Virtue Poker Whitepaper DRAFT

A P2P Decentralized Poker Platform Built Using Ethereum

Draft Version 0.1

July 2017

This document is for informational purposes only and does not constitute an offer or solicitation to sell shares or securities in Virtue Poker or any related or associated company. Any such offer or solicitation will be made only by means of a confidential offering memorandum and in accordance with the terms of all applicable securities and other laws.

This document is a draft, and provided only as a courtesy and to begin gathering industry and community feedback. This document is not to be considered final, and all information contained herein is subject to change without notice. To the extent that Virtue Poker someday in the future offers for sale any products or services, including any tokens, you must refer to and review any terms, conditions and disclosures in effect at that time, including any updated versions of this whitepaper.

Table of Contents

1. Abstract

Virtue Poker is a decentralized platform for playing online poker with real money. It leverages the Ethereum blockchain to provide the first blockchain-based online poker experience where players never have to deposit money on a site, the shuffle is provably random, and cards are cryptographically secure.

1.1 Value Propositions

On Virtue Poker, there are no servers that store players funds and each player is involved in card shuffling. Our goals are to:

1.1.1 Eliminate Player Deposit Risk

Virtue Poker will enable players to have full custody over their funds by using Ethereum smart contracts to escrow tournament buy-ins and autonomously distribute payouts based on game outcomes.

1.1.2 Solve the Lingering Trust Issue regarding Gameplay Fairness

Using a peer-to-peer, cryptographic shuffling protocol called Mental Poker, all players seated at a table are involved in card shuffling, and reach consensus at the end of each hand using a Byzantine Fault Tolerant consensus mechanism.

1.1.3 Reduce Player Costs and Create a Balanced Poker Ecosystem

Our innovative peer-to-peer and decentralized architecture, coupled with our use of Ethereum, allows for Virtue Poker to eliminate costly server and payment processing expenses. Our aim is to pass these operational savings back to our players via lower rake, and rakeback systems that encourage player retention, creating a more balanced poker ecosystem.

1.1.4 Build out an Extensible Decentralized Poker Network

Virtue Poker's goal is to build out a core underlying decentralized online poker network that developers and third-party operators can plug-into and build on top of. We hope that new functionalities are built on top of the platform.

1.2 Short-Term Objective

The success of a new online poker platform is largely dependent on network effects in maximizing liquidity pools. Our goal is to be the first decentralized online poker platform to market and to leverage this first-mover advantage in establishing Virtue Poker as a legitimate market contender.

Our goal is to create a new innovative user experience and to complete a production ready application that will be deployed to the Ethereum main net. In order to accomplish these goals, Virtue Poker will build out our development and marketing teams, and host a pre-launch tournament with well-known online and live tournament professionals and broadcast this event live on Twitch.

1.3 Long Term Growth Strategy

There are 4 stages to our growth strategy following our Pre-Launch event: Private Beta, Limited Release, Full-Scale Launch, and Third-Party Integration.

Our strategy is comprised of two macro phases: (1) to first build out the technology and liquidity for our platform as a B2C operator to prove the desirability, integrity, and credibility of our solution, (2) and then expand globally through white labeling our software to enable new licensees in markets across the globe to seamlessly and cheaply start their own online poker room using our core underlying technology.

2. Problems with Online Poker

2.1 Introduction

Online gambling has its historical roots in the dot com bubble and has since grown to become a multi-billion industry expected to grow to over $50 billion by 2021.[1] Within this global industry emerged the subsector of online poker rooms that brought popular card games such as Texas Hold'em that were at one point only accessible through sparsely located land-based casinos, underground venues, and home games among friends, to a global audience available to anyone with an internet connection and a computer. The growth of online poker rooms ignited following the televised World Series of Poker Main Event in 2003 which broadcasted an unknown accountant named Chris Moneymaker winning over $2.5 million.

Today, the global online poker market is over $2.5 billion dollars. Globally, the online poker market is dominated by Europe and Asia, with 47% and 30% of the market respectively, with North America comprising 13%, Oceania 6%, and Latin America 2%.[2]

Unfortunately, the online poker industry has been subject to numerous scandals, and has fallen victim to malicious users over the past decade. While top poker sites such as PokerStars have adapted their platform to this problematic behavior, many sites have failed to adjust, creating a lingering perception of distrust among many players. In addition, increased competition, higher fees, and an unequal playing field has led to an imbalance in the poker economy leading to slower growth.

2.2 Misuse of Player Funds

2.2.1 Absolute Bet and Ultimate Bet Scandal

In May 2008 after years of player complaints, the third largest poker network Cereus Network (Ultimate Bet and Absolute Poker) based on the Kahnawake Mohawk Territory in Canada admitted that insider cheating had occurred whereby a former employee gained access to an administrator's account that allowed him to view all players' cards on the platform. Over the several years that the fraud occurred, this individual along with his co-conspirators stole tens of millions of dollars.[3]

2.2.2 Full Tilt

On April 15th 2011, a day known as "Black Friday" in the online poker community, US federal prosecutors indicted the founders of the three largest online poker websites, PokerStars, Full Tilt Poker, and Absolute Poker, and those sites stopped offering real-money gameplay to US citizens. When Full Tilt reopened their operation shortly thereafter, it was discovered they had a $150 million shortfall on player deposits.[4]

---

[1] 888 2016 Annual Report: http://corporate.888.com/sites/default/files/888%20AR%202016%20Hyperlinked%20PDF.pdf
[2] Playtech 2015 Annual Report: 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. Safest Poker Sites, n.d. Web. 07 Oct. 2016.
[4] http://www.pokerupdate.com/poker-opinion/544-13-biggest-poker-scandals-last-decade/

2.2.3 Lock Poker

In 2015 Lock Poker, which had offered games to US residents, was shut down after failing to honor player withdrawals for nearly a year. Their owner had used player deposits as personal spending money among other things. Players lost an estimated $15-$24 million.[5]

2.3 Poker Bots

Poker Bots can sit across multiple tables, and can run without human oversight. Poker Bots vary in their complexity: they can be bought off-the-shelf, or can be custom built and employed by an individual actor. They vary in their degrees of success, and ultimately only the most sophisticated of bots can beat highly skilled professional players.

In 2015, it was reported that a bot-ring on PokerStars won nearly $1.5 million in $0.50/$1.00 and $1/$2 cash games.[6] This scandal overshadows a persistent and prevalent problem in online poker. There are companies such as WarBot that sell bots off-the-shelf to users who can run them on all platforms, including PokerStars.[7] Publicly traded companies such as 888 Holdings have “low” security procedures to protect players against bots. 888 even has a blog post about “How to Play Against Poker Bots” calling them “weak.”[8]

Yet, recently in 2017, Carnegie Mellon University recently ran a competition called “Brains vs Artificial Intelligence: Upping the Ante” where four of the world’s best online heads-up poker pros competed against a poker bot called Libratus – and lost.[9] While Libratus is powered by a supercomputer, the threat poker bots pose for the future success of the industry is significant.

2.4 Third-Party Tools and Software

Many online players use third-party tools and software that targets recreational players via a multitude of methods.[10] These tools include (but aren’t limited to):

Player Databases: A database of players that can be queried to find players with low win rates across multiple poker networks

Auto-Seating: Automatically seats players at quality checked cash game and Sit & Go’s, as well as color coding players based on player statistics

Player Scanning: Scans players currently in a poker site’s lobby who match specific criteria

Heads-Up-Displays: Displays real-time stats of opponents at active tables

[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

These tools are designed to give players access to information about their opponents and are typically used by regular online poker players. Unfortunately, these tools create a disadvantage for recreational players that are not employing these programs, and unknowingly are targeted by highly skilled professionals.

2.5 Unequal Rake

Rake today is collected via tournaments or cash games. For tournaments, a percentage close to 10% is added to the buy-in. In cash games, a certain percentage is taken from every hand that goes to the flop. The cash game rake online today is commonly 3-5% with a cap between $0.30-$5 per hand. While the rake differs slightly at various sites, overall the rake structure is very similar across all online poker rooms.

Figure 1 shows the current rake structure for PokerStars.[11] At first glance, this structure seems to make sense: in absolute terms, higher stakes players are paying more rake than lower stakes players, and are more valuable customers:

Figure 1: PokerStars Rake Example

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

Yet notice that the cap on the lowest stakes ($0.01/$0.02) for a 5+ person game is 15x the big blind, and for a $3/$6 game, the cap is .58x the big blind.

According to a 2011 research study by the University of Hamburg which analyzed over 2.5 million hands over a 6 month period on PokerStars among other sites, on average each player at $0.01/$0.02 pays 12.5 BB (Big Blinds) per 100 hands in rake, while those at $3/$6 pay 2.58 BB per

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

100 hands.[12] Figure 2 summarizes the average rake paid per 100 hands at each different level according to the study:

Figure 2: Rake Across Stakes

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

As stakes increase, the rake in relation to the big blind decreases dramatically. A win rate of 4-6 BB per 100 is an excellent win-rate for online poker standards. With the current rake structures, most winning players at the lower levels become losing players while only those at the highest levels having a chance of earning income from playing online.

2.6 The Broken Poker Economy

2.6.1 Definition

The poker economy has three key inputs: Deposits, Rake, and Withdrawals. In order for the global poker economy to grow the following function must be true:

$$\textit{Net Deposits} > \textit{Rake} + \textit{Withdrawals}$$

This model requires a constant supply of deposits to survive. Professional players have a net positive on their withdrawals, while recreational players generally have a net positive on deposits creating balance in the ecosystem. In order for the economy to grow, new players must deposit at a higher rate than professionals withdraw.

2.6.2 The Problem

Unfortunately, semi-professionals and professionals are winning at a higher rate than recreational players are depositing, creating a strain on the poker economy. This is due to increased competition as poker strategy has become publicly available through online tutorials, blogs, and other literature, and due to the unfavorable dynamic created for recreational players from disproportionate rake, third-party tools that track and hunt less seasoned players, and distrust among recreational players regarding the integrity of online poker.

[12] *THE GAMBLING HABITS OF ONLINE POKER PLAYERS: The Journal of Gambling Business and Economics 2011 Vol 6

2.7 Global Market Fragmentation

Due to the regulatory constraints placed on the industry, operators are restricted in their ability to serve customers across major jurisdictions and regions. Jurisdictions are categorized into the following categories based on regulatory response (exact nomenclature varies):

2.7.1 Black Markets

Black Markets are jurisdictions that either have classified online poker as illegal or only allow intrastate games to be played.

2.7.2 Dark Grey Markets

Dark Grey Markets are jurisdictions that don't explicitly prohibit online gambling and/or have legislation that is unclear.

2.7.3 Grey Markets

Grey Markets are jurisdictions that have regulated online gambling, or have not taken any action against remote operators.

2.8 Types of Operators

Within this regulatory framework, operators choose either to operate in multiple markets with a single or multiple licenses, or all markets with a single or no license. These can be classified as "on-shore" operators, and "offshore" operators.

2.8.1 Onshore Operators

Regulated operators have obtained minimally at least one gaming license from a respected gaming authority and operate typically in most grey and dark-grey markets. These operators adhere to AML/KYC, tax, and other compliance policies, and many are publicly traded companies on various exchanges around the globe. Onshore operators include: Amaya (PokerStars, Full Tilt) William Hill Online, Playtech (iPoker network), 888 Holdings, Unibet, GVC Holdings (PartyPoker, bwin.party), Winamax

2.8.2 Offshore Operators

Unregulated operators typically reside in offshore jurisdictions in Costa Rica, Curacao, Cyprus or on Indian Reservations. They have typically offered their services to customers globally including Black Markets. There is relatively minimal data that can be obtained on these operators. Offshore Operators include: PaiWangLuo Network (Ignition, Bovada), Merge Gaming (Carbon Poker), Winning Poker Network (America's Cardroom), Global Gaming Network, TheHive, Tiger Gaming (Chico)

An increased number of jurisdictions and countries around the world have begun regulating online poker, leading to a greater portion of regulated online poker traffic.

2.9 Limited Competition

Online poker networks' success is dependent upon establishing large global liquidity pools of players. Therefore over time, the market has been reduced to a few large operators within their respective target markets, leaving players with limited playing options and enabling operators to charge higher fees to players.

2.9.1 Regulated B2C Market

Within the regulated B2C market, PokerStars has positioned itself as the market leader, with nearly $2 billion in annual revenue, and around 50% of global online traffic dependent upon varying sources of data. They operate in nearly every country in the world (30 blacklisted markets), and have the largest cash prizes and weekly tournaments. They have hosted the world's largest online poker tournament (253,000 entries), and have given away the largest prize pool ($75.6 million). They have dealt over 145 billion hands of poker, and they sponsor the top poker professionals and live tours[13]. And they have had household names such as Kevin Hart, Usain Bolt, Rafa Nadal and Ronaldo as brand ambassadors. PokerStars has invested in player protections such as top-of-the line bot detection, numerous payment processing options, and multi-accounting prevention, and they have been able to build the largest liquidity pool in the world.

There are two major disadvantages in using PokerStars: (1) Their services come at a high cost to players via high rake structures and (2) their platform is highly competitive. Players competing on their platform are faced with higher rake and stronger competition making it more difficult for even the best players to earn a steady income from playing online. And due to their market leading position, they are able to operate with minimal pushback from players, enabling them to eliminate long-standing loyalty programs, increase fees, and pull out of markets with minimal notice.

2.9.2 Unregulated B2C Market

The unregulated online poker market is slightly more fragmented but has still come to come to be dominated by the Winning Poker Network, and newly branded PaiWangLuo Network (Ignition, Bovada). These companies are more willing to service the Black Markets and lack transparency in their business practices. Generally speaking, these sites put minimal investment into anti-cheating practices such as bot detection or multi-accounting, leaving players to fend for themselves on their platforms.

Many players have gravitated to these platforms due to either limited playing options, or high competition on regulated platforms. Yet, the lack of due diligence and reporting requirements of these companies leaves players with a lack of insight into daily operations, and provides minimal recourse options should these sites go offline, lock players out of their accounts, or be accused of wrongdoing.

[13] *PokerStars 2015 Annual Investor Form: http://www.amaya.com/pdf/amaya---2015-aif---final.pdf

2.10 Random Number Generator Certification Practices

Online poker is different from live games in a key domain: in a live game, players can see the dealer shuffle the deck of cards, whereas in the online sphere players must *trust* that the RNG of the operator is operating sufficiently. Nearly every online operator has their RNG certified by a pre-approved third-party. RNG testing companies include iTech Labs, and Gaming Laboratories International. The integrity of these companies rarely comes into question, and generally speaking these auditors complete their jobs sufficiently.

More interestingly is the lack of oversight after an operator receives their certificate. The Malta Gaming Authority uses the following language on their website: "After the certification process required for issue of the full five year licence, the gaming system need not be tested regularly, but there will be follow up audits by the Gaming Authority when deemed prudent."[14] The Isle of Man uses the following language in their Guidance for Online Gambling: "While many operators may have their games' RNG checked on a more frequent periodic basis, the GSC will have an operator's RNG checked at least twice in a licence's 5 year lifespan."[15] This lack of oversight has contributed to a prevalent belief among online poker that the games in certain instances may not be entirely fair.

2.11 Conclusion

There are numerous disadvantages poker players face in the current online poker marketplace. Players must combat malicious software, high fees and stiff competition in the regulated markets, and in black markets are forced into playing on sites that lack accountability and transparency. And overall, increased competition, higher fees, and distrust among recreational players has led to increased strain on the global poker economy.

[14] http://www.cc-advocates.com/gaming-law/license-requirements.htm
[15] https://www.gov.im/media/1349489/guidance-notes-for-making-an-online-gambling-application.pdf

3. The Virtue Solution

The Virtue Poker team has spent years researching the current market dynamics in the existing industry, and our goal is to address these shortfalls in creating a new decentralized online poker network with trust, transparency, and accountability built in. Our goal is to reinvigorate online poker through the utilization of the Ethereum blockchain, peer-to-peer networking, user-owned identity, and cryptographically secured cards, with the aim to create an improved playing experience, at a lower cost to players. More importantly, using these new frameworks, our aim is to fix the broken poker economy by both reducing costs to players via lower rake, building out rakeback structures that encourage player retention, and through creating the most safe and secure online poker platform that will enable players to have fun on our platform, creating a more balanced online poker ecosystem.

3.1 User Flow

Virtue Poker is a server-less application that will run without storing customer funds, and all players will be involved in card shuffling. The user flow can be described as follows:

3.1.1 Download Virtue Poker Client

A user will visit www.virtue.poker and download our client for either Windows, Mac or Linux. The application is downloadable and includes a shuffler, game engine, and user interface.

3.1.2 Registration

Users will then be required to create a uPort identity (if they haven't already created one). The user will have to receive an attestation regarding country of residence and age prior to playing on Virtue Poker when required.

3.1.3 Fund a Light Wallet

The user will be brought to a page that directs them to fund the light wallet that is pre-built into the client.

3.1.4 Create a Game or Join a Game

The user will have the option to create a private game where he or she can invite other players to join, or go to our lobby which will show all publicly available games via our Casino registry.

3.1.5 Buy-In

The user can join either a public or private game by sending ETH or VPP (to be discussed later) to the table address of the game they'd wish to join. The table or smart contract will sit on the Ethereum blockchain and acts as an escrow account while gameplay is conducted. Each game on

Virtue Poker is represented by a table contract that has the custom parameters of that particular game.

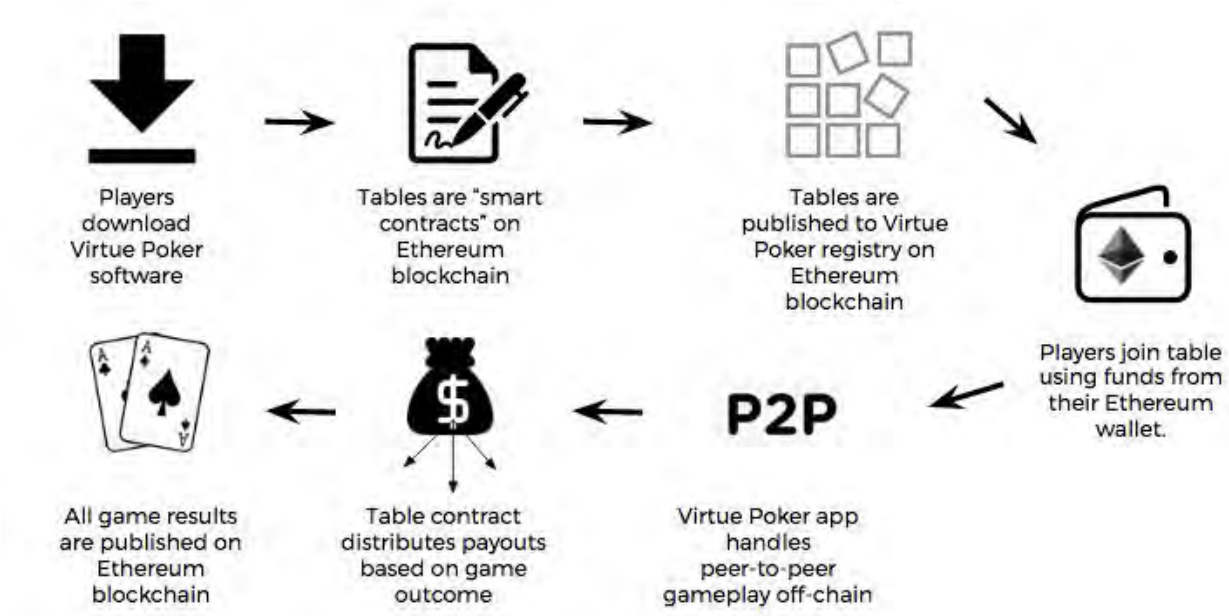
3.1.6 Gameplay

The peers at the table will form a P2P subnet and will use a mental poker protocol that requires each individual peer to shuffle the deck of cards.

3.1.7 Payout

When a tournament is completed, or when a player leaves the table for a cash game, the table contract will auto-execute and payout each individual player when winnings are due.

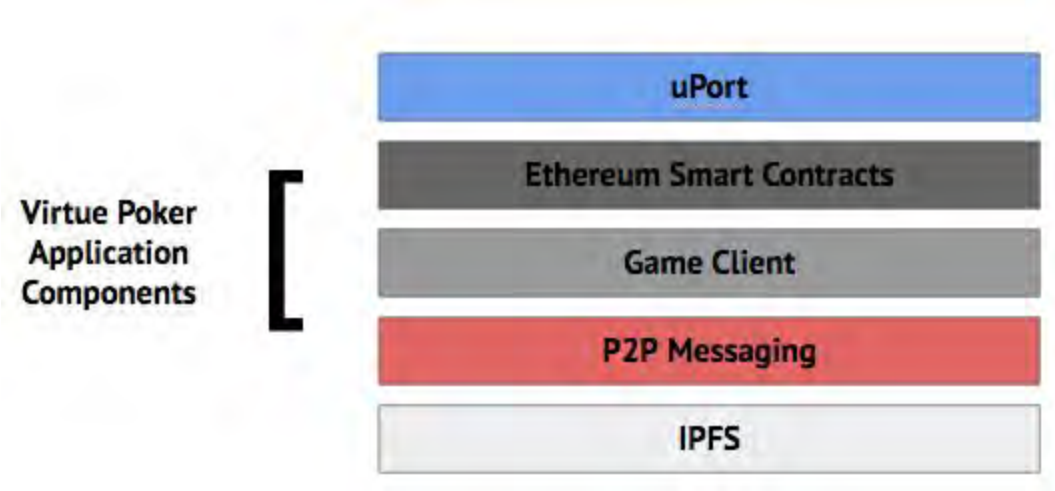
Figure 3: How Virtue Poker Works



3.2 Virtue Poker Components

The Virtue Poker platform will utilize several sub-components for different purposes within the application:

Figure 4: Virtue Poker Components



3.2.1 uPort

The Ethereum-based identity application uPort will be utilized as a registration and identity validation mechanism to prevent underage gambling and multi-accounting. Users will be required to sign-in via uPort each time they want to play games on Virtue.

3.2.2 Ethereum Smart Contracts

Ethereum contracts are utilized for several purposes: (1) as a registry (Lobby) for all active games on the platform (2) as a short-term escrow service for players seated at a given table (3) as a repository for all game-specific parameters such as buy-in amount, payout percentages, and game type, (4) reporting end game results.

3.2.3 Game Client

The Game Client will initially be a desktop application that is a state-engine that runs the game logic, shuffles and deals cards using a Mental Poker protocol, includes a light wallet, and connects to other players at a given poker table.

3.2.4 P2P Messaging

The P2P messaging backbone is utilized as a communication and synchronization tool to ensure the user interface for all players at a given table displays the identical game state.

3.2.5 IPFS[16]

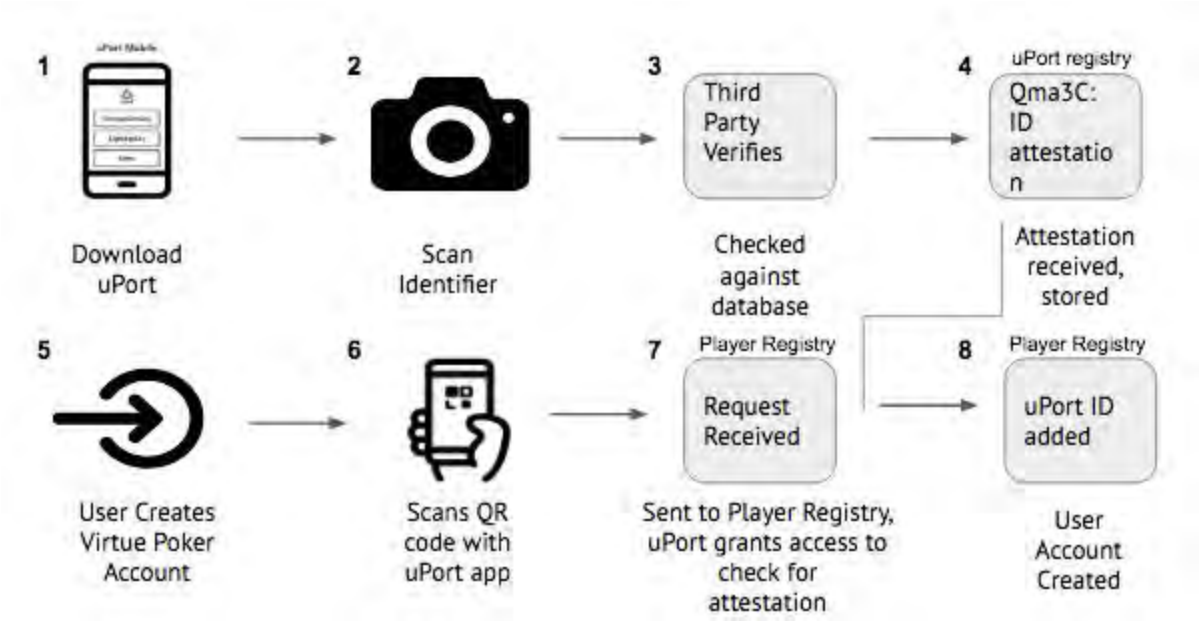
IPFS will be used to log hand histories for all games played on the platform. Logs can be retrieved at a later point in time for review either for compliance or for our game security team.

[16] The Virtue Poker team may choose to use alternative distributed storage solutions such as Swarm

3.3 Identity Management

Virtue Poker will use the self-sovereign identity application uPort to validate a player's' identity prior to allowing users to access the platform.[17] An example of this process is illustrated below:

Figure 5: Illustration of Identity Validation



Step 1: A user downloads the uPort mobile app, creates a uPort identity and then scans a copy of their proof of identity that is verified by a third-party. The attestation is then encrypted and stored in IPFS, and the user receives an attestation within their uPort ID regarding their identity.

Step2: A user makes an account on Virtue Poker and is presented with a QR code that the user scans with their uPort app

Step 3: A new account request is sent to a Virtue Poker Accounts contract with the associated uPort ID which checks for an attestation from the third party that has verified the user's identity.

Step 4: If successful, that user's uPort ID is paired with their Virtue Poker account address and is stored in the Virtue Poker Player Registry.

[17] https://www.uport.me/

3.4 Ethereum Smart Contracts

After a player has verified their identity and created their account, the user is brought to the “lobby or casino contract.

3.4.1 Casino Contract

The Casino contract functions as the lobby. It contains a registry of all available games, as well as recently completed games. Its functions include game creation as well as matchmaking and other frontend, user, and game-management tasks.

3.4.2 Table Contract

A Table Contract represents a single instance of a game of poker in Virtue Poker. When a decision is made to start a game of poker with a particular set of rules and limits and a given set of players, a new table contract is created and players join it to play. When that game is done, pots are paid, and the players leave, then that table contract is "closed" and no longer used other than as a reference point.

During play, the table contract serves several purposes. Primarily, it is the repository for all information regarding the rules and settings for the game being played. It also maintains a list of the players in the game, as well as information about them needed by the other players. In addition, it is where funds used for gameplay are escrowed, and is responsible for distributing winnings.

When a player joins a table contract, the funds necessary to cover the table buy-in are transferred to the table contract and credited internally to the player's stakes. The player then receives from the contract the information necessary in order to communicate with the other player at the table and play begins. As play progresses, the contract is informed as to the state of the game and updates its state accordingly. When the player leaves the game, the contract transfers any funds due to the same account from which the player originally paid them.

3.4.3 Player Interactions with Table Contracts

As currently architected, transactions by players are sent to table contracts in the following instances: (1) to join a table (2) at the end of each hand (3) when a game is completed (for tournaments) or when a player leaves a table (for cash games). Our goal is to minimize the number of transactions sent to Ethereum to reduce our gas costs and improve gameplay speed.

The table contracts include a “chip counter” which keeps tracks of the players’ stakes at each particular table. At the end of each hand, each player and the Justice (described in Section 4.2) cryptographically sign the end-results, and send a transaction to the table contract which updates each respective player’s stake accordingly. This consensus mechanism and transaction submission by the peers at each given table functions as a “oracle,” enabling the contract to keep an updated game state, and to know when to pay players. This process happens asynchronously as hands are played on the platform, meaning that players can move onto the next hand while previous hand result is validated by the blockchain.

3.4.4 Multi-table Tournament Contract

For tournaments that involve play across multiple tables, the multi-table tournament contract acts as an organizational tool that manages the distribution of players across the tables. Any aspects of the tournament that exist at a higher level than the table itself are handled by this contract.

3.4.5 Justice Management Contract

A "Justice" is a special case of the player client software which participates in the peer-to-peer gameplay of a table, but does not receive cards or place bets. Instead the Justice is externally incentivized to act as a "more trustworthy" peer in the table subnet in such a way that a set of them at a table can be used to resolve certain potential disputes that might arise and to log the game data.

In order to both distribute the workload as well as to discourage any potential for collusion between Justices and players, the Justices are assigned randomly to tables from a pool, and rotate through tables after a certain number of hands. The Justice Management Contract is responsible for both keeping a registry of available Justices as well as for assigning them to the poker tables. Justices will be discussed at greater length in Section 4.2

3.5 Mental Poker

3.5.1 Overview

In 1978 cryptographers Adi Shamir, Ron Rivest, and Leonard Adleman published a paper in response to a question that had been posed by the computer scientist Robert W. Floyd: "Is it possible to play a fair game of 'Mental Poker'?" This paper proposes an encryption scheme and communications protocol that allows two people at different locations to shuffle and deal virtual "cards" in a way that allows a game to be played without the need of a trusted third-party.[18] Over the ensuing years there have been numerous other papers published on the subject, expanding upon the ideas, offering alternative methods, and providing analysis and critique.

There have been, however, very few practical software applications employing Mental Poker techniques. In large part, this is because the cryptography involved can require enormous amounts computational power and communications resources, and software using them simply runs too slow for consumer use. In addition, the inherent "peer to peer" nature of Mental Poker can be difficult to manage and doesn't blend well with traditional server-based online game models.

The Virtue Poker team has spent the past two years examining how the use of blockchain and distributed storage technologies, in concert with cooperative peer-to-peer networking, can address some of these difficulties. The result is a downloadable application that can play a 6-handed game at speed and manage real player stakes using the Ethereum Blockchain.

Mental Poker ensures the decks are unreadable to any single player by encrypting and shuffling the cards cooperatively in a way that lets each card be "opened" by one, some, or the entire group. The protocol uses communicate encryption: cards can be encrypted or decrypted in any order. The basic algorithm is outlined in Section 3.5.2.

[18] A. Shamir, R. Rivest and L. Adleman. Mental Poker. *MIT Technical Report*, 1978.

3.5.2 Mental Poker Algorithm, The Two Pass Shuffle

The basic algorithm is as follows: Three players, Bob, Alice and Ted are seated at a table and are playing a game of Texas Hold'em. Bob is the dealer, and he generates a deck of 52 cards on his machine, only he can view the cards. Using Fisher-Yates /dev/urandom he shuffles the deck of cards, and then encrypts the deck with the same encryption key on each card, making the deck unreadable to anyone but himself. He then passes the now encrypted deck to Alice, who does the same thing: shuffles the deck of cards and then encrypts them. Finally, Alice passes the deck to Ted who goes through the same process.

The deck is now in its final ordered state, 1 through 52, and this order does not change throughout the course of the hand. Ted passes the now 3x encrypted deck of cards back to Bob, who takes off his "shuffle lock" and now encrypts each individual card with a different encryption key: B1, B2….B52. He passes the deck to Alice, who does the same thing: removes her "shuffle-key" and encrypts the deck with a unique encryption key A1, A2….A52. Alice then passes the deck back to Ted, who completes this same process.

Bob is assigned the first and second card in the deck, but he only possesses his encryption keys that correspond to these cards. Alice and Ted therefore share their encryption keys that correspond to the first two cards, A1 and A2, and T1 and T2 respectively, so that Bob holds all three decryption keys for his private cards. This enables Bob to view his private cards but no one else. This process is repeated for each player at the table, so each player can only view their own private cards.

All players call and the hand goes to the flop. The flop is denoted by cards 7, 8 and 9 in the deck. All players must share their encryption keys that correspond to the community cards, so that everyone can see these shared cards. This process continues until the end of the hand, where the winning player is awarded the pot, and all players reach consensus (described in detail in Section 4.2) by signing the end result of the hand which is sent to the Ethereum blockchain to update the game state (chip totals) for all players seated at the table. See Figures 6 through 9 that depict this process:

3.5.3 Two Rounds of Encryption: Shuffling the Deck and Indexing the Deck

"Multi-party shuffling" only requires that one of the peers perform a "proper" random shuffle in order to ensure that the entire deck is randomly ordered. If a player trusts that his own machine shuffled the deck properly then he can have confidence that the game is fair.

Figure 6: Shuffling and Encrypting the Deck[19]

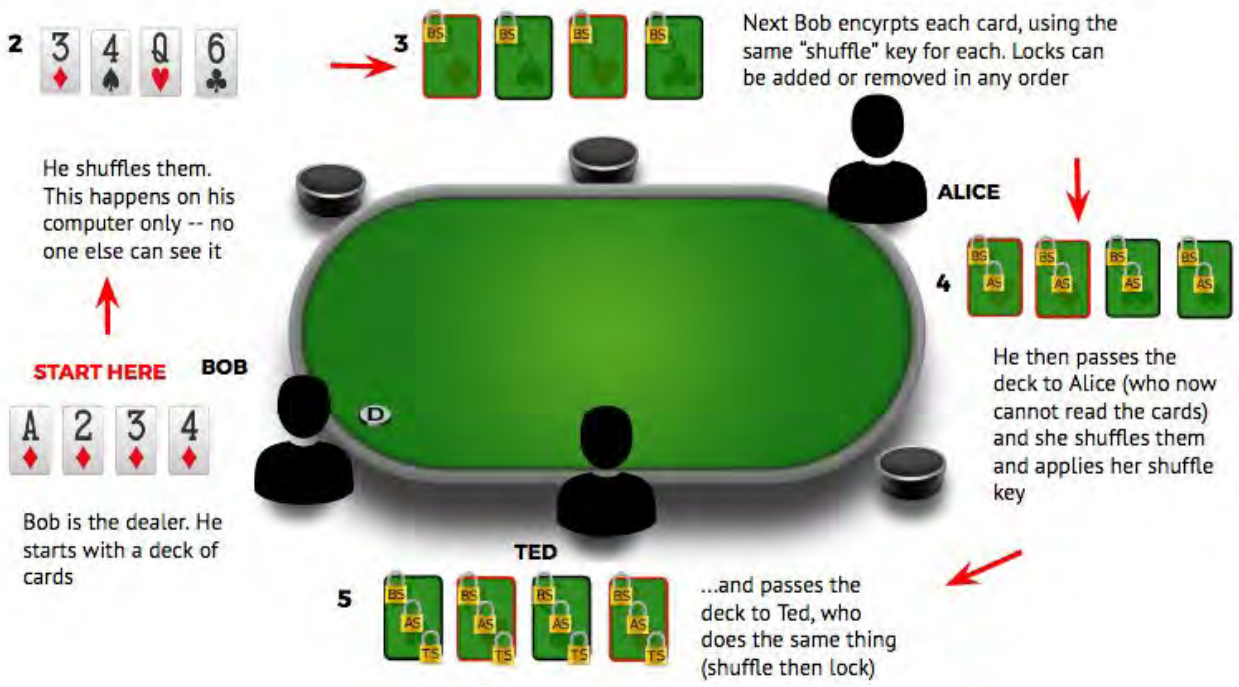
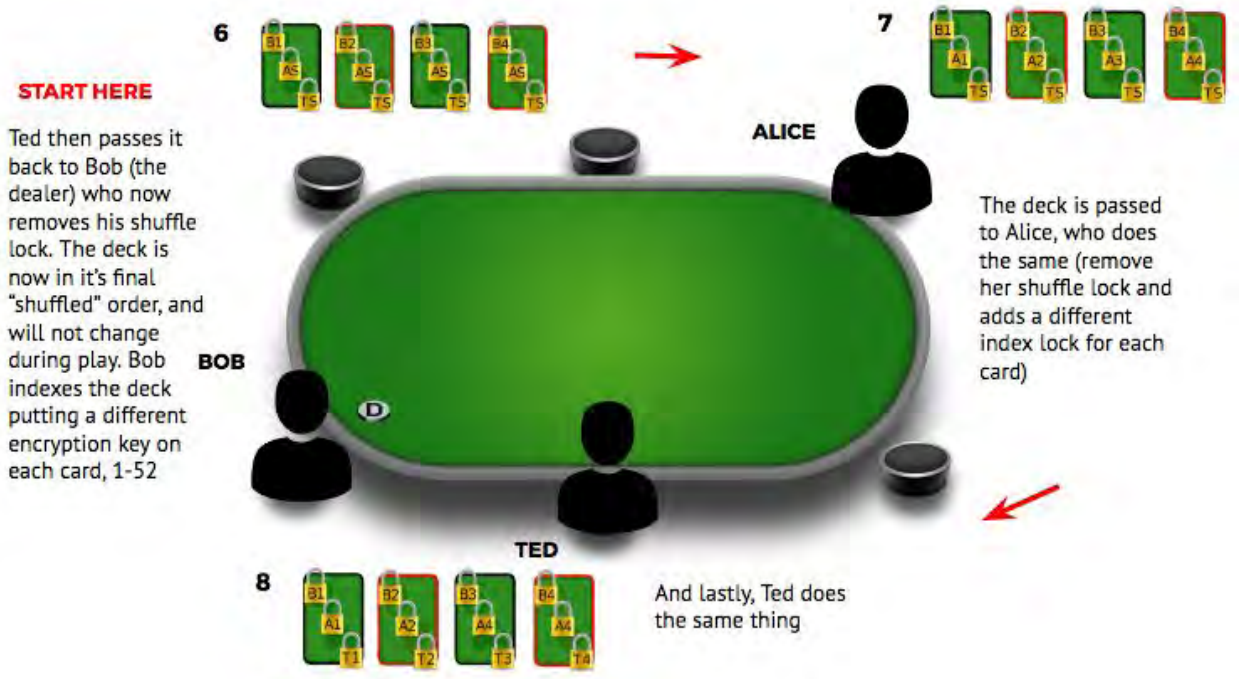


Figure 7: Indexing the Deck



[19] The four cards in figures 6 and 7 are meant to represent a full 52 card deck, not each player's private cards

3.5.4 Decryption and Gameplay

Figure 8: Player Key Sharing

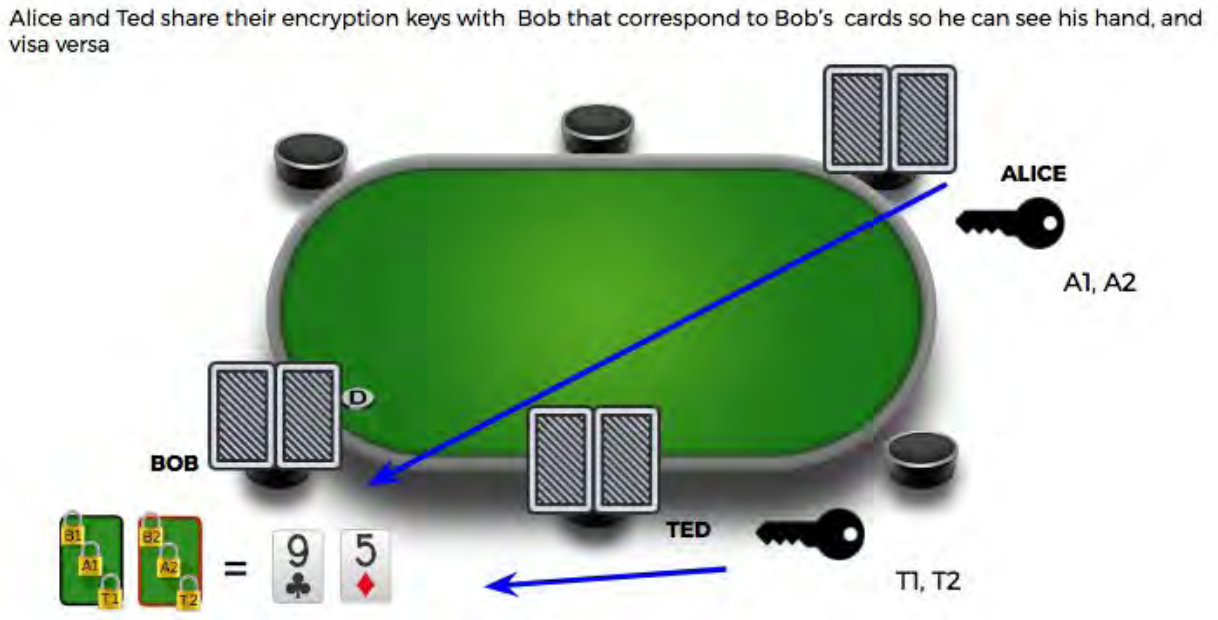


Figure 9: Community Cards[20]

[20] The turn and river community cards will be revealed the same way after the flop and turn rounds of betting have concluded

This process happens “under the hood:” the look and feel of a hand on Virtue Poker is similar to the experience players have come to expect with online platforms.

3.6 Peer-to-Peer Messaging

3.6.1 P2P Messaging for Game Client Synchronization

While the ideas behind Mental Poker make it possible for a deck to be shared and cards dealt and held secret by players in a peer-to-peer network with no need to trust a central server, other technologies are required in order to provide a practical, consumer-oriented poker service.

The downloadable game client software consists of separate "frontend" and "backend" processes. The frontend displays the current game state to the local user, and accepts input when appropriate and passes it to the backend, which then broadcasts it to the other clients in the game. The backend contains the logic needed to apply the rules of poker to the input events that it receives both from the frontend and from other clients. The result is that every client is actually applying the same code to the same data as all of the others.

3.6.2 Off-Chain Gameplay

A programmable blockchain technology like Ethereum makes it possible to have available a definitive and immutable data store for things that might otherwise be handled by a single server, like managing the players at a particular table. The ability for client software to interact with "contracts" on the blockchain also allows for trustless, distributed management of player funds and table stakes, and provides and immutable record of these interactions. But the blockchain cannot simply be used as a replacement for a server for all aspects of the game partly because data and instructions sent by a client take at best a few seconds to propagate across the chain, making it impractical to use it to manage game events at a finer granularity than at the hand level.

Game events occurring at a higher rate, like betting, must be managed by the client software itself, or more properly: by the software that manages the peer-to-peer "subnet" consisting of the clients playing at a particular table. The use of digital signatures allows each client to verify that messages received have been sent by the claimed sender, preventing forgery. Fault tolerant consensus formation techniques are used to ensure that at each step in the process of gameplay, every client agrees with every other client as to exactly what has happened. In addition to catching errors and hardware failures, Byzantine faults (intentionally bad data) are also detected.

At the end of each hand this "consensus" data - digitally signed by every client - is passed to the blockchain for processing, and the clients themselves move on to the next hand. Disagreements among clients, or peers at the table are resolved by Justices (described in Section 4.2).

3.7 IPFS: Game-log Storage of Hand Histories

In order to provide a permanent record of the actual play of each hand, the signed game event messages themselves need to be stored, as well as the state information tracked by the blockchain when it processes the end of a hand. This turns up a second weakness in current blockchain

technology: using the chain to store significant amounts of data can be expensive, so simply sending all of this log data to the blockchain is not practical.

Fortunately, there exist technologies (IPFS, Swarm) that are designed to provide reliable, distributed data storage. At the end of a hand, before reporting to the blockchain, the client software sends the hand's log data to IPFS, which provides it with a single "hash" value that can be used to locate it at a later time. That hash is included with the state data sent to the blockchain contract, and since each hand's log data includes the hash of the previous hand's log, it is possible to request from the blockchain the most recent hash, and use it to chain back through the entire logged history of the game. A distributed storage platform removes singular points of failure present in various forms of centralized storage systems.

3.8 Fees on Virtue Poker

The Virtue Poker team understands that rake is an important factor players take into consideration when choosing a poker site to play online. Our team has been researching innovative rake structures and will use our private beta to test various approaches in addition to sourcing feedback from the poker player community. Our aim is to reduce operational expenditures and pass back those savings to players and employ the lowest rake in online poker.

4. Game Security

There are several forms of cheating that plague online poker. Current operators such as PokerStars take game security seriously while others have limited precautions. Several common forms of cheating in online poker are outlined below.

4.1 Forms of Cheating on Virtue Poker

4.1.1 Collusion

Collusion is defined as two or more players collaborating at a table by sharing information with each other and utilizing cooperative betting strategies to create an advantage against other players at a given table for the purpose of financial gain.

4.1.2 Multi-accounting

A single user may use several accounts across one or multiple machines and then will take multiple seats at the same table to create an unfair advantage in a tournament or cash game.

4.1.3 Data Mining

PokerStars defines an “Unfair Advantage” as any instance in which a user accesses or compiles information on other players beyond that which the uUser has personally observed through the User’s own game play.”[21]

4.1.4 Poker Bots

As described previously, poker bots are either off-the-shelf or self programmed software programs that can operate on poker tables without human oversight. Virtue Poker will create separate arenas on our platform for human versus human gameplay and bot vs bot gameplay. Our team feels that it is appropriate if players wish to develop poker bots and challenge their bot against other poker bots. However, if a player is caught running a poker bot in a human only game, they will be banned from the platform permanently.

4.1.5 Account Sharing

Account sharing can be defined as when two or more players use one account to take advantage of the poker site or other players. The poker site can be taken advantage of if they offer higher % rewards, such as rakeback, with the more an account plays and rakes. Other players can be taken advantage with nefarious actions such as selling an account deep in a tournament, as well as a stronger player playing on a weaker player’s account to get action

[21] https://www.pokerstars.com/poker/room/tos/

4.2 The Justice System to Combat Cheating

In order to combat collusion and cheating, Virtue has developed the Justice System. Justices are non-playing peers that are assigned to poker tables who provide security and protection to players on the Virtue Poker network and in exchange receive fees from players. Justices are assigned to tables on the Virtue Poker network, and every few hands, are randomly reassigned to another table. Justices can be thought of as validator nodes on the Virtue Poker network, signing each transaction for every hand on the platform and submitting hand histories for storage to IPFS. The functions described below are automated: there is no manual oversight needed for a user to run a Justice node.

4.2.1 Core Functions of Justices

Justices provides three core functions to the Virtue Poker network:

4.2.2 Dispute Resolution

In the rare instance two peers at a table disagree as to the "state" of the table at the end of a hand or a game, a Justice can resolve the dispute in real-time and award the winner the pot.

4.2.3 Data-Feed

Each Justice submits each action of every hand to Interplanetary File System (IPFS) so that hand histories can be stored. This is a both required by gaming regulatory bodies and ensures essential services such as collusion detection, bot detection, and multi-accounting identification can be conducted.

4.2.4 Partial Storage of Player Encryption Keys

Justices will store a decryption key for the players at the table. The "Dropped Player Problem" for Mental Poker is defined as when a player drops out of a hand prior to a hand being completed. This is problematic, as all players must share encryption keys for community cards to be revealed and for a hand to be completed. Using Shamir's Secret Sharing, each player's keys can be encrypted and split amongst all players plus the Justice. If the player drops the Justice can request the pieces from each player and decrypt the assembled pieces so that the hand can be completed.

A Justice node on Virtue Poker can be activated by downloading the Justice client to a machine, opening the application and activating the Justice. A more detailed description of the Justice System is provided in Section 5.1.

5. VPP: Virtue Player Points

VPP have four core utilities within the Virtue Poker network: (1) VPP can be “locked” in a smart contract called the Justice Registry that enable users to stake tokens and validate hands on the network in exchange for fees from players, (2) VPP can be used as an in-game currency, (3) VPP can be used to access special tournaments, and (4) VPP can be earned as rakeback.

5.1 Becoming a Justice

The “Justice Pool” is composed of a limited number of users that are active on the Virtue Poker network. In order to become a Justice, users must acquire VPP, stake tokens in the Justice Registry, and must have their machine on and their application open and set to “active” in order to be assigned to tables. The assignment rate of Justices to tables is based on an individual Justice’s stake divided over the total number of tokens locked in the Justice Registry. If a Justice is caught cheating, colluding, or misreporting hand results, that Justice’s stake is seized and is kicked out of the Justice Pool. Justice submissions will be reviewed prior to a Justice removing their stake (plus fees accrued) from the registry.

5.1.1 Justice Submissions Review Process

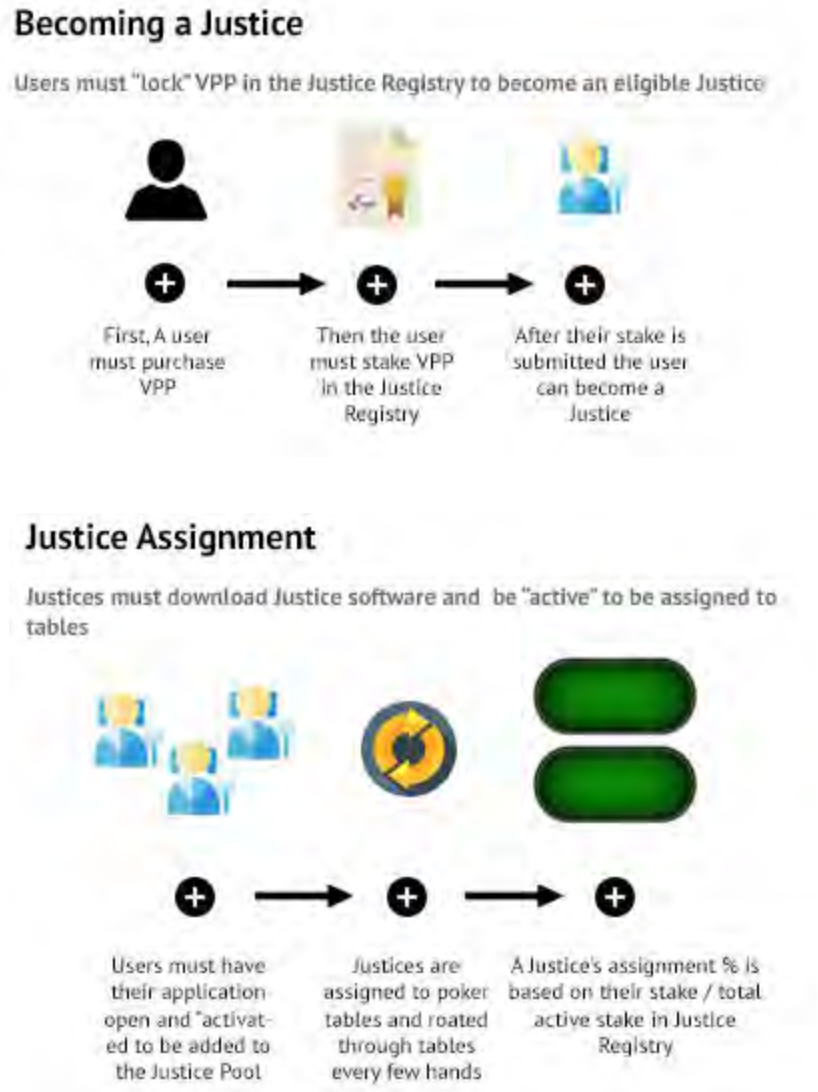
Initially, submissions by Justices to IPFS will be reviewed by a team of game security experts that will be consultants hired by Virtue Poker. The Virtue Poker team includes a game integrity and security expert who is assisting our developer team in building the Justice and setting up appropriate tracking software to detect red flags on the platform.

There are two ways for accusations of cheating to be submitted to our Game Security team. Players can submit a complaint or report suspicious activity, and these submissions will be reviewed and determined whether or not cheating has occurred. In addition, Virtue Poker will constantly run algorithms across the data submitted by Justices and all suspicious activity will be reviewed manually. If it is found that a player was cheating, a punishment will be levied and that player may be banned from the platform permanently.

5.1.2 Justice Fees

Fee’s generated on the Virtue Poker platform will be divided amongst the active Justice nodes on the Virtue Poker network. Fees will be accrued by Justices in both VPP and ETH. See Figure 10 for an illustration of the Justice System:

Figure 10: Justice System

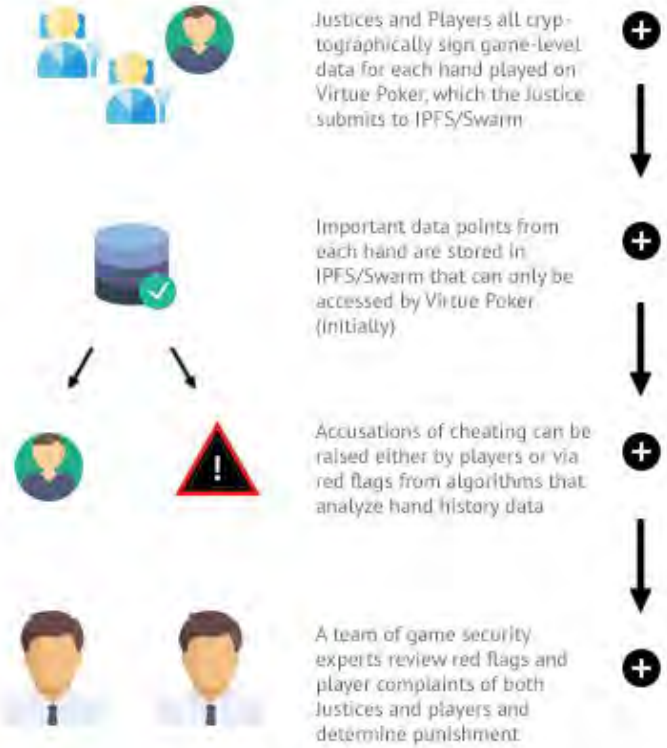


Justice Functions

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.



5.2 In-Game Currency

VPP can be used as in-game currency. Players can choose to participate in games denominated in VPP to grow their relative proportion of VPP in relation to other users.

5.3 Special Tournaments

Special tournaments and games can only be accessed with VPP, with users being able to compete to earn VPP or ETH. These tournaments will include, but are not limited to: guaranteed tournaments, freerolls, and special satellite events. In addition, the buy-in for Virtue Poker's initial kick-off tournament will only be open to users with VPP.

5.4 Rakeback Mechanism

VPP will be rewarded to users as a rakeback mechanism to reward our most loyal users. The mechanics of our rakeback system are still being tested, but more information regarding Virtue Poker's rakeback system will be revealed prior to our launch.

5.5 Token Sale

Virtue Poker will conduct our token sale before the end of summer. Additional details about our sale will be provided at a later date.

6. Roadmap

6.1 Key Activities

6.1.1 Platform Development

The Virtue Poker team has spent over 2 years developing our application, and will need to continue to build out our development team to build out a fully functional platform. Virtue Poker will hire developers to improve our P2P messaging backbone, create custom interfaces, optimize our smart contracts, and implement storage functionality. In addition, our team will integrate with ongoing Ethereum infrastructure projects including distributed storage, identity management, and stable coins.

6.1.2 Marketing

Virtue Poker will compete with market incumbents with large marketing budgets and sophisticated customer acquisition processes. We will dedicate significant marketing resources to guaranteed tournaments and freerolls, rakeback, marketing analytics software, and other paid marketing initiatives, including partnering with affiliates.

In addition, Virtue Poker will host a pre-launch tournament with online and live professionals prior to launch and broadcast the tournament on the live streaming platform Twitch to showcase the Virtue Poker Platform.

6.1.3 Sponsorships and PR

Virtue Poker will sponsor popular poker forums, websites, blogs, and events. In addition, our team will pursue an aggressive PR strategy to communicate our platform's value propositions to a broad audience.

6.1.4 Legal

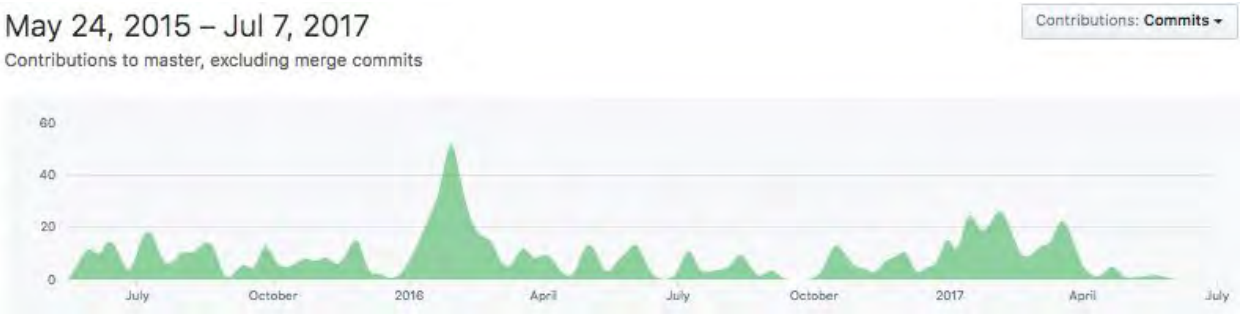
Our team has already begun consulting with well respected law firms including DLA Piper, ISOLAS and Ifrah Law, and with regulators around the globe. Our team plans to continue consulting with these resources as we navigate applicable legal and regulatory frameworks. Our team plans to pursue a gaming license prior to our launch to ensure our platform adheres to compliance standards and our players are sufficiently protected.

6.2 Development Roadmap

6.2.1 Current State

Virtue Poker was conceived in May 2015, and our prototype has been developed over the course of the last two years, see our history of GitHub commits:

Figure 11: GitHub Commits



Our application currently is 13,000+ lines of code, and has been tested weekly since its inception. Internally our team has been playing games of poker using a Mental Poker implementation that works on the Ethereum testnets.

The first version of Virtue Poker is desktop Python client that creates a custom smart contract for each table instance. Our team has successfully implemented a Mental Poker protocol for card shuffling and a game engine which is a state machine that connects with other peers via a P2P messaging protocol and hooks into Ethereum when peers create and join a particular table. Currently our application can play 6-handed and complete approximately 70-80 hands per hour.

6.2.2 Further Development

The Virtue Poker team has hired out our core team and will use the proceeds from our sale to continue to build out our team and the Virtue Poker platform. One of our goals is to redesign the Virtue Poker desktop app as an electron application. In order for our platform to be successful, the Virtue Poker application must undergo significant testing to ensure the games are sufficiently fair, the registration and identity verification method prevents low level multi-accounting and underage gambling, and our data storage mechanism is able to track data points necessary for compliance and to detect cheating.

6.2.3 Q4 2017[22]

Improve P2P Messaging Backbone
The application uses runtime-swappable plugin implementations for different transports, and is currently using a very basic HTTP-server-based message exploder. For deployment, Virtue Poker will implement a more industrial strength backbone.

Justice Implementation
The presence of one or more Justices in a game allows for permanent offline (IPFS) archival of peer-level gameplay - which is important when trying to detect collusion or bot play, or simply to

[22] Timelines and dates are subject to change

allow after-the-fact proof that things went properly. As part of the consensus mechanism a Justice prevents 2 players with hacked clients from cheating in a 3 player game: something other 51%-vulnerable consensus mechanisms cannot do.

Commercial Quality Front-End
Virtue Poker will re-skin our current application and build out a user interface for our lobby.

6.2.4 Q1 2018

uPort Integration for Identity Management
A user, when creating an Ethereum account for poker play, will be prompted to download the uPort mobile application and create an identity. The user will then associate his/her Virtue Poker account with their uPort ID. When joining a game, the user will use uPort to indicate that he is physically present, and we will use third-party attestations as our mechanism to combat low-level multi-accounting and account sharing.

Data Storage
Virtue Poker will use Justice nodes to collect and store gameplay at the hand level. We intend to store hand archive using IPFS, and to add a reference to the data to the table contract.

Build out Multi-Table Tournament Functionality
The “Multi-Table Tournament Contract” which will manage which tables are part of the tournament and what players are assigned to those tables. It will also manage tournament progress and resolution: who wins, and what. During gameplay, the 'table' is still the P2P subnet unit, and will function much as it currently does - but it will communicate with the MTT contract.

6.2.5 Q2 2018

Virtue Poker Private Alpha
Virtue Poker will conduct private user testing for pre-registered participants to debug our platform and to source feedback to improve upon our UI/UX.

Pre-Launch Event
Virtue Poker will organize a pre-launch event composed of well-known online and live professionals and live stream the event on Twitch

6.2.6 Q2/3 2018

Rakeback Mechanism
Based upon ongoing user testing, Virtue Poker will implement a tokenized rakeback mechanism using VPP.

Virtue Poker Limited Release (Open Beta)

Virtue Poker will launch our open beta to users around the world who can create and play in single table Sit & Go's and Cash Games.

6.2.7 Q4 2018

Virtue Poker Public Launch Tournament
Virtue Poker will publicly launch via a large guaranteed tournament enabling users around the world to play on our platform.

6.2.8 2019

Third-Party Operator Integration
In order to scale, Virtue Poker will enable third-party operators and licensees around the globe to create a custom skin on our platform and to create games on top of our underlying infrastructure.

7. Team

7.1 Core Team

Jim Berry, Lead Platform Developer: For 30 years Jim has worked on software ranging from the Hubble Space Telescope ground system to the Framingham Heart Study's Research Data Application to Linux drivers for an aerial image acquisition system to installing appropriate-technology email systems for developing nations in the South Pacific. Most of his career, however, has been spent working on computer games for companies like MicroProse, Looking Glass, and Electronic Arts - among others - specializing in physical simulation and graphics.

Ryan Gittleson, Head of Business Development and Marketing: Ryan is an experienced business development and marketing professional with a background in helping businesses and products increase sales. Before working on Virtue Poker, he worked as the Head of Customer Acquisition for a New York based startup called TodayTix, a Broadway ticketing mobile application, where he oversaw a growth in its user-base from 150,000 to over 700,000. He also worked for Time Out New York in their national advertising sales department, and holds a bachelor's degree from the University of Pennsylvania. He discovered Ethereum in August 2015, and instantly became captivated about the global potential of blockchain technology. He has worked with ConsenSys on Virtue Poker for the past two years.

Javier Franco Algarrada, Platform Developer: Javier is a senior software engineer with 10+ years of experience. He enjoys working on full stack applications involving multiple technologies and environments. He has been working for more than 5 years in gambling across different products like lottery, virtual sports, casino games and sportsbook. Always interested in cutting-edge technologies, he decided to move into blockchain projects last year. He holds a bachelor degree in computer science and a master's degree in web engineering.

Peter Marr, Game Security Consultant: Peter has been heavily involved in the online gaming industry for the last 12 years. Working professionally in it for over the last 9 years, specifically within online poker, Peter has gained invaluable experience in game security, financial fraud and back end operations. After leaving a top online poker site in 2013, Peter has consulted on projects in the online poker, casino and DFS industries. Peter came on board as a consultant for Virtue Poker to give direction on game security, operations and web admin design, as well pass on knowledge gained from playing over 1,000,000 hands of online poker. Peter currently oversees game security and works with the development team to further enhance the technical resources used by the operations team on a daily basis.

Catalin Dragu, Design: Catalin has been a digital designer since 2010. Now he's working together with ConsenSys, creating fresh and engaging DApps. He believes that good design gives you a

good spirit. And does his best trying to create a beautiful experience for the users so that they can enjoy it like a walk in the park.

Marlon Violette, UI Game Design: Passionate about the arts, Marlon graduated with a degree in Illustration. Book covers, video games and caricatures was his interest but now designing for the web has been the name of the game.

7.2 Advisors

Joe Lubin: Joe Lubin's career has involved various posts in the fields of technology and finance and in their intersection. Subsequent to graduating cum laude with a degree in Electrical Engineering and Computer Science from Princeton, he worked as research staff in the Robotics Lab at Princeton and then at Vision Applications, Inc. Software engineering, finance and cryptography were central during employment with Goldman Sachs, eMagine's consulting work on the IdenTrust project, and the founding and operation of a set of hedge funds run with a partner. Joseph co-founded the Ethereum Project, and has been working on Ethereum and more recently ConsenSys since January 2014.

James Slazas: James Slazas has over 15 years of experience in the financial industry. At Lehman Brothers, James managed a proprietary arbitrage book of derivatives and created a global risk management group for the HNW exposure of the London, Swiss and Hong Kong banks. Later James co-founded a hedge fund managing a portfolio of life settlements, uniquely acquiring assets as contributions as well as pricing assets from both the VBT mortality tables, as well as, underwriting internally to determine longevity risk. Utilizing the health care components of the fund, James successfully negotiated a preferred status from the Centers for Medicare and Medicaid's Regional Extension Centers of AZ, CA, FL, NJ, and NY to rollout Med A-Z/Healthcare Inside's nationwide electronic health record (EHR) and billing services as well as a joint binding agreement with HCL America, a '$6 billion publicly traded company to provide patient support analytics and medical billing services to laboratories, ACO's, private practices, and hospitals.

Patrick Berarducci: Pat is Associate General Counsel for ConsenSys and a full-stack software engineer. Before joining ConsenSys, Pat practiced law for 7 years at Sullivan & Cromwell LLP and co-founded a health-tech startup. Pat is particularly interested in leveraging his legal, software and entrepreneurial experience in conjunction with blockchain technology to disrupt industries, markets and networks.

Andrew Keys: Andrew is the Head of Global Business Development for ConsenSys with capital markets, technology, and entrepreneurial experience. Previously, Andrew worked for UBS investment bank in equities analysis. Later, he was responsible for creation and distribution of life settlement products to hedge funds and investment banks. After, he co-founded a revenue cycle management company where he learned about Bitcoin and eventually Ethereum.

Andrew drives strategic technological partnerships, business development, and communications for ConsenSys and Co-founded ConsenSys Enterprise, to create Ethereum blockchain solutions for Fortune 500 clientele.

7.3 Legal Partners

Ifrah Law PLLC, US Gaming Matters: Ifrah Law has represented iGaming clients since the inception of the industry, and now represents many of the largest iGaming companies and industry associations around the world. They have been at the center of most of the important prosecutions and lawsuits in the iGaming industry: our clients include the online poker sites Full Tilt Poker and PokerStars, for whom Jeff Ifrah negotiated a historic agreement in 2011 with the Department of Justice which paved the way for iGaming in the United States. Ifrah Law was also instrumental in the creation of the legislative and regulatory frameworks in the three states which currently permit online gaming: Delaware, New Jersey and Nevada.

ISOLAS LLP, Gibraltar Law: ISOLAS is a full service Gibraltar law firm and advises on the full range of legal solutions Gibraltar has to offer. An award winning law firm, ranked by the world's leading directories as a leading firm in Gibraltar, their focus remains solidly on the client and delivering solutions. Trusted since 1892, ISOLAS LLP is this year celebrating 125 years in Gibraltar, the longest established law firm in Gibraltar.

8. Appendix: Virtue Poker Architecture

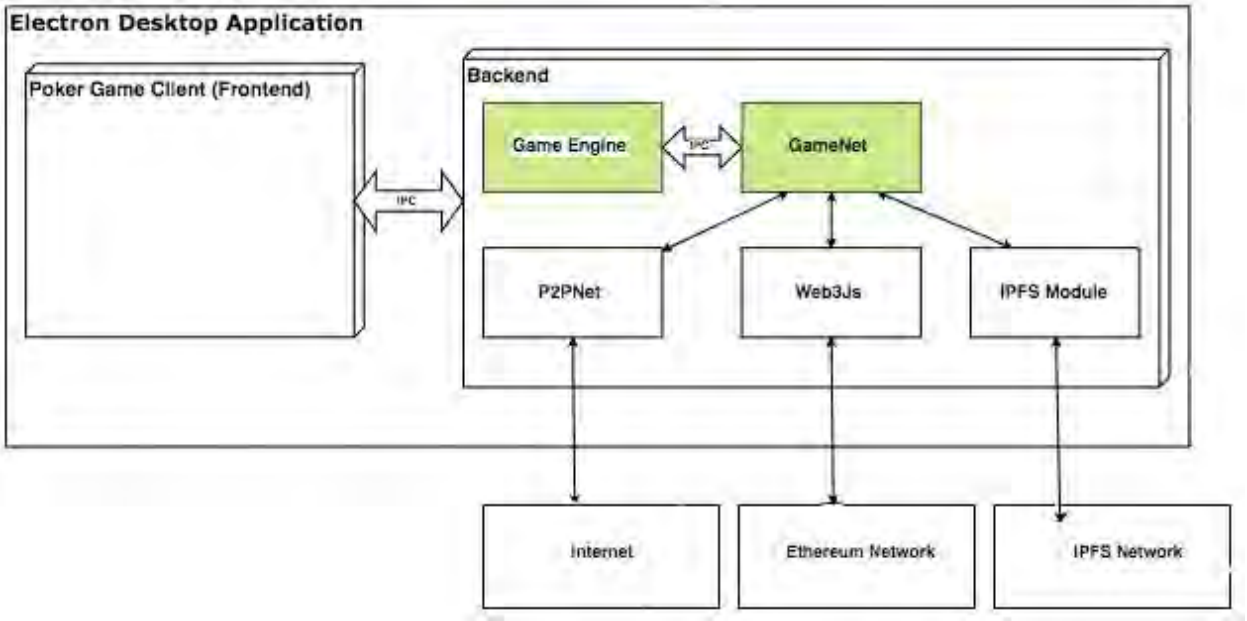
Virtue Poker is still under heavy development, parts in this section are subject to change.

8.1 System Architecture

Virtue Poker aims to be a fully decentralized poker platform. Virtue Poker achieves this goal by using new technologies like Ethereum and IPFS along with other solutions.

The Virtue Poker desktop app is an electron desktop application which includes the game engine, the poker game client and the network infrastructure to allow for communications with the Ethereum blockchain as well as a peer-to-peer subnet for game instances to use for the lower-latency messaging required for human gameplay.

Figure 12: Application Architecture



8.1.1 Components

The major components of the electron desktop application are:

- **Game Engine:** Contains the poker game logic.
- **Ethereum:** Uses as a repository for game parameters, escrow service, results reporting, player management across multiple tables, and Justice Management
- **GameNet:** Provides a single component the engine can use to communicate with the outside world
- **P2PNet:** Used by GameNet to manage a game-instance-specific p2p subnet

- **Web3.js:** The Ethereum compatible JavaScript API which implements that communicates with the Ethereum nodes (https://github.com/ethereum/web3.js/)
- **Electron Desktop Application:** Cross platform framework
- **Poker Game Client:** The poker game client that will be used by the users to play the game. This is an HTML5 web application written with the React Ecosystem.
- **IPFS Client:** Interfaces with the IPFS network to store game records. Users have the option of running their own IPFS node or connecting to the default Infura node.

8.2 Game Engine

8.2.1 State Machine

The game engine is the core of our application, it is the one who “makes the game go”. Our game engine is a finite-state machine that controls the transitions within the game state and implements the game rules. Depending on user interactions with the application and the network responses, the game engine will trigger actions and will move to the next state.

8.2.2: Connected or Offline State

Virtue Poker runs through the following process when a user logs into the application:

1. The application is not connected, so we are in an offline state.
2. The user inputs login details and perform a login.
3. The game engine will receive the inputs and triggers the action to perform the login.
4. After the login is done, the game engine will move to the next action and notify the Game UI.
5. If the login is successful we will move to a connected state.
6. If the login has an error we will keep the user in an offline state.

8.2.3: Lobby States

Our game engine states are classified in two groups:

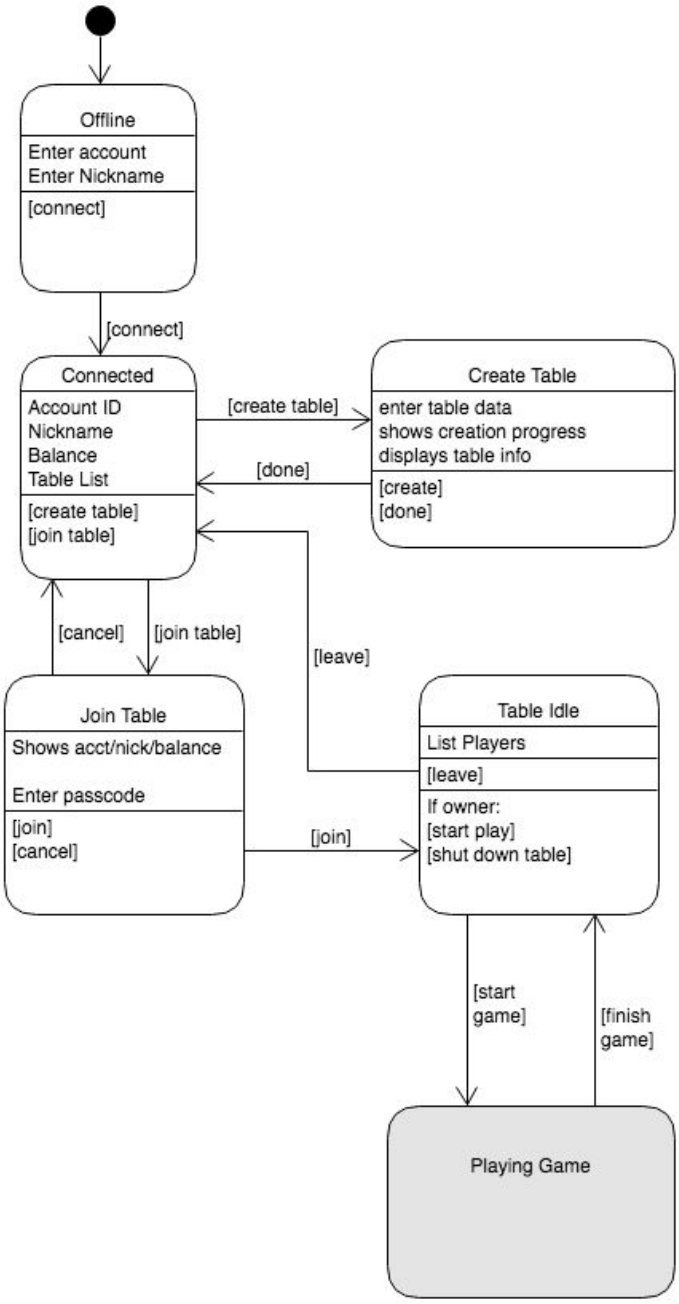
- **In play game states:** The game states when there is a game in play. We will call them “Game Play States”.
- **Not in play games states:** Any other actions that are not during a game play. We will call them “Lobby States”

Lobby States include:

- **Offline:** The user is not logged into the application. The user should login to move to a next step.
- **Connected:** The user has login and can do the following actions: create a table or join a table.
- **Create a Table:** The user is creating a table and should input the table information.
- **Join Table:** The user selects a table and joins that table.

- **Table Idle:** The user is waiting for other members to join the table so the game can start.

Figure 13: Lobby States



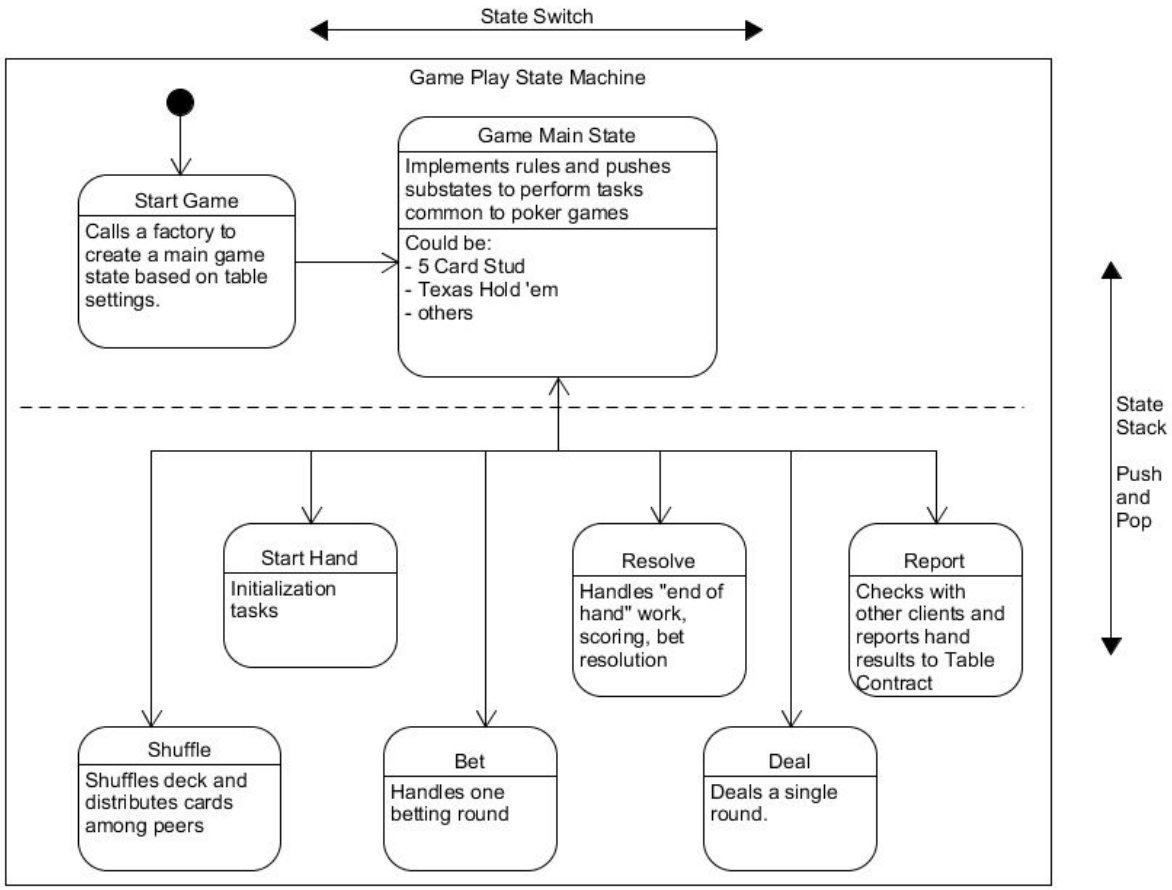
8.2.4: Game Play States

In play game states include:

- **On Deck:** The player is waiting for the hand to start.
- **Start Hand:** The hand starts when it is agreed who is playing the hand.

- **Shuffle:** In this state, the deck is shuffled and encrypted during the process.
- **Deal:** We will have a number of dealing rounds depending on the poker game we are playing. For example, in Texas Hold'em, we will have: pre-flop, flop, turn and river.
- **Bet:** It is the moment of betting. The player will decide if he wants to check, bet, fold or raise depending on the moment of the game.
- **Check Deal:** The game engine is checking with the rules of the game if we still need to do another deal or we have finished with all the card deals.
- **Showdown:** It is the moment where the player decides to reveal or muck their hole cards.
- **Resolve:** The results of the hand are shown in this state.
- **Report:** The hand results are sent to the game/table contract and the winner(s) will receive the pot.

Figure 14: Gameplay States



8.3 Ethereum Table Contract

Playing a game of poker solely on the Ethereum blockchain proves to be exceedingly costly in terms of the amount of gas required to deploy and interact with the smart contract. In order to make game play feasible, the contract was designed to manage players and verify the results of each hand, leaving the game logic to be handled off chain.

8.3.1 Functions

VirtuePokerTable

- Description: Initializes the poker table with the provided parameters.

Join_table

- Description: Joins a table, creates a Player struct with the provided parameters, and returns an error message, if any.

Get_player_seat

- Description: Returns the seat number of the user who sent the message or -1 if user does not have a seat.

Get_player_p2pid

- Description: Returns the p2pid for the player specified by the seat number or an empty string.

Hand_results_hash

- Description: Computes a sha3 hash of the parameters provided by the user.

Recover_sig_addr

- Description: Returns address associated with the key pair used to sign the hash.

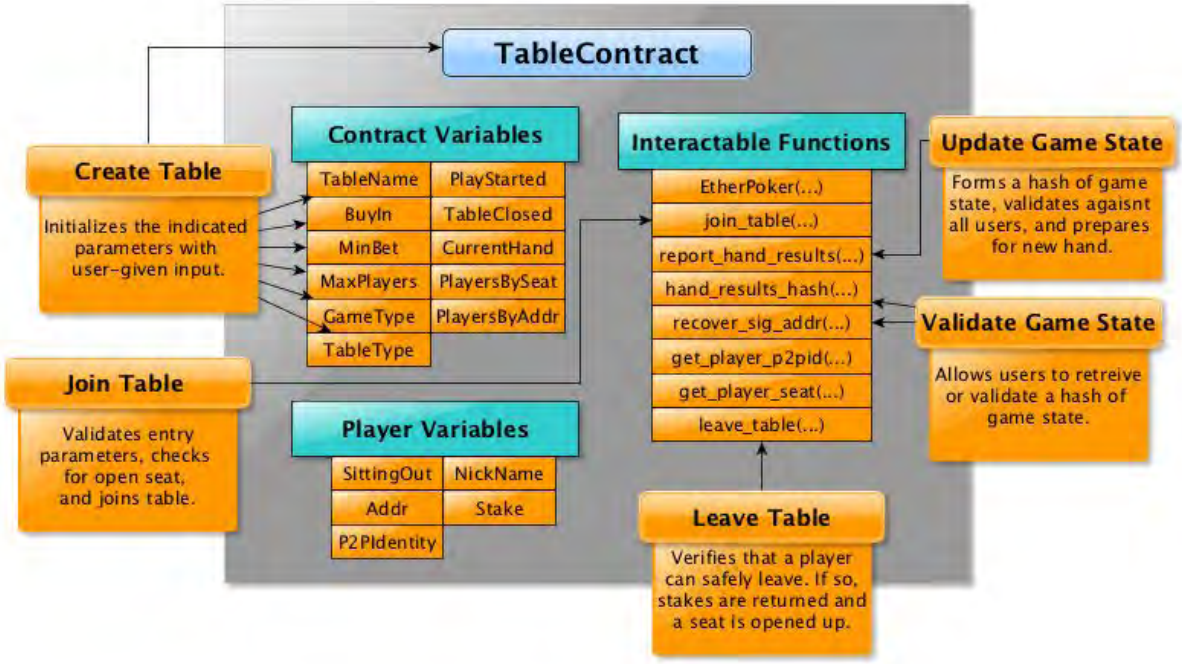
Report_hand_results

- Description: Verifies that all players have signed the game data and returns an error message, if any.

Leave_table

- Description: Unseats the player and sends back the player's earnings.

Figure 15: Table Contract Variables



8.4 GameNet

The GameNet provides the interface for the communication of our application. We have two main communication flows:

- Communication with other players, using the P2PNet.
- Communication with the Ethereum Network, using Web3.js

Joining a poker table is an example of when a user interacts with the Ethereum network. When the user joins to a poker table, he is buying into the table and sending his funds from his wallet. Another important part of GameNet is the module responsible for storing your funds in a private and secure way: the keystore.

8.4.1 KeyStore

A Wallet that stores your funds is represented by a key pair of a public and a private key:

- The public key is the public address that is used for receive funds.
- The private key is the one that is used for send funds.

The funds are sent in a transaction, and the transaction is signed by the private key. It is important to mention that your funds are as secure as your private key is, as if anyone has access to your private key, he will have access to all your funds.

Our key store uses the same key derivation functions (Scrypt), symmetric ciphers (AES-128-CTR), and message authentication codes as geth, the official Go implementation of the Ethereum protocol.

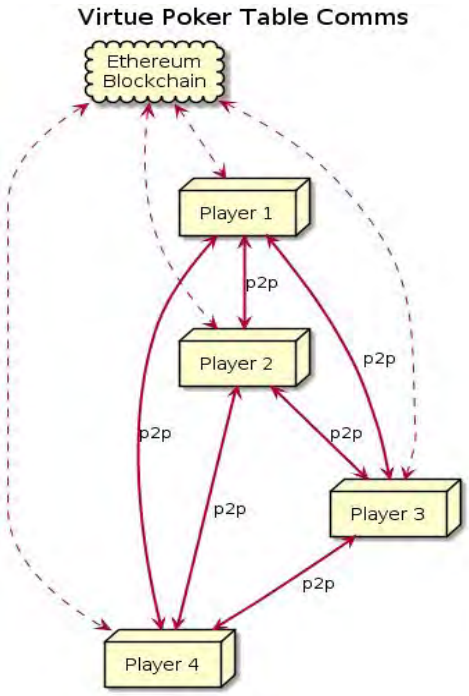
Your keys will be stored in your hard drive and will be secured by a password that you will need to use when you play on Virtue Poker.

8.5 P2PNet

The P2PNet is responsible for all the communication of the game that are done between the users without using the Ethereum Network. In DApps context, this is known as “off-chain”. Ethereum Network resources are used across all the DApps so we do need to be as efficient as possible in our DApps, and all transactions to the Ethereum Network have a gas cost. We are working to minimize the size of our contracts to limit the gas cost, and limit communications to the Ethereum blockchain to reduce operational costs and improve gameplay speed.

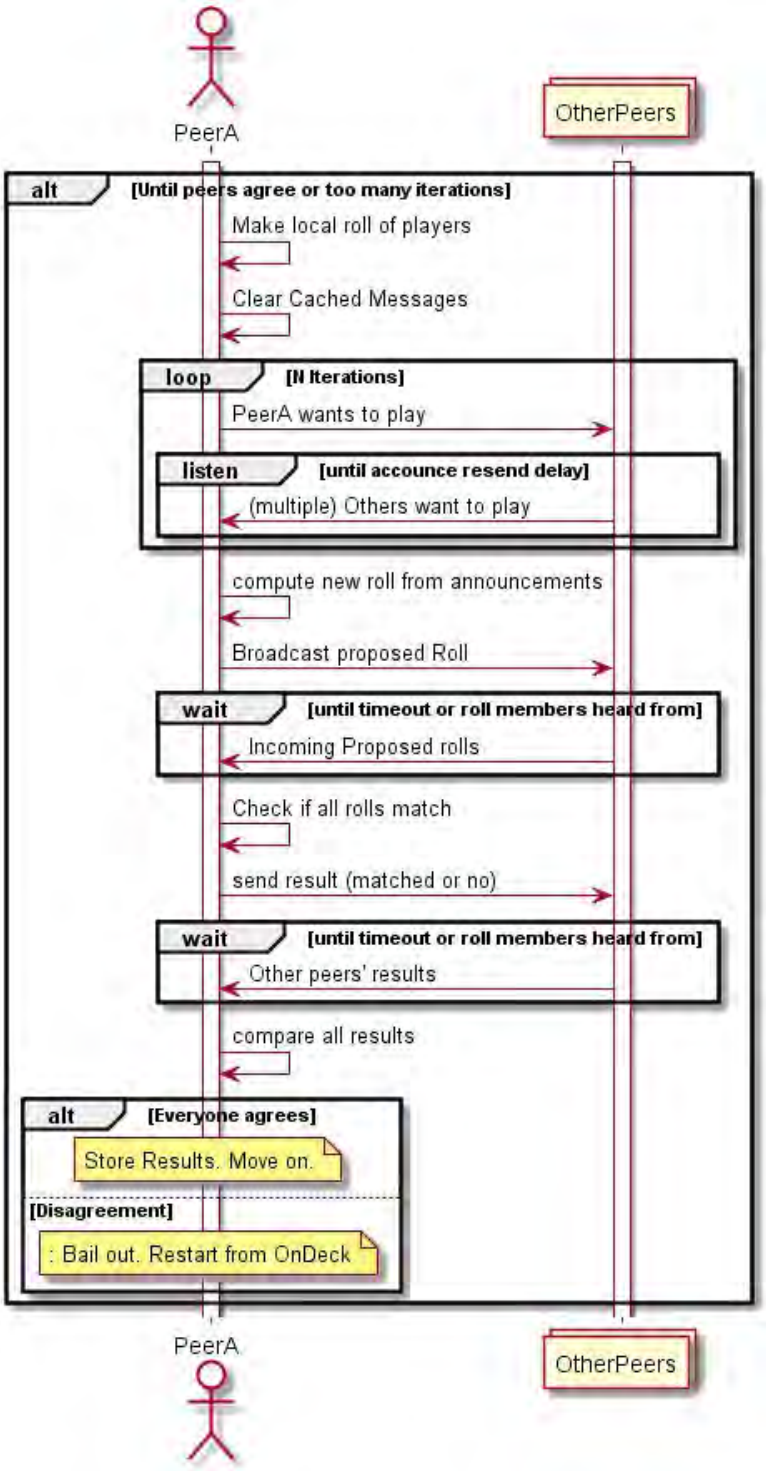
Our P2PNet is not using state channels as they are defined but at some level everything (except chat) carried by P2PNet is part of a "state subnet" where all of the game clients are agreeing off-chain with one another as to what has happened - and in a way where the blockchain can verify that they agreed - but can't actually go back and replay each individual "move".

Figure 16: P2P Communications



At the start of each hand, players at a given table all simultaneously begin a “roll-call” to check for messages from each of the other players seated, and they all come to agreement about who will be included in the next hand. Figure 17 illustrates this process:

Figure 17: "Roll Call"



8.6 Web3.js

Web3.js is the Ethereum compatible JavaScript API which implements the Generic JSON RPC spec. Web3.js is a official library created by the Ethereum Team. We are using Web3.js to:

- **Compile a contract**: Our contracts are precompiled and tested properly before compiling them with Web3.js. Compile a contract is required before deploying a contract using web3.js
- **Deploy a contract**: Web3Js provide and easy and secure javascript API for deploy a contract.
- **Contract call**: After a contract is deployed, any interaction with the contract is a call to the contract that is also done using web3.js interface.
- **Transactions**: Any other actions that involve access to the Ethereum Network will be always done using Web.js

8.7 Electron

Our desktop application is based in Electron. Electron is an open source framework, created by Github, for creating native applications with web technologies like JavaScript, HTML, and CSS.
We have chosen electron because:

1. **It is a cross platform framework**: Code once and you have a product that can work in multiple platforms: windows, mac and linux.
2. **It is based in web technologies**: We can build our application with the same technologies that are used to build websites without the need of hiring developers for specific platforms.
3. **Improve development cost**: The Virtue Poker team wants to use our resources in the most effective way. Our team can reduce development costs by hiring talented developers who don't necessarily need to have specific platform expertise.
4. **Improve development velocity**: As we don't need to hire developers for coding in specific platforms, all our resources will be focused in the development of one product that will work in multiple platforms using Electron
5. **There is currently more than 300 applications** Electron has been used successfully in previous Ethereum-based projects including: Mist Ethereum Wallet, Atom, Visual Studio Code, and the Jaxx Wallet.

8.7.1 Electron Architecture

Electron architecture is based in:

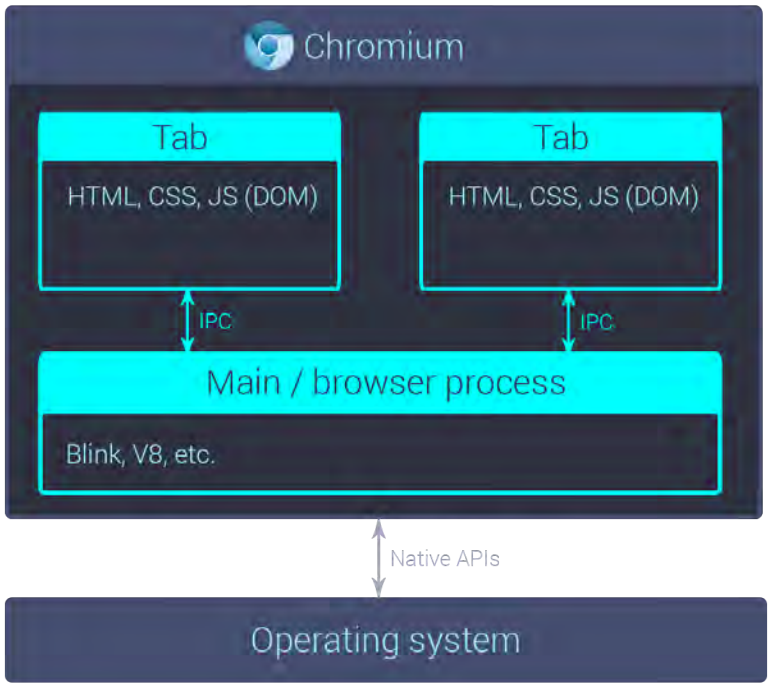
- **Chromium**: Chromium is the browser engine that is used by Google Chrome and Chrome Os. This allows us to build our application using web technologies.
- **NodeJs:** Node is a javascript engine build on top of Chrome/Chromium V8 javascript engine. Nodes provides access to the operative system resources (for example, the filesystem).

Every new version of Electron provides the latest version of Chromium and NodeJS. The latest version of Electron when this document has been written is Electron 1.6.11 that contains:

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

For more details on electron you can check: https://electron.atom.io/

Figure 18: Chromium

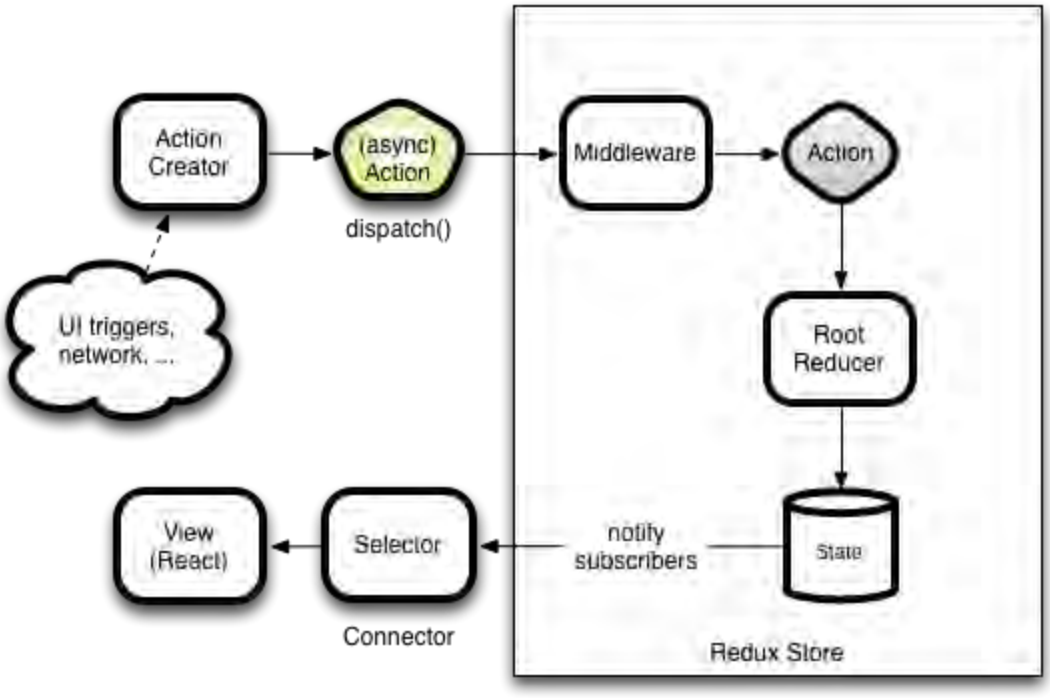


8.8 Poker Game Client

8.8.1 Game Client Architecture

We have decided to develop our game client using the React ecosystem. We have decided to use React-Redux architecture.

Figure 19: React



8.8.2 Game Play

The game UI will have two main components that will be displayed in different windows:
1. Lobby.
2. Table Game

When the user starts the game he will be in the lobby and will able to perform the below actions:

Login: The user will use his credentials to login into the application.
Create a game table: The user will be able to create a private (only private or also public) game table.
List all the available tables: The lobby will display all the available game tables that the users can join for play.
Join a game: The user will be able to join to a game table or a game tournament.
Wallet Management: The user will be able to manage his virtual poker wallet.
Play a game: The game table will be open in the table game ui component in a different window.
Play multiple games at the same time: The user will be able to join to multiple games at the same time.

8.9 Game Records and IPFS

The Interplanetary File System, or IPFS for short, is a peer-to-peer, distributed file system that allows for content to be stored and served in an efficient, fault-tolerant manner. Files stored on the

network are also content addressed, allowing for the creation of tamper-resistant data structures to be build on top of the file system.

Online poker platforms expose a variety of methods that allow players to collude and manipulate fair play of the game. While regulatory bodies require that game data is tracked and screened for malicious use, decentralized platforms introduce further complications in tracking records and authenticating data. To the end of transparency, Virtue Poker uses IPFS to store and distribute game records in a decentralized manner, ensuring that no single user is responsible for the integrity of the game data. Because IPFS files are content addressed (meaning that their hash-based identification comes from the contents of the file itself), any discrepancies between logs, that may have resulted from intentional or accidental changes, can be easily found by our Game Security Team.