



VIRTUE POKER

Informe de Virtue Poker

Una plataforma de póquer descentralizada creada con Ethereum

Versión borrador 0.9

Marzo de 2018

El presente documento solo tiene fines informativos y no constituye una oferta o solicitud para vender acciones o valores en Virtue Poker, o en cualquier empresa relacionada o asociada. Toda oferta o solicitud solo se realizará mediante un memorando de oferta confidencial y acorde a las condiciones aplicables de valores y otras leyes.

Este documento es un borrador y solo se proporciona a modo de cortesía y con el objeto de iniciar el proceso de retroalimentación de la industria y de la comunidad. Este documento no debe considerarse como final y toda la información que se incluye está sujeta a cambio sin aviso previo. En la medida en que Virtue Poker, en algún momento del futuro, ofrezca cualquier producto o servicio en venta, que incluye fichas, deberá consultar y revisar las condiciones y acuerdos de confidencialidad vigentes en dicho momento. Esto es válido para cualquier versión actualizada del presente Informe.

Tabla de contenido

Tabla de contenido

1. Resumen

- 1.1 Propositiones de valor
 - 1.1.1 Eliminar el riesgo del depósito del jugador
 - 1.1.2 Resolver el persistente problema de confianza respecto a la rectitud en el juego
 - 1.1.3 Reducir los costos del jugador y crear un ecosistema de póquer equilibrado
 - 1.1.4 Desarrollar una red de póquer descentralizada extensible
- 1.2 Objetivo de corto plazo
- 1.3 Estrategia de crecimiento a largo plazo

2. Problemas con el póquer en línea

- 2.1 Introducción
- 2.2 Mal uso de los fondos del jugador
 - 2.2.1 Apuesta absoluta y apuesta definitiva
 - 2.2.2 Full Tilt Poker
 - 2.2.3 Lock Poker
- 2.3 Bots de Póquer
- 2.4 Herramientas y software de terceros
- 2.5 Rake desigual
- 2.6 La economía interrumpida del póquer
 - 2.6.2 El problema
- 2.7 Fragmentación del mercado global
 - 2.7.1 Mercados negros
 - 2.7.2 Mercados gris oscuro
 - 2.7.3 Mercados grises
- 2.8 Tipos de operadores
 - 2.8.1 Operadores 'onshore'
 - 2.8.1 Operadores 'offshore'
- 2.9 Competencia limitada
 - 2.9.1 Mercado B2C regulado
 - 2.9.1 Mercado B2C no regulado
- 2.10 Prácticas de certificación de generador de números aleatorios
- 2.11 Conclusión

3. La solución Virtue

- 3.1 Flujo del usuario
 - 3.1.1 Descargar Virtue Poker Client
 - 3.1.2 Registro
 - 3.1.3 Financiar una Cartera
 - 3.1.4 Crear un juego o unirse a un juego
 - 3.1.5 Buy-In
 - 3.1.6 Juego
 - 3.1.7 Payout

- 3.2.1 uPort
- 3.2.2 Contratos inteligentes de Ethereum
- 3.2.3 Game Client
- 3.2.4 Mensajería P2P
- 3.2.5 IPFS
- 3.3 Administración de identidad
- 3.4 Contratos inteligentes de Ethereum
 - 3.4.1 Contrato de casino
 - 3.4.2 Contrato de mesa
 - 3.4.3 Interacciones de jugadores con los contratos de mesa
 - 3.4.4 Contrato de torneo de mesas múltiples
 - 3.4.5 Contrato de administración de jueces
- 3.5 Mental Poker
 - 3.5.1 Descripción general
 - 3.5.2 Algoritmo de Mental Poker: el barajado de dos pasadas
 - 3.5.3 Dos rondas de cifrado: barajar el mazo e indexar el mazo
- 3.6 Mensajería punto a punto (P2P)
 - 3.6.1 Mensajería P2P para sincronización del juego de cliente
 - 3.6.2 Juego fuera de blockchain
- 3.7 IPFS: Almacenamiento de registro de juegos de historias de manos
- 4. Seguridad del juego**
 - 4.1 Formas de hacer trampa en el póquer en línea
 - 4.1.1 Colusión
 - 4.1.2 Contabilidad múltiple
 - 4.1.3 Minería de datos
 - 4.1.4 Bots de póquer
 - 4.1.5 Cuenta compartida
 - 4.2 El sistema de jueces para combatir las trampas
 - 4.2.1 Funciones principales de los jueces
 - 4.2.2.1 Resolución de disputas
 - 4.2.2.2 Fuente de alimentación de datos
 - 4.2.2.3 Almacenamiento parcial de las claves de cifrado del jugador
- 5. VPP: Virtue Player Points (Puntos de jugador de Virtue)**
 - 5.1 Para convertirse en juez
 - 5.1.1 Proceso de revisión de solicitudes para ser juez
 - 5.1.2 Remuneración de los jueces
 - 5.2 Moneda de juego
 - 5.3 Torneos especiales
- 6. Hoja de ruta**
 - 6.1 Actividades clave
 - 6.1.1 Desarrollo de la plataforma
 - 6.1.2 Crecimiento de la comunidad
 - 6.1.3 Patrocinios y relaciones públicas
 - 6.1.4 Aspectos legales

- 6.2 Hoja de ruta de desarrollo
 - 6.2.1 Estado actual
 - 6.2.2 Desarrollos futuros
 - 6.2.3 Primer trimestre de 2018
 - 6.2.4 Segundo trimestre de 2018
 - 6.2.5 Segundo y tercer trimestre de 2018
 - 6.2.6 Cuarto trimestre de 2018
 - 6.2.7 2019

7. El equipo

- 7.1 Equipo central
- 7.2 Asesores
- 7.4 Equipo de Virtue Poker
- 7.4 Socios legales

8. Apéndice: La arquitectura de Virtue Poker

- 8.1 Arquitectura del sistema
 - 8.1.1 Componentes
- 8.2 Motor de juego
 - 8.2.1 Máquina de estado
 - 8.2.2: Estado conectado o fuera de línea
 - 8.2.3: Estados del lobby
 - 8.2.4: Estados de juego

_Toc256000119

- 3.4.2 Contrato de mesa de Ethereum
 - 8.3.1 Funciones
- 8.4 GameNet
 - 8.4.1 Almacén de claves
- 8.5 P2PNet
- 8.6 Web3.js
- 8.7 Electron
- 8.8 Cliente del juego de póquer
 - 8.8.1 Arquitectura del cliente de juego
 - 8.8.2 Juego

1. Resumen

El póquer en línea ha crecido desde un puñado de empresas emergentes a principios de la década del 2000, hasta la industria multimillonaria en que se ha convertido hoy. Y desde su concepción, el póquer ha enfrentado dos problemas críticos: el juego justo y la seguridad de los fondos de los jugadores. Estos dos problemas estuvieron al centro de una serie de escándalos en la industria que acabaron con varias empresas líderes en el negocio del póquer en línea.

Virtue Poker cambia todo eso. Es una plataforma descentralizada para jugar al póquer en línea con dinero real. Aprovecha el blockchain de Ethereum para proporcionar la primera experiencia de póquer en línea basada en blockchain donde los jugadores nunca deberán depositar dinero en un sitio, donde las cartas se barajan de forma comprobadamente aleatoria y las cartas son cifradas.

1.1 Propositiones de valor

En Virtue Poker, no hay servidores que almacenen los fondos de los jugadores y cada jugador participa al momento de barajar las cartas. Nuestros objetivos son:

1.1.1 Eliminar el riesgo del depósito del jugador

Virtue Poker permite a los jugadores tener tutela permanente de sus fondos mediante el uso de contratos inteligentes de Ethereum para custodiar los buy-in de los torneos y distribuir los pagos de forma autónoma en función de los resultados del juego.

1.1.2 Resolver el persistente problema de confianza respecto a la rectitud en el juego

Mediante el uso de un protocolo de ordenamiento criptográfico aleatorio punto a punto llamado Mental Poker, todos los jugadores sentados en una mesa participan al momento de barajar las cartas y logran el consenso al final de cada mano utilizando un mecanismo de consenso de Tolerancia a falla bizantina (BFT).

1.1.3 Reducir los costos del jugador y crear un ecosistema de póquer equilibrado

La innovadora arquitectura descentralizada punto a punto de Virtue Poker, junto al uso de Ethereum, le permite a Virtue Poker eliminar los costosos gastos de procesamiento de pagos y servidores. En el sistema Virtue Poker, la mayoría de las funciones de los juegos que normalmente se realizan en servidores centralizados, se distribuyen, y los fondos de los jugadores siempre permanecen en carteras que están aseguradas por *contratos inteligentes*. Virtue Poker transferirá estos ahorros a los jugadores a través de incentivos más bajos de rake y jugadores, permitiendo que más dinero permanezca en el ecosistema del póquer.

1.1.4 Desarrollar una red de póquer descentralizada extensible

El objetivo de Virtue Poker es desarrollar una red principal descentralizada subyacente de póquer en línea, a la cual los desarrolladores y operadores de terceros puedan agregar y sobre la cual pueden construir. Es nuestro deseo, y esperamos que se creen nuevas funcionalidades sobre la plataforma.

1.2 Objetivo de corto plazo

Virtue Poker está construyendo una aplicación lista para producción que se implementará en la red principal de Ethereum. Para lograr esto y llevar a la compañía hacia su lanzamiento, Virtue Poker desarrollará sus equipos de desarrollo y marketing. El equipo de desarrollo se enfocará en desarrollar la interfaz de usuario, el barajado distribuido y tecnologías de blockchain. El equipo de marketing trabajará en el desarrollo de compromiso de nuestros usuarios alfa para obtener retroalimentación del producto e iterar el diseño de la plataforma antes del lanzamiento.

1.3 Estrategia de crecimiento a largo plazo

Nuestra estrategia a largo plazo se compone de dos fases generales: (1) como operador de empresa a consumidor (B2C), desarrollar tecnología y liquidez para la plataforma, con el objetivo de demostrar la conveniencia, integridad y credibilidad de nuestra solución, y (2) expandirse globalmente a través del formato de etiqueta blanca para permitir nuevos titulares de licencia en mercados de todo el mundo. Esto

permite a las empresas de terceros iniciar, sin problemas y de manera económica, su propia sala de póquer en línea basada en blockchain utilizando nuestra tecnología principal y proporcionar un flujo continuo de ingresos.

2. Problemas con el póquer en línea

2.1 Introducción

Los juegos en línea se han convertido en una industria multimillonaria. Se espera que alcance los \$50 mil millones para el año 2021.¹ El póquer ha estado al centro de este éxito fenomenal. El crecimiento de las salas de póquer en línea estalló luego del Evento Principal de la Serie Mundial de Póquer televisado en 2003, en el que un jugador aficionado desconocido, un contador llamado Chris Moneymaker, ganó \$2,5 millones.

En la actualidad, el mercado global del póquer en línea supera los \$ 2.500 millones de dólares. A nivel mundial, el mercado está dominado por Europa y Asia, con 47% y 30% del mercado, respectivamente, América del Norte con 13%, Oceanía con 6% y Latinoamérica con 2%.²

Desgraciadamente, la industria del póquer en línea ha enfrentado varios escándalos y ha sido víctima de usuarios malintencionados. Aunque los principales sitios de póquer como PokerStars.com han adaptado su plataforma a este comportamiento problemático, muchos sitios no se han ajustado, creando una desconfianza persistente entre muchos jugadores.

2.2 Mal uso de los fondos del jugador

2.2.1 Apuesta absoluta y apuesta definitiva

Luego de años de quejas de los jugadores, Cereus Network, la tercera red de póquer más grande (operadores de Ultimate Bet y Absolute Poker) admitió que un ex empleado había obtenido acceso a una cuenta de administrador que le permitía ver todas las cartas de los jugadores en la plataforma. Durante los años que duró el fraude, este individuo y sus cómplices robaron decenas de millones de dólares.³

2.2.2 Full Tilt Poker

El 15 de abril de 2011, día conocido como el "viernes negro" en la comunidad del póquer en línea, los fiscales federales de EE. UU. acusaron a los fundadores de los tres mayores sitios web de póquer en línea, PokerStars, Full Tilt Poker y Absolute Poker, y obligaron a esos sitios a dejar de ofrecer un juego con dinero real a los ciudadanos estadounidenses. Cuando Full Tilt se reabrió poco después fuera de EE. UU., se descubrió que tenía un déficit de \$360 millones (es decir, se habían malversado \$360 millones en depósitos de los jugadores). La compañía cerró sus operaciones poco después.⁴

¹ Informe anual de 888 de 2016: <http://corporate.888.com/sites/default/files/888%20AR%202016%20Hyperlinked%20PDF.pdf>

² Informe anual de Playtech de 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." Los sitios de póquer más seguros. Safest Poker Sites, n.d. Web. 07 de octubre, 2016.

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

2.2.3 Lock Poker

En el año 2015, Lock Poker, que ofrecía juegos a residentes de EE.UU., cerró después de incumplir con los retiros de los jugadores durante casi un año. Los jugadores perdieron aproximadamente \$15- \$24 millones.⁵

2.3 Bots de Póquer

Un bot de póquer es un programa de software que emula a jugadores reales en línea. Los bots de póquer pueden ubicarse en varias mesas y pueden ejecutarse sin supervisión humana. Los bots de póquer varían en complejidad: se pueden comprar listos para usar o se pueden crear de forma personalizada, y ser empleados por un actor individual.

En 2015, un grupo de bots ganó casi \$1,5 millones en juegos en efectivo de \$0,50/\$1,00 y \$1/\$2 en PokerStars.⁶ Hay empresas como WarBot que venden bots listos para usar a los usuarios y que pueden ser operados en todas las plataformas.⁷ Las empresas que cotizan en la bolsa, como 888 Holdings, tienen procedimientos de seguridad, en gran parte ineficaces, para proteger a los jugadores contra los bots. Esta empresa incluso tiene una publicación de blog titulada "Cómo jugar contra bots de póquer", llamándolos "débiles"⁸.

Pero los robots son, de hecho, una amenaza real. En 2017, la Universidad Carnegie-Mellon organizó una competencia llamada "Cerebros vs. inteligencia artificial: alzar el antes", en la que cuatro de los mejores profesionales del póquer heads-up compitieron contra un bot de póquer denominado Libratus, y perdieron.⁹ Aunque Libratus es operado por una supercomputadora, los bots de póquer de todos los tipos representan una amenaza significativa para el éxito futuro de la industria.

2.4 Herramientas y software de terceros

Muchos jugadores en línea usan herramientas y software de terceros orientados a jugadores recreativos.¹⁰ Estas herramientas incluyen (pero no se limitan a):

Bases de datos de jugadores: una base de datos de jugadores que se puede consultar para encontrar jugadores con bajas tasas de ganancias en múltiples redes de póquer

Asientos automáticos: sienta automáticamente a los jugadores en los juegos con efectivo de calidad y en los torneos de Sit & Go, y también asigna códigos de colores a los jugadores según sus estadísticas

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>

Escaneo de jugadores: escanea a los jugadores que se encuentran en el momento en el lobby de un sitio de póquer y que cumplen criterios específicos

Visualizaciones de heads-up: muestra las estadísticas en tiempo real de los oponentes en las mesas activas

Estas herramientas están diseñadas para entregar a los jugadores acceso a información sobre sus oponentes. Desgraciadamente, estas herramientas crean una desventaja para los jugadores recreativos que no usan estos programas, que sin saberlo son blanco de profesionales altamente calificados.

2.5 Rake desigual

El rake se recolecta en torneos o juegos en dinero en efectivo. Para los torneos, se agrega un porcentaje, típicamente 6-10%, al buy-in. En los juegos con dinero en efectivo, se deduce un porcentaje de cada mano. El rake de juegos con efectivo en línea es típicamente 3-5%, con un límite entre \$0,30 y \$5 por mano, dependiendo de los límites con que se juegue. Si bien los rakes difieren ligeramente en diversos sitios, en general, la estructura del rake es muy similar en todas las salas de póquer en línea.

La Figura 1 muestra la estructura actual de rake de PokerStars.¹¹ A primera vista, esta estructura parece tener sentido: en términos absolutos, los jugadores con apuestas mayores pagan más comisión que los jugadores con apuestas menores, y son clientes más valiosos:

Figura 1: Ejemplo de rake de 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

Cabe notar que del límite para las apuestas más bajas (\$0,01/\$0,02) para un juego de más de 5 personas es 15 veces la ciega grande, pero para un juego de \$3/\$6, el límite es de 0,58 veces la ciega grande.

Según un estudio de investigación de 2011 de la Universidad de Hamburgo, que analizó más de 2,5 millones de manos durante un período de seis meses en PokerStars y otros sitios, cada jugador de \$ 0,01/\$ 0,02 paga de rake un promedio de 12,5 BB (ciegas grandes) por cada 100 manos, mientras que los de \$3/\$ 6 pagan 2,58 BB por cada 100 manos.¹² La Figura 2 resume el rake promedio pagado por cada 100 manos en cada nivel diferente según el estudio:

Figura 2: Rake entre apuestas

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

A medida que aumenta la apuesta, disminuye drásticamente el rake en relación con la ciega grande. Una tasa de ganancias de 4-6 BB por cada 100 manos es excelente para los estándares de póquer en línea. Con las estructuras de rake actuales, la mayoría de los jugadores ganadores se convierten en jugadores perdedores cuando juegan con límites bajos, mientras que solo aquellos en los niveles más altos tienen la oportunidad de tener ingresos al jugar en línea.

2.6 La economía interrumpida del póquer

2.6.1 Definición

La economía del poker tiene tres entradas clave: depósitos, rake y retiros. Para que la economía mundial del póquer crezca, la siguiente fórmula debe operar:

$$\text{Depósitos} > (\text{Rake} + \text{Retiros})$$

Este modelo requiere un suministro constante de depósitos para sobrevivir. Los jugadores profesionales tienen un saldo neto positivo sobre los retiros (es decir, ganan más de lo que pierden, y lo retiran), mientras que los jugadores recreativos generalmente tienen un saldo neto negativo, creando un ecosistema equilibrado.

2.6.2 El problema

Desgraciadamente, los jugadores ganadores (generalmente semiprofesionales y profesionales) tienen una tasa mayor a lo que depositan los jugadores perdedores, creando una presión sobre la economía del póquer. Esto se debe a una mayor competencia ya que la estrategia del póquer se ha hecho pública y disponible a través de tutoriales en línea, blogs y otra literatura, y debido a la dinámica desfavorable creada para jugadores recreativos derivados de un rake desproporcionado, herramientas de terceros que rastrean y cazan jugadores menos experimentados y la desconfianza entre los jugadores recreativos con respecto a la integridad del póquer en línea.

2.7 Fragmentación del mercado global

Las regulaciones restringen la capacidad de los operadores para servir a los clientes en las principales jurisdicciones y regiones. Las jurisdicciones se clasifican en las siguientes categorías en función de la respuesta reglamentaria (la nomenclatura exacta varía):

2.7.1 Mercados negros

Los mercados negros son jurisdicciones que han clasificado al poker en línea como ilegal o solo permiten los juegos dentro del estado.

2.7.2 Mercados gris oscuro

Los mercados gris oscuro son jurisdicciones que no prohíben explícitamente el juego en línea y/o tienen una legislación poco clara.

2.7.3 Mercados grises

Los mercados grises son jurisdicciones que han regulado los juegos de azar en línea, o no han tomado ninguna medida contra los operadores remotos.

2.8 Tipos de operadores

Dentro de este marco regulatorio, los operadores eligen operar en múltiples mercados con una sola licencia o múltiples licencias, o en todos los mercados con una sola licencia o sin una licencia. Estos se pueden clasificar como *operadores 'onshore'* y *operadores 'offshore'*.

2.8.1 Operadores 'onshore'

Los operadores regulados han obtenido al menos una licencia de juego de una autoridad de juego reconocida y operan normalmente en la mayoría de los mercados grises y grises oscuros. Por lo general, estos operadores cumplen a las regulaciones contra el lavado de dinero (AML), Conozca a su cliente (KYC), políticas de impuestos y otras políticas de cumplimiento, y muchas son compañías que cotizan en varias bolsas en todo el mundo. Los operadores 'onshore' incluyen a The Stars Group (PokerStars, Full Tilt Poker), William Hill Online, Playtech (red iPoker), GVC Holdings (PartyPoker, bwin.party), 888 Holdings, Unibet, Winamax y otros.

2.8.1 Operadores 'offshore'

Los operadores no regulados suelen residir en jurisdicciones extraterritoriales en Costa Rica, Curazao, Chipre o en reservas indígenas. Por lo general, ofrecen sus servicios en todo el mundo, incluidos los mercados negros. Hay datos relativamente pocos datos que se pueden obtener de estos operadores.

Los

operadores incluyen: PaiWangLuo Network (Ignition, Bovada), Merge Gaming (Carbon Poker), Winning Poker Network (America's Cardroom), Global Gaming Network, TheHive, Tiger Gaming (Chico) y muchos otros.

Muchas jurisdicciones y países de todo el mundo han comenzado a reglamentar el póquer en línea, lo que ha aumentado la proporción del tráfico regulado de póquer en línea.

2.9 Competencia limitada

El éxito de las redes de póquer en línea depende del establecimiento de grandes pozos globales de liquidez de jugadores. Con el tiempo, el mercado se ha reducido a unos pocos operadores grandes dentro de sus respectivos mercados objetivo, dejando a los jugadores con opciones de juego limitadas y permitiendo a los operadores cobrar tarifas más altas a los jugadores.

2.9.1 Mercado B2C regulado

Dentro del mercado B2C regulado, PokerStars se ha posicionado como el líder del mercado, con más de \$850 millones en ingresos anuales y aproximadamente 60% del tráfico mundial en línea. Opera en casi todos los países del mundo (incluidos 30 mercados en la lista negra) y tiene los premios en efectivo y torneos más importantes. Ha organizado el torneo de póquer en línea más grande del mundo (253.000 entradas) y ha regalado el mayor pozo de premios (\$8 millones). Ha repartido más de 145 mil millones de manos de póquer,

y patrocina a los mejores profesionales del poker, realizando giras en vivo. Y además tiene nombres tan destacados como Kevin Hart, Usain Bolt, Rafa Nadal y Ronaldo como embajadores de la marca. PokerStars ha invertido en protección para jugadores, como detección de bots de primera línea, numerosas opciones de procesamiento de pagos y prevención de contabilidad múltiple, y han podido crear el mayor pozo de liquidez del mundo.

Existen dos desventajas principales al jugar en PokerStars: (1) sus servicios son costosos para los jugadores como resultado de las estructuras de un alto valor de rake y, (2) la competencia en PokerStars es considerablemente más calificada que en otras plataformas. Y debido a su posición líder en el mercado, pueden operar con un mínimo de oposición de parte de los jugadores, lo que les permite reducir o eliminar los antiguos programas de lealtad, aumentar las tarifas y retirarse de los mercados con poca participación.

2.9.1 Mercado B2C no regulado

El mercado de poker en línea no regulado está algo más fragmentado, pero está dominado por Winning Poker Network (America's Cardroom) y la recientemente renombrada PaiWangLuo Network (Ignition, Bovada). Estas empresas están más dispuestas a servir los mercados negros y carecen de transparencia en sus prácticas comerciales. En términos generales, estos sitios invierten poco en prácticas contra las malas prácticas, como detección de bots o contabilidad múltiple, lo que deja a los jugadores solos en las plataformas.

Muchos jugadores han llegado a estas plataformas debido a opciones de juego limitadas o debido a la dura competencia en las plataformas reguladas. Sin embargo, la falta de debida diligencia y los requisitos para los informes dejan a los jugadores con un mínimo de recursos si estos sitios se desconectan, bloquean a los jugadores de sus cuentas o son acusados de irregularidades.

2.10 Prácticas de certificación de generador de números aleatorios

El póquer en línea es diferente de los juegos en vivo en un dominio clave: en un juego en vivo, los jugadores pueden ver al repartidor barajar el mazo de cartas, mientras que en la esfera en línea los jugadores deben *confiar* que el generador de números aleatorios (RNG) del operador sea operando adecuadamente. Casi todos los operadores en línea tienen su RNG certificado por terceros previamente autorizados. Las compañías de pruebas de RNG incluyen a iTech Labs (itechlabs.com) y Gaming Laboratories International (gaminglabs.com).

Desgraciadamente, incluso con las pruebas de RNG, existe una sorprendente falta de supervisión después que un operador recibe su certificación. Malta Gaming Authority utiliza el siguiente lenguaje en su sitio web: "Después del proceso de certificación requerido para la emisión de la licencia completa de cinco años, el sistema de juego no necesita ser probado regularmente, sin embargo, la Autoridad de Juego realizará auditorías de seguimiento cuando se considere prudente". La Isla de Man utiliza el siguiente lenguaje en su Guía para el juego en línea: "Aunque muchos operadores pueden revisar el RNG de sus juegos más frecuentemente, el GSC revisará el RNG del operador al menos dos veces durante la vida útil

de cinco años de una licencia".Esta falta de supervisión ha contribuido a la creencia prevalente entre los jugadores de póquer en línea, que los juegos pueden no ser del todo justos.¹³¹⁴

2.11 Conclusión

Los jugadores de póquer enfrentan numerosas desventajas en el mercado actual del póquer en línea. Los jugadores deben combatir el software malicioso, altas tarifas y una dura competencia en los mercados regulados, y en los mercados negros, se ven obligados a jugar en sitios que carecen de responsabilidad y transparencia. Y en general, el aumento de la competencia, las tarifas más altas y la desconfianza entre los jugadores recreativos ha llevado a una mayor tensión en la economía mundial del póquer.

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

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

3. La solución Virtue

Virtue Poker ha invertido años para investigar la dinámica del mercado de la industria del póquer en línea. Nuestro objetivo es revitalizar el póquer en línea mediante la creación de una red descentralizada de póquer en línea que incorpore confianza, transparencia y responsabilidad. Lo lograremos mediante la utilización de blockchain de Ethereum, redes punto a punto, identidad de propiedad del usuario y tarjetas protegidas por cifrado, que nos permiten ofrecer una mejor experiencia de juego a un menor costo para los jugadores. Más importante aún, utilizando estos nuevos marcos, buscamos solucionar el problema de la economía del poker al reducir los costos para los jugadores a través de un rake más bajo, crear estructuras de rakeback que fomenten la retención de jugadores, creando la plataforma de poker en línea más segura de la industria.

3.1 Flujo del usuario

Virtue Poker es una aplicación sin servidor que se ejecuta sin almacenar los fondos de los clientes e involucra a todos los jugadores al momento de barajar las cartas. El flujo del usuario es:

3.1.1 Descargar Virtue Poker Client

El usuario visita www.virtue.poker y descarga un cliente de Windows, Mac o Linux. La aplicación incluye un mezclador de cartas, un motor de juego y la interfaz de usuario.

3.1.2 Registro

El usuario luego crea una identidad uPort (uport.me) (si aún no la ha creado). El usuario firma digitalmente una certificación del país de residencia y la edad.

3.1.3 Financiar una Cartera

El usuario accede a una página que lo dirige a financiar la cartera liviana que está previamente incorporada en el software de cliente.

3.1.4 Crear un juego o unirse a un juego

Luego, el usuario puede ir a nuestro lobby que mostrará todos los juegos disponibles públicamente o crear un juego privado e invitar a otros jugadores.

3.1.5 Buy-In

El usuario puede unirse a un juego público o privado enviando Ether (ETH) o Virtue Player Points (VPP) a la dirección de la mesa de juego a la que desea unirse. El contrato inteligente se encuentra en la blockchain de Ethereum y actúa como una cuenta en custodia mientras el juego está en progreso. Cada juego es representado por un contrato de mesa que contiene los parámetros personalizados de ese juego en particular.

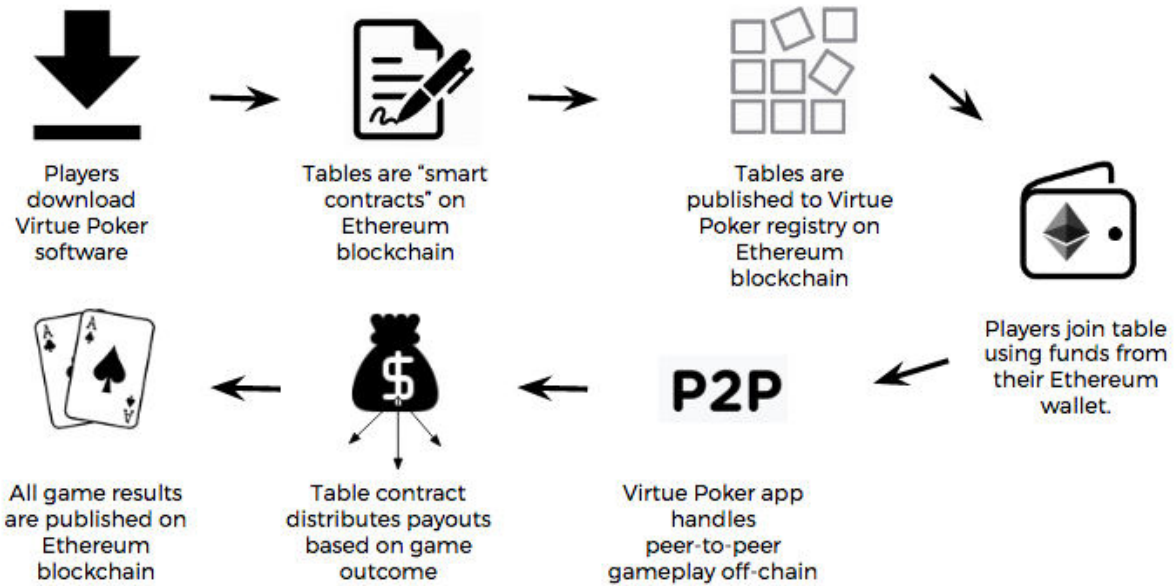
3.1.6 Juego

Los compañeros en la mesa forman una subred P2P y usan un protocolo de Mental Poker que requiere que cada compañero individual baraje y cifre el mazo de cartas.

3.1.7 Payout

Cuando se termina un torneo, o cuando un jugador sale de una mesa de juego en efectivo, el contrato de la mesa se autoejecuta y cada jugador recibe sus ganancias (si corresponde).

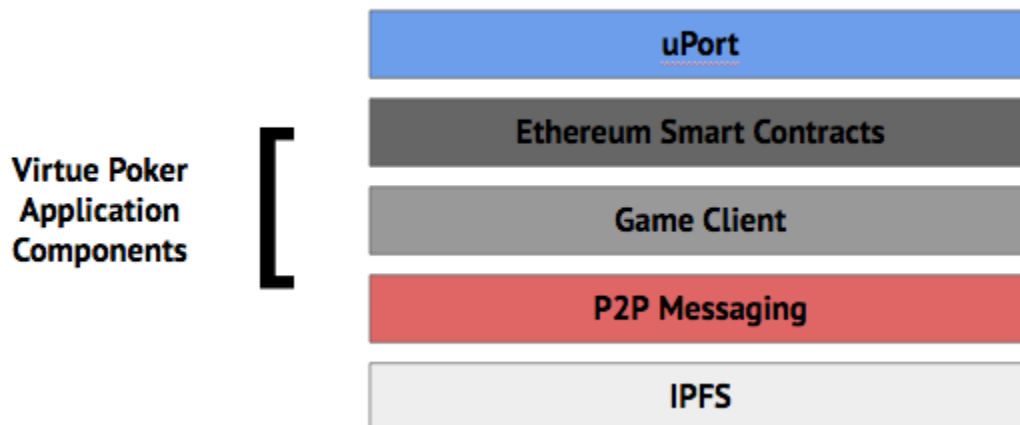
Figura 3: Cómo funciona Virtue Poker



3.2 Componentes de Virtue Poker

La plataforma de Virtue Poker utiliza varios subcomponentes dentro de la aplicación:

Figura 4: Componentes de Virtue Poker



3.2.1 uPort

La aplicación de identidad independiente basada en Ethereum, uPort, se utiliza como un mecanismo de registro y validación de identidad para prevenir el juego de menores de edad y la contabilidad múltiple. Los usuarios deben registrarse a través de uPort cada vez que deseen participar en juegos de Virtue.

3.2.2 Contratos inteligentes de Ethereum

Los contratos de Ethereum se utilizan: (1) como un registro (lobby) para todos los juegos activos en la plataforma, (2) como un servicio de custodia a corto plazo para los jugadores sentados en una mesa determinada, (3) como un repositorio para todos los parámetros específicos del juego, tales como, cantidad de buy-in, porcentajes de pago y tipo de juego, y (4) para informar los resultados del juego.

3.2.3 Game Client

Game Client es una aplicación de escritorio, un motor de estado que ejecuta la lógica del juego, baraja y reparte cartas utilizando un protocolo de Mental Poker, incluye una cartera liviana y se conecta con otros jugadores en una determinada mesa de poker.

3.2.4 Mensajería P2P

Una red troncal de mensajería P2P se utiliza como herramienta de comunicación y sincronización para garantizar que la interfaz de usuario muestre un estado de juego idéntico para todos los jugadores de una mesa determinada.

3.2.5 IPFS

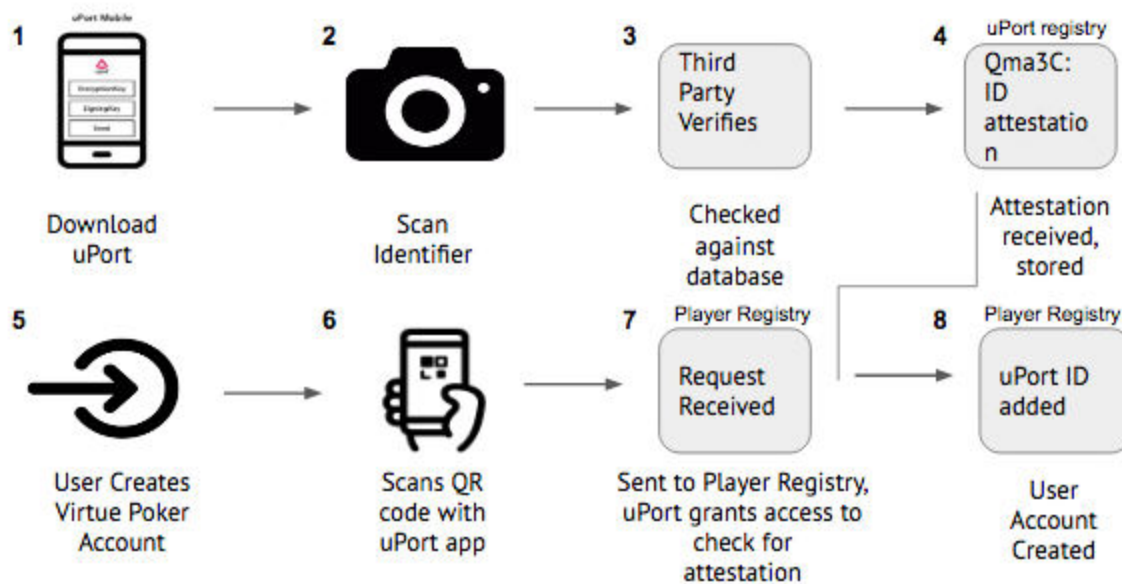
El Sistema de archivos interplanetarios (IPFS) se utiliza para registrar historiales de manos para todos los juegos en la plataforma. Los registros se pueden recuperar para su revisión, ya sea para el cumplimiento o para nuestro equipo de seguridad de juego. Este es también el componente que proporciona historiales de manos al usuario.

3.3 Administración de identidad

Virtue Poker utiliza la aplicación de identidad independiente uPort para validar la identidad de un jugador antes de permitir su acceso a la plataforma.¹⁵ Un ejemplo de este proceso se ilustra a continuación:

Figura 5: Ilustración de validación de identidad

¹⁵ <https://www.uport.me/>



Paso 1: Un usuario descarga la aplicación móvil uPort, crea una identidad uPort y luego escanea una copia de su comprobante de identidad verificado por terceros. La certificación se cifra y almacena en IPFS y el usuario recibe una certificación dentro de su ID de uPort respecto de su identidad.

Paso 2: Un usuario crea una cuenta en Virtue Poker y recibe un código QR que el usuario escanea con la aplicación uPort.

Paso 3: Se envía una nueva solicitud de cuenta a un contrato de Virtue Poker Accounts con la ID de uPort asociada, que verifica la certificación de terceros que ha verificado la identidad del usuario.

Paso 4: Si tiene éxito, la ID de uPort de ese usuario se asocia con su dirección de cuenta de Virtue Poker y se almacena en el Registro de jugadores de Virtue Poker.

3.4 Contratos inteligentes de Ethereum

Después de que un jugador ha verificado su identidad y creado su cuenta, al usuario se le lleva al Lobby, que es un contrato inteligente del casino.

3.4.1 Contrato de casino

El contrato del casino funciona como lobby. Contiene un registro de todos los juegos disponibles, así como de los juegos recientemente finalizados. Sus funciones incluyen la creación de juegos, así como la asociación a juegos y otras tareas de administración de front end, usuarios y juegos.

3.4.2 Contrato de mesa

Un Contrato de mesa representa una instancia única de un juego de póquer. Cuando se toma la decisión de comenzar un juego de póquer con un conjunto particular de reglas y límites, y un grupo determinado

de jugadores, se crea un nuevo contrato de mesa y los jugadores se unen a él para jugar. Cuando se termina el juego, se pagan las ganancias, los jugadores se van y el contrato de la mesa se cierra. Ya no se usa más que como punto de referencia.

Durante el juego, el contrato de la mesa sirve para varios propósitos. En primer lugar, es el repositorio de toda la información sobre las reglas y la configuración del juego que se está jugando. También posee una lista de los jugadores en el juego y la información sobre ellos que necesitan los otros jugadores. Además, el contrato de la mesa es donde los fondos utilizados para el juego son custodiados, y es responsable de distribuir las ganancias.

Cuando un jugador se une a una mesa, los fondos necesarios para cubrir el buy-in de la mesa se transfieren al contrato de la mesa y se acreditan internamente a la banca del jugador. El contrato proporciona la información necesaria para comunicarse con los otros jugadores en la mesa y comienza el juego. A medida que avanza el juego, se envía información al contrato sobre el estado del juego y se actualiza su estado según ésta. Cuando el jugador abandona el juego, el contrato transfiere cualquier ganancia adeudada a la misma cuenta desde la cual el jugador originalmente pagó.

3.4.3 Interacciones de jugadores con los contratos de mesa

Las transacciones de los jugadores se envían a los contratos de mesa en los siguientes casos: (1) para unirse a una mesa, (2) al final de cada mano, (3) cuando se termina un juego (en torneos) o cuando un jugador deja una mesa (para juegos de dinero en efectivo). Nuestro objetivo es minimizar la cantidad de transacciones enviadas a Ethereum para reducir los costos de operación y aumentar la velocidad de juego.

Los contratos de mesa incluyen un contador de fichas que hace seguimiento de las apuestas de los jugadores en cada mesa. Al final de cada mano, cada jugador, y los Jueces (descritos en la Sección 4.2), firman los resultados de manera cifrada y envían una transacción al contrato de mesa que actualiza la apuesta de cada jugador en consecuencia. Este mecanismo de consenso, y el envío de transacciones por parte de los jugadores de cada mesa determinada, funciona como un "oráculo", lo que permite que el contrato mantenga un estado de juego actualizado y que se sepa cuándo pagar a los jugadores. Este proceso ocurre de forma asíncrona mientras se juegan las manos en la plataforma, lo que significa que los jugadores pueden pasar a la siguiente mano, mientras el resultado de la mano anterior es validado por blockchain.

3.4.4 Contrato de torneo de mesas múltiples

Para los torneos que involucran el juego en múltiples mesas, el contrato del torneo de múltiples mesas funciona como una herramienta organizacional que administra la distribución de jugadores en las mesas. Cualquier aspecto del torneo que exista en un nivel más alto que la mesa misma, se maneja mediante este contrato.

3.4.5 Contrato de administración de jueces

Un juez es un caso especial del software de cliente del jugador que participa en el juego punto a punto de una mesa, pero no recibe cartas ni realiza apuestas. El juez recibe incentivos externos (un pago)

para actuar como un par confiable en la subred de la mesa. Un equipo de jueces se asigna al azar a cada mesa, y ellos resuelven disputas y registran los datos del juego.

Para distribuir la carga de trabajo y evitar la colusión entre jueces y jugadores, los jueces se asignan aleatoriamente a las mesas entre los integrantes de un grupo y rotan entre las mesas después de un cierto número de manos. El Contrato de administración de jueces es responsable tanto de mantener un registro de los jueces disponibles, como de asignarlos a las mesas de póquer. Los jueces se analizan con mayor detalle en la Sección 4.2.

3.5 Mental Poker

3.5.1 Descripción general

En 1978, los criptógrafos Adi Shamir, Ron Rivest y Leonard Adleman publicaron un artículo en respuesta a una pregunta que había planteado el científico informático Robert W. Floyd: "¿Es posible jugar un juego justo de 'Mental Poker'?". Este informe propone un esquema de cifrado y un protocolo de comunicaciones que permite a dos personas en diferentes lugares barajar y repartir cartas virtuales de una manera que permita que un juego se juegue sin la necesidad de un tercero de confianza.¹⁶ A lo largo de los años, se han publicado numerosos informes sobre el tema, que amplían las ideas, ofrecen métodos alternativos y proporcionan análisis y críticas.

Sin embargo, han habido muy pocas aplicaciones de software prácticas que empleen técnicas de Mental Poker. En gran parte, esto se debe a que el cifrado involucrado puede requerir enormes cantidades de recursos de comunicación y poder computacional, y el software que lo utiliza simplemente funciona demasiado lento para el uso de los consumidores. Además, la naturaleza inherente P2P en Mental Poker puede ser difícil de administrar y no se combina bien con los modelos tradicionales de juegos en línea basados en servidores.

El equipo de Virtue Poker ha pasado los últimos dos años examinando cómo el uso de blockchain y las tecnologías de almacenamiento distribuido, en conjunto con las redes cooperativas punto a punto, pueden abordar estas dificultades. El resultado es una aplicación descargable, capaz de jugar un juego a gran velocidad y administrar apuestas con dinero real utilizando el blockchain de Ethereum.

Mental Poker garantiza que ningún jugador individual pueda leer las barajas, al cifrar y barajar las cartas de forma cooperativa, con el objetivo de que cada persona, algunas personas o todo el grupo sea capaz de "abrir" cada carta. El protocolo usa cifrado de comunicación: las tarjetas se pueden cifrar o descifrar en cualquier orden. El algoritmo básico se describe en la Sección 3.5.2.

3.5.2 Algoritmo de Mental Poker: el barajado de dos pasadas

Tres jugadores, Bob, Alice y Ted están sentados en una mesa y están jugando un juego de Texas Hold'em. Bob reparte y genera una baraja de 52 cartas en su máquina; solo él puede ver las cartas. Utilizando un algoritmo de Fisher-Yates al barajar, baraja un mazo de cartas y luego cifra el mazo con la misma clave

¹⁶ A. Shamir, R. Rivest y L. Adleman. Mental Poker. *MIT Technical Report*, 1978.

de cifrado en cada carta, lo que hace que el mazo sea legible solo para él. Luego pasa el mazo cifrado a Alice, quien hace lo mismo: baraja el mazo de cartas y luego las cifra. Finalmente, Alice le pasa el mazo a Ted, quien pasa por el mismo proceso.

El mazo ahora se encuentra en su estado final ordenado, de 1 a 52, y este orden no cambia durante la mano. Ted le transfiere el mazo de cartas cifrado 3 veces de vuelta a Bob, quien se quita su "bloqueo de baraja" y ahora cifra cada carta individual con una clave de cifrado diferente: B1, B2 ...B52. Pasa el mazo a Alice, que hace lo mismo: elimina su "bloqueo de baraja" y cifra el mazo con una clave de cifrado única A1, A2 ... A52. Finalmente, Alice le pasa el mazo a Ted, quien pasa por el mismo proceso. A Bob se le asigna la primera y la segunda carta del mazo, pero él solo posee sus claves de cifrado para estas cartas. Por lo tanto, Alice y Ted comparten sus claves de cifrado que corresponden a las dos primeras cartas, A1 y A2, y T1 y T2, respectivamente, de modo que Bob tiene las tres claves de cifrado para sus cartas privadas. Esto le permite a Bob ver sus cartas privadas, pero a nadie más. Este proceso se repite para cada jugador en la mesa, por lo que cada jugador solo puede ver sus propias cartas privadas.

Todos los jugadores juegan y la mano va a flop. El flop se denota con las cartas 7, 8 y 9 en el mazo. Todos los jugadores deben compartir sus claves de cifrado que corresponden a las cartas comunitarias, para que todos puedan ver estas tarjetas compartidas. Este proceso continúa hasta el final de la mano, donde el jugador ganador recibe el pozo y todos los jugadores alcanzan el consenso (descrito en detalle en la Sección 4.2) al firmar el resultado final de la mano que se envía al blockchain de Ethereum para actualizar el estado del juego para todos los jugadores sentados en la mesa. Vea las Figuras 6 a 9 que describen este proceso.

3.5.3 Dos rondas de cifrado: barajar el mazo e indexar el mazo

El "barajado de múltiples partes" solo requiere que uno de los pares baraje aleatoria y correctamente para garantizar que todo el mazo se ordene aleatoriamente. Si un jugador confía en que su equipo barajó correctamente el mazo, puede confiar en que el juego es justo.

Figura 6: Mezclar y cifrar el mazo¹⁷

¹⁷ Las cuatro cartas en las figuras 6 y 7 buscan representar una baraja completa de 52 cartas, no las cartas privadas de cada jugador

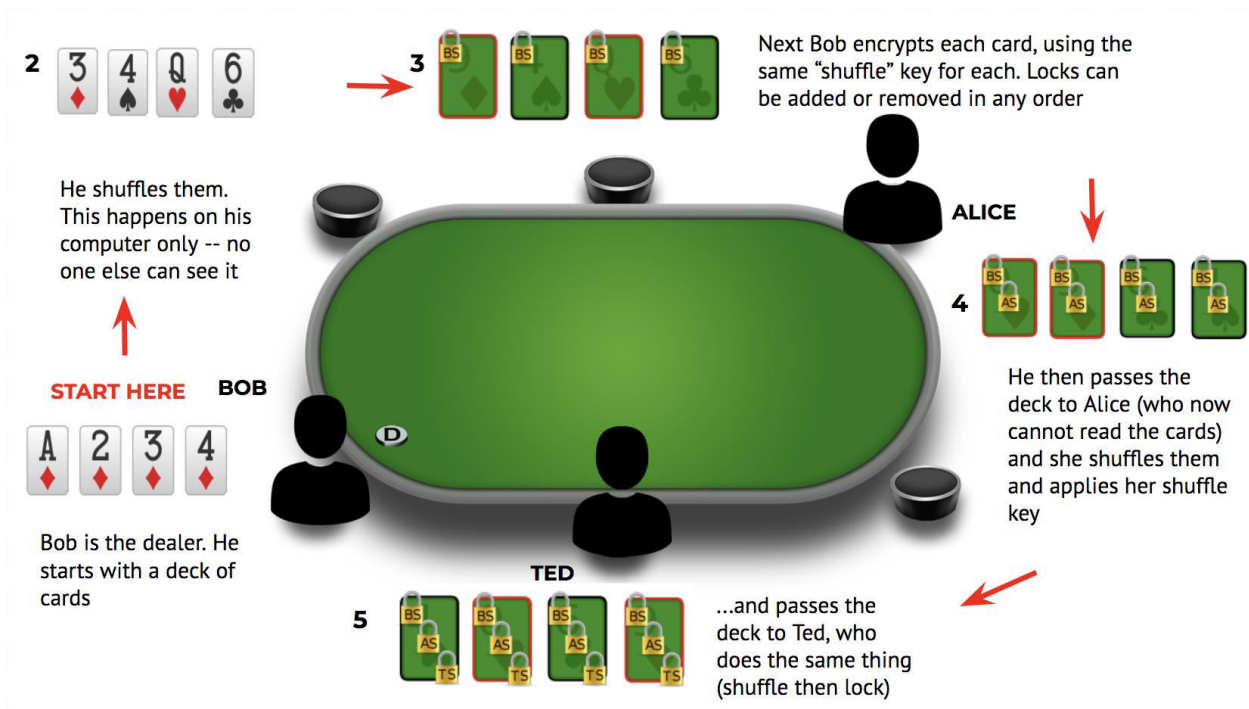
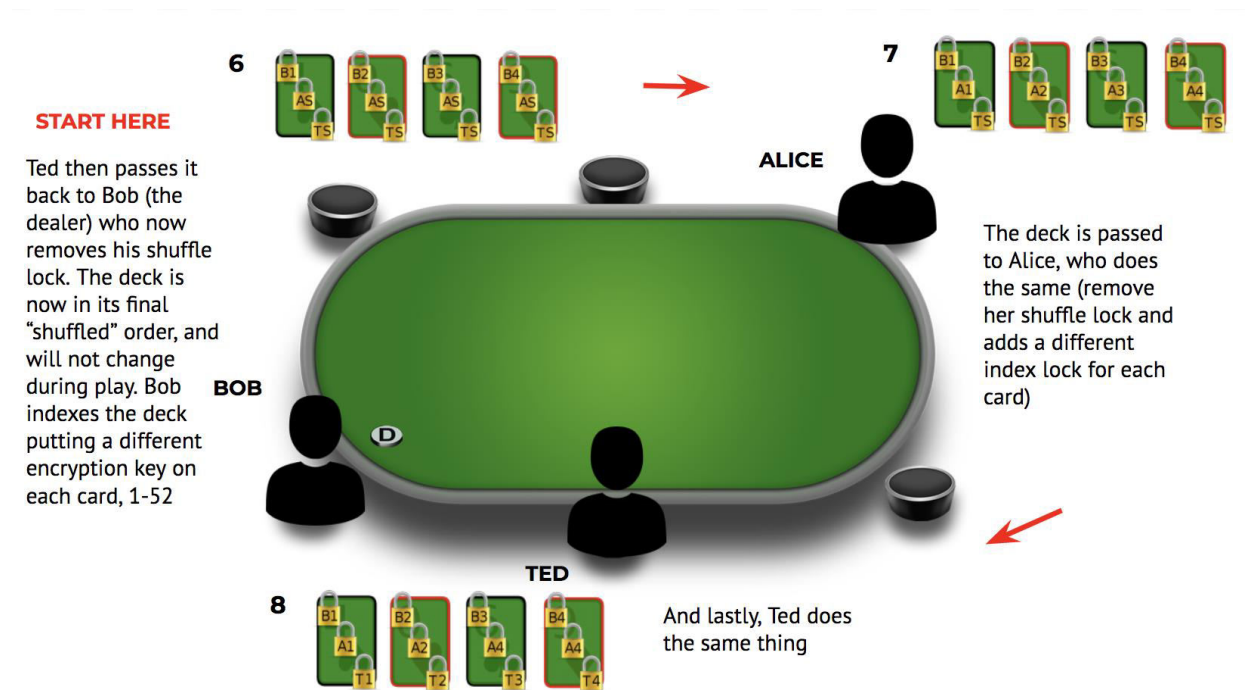


Figura 7: Indexación del mazo



3.5.4 Descifrado y juego

Figura 8: Compartir las claves del jugador

Alice and Ted share their encryption keys with Bob that correspond to Bob's cards so he can see his hand, and visa versa

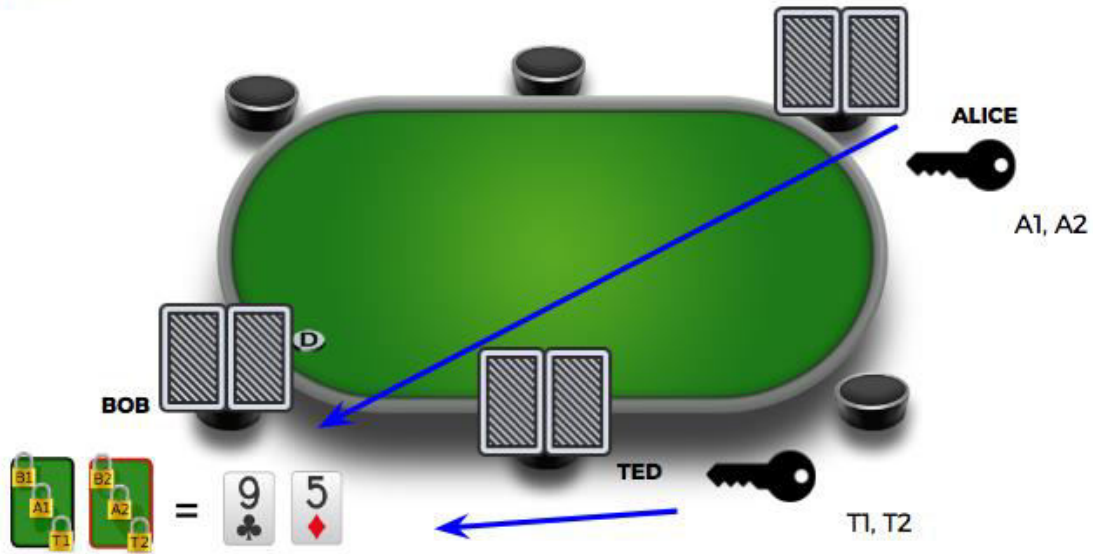
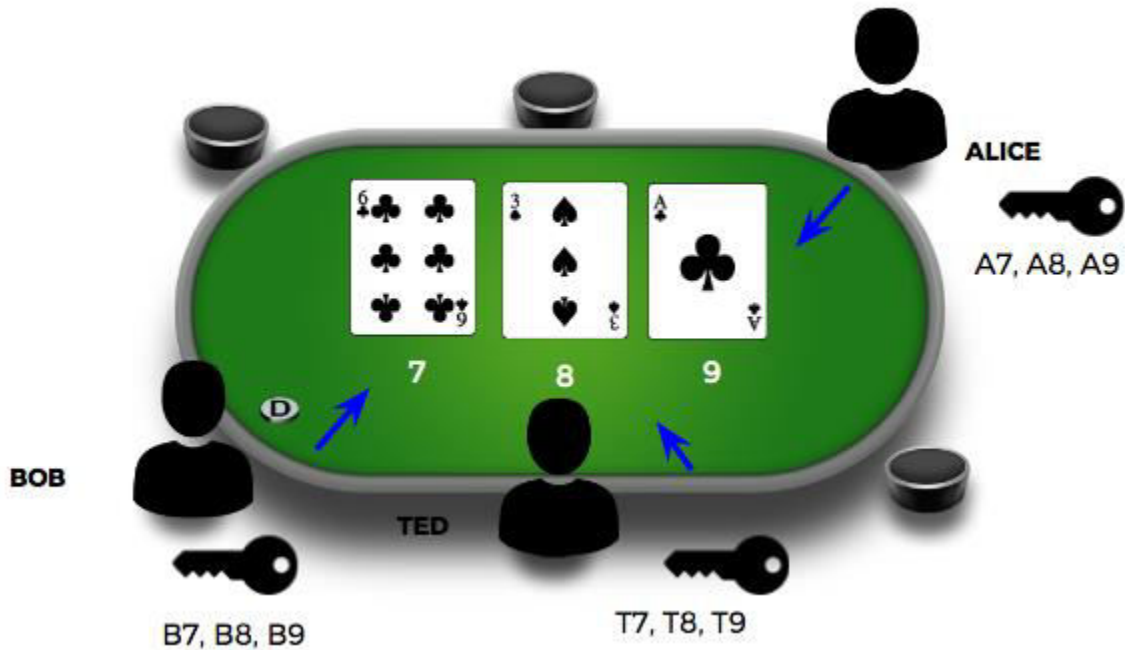


Figura 9: Cartas comunitarias¹⁸

All players share their keys for community cards so everyone can see them



Este proceso ocurre "bajo el capó": la apariencia y sensación de una mano en Virtue Poker es similar a la experiencia que los jugadores esperan de las plataformas en línea.

¹⁸ Las cartas de la comunidad turn y river se mostrarán de la misma forma una vez que hayan concluido el flop y las rondas de apuestas.

3.6 Mensajería punto a punto (P2P)

3.6.1 Mensajería P2P para sincronización del juego de cliente

Si bien las ideas detrás de Mental Poker hacen posible que un mazo sea compartido y las cartas sean repartidas y mantenidas en secreto por los jugadores de una red punto a punto sin necesidad de confiar en un servidor central, se requieren otras tecnologías para proporcionar un servicio de póquer práctico y orientado al consumidor.

El software de cliente descargable del juego consiste en procesos de front-end y back-end independientes. El front-end muestra el estado actual del juego al usuario local, acepta respuesta cuando corresponde y la pasa al servidor, que luego la transmite a los demás clientes del juego. El back-end contiene la lógica necesaria para aplicar las reglas del póquer a los eventos de respuesta que recibe tanto desde el front-end como desde otros clientes. El resultado es que cada cliente aplica el mismo código a los mismos datos que los demás.

3.6.2 Juego fuera de blockchain

Una tecnología de blockchain programable como Ethereum permite un almacén de datos definitivo e inmutable para elementos que de otro modo podrían manejarse en un solo servidor, como administrar a los jugadores en una mesa en particular. La capacidad del software de cliente para interactuar con Smart Contracts en blockchain también permite la administración distribuida y sin necesidad de confianza de los fondos del jugador y las apuestas en la mesa, y proporciona un registro inmutable de estas interacciones. Pero blockchain no puede utilizarse simplemente en reemplazo de un servidor para todos los aspectos del juego, en parte debido a que los datos y las instrucciones enviadas por el cliente tardan, en el mejor de los casos, unos segundos para propagarse por la cadena, por ello, no es práctico utilizarlo para administrar eventos de juego más granulares que a nivel de mano.

Los eventos de juego que ocurren a un ritmo superior, como las apuestas, deben ser administrados por el software de cliente mismo o, más apropiadamente, por el software que administra la subred punto a punto que consiste en los clientes que juegan en una mesa en particular. El uso de firmas digitales permite a cada cliente verificar que los mensajes recibidos hayan sido enviados por el remitente correspondiente, evitando la falsificación. Las técnicas de formación de consenso tolerantes a fallas se utilizan para garantizar que en cada paso del proceso de juego, cada cliente concuerde con los demás clientes individuales respecto de lo que sucedió exactamente. Además de detectar errores y fallas de hardware, también se detectan fallas bizantinas (datos intencionalmente incorrectos).

Al final de cada mano, estos datos de consenso, firmados digitalmente por cada cliente, se pasan a blockchain para su procesamiento y los clientes pasan a la siguiente mano. Los jueces (que se describen en la Sección 4.2) resuelven los desacuerdos entre clientes o pares en la mesa.

3.7 IPFS: Almacenamiento de registro de juegos de historias de manos

Para proporcionar un registro permanente del juego real de cada mano, los mensajes de evento de juego firmados deben almacenarse, así como la información de estado rastreada por blockchain cuando procesa el final de una mano. Esto genera una segunda debilidad en la tecnología actual de blockchain:

el uso de la cadena para almacenar cantidades significativas de datos puede requerir muchos recursos, por lo que no es práctico enviar todos estos datos de registro a blockchain.

Afortunadamente, tecnologías como el Sistema de archivos interplanetarios (IPFS) están diseñados para proporcionar un almacenamiento de datos confiable y distribuido. Al final de una mano, antes de informar a blockchain, el software de cliente envía los datos de registro de la mano a IPFS, que le proporciona un único valor hash que puede utilizarse para localizarlo en otro momento. Ese hash se incluye con los datos de estado enviados al contrato de blockchain, y dado que los datos de registro de cada mano incluyen el hash del registro de la mano anterior, es posible solicitar el hash más reciente de blockchain y usarlo para encadenar nuevamente todo el registro de la historia del juego. Una plataforma de almacenamiento distribuido elimina los puntos de falla individuales presentes en diversas formas de sistemas de almacenamiento centralizados.

4. Seguridad del juego

4.1 Formas de hacer trampa en el póquer en línea

4.1.1 Colusión

La colusión se define como dos o más jugadores que colaboran en una mesa compartiendo información entre ellos y utilizando estrategias cooperativas para crear una ventaja contra otros jugadores.

4.1.2 Contabilidad múltiple

Un usuario individual puede usar varias cuentas en una o más computadoras y luego tomar varios asientos en la misma mesa para crear una ventaja injusta en un torneo o en un juego de dinero en efectivo.

4.1.3 Minería de datos

Los jugadores a veces comparten información acerca de otros jugadores, lo que incluye historiales de manos y notas de jugadores. Esta información compartida se compila para proporcionar al jugador información desconocida sobre otros jugadores.

4.1.4 Bots de póquer

Como se describió anteriormente, los bots de póquer son programas de software estándar o personalizados que pueden operar en mesas de póquer sin supervisión humana.

4.1.5 Cuenta compartida

Las cuentas compartidas se producen cuando dos o más jugadores usan una sola cuenta para aprovecharse del sitio de póquer o de otros jugadores. Se pueden aprovechar del sitio de póquer si ofrecen premios porcentuales más altos, como de rakeback, según la cantidad de juego y rake. Es posible aprovecharse de otros jugadores con acciones nefastas como vender una cuenta cuando el torneo ya está avanzado, así como cuando un jugador más fuerte juega utilizando la cuenta de un jugador más débil.

4.2 El sistema de jueces para combatir las trampas

Virtue ha desarrollado el Sistema de jueces para combatir la colusión y las trampas. Los jueces son árbitros que no juegan y se asignan al azar a las mesas de póquer. Proporcionan seguridad y protección a los jugadores de la red de Virtue Poker y reciben honorarios a cambio. Los jueces pueden considerarse nodos de validación en la red de Virtue Poker, firmando cada transacción para cada mano en la plataforma y enviando historiales de manos para su almacenamiento en IPFS. Los jueces se rotan automáticamente cada pocas manos.

Las funciones que se describen a continuación son automáticas: no se necesita supervisión manual para que un usuario ejecute un nodo de juez.

4.2.1 Funciones principales de los jueces

Los jueces brindan tres funciones principales a la red de Virtue Poker:

4.2.2.1 Resolución de disputas

En el raro caso que dos compañeros de una mesa no estén de acuerdo con el estado de la mesa al final de una mano o de un juego, el juez resuelve la disputa en tiempo real y otorga el pozo al ganador.

4.2.2.2 Fuente de alimentación de datos

Cada juez envía cada una de las acciones de cada mano a IPFS de forma que sea posible almacenar historiales de manos. Esto es exigido por los organismos reguladores de juego y permite servicios esenciales tales como la detección de colusión, detección de bot e identificación de contabilidad múltiple.

4.2.2.3 Almacenamiento parcial de las claves de cifrado del jugador

El "Problema del jugador que se retira" de Mental Poker ocurre cuando un jugador se sale de una mano antes de terminarla. Esto es problemático, ya que todos los jugadores deben compartir claves de cifrado para que se revelen las cartas comunitarias y para que se termine una mano. Usando Shamir's Secret Sharing, las claves de cada jugador se pueden cifrar y dividir entre todos los jugadores además del juez. Si el jugador se retira por algún motivo, el juez puede solicitar las piezas de cada jugador y descifrar las piezas ensambladas para que la mano pueda terminarse.

Un nodo de juez en Virtue Poker se puede activar descargando el cliente de juez a un equipo, abriendo la aplicación y activando al juez. Una descripción más detallada del Sistema de jueces se proporciona en la Sección 5.1.

5. VPP: Virtue Player Points (Puntos de jugador de Virtue)

Los Puntos de Virtue Player (VPP) tienen tres funciones centrales dentro de la red de Virtue Poker: (1) se pueden usar como moneda del juego, (2) se pueden comprometer en un contrato inteligente llamado Registro de jueces que permite a los usuarios apostar fichas y validar manos en la red a cambio de una tarifa, y (3) se pueden usar para acceder a torneos especiales.

5.1 Para convertirse en juez

El grupo de jueces está compuesto por un número limitado de usuarios que se encuentran activos en la red de Virtue Poker. Para convertirse en Juez, los usuarios deben, (a) adquirir VPP, (b) poner fichas en el Registro de jueces y, (c) deben tener su computadora encendida, la aplicación Virtue Poker abierta y configurada en *activa*, con el fin de que sea asignada a las mesas.

5.1.1 Proceso de revisión de solicitudes para ser juez

Inicialmente, un equipo de expertos en seguridad del juego revisará las solicitudes de los jueces a IPFS. El equipo de Virtue Poker incluye un experto en integridad y seguridad del juego que ayuda a nuestro equipo de desarrollo en la construcción del Sistema de jueces y a configurar el software de seguimiento apropiado para detectar señales de alerta en la plataforma.

Existen dos formas para que las acusaciones de fraude se envíen a nuestro equipo de Seguridad de jueces. Los jugadores pueden enviar una queja de actividad sospechosa, y estas presentaciones se revisan para determinar si se ha producido una trampa. Además, Virtue Poker ejecuta constantemente algoritmos a los datos enviados por los jueces y todas las actividades sospechosas se revisan manualmente. Si se descubre que un jugador hizo trampa, se aplica un castigo y ese jugador puede ser expulsado de la plataforma de forma permanente.

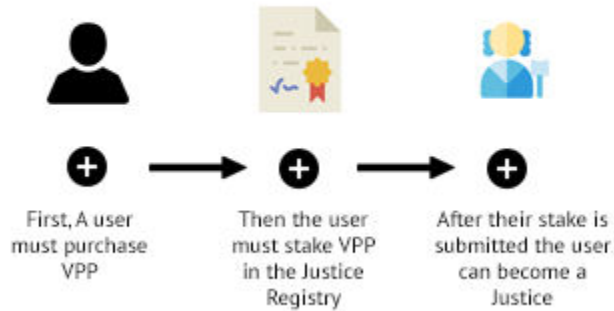
5.1.2 Remuneración de los jueces

La remuneración de los jueces generada en la plataforma de Virtue Poker se dividirán entre los nodos de juez activos en la red de Virtue Poker. Las remuneraciones son acumuladas por los jueces tanto en VPP como en ETH. En la Figura 10 puede ver una ilustración del Sistema de jueces.

Figura 10: Sistema de jueces

Becoming a Justice

Users must "lock" VPP in the Justice Registry to become an eligible Justice



Justice Assignment

Justices must download Justice software and be "active" to be assigned to tables



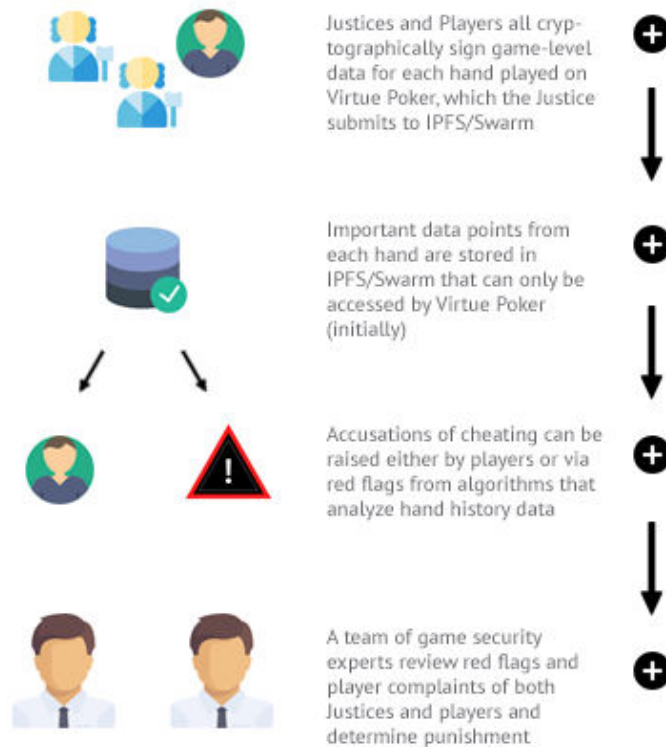
Justice Functions

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 occurred, either by Players or Justices.



5.2 Moneda de juego

Es posible utilizar VPP como moneda del juego. Los jugadores pueden elegir participar en juegos en VPP para aumentar su proporción relativa de VPP en relación con otros usuarios.

5.3 Torneos especiales

Solo se puede acceder a torneos y juegos especiales con VPP y los usuarios pueden competir para ganar VPP o ETH. Estos torneos incluirán, entre otros, torneos garantizados, freerolls y eventos satélite especiales.

6. Hoja de ruta

6.1 Actividades clave

6.1.1 Desarrollo de la plataforma

El equipo de Virtue Poker ha dedicado casi tres años a desarrollar nuestro sistema, y deberá aumentar los integrantes de nuestro equipo de desarrollo para construir una plataforma completamente funcional. Virtue Poker contratará desarrolladores para mejorar nuestra red troncal de mensajería P2P, crear interfaces personalizadas, optimizar nuestros contratos inteligentes e implementar funcionalidades de almacenamiento. Además, nuestro equipo se integrará con los proyectos de infraestructura actuales de Ethereum, que incluyen almacenamiento distribuido, gestión de identidades y monedas estables.

6.1.2 Crecimiento de la comunidad

Virtue Poker competirá con actores de mercado con grandes presupuestos y sofisticados procesos de adquisición de clientes. Dedicaremos recursos significativos para hacer crecer una red global de personas interesadas en el éxito final de una plataforma descentralizada de póquer, lo que incluye potenciar a nuestros usuarios, ejecutar torneos garantizados y freerolls, rakeback, software de análisis y otras iniciativas.

6.1.3 Patrocinios y relaciones públicas

Virtue Poker patrocinará populares foros de póquer, sitios web, blogs y eventos. Además, nuestro equipo adoptará una estrategia agresiva de relaciones públicas para comunicar las propuestas de valor de nuestra plataforma a un público amplio.

6.1.4 Aspectos legales

Nuestro equipo se encuentra consultando con respetadas oficinas de abogados de juegos, incluidos DLA Piper, ISOLAS y Ifrah Law, además de reguladores en todo el mundo. Continuaremos consultando estos recursos a medida que naveguemos por los marcos legales y regulatorios aplicables. Nuestro equipo planea obtener una licencia de juego antes de nuestro lanzamiento para garantizar que nuestra plataforma cumpla con los estándares de cumplimiento y que nuestros jugadores estén suficientemente protegidos.

6.2 Hoja de ruta de desarrollo

6.2.1 Estado actual

Virtue Poker se concibió en mayo de 2015 y nuestro prototipo se desarrolló durante los últimos dos años.

Nuestra aplicación ha sido probada semanalmente desde su inicio. Internamente, nuestro equipo ha estado jugando juegos de póquer utilizando una implementación de Mental Poker que funciona en las redes de prueba de Ethereum.

La primera versión de Virtue Poker es un cliente de escritorio de Python que crea un contrato inteligente personalizado para cada instancia de mesa. Nuestro equipo ha implementado con éxito un protocolo de

Mental Poker para barajar cartas y un motor de juego. El motor del juego es una máquina de estados que se conecta con otros pares a través de un protocolo de mensajería P2P y se conecta con Ethereum cuando los pares crean y se unen a una mesa en particular. Actualmente nuestra aplicación puede jugar juegos de 6 manos a una velocidad de 70-80 manos por hora, a la par con las redes de póquer en línea existentes.

6.2.2 Desarrollos futuros

Virtue Poker ha contratado a nuestro equipo principal y utilizará fondos internos para continuar desarrollando al equipo y la plataforma de Virtue Poker. Uno de nuestros objetivos es rediseñar la aplicación de escritorio de Virtue Poker como una aplicación Electron. Para que nuestra plataforma sea exitosa, la aplicación Virtue Poker debe someterse a pruebas significativas para garantizar que los juegos sean lo suficientemente justos, el método de registro y verificación de identidad prevenga la contabilidad múltiple de bajo nivel y el juego de menores, y nuestro mecanismo de almacenamiento de datos pueda rastrear puntos de datos necesarios para el cumplimiento y para detectar trampas.

Mejorar la red troncal de mensajería P2P

La aplicación utiliza implementaciones plug-in de tiempo de ejecución intercambiable para diferentes transportes y actualmente está utilizando un explorador muy básico de mensajes basado en el un servidor HTTP. Para la implementación, Virtue Poker utilizará una red troncal industrial más potente.

Implementación de jueces

La presencia de uno o más jueces en un juego permite archivar permanentemente fuera de línea (IPFS) el juego punto a punto, lo que es importante cuando se trata de detectar la colusión o juego de bots, o simplemente para posteriormente reunir pruebas de que las cosas marcharon correctamente. Como parte del mecanismo de consenso, un juez evita que 2 jugadores con clientes hackeados hagan trampa en un juego de 3 jugadores, algo que otros mecanismos de consenso 51% vulnerables no pueden hacer.

Front-End de calidad comercial

Virtue Poker actualizará la máscara de nuestra aplicación actual y creará una interfaz de usuario para nuestro lobby antes de la primera ronda de pruebas de usuarios.

6.2.3 Primer trimestre de 2018

Administración de identidad

Inicialmente, el equipo de Virtue Poker integrará un servicio de verificación de identidad de terceros (consulte <https://www.hooyu.com/>). A medida que sigamos trabajando con reguladores de todo el mundo, les presentaremos soluciones de identidad autónoma como uPort. Nuestro objetivo es eventualmente mover nuestro proceso de inicio de sesión a una solución descentralizada.

Almacenamiento de datos

Virtue Poker utilizará nodos de jueces para recopilar y almacenar juegos a nivel de mano. Tenemos la intención de almacenar historiales de manos utilizando IPFS y agregar una referencia a los datos en el contrato de la mesa. Inicialmente, usaremos un mecanismo de almacenamiento de datos centralizado para nuestro Alfa.

6.2.4 Segundo trimestre de 2018

Alfa privado de Virtue Poker

Virtue Poker llevará a cabo pruebas de usuario privadas para depurar nuestra plataforma y obtener retroalimentación de las fuentes para mejorar nuestra UI/UX. Aquellos que participen de la Venta de fichas de Virtue Poker (fase 1) serán invitados a unirse al programa Alfa.

Evento pre-lanzamiento

Virtue Poker organizará un evento de prelanzamiento compuesto por reconocidos profesionales en línea y en vivo, y transmitirá en vivo el evento en Twitch.

6.2.5 Segundo y tercer trimestre de 2018

Mecanismo de rakeback

En base en las pruebas continuas de los usuarios, Virtue Poker implementará un mecanismo de rakeback con fichas utilizando VPP.

Desarrollo de la funcionalidad de torneo de múltiples mesas

El Contrato de torneo de múltiples mesas administra qué mesas son parte del torneo y qué jugadores están asignados a esas mesas. También gestiona el progreso y la resolución del torneo: quién gana y qué gana. Durante el juego, la mesa sigue siendo la unidad de subred P2P y funciona de forma muy similar a como lo hace actualmente, pero se comunica con el Contrato de torneo de múltiples mesas.

Versión limitada de Virtue Poker (versión beta abierta)

Virtue Poker lanzará la versión beta abierta para usuarios de todo el mundo que puedan crear y jugar torneos Sit & Go de mesa única y juegos de dinero en efectivo.

6.2.6 Cuarto trimestre de 2018

Torneo de lanzamiento público de Virtue Poker

Virtue Poker se lanzará públicamente a través de uno o más grandes torneos garantizados, permitiendo a usuarios de todo el mundo jugar en nuestra plataforma.

6.2.7 2019

Integración de operadores de terceros

Virtue Poker permitirá a los operadores de terceros y a los titulares de licencia en todo el mundo crear máscaras personalizadas en nuestra plataforma y crear juegos sobre nuestra infraestructura. Esto nos permitirá escalar más rápidamente a un nivel de liquidez atractivo para los jugadores.

7. El equipo

7.1 Equipo central

Jim Berry, Desarrollador jefe de la plataforma: Durante los últimos 30 años, Jim ha trabajado en software que abarca desde el sistema terrestre del Telescopio Espacial Hubble, hasta la Aplicación de datos de investigación de Framingham Heart Study, controladores Linux para un sistema de adquisición de imágenes aéreas, y la instalación de sistemas de correo electrónico de tecnología apropiada para países en desarrollo en el Pacífico Sur. La mayor parte de su carrera, sin embargo, se ha dedicado a trabajar en juegos de computadora para compañías como MicroProse, Looking Glass Technologies y Electronic Arts, entre otras, que se especializan en simulación física y gráfica.

Ryan Gittleson, Cofundador: Ryan es un experimentado profesional de desarrollo de negocios y marketing, con experiencia en el desarrollo de ventas para empresas y productos. Antes de trabajar en Virtue Poker, Ryan fue Jefe de Adquisición de Clientes de TodayTix, una aplicación móvil de venta de boletos de Broadway, donde supervisó el crecimiento de su base de usuarios de 150.000 usuarios a más de 700.000. Descubrió Ethereum en agosto de 2015 y quedó cautivado inmediatamente por el potencial global de la tecnología blockchain. Ha trabajado con ConsenSys en Virtue Poker durante los últimos dos años. Ryan tiene una licenciatura de la Universidad de Pensilvania.

Dan Goldman, Director de marketing: Dan tiene más de 20 años de experiencia en compañías de marketing en línea. Fue el responsable del ascenso de PokerStars, la compañía de póquer en línea más grande del mundo, haciendo crecer a la empresa hasta convertirla en una organización con más de 100 millones de jugadores. Antes de PokerStars, Dan dirigió las iniciativas de marketing para uno de los sitios de comparación de compras en línea más grandes, lo que llevó a su adquisición por parte de Experian. Formó parte del equipo que comercializó la programación orientada a objetos, desarrollando Digitalk desde una startup a una posición de liderazgo con su lenguaje de programación Smalltalk/V. Dan también supervisó el desarrollo y lanzamiento de un sitio de juegos en línea basado en casinos para uno de los casinos más grandes de Estados Unidos.

Javier Franco Algarrada, Jefe del equipo de desarrollo de Blockchain: Javier es un ingeniero de software sénior con más de 10 años de experiencia. Le gusta trabajar en aplicaciones de pila completa que involucran múltiples tecnologías y ser una parte activa en el ciclo completo de desarrollo de software del producto. Después de liderar otros proyectos técnicos, ha continuado su desarrollo profesional para liderar el desarrollo de Virtue Poker. Ha trabajado durante más de 7 años en el área de las apuestas en diferentes productos como lotería, deportes virtuales, juegos de casino y apuestas deportivas. Debido a que siempre ha estado interesado en tecnologías de punta, decidió cambiarse a proyectos de blockchain el año pasado. Tiene una licenciatura en informática y una maestría en ingeniería web.

Catalin Dragu, Diseño: Catalin ha sido diseñador digital desde 2010. Ahora trabaja en ConsenSys en la creación de DApps frescas y atractivas. Él cree que un buen diseño entrega un buen espíritu. Y hace su

mejor esfuerzo al tratar de crear una experiencia atractiva para los usuarios, de forma que puedan disfrutarla tanto como un paseo por el parque.

José Díaz, Jefe de producto: José tiene un historial como emprendedor e innovador sénior con más de dieciocho años de experiencia en la industria del juego como CTO, Director de desarrollo de productos, Desarrollador de software y Gerente de TI. Con un MBA y un alto título universitario en informática, se unió a Virtue Poker como Jefe de producto, atraído por la tecnología innovadora que utiliza Virtue Poker. Los antecedentes de José incluyen un historial de entrega exitosa de proyectos de alto perfil, la definición de nuevas estrategias de desarrollo en nuevas plataformas, el liderazgo de equipos fuertes y gestión de relaciones con clientes clave.

Colum Higgins, Gerente sénior de productos: Colum Higgins obtuvo un doctorado en física de CERN a principios de la década del 90. Pasó los siguientes 10 años en roles técnicos en supercomputación, como consultor de middleware empresarial y finalmente como fundador y CTO de una startup de tecnología durante tres años y medio. En 2003, Colum terminó un MBA y se mudó a China, donde creó un sistema de demostración 3G para Ericsson y trabajó en proyectos de eGovernment para gobiernos regionales y de la Unión Europea. En 2007, Colum se unió a Full Tilt Poker como Gerente de programa y Analista de negocios. En Full Tilt Poker, Colum dirigió los requisitos para los requisitos más importantes, incluida la reescritura de un cliente de juego, la regulación en Francia, las mesas para principiantes y las entradas para torneos.

Daniel Ortega, Desarrollador de back-end: Daniel ha sido ingeniero de software durante los últimos 12 años, después de haber aprendido y trabajado en un conjunto de sectores heterogéneos, desde el mundo de las obras civiles hasta el nicho de las aerolíneas, pasando por el dominio del juego. Daniel siempre trata de salir de su zona de confort y constantemente ha intentado trabajar con las últimas tecnologías durante su carrera.

Álvaro Rodríguez Villalba, Desarrollador de front-end: Álvaro es un desarrollador especialista en JavaScript y desarrollador de Android. Fue cofundador de una startup llamada Kultur, donde fue desarrollador web y de Android y trabajó durante más de dos años en el desarrollo de una aplicación web para la simulación de enlaces de comunicación por satélite y creó varias plataformas basadas en JS como desarrollador independiente. Álvaro se graduó en 2017 del programa de ConsenSys Academy.

Lucas Cullen, Desarrollador de la plataforma Blockchain: Lucas es un desarrollador especializado en software y solidez, que anteriormente trabajó para startups y bancos, con experiencia en matemáticas. Él escuchó por primera vez acerca de Bitcoin en 2011, lo comenzó a explotar poco después, y ha estado hablando de bitcoin a quien quiera escuchar desde entonces. Ha trabajado en Accenture y en la Autoridad Monetaria de Singapur en el "[Proyecto Ubin](#)", utilizando el producto empresarial Ethereum de JP Morgan denominado Quorum. Anteriormente, dirigió su propia empresa de consultoría de software, proporcionando educación y desarrollo de software para proyectos de Bitcoin y blockchain. Dirige el grupo de Bitcoin Brisbane, es miembro de la junta directiva de [Blockchain Australian](#) y es Australian Coloured Coin Ambassador.

7.2 Asesores

Joseph Lubin: La carrera de Joe Lubin ha involucrado varios puestos en los campos de la tecnología y las finanzas, y lugar en que intersectan. Después de graduarse como *cum laude* con títulos en Ingeniería eléctrica e informática de Princeton, integró el equipo de investigación de Robotics Lab en Princeton y luego en Vision Applications. La ingeniería de software, las finanzas y el cifrado fueron fundamentales durante el empleo de Joe en Goldman Sachs, el trabajo de consultoría de eMagine en el proyecto IdenTrust y la fundación y operación de un conjunto de fondos de cobertura administrados con un socio. Joe cofundó el Proyecto Ethereum y ha estado trabajando en Ethereum y, más recientemente, en ConsenSys, desde enero de 2014.

James Slazas: James Slazas tiene más de 15 años de experiencia en la industria financiera. En Lehman Brothers, James administró un libro de arbitraje patentado de derivados y creó un grupo global de gestión de riesgos para la exposición HNW de los bancos de Londres, Suiza y Hong Kong. James es cofundador de un fondo de cobertura que administra una cartera de acuerdos de seguros de vida. Utilizando los componentes de atención médica del fondo, James negoció exitosamente el estado preferencial de los Centros de Extensión Regional de Medicare y Medicaid de AZ, CA, FL, NJ y NY para implementar el registro de salud electrónico (EHR) nacional de Med AZ/Healthcare Inside y los servicios de facturación, así como un acuerdo vinculante conjunto con HCL America para proporcionar análisis de soporte al paciente y servicios de facturación médica a laboratorios, ACO, consultorios privados y hospitales.

Patrick Berarducci: Pat es Consejero general adjunto de ConsenSys e ingeniero especialista en software. Antes de unirse a ConsenSys, Pat ejerció la abogacía durante siete años en Sullivan & Cromwell LLP y cofundó una nueva empresa de tecnología de atención de salud. Pat está particularmente interesado en aprovechar su experiencia legal, empresarial y en software, junto con la tecnología blockchain, para revolucionar industrias, mercados y redes.

Andrew Keys: Andrew es el Director de desarrollo de negocios globales de ConsenSys, con experiencia en mercados de capitales, tecnología y empresas. Anteriormente, Andrew trabajó para el banco de inversión UBS, en análisis de valores. Más tarde, fue responsable de la creación y distribución de productos de liquidación de seguros de vida para fondos de cobertura y bancos de inversión. Luego, cofundó una compañía de administración de ciclo de ingresos donde aprendió sobre Bitcoin y eventualmente Ethereum. Andrew dirige asociaciones tecnológicas estratégicas, desarrollo de negocios y comunicaciones para ConsenSys y cofundó ConsenSys Enterprise para crear soluciones de blockchain de Ethereum para empresas Fortune 500.

Robert Davidman: Más recientemente, Robert ocupó el cargo de CMO global interino de Ruby, supervisando el marketing y la estrategia digital para la cartera innovadora de marcas de Ruby, que incluye Ashley Madison, Cougar Life y Established Men. Actualmente Robert lidera la estrategia de marketing global y norteamericana para una serie de marcas líderes como socio en The Fearless Group en la ciudad de Nueva York, la cual cofundó. Los clientes en la industria del juego incluyen a Bwin.Party (PartyPoker), Pala Interactive (Palacasino.com, PalaPoker.com, Palabingousa.com), 888 Holdings (888.com) y Lottoland.com, entre otros. Desde 2001, Robert ha trabajado con varias propiedades de juegos en línea, tanto como comercializador y operador en todo el mundo. Robert se desempeñó como

jefe de servicios de transmisión internacional para Yahoo! de 1999 a 2001, donde lanzó el negocio de streaming del portal web fuera de EE. UU. y Canadá en más de 24 países. Antes de Yahoo!, desde 1995 a 1999, Robert fue el noveno empleado de Broadcast.com y lideró todas las ventas y el marketing para el pionero de la transmisión por Internet.

7.4 Equipo de Virtue Poker

Phil Ivey: Ivey logró el empate en el segundo puesto de todos los tiempos, con 10 brazaletes de la Serie Mundial de Póquer, y ocupa el sexto lugar de todos los tiempos con más de \$23 millones en ganancias en vivo. Además, es uno de los jugadores en línea con mejores resultados, con ganancias de más de \$10 millones. Ha sobresalido en todos los formatos (torneos, juegos con dinero en efectivo en vivo, juegos en línea con dinero en efectivo) y estableció un récord formando parte de 9 mesas finales del Torneo Mundial de Póquer (9 World Poker Tour Final Tables). Entre 2002 y 2009, Ivey se ubicó en el Top 25 en cuatro ocasiones diferentes en el Evento Principal de la Serie Mundial, y fue nominado unánimemente al Salón de la Fama de WSOP este año.

Dan Colman: Mejor conocido por vencer a Daniel Negreanu y ganar el buy-in de Big One for One Drop de \$ 1.000.000 en la [Serie Mundial de Póquer de 2014](#). Dan ha ganado más de \$28 millones en ganancias en juegos en vivo en su carrera, ocupando el tercer lugar de todos los tiempos.

Brian Rast: Brian Rast, conocido en línea como "tsarrast", quien ganó tres veces la Serie Mundial de Póquer, y se une al equipo como asesor de la compañía. Brian ganó el evento \$1.500 Pot-Limit Hold'em en 2011; ganó el Campeonato de Jugadores de \$ 50.000 dos veces en 2011 y 2016, con victorias en el heads-up contra Phil Hellmuth y Justin Bonomo, respectivamente. Brian ocupa el décimo lugar de todos los tiempos con más de \$20 millones en ganancias en juegos en vivo a lo largo de su carrera.

7.4 Socios legales

Ifrah Law PLLC (US Gaming Matters): Ifrah Law ha representado a los clientes del iGaming desde el comienzo de la industria y ahora representa a muchas de las compañías de iGaming y asociaciones industriales más grandes de todo el mundo. La firma ha estado al centro de la mayoría de los procesos y litigios más importantes de la industria del iGaming, incluidos los sitios de poker en línea Full Tilt Poker y PokerStars, para quienes Jeff Ifrah negoció un acuerdo histórico en 2011 con el Departamento de Justicia que allanó el camino para el iGaming en Estados Unidos. Ifrah Law también fue instrumental en la creación de marcos legislativos y regulatorios en los tres estados que actualmente permiten juegos en línea: Delaware, Nueva Jersey y Nevada.

ISOLAS LLP, Gibraltar Law: ISOLAS es un bufete de abogados con servicio completo en Gibraltar y asesora sobre la gama completa de soluciones legales que Gibraltar tiene para ofrecer. Como una galardonada firma de abogados clasificada por los principales directorios del mundo como la firma líder de Gibraltar, el enfoque de ISOLAS se mantiene sólidamente en el cliente y en la entrega de soluciones.



En funcionamiento desde 1892 (ISOLAS LLP celebra este año sus 125 años en Gibraltar), es el bufete de abogados más antiguo de Gibraltar.

8. Apéndice: La arquitectura de Virtue Poker

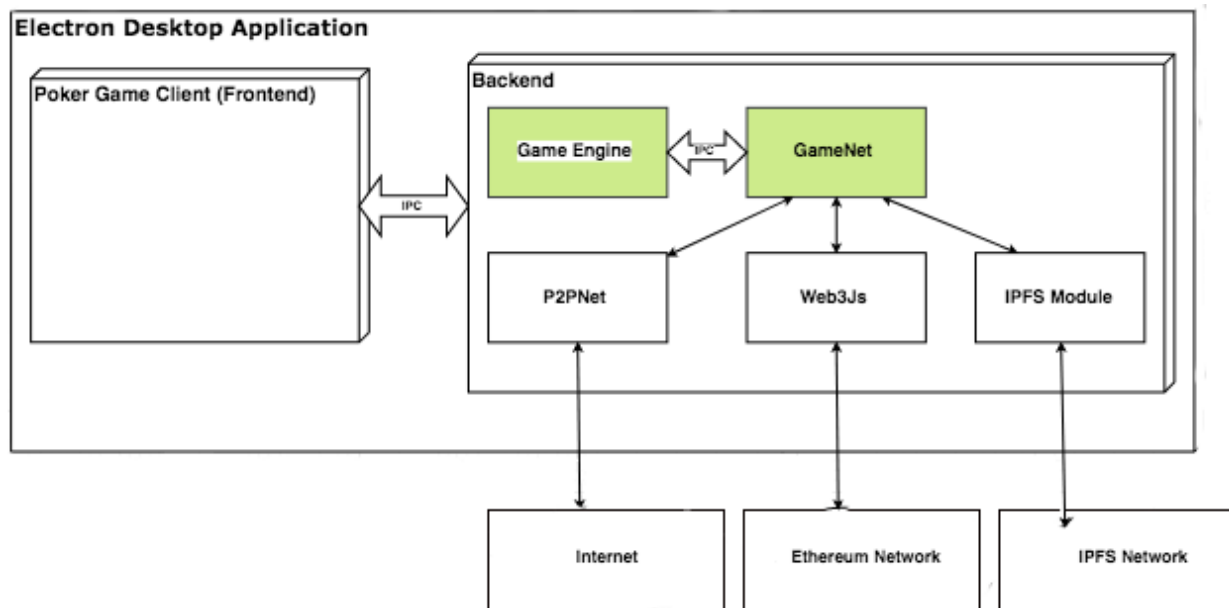
Virtue Poker todavía está en desarrollo. Partes de esta sección están sujetas a cambios.

8.1 Arquitectura del sistema

Virtue Poker es una plataforma de póquer totalmente descentralizada. Virtue Poker logra este objetivo utilizando nuevas tecnologías como Ethereum y IPFS, junto a otras soluciones.

La aplicación de escritorio Virtue Poker es una aplicación de escritorio Electron que incluye el motor de juego, el cliente de juego de póquer y la infraestructura de red para comunicarse con el blockchain de Ethereum, así como con una subred punto a punto, para que las instancias de juego las utilicen en los mensajes de latencia necesarios para el juego humano.

Figura 12: Arquitectura de la aplicación



8.1.1 Componentes

Los principales componentes de la aplicación de escritorio de electron son:

- **Motor de juego:** Contiene la lógica del juego de póquer.
- **Ethereum:** Se utiliza como un repositorio de parámetros de juego, servicio de custodia, informes de resultados, gestión de jugadores en varias mesas y administración de los jueces.

- **GameNet:** Proporciona un componente único que el motor puede usar para comunicarse con el mundo exterior
- **P2PNet:** Utilizado por GameNet para gestionar una subred P2P específica de la instancia del juego
- **Web3.js:** La API de JavaScript compatible con Ethereum que implementa la comunicación con los nodos de Ethereum
- **Aplicación de escritorio de Electron:** Marco de plataforma cruzada
- **Poker Game Client:** El cliente que se usa para jugar el juego. Es una aplicación web HTML5 escrita utilizando React Ecosystem.
- **Cliente IPFS:** Interfaz con la red IPFS para almacenar registros del juego.

8.2 Motor de juego

8.2.1 Máquina de estado

El motor de juego es el núcleo de nuestra aplicación, una máquina de estado finito que controla las transiciones dentro del estado del juego e implementa las reglas del juego. Dependiendo de las interacciones del usuario con la aplicación y las respuestas de la red, el motor de juego activa acciones y pasa al siguiente estado.

8.2.2: Estado conectado o fuera de línea

Virtue Poker ejecuta el siguiente proceso cuando un usuario inicia sesión en la aplicación:

1. La aplicación no está conectada, por lo que estamos ante un estado sin conexión.
2. El usuario ingresa los detalles de inicio de sesión y realiza un inicio de sesión.
3. El motor de juego recibe las entradas y desencadena la acción para realizar el inicio de sesión.
4. Una vez hecho el inicio de sesión, el motor de juego pasa a la siguiente acción y notifica a la interfaz de usuario.
5. Si el inicio de sesión es exitoso, pasamos a un estado conectado.
6. Si el inicio de sesión falla, mantenemos al usuario en un estado fuera de línea.

8.2.3: Estados del lobby

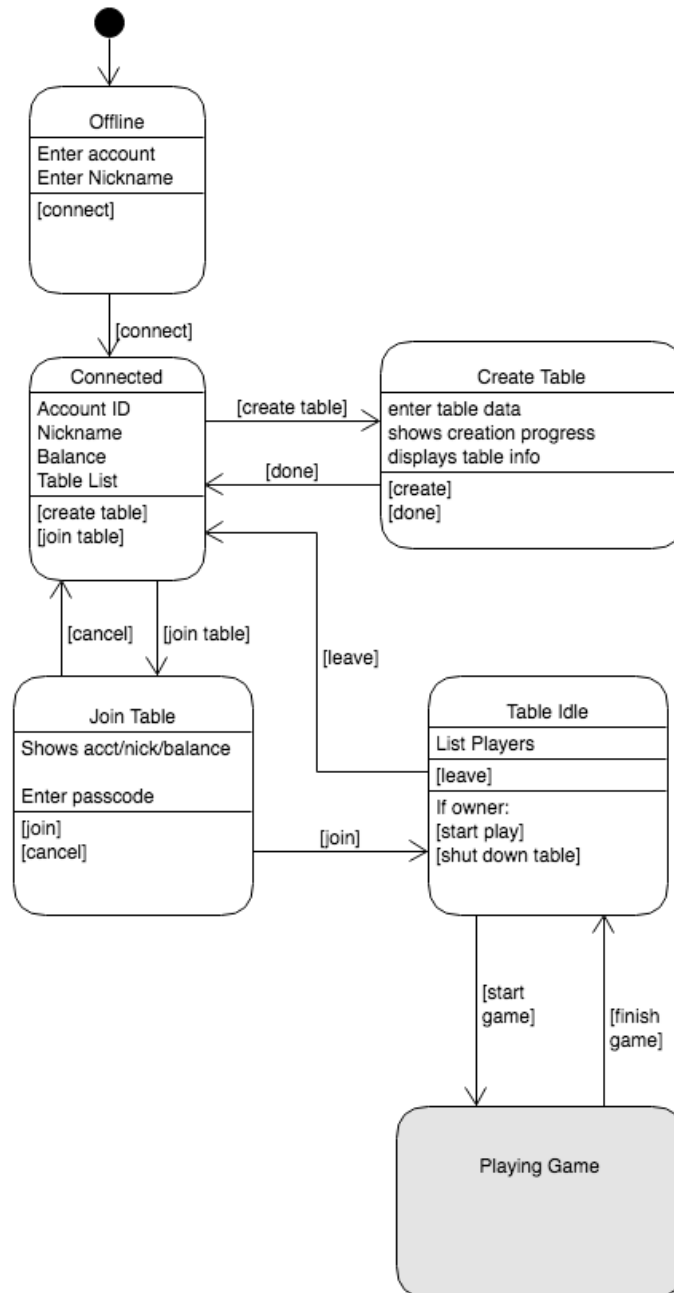
Nuestros estados del motor de juego se clasifican en dos grupos:

- **Estados de juego:** El juego indica cuándo se está jugando un juego.
- **Estados del lobby:** Cualquier estado que ocurra en otra instancia diferente a la de juego.

Los estados del lobby incluyen:

- **Sin conexión:** El usuario no ha iniciado sesión.
- **Conectado:** El usuario ha iniciado sesión y puede crear una mesa o unirse a ella.
- **Crear una mesa:** El usuario está creando una mesa.
- **Unirse a la mesa:** El usuario selecciona una mesa y se une a ella.
- **Mesa inactiva:** El usuario está esperando que otros miembros se unan a la mesa para que el juego pueda comenzar.

Figura 13: Estados del lobby



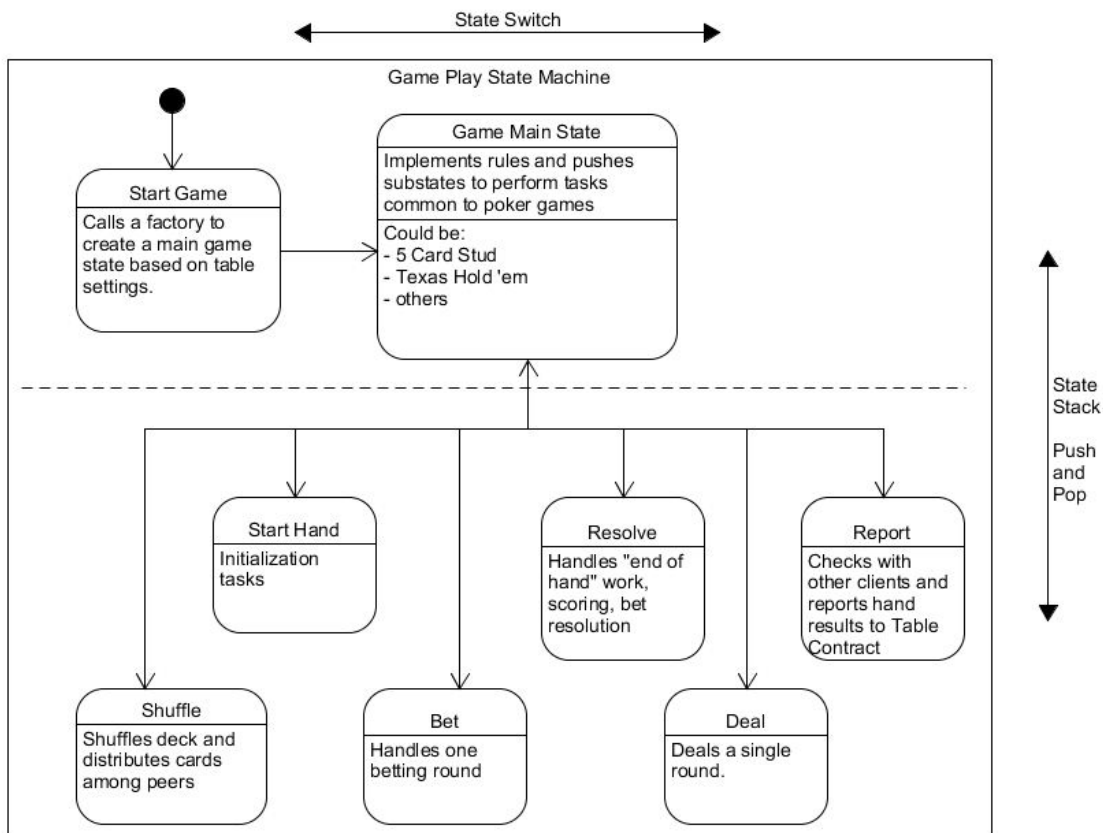
8.2.4: Estados de juego

En los estados en el juego incluyen:

- **On Deck:** El jugador está esperando que comience la mano.
- **Iniciar mano:** Los jugadores están listos para comenzar una mano.
- **Barajar:** El mazo se baraja y se cifra.

- **Repartir:** Existe una serie de rondas de entrega de cartas dependiendo del juego de póquer que se esté jugando. Por ejemplo, en Texas Hold'em, tendremos: pre-flop, flop, turn y river.
- **Apuesta:** El jugador decide si quiere pasar, apostar, retirarse o subir la apuesta, dependiendo del estado del juego.
- **Revisar entrega de cartas:** El motor de juego verifica las reglas del juego para determinar si se deben repartir más cartas.
- **Showdown:** El momento en que las manos que aún están activas se muestran o se van a muck.
- **Resolver:** Se muestran los resultados de la mano.
- **Informe:** Los resultados de la mano se envían al contrato del juego/mesa y el ganador recibe el pozo.

Figura 14: Estados de juego



3.4.2 Contrato de mesa de Ethereum

Jugar un juego de póquer únicamente en el blockchain de Ethereum requiere considerables recursos y tiempo. Para hacer que el juego sea fluido, los contratos de mesa están diseñados para administrar

jugadores y verificar los resultados de cada mano, dejando que la lógica del juego se maneje fuera de la cadena.

8.3.1 Funciones

VirtuePokerTable: Inicia la mesa de poker con los parámetros proporcionados.

Join_table: Se une a una mesa, crea una estructura de jugadores con los parámetros proporcionados y devuelve un mensaje de error, si corresponde.

Get_player_seat: Devuelve el número de asiento del usuario que envió el mensaje, o -1 si el usuario no tiene un asiento.

Get_player_p2pid: Devuelve el p2pid para el jugador especificado por el número de asiento o una cadena vacía.

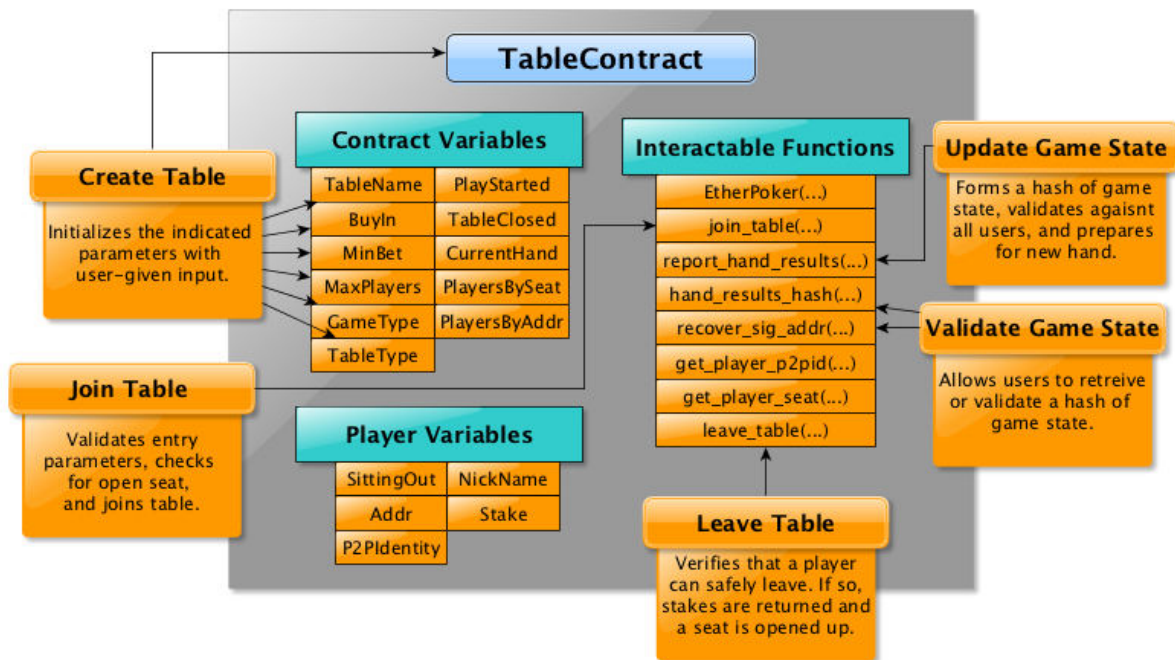
Hand_results_hash: Calcula un hash sha3 de los parámetros proporcionados por el usuario.

Recover_sig_addr: Devuelve la dirección asociada con el par de claves utilizado para firmar el hash.

Report_hand_results: Verifica que todos los jugadores hayan firmado los datos del juego y devuelve un mensaje de error, si corresponde.

Leave_table: Saca del juego al jugador y devuelve las ganancias del jugador.

Figura 15: Variables del contrato de mesa



8.4 GameNet

GameNet proporciona la interfaz para la comunicación de nuestra aplicación. Tenemos dos flujos principales de comunicación:

- Comunicación con otros jugadores utilizando P2PNet.

- Comunicación con la red Ethereum utilizando Web3.js

Unirse a una mesa de poker es un ejemplo de cuando un usuario interactúa con la red de Ethereum.

Cuando el usuario se une a una mesa de poker, está apostando en la mesa y enviando sus fondos desde su cartera. Otra parte importante de GameNet es el módulo responsable de almacenar sus fondos de forma privada y segura: el almacén de claves.

8.4.1 Almacén de claves

Una cartera que almacena sus fondos está representada por un par de claves públicas y privadas:

- La clave pública es la dirección pública que se usa para recibir fondos.
- La clave privada es la que se usa para enviar fondos.

Los fondos se envían en una transacción y la transacción se firma con la clave privada. Es importante mencionar que sus fondos son tan seguros como su clave privada, ya que si alguien tiene acceso a su clave privada, tendrá acceso a todos sus fondos.

Nuestro almacén de claves utiliza las mismas funciones de derivación de clave (Scrypt), cifrado simétrico (AES-128-CTR) y códigos de autenticación de mensaje como geth, la implementación oficial de Go del protocolo de Ethereum.

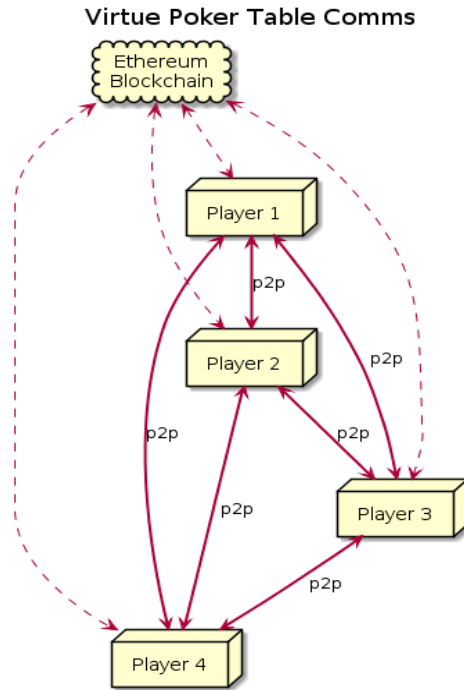
Sus claves se almacenarán en su disco duro y estarán protegidas por una contraseña que usted utilizará al jugar en Virtue Poker.

8.5 P2PNet

P2PNet es responsable de toda la comunicación que se realiza entre los usuarios sin utilizar la red de Ethereum. En el contexto DApps, esto se conoce como *off-chain*. Los recursos de la red de Ethereum se utilizan en todas las DApps y todas las transacciones a la red de Ethereum tienen un costo de operación, por lo que debemos ser lo más eficientes posible en DApps. Estamos trabajando para minimizar el tamaño de nuestros contratos para limitar los gastos generales y limitar las comunicaciones al blockchain de Ethereum para reducir los costos operativos y mejorar la velocidad del juego.

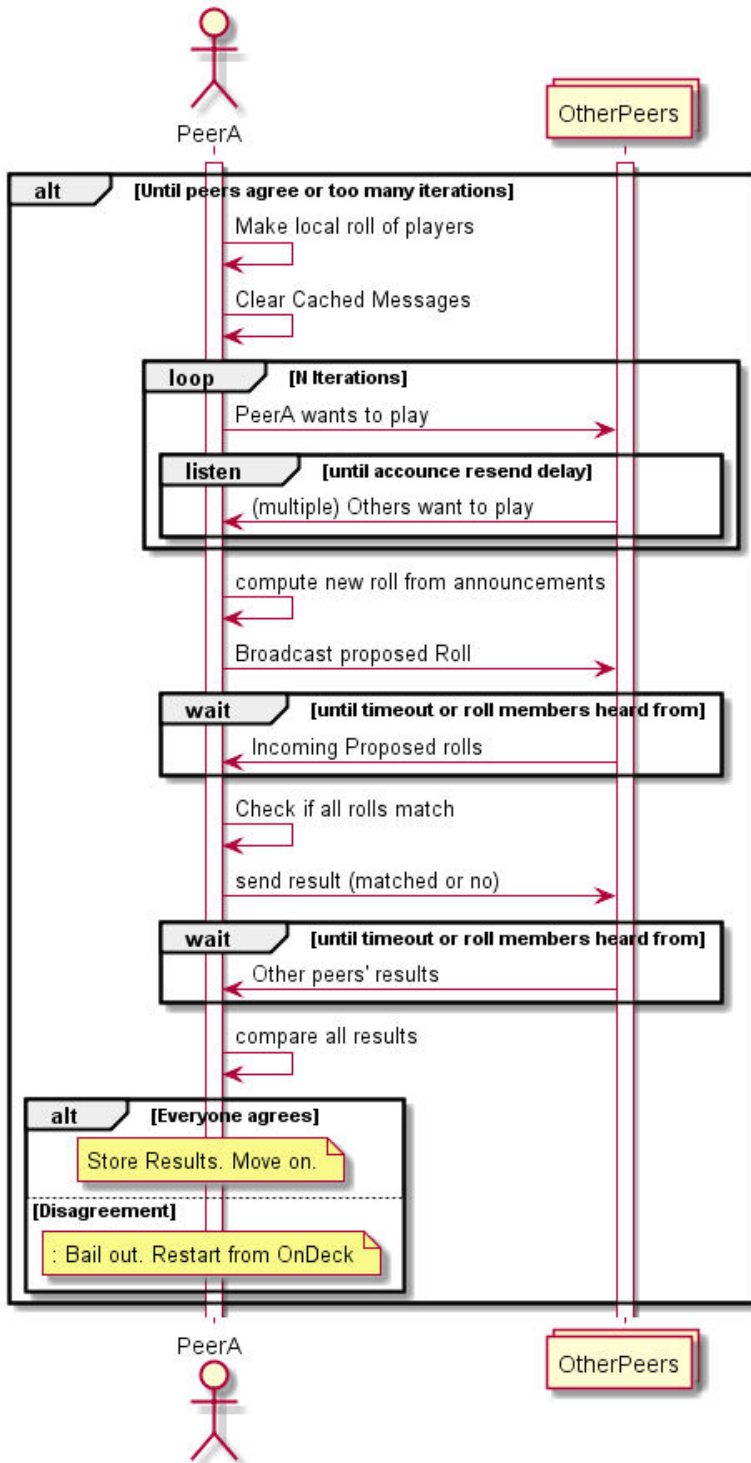
Nuestra P2PNet no está utilizando los canales de estado tal como están definidos, pero en cierto nivel, todo (excepto el chat) lo que transporta P2PNet es parte de una subred de estado en la que todos los clientes del juego se ponen de acuerdo sobre lo sucedido. Esto se hace de una manera en que blockchain puede verificar que estuvieron de acuerdo pero en realidad no puede retroceder y reproducir cada movimiento individual.

Figura 16: Comunicaciones P2P



Al comienzo de cada mano, los jugadores de una mesa determinada comienzan simultáneamente "a pasar lista" para verificar los mensajes de cada uno de los otros jugadores sentados y todos llegan a un acuerdo sobre quién será incluido en la próxima mano. La Figura 17 ilustra este proceso:

Figura 17: "Pasar lista"



8.6 Web3.js

[Web3.js](#) es la API Javascript compatible con Ethereum <https://github.com/ethereum/wiki/wiki/JavaScript-API> que implementa la especificación RPC [Generic JSON](#). Web3.js es una biblioteca oficial creada por el equipo de Ethereum Team. Nosotros utilizamos Web3.js para:

- **Compilar un contrato:** Nuestros contratos se precompilan y se prueban adecuadamente antes de compilarlos con Web3.js. Es necesario compilar un contrato antes de la implementación con web3.js.
- **Implementar un contrato:** Web3.js proporciona una API de Javascript fácil y segura para implementar un contrato.
- **Llamada de contrato:** Después de implementar un contrato, cualquier interacción con el contrato es una llamada al contrato que también se realiza mediante la interfaz web3.js.
- **Transacciones:** Cualquier otra acción que implique el acceso a la red de Ethereum siempre se realizará utilizando Web.js.

8.7 Electron

Nuestra aplicación de escritorio se basa en Electron. Electron se ha utilizado con éxito en proyectos anteriores basados en Ethereum, incluidos Mist Ethereum Wallet, Atom, Visual Studio Code y Jaxx Wallet. Electron es un marco de código abierto, creado por Github, para crear aplicaciones nativas con tecnologías web como JavaScript, HTML y CSS. Hemos elegido Electron porque:

1. **Es un marco multiplataforma:** Codifica una vez y tiene un producto capaz de funcionar en múltiples plataformas, en nuestro caso, Windows, Mac y Linux.
2. **Se basa en tecnologías web:** Podemos construir nuestra aplicación con las mismas tecnologías que se utilizan para construir sitios web sin la necesidad de contratar desarrolladores para plataformas específicas.
3. **Mejora el costo de desarrollo:** Podemos reducir los costos de desarrollo mediante la contratación de desarrolladores con talento que no necesariamente necesitan tener experiencia en plataformas específicas
4. **Mejora la velocidad de desarrollo:** Debido a que no necesitamos contratar desarrolladores para programar en plataformas específicas, todos nuestros recursos se enfocarán en el desarrollo de un producto que funciona en múltiples plataformas utilizando Electron.

8.7.1 Arquitectura de Electron

La arquitectura de Electron se basa en:

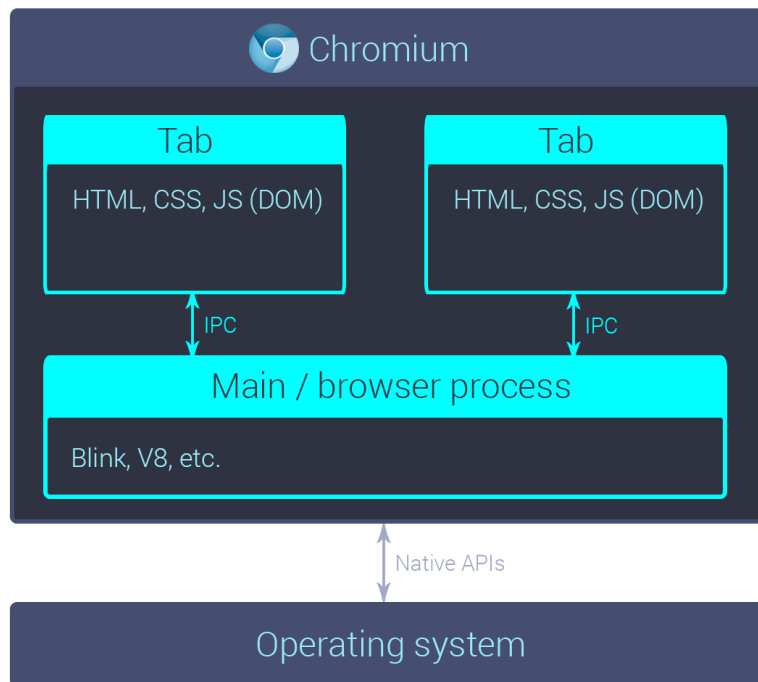
- **Chromium:** el motor de navegador utilizado por Google Chrome y Chrome OS. Esto nos permite construir nuestra aplicación utilizando tecnologías web.
- **NodeJs:** Node es un motor de Javascript creado sobre el motor Javascript Chromium V8/Chrome. Node proporciona acceso a los recursos del sistema operativo (por ejemplo, el sistema de archivos).

Cada nueva versión de Electron proporciona la última versión de Chromium y NodeJS. La versión actual de Electron en este documento es Electron 1.6.11, que contiene:

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

Aquí encontrará más detalles sobre Electron: <https://electron.atom.io/>

Figura 18: Chromium

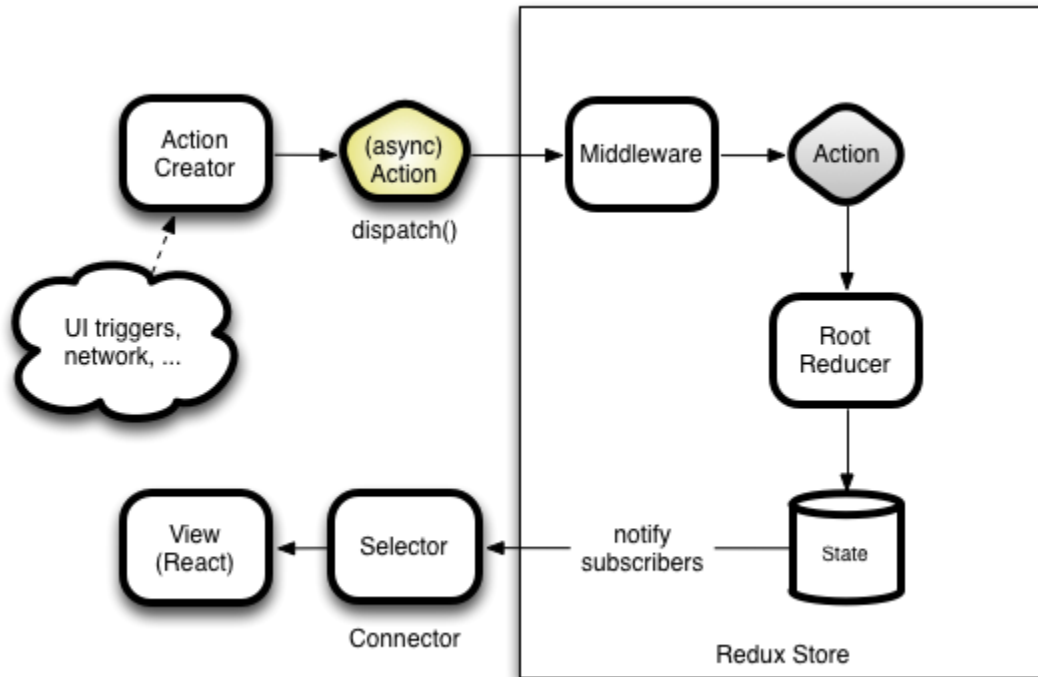


8.8 Cliente del juego de póquer

8.8.1 Arquitectura del cliente de juego

Nuestro cliente de juego está construido usando la arquitectura React React-Redux.

Figura 19: React



8.8.2 Juego

La interfaz de usuario del juego tendrá dos componentes principales que aparecerán en diferentes ventanas:

- Lobby
- Juego de mesa

Cuando el usuario inicie el juego, estará en el lobby y podrá realizar las siguientes acciones:

Iniciar sesión: El usuario usará sus credenciales para iniciar sesión en la aplicación.

Crear una mesa de juego: El usuario podrá crear una mesa de juego privada (solo privada o también pública).

Enumerar todas las mesas disponibles: En el lobby aparecerá una lista de todas las mesas de juego disponibles a las que los usuarios pueden unirse para jugar.

Unirse a un juego: el usuario podrá unirse a una mesa de juego o a un torneo de juego.

Administración de carteras: El usuario podrá administrar su cartera virtual de póquer.

Jugar un juego: La mesa de juego se abrirá en el componente de la interfaz de usuario del juego de la mesa en una ventana diferente.

Jugar múltiples juegos al mismo tiempo: El usuario podrá unirse a varios juegos al mismo tiempo.
