre la figure 4(b). Les genres de ces MMO sont variés, on y trouve des jeux de rôle (RPG), des jeux de stratégie, des jeux de collection, etc.

## 5 Conception

Architecture P2P basée sur la technologie Blockchain, en particulier Ethereum, pour l'implémentation d'un jeu multijoueur en utilisant les smart-contracts. Le réseau pair-à-pair, ou peer-to-peer (P2P) en anglais, est un modèle de réseau informatique qui s'appuie sur internet, où chaque ordinateur sert à la fois d'émetteur (il distribue les données numériques) et de récepteur (il reçoit les données numériques). Certains l'utilisent pour partager des vidéos ou des documents audio (album de musique), mais aussi pour effectuer des transactions monétaires. L'échange pair-à-pair entre plusieurs utilisateurs s'effectue sans autorité centrale, c'est-à-dire qu'aucune autorité ne contrôle cet échange. Les internautes s'exposent à des sanctions pénales et financières lorsqu'ils partagent des fichiers dont ils ne disposent pas des droits.

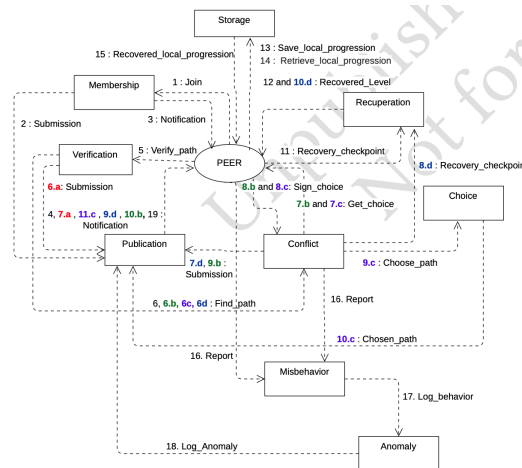


FIGURE 6

Ce jeu propose différents services aux utilisateurs, pour leur permettre de vivre de belles expériences. Parmi ces services, nous trouverons : Membership, Verification, Publication, Conflict, Choice, Recupération, Misbehavior, Anomaly, Application, Storage. Mais seulement 8 d'entre eux sont des services essentiels et deux optionnels. Les services essentiels sont Membership, Verification, Publication, Conflict, Choice, Recupération, Misbehavior et Anomaly. Nous allons donc nous concentrer sur ceux là.

- **Membership** : Permet à l'utilisateur de pouvoir se créer un compte lors de sa première connexion et d'obtenir deux identifications avec lesquelles il pourra se connecter à chaque fois qu'il voudra jouer, un identifiant user et un identifiant game, lui permettant par la suite de jouer à plusieurs parties.

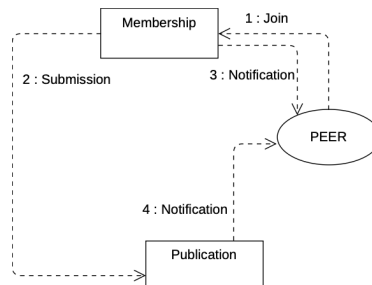


FIGURE 7

- **Verification** : Permet de vérifier si l'utilisateur est légitime à passer au niveau suivant. Si les conditions nécessaires au passage de niveau supérieur sont remplies, si elles sont remplies, on passe au service Publication sinon au service Conflict qui résoudra le problème.

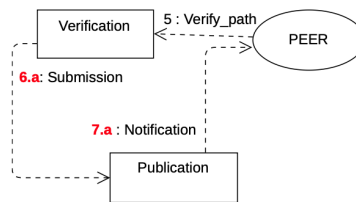


FIGURE 8

- **Publication** : Le seul service autorisé à écrire sur la blockchain, ainsi que le seul à avoir la capacité de mettre à jour l'état de la partie. Le service écrit à la blockchain le résultat de la demande du client, en l'occurrence si le niveau a été passé et notifie les pairs de cette nouvelle information qui doit être mise à jour.
- **Conflict** : C'est le service utilisé pour résoudre le problème.

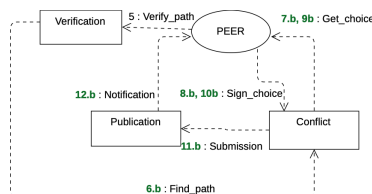


FIGURE 9

- **Choice** : Un pair décide de donner le choix du chemin qu'il va prendre à la blockchain.

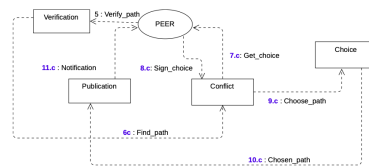


FIGURE 10

- **Recuperation** : Permet de récupérer un précédent état de jeu. L'état de jeu à récupérer est `recovered_path` et se trouve à `recovery_checkpoint_location`.

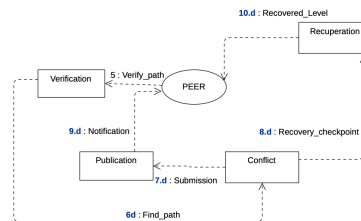


FIGURE 11

- **Misbehaviour** : Ce service peut être appelé par un pair directement ou par le service Conflict. Son but est de compiler toutes les demandes de comportement faites.

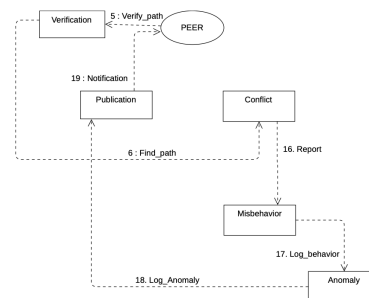


FIGURE 12

- **Anomaly** : Sert de filtre pour effectuer la différence entre une vraie attaque Byzantine et une fausse vraie attaque.

Après avoir étudié tous les services disponibles dans le document Blockchain-based Massively Multiplayer Online Game framework and Modular decentralized blockchain-based game architecture, nous avons décidé de nous concentrer sur le service Verification qui dont l'implémentation nous semble la plus intéressante.

## 6 État d'avancement

### 6.1 Analyse du document : Blockchain-based Massively Multi-player Online Game framework and Modular decentralized blockchain-based game architecture

Ce document se divise en deux parties distinctes : la première concerne l'analyse et la présentation d'une architecture adaptée aux jeux en ligne, tandis que la seconde aborde les différents algorithmes liés à l'architecture Peer-to-Peer, avec la blockchain comme espace de stockage.

### 6.2 Recherche de failles ou améliorations possibles dans l'architecture présentée

En examinant attentivement l'architecture **MDBBGA** proposée dans le document analysé précédemment [1], nous avons relevé quelques potentielles vulnérabilités et amélioration que nous allons adresser lors de la phase de réalisation de ce projet. En particulier dans le service "Verification" où, du fait que l'avancement à l'intérieur du niveau ne soit enregistré qu'en local et envoyé vers ce service que lors du passage au niveau suivant, il serait possible aux joueurs de partager leur progression et de permettre à d'autres d'avancer au niveau suivant ou d'obtenir des éléments en jeu sans y avoir réellement joué. (+ Amélioration potentielle)

### 6.3 Expérimentation avec les smart contracts

Pour mener à bien nos expérimentations, nous avons choisi d'utiliser l'IDE **REMIX**, qui propose un environnement en ligne permettant la création, la modification et le déploiement de contrats intelligents basés sur la technologie de la blockchain. Cet outil est spécifiquement conçu pour être utilisé avec Ethereum. L'objectif de nos expériences était d'observer le comportement des contrats intelligents, leurs objectifs et les avantages qu'ils peuvent apporter à la technologie de la blockchain.



## Références

- [1] Chan Yip Hon Boris. Blockchain-based Massively Multiplayer Online Game framework and Modular decentralized blockchain-based game architecture. 2017.
- [2] Mohsen Ghaffari, Behnoosh Hariri, Shervin Shirmohammadi, and Dewan Tanvir Ahmed. A Dynamic Networking Substrate for Distributed MMOGs. *IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING*, 3(2) :289–302, June 2015. Num Pages : 14 Place : Piscataway Publisher : Ieee-Inst Electrical Electronics Engineers Inc Web of Science ID : WOS :000209845800014.
- [3] Raphael Burkert, Philipp Horwat, Rico Luetsch, Natalie Roth, Dennis Stamm, Fabian Stamm, Jan Vogt, and Marc Jansen. Decentralized Online Multiplayer Game Based on Blockchains. In J. Prieto, A. Partida, P. Leitao, and A. Pinto, editors, *BLOCKCHAIN AND APPLICATIONS*, volume 320, pages 44–53, Cham, 2022. Springer International Publishing Ag. ISSN : 2367-3370, 2367-3389 Num Pages : 10 Series Title : Lecture Notes in Networks and Systems Web of Science ID : WOS :000792443800005.
- [4] Amir Yahyavi and Bettina Kemme. Peer-to-Peer Architectures for Massively Multiplayer Online Games : A Survey. *ACM COMPUTING SURVEYS*, 46(1) :9, October 2013. Num Pages : 51 Place : New York Publisher : Assoc Computing Machinery Web of Science ID : WOS :000327453300009.
- [5] Sarmad A. Abdulazeez, Abdenmour El Rhalibi, Madjid Merabti, and Dhiya Al-Jumeily. Survey of Solutions for Peer-to-Peer MMOGs. In *2015 INTERNATIONAL CONFERENCE ON COMPUTING, NETWORKING AND COMMUNICATIONS (ICNC)*, pages 1106–1110, New York, 2015. IEEE. Num Pages : 5 Web of Science ID : WOS :000380557400201.
- [6] Ho Yin Yuen, Feijie Wu, Wei Cai, Henry C. B. Chan, Qiao Yan, and Victor C. M. Leung. Proof-of-Play : A Novel Consensus Model for Blockchain-based Peer-to-Peer Gaming System. In *BSCI '19 : PROCEEDINGS OF THE 2019 ACM INTERNATIONAL SYMPOSIUM ON BLOCKCHAIN AND SECURE CRITICAL INFRASTRUCTURE*, pages 19–28, New York, 2019. Assoc Computing Machinery. Num Pages : 10 Web of Science ID : WOS :000848505900003.
- [7] Emanuele Carlini, Laura Ricci, and Massimo Coppola. Integrating centralized and peer-to-peer architectures to support interest management in massively multiplayer on-line games. *CONCURRENCY AND COMPUTATION-PRACTICE & EXPERIENCE*, 27(13) :3362–3382, September 2015. Num Pages : 21 Place : Hoboken Publisher : Wiley Web of Science ID : WOS :000360178400012.
- [8] Mingli Wu, Kun Wang, Xiaoqin Cai, Song Guo, Minyi Guo, and Chunming Rong. A Comprehensive Survey of Blockchain : From Theory to IoT Applications and Beyond. *IEEE INTERNET OF THINGS JOURNAL*, 6(5) :8114–8154, October 2019. Num Pages : 41 Place : Piscataway Publisher : Ieee-Inst Electrical Electronics Engineers Inc Web of Science ID : WOS :000491295800064.
- [9] Seyed Mojtaba Hosseini Bamakan, Amirhossein Motavali, and Alireza Babaei Bondarti. A survey of blockchain consensus algorithms performance evaluation criteria. *EXPERT SYSTEMS WITH APPLICATIONS*, 154 :113385, September 2020. Num Pages : 21 Place : Oxford Publisher : Pergamon-Elsevier Science Ltd Web of Science ID : WOS :000536128300006.
- [10] Caixiang Fan, Sara Ghaemi, Hamzeh Khazaei, and Petr Musilek. Performance Evaluation of Blockchain Systems : A Systematic Survey. *IEEE ACCESS*, 8 :126927–126950, 2020. Num Pages : 24 Place : Piscataway Publisher : Ieee-Inst Electrical Electronics Engineers Inc Web of Science ID : WOS :000551844800001.
- [11] Leo Besancon, Catarina Ferreira Da Silva, and Parisa Ghodous. Towards Blockchain Interoperability : Improving Video Games Data Exchange. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 81–85, Seoul, Korea (South), May 2019. IEEE.
- [12] Ran Guo, Weijie Chen, Lejun Zhang, Guopeng Wang, and Huiling Chen. Smart Contract Vulnerability Detection Model Based on Siamese Network (SCVSN) : A Case Study of Reentrancy Vulnerability. *Energies*, 15(24) :9642, December 2022.

- [13] Akhil Mittal. *Smart Contract Development with Solidity and Ethereum*. BPB Publications, Delhi, 2020.
- [14] Mayukh Mukhopadhyay. *Ethereum Smart Contract Development : Build blockchain-based decentralized applications using solidity*. Packt Publishing, Birmingham, 2018. OCLC : 1028224877.
- [15] Feijie Wu, Ho Yin Yuen, Henry C. B. Chan, Victor C. M. Leung, and Wei Cai. Infinity Battle : A Glance at How Blockchain Techniques Serve in a Serverless Gaming System. In *MM '20 : PROCEEDINGS OF THE 28TH ACM INTERNATIONAL CONFERENCE ON MULTIMEDIA*, pages 4559–4561, New York, 2020. Assoc Computing Machinery. Num Pages : 3 Web of Science ID : WOS :000810735004096.
- [16] Jusik Yun, Yunyeong Goh, Jong-Moon Chung, OkSeok Kim, SangWoo Shin, Jin Choi, and Yoora Kim. MMOG User Participation Based Decentralized Consensus Scheme and Proof of Participation Analysis on the Bryllite Blockchain System. *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS*, 13(8) :4093–4107, August 2019. Num Pages : 15 Place : Gangnam-Gu Publisher : Ksii-Kor Soc Internet Information Web of Science ID : WOS :000484076400015.
- [17] Dapeng Li, Liang Hu, and JianFeng Chu. A more efficient secure event signature protocol for massively multiplayer online games based on P2P. In P. Yarlagaadda, editor, *PROCEEDINGS OF THE 2016 INTERNATIONAL FORUM ON MECHANICAL, CONTROL AND AUTOMATION (IFMCA 2016)*, volume 113, pages 291–299, Paris, 2017. Atlantis Press. ISSN : 2352-5401 Num Pages : 9 Series Title : AER-Advances in Engineering Research Web of Science ID : WOS :000416096600046.
- [18] Sukrit Kalra, Rishabh Sanghi, and Mohan Dhawan. Blockchain-based Real-time Cheat Prevention and Robustness for Multi-player Online Games. In *CONEXT'18 : PROCEEDINGS OF THE 14TH INTERNATIONAL CONFERENCE ON EMERGING NETWORKING EXPERIMENTS AND TECHNOLOGIES*, pages 178–190, New York, 2018. Assoc Computing Machinery. Num Pages : 13 Web of Science ID : WOS :000455383800016.
- [19] Stefano Ferretti, Marco Rocchetti, and Roberta Zioni. A Statistical Approach to Cheating Countermeasure in P2P MOGs. In *2009 6TH IEEE CONSUMER COMMUNICATIONS AND NETWORKING CONFERENCE, VOLS 1 AND 2*, pages 1267–1271, New York, 2009. IEEE. Num Pages : 5 Web of Science ID : WOS :000268009200306.
- [20] Nirav Patel, Arpit Shukla, Sudeep Tanwar, Neeraj Kumar, and Joel J. P. C. Rodrigues. *GiNA* : A Blockchain-based Gaming scheme towards Ethereum 2.0. In *IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS (ICC 2021)*, New York, 2021. IEEE. ISSN : 1550-3607 Num Pages : 6 Series Title : IEEE International Conference on Communications Web of Science ID : WOS :000719386002149.
- [21] Wikipedia. Botnet, 2007.
- [22] Douglas Comer and Adib Rastegarnia. Osdf : A framework for software defined network programming. 2017.
- [23] Steven Webb and Sieteng Soh. Cheating in networked computer games : a review. In *ACM International Conference Proceeding Series ; Vol. 274 : Proceedings of the 2nd international conference on Digital interactive media in entertainment and arts ; 19-21 Sept. 2007*, pages 105–112. ACM, 2007.