VIRTUE POKER

Livre blanc de Virtue Poker

Une plateforme de poker P2P décentralisée fondée sur l'utilisation d'Ethereum

Version préliminaire 0.9

Mars 2018

Ce document est fourni exclusivement à titre d'information et ne constitue en aucun cas une offre ou une sollicitation de vente d'actions ou de titres de Virtue Poker, ou toute autre entreprise liée ou associée. Pareille offre ou sollicitation se fera uniquement au moyen d'une notice d'offre confidentielle et conformément aux termes de toutes les lois applicables sur les valeurs mobilières et autres lois.

Ce document est une ébauche ; il est fourni à titre gracieux uniquement, afin de commencer à recueillir des commentaires de l'industrie et de la communauté. Ce document ne doit pas être considéré comme un document final, et toutes les informations qu'il contient sont sujettes à modification sans préavis. Dans la mesure où, à l'avenir, Virtue Poker proposera à la vente des produits et des services, y compris des jetons, vous devez vous référer aux termes, conditions et divulgations alors en vigueur, y compris toute version modifiée de ce livre blanc.

Table des matières

1. Résumé

Le poker en ligne s'est beaucoup développé ces dernières années : entre le début des années 2000 et aujourd'hui, il est passé d'une poignée de start-ups à une industrie de plusieurs milliards de dollars. Depuis ses débuts, le poker en ligne a été confronté à deux problèmes majeurs : l'équité des jeux et la sécurisation des fonds des joueurs. Ces deux problèmes se sont trouvés au cœur d'une série de scandales dans l'industrie, qui ont provoqué la chute de plusieurs entreprises à la tête du marché du poker en ligne.

Virtue Poker a décidé de changer les choses. Il s'agit d'une plateforme décentralisée pour jouer au poker en ligne avec de l'argent réel. Elle exploite le système Ethereum afin de proposer la toute première expérience de poker en ligne basée sur une blockchain. Avec Virtue Poker, les joueurs n'ont pas besoin de déposer de l'argent sur un site, le mélange des cartes est prouvé comme étant réellement aléatoire et les cartes sont sécurisées de manière cryptographique.

1.1 Propositions de valeur

Virtue Poker n'utilise aucun serveur pour stocker les fonds des joueurs et chaque joueur prend part au mélange des cartes. Nos objectifs sont les suivants :

1.1.1 Éliminer les risques liés aux dépôts des joueurs

Virtue Poker permet au joueurs d'être les seuls détenteurs de leurs fonds en utilisant les contrats intelligents d'Ethereum pour déposer en fiducie les droits d'entrée des tournois et distribuer les prix de manière autonome en se basant sur les résultats des jeux.

1.1.2 Résoudre le problème de confiance persistant concernant l'équité des jeux

Grâce à l'utilisation de Mental Poker, un protocole pair à pair de mélange cryptographique, tous les joueurs assis autour de la table participent au mélange des cartes, et parviennent à un consensus à la fin de chaque main en utilisant un mécanisme consensuel de tolérance aux fautes byzantines.

1.1.3 Réduire les coûts s'appliquant aux joueurs et créer un écosystème de poker équilibré

L'architecture décentralisée et pair à pair innovante de Virtue Poker, associée à l'utilisation d'Ethereum, permet à Virtue Poker de se passer de serveurs et de frais de traitement de paiements coûteux. La plupart des fonctions de jeu qui sont habituellement effectuées sur des serveurs centralisés sont distribuées dans le système Virtue Poker, et les fonds des joueurs ne sortent jamais de leurs porte-monnaie sécurisés par des *contrats intelligents*. Virtue Poker fait profiter de ces économies aux joueurs à travers des rakes moins élevés et des avantages, ce qui permet de garder plus d'argent dans l'écosystème de poker.

1.1.4 Bâtir un réseau de poker décentralisé extensible

Virtue Poker a pour objectif de bâtir un réseau décentralisé de poker en ligne qui serve de base à des développeurs et des opérateurs tiers pour s'y connecter et y développer de nouvelles idées. Nous espérons donc que de nouvelles fonctionnalités seront apportées à la plateforme.

1.2 Objectif à court terme

Virtue Poker développe une application prête à l'emploi, qui sera déployée sur le mainnet d'Ethereum. Afin d'atteindre cet objectif et de préparer le lancement de l'entreprise, Virtue Poker constituera nos équipes de développement et de marketing. L'équipe de développement se concentrera sur la conception de l'interface utilisateur et des technologies de mélange distribué et de blockchain. Quant à l'équipe marketing, elle s'occupera de développer l'engagement avec nos utilisateurs alpha afin d'obtenir des commentaires sur le produit et d'apporter les dernières modifications au design de la plateforme avant son lancement.

1.3 Stratégie de croissance à long terme

Notre stratégie de croissance à long terme comprend deux macro-étapes : (1) produire la technologie et la liquidité pour la plateforme en tant qu'opérateur d'entreprise à consommateur (B2C) afin de prouver l'attractivité, l'intégrité et la crédibilité de notre solution, et (2) se développer mondialement en tant que

marque blanche afin de permettre à de nouveaux titulaires d'entrer sur les marchés à travers le monde. En effet, cela permet à des entreprises tierces de lancer facilement et à moindre coût leur propre salle de poker en ligne, basée sur une blockchain, en utilisant notre technologie centrale, en plus d'assurer une source de revenus stable.

2. Problèmes liés au poker en ligne

2.1 Introduction

L'industrie des paris en ligne représente aujourd'hui plusieurs milliards de dollars. Elle devrait d'ailleurs atteindre les 50 milliards de dollars d'ici 2021.[1] Le poker se trouve au centre de ce succès phénoménal. La forte croissance des salles de poker en ligne a fait suite à la retransmission télévisée du tournoi Main Event des World Series of Poker en 2003, au cours duquel un joueur de poker amateur alors inconnu, Chris Moneymaker, comptable, remporter 2,5 millions de dollars.

Aujourd'hui, le marché mondial du poker en ligne représente plus de 2,5 milliards de dollars. Au niveau international, le marché est dominé par l'Europe et l'Asie, qui constituent respectivement 47 % et 30 % du marché, suivies par l'Amérique du Nord (13 %), l'Océanie (6 %) et l'Amérique Latine (2 %).[2]

Malheureusement, l'industrie du poker en ligne a souffert de plusieurs scandales et est devenue la cible d'utilisateurs mal intentionnés. Les principaux sites, tels que PokerStars.com, ont adapté leur plateforme pour faire face à ce comportement problématique, mais de nombreux sites n'ont pas réussi à faire de même, suscitant ainsi une véritable méfiance chez de nombreux joueurs.

2.2 Détournement des fonds des joueurs

2.2.1 Absolute Poker et Ultimate Bet

Après de nombreuses complaintes de la part des joueurs pendant des années, Cereus Network, le troisième plus grand réseau de poker (exploitant de Ultimate Bet et Absolute Poker), a finalement admis qu'un ancien employé avait réussi à accéder à un compte administrateur qui lui permettait de voir les cartes de tous les joueurs présents sur la plateforme. Cet individu et ses complices ont volé des dizaines de millions de dollars au cours des années durant lesquelles ils ont opéré leurs méfaits.[3]

2.2.2 Full Tilt Poker

Le 15 avril 2011, jour désormais connu sous le nom de « Black Friday » au sein de la communauté du poker en ligne, des procureurs fédéraux américains ont inculpé les fondateurs des trois plus grands sites de poker en ligne (PokerStars, Full Tilt Poker et Absolute Poker), et ont forcé ces sites à cesser de proposer des jeux impliquant de l'argent réel aux citoyens américains. Il s'est avéré par la suite, lors de la réouverture de Full Tilt hors des États-Unis, que l'entreprise accumulait un déficit de 360 millions de dollars (c'est-à-dire qu'elle avait détourné 360 millions de dollars de dépôts de joueurs). L'entreprise a cessé toute activité peu de temps après.[4]

---

1 Rapport 888 annuel 2016 : http://corporate.888.com/sites/default/files/888%20AR%202016%20Hyperlinked%20PDF.pdf

2 Rapport Playtech annuel 2015 : http://playtech-ir.production.investis.com/~/media/Files/P/Playtech-IR/results-reports-webcasts/2016/2015-report-and-accounts-v2.pdf

3 « Ultimate Bet Review - Scandalous History and Failure of UB », Safest Poker Sites, n.d. Web, 7 oct. 2016.

4 http://www.pokerupdate.com/poker-opinion/544-13-biggest-poker-scandals-last-decade/

2.2.3 Lock Poker

En 2015, Lock Poker, plateforme de jeux destinée aux résidents américains, a mis la clé sous la porte après près d'une année sans pouvoir à honorer les retraits d'argent des joueurs. On estime que ces derniers ont perdu entre 15 et 24 millions de dollars.[5]

2.3 Robots de poker

Un robot de poker est un programme logiciel qui imite de vrais joueurs en ligne. Les robots de poker peuvent s'assoir à plusieurs tables, et n'ont pas besoin de supervision humaine pour fonctionner. Ils varient en complexité : ils sont disponibles en vente libre, ou peuvent être conçus sur mesure et utilisés par un individu isolé.

En 2015, un réseau de robots opérant sur PokerStars a gagné près de 1,5 million de dollars en jouant des parties à 0,50/1 $ et 1/2 $.[6]Il existe des entreprises, telles que WarBot, spécialisées dans la vente libre de robots auprès d'utilisateurs qui peuvent s'en servir sur toutes les plateformes.[7]Des sociétés inscrites en bourse, telles que 888 Holdings, ne possèdent pas de procédures de sécurité suffisamment efficaces pour protéger les joueurs de ces robots. 888 Holdings a même publié un article de blog intitulé « Robots de poker : comment jouer contre eux ? » dans lequel ces derniers sont qualifiés de « faibles [8]».

Pourtant, les robots s'avèrent de réelles menaces. En 2017, l'université Carnegie-Mellon a organisé une compétition intitulée « Cerveaux vs Intelligence artificielle : faites vos jeux ! », durant laquelle quatre des meilleurs joueurs professionnels de poker en ligne au monde ont affronté un robot de poker nommé Libratus. Ils ont tous perdu ![9]Même si Libratus, pour sa part, fonctionne grâce à un superordinateur, les robots de poker de tout type représentent une menace considérable pour le succès futur de l'industrie.

2.4 Logiciels et outils tiers

De nombreux joueurs utilisent des logiciels et outils tiers qui ciblent les joueurs amateurs. Voici une liste non exhaustive de ces outils :[10]

Bases de données de joueurs : Une base de données de joueurs qui peut être interrogée afin de trouver des joueurs avec un faible pourcentage de victoires parmi plusieurs réseaux de poker

Placement automatique : Place automatiquement les joueurs dans des parties de poker et dans des tournois Sit & Go contrôlés comme étant de qualité, avec un code couleurs pour les joueurs en fonction de leurs statistiques

---

5 http://www.pokerupdate.com/poker-opinion/544-13-biggest-poker-scandals-last-decade/

6 https://www.pokernews.com/news/2015/06/pokerstars-and-players-react-to-the-bot-scandal-21935.htm

7 http://www.poker-bot.org/main/

8 https://www.888poker.com/magazine/strategy/playing-against-poker-bots/

9 https://www.cmu.edu/news/stories/archives/2017/january/AI-tough-poker-player.html

10 http://www.sharkscope.com/#Tools-And-Apps.html

Scanner de joueurs : Scanne les joueurs présents sur la page d'accueil d'un site de poker, qui correspondent à des critères spécifiques

Affichage tête haute : Affiche en temps réel les statistiques des concurrents présents aux tables actives

Ces outils sont conçus pour permettre aux joueurs d'accéder à des informations sur leurs concurrents. Malheureusement, ils désavantagent les joueurs amateurs qui ne les utilisent pas et qui ne savent pas qu'ils sont ciblés par des professionnels hautement qualifiés.

2.5 Rakes inéquitables

Les rakes sont prélevés sur les tournois ou les parties de poker. Pour les tournois, un pourcentage, habituellement compris entre 6 et 10 %, est ajouté au droit d'entrée. Pour les parties de poker, un pourcentage est soustrait à chaque main. Les rakes des parties en ligne s'élèvent habituellement à entre 3 et 5 %, avec un plafond situé entre 0,30 et 5 $ par main en fonction des limites jouées. Même si les rakes diffèrent légèrement d'un site à l'autre, leur structure générale reste très similaire dans toutes les salles de poker en ligne.

La figure 1 montre la structure des rakes actuelle de PokerStars.[11] Elle semble logique au premier abord : en termes absolus, les joueurs avec les mises les plus élevées payent plus de rake que les joueurs avec des mises inférieures, et représentent donc des clients avec plus de valeur :

Figure 1 : Exemple des rakes sur PokerStars

11 https://www.pokerstars.com/poker/room/rake/

US Dollar Games

No Limit and Pot Limit*

Stakes	% Rake	2 Player Cap	3-4 Player Cap	5+ Player Cap
$0.01/$0.02	3.50%	$0.30	$0.30	$0.30
$0.02/$0.05	4.15%	$0.50	$0.50	$1.00
$0.05/$0.10 to $0.08/$0.16	4.50%	$0.50	$1.00	$1.50
$0.10/$0.25	4.50%	$0.50	$1.00	$2.00
$0.25/$0.50	5.00%	$0.75	$0.75	$2.00
$0.50/$1	5.00%	$1.00	$1.00	$2.50
$1/$2	5.0%	$1.25	$1.25	$2.75
$2/4	5.0%	$1.50	$1.50	$3.00
$2.50/$5	5.0%	$1.50	$1.50	$3.00
$3/$6	5.0%	$1.50	$1.50	$3.50

Vous remarquerez que le plafond sur les mises les plus basses (0,01 $/0,02 $) pour un jeu avec plus de 5 personnes correspond à 15 fois la grosse blind, mais pour un jeu à 3 $/6 $, le plafond correspond à 0,58 fois la grosse blind.

En 2011, une étude réalisée par l'université de Hambourg a analysé 2,5 millions de mains jouées sur PokerStars et d'autres sites de poker, et ce sur une période de six mois. Elle révèle que chaque joueur misant 0,01 $/0,02 $ paie un rake moyen de 12,5 BB (Big Blind) pour 100 mains, tandis que ceux misant 3 $/6 $ paient 2,58 BB pour 100 mains.[12] La figure 2 synthétise le rake moyen payé pour 100 mains à chaque niveau selon l'étude :

Figure 2 : Rake en fonction des mises

Blinds	Stake Level	Rake/100 Hands Per Player	Rake/100 Hands Played (BB)
$0.01/$0.02	Micro	$0.25	12.5
$0.02/$0.05	Micro	$0.50	10
$0.05/$0.10	Micro	$0.90	9
$0.10/$0.25	Micro	$2.00	8
$0.25/$0.50	Low	$3.50	7
$0.50/$1.00	Low	$6.25	6.25
$1/$2	Mid	$10.00	5
$2/$4	Mid	$12.25	3.1
$3/$6	Mid	$15.49	2.58
$5/$10	High	$21.00	2.1
$10/$20	High	$35.00	1.75

12 « THE GAMBLING HABITS OF ONLINE POKER PLAYERS », The Journal of Gambling Business and Economics 2011 Vol. 6

À mesure que les mises augmentent, la proportion du rake par rapport à la grosse blind diminue de façon spectaculaire. Un taux de gain de 4 à 6 BB pour 100 mains est un très bon taux selon les standards de poker en ligne. En raison des structures de rakes actuelles, la plupart des joueurs gagnants deviennent perdants lorsqu'ils jouent en micro-limites, tandis que seuls ceux se situant aux niveaux les plus élevés ont une chance de faire des bénéfices en jouant en ligne.

2.6 L'économie délabrée du poker

2.6.1 Définition

L'économie du poker comprend trois données clés : les dépôts, les rakes et les retraits. Il faut que la fonction suivante se vérifie pour que l'économie mondiale du poker puisse croître :

$$\text{Dépôts} > (\text{Rake} + \text{retraits})$$

Ce modèle nécessite un apport de dépôts constant afin de perdurer. Les joueurs professionnels ont un net positif sur les retraits (c'est-à-dire qu'ils gagnent plus qu'ils ne perdent, et retirent ces gains), tandis que les joueurs amateurs ont généralement un net négatif, ce qui crée un écosystème équilibré.

2.6.2 Le problème

Malheureusement, les joueurs victorieux (généralement des semi-professionnels ou des professionnels) gagnent plus souvent que les joueurs perdants ne déposent de l'argent, créant ainsi une tension dans l'économie du poker. Tout cela est la conséquence d'une compétition accrue depuis que les stratégies de poker se sont démocratisées avec les tutoriels en ligne, les blogs et autre documentation, mais aussi en raison de la dynamique défavorable que connaissent les joueurs amateurs, provoquée par des rakes disproportionnés, des outils tiers qui suivent et cherchent les joueurs moins expérimentés, et une méfiance répandue parmi les joueurs amateurs en ce qui concerne l'intégrité du poker en ligne.

2.7 Fragmentation du marché international

Une réglementation limite les opérateurs dans leur capacité à servir les clients selon les grandes juridictions et régions. Les juridictions sont classées selon les catégories suivantes, basées sur la réglementation en vigueur (la nomenclature exacte peut varier) :

2.7.1 Les marchés noirs

Les marchés noirs sont des juridictions qui ont soit désigné le poker comme illégal ou seulement autorisé les parties à l'intérieur de leur zone.

2.7.2 Les marchés gris foncé

Les marché gris foncé correspondent à des juridictions qui n'interdisent pas explicitement les jeux d'argent en ligne et/ou possèdent des législations ambiguës.

2.7.3 Les marchés gris

Les marchés gris sont des juridictions qui encadrent les jeux d'argent en ligne, ou qui n'ont pas pris de mesures à l'encontre des opérateurs étrangers.

2.8 Les différents types d'opérateurs

Au sein de ce cadre réglementaire, les opérateurs choisissent d'opérer soit sur plusieurs marchés avec une licence unique ou plusieurs licences, soit sur tous les marchés avec une licence unique ou aucune licence. On peut donc distinguer ces opérateurs en deux groupes : les opérateurs *onshore* et les opérateurs *offshore*.

2.8.1 Les opérateurs onshore

Il s'agit d'opérateurs réglementés ayant obtenu au moins une licence de jeu auprès d'une autorité de régulation des jeux reconnue. Ils opèrent généralement sur la plupart des marchés gris et gris foncé. En général, ces opérateurs adhèrent aux politiques fiscales, de lutte contre le blanchiment d'argent (AML en anglais), Know Your Customer (KYC) et autres politiques de conformité. La plupart d'entre eux sont des sociétés cotées en bourse sur différents marchés dans le monde. Parmi ces opérateurs onshore, on trouve : The Stars Group (PokerStars, Full Tilt Poker), William Hill Online, Playtech (réseau iPoker), GVC Holdings (PartyPoker, bwin.party), 888 Hi-oldings, Unibet, Winamax et bien d'autres.

2.8.2 Les opérateurs offshore

Les opérateurs non réglementés sont en majorité implantés dans des juridictions offshore (au Costa Rica, sur l'île de Curaçao, de Chypre ou dans des réserves indiennes). En général, ils proposent leurs services à l'international, y compris sur les marchés noirs. Il existe très peu d'informations sur ce genre d'opérateurs. Voici des exemples
d'opérateurs offshore : PaiWangLuo (Ignition, Bovada), Merge Gaming (Carbon Poker), Winning Poker Network (America’s Cardroom), Global Gaming Network, TheHive, Tiger Gaming (Chico) et bien d'autres encore.

De nombreuses juridictions et régions dans le monde ont commencé à réglementer le poker en ligne, permettant ainsi d'augmenter la part réglementée du trafic de poker en ligne.

2.9 Concurrence limitée

Le succès des réseaux de poker en ligne dépend de la constitution de larges banques mondiales de liquidités de joueurs. Au fil du temps, le marché s'est réduit à un petit nombre de gros opérateurs au sein de leurs propres marchés cibles, obligeant les joueurs à se contenter d'options de jeu limitées et permettant aux opérateurs de leur demander des frais toujours plus élevés.

2.9.1 Le marché B2C réglementé

PokerStars domine le marché B2C réglementé, avec pas moins de 850 millions de dollars de chiffre d'affaires annuel et environ 60 % du trafic mondial en ligne. Le groupe opère dans quasiment tous les pays du monde (dont 30 marchés figurant sur « liste noire »), et propose les plus gros tournois et prix en argent. Il a animé le pus grand tournoi de poker en ligne au monde (253 000 participations) et a offert la plus importante cagnotte à

ce jour (8 millions de dollars). De plus, PokerStars a géré plus de 145 milliards de mains de poker et il sponsorise les meilleurs professionnels du milieu, ainsi que des retransmissions de tournois. Kevin Hart, Usain Bolt, Rafa Nadal et Ronaldo font partie des ambassadeurs connus de la marque. PokerStars a investi dans la protection des joueurs : détecteurs de robots de haute qualité, nombreuses options de traitement de paiement et prévention contre les comptes multiples. Il ont réussi à bâtir la plus importante banque de liquidités au monde.

Néanmoins, jouer sur PokerStars s'accompagne de deux inconvénients majeurs : (1) les services qu'il propose aux joueurs sont onéreux à cause des structures de rakes élevées et (2) la concurrence sur PokerStars est nettement plus expérimentée que sur d'autres plateformes. Grâce à sa position de leader sur le marché, le groupe peut opérer en connaissant très peu de réticences de la part des joueurs, ce qui lui permet de réduire ou de supprimer les programmes de fidélité, d'augmenter les frais et de se retirer des marchés à la dernière minute.

2.9.2 Le marché B2C non réglementé

Le marché non réglementé du poker en ligne est légèrement plus fragmenté. Il est dominé par Winning Poker Network (America's Cardroom) et PaiWangLuo Network (Ignition, Bovada), qui a récemment changé de nom. Ces sociétés sont plus à même d'alimenter les marchés noirs et elles manquent de transparence en ce qui concerne leurs pratiques commerciales. De manière générale, ces sites investissent très peu dans les solutions anti-triche telles que la détection de robots ou de comptes multiples, obligeant les joueurs à se débrouiller seuls sur leurs plateformes.

De nombreux joueurs ont été séduits par ces plateformes, lassés des options de jeux limitées ou de la concurrence acharnée qui existent autre part. Cependant, l'absence de due diligence et d'exigences concernant le signalement des fraudes laisse les joueurs avec peu de recours dans l'éventualité où ces sites viendraient à disparaître, bloquer l'accès des joueurs à leur compte ou être accusés d'actes répréhensibles.

2.10 Générateur de nombres aléatoires certifié

Il existe une différence majeure entre le poker en ligne et les jeux en direct : lors d'un jeu en direct, les joueurs peuvent voir le dealer mélanger les cartes devant eux, tandis qu'en ligne, ils doivent *faire confiance* au générateur de nombres aléatoires (RNG en anglais) de l'opérateur et espérer qu'il fonctionne correctement. La quasi totalité des opérateurs en ligne possèdent un RNG certifié par un organisme tiers déjà approuvé. Parmi les sociétés qui s'occupent de tester les RNG, on trouve iTech Labs (itechlabs.com) et Gaming Laboratories International (gaminglabs.com).

Malheureusement, malgré le contrôle des RNG, il existe un manque de surveillance surprenant après l'obtention d'une certification. La Malta Gaming Authority (autorité de régulation des jeux de Malte) offre cette explication sur son site : « Après le passage du processus de certification donnant lieu à l'obtention d'une licence d'une durée de cinq ans, le système de jeu ne nécessite aucun contrôle régulier. Cependant, des inspections seront réalisées par l'autorité de régulation des jeux lorsque cela sera jugé nécessaire. »[13]L'Île de Man, quant à elle, s'exprime dans les termes suivants dans ses conseils sur les jeux

13 http://www.cc-advocates.com/gaming-law/license-requirements.htm

d'argent en ligne : « La GSC (Gambling Supervision Commission) s'assure que les RNG des opérateurs soient contrôlés au moins deux fois au cours des cinq années de validité de la licence, même si bon nombre d'opérateurs font déjà vérifier leur RNG à une fréquence plus importante. »[14] Ce manque de surveillance est à l'origine d'une croyance populaire chez les joueurs de poker en ligne, selon laquelle les jeux ne seraient pas totalement équitables.

2.11 Conclusion

Les joueurs de poker doivent faire face à de nombreux inconvénients sur le marché actuel du poker en ligne. Ils doivent affronter des logiciels malveillants, des frais élevés et une concurrence acharnée sur les marchés réglementés, et sont obligés de jouer sur des sites Web qui manquent de responsabilité et de transparence sur les marchés noirs. Dans l'ensemble, cette concurrence féroce, ces frais élevés et la méfiance des joueurs amateurs ont contribué à augmenter la pression qui pèse sur l'économie mondiale du poker.

14 https://www.gov.im/media/1349489/guidance-notes-for-making-an-online-gambling-application.pdf

3. La solution Virtue

Virtue Poker a étudié la dynamique du marché de l'industrie du poker en ligne pendant de nombreuses années. Notre objectif est de redynamiser le poker en ligne en créant un réseau de poker en ligne décentralisé reposant sur la confiance, la transparence et la responsabilité. Pour cela, nous utiliserons la blockchain Ethereum, la mise en réseau pair à pair, l'identité réelle des utilisateurs et des cartes sécurisées par cryptographie, ce qui nous permettra d'offrir une meilleure expérience de jeu aux joueurs, et ce à un coût moins élevé. Mais surtout, en utilisant ces nouvelles structures, nous cherchons à redresser l'économie chancelante du poker en réduisant les coûts pour les joueurs grâce à des rakes moins élevés, en mettant en place des rakebacks qui encouragent les joueurs à rester, et en créant la plateforme de poker en ligne la plus sécurisée du marché.

3.1 Parcours utilisateur

Virtue Poker est une application sans serveur qui fonctionne sans stockage des fonds des utilisateurs et implique tous les joueurs dans le mélange des cartes. Voici les étapes du parcours utilisateur :

3.1.1 Téléchargement du client Virtue Poker

L'utilisateur se rend sur www.virtue.poker et télécharge un client Windows, Mac ou Linux. L'application comprend un mélangeur, un moteur de jeu et une interface utilisateur.

3.1.2 Inscription

L'utilisateur peut se créer une identité uPort (uport.me) (s'il n'en possède pas déjà une). Il signe ensuite numériquement une attestation concernant son pays de résidence et son âge.

3.1.3 Approvisionnement du porte-monnaie

L'utilisateur est dirigé vers une page l'invitant à approvisionner le porte-monnaie pré-construit dans le client.

3.1.4 Créer ou rejoindre une partie

L'utilisateur peut ensuite se rendre sur le lobby, où il pourra accéder à toutes les parties publiques ou créer des parties privées pour y inviter d'autres joueurs.

3.1.5 Achats intégrés

Le joueur a le choix entre rejoindre une partie publique en envoyant de l'Ether ou des points Virtue Player (VPP) à l'adresse de la table qu'il souhaite rejoindre. Le « smart contract », ou contrat intelligent s'exécute automatiquement sur la blockchain et fait office de fiducie tant que la partie est en cours. Chaque partie est représentée par un contrat de table lié à des paramètres spécifiques à la partie.

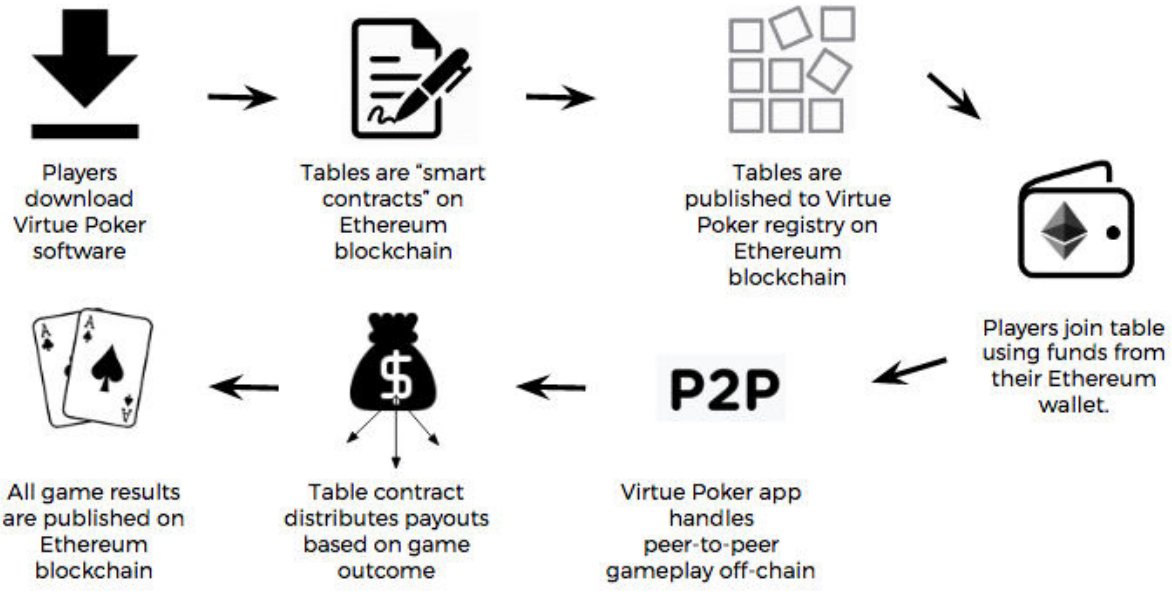
3.1.6 Jeu

Les joueurs forment un sous-réseau P2P et font appel à un protocole « Mental Poker » qui nécessite le mélange et le chiffrement du jeu de cartes par chacun des pairs.

3.1.7 Versement des gains

À la fin d'un tournoi, ou lorsqu'un joueur quitte une partie libre, le contrat lié à la table s'exécute automatiquement et chaque joueur reçoit les gains qui lui sont dus (ou aucun, le cas échéant).

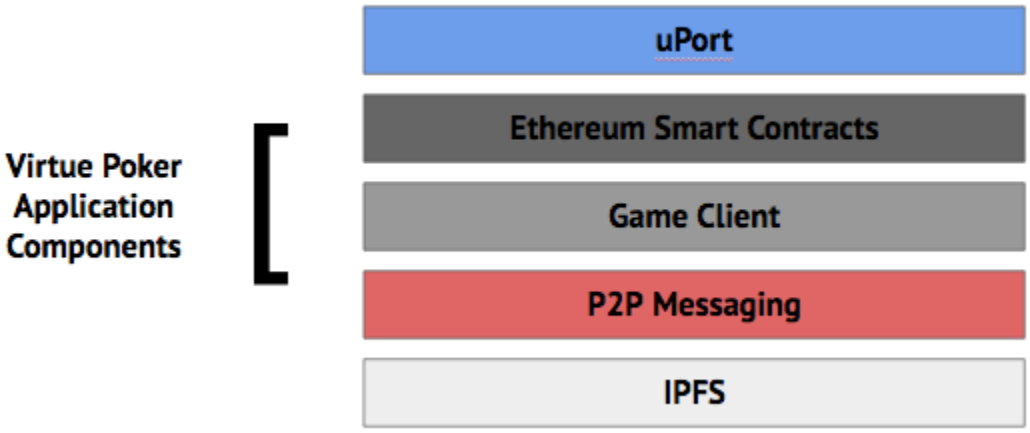
Figure 3 : Fonctionnement de Virtue Poker



3.2 Composantes de Virtue Poker

La plateforme Virtue Poker repose sur plusieurs sous-composantes qui constituent l'application :

Figure 4 : Composantes de Virtue Poker



3.2.1 uPort

Cette application de gestion d'identité auto-souveraine basée sur Ethereum, sert de mécanisme d'inscription et de validation de l'identité afin d'empêcher les mineurs de jouer et de barrer la route aux multi-comptes. Les utilisateurs doivent se connecter via uPort à chaque fois qu'ils souhaitent jouer sur Virtue.

3.2.2 Les contrats intelligents d'Ethereum

Les contrats d'Ethereum servent à la fois de registre (lobby) de toutes les parties actives sur la plateforme et de service de fiducie pour les joueurs de chaque table. Il permettent également de répertorier les paramètres de jeu, tels que les montants des buy-ins, les pourcentages de gains ou le type de partie, et de rassembler les résultats de toutes les parties.

3.2.3 Client du jeu

Le Client du jeu est une application de bureau, un moteur d'état qui gère la logique du jeu. Il permet de mélanger, de distribuer les cartes via un protocole Mental Poker et de connecter les joueurs d'une table de poker entre eux. Il dispose également d'un light wallet.

3.2.4 Messagerie P2P

Une architecture de messagerie P2P est employée comme outil de communication et de synchronisation, afin que l'interface utilisateur affiche le même état de la partie pour tous les joueurs d'une même table.

3.2.5 Protocole IPFS

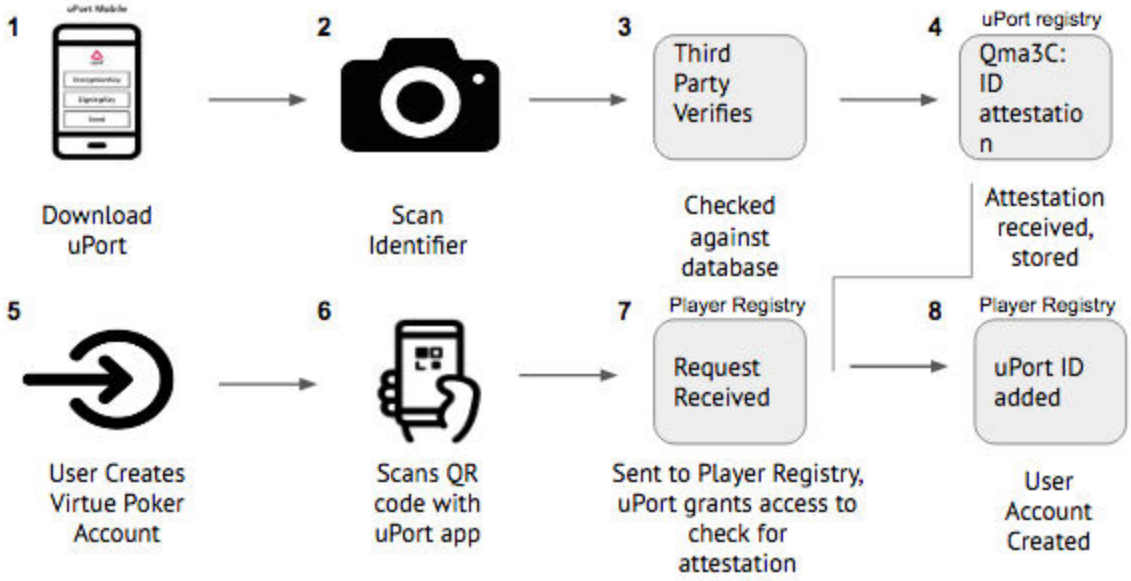
Le protocole IPFS (Interplanetary File System, ou système de fichier inter-planétaire) fournira un historique des mains pour toutes les parties de la plateforme. Les journaux peuvent être récupérés pour examen, soit pour en étudier la conformité, soit pour l'usage de l'équipe chargée de la sécurité du jeu. Cette composante fournit également les historiques de leurs mains aux utilisateurs.

3.3 Gestion de l'identité

Virtue Poker fait appel à uPort, une application de gestion d'identité auto-souveraine, afin de valider l'identité des joueurs avant leur accès à la plateforme.[15] Le processus d'identification est présenté dans la figure ci-dessous :

Figure 5 : Schéma du processus de validation de l'identité

15 https://www.uport.me/



Étape 1 : L'utilisateur télécharge l'application mobile uPort, créer un profil uPort puis scanne une pièce d'identité, qui est ensuite vérifiée par un tiers. L'attestation est ensuite chiffrée et stockée dans le protocole IPFS ; suite à cela, l'utilisateur reçoit une attestation accompagnée de son identifiant uPort.

Étape 2 : L'utilisateur crée un compte sur Virtue Poker et voit s'afficher un code QR qu'il lui faut scanner à l'aide de l'application uPort.

Étape 3 : Une nouvelle demande de compte est envoyée à un contrat Virtue Poker Accounts avec l'identifiant uPort associé. Le contrat vérifie alors que l'identité de l'utilisateur a bien été attestée par un tiers.

Étape 4 : Si l'étape précédente est validée, l'identifiant uPort de cet utilisateur sera couplé à l'adresse du compte Virtue Poker, puis stocké dans le registre des joueurs Virtue Poker.

3.4 Les contrats intelligents d'Ethereum

Une fois son identité vérifiée et son compte créé, l'utilisateur est redirigé vers le Lobby, un contrat intelligent de type casino.

3.4.1 Contrat casino

Le contrat casino sert de lobby. Il contient un répertoire de toutes les parties disponibles ou récemment terminées. Il est également possible d'y créer une partie ou d'y trouver des adversaires, ainsi que d'y effectuer toute sorte de tâches de gestion du jeu ou du profil.

3.4.2 Contrat de table

Un contrat de table correspond à une partie de poker. Lorsqu'une partie de poker est lancée avec un ensemble particulier de règles, de limites, ainsi qu'un groupe de joueurs, un nouveau contrat de table est créé et les utilisateurs sont invités à le rejoindre pour jouer. Une fois la partie terminée, les gains sont distribués, les joueurs quittent la partie et le contrat de table est fermé. Il n'aura alors plus d'autre utilité que celui de point de référence.

Au cours de la partie, le contrat de table remplit plusieurs rôles. Tout d'abord, il répertorie toutes les informations concernant les règles et paramètres de la partie. Il permet également de dresser une liste des joueurs et des informations les concernant, dont les autres joueurs pourraient avoir besoin. L'argent utilisé lors du jeu est conservé en fiducie dans le contrat, qui redistribue par ailleurs les gains à la fin de la partie.

Lorsqu'un joueur rejoint une table, les fonds nécessaires au buy-in sont transférés au contrat de table et crédités en interne au joueur. Le contrat fournit ensuite les informations nécessaires au joueur pour communiquer avec ses adversaires de table avant le début de la partie. Au fil de cette dernière, le contrat reçoit des indications sur l'état de la partie et met à jour son état en conséquence. Lorsqu'un joueur quitte la partie, le contrat transfert tous les gains dus sur le même compte utilisé pour le buy-in.

3.4.3 Interactions des joueurs avec le contrat de table

Les transactions effectuées par les joueurs sont envoyées au contrat de table dans les cas suivants : (1) lorsqu'un joueur rejoint une table ; (2) à la fin de chaque main ; (3) à la fin d'une partie (pour les tournois) ou lorsqu'un joueur quitte la table (pour les parties libres). Notre objectif est d'effectuer le moins de transactions possible vers Ethereum afin de réduire les coûts et d'améliorer la vitesse du jeu.

Les contrats de table comprennent un compteur de jetons afin d'assurer le suivi des mises des joueurs à chaque table. À la fin d'une main, chaque joueur, ainsi que les arbitres (tels que décrits dans la section 4.2) apposent leur signature cryptographique puis envoient une transaction au contrat de table, qui met alors à jour les mises de chaque joueur. Ce mécanisme de consensus, associé à la soumission des transactions par les joueurs de chaque table, porte le nom d'« oracle » : il permet au contrat de fournir des informations à jour sur l'état de la partie, afin de savoir quand payer les joueurs. Ce processus a lieu de façon asynchrone à mesure que les mains sont jouées sur la plateforme. Autrement dit, les joueurs peuvent passer à la main suivante pendant que celle en cours est validée par la blockchain.

3.4.4 Contrats de tournoi à plusieurs tables

Dans le cas des tournois où les joueurs sont répartis sur plusieurs tables, le contrat de tournoi à plusieurs tables sert d'outil d'organisation afin de gérer la répartition des joueurs sur les tables. Tous les aspects du tournoi qui s'appliquent à plus d'une table sont gérés par ce contrat.

3.4.5 Contrat de gestion des arbitres

Un arbitre est une occurrence spécifique du logiciel client du joueur, qui participe au jeu de pair à pair d'une table sans pour autant recevoir de cartes ou miser. L'arbitre est un acteur extérieur, encouragé (contre rémunération) à agir en tant que pair de confiance au niveau du sous-réseau de la table. Une

équipe d'arbitres est affectée au hasard à chaque table ; ils sont chargés de régler les différends et d'enregistrer les données de jeu.

Afin de répartir la charge de travail et d'empêcher toute collusion entre les joueurs et les arbitres, ces derniers sont affectés de manière aléatoire aux différentes tables d'un même groupe, et migrent d'une table à l'autre après un certain nombre de mains. Le contrat de gestion des arbitres vise à tenir un registre des arbitres disponibles afin de les affecter aux différentes tables de poker. Le rôle des arbitres est expliqué en détail dans la section 4.2.

3.5 Mental Poker

3.5.1 Vue d'ensemble

En 1978, les cryptographes Adi Shamir, Ron Rivest et Leonard Adleman ont publié un article visant à répondre à la question de l'informaticien Robert W. Floyd : « Est-il possible de jouer une partie équitable de "Mental Poker" ? » Dans cet article, les trois auteurs proposent un modèle de chiffrement et un protocole de communications qui permettent à deux personnes à différents endroits de mélanger et distribuer des cartes virtuelles de façon à permettre le déroulement d'une partie sans intervention d'un tiers de confiance.[16] Au fil des ans, de nombreux textes ont été publiés à ce sujet, certains développant les idées originales, d'autres proposant des méthodes alternatives ou fournissant une analyse ou une critique du modèle de 1978.

Néanmoins, il existe peu de mises en pratique logicielles des techniques de Mental Poker, et pour cause : une telle cryptographie nécessite une puissance de calcul considérable ainsi que des outils de communication de grande envergure, et les logiciels associés s'en retrouvent trop lent pour que les consommateurs puissent l'utiliser. Par ailleurs, du fait de sa nature essentiellement pair à pair, le Mental Poker s'avère difficile à gérer et s'adapte mal aux modèles de jeux en ligne traditionnels, basés sur serveur.

Depuis deux ans, l'équipe Virtue Poker tente de résoudre ces problèmes grâce à l'association d'une blockchain, de solutions de stockage distribué et d'un réseau coopératif pair-à-pair. Il en résulte une application téléchargeable qui permet de jouer une partie à vitesse normale et de gérer les mises en devises réelles grâce à une blockchain Ethereum.

Grâce à une méthode coopérative de chiffrement et de mélange des cartes, le Mental Poker garantit qu'aucun joueur ne pourra lire les jeux ; ainsi, chaque carte peut être « ouverte » par un ou plusieurs joueurs, voire l'ensemble du groupe. Le protocole utilise un chiffrement des communications, qui permet de chiffrer ou déchiffrer les cartes dans n'importe quel ordre. L'algorithme de base employé par Virtue Poker est décrit dans la section 3.5.2.

16 A. Shamir, R. Rivest et L. Adleman, Mental Poker, *Rapport technique du MIT*, 1978.

3.5.2 L'algorithme Mental Poker : le mélange à double chiffrement

Trois joueurs nommés Bob, Alice et Ted sont assis à une table et jouent une partie de Texas Hold'em. Bob, le croupier, génère un jeu de 52 cartes sur la machine ; il est le seul à pouvoir voir les cartes. Grâce à un algorithme Fisher-Yates, il mélange les cartes puis chiffre le jeu en attribuant la même clé de chiffrement à chaque carte. Ainsi, personne d'autre que lui ne peut voir le jeu. Il passe ensuite le jeu chiffré à Alice, qui fait de même : elle mélange le jeu de cartes, puis le chiffre elle aussi. Enfin, Alice passe le jeu à Ted, qui réitère l'opération.

Le jeu est désormais dans l'ordre définitif : de la première à la 52e carte, aucune ne changera de place au cours de la main. Ted passe ensuite le jeu de cartes chiffré trois fois à Bob, qui « déverrouille » le jeu mélangé puis chiffre chacune des cartes grâce à une clé différente : B1, B2... jusqu'à B52. Il passe ensuite le jeu à Alice, qui imite Bob : elle « déverrouille » le jeu mélangé, chiffre chaque carte avec sa propre clé : A1, A2, jusqu'à A52. Alice donne les cartes à Ted, qui effectue la même action. Bob reçoit les deux premières cartes du jeu, mais ne possède que ses clés de chiffrement pour ces cartes. Alice et Ted partagent alors leurs clés de chiffrement pour les deux premières cartes, soit A1, A2, T1 et T2. Bob dispose ainsi des trois clés de chiffrement nécessaires pour accéder à ses propres cartes. En revanche, il ne peut voir les cartes des autres joueurs. Ce processus est réitéré pour chaque joueur de la table afin que tous puissent voir leur propre main.

Tous les joueurs suivent alors, et le flop est dévoilé. Celui-ci contient les cartes numérotées 7, 8 et 9 du jeu. Tous les joueurs doivent partager les clés de chiffrement correspondant aux cartes sur la table, afin que tout le monde puisse les voir. Ce processus se poursuit jusqu'à la fin de la main, où le gagnant remporte le pot, et l'ensemble des joueurs parvient à un consensus (développé dans la section 4.2) en signant le résultat de la main. Ce résultat est ensuite envoyé à la blockchain Ethereum afin de mettre à jour l'état de la partie pour tous les joueurs assis à la table. Pour une illustration du processus, référez-vous aux figures 6 à 9.

3.5.3 Deux séries de chiffrement : mélange et indexation du jeu

Le « mélange multipartie » nécessite un seul mélange par l'un des joueurs afin de s'assurer que toutes les cartes sont arrangées de façon aléatoire. Si un joueur estime que sa propre machine a bien mélangé le jeu, il peut être sûr que le jeu sera équitable.

Figure 6 : Mélange et chiffrement du jeu[17]

[17] Les quatre cartes des figures 6 et 7 sont censées représenter un jeu complet de 52 cartes, et non les cartes de chaque joueur.

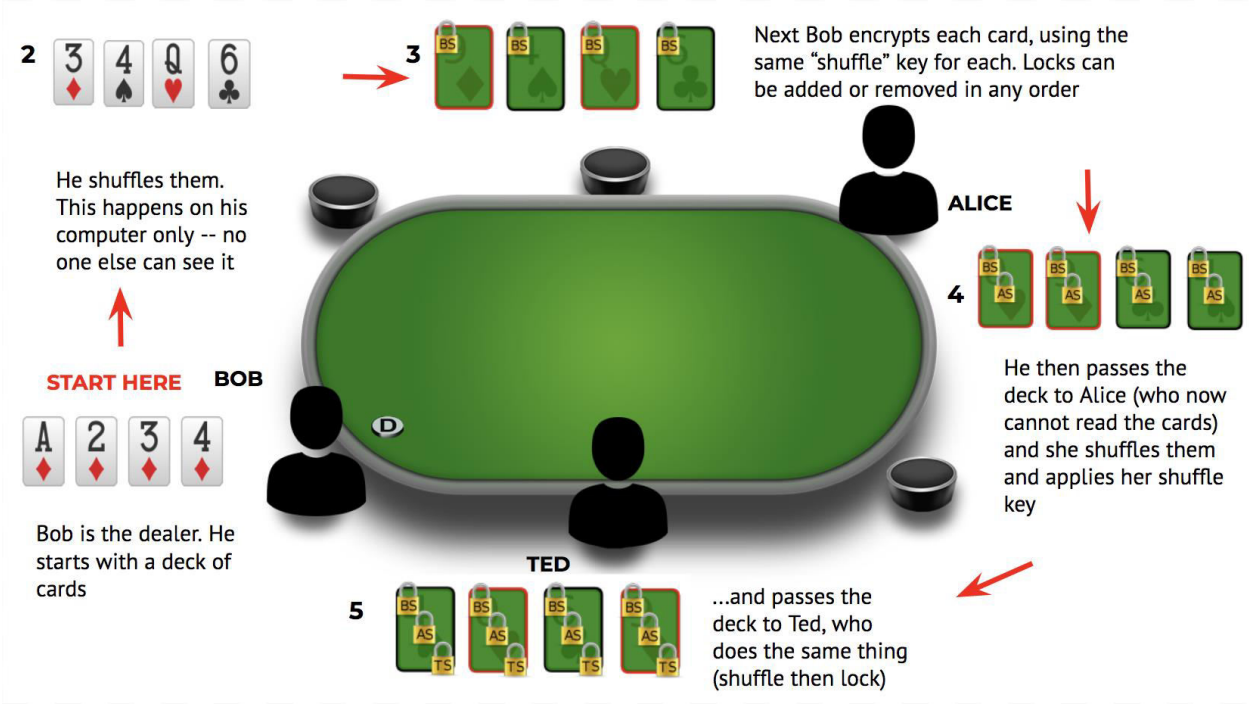
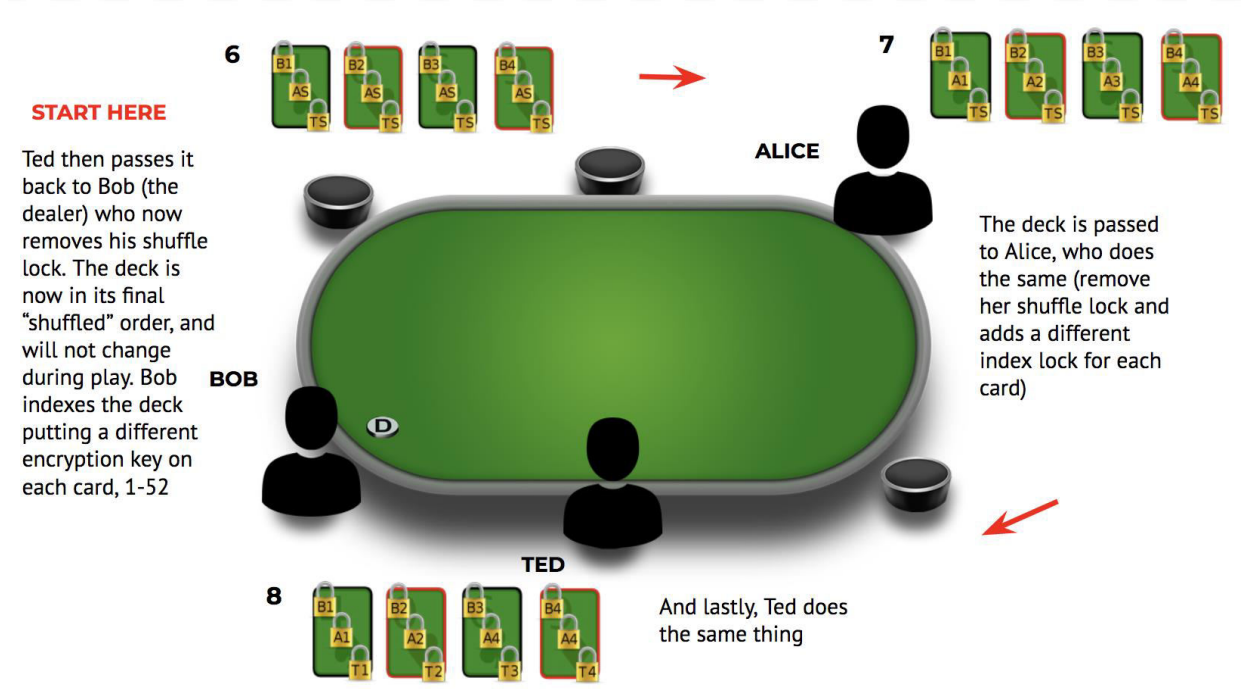


Figure 7 : Indexation du jeu



3.5.4 Déchiffrement et déroulement de la partie

Figure 8 : Partage des clés entre joueurs

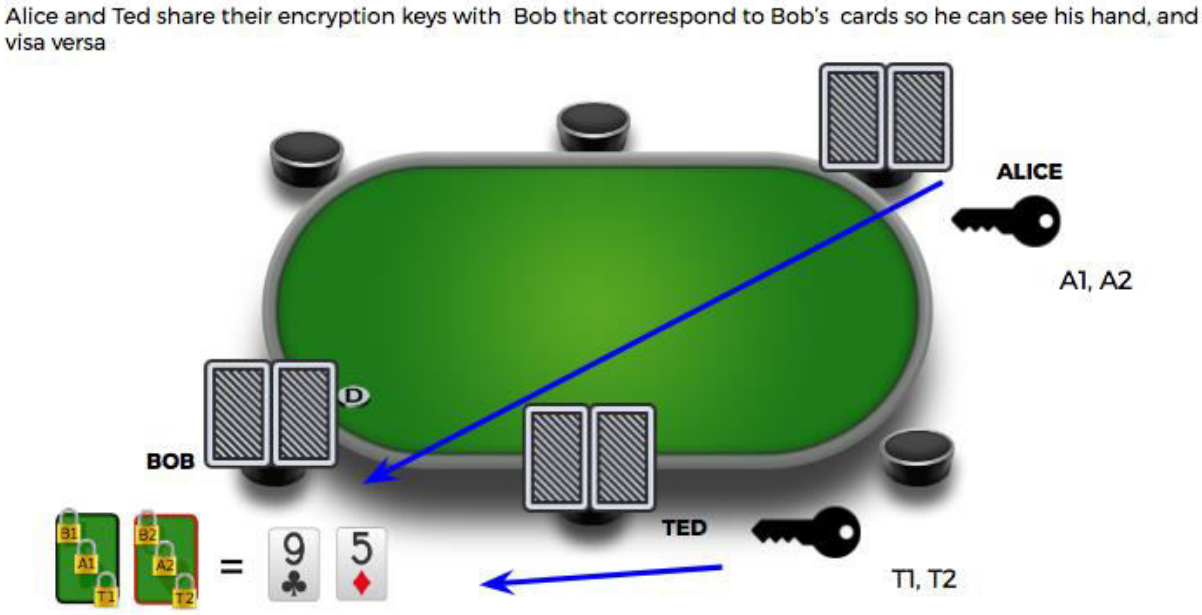


Figure 9 : Cartes communes[18]

Ce processus a lieu « en coulisses » : l'aspect d'une main dans Virtue Poker est le même que celui auquel un joueur pourrait s'attendre sur d'autres plateformes en ligne.

[18] Les cartes communes « turn » et « river » seront révélées de la même façon, une fois le flop et les tours d'enchères terminés.

3.6 La messagerie pair-à-pair

3.6.1 La messagerie pair-à-pair au service de la synchronisation du client du jeu

Le concept du Mental Poker permet de partager un jeu, de distribuer des cartes puis de les tenir secrètes grâce aux joueurs eux-mêmes au sein d'un réseau pair-à-pair, et sans faire appel à un serveur centralisé. Cependant, il est nécessaire de faire appel à d'autres technologies afin d'offrir un service de poker pratique et adapté au consommateur.
Le logiciel client du jeu téléchargeable est constitué de deux processus distincts : un processus front-end, et un back-end. Le processus front-end affiche l'état actuel de la partie à l'utilisateur local, accepte les entrées s'il y a lieu puis les transfère au processus back-end, qui les diffuse ensuite aux autres joueurs. Le processus back-end renferme la logique nécessaire pour appliquer les règles du poker aux événements d'entrées envoyés par le front-end et les autres clients. Au final, tous les clients appliquent le même code aux mêmes données.

3.6.2 Déroulement de la partie hors chaîne

Une technologie de blockchain programmable telle qu'Ethereum permet de stocker les données définitivement et de façon inaltérable, pour des éléments qui pourraient, dans un autre contexte, être gérés par un seul serveur, comme le contrôle des joueurs à une table. Comme le logiciel client a la possibilité d'interagir avec les contrats intelligents de la blockchain, il permet également une gestion distribuée et sans nécessité de confiance des fonds de chaque joueur et des mises de chaque table tout en fournissant un registre fixe de ces interactions. En revanche, la blockchain ne peut pas remplacer à elle seule un serveur pour tous les aspects du jeu. En effet, quelques secondes sont nécessaires à la propagation des données et instructions envoyées par un client ; il serait donc peu pratique d'utiliser cette chaîne de blocs pour gérer les événements du jeu à une autre granularité que celle de la main.

Les événements du jeu ayant lieu à un niveau plus élevé, tel que les paris, doivent être gérés par le logiciel client ou plutôt, par le logiciel qui traite le sous-réseau pair-à-pair (soit les joueurs d'une même table). L'utilisation de signatures numériques permet à tous les clients de vérifier que les messages reçus ont bien été envoyés par l'expéditeur, afin d'empêcher la contrefaçon. Par ailleurs, des techniques de formation au consensus de tolérance aux pannes permettent de confirmer que chaque client du jeu est d'accord avec le reste des joueurs quant aux événements du jeu, et ce à chaque étape du déroulement de la partie. En plus de détecter les erreurs et les défaillances matérielles, ce processus permet également de déceler les données volontairement erronées, à l'image du problème des généraux byzantins.

À la fin de chaque main, les données du consensus (signé numériquement par tous les clients) sont transmises à la blockchain pour être traitées, et les clients passent à la main suivante. Tout désaccord entre les clients ou les paris sont réglés par les arbitres (ce processus est décrit dans la section 4.2).

3.7 Protocole IPFS : Stockage de l'historique des mains dans le journal de la partie

Afin d'obtenir une trace permanente de chaque main, les messages signés liés aux événements du jeu doivent eux-mêmes être stockés, au même titre que les informations sur le statut récupérées par la blockchain à la fin de chaque main. Cette situation met en lumière une autre faiblesse de la technologie

des chaînes de blocs actuelle : utiliser la blockchain pour stocker des quantités de données considérables peut peser lourd sur les ressources. Envoyer l'ensemble des données collectées à la blockchain s'avère donc une solution peu pratique.

Fort heureusement, il existe des technologies comme le protocole IPFS (Interplanetary file system, ou système de fichier inter-planétaire) conçues pour offrir un stockage distribué et fiable des données. À la fin d'une main, avant que le rapport ne soit envoyé à la blockchain, le logiciel client envoie les données collectées au protocole IPFS qui génère alors un hash unique, qu'il est possible d'utiliser ultérieurement pour retrouver les données. Ce hash est inclus dans les données d'état envoyées au contrat de la blockchain. Ainsi, comme les données collectées pour chaque main contiennent le hash lié au journal de la main précédente, il est possible de demander le hash le plus récent via la blockchain et de l'utiliser pour accéder à tout l'historique de la partie. Une plateforme de stockage distribué permet en outre de supprimer les points de défaillance uniques présents sous diverses formes dans les systèmes de stockage centralisé.

4. Sécurité au sein du jeu

4.1 Formes de triche dans le poker en ligne

4.1.1 Collusion

La collusion correspond à l'entente entre deux ou plusieurs joueurs d'une table, qui partagent des informations entre eux et font appel à des stratégies de coopération pour disposer d'un avantage sur les autres joueurs.

4.1.2 Comptes multiples

En utilisant de multiples comptes sur une ou plusieurs machines, puis en occupant plusieurs place à une même table, un joueur unique dispose d'un avantage déloyal sur les autres participants d'un tournoi ou d'une partie libre.

4.1.3 Exploration des données

Les joueurs échangent parfois des données à propos d'autres joueurs, notamment des historiques de mains et des remarques. Ainsi collectées, ces données constituent des informations sur les autres joueurs auxquelles un participant ne pourrait pas avoir accès dans d'autres circonstances.

4.1.4 Robots de poker

Comme il a été dit précédemment, les robots de poker sont des programmes logiciels en vente libre ou conçus sur mesure qui interviennent à des tables de poker sans surveillance humaine.

4.1.5 Partage de compte

Le partage de compte consiste en l'utilisation d'un même compte par un ou plusieurs joueurs pour profiter du site de poker ou des autres joueurs. Il est possible de profiter du site de poker si ce dernier offre des primes plus élevées, telles qu'un rakeback, en fonction du temps de jeu et du montant du rake. De même, des actes malveillants comme la liquidation d'un compte au cours d'un tournoi ou la participation d'un joueur expérimenté sur le compte d'un joueur plus faible, constituent des façons de profiter des autres joueurs.

4.2 Mise en place du système d'arbitres pour lutter contre la triche

Virtue a développé un système composé d'arbitres afin de lutter contre la collusion et la triche. Il s'agit d'arbitres non joueurs, affectés de façon aléatoire aux tables de poker. Ces arbitres garantissent la sécurité et la protection des joueurs sur le réseau Virtue Poker ; en échange, ils reçoivent une commission. En tant que validateurs, leur rôle consiste à signer toutes les transactions de la plateforme et à envoyer les historiques de mains pour qu'ils soient stockés dans le protocole IPFS. Les arbitres sont remplacés automatiquement au bout de quelques mains.
Les fonctions décrites ci-dessous sont automatisées : aucun contrôle manuel n'est nécessaire à l'utilisateur pour exécuter un nœud d'arbitre.

4.2.1 Fonctions principales des arbitres

Les arbitres effectuent trois fonctions de base sur le réseau Virtue Poker :

4.2.2.1 Résolution des conflits

Dans les rares cas où deux pairs d'une même table seraient en désaccord quant à l'état de la table à la fin d'une main ou d'une partie, un arbitre se chargera de résoudre le conflit en temps réel et d'attribuer le pot au vainqueur.

4.2.2.2 Flux de données

Chaque arbitre a pour rôle d'envoyer le déroulement de chaque main au protocole IPFS afin que l'historique des mains soit conservé. Il s'agit d'une exigence provenant des organismes de réglementation du jeu, qui permet le fonctionnement des services essentiels comme la détection de la collusion et des robots, ainsi que l'identification des comptes multiples.

4.2.2.3 Stockage partiel des clés de chiffrement joueur

Au Mental Poker, le problème de l'« abandon du joueur » se produit lorsqu'un joueur quitte une main avant que celle-ci ne soit terminée. Cela pose un problème considérable puisque tous les joueurs sont obligés de partager leurs clés de chiffrement afin de dévoiler les cartes communes ou de terminer une main. Grâce au partage de clé secrète de Shamir, la clé de chaque joueur peut être chiffrée et partagée entre les joueurs et l'arbitre. Ainsi, si un joueur quitte la main sans raison, l'arbitre peut récupérer les morceaux de clé auprès de chaque joueur afin de reconstituer la clé de chiffrement et de terminer la main.

Sur Virtue Poker, un nœud d'arbitre peut être activé en activant le client arbitre sur une machine après avoir téléchargé et ouvert l'application. Le système d'arbitres est détaillé dans la section 5.1 de ce livre blanc.

5. VPP : Virtue Player Points

Les Virtue Player Points présentent trois utilités au sein du réseau Virtue Poker : (1) ils peuvent servir de monnaie dans le jeu ; (2) ils peuvent être mis en gage dans un contrat intelligent appelé le « registre des arbitres », qui permet aux utilisateurs de miser des jetons et de valider des mains sur le réseau contre rémunération ; enfin, (3) ils peuvent être utilisés pour accéder à des tournois spéciaux.

5.1 Devenir juge

L'équipe des juges est composée d'un nombre limité d'utilisateurs actifs sur le réseau Virtue Poker. Pour devenir juge, les utilisateurs doivent (a) acquérir des VPP (Virtue Poker Points), (b) miser des jetons dans le registre des juges et (c) allumer leur ordinateur, avec l'application Virtue Poker ouverte et configurée sur *active* afin d'être assignés à des tables.

5.1.1 Procédure d'examen des soumissions par les juges

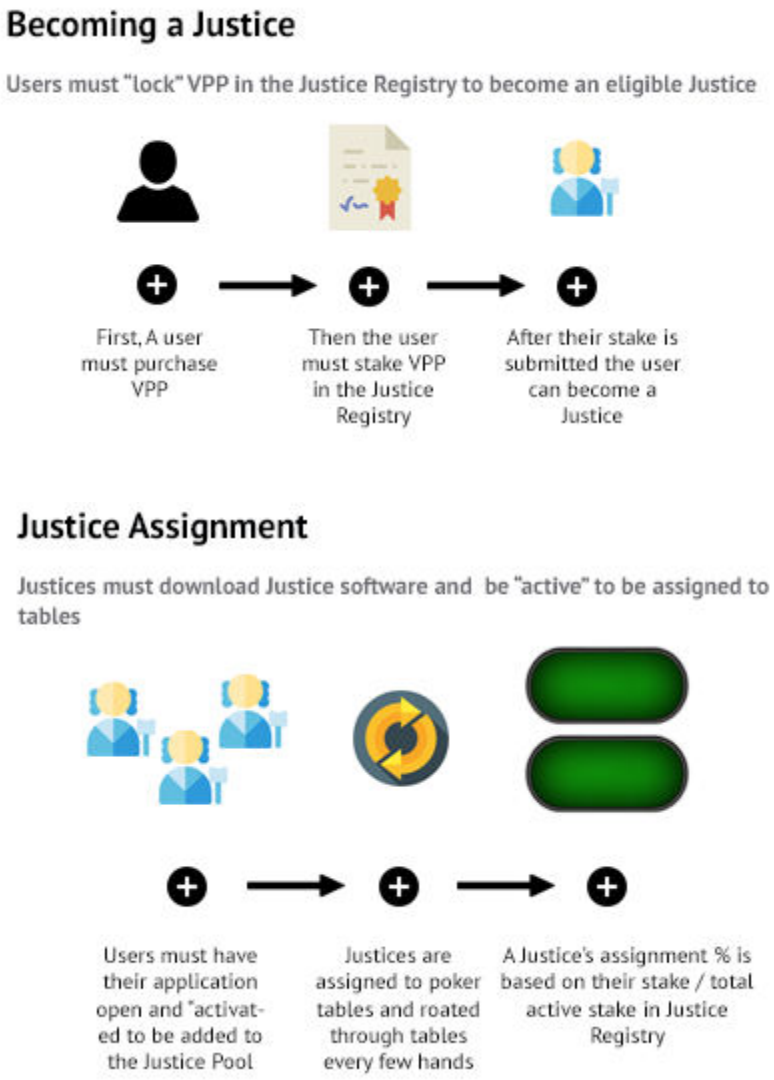
Pour commencer, les soumissions des juges au système IPFS sont contrôlées par une équipe d'experts en sécurité des jeux. L'équipe Virtue Poker dispose d'un expert en sécurité et en intégrité des jeux, qui aide notre équipe de développement à élaborer le système de justice et à configurer les logiciels de suivi appropriés afin de détecter tout problème sur la plateforme.

Il existe deux moyens d'accuser quelqu'un de tricherie et d'en informer notre équipe chargée de la sécurité du jeu. Les joueurs peuvent envoyer une réclamation en cas d'activité suspecte, laquelle est examinée afin de déterminer s'il y a bien eu tricherie. En outre, Virtue Poker exécute constamment des algorithmes à travers toutes les données envoyées par les juges et toute activité suspecte est examinée manuellement. Si on découvre qu'un joueur triche, une sanction est appliquée et le joueur est banni de la plateforme de façon permanente.

5.1.2 Rémunération des juges

Sur la plateforme Virtue Poker, la rémunération des juges est répartie entre les différents nœuds des membres actifs sur le réseau. La rémunération est versée en VPP et en ETH. Consultez la Figure 10 pour obtenir une illustration du système de justice.

Figure 10 : Système de justice

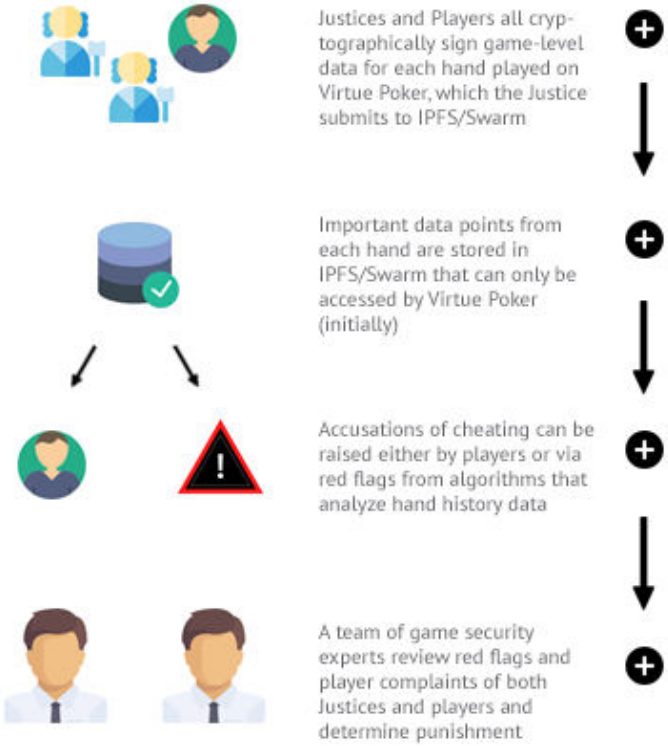


Justice Functions

Justices services are automatically completed, and in return for providing security and being honest, they earn fees from the Virtue Poker platform

Game Integrity Review

Data submitted by Justices are reviewed by a team of Game Security experts which analyzes red flags and determines if cheating has occured, either by Players or Justices.



VIRTUE POKER

5.2 Monnaie de jeu

Les VPP (Virtue Player Points) peuvent être utilisés comme monnaie de jeu. Les joueurs peuvent choisir de participer à des jeux libellés en VPP afin d'accroître leur part de VPP par rapport aux autres utilisateurs.

5.3 Tournois spéciaux

Les jeux et les tournois spéciaux ne sont accessibles qu'avec des VPP. Les joueurs peuvent s'affronter pour gagner des VPP ou ETH. Ces tournois incluent, sans s'y limiter, les tournois garantis, les freerolls et les événements satellites spéciaux.

6. Feuille de route

6.1 Principales activités

6.1.1 Développement de la plateforme

L'équipe de Virtue Poker a consacré près de trois ans au développement de son système. Il nous faudra agrandir notre équipe de développement afin de construire une plateforme parfaitement fonctionnelle. Virtue Poker va embaucher des développeurs afin d'améliorer son backbone de messagerie P2P, créer des interfaces personnalisées, optimiser ses « smart contracts » et mettre en œuvre une fonctionnalité de stockage. En outre, notre équipe va s'intégrer aux projets d'infrastructure Ethereum en cours, y compris le stockage distribué, la gestion des identités et les monnaies stables.

6.1.2 Agrandissement de la communauté

Virtue Poker va rivaliser avec les références du marché, aux budgets élevés et aux procédés d'acquisition de clients sophistiqués. Nous allons consacrer d'importantes ressources au développement d'un réseau mondial de personnes qui seraient intéressées par le succès d'une plateforme de poker décentralisée, y compris en valorisant nos utilisateurs, en exécutant des tournois garantis et des freerolls, des rakebacks, des logiciels d'analyse et autres initiatives.

6.1.3 Sponsoring et relations publiques

Virtue Poker va sponsoriser les plus grands forums, sites Web, blogs et événements de poker. En outre, notre équipe va poursuivre une stratégie de relations publiques agressive pour communiquer les propositions de valeur de notre plateforme à un large public.

6.1.4 Aspects juridiques

Notre équipe est en relation avec d'éminents cabinets d'avocats spécialisés dans le jeu, parmi lesquels DLA Piper, ISOLAS et Ifrah Law, mais également avec des régulateurs à travers le monde. Nous allons continuer à consulter ces ressources afin de connaître les cadres juridiques et réglementaires applicables. Notre équipe prévoit d'obtenir une licence de jeu avant notre lancement afin de nous assurer que notre plateforme est conforme aux normes et que nos joueurs sont suffisamment protégés.

6.2 Feuille de route du développement

6.2.1 État actuel

Virtue Poker a été conçu en mai 2015, et notre prototype a été développé au cours des deux dernières années.

Notre application est testée chaque semaine depuis sa création. En interne, notre équipe fait des parties de poker via une implémentation Mental Poker qui repose sur les testnets Ethereum.

La première version de Virtue Poker est un client bureau en langage Python qui crée un contrat intelligent et personnalisé pour chaque instance de table. Notre équipe a réussi à mettre en place un protocole Mental

Poker pour le battage des cartes et un moteur de jeu. Le moteur de jeu est une machine d'états qui se connecte aux autres pairs à l'aide d'un protocole de messagerie P2P et qui se raccorde à Ethereum quand des pairs sont créés et qu'ils rejoignent une table. À l'heure actuelle, notre application permet de jouer des parties à 6 joueurs à un taux de 70 à 80 mains par heure, au même niveau que les actuels réseaux de poker en ligne.

6.2.2 Autres développements

Virtue Poker a engagé une équipe de base et va utiliser un financement interne pour continuer à bâtir l'équipe et la plateforme de Virtue Poker. L'un de nos objectifs est de revoir l'application de bureau Virtue Poker et d'en faire une application Electron. Pour que notre plateforme soit une réussite, l'application Virtue Poker doit subir d'importants tests afin de s'assurer que les jeux sont suffisamment justes, que la méthode d'inscription et de vérification d'identité empêche la tenue de plusieurs comptes et l'utilisation par des mineurs, et que notre mécanisme de stockage des données est capable de suivre les points de données nécessaires pour rester en conformité et détecter les tricheries.

Amélioration du backbone de messagerie P2P
L'application utilise des implémentations de plug-in remplaçables selon le runtime pour différents transports. Elle utilise actuellement un Exploder de messages basé sur un serveur HTTP. Pour son déploiement, Virtue Poker va implémenter un backbone plus résistant.

Mise en place des juges
La présence d'un ou de plusieurs juges dans une partie permet un archivage hors connexion permanent (IPFS) du jeu au niveau de l'homologue, ce qui est important lorsqu'on essaie de détecter une complicité ou un robot dans une partie, ou simplement pour
obtenir la preuve que la partie s'est correctement déroulée. Dans le cadre du mécanisme de consensus, un juge empêche 2 joueurs de tricher dans une partie à trois joueurs, ce que ne peuvent pas faire les mécanismes de consensus vulnérables à 51 %.

Qualité commerciale côté utilisateur
Virtue Poker va revoir l'apparence de son application actuelle et mettre au point une interface utilisateur destinée à notre lobby avant la première phase d'essai auprès des utilisateurs.

6.2.3 Premier trimestre 2018

Gestion de l'identité
Au départ, l'équipe de Virtue Poker va intégrer un service externe chargé de la vérification des identités (voir https://www.hooyu.com/). Comme nous allons continuer à travailler avec des organismes de réglementation partout dans le monde, nous allons leur présenter des solutions d'identité auto-souveraine comme uPort. Notre objectif est de parvenir à déplacer notre processus d'identification vers une solution décentralisée.

Stockage de données
Virtue Poker va utiliser les nœuds des juges pour recueillir et enregistrer les parties à chaque tour. Nous avons l'intention d'enregistrer les historiques des mains à l'aide du au système IPFS et d'ajouter une référence aux données présentes dans le contrat de la table. Au départ, nous allons utiliser un mécanisme de stockage centralisé des données pour notre version Alpha.

6.2.4 Deuxième trimestre 2018

Version Alpha privée de Virtue Poker
Virtue Poker va conduire un test privé auprès d'utilisateurs afin de déboguer notre plateforme et d'obtenir des commentaires pour améliorer notre UI/UX. Les participants à la vente de jetons Virtue Poker (phase 1) seront invités à participer au programme Alpha.

Événement de pré-lancement
Virtue Poker va organiser un événement de pré-lancement regroupant des joueurs en ligne et professionnels connus. L'événement sera diffusé en direct sur Twitch.

6.2.5 Deuxième et troisième trimestres 2018

Mécanisme de rakeback
En tenant compte des tests en cours auprès des utilisateurs, Virtue Poker va mettre en place un mécanisme de rakeback sous forme de jetons en utilisant des VPP.

Création d'une fonctionnalité de tournoi multi-tables
Le contrat de tournoi multi-tables gère les tables qui font partie du tournoi et les joueurs assignés à ces tables. Il gère également l'évolution et la résolution du tournoi : qui gagne et quoi. Pendant le jeu, la table constitue toujours l'unité de sous-réseau P2P et fonctionne à peu près comme maintenant, mais elle communique avec le contrat de tournoi multi-tables.

Édition limitée de Virtue Poker (bêta ouverte)
Virtue Poker va proposer une version bêta ouverte aux utilisateurs du monde entier qui peuvent créer et jouer à des tournois Sit & Go et des cash-games à une table.

6.2.6 Quatrième trimestre 2018

Tournoi de lancement public de Virtue Poker
Le lancement public de Virtue Poker s'effectuera au moyen d'un ou plusieurs tournois garantis, permettant ainsi aux utilisateurs du monde entier de jouer sur notre plateforme.

6.2.7 2019

Intégration d'opérateurs tiers
Virtue Poker va permettre à des opérateurs et détenteurs de licence à travers le monde de créer des apparences personnalisées sur notre plateforme ainsi que des jeux basés sur notre infrastructure. De cette manière, nous pourrons évoluer plus rapidement à un niveau de liquidités qui attirera les joueurs.

7. Équipe

7.1 Équipe principale

Jim Berry, Lead Platform Developer : Ces trente dernières années, Jim a travaillé sur différents logiciels, du système terrestre du télescope spatial Hubble à l'application de données de recherche de l'institut Framingham Heart Study, en passant par les pilotes Linux destinés au système d'acquisition d'images aériennes et l'installation de systèmes de messagerie appropriés pour des pays en développement dans la région Pacifique Sud. Il a toutefois consacré une grande partie de sa carrière à la mise au point de jeux sur ordinateur pour des entreprises telles que MicroProse, Looking Glass Technologies et Electronic Arts, se spécialisant dans la simulation physique et le graphisme.

Ryan Gittleson, Co-Founder : Ryan est un professionnel expérimenté dans les domaines du marketing et du développement commercial, aidant notamment des entreprises à accroître leur chiffre d'affaires et la vente de leurs produits. Avant de travailler chez Virtue Poker, Ryan occupait le poste de Head of Customer Acquisition pour TodayTix, application mobile de vente de billets de spectacles sur Broadway, où il a supervisé la croissance de la base d'utilisateurs, laquelle est passée de 150 000 à plus de 700 000 utilisateurs. Il a découvert Ethereum en août 2015 et s'est tout de suite intéressé au potentiel mondial de la technologie de la blockchain. Ces deux dernières années, il a travaillé aux côtés de la société ConsenSys pour développer Virtue Poker. Ryan est titulaire d'un Bachelor Degree de l'université de Pennsylvanie.

Dan Goldman, Chief Marketing Officer : Dan possède plus de vingt années d'expérience dans le marketing des entreprises en ligne. Il a joué un rôle déterminant dans la croissance de la plus grande société de poker en ligne au monde, PokerStars, lui permettant de passer du statut de start-up à une plateforme comptant plus de 100 millions de joueurs. Avant PokerStars, Dan a dirigé le département marketing de l'un des plus grands sites de comparateurs de prix sur Internet, conduisant à son acquisition par Experian. Il a fait partie de l'équipe qui a commercialisé la programmation orientée objet, permettant à la start-up Digitalk de s'imposer comme le leader du marché avec son langage de programmation Smalltalk/V. Dan a également supervisé le développement et le lancement d'un site de casino en ligne pour l'un des plus grands casinos des États-Unis.

Javier Franco Algarrada, Blockchain Development Team Lead : Javier est un ingénieur logiciel confirmé, doté de plus de dix années d'expérience. Il aime travailler sur le développement d'applications de A à Z, recourant à diverses technologies, et participer activement au développement logiciel complet d'un produit. Après avoir mené d'autres projets techniques, il s'est proposé de diriger le développement de Virtue Poker. Il a travaillé pendant plus de 7 ans dans l'univers des jeux de hasard à travers différents produits comme la loterie, les sports virtuels, les jeux de casino et les paris sportifs. Passionné depuis toujours par les technologies de pointe, il a décidé de s'orienter vers des projets de blockchain l'année dernière. Il est titulaire d'un Bachelor Degree en informatique et d'un Master Degree en génie de développement Web.

Catalin Dragu, Design : Catalin est designer numérique depuis 2010. Il collabore aujourd'hui avec ConsenSys, créant des dApps originales et engageantes. Il est convaincu qu'un bon design suscite un bon esprit. Il s'efforce de créer une expérience soignée afin que les utilisateurs puissent en profiter comme une balade dans un parc.

Jose Diaz, Head of Product : Jose possède une expérience éprouvée dans l'entreprenariat et l'innovation, comptant plus de dix-huit ans d'expérience dans le secteur des jeux de hasard aux postes de CTO, Product Development Director, Software Developer et IT Manager. Jose est titulaire d'un MBA et d'un diplôme universitaire en informatique. Attiré par la technologie innovante qu'utilise Virtue Poker, il a rejoint l'entreprise au poste de chef de produit. Au cours de sa carrière, Jose a notamment mené à bien des projets très médiatisés, défini de nouvelles stratégies de développement sur de nouvelles plateformes, dirigé des équipes performantes et géré des relations avec d'importants clients.

Colum Higgins, Senior Product Manager : Colum Higgins a obtenu un PhD en physique au CERN au début des années 1990. Les dix années suivantes, il a occupé des postes techniques en supercomputing, puis il a travaillé comme consultant en intergiciels pour une entreprise, avant de fonder une start-up technologique et de devenir CTO pendant trois ans et demi. En 2003, Colum a décroché un MBA et s'est envolé pour la Chine, où il a créé un système de démonstration de la 3G pour Ericsson et où il a travaillé sur des projets d'administration électronique pour des gouvernements de la région ainsi que pour l'Union européenne. En 2007, Colum a rejoint Full Tilt Poker en tant que gestionnaire des programmes et analyste d'entreprise. Chez Full Tilt Poker, Colum a supervisé les exigences de fonctionnalités phares (nouvelle version de jeu, réglementation en France, tables pour débutants, tickets de tournois...).

Daniel Ortega, Back-End Developer : Daniel est ingénieur logiciel depuis 12 ans. Il s'est formé et a travaillé dans des secteurs variés, du génie civil à l'industrie aéronautique, en passant par les jeux de hasard. Daniel s'emploie constamment à sortir de sa zone de confort. Au cours de sa carrière, il a toujours cherché à travailler avec les dernières technologies.

Alvaro Rodríguez Villalba, Front-End Developer : Alvaro est développeur full-stack JavaScript et développeur Android. Il a cofondé la start-up Kultur, où il occupait le poste de développeur Web et Android. Il a consacré plus de deux ans au développement d'une application Web destinée à la simulation des liaisons de communication satellite. Il a également créé plusieurs plateformes basées sur JS en tant que développeur freelance. Alvaro est diplômé du programme ConsenSys Academy de 2017.

Lucas Cullen, Blockchain Platform Developer : Lucas est développeur de logiciels full-stack et Solidity. Il a travaillé pour des start-ups et des banques, et il possède une formation en mathématiques. C'est en 2011 qu'il a entendu parler du Bitcoin et depuis, il ne cesse d'en vanter les mérites. Il a travaillé avec Accenture et la Monetary Authority de Singapour sur le « Project Ubin », utilisant un produit Ethereum de la société de JP Morgan baptisé Quorum. Avant cela, il a dirigé sa propre société de conseils en logiciels, proposant des formations et développant des logiciels pour des projets autour du Bitcoin et de la blockchain. Il dirige le groupe Bitcoin Brisbane, il est membre du conseil de Blockchain Australian et il est également ambassadeur de la monnaie australienne Coloured Coin.

7.2 Conseillers

Joseph Lubin : Au cours de sa carrière, Joe Lubin a occupé divers postes dans les domaines de la technologie et de la finance, et à l'intersection des deux. Diplômé avec *mention honorifique* en génie électronique et en informatique à l'université de Princeton, il a travaillé dans l'équipe de recherche du laboratoire Robotics Lab de Princeton, avant de rejoindre le département Vision Applications. Sa maîtrise du génie logiciel, de la finance et de la cryptographie ont permis à Joe de travailler chez Goldman Sachs. Il a également occupé le poste de consultant pour eMagine autour du projet IdenTrust, et il a participé à la création et à la gestion de fonds spéculatifs aux côtés d'un partenaire. Joe a cofondé le projet Ethereum. Depuis janvier 2014, il travaille également sur le projet de la société ConsenSys.

James Slazas : James Slazas possède plus de 15 ans d'expérience dans le secteur financier. Chez Lehman Brothers, James a géré un portefeuille d'arbitrage pour compte propre de produits dérivés et il a créé un groupe global de gestion des risques en matière d'exposition HNW (individus à valeur nette élevée) pour les banques de Londres, de Suisse et de Hong Kong. James est le cofondateur d'un fonds spéculatif gérant un portefeuille de « life settlements » (transaction financière lors de laquelle le propriétaire d'une assurance vie vend sa police à une tierce partie). En utilisant les composantes de santé du fonds, James a réussi à négocier un statut privilégié aux centres de Medicare et Medicaid dans divers États (AZ, CA, FL, NJ et NY) pour déployer les dossiers médicaux électroniques et les services de facturation de Med A-Z/Healthcare Inside. Il a également négocié un contrat exécutoire avec HCL America visant à fournir des outils d'analyse de la prise en charge des patients et des services de facturation de soins médicaux aux laboratoires, ACO (Accountable Care Organizations), cabinets privés et hôpitaux.

Patrick Berarducci : Pat occupe le poste de Associate General Counsel chez ConsenSys. Il est également ingénieur logiciel full-stack. Avant de rejoindre ConsenSys, Pat a pratiqué le droit pendant sept ans chez Sullivan & Cromwell LLP. Il a également cofondé une start-up spécialisée en technologie de la santé. Ce qui anime particulièrement Pat, c'est de tirer parti de son expérience en droit, logiciels et création d'entreprise pour révolutionner les secteurs, marchés et réseaux à l'aide de la technologie de la blockchain.

Andrew Keys : Andrew dirige le département Global Business Development chez ConsenSys. Il possède de l'expérience en marchés financiers, technologie et création d'entreprise.Avant cela, Andrew a travaillé pour la banque d'investissement UBS, dans l'analyse d'actions cotées en Bourse. Par la suite, il a créé et distribué des produits de vente d'assurances vie (life settlement) à des fonds spéculatifs et des banques d'investissement. Après quoi, il a cofondé une société de gestion des cycles des ventes, où il a découvert Bitcoin puis Ethereum. Andrew supervise les partenariats technologiques stratégiques, la prospection de clientèle et les communications pour ConsenSys. Il a cofondé ConsenSys Enterprise pour créer des solutions de blockchain Ethereum destinées aux entreprises du Fortune 500.

Robert Davidman : Dernièrement, Robert a occupé le poste de directeur marketing par intérim chez la société ruby, supervisant le marketing et la stratégie numérique de son portefeuille innovant de marques,

parmi lesquelles Ashley Madison, Cougar Life et Established Men. Actuellement, Robert dirige la stratégie marketing américaine et mondiale de plusieurs grandes marques en tant que partenaire de The Fearless Group à New York, agence qu'il a cofondée. Il compte plusieurs clients du secteur des jeux, dont les sociétés Bwin.Party (PartyPoker), Pala Interactive (Palacasino.com, PalaPoker.com, Palabingousa.com), 888 Holdings (888.com) ou Lottoland.com, pour n'en citer que quelques-unes. Depuis 2001, Robert a travaillé avec plusieurs sites de jeu en ligne à travers le monde, en tant que spécialiste du marketing et opérateur. Robert a occupé le poste de directeur des services de diffusion mondiale pour Yahoo! de 1999 à 2001, où il a déployé l'activité de streaming du portail Web à travers 24 pays, quand celle-ci n'était présente qu'aux États-Unis et au Canada. Entre 1995 et 1999, Robert était le 9e employé chez Broadcast.com, où il dirigeait les ventes et le marketing de ce pionnier du streaming sur Internet.

7.4 Équipe de Virtue Poker

Phil Ivey : Ivey a remporté 10 bracelets des World Series of Poker, soit le deuxième record de l'histoire. Il est classé 6e meilleur joueur mondial avec plus de 23 millions de dollars de gains en tournois. Par ailleurs, il est l'un des meilleurs joueurs de poker en ligne, accumulant plus de 10 millions de dollars de gains. Il excelle dans tous les domaines (tournois, cash-game live, cash-game online) et il a atteint 9 tables finales lors du World Poker Tour. Entre 2002 et 2009, Ivey s'est placé dans le Top 25 à quatre occasions lors du tournoi principal du World Series, et il a été nommé au Hall of Fame des WSOP en 2017.

Dan Colman : Il est célèbre pour avoir battu Daniel Negreanu et remporté un Big One for One Drop où le buy-in s'élevait à 1 000 000 de dollars lors des World Series of Poker 2014. Dan a accumulé plus de 28 millions de dollars de gains en tournois, faisant de lui le troisième meilleur joueur de l'histoire.

Brian Rast : Brian Rast, connu sous le pseudonyme de « tsarrast », compte 3 bracelets des World Series of Poker. Il rejoint l'équipe en tant que conseiller de l'entreprise. Brian a remporté le tournoi Pot-Limit Hold'em à 1 500 dollars en 2011 ; il a gagné à deux reprises le tournoi Players Championship à 50 000 dollars en 2011 et 2016, triomphant respectivement de Phil Hellmuth et Justin Bonomo. Il est classé 10e meilleur joueur mondial, avec plus de 20 millions de dollars de gains en tournois.

7.4 Partenaires juridiques

Ifrah Law PLLC (US Gaming Matters) : Ifrah Law représente des clients du secteur iGaming depuis l'apparition de ce marché. Le cabinet représente aujourd'hui nombre des plus grandes sociétés et associations du secteur iGaming à travers le monde. Le cabinet s'est trouvé au cœur des plus importants procès et poursuites en justice du secteur iGaming, y compris les affaires des sites de poker en ligne Full Tilt Poker et PokerStars, pour lesquels Jeff Ifrah a négocié un accord historique en 2011 avec le département de la Justice des États-Unis. Ifrah Law a également joué un rôle clé dans la création des cadres législatifs et réglementaires des trois États qui autorisent actuellement les jeux en ligne : le Delaware, le New Jersey et le Nevada.

ISOLAS LLP, Gibraltar Law : ISOLAS est un cabinet d'avocats basé à Gibraltar et offrant un large éventail de services et de conseils en solutions juridiques. Cabinet primé, classé parmi les entreprises les plus prestigieuses de Gibraltar par les plus grands répertoires professionnels, ISOLAS se concentre avant tout sur ses clients et sur les solutions qu'il peut leur apporter. Fiable depuis 1892, ISOLAS LLP fête cette année son 125e anniversaire à Gibraltar, soit le plus ancien cabinet d'avocats du territoire.

8. Annexe : architecture de Virtue Poker

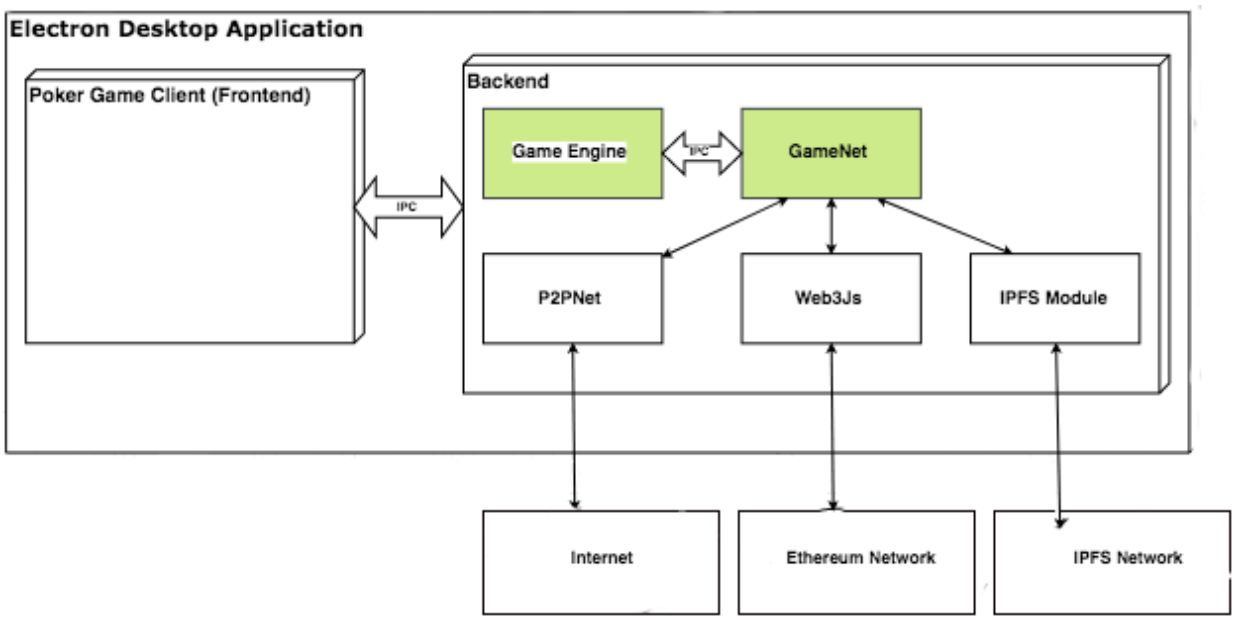
Virtue Poker est toujours en cours de développement. Certaines parties de cette rubrique peuvent changer.

8.1 Architecture du système

Virtue Poker est une plateforme de poker totalement décentralisée. Pour parvenir à cet objectif, Virtue Poker utilise des technologies innovantes comme Ethereum et IPFS, ainsi que d'autres solutions.

L'application de bureau Virtue Poker est une application de bureau Electron qui inclut le moteur de jeu, le client de jeu et l'infrastructure réseau permettant de communiquer avec la blockchain Ethereum, ainsi qu'un sous-réseau peer-to-peer destiné aux instances de jeu nécessitant une messagerie à faible temps de latence (jeu entre humains).

Figure 12 : Architecture de l'application



8.1.1 Composants

Les principaux composants de l'application de bureau Electron sont les suivants :

- **Moteur de jeu :** contient la logique du jeu de poker.

- **Ethereum :** sert de référentiel aux paramètres du jeu, compte escrow, rapports de résultats, gestion des joueurs sur plusieurs tables et gestion des juges.
- **GameNet :** fournit un composant unique que le moteur peut utiliser pour communiquer avec le monde extérieur.
- **P2PNet :** utilisé par GameNet pour gérer un sous-réseau P2P propre à une instance de jeu.
- **Web3.js :** API JavaScript compatible avec Ethereum qui met en place la communication avec les nœuds Ethereum.
- **Application de bureau Electron :** framework inter-plateformes.
- **Client de jeu :** client utilisé pour jouer au poker. Il s'agit d'une application Web HTML5 écrite à l'aide de l'écosystème React.
- **Client IPFS :** sert d'interface avec le réseau IPFS pour stocker les résultats du jeu.

8.2 Moteur de jeu

8.2.1 Automate fini

Le moteur de jeu est au cœur de notre application. Il s'agit d'un automate fini qui contrôle les transitions au sein de l'état du jeu et applique les règles du jeu. Selon les interactions de l'utilisateur avec l'application et les réponses du réseau, le moteur de jeu déclenche des actions et passe à l'état suivant.

8.2.2 État connecté ou hors ligne

Virtue Poker exécute le processus suivant lorsqu'un utilisateur se connecte à l'application :

1. L'application n'est pas connectée, on est donc en état hors ligne.
2. L'utilisateur entre ses identifiants et se connecte.
3. Le moteur de jeu reçoit les entrées et déclenche l'action pour effectuer la connexion.
4. Une fois la connexion effectuée, le moteur de jeu passe à l'action suivante et notifie l'interface utilisateur.
5. Si la connexion fonctionne, on passe à un état connecté.
6. Si la connexion échoue, l'utilisateur reste en état hors ligne.

8.2.3 États de lobby

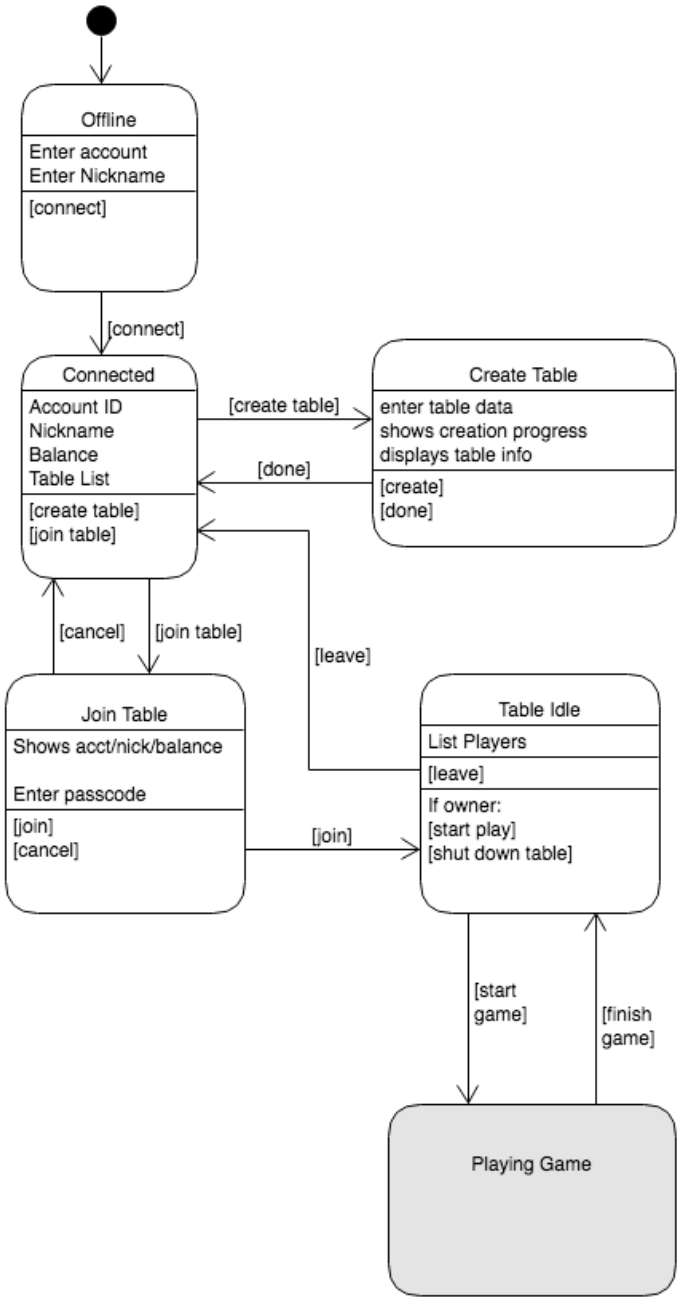
Les états de notre moteur de jeu sont classés en deux groupes :

- **États de jeu :** états du jeu quand une partie est en cours.
- **États de lobby :** tous les états qui surviennent en dehors de la partie.

Les états de lobby incluent :

- **Offline :** l'utilisateur n'est pas connecté.
- **Connected :** l'utilisateur s'est connecté et peut créer ou rejoindre une table.
- **Create a Table :** l'utilisateur crée une table.
- **Join Table :** l'utilisateur sélectionne une table et la rejoint.
- **Table Idle :** l'utilisateur attend que d'autres membres rejoignent la table afin que la partie puisse commencer.

Figure 13 : États de lobby



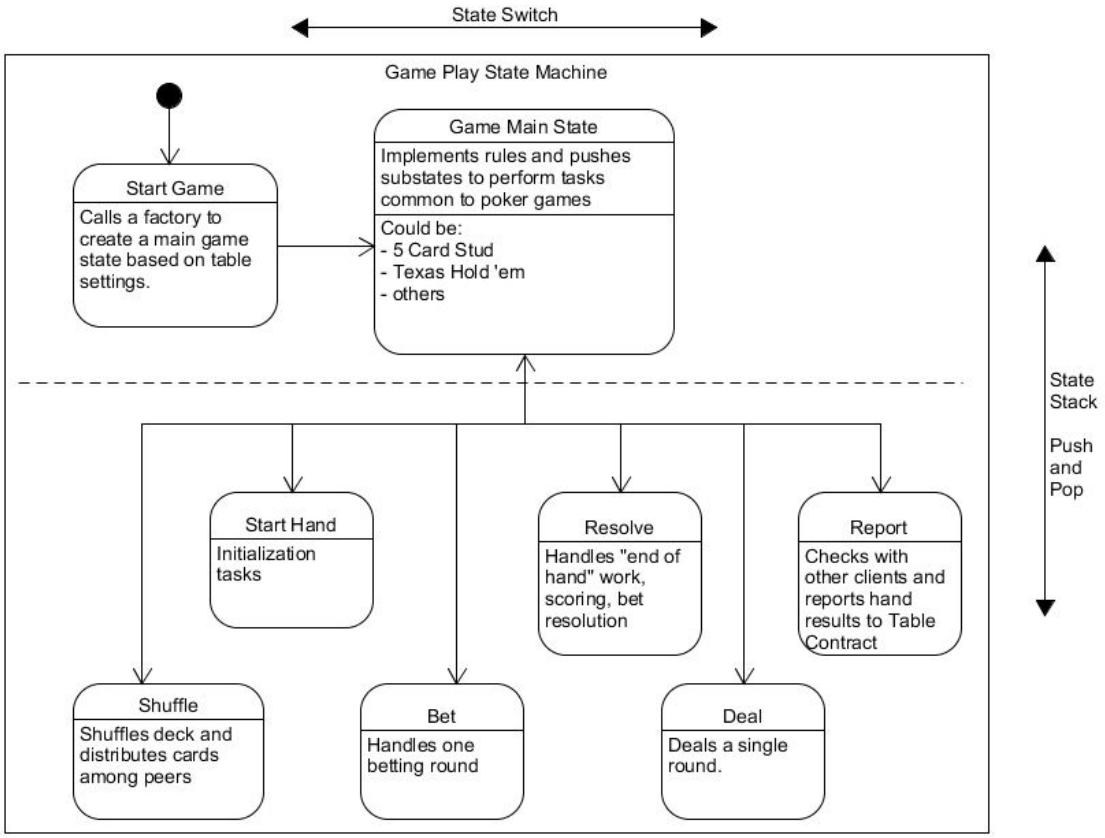
8.2.4 États de jeu

Les états de jeu incluent :

- **On Deck :** le joueur attend que la main commence.
- **Start Hand :** tous les joueurs sont prêts à commencer une main.
- **Shuffle :** le jeu de cartes est mélangé et crypté.

- **Deal :** il existe plusieurs phases de jeu selon la partie de poker qui est jouée. Par exemple, au Texas Hold'em, nous aurons : pré-flop, flop, turn et river.
- **Bet :** le joueur décide s'il veut checker, suivre, se coucher ou relancer selon l'état du jeu.
- **Check Deal :** le moteur de jeu consulte les règles pour déterminer s'il faut distribuer d'autres cartes.
- **Showdown :** moment où les mains encore actives sont dévoilées ou cachées.
- **Resolve :** les résultats des mains sont montrés.
- **Report :** les résultats des mains sont envoyés au contrat de jeu/table et le vainqueur remporte le pot.

Figure 14 : États de jeu



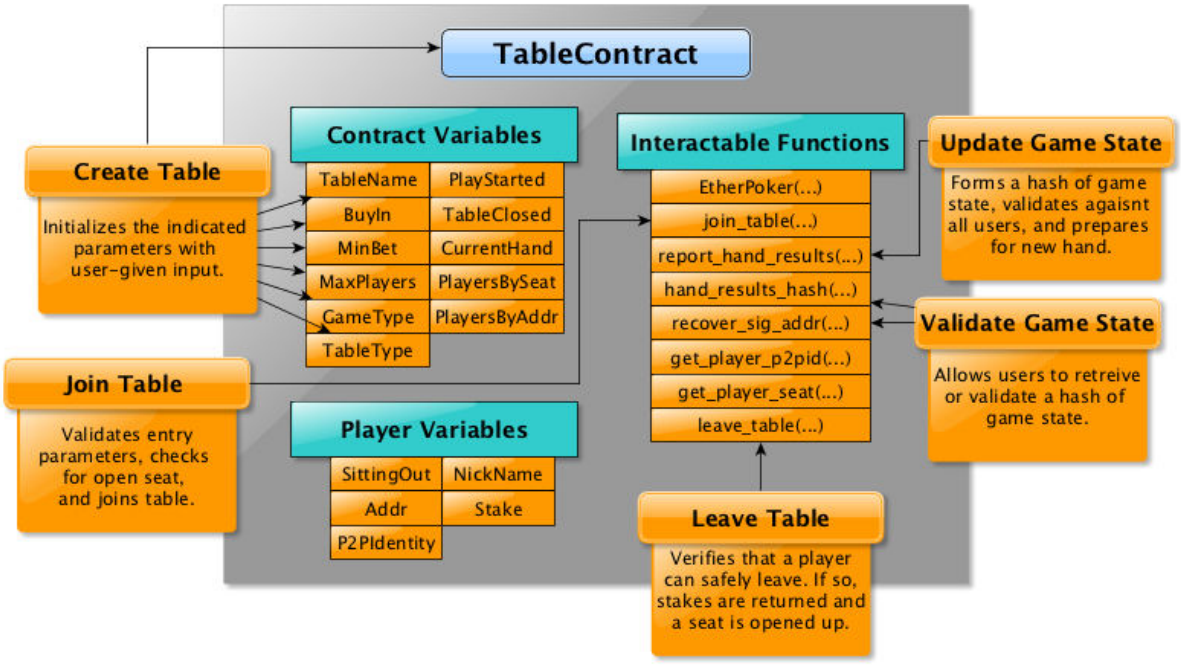
8.3 Contrat de table Ethereum

Jouer une partie de poker exclusivement sur la blockchain Ethereum nécessite du temps et des ressources considérables. Afin de rendre le jeu plus fluide, les contrats de table permettent de gérer les joueurs et de vérifier les résultats de chaque main, la logique de jeu étant exécutée hors chaîne.

8.3.1 Fonctions

VirtuePokerTable : initialise la table de poker avec les paramètres fournis.
Join_table : rejoint une table, crée une structure de joueur à l'aide des paramètres fournis, et envoie un message d'erreur, le cas échéant.
Get_player_seat : renvoie le numéro de siège de l'utilisateur qui a envoyé le message ou -1 si l'utilisateur n'a pas de siège.
Get_player_p2pid : renvoie le p2pid correspondant au joueur spécifié par le numéro de siège ou une chaîne vide.
Hand_results_hash : calcule un hachage SHA-3 des paramètres fournis par l'utilisateur.
Recover_sig_addr : renvoie l'adresse associée à la paire de clés utilisée pour signer le hachage.
Report_hand_results : vérifie que tous les joueurs ont signé les données du jeu et renvoie un message d'erreur le cas échéant.
Leave_table : élimine le siège du joueur et retourne les gains de celui-ci.

Figure 15 : Variables du contrat de table



8.4 GameNet

GameNet fournit l'interface de communication de notre application. Nous disposons de deux flux de communication principaux :

- Communication avec d'autres joueurs à l'aide de P2PNet.
- Communication avec le réseau Ethereum à l'aide de Web3.js

Par exemple, quand un utilisateur rejoint une table de poker, il interagit avec le réseau Ethereum.

Quand un utilisateur rejoint une table de poker, il verse de l'argent sur cette table et prélève les fonds de son portefeuille. GameNet est aussi le module qui se charge de stocker les fonds de manière privée et sécurisée : le keystore.

8.4.1 KeyStore

Le portefeuille qui stocke les fonds est représenté par une clé publique et une clé privée.

- La clé publique correspond à l'adresse publique utilisée pour recevoir les fonds.
- La clé privée sert à envoyer les fonds.

Les fonds sont envoyés au moyen d'une transaction, laquelle est signée par la clé privée. Les fonds sont sécurisés à condition que la clé privée le soit. Par conséquent, si quelqu'un accède à la clé privée, il accède également aux fonds.

Notre magasin de clés utilise les mêmes fonctions de dérivation de clés (Scrypt), chiffrement symétrique (AES-128-CTR) et codes d'authentification de messages que geth, l'implémentation officielle en Go du protocole Ethereum.

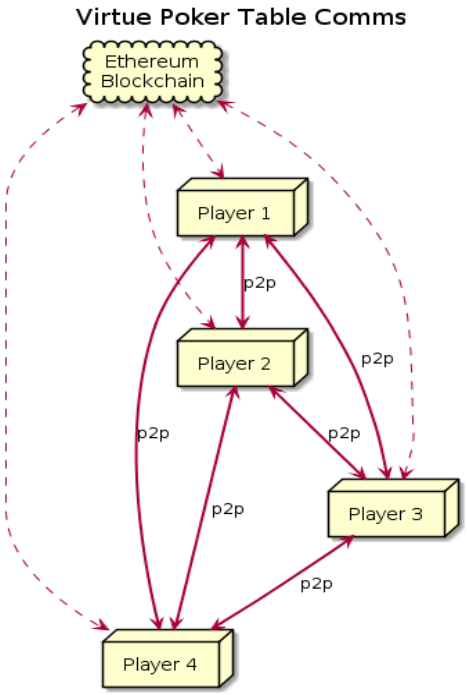
Les clés sont enregistrées sur le disque dur et sont sécurisées par un mot de passe qui s'utilise pour jouer sur Virtue Poker.

8.5 P2PNet

P2PNet se charge de toutes les communications effectuées entre les utilisateurs sans utiliser le réseau Ethereum. Dans le contexte des DApps, on parle de *off-chain*. Les ressources du réseau Ethereum sont utilisées à travers toutes les DApps et toutes les transactions vers le réseau Ethereum génèrent des frais, c'est pourquoi nous devons être aussi efficaces que possible avec les DApps. Nous tâchons de minimiser la taille de nos contrats afin de limiter la surcharge, et de limiter les communications avec la blockchain Ethereum afin de réduire les frais d'exploitation et d'améliorer la vitesse du jeu.

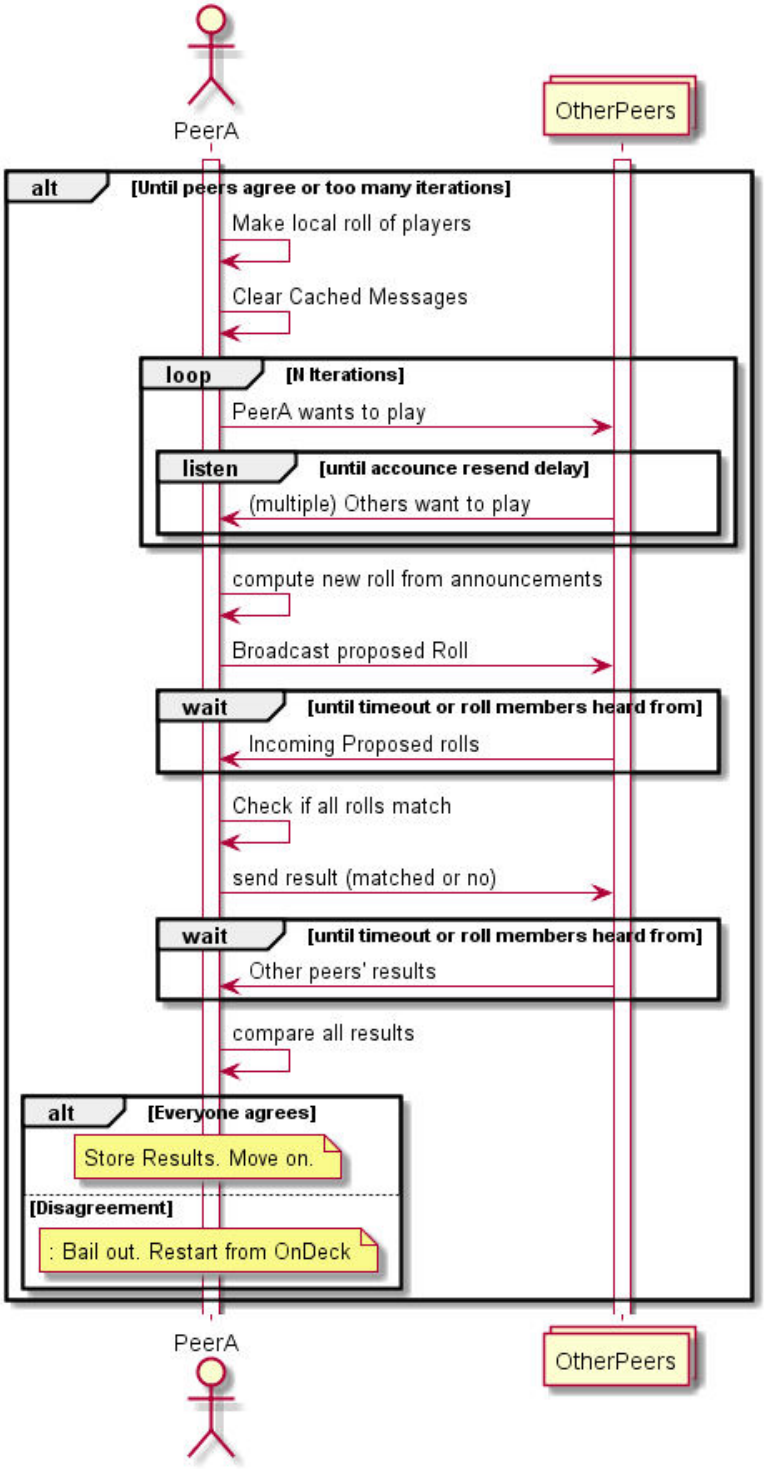
Notre P2PNet n'utilise pas les state channels tels qu'ils sont définis, mais à un certain niveau, tout ce qui est transporté par P2PNet (sauf le chat) fait partie d'un « state subnet » dans lequel tous les clients du jeu conviennent avec un autre off-chain de ce qui s'est passé. Cette opération s'effectue de telle sorte que la blockchain peut vérifier qu'il y a eu consensus, mais elle ne peut revenir en arrière et rejouer chaque déplacement individuel.

Figure 16 : Communications P2P



Au début de chaque main, tous les joueurs d'une table commencent un « roll-call » pour vérifier les messages provenant de chacun des autres joueurs assis, et se mettent tous d'accord sur les joueurs de la main suivante. La Figure 17 illustre ce processus :

Figure 17 : « Roll Call »



8.6 Web3.js

Web3.js est l'API JavaScript compatible avec Ethereum qui implémente la spécification Generic JSON RPC. Web3.js est une bibliothèque officielle créée par l'équipe Ethereum. Nous l'utilisons pour :

- **Compiler un contrat** : nos contrats sont pré-compilés et correctement testés avant de les compiler avec web3.js. La compilation d'un contrat est requise avant tout déploiement avec web3.js.
- **Déployer un contrat** : web3.js fournit une API Javascript simple et sécurisée pour déployer un contrat.
- **Appel de contrat** : une fois qu'un contrat est déployé, toute interaction avec celui-ci constitue un appel qui s'effectue également à l'aide de l'interface web3.js.
- **Transactions** : toute autre action impliquant l'accès au réseau Ethereum s'effectue toujours avec Web.js.

8.7 Electron

Notre application bureau est basée sur Electron. Electron a déjà été utilisé avec succès dans le cadre d'autres projets basés sur Ethereum, y compris Mist Ethereum Wallet, Atom, Visual Studio Code et Jaxx Wallet. Electron est un framework open-source, mis au point par Github, pour créer des applications natives à l'aide de technologies Web comme JavaScript, HTML et CSS. Nous avons choisi Electron pour les raisons suivantes :

1. **Framework multi-plateformes** : en codant une seule fois, on dispose d'un produit qui fonctionne sur plusieurs plateformes – dans notre cas, Windows, Mac et Linux.
2. **Basé sur des technologies Web** : nous pouvons créer notre application avec les mêmes technologies utilisées pour créer des sites Web, sans avoir à embaucher des développeurs pour des plateformes particulières.
3. **Réduit les frais de développement** : nous pouvons diminuer les coûts de développement en recrutant des développeurs de talent, qui n'ont pas forcément besoin de maîtriser une plateforme en particulier.
4. **Améliore la vitesse de développement** : comme nous n'avons pas besoin de recruter de développeurs pour coder certaines plateformes, toutes nos ressources sont consacrées au développement d'un seul produit qui fonctionne sur plusieurs plateformes avec Electron.

8.7.1 Architecture d'Electron

L'architecture d'Electron repose sur :

- **Chromium :** navigateur Web utilisé par Google Chrome et Chrome OS. Nous pouvons ainsi créer notre application à l'aide des technologies Web.

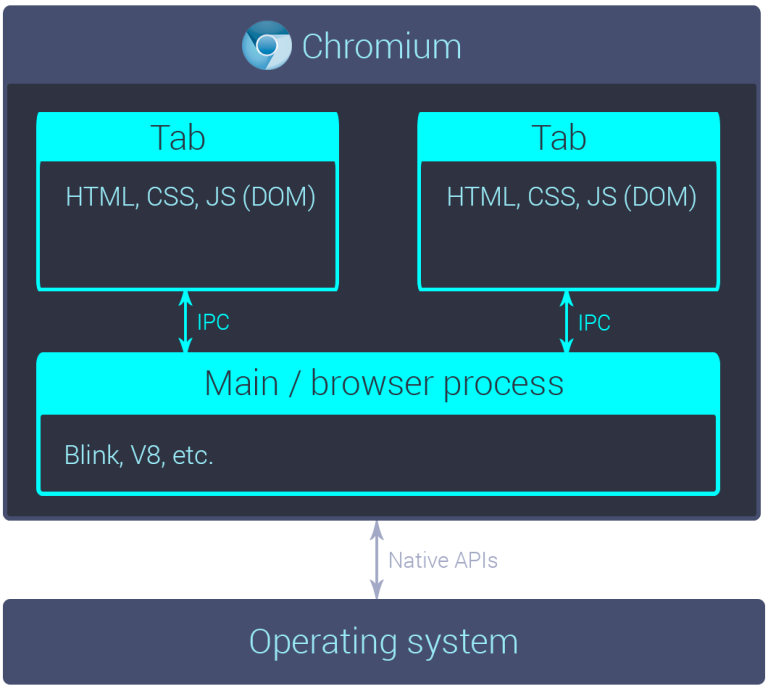
- **NodeJS :** Node est un moteur Javascript créé à partir du moteur Chrome/Chromium V8 Javascript. Il fournit un accès aux ressources du système d'exploitation (par exemple, le système de fichiers).

Chaque nouvelle version d'Electron fournit la toute dernière version de Chromium et NodeJS.
Lors de la rédaction de ce livre blanc, il s'agit de la version Electron 1.6.11, qui contient :

- Node **7.4**
- Chromium **56.0.2924.87**
- V8 **5.6.326.50**

Pour en savoir plus sur Electron, consultez la page : https://electron.atom.io/

Figure 18 : Chromium

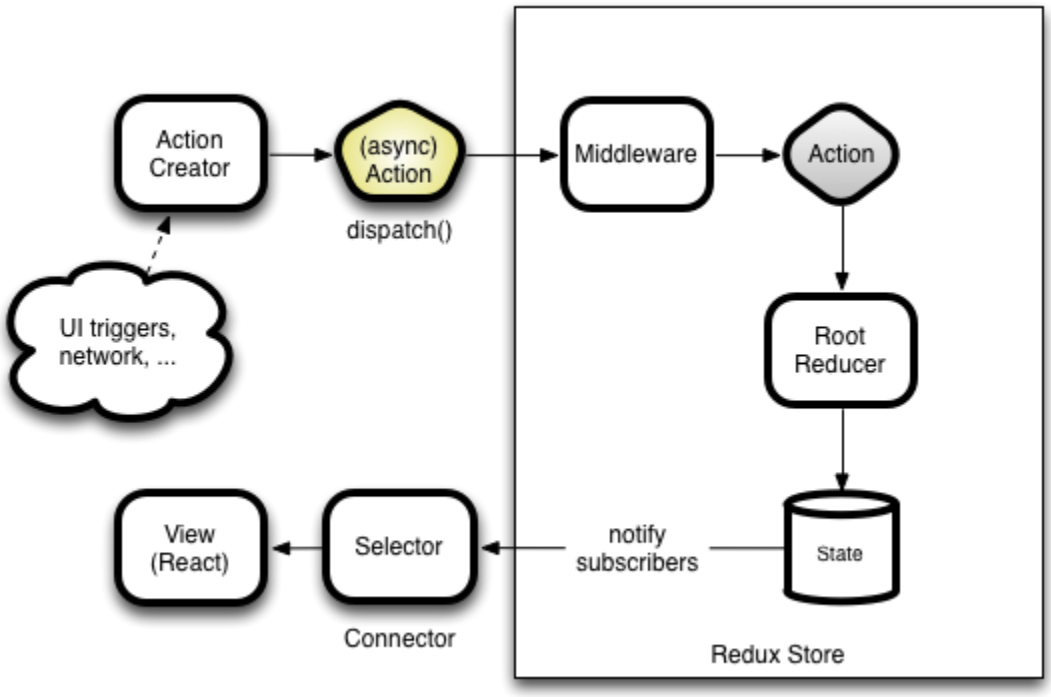


8.8 Client du jeu de poker

8.8.1 Architecture du client du jeu

Notre client du jeu est créé à l'aide de l'architecture React Redux.

Figure 19 : React



8.8.2 Jeu

L'interface utilisateur du jeu se composera de deux éléments qui s'afficheront dans différentes fenêtres :

- Lobby
- Table

Quand un joueur commence une partie, il se trouve dans le lobby et peut réaliser les actions suivantes :

Se connecter : l'utilisateur saisit ses identifiants pour se connecter à l'application.
Créer une table de jeu : l'utilisateur peut créer une table de jeu privée (seulement privée, ou bien publique).
Lister toutes les tables disponibles : le lobby affiche toutes les tables que les joueurs peuvent rejoindre pour jouer.

Rejoindre une partie : l'utilisateur peut rejoindre une table ou un tournois.
Gérer le portefeuille : l'utilisateur peut gérer son portefeuille de poker virtuel.
Jouer : la table de jeu s'ouvre dans le composant de l'interface utilisateur de la table, dans une fenêtre distincte.
Jouer plusieurs parties en même temps : l'utilisateur peut rejoindre plusieurs parties en même temps.
