VIRTUE POKER

Virtue Poker Whitepaper

A P2P Decentralized Poker Platform Built Using Ethereum

Draft Version 0.9

March 2018

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 white paper.

Table of Contents

Table of Contents

1. Abstract
    1.1 Value Propositions
        1.1.1 Eliminate Player Deposit Risk
        1.1.2 Solve the Lingering Trust Issue regarding Gameplay Fairness
        1.1.3 Reduce Player Costs and Create a Balanced Poker Ecosystem
        1.1.4 Build out an Extensible Decentralized Poker Network
    1.2 Short-Term Objective
    1.3 Long-Term Growth Strategy

2. Problems with Online Poker
    2.1 Introduction
    2.2 Misuse of Player Funds
        2.2.1 Absolute Bet and Ultimate Bet
        2.2.2 Full Tilt Poker
        2.2.3 Lock Poker
    2.3 Poker Bots
    2.4 Third-Party Tools and Software
    2.5 Unequal Rake
    2.6 The Broken Poker Economy
        2.6.2 The Problem
    2.7 Global Market Fragmentation
        2.7.1 Black Markets
        2.7.2 Dark Grey Markets
        2.7.3 Grey Markets
    2.8 Types of Operators
        2.8.1 Onshore Operators
        2.8.2 Offshore Operators
    2.9 Limited Competition
        2.9.1 Regulated B2C Market
        2.9.2 Unregulated B2C Market
    2.10 Random Number Generator Certification Practices
    2.11 Conclusion

3. The Virtue Solution
    3.1 User Flow

3.1.1 Download Virtue Poker Client
3.1.2 Registration
3.1.3 Fund a Wallet
3.1.4 Create a Game or Join a Game
3.1.5 Buy-In
3.1.6 Gameplay
3.1.7 Payout
3.2.1 uPort
3.2.2 Ethereum Smart Contracts
3.2.3 Game Client
3.2.4 P2P Messaging
3.2.5 IPFS
3.3 Identity Management
3.4 Ethereum Smart Contracts
3.4.1 Casino Contract
3.4.2 Table Contract
3.4.3 Player Interactions with Table Contracts
3.4.4 Multi-table Tournament Contract
3.4.5 Justice Management Contract
3.5 Mental Poker
3.5.1 Overview
3.5.2 Mental Poker Algorithm: The Two-Pass Shuffle
3.5.3 Two Rounds of Encryption: Shuffling the Deck and Indexing the Deck
3.6 Peer-to-Peer Messaging
3.6.1 P2P Messaging for Game Client Synchronization
3.6.2 Off-Chain Gameplay
3.7 IPFS: Game-log Storage of Hand Histories

4. Game Security
4.1 Forms of Cheating in Online Poker
4.1.1 Collusion
4.1.2 Multi-accounting
4.1.3 Data Mining
4.1.4 Poker Bots
4.1.5 Account Sharing
4.2 The Justice System to Combat Cheating
4.2.1 Core Functions of Justices
4.2.2.1 Dispute Resolution
4.2.2.2 Data Feed

4.2.2.3 Partial Storage of Player Encryption Keys

5. VPP: Virtue Player Points
    5.1 Becoming a Justice
        5.1.1 Justice Submissions Review Process
        5.1.2 Justice Fees
    5.2 In-Game Currency
    5.3 Special Tournaments

6. Roadmap
    6.1 Key Activities
        6.1.1 Platform Development
        6.1.2 Marketing
        6.1.3 Sponsorships and Public Relations
        6.1.4 Legal
    6.2 Development Roadmap
        6.2.1 Current State
        6.2.2 Further Development
        6.2.3 First Quarter 2018
        6.2.4 Second Quarter 2018
        6.2.5 Second-Third Quarters 2018
        6.2.6 Fourth Quarter 2018
        6.2.7 2019

7. Team
    7.1 Core Team
    7.2 Advisors
    7.4 Team Virtue Poker
    7.4 Legal Partners

8. Appendix: Virtue Poker Architecture
    8.1 System Architecture
        8.1.1 Components
    8.2 Game Engine
        8.2.1 State Machine
        8.2.2: Connected or Offline State
        8.2.3: Lobby States
        8.2.4: Game Play States
    8.3 Ethereum Table Contract
        8.3.1 Functions
    8.4 GameNet

8.4.1 KeyStore
8.5 P2PNet
8.6 Web3.js
8.7 Electron
8.8 Poker Game Client
8.8.1 Game Client Architecture
8.8.2 Game Play

1. Abstract

Online poker has grown from a handful of startups in the early 2000s to a multi-billion-dollar industry today. And since its inception, online poker has struggled with two critical issues: game fairness and security of player funds. These two issues were at the heart of a series of industry scandals that took down several leading companies in the online poker business.

Virtue Poker changes all that. It 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 enables 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

Virtue Poker's innovative peer-to-peer and decentralized architecture, coupled with the use of Ethereum, allows Virtue Poker to eliminate costly server and payment processing expenses. Most game functions that are typically performed on centralized servers are distributed in the Virtue Poker system, and player funds always remain in player wallets that are secured by *smart contracts*. Virtue Poker will pass these savings on to players via lower rake and player incentives, allowing more money to remain in the 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 and expect that new functionalities are built on top of the platform.

1.2 Short-Term Objective

Virtue Poker is building a production-ready application that will be deployed to the Ethereum mainnet. To accomplish this and to move the company towards launch, Virtue Poker will build out our development and marketing teams. The development team will focus on building out the user interface, distributed shuffle and blockchain technologies. The marketing team will create a series of pre-launch events, both live and online, to introduce the market to our innovative approach, and will build the marketing plan to launch Virtue Poker. Our launch strategy will consist of four stages: Alpha, Beta, Full-Scale Launch and Third-Party Integration.

1.3 Long-Term Growth Strategy

Our long-term strategy is comprised of two macro phases: (1) build out the technology and liquidity for the platform as a business-to-consumer (B2C) operator to prove the desirability, integrity and credibility of our solution and (2) expand globally through white-labeling to enable new licensees in markets across the globe. This allows third-party companies to seamlessly and inexpensively start their own blockchain-based online poker room using our core technology and provides an ongoing revenue stream.

2. Problems with Online Poker

2.1 Introduction

Online gambling has grown into a multi-billion industry expected to top $50 billion by 2021.[1] Poker has been at the heart of this phenomenal success. The growth of online poker rooms ignited following the televised World Series of Poker Main Event in 2003, in which an unknown amateur poker player, an accountant named Chris Moneymaker, won $2.5 million.

Today, the global online poker market is over $2.5 billion dollars. Globally, the 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 subjected to several scandals and has fallen victim to malicious users. While top poker sites such as PokerStars.com have adapted their platform to this problematic behavior, many sites have failed to adjust, creating a lingering distrust among many players.

2.2 Misuse of Player Funds

2.2.1 Absolute Bet and Ultimate Bet

After years of player complaints, Cereus Network, the third-largest poker network (operators of Ultimate Bet and Absolute Poker) admitted that a former employee had 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 and his co-conspirators stole tens of millions of dollars.[3]

2.2.2 Full Tilt Poker

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 forced those sites to stop offering real-money gameplay to US citizens. When Full Tilt reopened outside the US shortly thereafter, it was discovered they had a $360 million shortfall (that is, they had misappropriated $360 million in deposits from players). The company shut down operations shortly thereafter.[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 offered games to US residents, was shut down after failing to honor player withdrawals for nearly a year. Players lost an estimated $15-$24 million.[5]

2.3 Poker Bots

A poker bot is a software program that emulates real players online. Poker bots can sit across multiple tables, and can run without human oversight. Poker bots vary in complexity: they can be bought off-the-shelf, or can be custom-built and employed by an individual actor.

In 2015, a bot ring on PokerStars won nearly $1.5 million in $0.50/$1.00 and $1/$2 cash games.[6] There are companies such as WarBot that sell bots off-the-shelf to users who can run them on all platforms.[7] Publicly traded companies such as 888 Holdings have largely ineffective security procedures to protect players against bots. 888 even has a blog post entitled "How to Play Against Poker Bots," calling them "weak[8]."

But bots are, in fact, a real threat. In 2017, Carnegie-Mellon University ran a competition called "Brains vs Artificial Intelligence: Upping the Ante," in which 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, poker bots of all types pose a significant threat to the future success of the industry.

2.4 Third-Party Tools and Software

Many online players use third-party tools and software that target recreational players.[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 games and Sit & Go tournaments, 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

---

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

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

These tools are designed to give players access to information about their opponents. Unfortunately, these tools create a disadvantage for recreational players that are not using these programs, who are unknowingly targeted by highly-skilled professionals.

2.5 Unequal Rake

Rake is collected in tournaments or cash games. For tournaments, a percentage, typically 6-10%, is added to the buy-in. In cash games, a percentage is taken from each hand. Cash game rake online is typically 3-5% with a cap between $0.30-$5 per hand, depending on the limits being played. 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

Note that the cap on the lowest stakes ($0.01/$0.02) for a 5+ person game is 15x the big blind, but for a $3/$6 game, the cap is 0.58x the big blind.

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

According to a 2011 research study by the University of Hamburg, which analyzed over 2.5 million hands over a six-month period on PokerStars and other sites, each player at $0.01/$0.02 pays an average of 12.5 BB (big blinds) per 100 hands in rake, while those at $3/$6 pay 2.58 BB per 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 hands is excellent by online poker standards. With the current rake structures, most winning players become losing players when playing at low limits, 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:

$$\text{Deposits} > (\text{Rake} + \text{Withdrawals})$$

This model requires a constant supply of deposits to survive. Professional players have a net positive on withdrawals (that is, they win more than they lose, and withdraw it), while recreational players generally have a net negative, creating a balanced ecosystem.

2.6.2 The Problem

Unfortunately, winning players (typically semi-professionals and professionals) win at a higher rate than losing players deposit, 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

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

disproportionate rake, third-party tools that track and hunt less seasoned players, and distrust among recreational players regarding the integrity of online poker.

2.7 Global Market Fragmentation

Regulations restrict operators' 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 license or multiple licenses, or all markets with a single or no license. These can be classified as *onshore* operators and *offshore* operators.

2.8.1 Onshore Operators

Regulated operators have obtained at least one gaming license from a recognized gaming authority and operate typically in most grey and dark-grey markets. These operators typically adhere to anti-money laundering (AML), Know Your Customer (KYC), tax and other compliance policies, and many are publicly traded companies on various exchanges around the globe. Onshore operators include The Stars Group (PokerStars, Full Tilt Poker) William Hill Online, Playtech (iPoker network), GVC Holdings (PartyPoker, bwin.party), 888 Holdings, Unibet, Winamax and others.

2.8.2 Offshore Operators

Unregulated operators typically reside in offshore jurisdictions in Costa Rica, Curacao, Cyprus or on Indian reservations. They typically offer their services 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) and many others.

Many 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. 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 over $850 million in annual revenue and roughly 60% of global online traffic. They operate in nearly every country in the world (including 30 blacklisted markets), and have the largest cash prizes and tournaments. They have hosted the world's largest online poker tournament (253,000 entries), and have given away the largest prize pool ($8 million). They have dealt over 145 billion hands of poker, and sponsor top poker professionals and live tours. 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 playing on PokerStars: (1) Their services are costly to players as a result of high rake structures and (2) competition on PokerStars is considerably more skilled than on other platforms. And due to their market-leading position, they are able to operate with minimal pushback from players, enabling them to scale back or 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 is dominated by Winning Poker Network (America's Cardroom) and newly rebranded 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 stiff competition on regulated platforms. Yet the lack of due diligence and reporting requirements leaves players with minimal recourse should these sites go offline, lock players out of their accounts or be accused of wrongdoing.

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 Random Number Generator (RNG) of the operator is operating properly. Nearly every online operator has their RNG certified by a pre-approved third party. RNG testing companies include iTech Labs (itechlabs.com) and Gaming Laboratories International (gaminglabs.com).

Unfortunately, even with RNG testing, there is a surprising lack of oversight after an operator receives their certification. 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."[13] 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 license's 5 year lifespan."[14] This lack of oversight has contributed to a prevalent belief among online poker players that the games 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.

[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. The Virtue Solution

Virtue Poker has spent years researching the market dynamics of the online poker industry. Our goal is to reinvigorate online poker by creating a decentralized online poker network with trust, transparency and accountability built-in. We will accomplish this through the utilization of the Ethereum blockchain, peer-to-peer networking, user-owned identity and cryptographically secured cards, which allow us to present an improved playing experience at a lower cost to players. More importantly, using these new frameworks, we aim to fix the struggling poker economy by reducing costs to players via lower rake, building out rakeback structures that encourage player retention and creating the industry's most safe and secure online poker platform.

3.1 User Flow

Virtue Poker is a serverless application that runs without storing customer funds, and involves all players in card shuffling. The user flow is:

3.1.1 Download Virtue Poker Client

The user visits www.virtue.poker and downloads a Windows, Mac or Linux client. The application includes a shuffler, game engine and user interface.

3.1.2 Registration

The user then creates a uPort (uport.me) identity (if they haven't already created one). The user then digitally signs an attestation regarding country of residence and age.

3.1.3 Fund a Wallet

The user is 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 can then go to our lobby which will show all publicly available games or can create a private game and invite other players.

3.1.5 Buy-In

The user can join either a public or private game by sending Ether (ETH) or Virtue Player Points (VPP) to the table address of the game they want to join. The smart contract sits on the Ethereum blockchain and acts as an escrow account while the game is in progress. Each game is represented by a table contract that contains the custom parameters of that particular game.

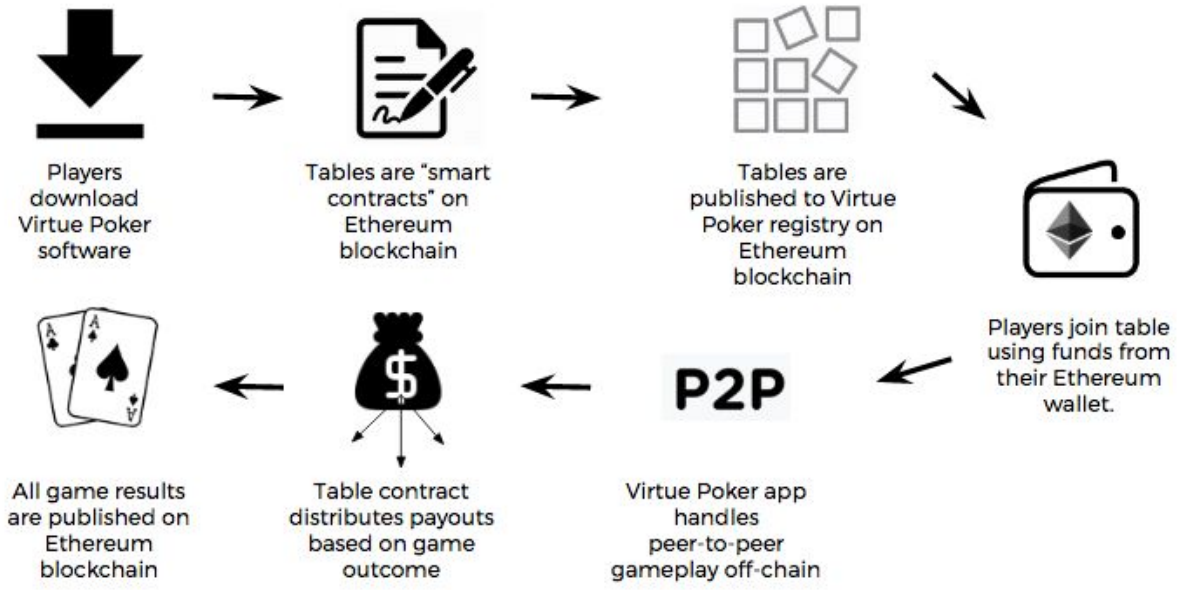
3.1.6 Gameplay

The peers at the table form a P2P subnet and use a Mental Poker protocol that requires each individual peer to shuffle and encrypt the deck of cards.

3.1.7 Payout

When a tournament is completed, or when a player a cash game table, the table contract auto-executes and each player is paid their winnings (if due).

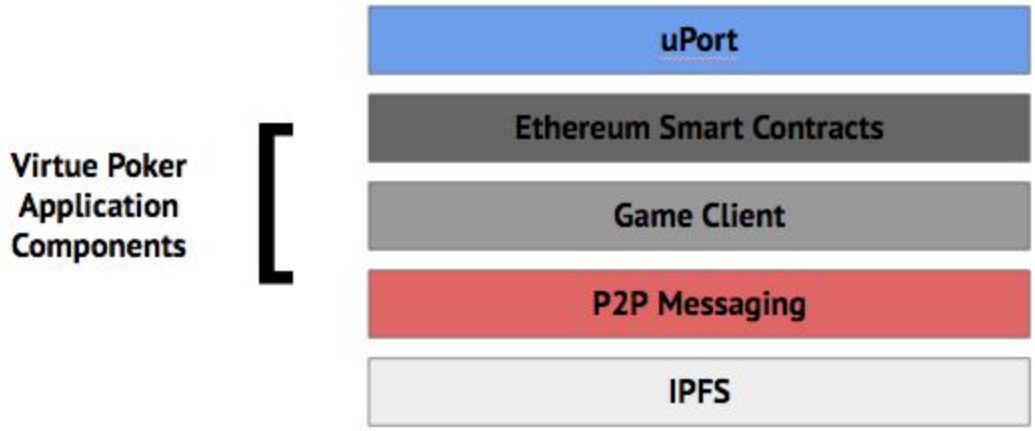
Figure 3: How Virtue Poker Works



3.2 Virtue Poker Components

The Virtue Poker platform utilizes several sub-components within the application:

Figure 4: Virtue Poker Components



3.2.1 uPort

The Ethereum-based self-sovereign identity application uPort is utilized as a registration and identity validation mechanism to prevent underage gambling and multi-accounting. Users are 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: (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 and (4) for reporting game results.

3.2.3 Game Client

The Game Client is a desktop application, 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

A 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.

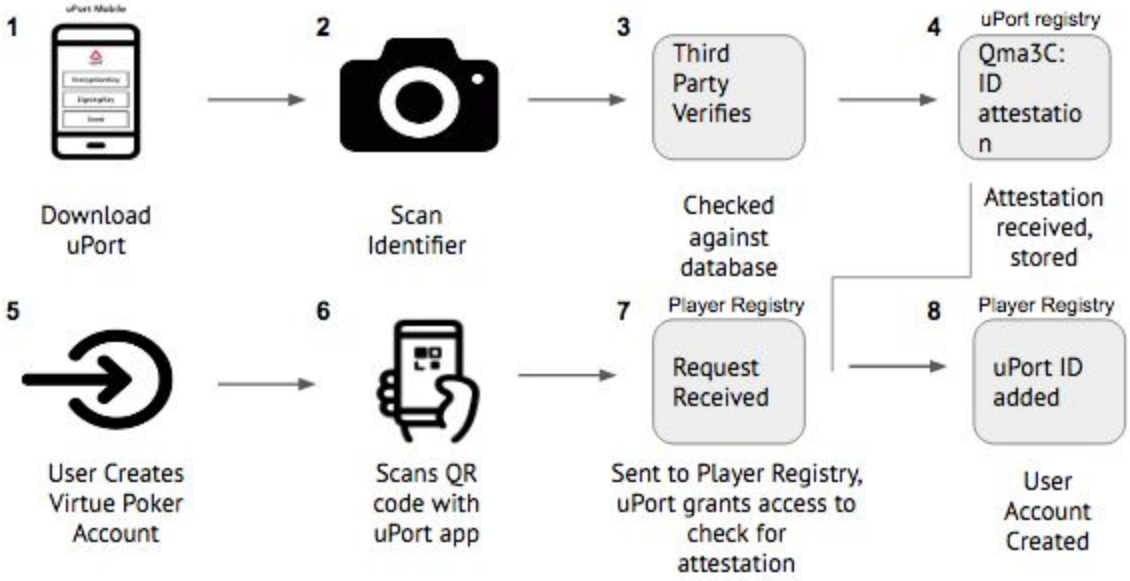
3.2.5 IPFS

The Interplanetary File System (IPFS) will be used to log hand histories for all games played on the platform. Logs can be retrieved for review either for compliance or for our game security team. This is also the component that supplies hand histories to the user.

3.3 Identity Management

Virtue Poker uses the self-sovereign identity application uPort to validate a player's identity prior to allowing access to the platform.[15] 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 creates an account on Virtue Poker and is presented with a QR code that the user scans with the 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.

3.4 Ethereum Smart Contracts

After a player has verified their identity and created their account, the user is brought to the Lobby, which is a casino smart contract.

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

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 front end, user and game management tasks.

3.4.2 Table Contract

A Table Contract represents a single instance of a game of 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, winnings are paid, the players leave and that table contract is closed. It is 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 and information about them needed by the other players. In addition, the table contract is where funds used for gameplay are escrowed, and is responsible for distributing winnings.

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

3.4.3 Player Interactions with Table Contracts

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 gas costs and improve gameplay speed.

The table contracts include a chip counter which keeps tracks of the players' stakes at each table. At the end of each hand, each player and the Justices (described in Section 4.2) cryptographically sign the results and send a transaction to the table contract which updates each player's stake accordingly. This consensus mechanism and transaction submission by the peers at each given table functions as an "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 on to the next hand while the 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. The Justice is externally incentivized (paid) to act as a trustworthy peer in the table subnet. A team of Justices is randomly assigned to each table, and they resolve disputes and log game data.

In order to distribute the workload and to prevent collusion between Justices and players, the Justices are assigned randomly to tables from a pool, and are rotated 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 poker tables. Justices are 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.[16] Over the years there have been numerous papers published on the subject, expanding upon the ideas, offering alternative methods and providing analysis and critique.

However, there have been very few practical software applications employing Mental Poker techniques. In large part, this is because the cryptography involved can require enormous amounts of computational power and communications resources, and software using them simply runs too slowly 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 these difficulties. The result is a downloadable application that can play a game at speed and manage real money player stakes using the Ethereum blockchain.

---

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

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 communication encryption: cards can be encrypted or decrypted in any order. The basic algorithm is outlined in Section 3.5.2.

3.5.2 Mental Poker Algorithm: The Two-Pass Shuffle

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 a Fisher-Yates shuffling algorithm,00 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 lock" 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 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[17]

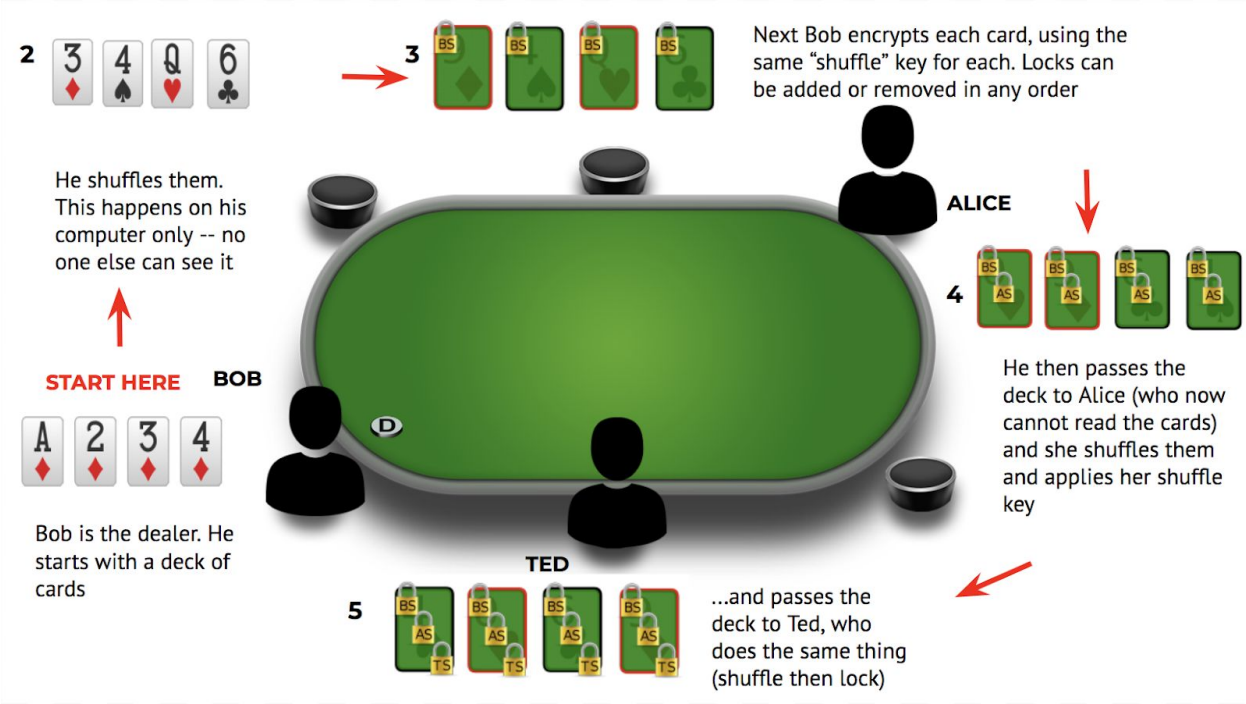
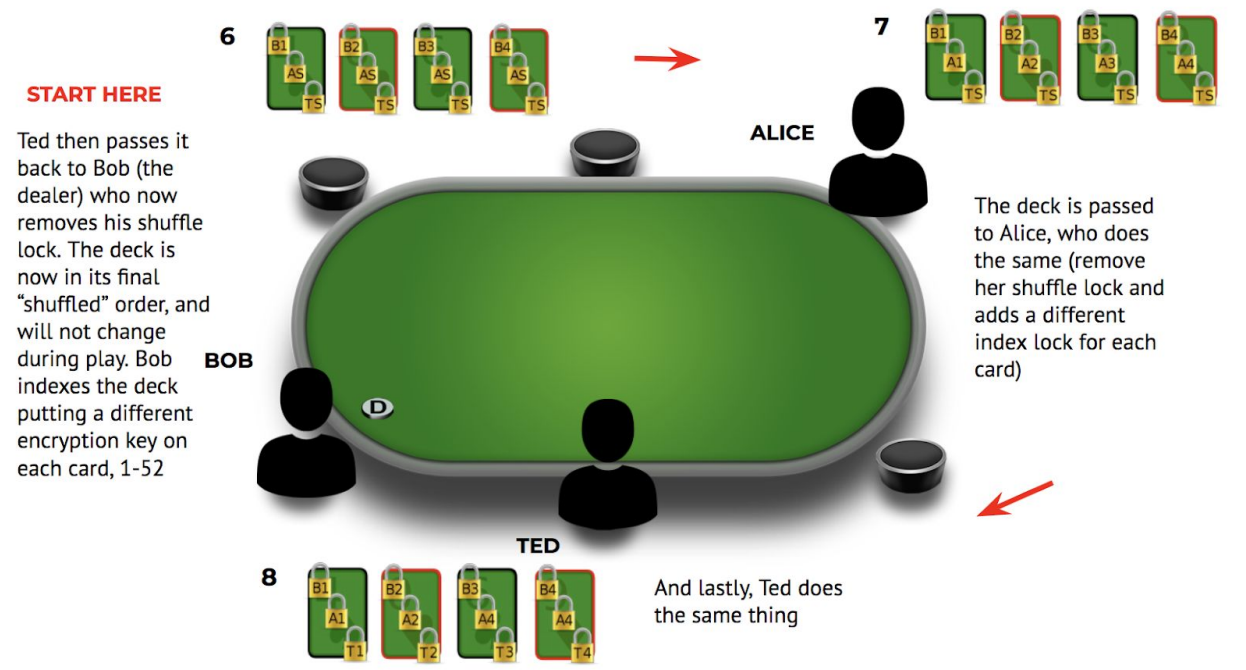


Figure 7: Indexing the Deck



[17] 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

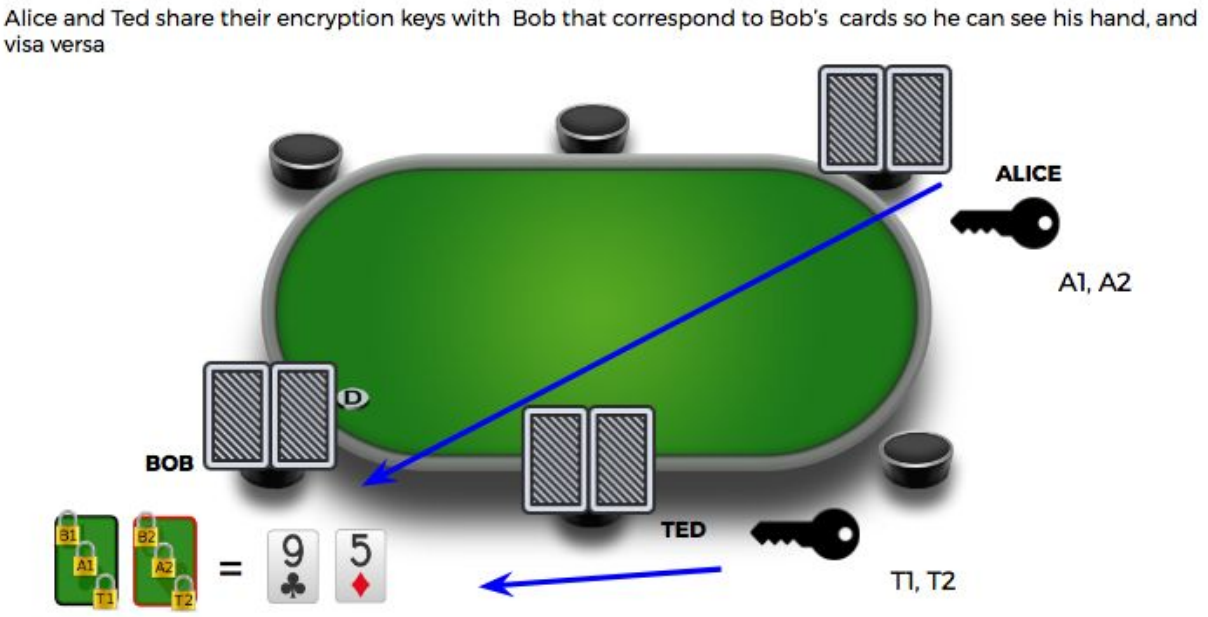


Figure 9: Community Cards[18]

[18] 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 front-end and back-end processes. The front end displays the current game state to the local user, accepts input when appropriate and passes it to the back end, which then broadcasts it to the other clients in the game. The back end contains the logic needed to apply the rules of poker to the input events that it receives both from the front end and from other clients. The result is that every client is 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 allows 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 Smart 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 resource-intensive, so simply sending all of this log data to the blockchain is not practical.

Fortunately, technologies like the Interplanetary File System (IPFS) 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 the most recent hash from the blockchain 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.

4. Game Security

4.1 Forms of Cheating in Online 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 strategies to create an advantage against other players.

4.1.2 Multi-accounting

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

4.1.3 Data Mining

Players sometimes share data about other players, including hand histories and player notes. This shared data is compiled to provide the player with otherwise-unknown information about other players.

4.1.4 Poker Bots

As described previously, poker bots are either off-the-shelf or customized software programs that can operate on poker tables without human oversight.

4.1.5 Account Sharing

Account sharing is 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 percentage rewards, such as rakeback, based on the amount of play and rake. 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.

4.2 The Justice System to Combat Cheating

Virtue has developed the Justice System to combat collusion and cheating. Justices are non-playing referees that are randomly assigned to poker tables. They provide security and protection to players on the Virtue Poker network and receive fees in exchange. 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. Justices are rotated automatically every few hands.
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:

4.2.2.1 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 resolves the dispute in real-time and awards the pot to the winner.

4.2.2.2 Data Feed

Each Justice submits each action of every hand to IPFS so hand histories can be stored. This is required by gaming regulatory bodies, and enables essential services such as collusion detection, bot detection and multi-accounting identification.

4.2.2.3 Partial Storage of Player Encryption Keys

The “Dropped Player Problem” of Mental Poker occurs when a player drops out of a hand prior to its completion. 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 out for any reason, 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

Virtue Player Points have three core utilities within the Virtue Poker network: (1) they can be used as an in-game currency, (2) they can be pledged in a smart contract called the Justice Registry that enable users to stake tokens and validate hands on the network in exchange for fees and (3) they can be used to access special tournaments.

5.1 Becoming a Justice

The Justice Pool is composed of a limited number of users that are active on the Virtue Poker network. To become a Justice, users must (a) acquire VPP, (b) stake tokens in the Justice Registry and (c) must have their computer on, the Virtue Poker application open and set to *active* in order to be assigned to tables.

5.1.1 Justice Submissions Review Process

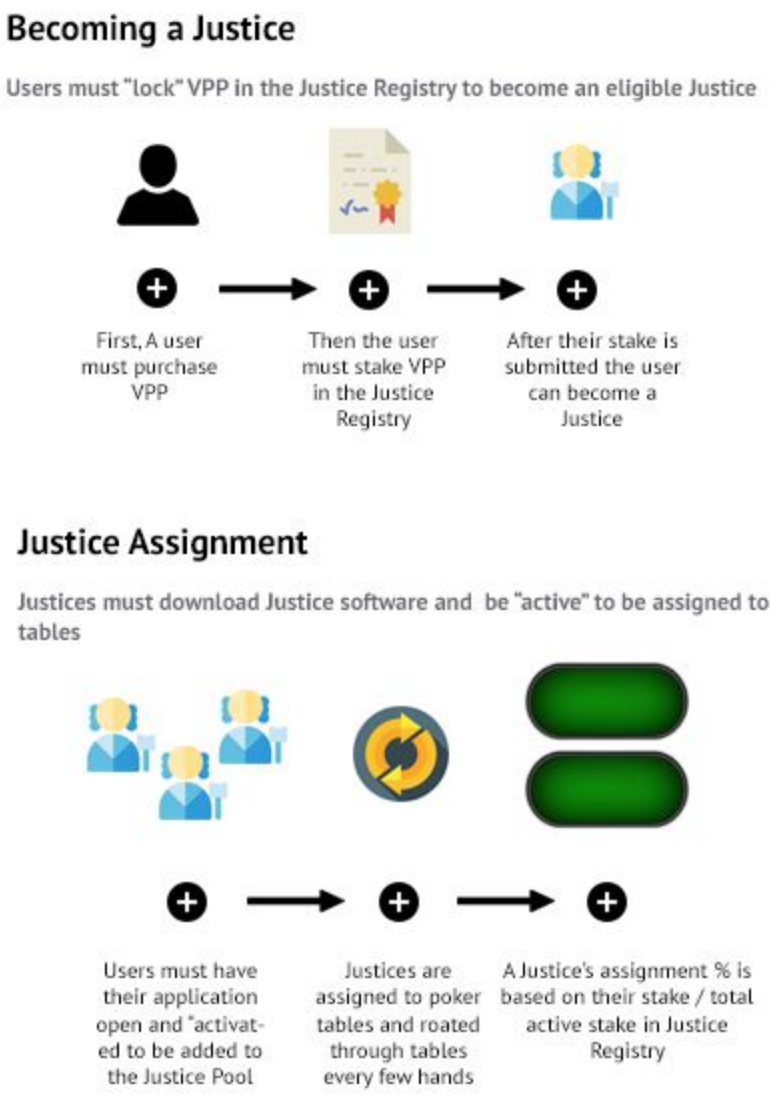
Initially, submissions by Justices to IPFS will be reviewed by a team of game security experts. The Virtue Poker team includes a game integrity and security expert who is assisting our development team in building the Justice System and setting up appropriate tracking software to detect red flags on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

There are two ways for accusations of cheating to be submitted to our Game Security team. Players can submit a complaint of suspicious activity, and these submissions are reviewed to determine if cheating has occurred. In addition, Virtue Poker constantly runs algorithms across the data submitted by Justices and all suspicious activity is reviewed manually. If it is found that a player cheated, a punishment is levied and that player may be banned from the platform permanently.

5.1.2 Justice Fees

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

Figure 10: Justice System

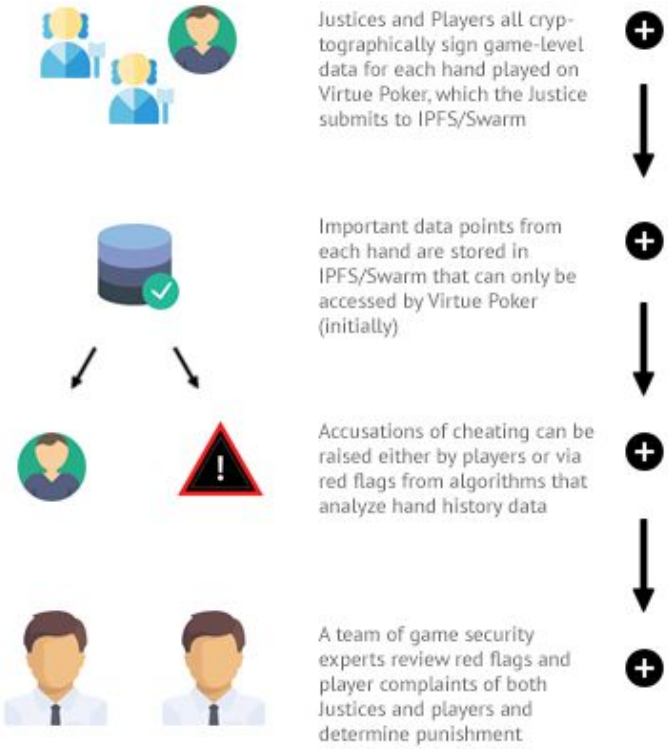


Justice Functions

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.

6. Roadmap

6.1 Key Activities

6.1.1 Platform Development

The Virtue Poker team has spent nearly three years developing our system, and will need to grow 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 who have 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.

6.1.3 Sponsorships and Public Relations

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 is consulting with respected gaming law firms including DLA Piper, ISOLAS and Ifrah Law, and with regulators around the globe. We will 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 that 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.

Our application 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 a 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. The game engine 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 games at a rate of 70-80 hands per hour, on par with existing online poker networks.

6.2.2 Further Development

Virtue Poker has hired our core team and will use internal funding 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.

Improve P2P Messaging Backbone
The application uses runtime-swappable plug-in 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 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 prior to the first round of user testing.

6.2.3 First Quarter 2018

Identity Management
Initially, the Virtue Poker team will integrate a third-party ID verification service (See https://www.hooyu.com/). As we continue to work with regulators around the globe, we will introduce them to self-sovereign identity solutions such as uPort. And our goal is to eventually move our log-in process to a decentralized solution.

Data Storage
Virtue Poker will use Justice nodes to collect and store gameplay at the hand level. We intend to store hand histories using IPFS, and to add a reference to the data in the table contract. Initially, we will use a centralized data storage mechanism for our Alpha.

6.2.4 Second Quarter 2018

Virtue Poker Private Alpha
Virtue Poker will conduct private user testing to debug our platform and to source feedback to improve upon our UI/UX. Participants in the Virtue Poker Token Offering (Phase 1) will be invited to join the Alpha program.

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.

6.2.5 Second-Third Quarters 2018

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

Build out Multi-Table Tournament Functionality
The Multi-Table Tournament Contract manages which tables are part of the tournament and what players are assigned to those tables. It also manages tournament progress and resolution: who wins, and what. During gameplay, the table is still the P2P subnet unit, and functions much as it currently does, but it communicates with the Multi-Table Tournament Contract.

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 tournaments and cash games.

6.2.6 Fourth Quarter 2018

Virtue Poker Public Launch Tournament
Virtue Poker will publicly launch via one or more large guaranteed tournaments, enabling users around the world to play on our platform.

6.2.7 2019

Third-Party Operator Integration
Virtue Poker will enable third-party operators and licensees around the globe to create custom skins on our platform and to create games on top of our infrastructure. This will allow us to scale up more quickly to a liquidity level that will be attractive to players.

7. Team

7.1 Core Team

Jim Berry, Lead Platform Developer: For the past 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 Technologies and Electronic Arts - among others - specializing in physical simulation and graphics.

Ryan Gittleson, Co-Founder: Ryan is an experienced business development and marketing professional with a background in helping businesses and products increase sales. Before working on Virtue Poker, Ryan was Head of Customer Acquisition for TodayTix, a Broadway ticketing mobile application, where he oversaw its user-base growth from 150,000 users to over 700,000. He discovered Ethereum in August 2015, and instantly became captivated by the global potential of blockchain technology. He has worked with ConsenSys on Virtue Poker for the past two years. Ryan holds a bachelor's degree from the University of Pennsylvania.

Dan Goldman, Chief Marketing Officer: Dan has more than 20 years of experience in marketing companies online. He was responsible for the rise of the world's largest online poker company, PokerStars, taking the company from a startup to over 100 million players. Before PokerStars, Dan headed marketing for one of the largest online shopping comparison sites, leading to its acquisition by Experian. He was part of the team that commercialized object-oriented programming, leading Digitalk from a startup to a leadership position with its Smalltalk/V programming language. Dan also oversaw the development and launch of a casino-based online gaming site for one of the United States' largest casinos.

Javier Franco Algarrada, Blockchain Development Team Lead: Javier is a senior software engineer with 10+ years of experience. He enjoys working on full stack applications involving multiple technologies and to be an active part in the full software development life cycle of the product. After leading other technicals projects, he has stepped up to lead the development of Virtue Poker.He has been working for more than 7 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.

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.

Jose Diaz, Head of Product: Jose has an entrepreneurial and innovative senior background with more than eighteen years of experience in the Gambling industry as CTO, Product Development Director, Software Developer and IT Manager. With an MBA and a high university degree in Computer Science he joined Virtue Poker as Head of Product, attracted by the innovative technology Virtue Poker uses. Jose's background includes track record of successful deliverance of high profile projects, defining new development strategies in new platforms, leading strong teams and managing relationships with key clients.

Colum Higgins, Senior Product Manager: Colum Higgins obtained a PhD in physics from CERN in the early 90's. He spent the next 10 years in technical roles in supercomputing, as an Enterprise middleware consultant and finally as a tech startup founder and CTO for 3 and a half years. In 2003 Colum completed an MBA and moved to China where he created a 3G demonstration system for Ericsson and worked on eGovrnment projects for regional governments and the European Union. In 2007 Colum joined Full Tilt Poker as a program manager and business analyst. At Full Tilt Poker Colum drove the requirements for flagship features including a game client rewrite, regulation in France, beginner's tables and tournament tickets.

Daniel Ortega, Back-End Developer: Daniel has been a software engineer for the last 12 years, having learned from and worked on a set of heterogeneous sectors, from the civil works world to the airlines niche, passing through the gambling domain. Daniel is always trying to push himself out of his comfort zone, and has constantly tried to work with the latest technologies across his career.

Alvaro Rodríguez Villalba, Front-End Developer: Alvaro is a full stack Javascript developer and Android developer. He co-founded a startup called Kultur where he was the web and Android developer, working for more than two years developing a web application for the simulation of satellite communication links, and created several JS-based platforms as a freelance developer. Alvaro is a 2017 graduate of the ConsenSys Academy program.

Lucas Cullen, Blockchain Platform Developer: Lucas is a full stack software and solidity developer, previously working for startups and banks has a background in mathematics. He first heard about Bitcoin in 2011, started mining soon after that, and has been talking about bitcoin to whoever will listen ever since. He has worked with Accenture and the Monetary Authority of Singapore on "Project Ubin," using JP Morgan's enterprise Ethereum product called Quorum. Previously, he ran his own software consultancy company, providing education and developing software for Bitcoin and blockchain projects. He runs the Bitcoin Brisbane meetup, is a board member of Blockchain Australian and is the Australian Coloured Coin Ambassador.

7.2 Advisors

Joseph Lubin: Joe Lubin's career has involved various posts in the fields of technology and finance and in their intersection. After graduating *cum laude* with degrees in Electrical Engineering and Computer Science from Princeton, he worked as research staff in the Robotics Lab at Princeton and then at Vision Applications. Software engineering, finance and cryptography were central during Joe's 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. Joe 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. James co-founded a hedge fund managing a portfolio of life settlements. 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 to provide patient support analytics and medical billing services to laboratories, ACOs, 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 seven 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 companies.

Robert Davidman: Most recently Robert served as interim Global CMO for ruby, overseeing marketing and digital strategy for ruby's innovative portfolio of brands, including Ashley Madison, Cougar Life and Established Men. Currently Robert leads US and global marketing strategy for a roster of leading brands as a partner at The Fearless Group in New York City, which he co-founded. Clients in the gaming industry include Bwin.Party (PartyPoker), Pala Interactive (Palacasino.com, PalaPoker.com, Palabingousa.com), 888 Holdings (888.com), Lottoland.com among a few. Since 2001 Robert has worked with several online gaming properties both as a marketer and operator

around the globe. Robert served as the head of International Broadcast Services for Yahoo! from 1999-2001 where he launched the web portal's streaming business outside the US and Canada in over 24 countries. Prior to Yahoo! from 1995-1999 Robert was the 9th employee at Broadcast.com leading all sales and marketing for the internet streaming pioneer.

7.4 Team Virtue Poker

Phil Ivey: Ivey is tied for second all-time with 10 World Series of Poker bracelets, and is ranked 6th all-time with over $23 million in live earnings. In addition, he is one of the top performing online players, with winnings over $10 million. He has exceled in all formats (tournament, live cash games, online cash games) and has been to a record 9 World Poker Tour Final Tables. Between 2002 and 2009, Ivey placed in the Top 25 on four separate occasions in the World Series Main Event, and was a unanimous inductee to the WSOP Hall of Fame this year.

Dan Colman: Best known for beating Daniel Negreanu and winning the $1,000,000 buy-in Big One for One Drop at the 2014 World Series of Poker. Dan has made over $28 million in live earnings in his career, sitting 3rd all-time.

Brian Rast: Brian Rast, known online as "tsarrast, is a 3-time World Series of Poker Bracelet winner, and is joining the team as an advisor to the company. Brian won the $1,500 Pot-Limit Hold'em event in 2011; and won the $50,000 Players Championship twice in 2011 and 2016, with heads-up victories against Phil Hellmuth and Justin Bonomo respectively. He ranks 10th all-time with over $20 million in live earnings over his career.

7.4 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, including 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, ISOLAS' 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

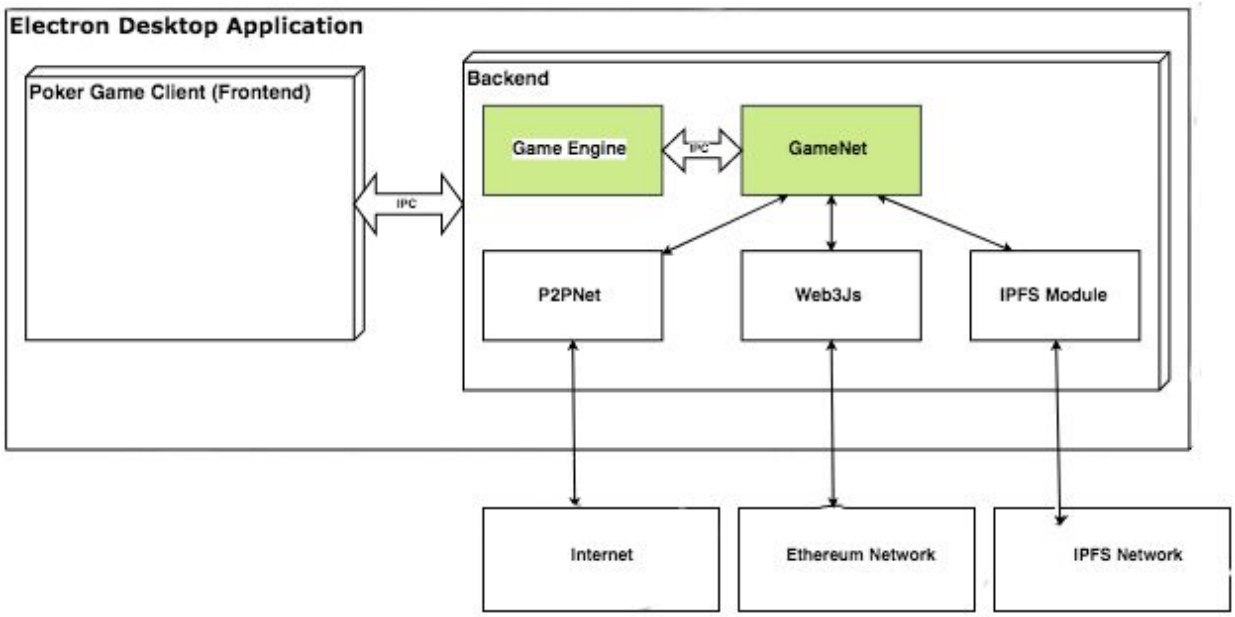
Virtue Poker is still in development. Parts of this section are subject to change.

8.1 System Architecture

Virtue Poker is 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 communicate 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 communication with the Ethereum nodes
- **Electron Desktop Application:** Cross platform framework
- **Poker Game Client:** The client that is used to play the game. This is an HTML5 web application written utilizing the React Ecosystem.
- **IPFS Client:** Interfaces with the IPFS network to store game records.

8.2 Game Engine

8.2.1 State Machine

The game engine is the core of our application, 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 triggers actions and moves to the next state.

8.2.2: Connected or Offline State

Virtue Poker executes 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 performs a login.
3. The game engine receives the inputs and triggers the action to perform the login.
4. After the login is done, the game engine moves to the next action and notifies the UI.
5. If the login is successful, we move to a connected state.
6. If the login fails, we keep the user in an offline state.

8.2.3: Lobby States

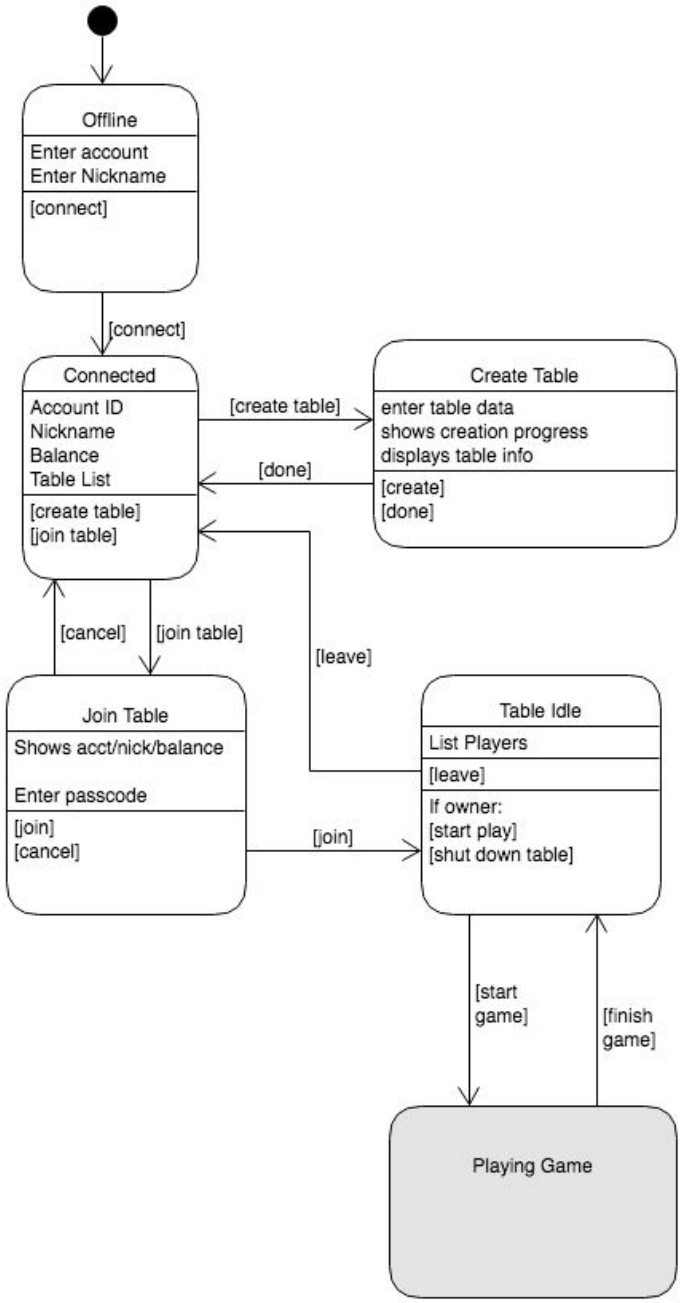
Our game engine states are classified in two groups:

- **Game Play States:** The game states when there is a game in play.
- **Lobby States:** Any states that occur other than during game play.

Lobby States include:

- **Offline:** The user is not logged in.
- **Connected:** The user has logged in and can create a table or join a table.
- **Create a Table:** The user is creating a table.
- **Join Table:** The user selects and joins a table.
- **Table Idle:** The user is waiting for other members to join the table so the game can start.

Figure 13: Lobby States



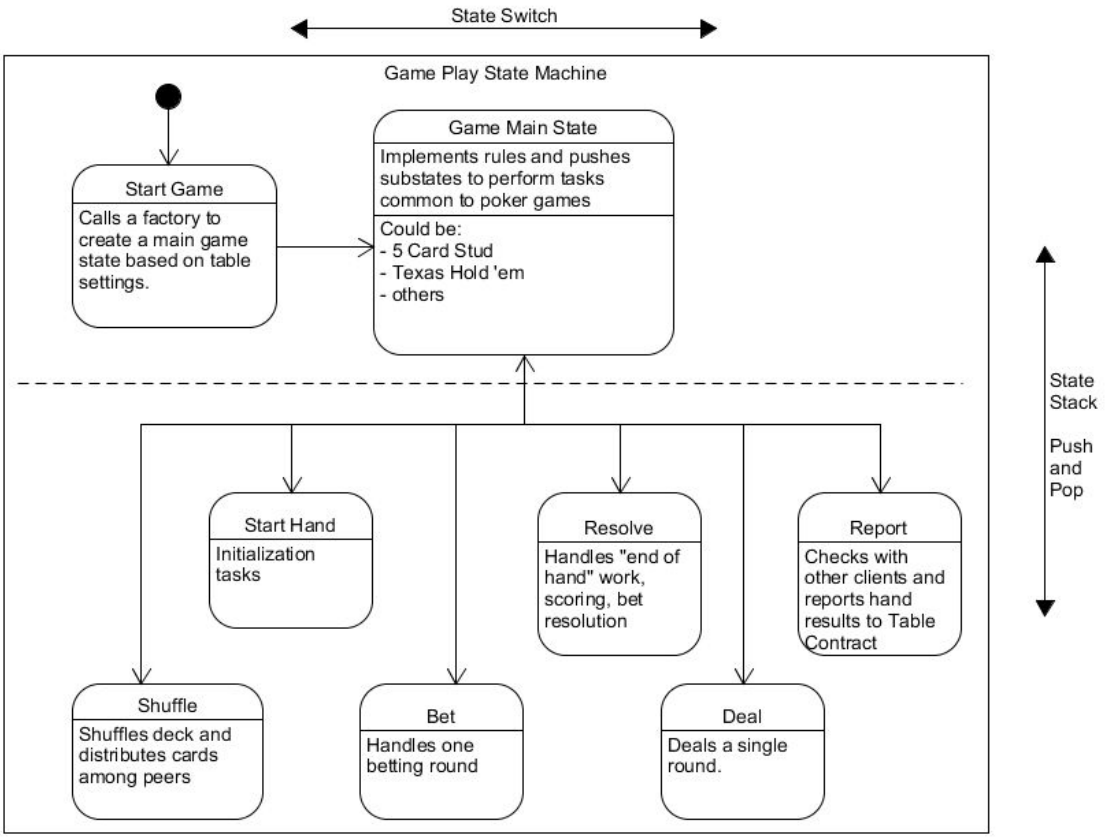
8.2.4: Game Play States

In play game states include:

- **On Deck:** The player is waiting for the hand to start.
- **Start Hand:** Players are all ready to begin a hand.
- **Shuffle:** The deck is shuffled and encrypted.

- **Deal:** There are a number of dealing rounds depending on the poker game being played. For example, in Texas Hold'em, we will have: pre-flop, flop, turn and river.
- **Bet:** The player decides if he wants to check, bet, fold or raise depending on the state of the game.
- **Check Deal:** The game engine checks with the rules of the game to determine if we need to deal more cards.
- **Showdown:** The moment when hands that are still active are displayed or mucked.
- **Resolve:** The results of the hand are shown.
- **Report:** The hand results are sent to the game/table contract and the winner receives the pot.

Figure 14: Gameplay States



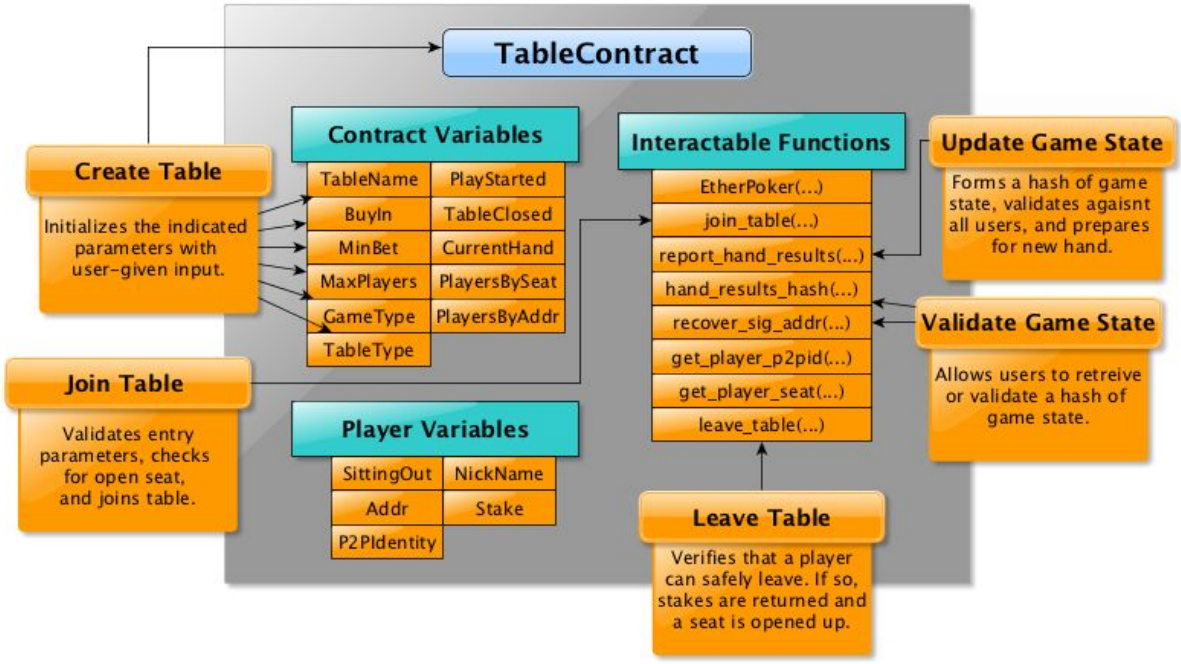
8.3 Ethereum Table Contract

Playing a game of poker solely on the Ethereum blockchain requires considerable resources and time. In order to make game play smooth, Table Contracts are 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: Initializes the poker table with the provided parameters.
Join_table: Joins a table, creates a Player struct with the provided parameters, and returns an error message, if any.
Get_player_seat: Returns the seat number of the user who sent the message or -1 if user does not have a seat.
Get_player_p2pid: Returns the p2pid for the player specified by the seat number or an empty string.
Hand_results_hash: Computes a sha3 hash of the parameters provided by the user.
Recover_sig_addr: Returns address associated with the key pair used to sign the hash.
Report_hand_results: Verifies that all players have signed the game data and returns an error message, if any.
Leave_table: 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 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 to receive funds.
- The private key is the one that is used to 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.

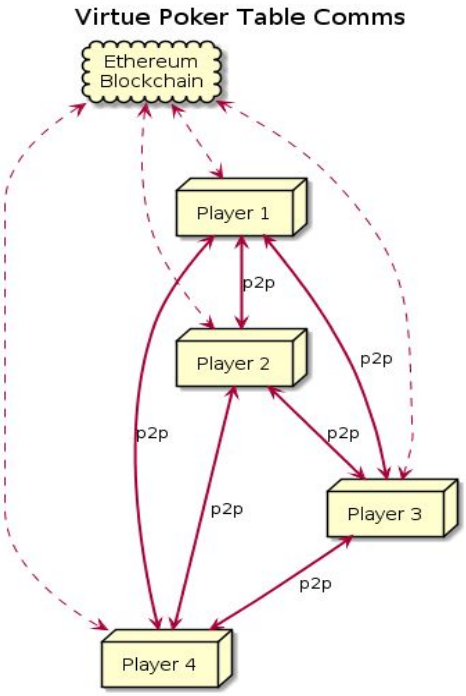
Your keys will be stored in your hard drive and will be secured by a password that you will use when you play on Virtue Poker.

8.5 P2PNet

The P2PNet is responsible for all communication that is 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 and all transactions to the Ethereum Network have a gas cost, so we need to be as efficient as possible in DApps. We are working to minimize the size of our contracts to limit overhead, and to limit communications to the Ethereum blockchain to reduce operational costs and improve gameplay speed.

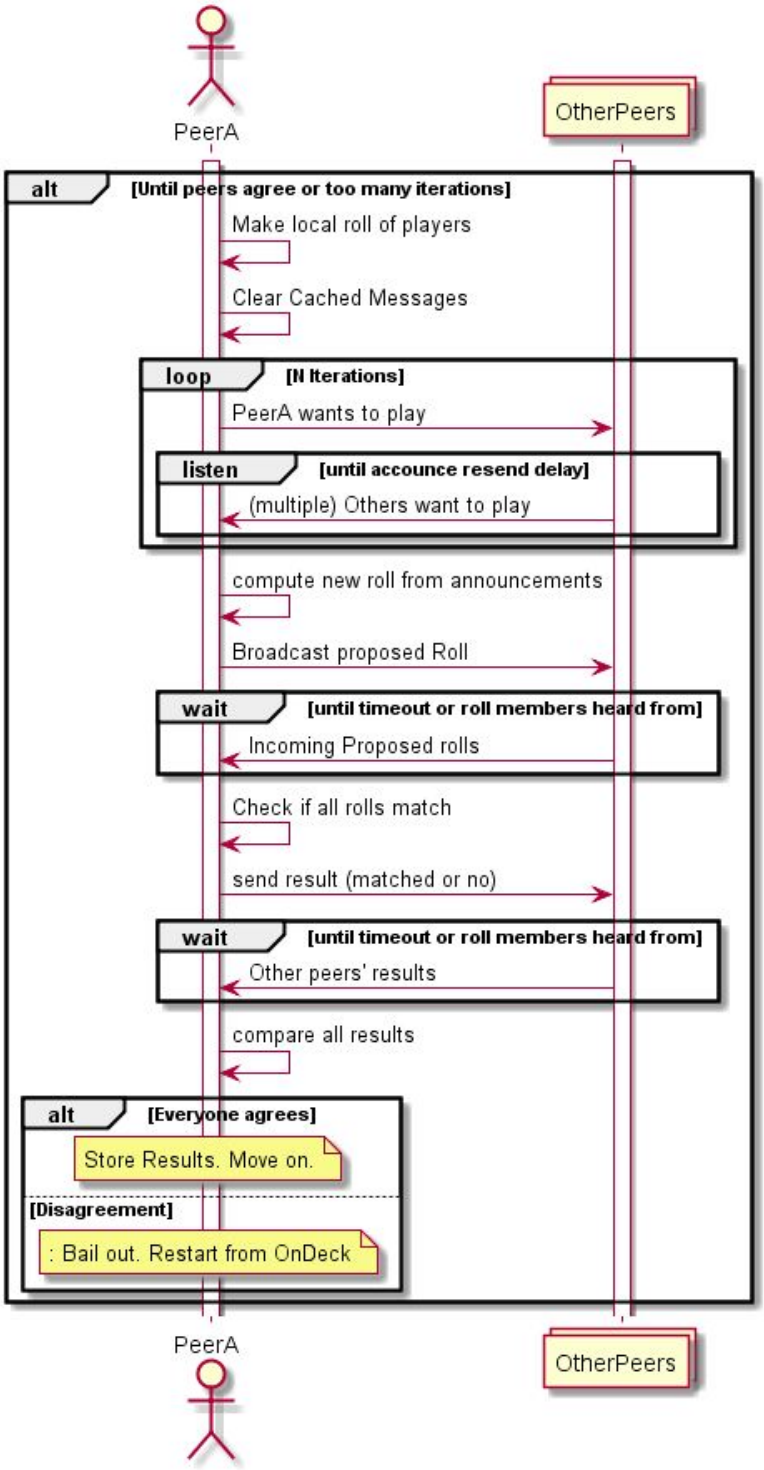
Our P2PNet is not using state channels as they are defined, but at some level everything (except chat) carried by P2PNet is part of a state subnet in which all of the game clients agree with one another off-chain as to what happened. This is done in a way where the blockchain can verify that they agreed 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 seated players, 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 use Web3.js to:

- **Compile a contract**: Our contracts are precompiled and tested properly before compiling them with Web3.js. Compiling a contract is required before deployment using web3.js.
- **Deploy a contract**: Web3.js provides an 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 always be done using Web.js.

8.7 Electron

Our desktop application is based in Electron. Electron has been used successfully in previous Ethereum-based projects including the Mist Ethereum Wallet, Atom, Visual Studio Code and the Jaxx Wallet. 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 – in our case, 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 to hire developers for specific platforms.
3. **Improve development cost**: We 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 on specific platforms, all our resources will be focused on the development of one product that will work in multiple platforms using Electron.

8.7.1 Electron Architecture

Electron architecture is based on:

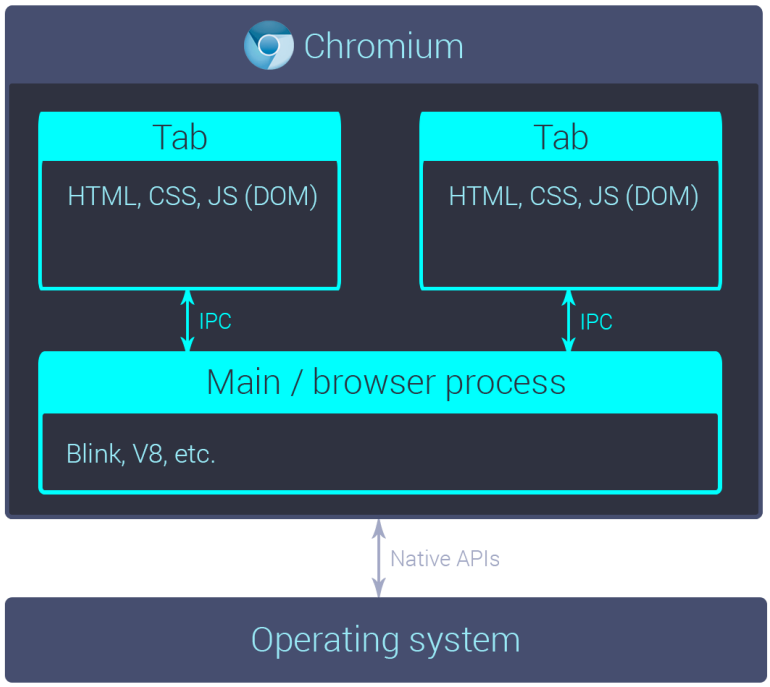
- **Chromium**: the browser engine that is used by Google Chrome and Chrome OS. This allows us to build our application using web technologies.
- **NodeJs:** Node is a Javascript engine build on top of Chrome/Chromium V8 Javascript engine. Nodes provides access to the operative system resources (for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

Every new version of Electron provides the latest version of Chromium and NodeJS. The current version of Electron at this writing is Electron 1.6.11, which contains:

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

More details on Electron are available here: https://electron.atom.io/

Figure 18: Chromium

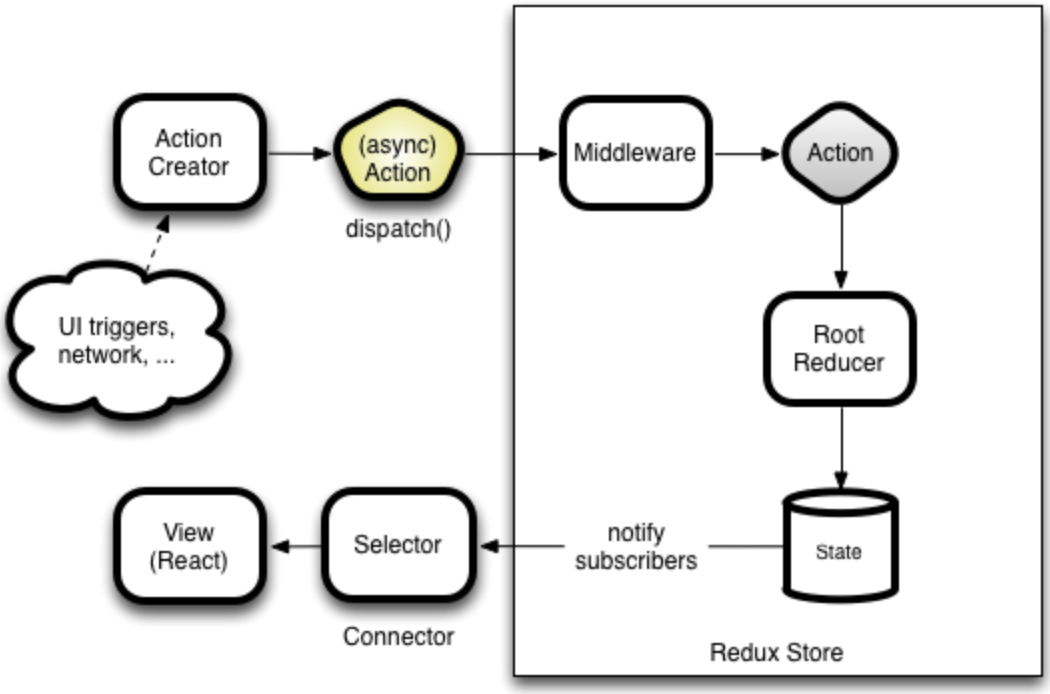


8.8 Poker Game Client

8.8.1 Game Client Architecture

Our game client is built using the React 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:

- Lobby
- Table Game

When the user starts the game, he will be in the lobby and will able to perform these 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.