VIRTUE POKER

Whitepaper: Virtue Poker

Nutzung von Ethereum zum Aufbau einer dezentralen P2P-Poker-Plattform

Entwurf (Version 0.9)

März 2018

Dieses Dokument ist nur zu Informationszwecken gedacht und begründet weder ein Verkaufsangebot noch eine Kaufaufforderung für Aktien oder Wertpapiere der Firma Virtue Poker oder mit ihr verbundener oder angegliederter Unternehmen. Derartige Verkaufsangebote oder Kaufaufforderungen erfolgen gegebenenfalls im Wege eines Privatplatzierungsprospekts und unter Einhaltung sämtlicher anwendbaren gesetzlichen Vorschriften.

Bei diesem Dokument handelt es sich um einen Entwurf, der aus Kulanz und in der Absicht bereitgestellt wird, erste Reaktionen und Rückmeldungen von Branchenvertretern und Mitgliedern der Community einzuholen. Dieses Dokument ist nicht als endgültige Fassung zu verstehen, und sämtliche darin enthaltenen Informationen können sich jederzeit ohne Vorankündigung ändern. Sofern und soweit Virtue Poker zukünftig Produkte oder Dienstleistungen – einschließlich Tokens – zum Verkauf anbietet, sind die zu diesem Zeitpunkt gültigen Vertragsbedingungen und Vorgaben zu beachten, einschließlich die jeweils aktuelle Fassung dieses Whitepapers.

Inhaltsverzeichnis

1. Zusammenfassung

Online-Poker hat sich seit den frühen 2000er Jahren von ein paar wenigen Startups zu einer Wirtschaftssparte entwickelt, in der es um Milliardenbeträge geht. Zwei schwerwiegende Probleme begleiten diese Entwicklung bereits seit Anbeginn: Fairness beim Spiel und Sicherheit der von den Spielern eingesetzten Geldbeträge. Diese beiden Themen standen im Brennpunkt bei einer Reihe von Branchenskandalen, die mehrere führende Anbieter im Online-Poker-Geschäft die Lizenz kosteten.

Virtue Poker setzt solchen Machenschaften ein Ende. Hierbei handelt es sich um eine dezentrale Plattform zum Online-Poker-Spielen unter Einsatz von Echtgeld. Sie basiert auf dem Blockchain-System Ethereum und bietet Nutzern als erster Blockchain-basierter Online-Poker-Anbieter eine Spielerfahrung, bei der keine Einzahlung von Geldbeträgen auf einer Website erforderlich wird und die Karten nachweislich nach dem Zufallsprinzip gemischt und kryptografisch gesichert werden.

1.1 Nutzenversprechen

Bei Virtue Poker werden die Spielmittel nicht auf Servern gespeichert, und alle Spieler sind am Mischen der Karten beteiligt. Dadurch wollen wir folgende Ziele erreichen:

1.1.1 Ausschluss der mit der Einzahlung verbundenen Risiken

Virtue Poker gibt Spielern die Möglichkeit, ihre Spielmittel im eigenen Gewahrsam zu behalten. Mithilfe von Ethereum Smart Contracts werden Turniereinsätze treuhänderisch verwaltet und Auszahlungen abhängig vom jeweiligen Spielausgang autonom verteilt.

1.1.2 Vertrauensbildung in Bezug auf Fairness beim Spiel

Die Karten werden unter Nutzung eines kryptografischen Peer-to-Peer-Protokolls namens „Mental Poker“ gemischt, wobei alle an einem Tisch sitzenden Spieler einbezogen sind. Am Ende jeder Hand wird zur Konsensbildung ein Konsensmechanismus mit Byzantinischer-Fehler-Toleranz angewandt.

1.1.3 Reduzierung der Kosten für Spieler und Aufbau eines ausgewogenen Poker-Ökosystems

Virtue Poker basiert auf einer innovativen dezentralen Peer-to-Peer-Architektur. Im Verbund mit der Nutzung von Ethereum lassen sich dadurch Kosten für Server und Zahlungsabwicklung einsparen. Die Mehrzahl der Spielfunktionen, die im Normalfall auf zentralen Servern ausgeführt werden, werden im Virtue-Poker-System verteilt. Die Spielmittel verbleiben stets in durch *Smart Contracts* gesicherten Wallets im Gewahrsam der Spieler. Durch niedrigere Hausanteile und weitere Anreize sollen diese Einsparungen den Spielern zugutekommen, sodass insgesamt mehr Geld im Poker-Ökosystem verbleibt.

1.1.4 Auf- und Ausbau eines erweiterbaren dezentralen Poker-Netzwerks

Virtue Poker plant den Aufbau der zugrundeliegenden Kern-Architektur für ein dezentrales Online-Poker-Netzwerk, die Entwicklern und Fremdbetreibern als Grundlage zur Integration und Weiterentwicklung dienen soll. Unsere Hoffnung und Erwartung ist, dass die Plattform zukünftig durch neue Funktionen erweitert wird.

1.2 Kurzfristige Zielsetzung

Virtue Poker arbeitet am Aufbau einer serienreifen Anwendung, die in das Ethereum-Mainnet integriert werden soll. Zu Verwirklichung dieses Ziels und Vorbereitung der Markteinführung baut Virtue Poker die Abteilungen Entwicklung und Marketing aus. Die Abteilung Entwicklung soll schwerpunktlich am Auf- und Ausbau der Nutzeroberfläche sowie der verteilten Misch- und Blockchain-Technologien arbeiten. Die Marketing-Abteilung wird sich um die Einbindung unserer Alpha-Nutzer kümmern, um Feedback zu dem Produkt einzuholen und die Plattform im Vorfeld der Markteinführung im iterativen Verfahren zu optimieren.

1.3 Langfristige Wachstumsstrategie

Zur Entfaltung unserer langfristigen Strategie sind zwei Makrophasen vorgesehen: (1) Auf- und Ausbau der erforderlichen Technologie und Liquidität, damit die Plattform als Anbieter im Verbrauchermarkt

(B2C) operieren und die Attraktivität, Integrität und Glaubwürdigkeit unseres Konzepts unter Beweis stellen kann, und (2) weltweite Expansion als Weißprodukt zum Vertrieb durch Lizenznehmer in unterschiedlichen regionalen Märkten. Dadurch soll Fremdbetreibern der nahtlose und kostengünstige Aufbau eigener auf Blockchain-Technologie basierender Online-Pokerräume durch Nutzung unserer Haupttechnologie ermöglicht und zugleich eine dauerhafte Einnahmequelle geschaffen werden.

2. Probleme beim Online-Pokern

2.1 Einleitung

Online-Casinos haben sich als Wirtschaftssparte etabliert, in der es um Milliardenbeträge geht. Laut Prognosen ist davon auszugehen, dass die in diesem Bereich erwirtschafteten Umsätze bereits 2021 die 50-Milliarden-Dollar-Grenze überschreiten.[1] Poker zählt zu den Hauptmotoren dieser phänomenalen Erfolgsgeschichte. Entscheidender Auslöser des Wachstumsbooms der Online-Pokerräume war die Fernsehübertragung des Main Event der World Series of Poker 2003, bei dem der Buchhalter Chris Moneymaker, ein bislang unbekannter Amateur, 2,5 Millionen US-Dollar gewann.

Heute liegen die im globalen Online-Pokergeschäft erwirtschafteten Umsätze bei über 2,5 Milliarden US-Dollar. Im globalen Vergleich dominieren Europa und Asien mit Marktanteilen von 47 bzw. 30 Prozent, gefolgt von Nordamerika (13 Prozent), Ozeanien (6 Prozent) und Lateinamerika (2 Prozent).[2]

Leider wurde die Online-Poker-Branche in den vergangenen Jahren von mehreren Skandalen erschüttert und von böswilligen Akteuren missbraucht. Zwar haben führende Anbieter wie PokerStars.com durch entsprechende Anpassung ihrer Plattformen auf dieses problematische Verhalten reagiert. Andere Anbieter haben derartige Reaktionen jedoch bis dato vermissen lassen, was zu einem anhaltenden Vertrauensverlust seitens vieler Spieler führte.

2.2 Missbrauch von Spielmitteln

2.2.1 Absolute Bet und Ultimate Bet

Nach jahrelangen Beschwerden seitens der Spieler gab das drittgrößte Poker-Netzwerk, Cereus Network (Betreiber von Ultimate Bet und Absolute Poker) zu, dass ein ehemaliger Mitarbeiter sich Zugriff auf ein Administratoren-Konto verschafft hatte und dadurch die Karten sämtlicher Spieler auf der Plattform einsehen konnte. Im Laufe mehrerer Jahre war es dieser Person und ihren Mitverschwörern gelungen, einen zweistelligen Millionenbetrag zu entwenden.[3]

2.2.2 Full Tilt Poker

Der 15. April 2011 wird in der Online-Poker-Community als „Schwarzer Freitag“ bezeichnet. Es ist das Datum der Anklageerhebung gegen die Gründer der drei größten Online-Poker-Websites – PokerStars, Full Tilt Poker and Absolute Poker – durch die US-Staatsanwaltschaft, die den betreffenden Websites die Ausrichtung von Glücksspielen mit Echtgeld für US-Bürger verbot. Als Full Tilt kurze Zeit später außerhalb der USA das Geschäft wiederaufnahm, stellte sich heraus, dass das Unternehmen ein Defizit in Höhe von 360 Millionen US-Dollar verzeichnete (mit anderen Worten,

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

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

3 „Ultimate Bet Review – Scandalous History and Failure of UB.“ Safest Poker Sites. Safest Poker Sites, ohne Jahresangabe Web. 7 Okt. 2016.

Einzahlungen von Spielern in Höhe von 360 Millionen US-Dollar veruntreut hatte). Wenig später stellte das Unternehmen den Betrieb endgültig ein.[4]

2.2.3 Lock Poker

Dem US-amerikanischen Anbieter Lock Poker wurde 2015 die Lizenz entzogen, nachdem Geldauszahlungen an Spieler fast ein Jahr lang verweigert worden waren. Die Verluste der betroffenen Spieler werden auf 15 bis 24 Millionen US-Dollar geschätzt.[5]

2.3 Poker Bots

Ein Poker Bot ist ein Software-Programm, das sich online als menschlicher Spieler ausgibt. Poker Bots können an mehreren Tischen zugleich sitzen und ohne menschliche Beaufsichtigung laufen. Poker Bots sind unterschiedlich komplex: Teils handelt es sich um Serienprodukte, teils um nutzerspezifische Sonderanfertigungen, die von einem einzelnen Akteur eingesetzt werden.

Im Jahr 2015 gewann ein Bot-Ring auf PokerStars knapp 1,5 Millionen US-Dollar in Bargeldspielen um Einsätze von 0,50/1,00 USD und 1,00/2,00 USD.[6] Anbieter wie WarBot verkaufen gebrauchsfertige Bots zur Nutzung auf sämtlichen Plattformen.[7] Die von börsennotierten Unternehmen wie 888 Holdings eingesetzten Sicherheitsvorkehrungen zum Schutz von Spielern gegen Bots haben sich weitgehend als ineffizient erwiesen. In einem von 888 Holdings veröffentlichten Blog-Beitrag zum Thema „How to Play Against Poker Bots“ werden diese als „schwache“ Gegner bezeichnet[8].

In Wirklichkeit stellen Bots jedoch eine echte Gefahr dar. Die Carnegie-Mellon University in Pittsburgh ließ 2017 unter dem Motto „Hirnzellen gegen Künstliche Intelligenz“ vier der weltbesten Profis im Heads-Up-Poker gegen einen Poker Bot namens Libratus antreten – der Poker Bot siegte.[9] Wenngleich nicht alle Poker Bots von einem Supercomputer angetrieben werden wie Libratus, stellen sie insgesamt eine erhebliche Bedrohung für den zukünftigen Erfolg der Branche dar.

2.4 Tools und Software von Drittanbietern

Viele Online-Spieler benutzen Tools und Software von Drittanbietern, die sich gezielt an Freizeitspieler richten.[10] Insbesondere sind hier folgende Tools zu nennen:

Spieler-Datenbanken: Datenbanken, die sich nach Spielern mit niedrigen Gewinnquoten aus verschiedenen Poker-Netzwerken durchsuchen lassen

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

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

Auto-Seating: Automatische Verteilung der Spieler an den Tischen bei qualitätsgeprüften Bargeldspielen und „Sit & Go“-Turnieren sowie farbliche Kodierung von Spielern nach Spielerstatistiken

Spieler-Scanning: Scannt die Spieler, die sich aktuell in der Lobby einer Poker-Plattform befinden, nach bestimmten Kriterien

Heads-Up-Anzeige: Echtzeit-Anzeige von Spielerstatistiken für Kontrahenten an aktiven Tischen

Diese Tools wurden zu dem Zweck entwickelt, Spielern die Möglichkeit zu geben, sich Informationen über ihre Mitspieler zu verschaffen. Leider bedeutet ihre weit verbreitete Verwendung einen Nachteil für Freizeitspieler, die sie nicht benutzen und ohne ihr Wissen von routinierten Profis ins Visier genommen werden.

2.5 Ungleicher Hausanteil

Bei Turnieren und Bargeldspielen kassiert der Betreiber einen Hausanteil („Rake“). Bei Turnieren wird eine Provision erhoben, die im Normalfall zwischen 6 und 10 Prozent des Mindesteinsatzes beträgt. Bei Bargeldspielen wird ein bestimmter Prozentsatz aus jeder Hand abgeführt. Dieser Prozentsatz liegt im Normalfall zwischen 3 und 5 Prozent mit einer Deckelung von 0,30 bis 5,00 US-Dollar pro Hand, je nachdem, um welche Höchsteinsätze gespielt wird. Die Höhe des jeweils eingezogenen Hausanteils kann zwar von einem Anbieter zum nächsten variieren, jedoch sind die Hausanteile insgesamt bei allen Online-Pokerräumen ganz ähnlich strukturiert.

Abbildung 1 veranschaulicht die aktuelle Strukturierung des Hausanteils bei PokerStars.[11] Auf den ersten Blick erscheint diese Struktur einleuchtend, da Spieler mit höheren Wetteinsätzen rein rechnerisch einen höheren Hausanteil zahlen als Spieler mit niedrigeren Wetteinsätzen und ihr Wert für den Website-Betreiber höher ist:

Abbildung 1: Hausanteil bei PokerStars als Beispiel

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

US Dollar Games

No Limit and Pot Limit*

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

Dabei ist zu beachten, dass der Hausanteil für ein Spiel mit mindestens fünf Spielern im Niedrigsteinsatz-Bereich (0,01/0,02 USD) in 15-facher Höhe des Big Blind gedeckelt ist. Bei Einsätzen von 3,00/6,00 US-Dollar ist der Hausanteil in 0,58-facher Höhe des Big Blind gedeckelt.

Forscher der Universität Hamburg werteten in einer Studie über einen Zeitraum von sechs Monaten mehr als 2,5 Millionen Hände auf PokerStars und anderen Websites aus und fanden heraus, dass Spieler mit Einsätzen von 0,01/0,02 US-Dollar durchschnittlich einen Hausanteil von 12,5 BB (Big Blinds) pro 100 Hände zahlen. Bei Einsätzen von 3,00/6,00 US-Dollar beträgt der durchschnittliche Hausanteil nur noch 2,58 BB pro 100 Hände. [12] Abbildung 2 zeigt den in der Studie ermittelten durchschnittlichen Hausanteil pro 100 Hände für unterschiedliche Spieleinsätze:

Abbildung 2: Hausanteil bei unterschiedlichen Einsätzen

12 THE GAMBLING HABITS OF ONLINE POKER PLAYERS: The Journal of Gambling Business and Economics 2011 Bd. 6

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

Je höher die Einsätze, desto niedriger der Hausanteil im Verhältnis zum Big Blind. Eine Gewinnquote von 4 bis 6 BB pro 100 Hände gilt im Online-Poker als hervorragend. Bei der aktuell üblichen Strukturierung des Hausanteils verlieren auch Gewinner, wenn um niedrige Einsätze gespielt wird. Ein Einkommen kann nur verdienen, wer um hohe und höchste Einsätze spielt.

2.6 Die Krise der Poker-Wirtschaft

2.6.1 Begriffsklärung

Die Poker-Wirtschaft lebt hauptsächlich von drei Produktionsfaktoren: Einzahlungen, Hausanteilen und Auszahlungen. Ein globales Wachstum ist nur möglich, wenn folgende Bedingung zutrifft:

$$\text{Einzahlungen} > (\text{Hausanteil} + \text{Auszahlungen})$$

Dieses Modell erfordert eine ständige Zufuhr von Einzahlungen, um überlebensfähig zu bleiben. Poker-Profis erwirtschaften bezüglich ihrer Auszahlungen eine positive Nettobilanz – mit anderen Worten, sie gewinnen mehr, als sie verlieren –, Freizeitspieler in der Regel eine negative Nettobilanz, sodass sich insgesamt ein ausgewogenes Ökosystem ergibt.

2.6.2 Problemlage

Jedoch wird die Poker-Wirtschaft dadurch unter Druck gesetzt, dass die Gewinne der Profis und Semiprofis höher sind als die Einzahlungen der Freizeitspieler. Die Ursachen dafür liegen in der Verschärfung des Wettbewerbs im Zuge der allgemeinen Verbreitung von Poker-Strategien in Form von Online-Tutorials, Blogs u. ä.; der Benachteiligung von Freizeitspielern durch unverhältnismäßig hohe Hausanteile; der Nutzung von Drittanbieter-Tools, um weniger routinierte Spieler aufs Korn zu nehmen; und einem Vertrauensverlust unter Freizeitspielern bezüglich der Integrität des Online-Pokern.

2.7 Fragmentierung des globalen Marktes

In einigen maßgeblichen Territorien und Regionen wird die Möglichkeit zum Betreiben von Online-Poker-Plattformen regulatorisch eingeschränkt. Bezüglich der Reaktion der jeweils zuständigen Aufsichtsbehörden auf das Angebot von Online-Poker-Plattformen in den betreffenden Territorien lassen sich folgende Kategorien unterscheiden (wobei die im Einzelnen verwendeten Bezeichnungen variieren):

2.7.1 Schwarzmärkte

Schwarzmärkte sind Territorien, in denen Online-Poker entweder rechtswidrig oder nur bundesstaatsintern erlaubt ist.

2.7.2 Dunkelgraue Märkte

Dunkelgraue Märkte sind Territorien, in denen Online-Glücksspiel nicht explizit verboten bzw. die einschlägige Rechtslage ungeklärt ist.

2.7.3 Graue Märkte

Graue Märkte sind Territorien, in denen Online-Glücksspiel reguliert wird bzw. die keine Maßnahmen gegen Fernanbieter ergriffen haben.

2.8 Kategorisierung der Anbieter

Innerhalb dieses regulatorischen Rahmens stehen Betreiber von Online-Poker-Plattformen vor der Wahl, entweder mit einer oder mehreren Lizenzen in mehreren Märkten oder mit einer einzigen bzw. ohne Lizenz in allen Märkten zu operieren. Entsprechend sind sie als *Onshore*- bzw. *Offshore*- Anbieter zu klassifizieren.

2.8.1 Onshore-Anbieter

Regulierte Anbieter haben eine oder mehrere Lizenzen von einer anerkannten für Glücksspiel zuständigen Stelle eingeholt und operieren im Normalfall in den meisten grauen und dunkelgrauen Märkten. Diese Anbieter halten sich in der Regel an einschlägige Compliance-Richtlinien bezüglich Geldwäsche, Kundenidentifizierung, Steuerpflicht usw. In vielen Fällen handel es sich um Unternehmen, die weltweit an verschiedenen Börsen notiert sind. Diese Kategorie umfasst unter anderen die folgenden Anbieter: The Stars Group (PokerStars, Full Tilt Poker) William Hill Online, Playtech (iPoker network), GVC Holdings (PartyPoker, bwin.party), 888 Holdings, Unibet, Winamax.

2.8.1 Offshore-Anbieter

Unregulierte Anbieter haben ihren Sitz häufig in Offshore-Territorien in Costa Rica, Curacao, Zypern oder auf Indianerreservaten. Sie bieten ihre Leistungen weltweit an, u. a. auch auf Schwarzmärkten. Zu diesen Anbietern lassen sich kaum zuverlässige Angaben einholen.
In diese Kategorie fallen u. a. folgende Anbieter: PaiWangLuo Network (Ignition, Bovada), Merge Gaming (Carbon Poker), Winning Poker Network (America’s Cardroom), Global Gaming Network, TheHive, Tiger Gaming (Chico).

Mittlerweile wird Online-Poker weltweit in zahlreichen Territorien und Staaten reguliert, sodass der Anteil des regulierten Online-Poker-Geschäfts im Steigen begriffen ist.

2.9 Eingeschränkter Wettbewerb

Voraussetzung für den wirtschaftlichen Erfolg von Online-Poker-Netzwerken ist die Herstellung großer globaler Liquiditätspoole von Spielern. Im Laufe der Zeit fand eine zunehmende Konzentration auf einige wenige große Anbieter innerhalb der jeweiligen Zielmärkte statt. Aus Spielersicht hat dies zu

einem eingeschränkten Angebot an Spielmöglichkeiten geführt und eine Situation geschaffen, die es Betreibern von Online-Poker-Plattformen einfach macht, die Spielgebühren zu erhöhen.

2.9.1 Regulierter Verbrauchermarkt

Mit einem Jahresumsatz von über 850 Millionen US-Dollar und einem globalen Marktanteil von ca. 60 Prozent konnte PokerStars sich als führender Anbieter im regulierten Verbrauchermarkt positionieren. Als Veranstalter der größten Turniere mit den höchsten Bargeldpreisen ist das Unternehmen weltweit beinahe flächendeckend vertreten (u. a. auch auf 30 Märkten, die auf der schwarzen Liste stehen) . PokerStars war Veranstalter des bislang größten Online-Pokerturniers der Welt mit 253.000 Teilnehmern und hat den größten Preispool in Höhe von acht Millionen US-Dollar vergeben. Insgesamt hat das Unternehmen bereits über 145 Milliarden Poker-Hands ausgeteilt. Es sponsert Weltklassespieler und Live-Tourneen. Prominente Persönlichkeiten wie Kevin Hart, Usain Bolt, Rafa Nadal und Ronaldo sind als Markenbotschafter für PokerStars tätig. Neben Investitionen in Maßnahmen zum Schutz der Spieler wie erstklassige Bot-Erkennung, unterschiedliche Optionen zur Zahlungsabwicklung und Verhinderung von Mehrfachkonten („Multi-Accounting“) konnte PokerStars den weltweit größten Liquiditätspool aufbauen.

Aus Spielersicht hat PokerStars zwei erhebliche Nachteile: (1) Die angebotenen Leistungen sind aufgrund der hohen Hausanteile mit hohen Kosten verbunden, und (2) der Standard der Konkurrenz ist wesentlich höher als bei anderen Plattformen. Zudem ist das Unternehmen aufgrund seiner Position als Marktführer mehr oder weniger immun gegen Widerstände seitens der Spieler. Konkret heißt das, es kann mit minimaler Vorankündigung etablierte Treueprogramme zurückschrauben oder einstellen, Gebühren erhöhen oder sich aus bestimmten Märkten zurückziehen.

2.9.1 Unregulierter Verbrauchermarkt

Der unregulierte Markt für Online-Poker ist etwas stärker fragmentiert, jedoch gibt es auch hier eindeutig dominante Anbieter, nämlich Winning Poker Network (America’s Cardroom) und das kürzlich umfirmierte PaiWangLuo Network (Ignition, Bovada). Diese Unternehmen sind eher bereit, auf Schwarzmärkten zu operieren, und wenig transparent in Bezug auf ihre Geschäftspraktiken. Allgemein gesprochen investieren diese Anbieter nur minimal in Maßnahmen zur Betrugsabwehr wie Bot-Erkennung oder Verhinderung on Mehrfachkonten, sodass Spieler auf ihren Plattformen diesbezüglich so gut wie keine Unterstützung erhalten.

Viele Spieler landen bei diesen Anbietern entweder aus Mangel an Alternativen oder weil die Konkurrenz auf den regulierten Plattformen zu stark ist. Jedoch führt das Fehlen einer Sorgfalts- und Berichterstattungspflicht dazu, dass Spieler so gut wie keine Möglichkeiten haben, Ansprüche geltend zu machen für den Fall, dass die Websites offline gehen, Spielerkonten sperren oder ihnen Fehlverhalten vorgeworfen wird.

2.10 Zertifizierungsverfahren für Random Number Generators

Online-Poker unterscheidet sich in einer wesentlichen Hinsicht von Live-Spielen im Casino: Im Online-Spiel können die Spieler nicht wie im Casino dem Dealer beim Mischen beim Karten zuschauen. Stattdessen müssen sie darauf *vertrauen*, dass der Random Number Generator (RNG) des Anbieters ordnungsgemäß funktioniert. Fast alle Online-Anbieter lassen ihre RNGs von einer vorab genehmigten

unabhängigen Instanz zertifizieren. Zu den einschlägigen Anbietern zählen u. a. iTech Labs (itechlabs.com) und Gaming Laboratories International (gaminglabs.com).

Leider ist über die einmal erfolgte RNG-Zertifizierung hinaus ein verblüffender Mangel an Beaufsichtigung zu konstatieren. So findet sich auf der Website der für Glücksspiele zuständigen maltesischen Aufsichtsbehörde folgende Formulierung: „Im Anschluss an das Zertifizierungsverfahren als Voraussetzung für die Erteilung einer vollumfänglichen Lizenz für fünf Jahre sind keine regelmäßigen Überprüfungen des Glücksspiel-System erforderlich; jedoch liegt es im Ermessen der Aufsichtsbehörde, Auditverfahren zur Nachkontrolle anzusetzen.“ [13] Im Leitfaden für Online-Glücksspiel der Isle of Man heißt es: „Die Aufsichtskommission für Glücksspiele (GSC) lässt den RNG jedes Anbieters mindestens zweimal während der fünfjährigen Laufzeit der Lizenz überprüfen, wobei viele Anbieter den RNG für ihre Spiele ggf. in häufigeren Abständen überprüfen lassen.“[14] Diese fehlende Beaufsichtigung hat in Spielerkreisen zur Verbreitung des Verdachts beigetragen, dass die Spiele womöglich nicht hundertprozentig fair ablaufen.

2.11 Schlussfolgerungen

Im aktuellen Markt für Online-Poker haben Spieler mit zahlreichen Nachteilen zu kämpfen. In regulierten Märkten stellen ihnen Schadsoftware, hohe Spielgebühren und starke Konkurrenz Hindernisse in den Weg. In Schwarzmärkten werden sie genötigt, auf Websites zu spielen, auf denen es an Rechenschaftspflicht und Transparenz mangelt. Insgesamt setzen verschärfter Wettbewerb, höhere Gebühren und wachsendes Misstrauen unter Freizeitspielern das globale Poker-Geschäft zunehmend unter Druck.

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. Die Virtue-Lösung

Virtue Poker hat sich in jahrelanger Forschungsarbeit mit der Marktdynamik des Online-Poker-Geschäfts befasst. Wir verfolgen das Ziel einer Neubelebung des Online-Poker-Spiels durch Aufbau eines dezentralen Online-Poker-Netzwerks, in das Vertrauen, Transparenz und Rechenschaftspflicht von vornherein integriert sind. Zur Verwirklichung dieses Ziels nutzen wir das Blockchain-System Ethereum, Peer-to-Peer-Netzwerke, nutzereigene Identitäten und kryptografisch gesicherte Karten und können dadurch ein besseres Spielerlebnis ermöglichen, das zudem für die Spieler mit geringeren Kosten verbunden ist. Noch entscheidender ist, dass wir mithilfe dieser neuen Rahmenbedingungen das Poker-Geschäft von seiner derzeitigen Malaise heilen wollen. Konkret haben wir vor, durch geringere Hausanteile die Kosten für die Spieler zu reduzieren, Rakeback-Strukturen anzubieten, die für verbesserte Spielerbindung sorgen, und die branchenweit sicherste und vertrauenswürdigste Online-Poker-Plattform aufzubauen.

3.1 Ablauf aus Nutzersicht

Virtue Poker ist eine serverlose Anwendung, die die Spielmittel der Kunden nicht speichert und sämtliche Spieler am Mischen der Karten beteiligt. Für den Nutzer sieht der Ablauf folgendermaßen aus:

3.1.1 Clientseitige Virtue-Poker-Anwendung herunterladen

Der Nutzer lädt von der Website www.virtue.poker einen Client für Windows, Mac oder Linux herunter. Die Anwendung umfasst ein Programm zum Kartenmischen, eine Spiel-Engine und eine Benutzeroberfläche.

3.1.2 Anmeldung

Als nächstes legt der Nutzer eine uPort-Identität (uport.me) an (sofern noch nicht vorhanden). Anschließend muss der Nutzer digital eine Bescheinigung bezüglich Wohnsitzstaat und Alter unterschreiben.

3.1.3 Spielmittel in ein Wallet einzahlen

Im nächsten Schritt muss der Spieler ein in die Anwendung integriertes Light Node Wallet auffüllen und wird auf die entsprechende Seite weitergeleitet.

3.1.4 Neues Spiel beginnen oder Aktives Spiel auswählen

In unserer Lobby werden dem Nutzer sämtliche öffentlich zugänglichen Spiele zur Auswahl angezeigt. Alternativ besteht die Möglichkeit, ein eigenes privates Spiel zu beginnen.

3.1.5 Einzahlung von Einsätzen

Um an einem öffentlichen oder privaten Spiel teilnehmen zu können, muss der Nutzer Ether (ETH) oder Virtue Player Points (VPP) an die jeweilige Tischadresse schicken. Der Smart Contract wird auf der Ethereum-Blockchain hinterlegt und dient als Treuhandkonto, solange das Spie läuft. Für jedes Spiel werden eigene Parameter in einem Tisch-Contract festgelegt.

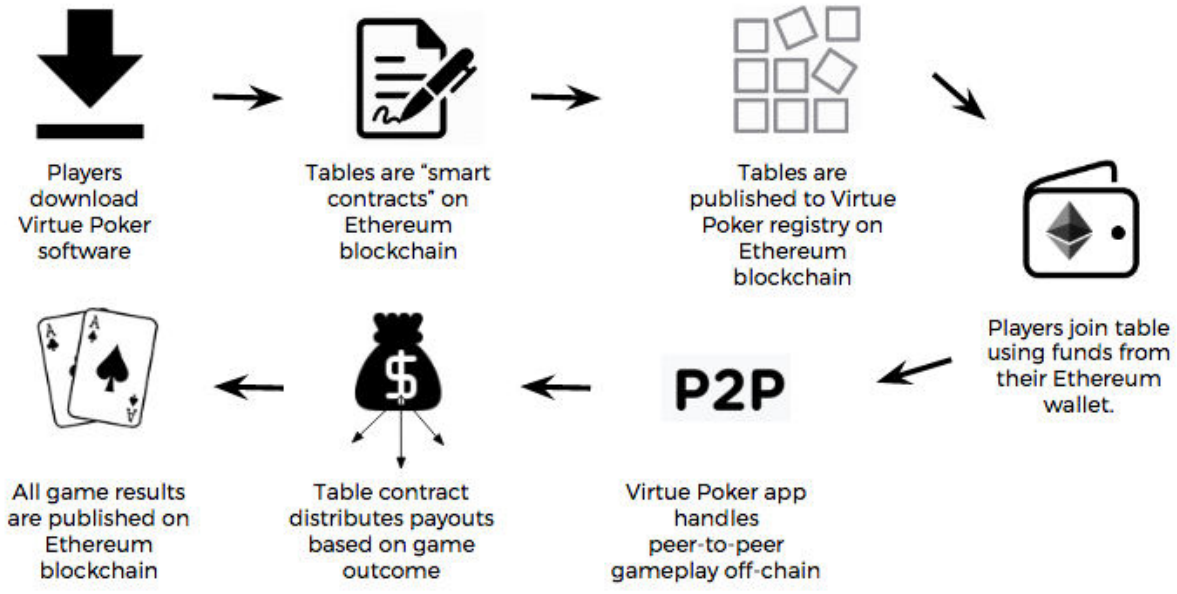
3.1.6 Spielverlauf

Die Spieler am Tisch bilden ein P2P-Subnetz und wenden ein „Mental Poker“-Protokoll an, bei dem alle Spieler im Peer-to-Peer-Verfahren der Reihe nach die Karten mischen und verschlüsseln.

3.1.7 Auszahlung

Wenn das Turnier abgeschlossen ist oder ein Spieler beim Bargeldspiel den Tisch verlässt, wird der Tisch-Contract automatisch ausgeführt und jedem Spieler sein jeweils fälliger Gewinn ausgezahlt.

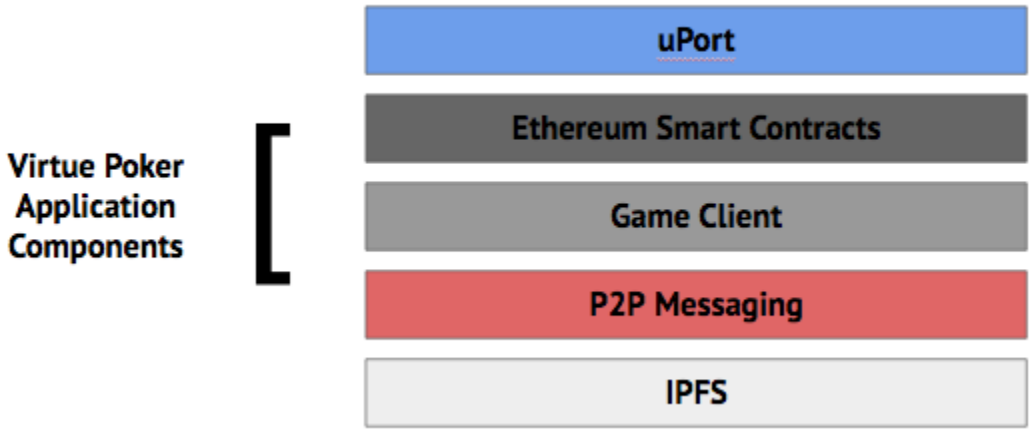
Abbildung 3: Virtue Poker – Spielverlauf



3.2 Virtue Poker – Komponenten

Die Anwendung besteht aus mehreren untergeordneten Komponenten:

Abbildung 4: Virtue Poker – Komponenten



3.2.1 uPort

Die Blockchain-basierte Anwendung uPort, die auf dem Prinzip der Self-Sovereign Identity beruht, wird als Mechanismus zur Anmeldung und Identitätsprüfung verwendet, um Minderjährige vom Spiel auszuschließen und die Nutzung von Mehrfachkonten zu verhindern. Nutzer müssen sich jedes Mal über uPort anmelden, um auf der Virtue-Plattform spielen zu können.

3.2.2 Ethereum Smart Contracts

Ethereum-Contracts werden zu folgenden Zwecken genutzt: (1) als Registrierungsdatenbank (Lobby) für sämtliche aktuell aktiven Spiele auf der Plattform, (2) als kurzfristige Treuhandleistung für alle Spieler an einem bestimmten Tisch, (3) zur Hinterlegung aller spielspezifischen Parameter wie Mindesteinsatz, Auszahlungsanteile und Spielart und (4) zur Berichterstattung über Spielergebnisse.

3.2.3 Spiel-Client

Der Spiel-Client ist eine Zustandsmaschine die als Desktop-Anwendung die Spiellogik verwaltet und Karten anhand eines „Mental Poker"-Protokolls mischt und austeilt. Sie beinhaltet ein Light Node Wallet und dient zur Verbindung der Spieler untereinander.

3.2.4 P2P-Messaging

Ein P2P-Messaging-Backbone wird als Kommunikations- und Synchronisationstool eingesetzt, um sicherzustellen, dass der Spielzustand auf der Benutzeroberfläche für alle Spieler an einem bestimmten Tisch identisch angezeigt wird.

3.2.5 IPFS

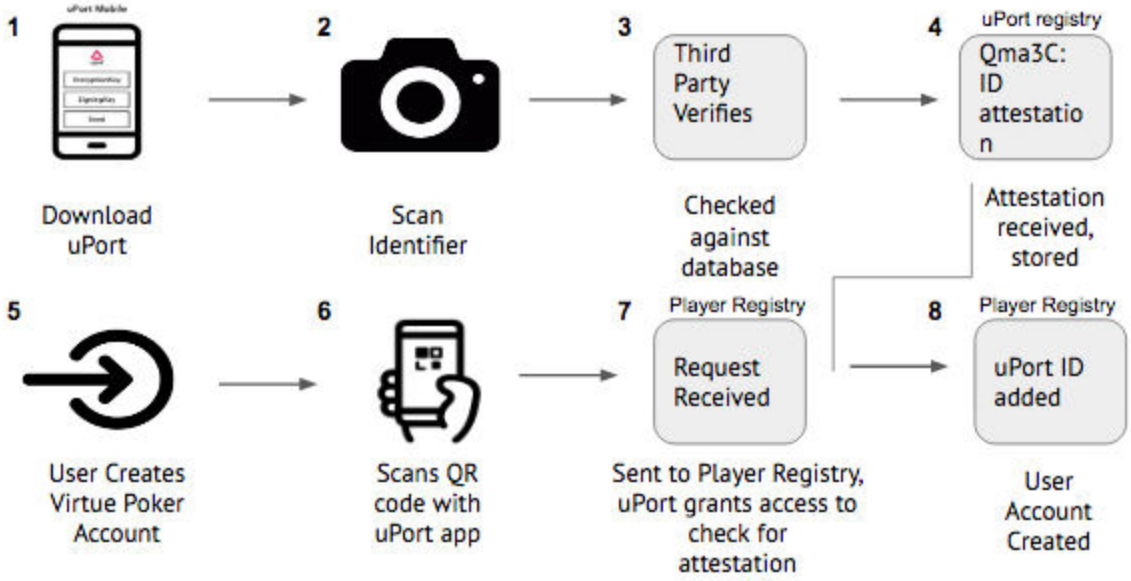
Das Interplanetary File System (IPFS) wird zur Protokollierung der Handverläufe für alle auf der Plattform gespielten Spiele genutzt. Die Protokolle können zur Überprüfung zu Compliance-Zwecken oder durch unser für die Sicherheit der Spiele zuständiges Team abgerufen werden. Zudem stellt diese Komponente der Architektur den Nutzern Handverläufe bereit.

3.3 Identitätsverwaltung

Bevor ein Spieler Zugang zur Virtue-Poker-Plattform erhält, wird seine Identität mithilfe der Anwendung uPort überprüft, die auf dem Prinzip der Self-Sovereign Identity beruht.[15] Das folgende Schaubild zeigt dieses Verfahren im Einzelnen:

Abbildung 5: Identitätsprüfung

15 https://www.uport.me/



1. Schritt: Der Nutzer lädt die uPort-App für Mobilgeräte herunter, legt eine uPort-Identität herunter und scannt einen Identitätsnachweis ein, der von einem Dritten bestätigt werden muss. Diese Bescheinigung wird dann verschlüsselt und im IPFS hinterlegt, und der Nutzer erhält innerhalb seiner uPort-ID eine Bescheinigung zur Bestätigung seiner Identität.

2. Schritt: Der Nutzer legt ein Konto auf Virtue Poker an und bekommt einen QR-Code zugewiesen, den er mit der uPort-App scannt.

3. Schritt: Ein Antrag auf Erstellung eines Neukontos wird zusammen mit dem damit verknüpften uPort-ID an einen Virtue-Poker-Contract geschickt, der daraufhin das Vorhandensein einer Bescheinigung zur Bestätigung der Identität des Nutzers überprüft.

4. Schritt: Nach erfolgreicher Überprüfung wird die uPort-ID des Nutzers mit der Adresse seines Virtue-Poker-Kontos verkuppelt und in der Registrierungsdatenbank von Virtue Poker hinterlegt.

3.4 Ethereum Smart Contracts

Im Anschluss an die erfolgreiche Identitätsprüfung und Kontoerstellung wird der Nutzer in die Lobby weitergeleitet. Es handelt sich hierbei um einen Casino Smart Contract.

3.4.1 Casino-Contract

Der Casino-Contract fungiert als Lobby. Er enthält eine Registrierungsdatenbank sämtlicher aktuell aktiven sowie kürzlich abgeschlossenen Spiele. Neben anderen Aufgaben in den Bereichen Front End, Nutzer- und Spieleverwaltung ist er für das Erstellen von Spielen und die Spielersuche (Matchmaking) zuständig.

3.4.2 Tisch-Contract

Ein Tisch-Contract gilt jeweils für eine Instanz eines Pokerspiels. Bei jeder Entscheidung, ein Spiel mit bestimmten Regeln und Höchst- und Mindesteinsätzen und einer bestimmten Gruppe Spieler zu beginnen, wird ein neuer Tisch-Contract erstellt, den die Spieler dann bestätigen, um am Spiel teilnehmen zu können. Nach Abschluss des Spiels werden die Gewinne ausgezahlt, die Spieler verlassen den Tisch und der Tisch-Contract wird geschlossen. Von diesem Zeitpunkt an dient er nur noch als Bezugspunkt.

Während des Spielverlaufs erfüllt der Tisch-Contract mehrere Funktionen. In erster Linie werden darin sämtliche Angaben zu den Regeln und Einstellungen für das laufende Spiel hinterlegt. Er verwaltet zudem ein Verzeichnis aller beteiligten Spieler mit allen Angaben, die andere Spieler benötigen. Zudem werden über den Tisch-Contract alle Geldeinsätze der Spieler treuhänderisch verwaltet sowie die Gewinne entsprechend verteilt.

Wenn ein neuer Spieler an einen Tisch kommt, wird die erforderliche Einzahlung an den Tisch-Contract überwiesen und intern dem Spieler als Wetteinsatz gutgeschrieben. Der Contract stellt dann die erforderlichen Angaben zur Kommunikation mit den anderen Spielern am Tisch bereit, und das Spiel beginnt. Während des Spiels wird der Contract laufend über den jeweiligen Stand informiert und aktualisiert ihn entsprechend. Wenn ein Spieler den Tisch wieder verlässt, werden ggf. fällige Gewinne auf dasselbe Konto überwiesen, von dem aus der Spieler sie anfänglich eingezahlt hat.

3.4.3 Interaktionen der Spieler mit Tisch-Contracts

Spieler-Transaktionen werden zu folgenden Zeitpunkten an die Tisch-Contracts weitergeleitet: (1) wenn der Spieler neu an einen Tisch kommt, (2) am Ende jeder Hand und (3) nach Abschluss eines Spiels (bei Turnieren) bzw. wenn ein Spieler einen Tisch verlässt (bei Bargeldspielen). Wir sind bestrebt, die Anzahl der an Ethereum übergebenen Transaktionen möglichst gering zu halten, um Gaskosten zu sparen und den Spielverlauf zu beschleunigen.

Tisch-Contracts beinhalten einen Jeton-Zähler, der die Wetteinsätze der Spieler an jedem einzelnen Tisch auf dem aktuellen Stand anzeigt. Am Ende jeder Hand werden die Ergebnisse kryptografisch von allen Spielern und den Schlichtern (siehe Abschnitt 4.2) signiert und in Form einer Transaktion im Tisch-Contract hinterlegt, sodass die Einsätze der Spieler entsprechend aktualisiert werden. Dieser Konsens-Mechanismus und die Hinterlegung einer Transaktion durch die am jeweiligen Spiel beteiligten Peers hat die Funktion eines „Orakels“, indem der Spielzustand sowie die jeweils erforderlichen Auszahlungen an die Spieler im Contract aktualisiert werden. Dieses Verfahren läuft asynchron ab, während auf der Plattform weitere Hände gespielt werden, sodass Spieler bereits mit der nächsten Hand beginnen können, während das Ergebnis der vorherigen Hand von der Blockchain überprüft wird.

3.4.4 Contract für Turniere mit mehreren Tischen

Für Turniere, bei denen an mehreren Tischen gespielt wird, gilt ein Turnier-Contract, der als organisatorisches Tool die Verteilung der Spieler über mehrere Tische verwaltet. Sämtliche Aspekte des Turniers, die eine dem Tisch übergeordneten Ebene betreffen, fallen in die Zuständigkeit dieses Contracts.

3.4.5 Schlichter-Contract

Ein Schlichter ist ein Sonderfall der Client-Software für Spieler, der zwar am Peer-to-Peer-Spielverlauf an einem Tisch teilnimmt, aber weder Karten ausgeteilt bekommt noch Einsätze setzen darf. Der Schlichter erhält ein Honorar dafür, dass er als vertrauenswürdiger Peer im Subnetz des jeweiligen Tisches agiert. Jedem Tisch wird nach dem Zufallsprinzip ein Team von Schlichtern zugewiesen, die Streitigkeiten beilegen und Spieldaten protokollieren.

Zur effizienten Verteilung der Arbeitslast und Verhinderung von Absprachen zwischen Schlichtern und Spielern werden die Schlichter nach dem Zufallsprinzip aus einem Pool ausgewählt und den Tischen zugewiesen. Nach einer bestimmten Anzahl von Händen rotieren sie an einen anderen Tisch. Der Schlichter-Contract ist für die Führung einer Registrierungsdatenbank verfügbarer Schlichter und deren Zuweisung an Pokertische zuständig. Nähere Einzelheiten zum Schlichter-Prinzip entnehmen Sie bitte Abschnitt 4.2.

3.5 Mental Poker

3.5.1 Zusammenfassung

Bereits 1978 veröffentlichten die Kryptografen Adi Shamir, Ron Rivest und Leonard Adleman einen Aufsatz als Antwort auf die von dem Computerwissenschaftler Robert W. Floyd gestellte Frage: „Ist es möglich, Mental Poker unter fairen Bedingungen zu spielen?“ Die hier vorgestellte Lösung sieht ein Verschlüsselungs- und Kommunikationsprotokoll vor, mit dem es möglich wird, dass zwei Spieler an unterschiedlichen Standorten virtuelle Karten mischen und austeilen, ohne einen vertrauenswürdigen Dritten einbeziehen zu müssen.[16] Seitdem sind zu diesem Thema zahlreiche Aufsätze erschienen, in denen die von Shamir, Rivest und Adleman präsentierten Ideen erweitert, alternative Verfahren vorgeschlagen und Analysen und Kritiken angeboten werden.

Indes gibt es bislang nur sehr wenige praxistaugliche Software-Anwendungen, in denen „Mental Poker“-Techniken zum Einsatz kommen. Unter anderem liegt dies daran, dass die kryptografischen Anforderungen mit einem enormen Aufwand an Rechenleistung und Kommunikationsressourcen verbunden sind und die darauf aufbauende Software schlicht und einfach nicht schnell genug arbeitet, um für den Verbrauchermarkt interessant zu sein. Hinzu kommt, dass der dem „Mental Poker“-Protokoll inhärente Peer-to-Peer-Charakter die Verwaltung und Überwachung erschwert und mit traditionellen server-basierten Online-Spiel-Modellen kaum unter einen Hut zu bringen ist.

Das Team von Virtue Poker hat in den vergangenen zwei Jahren untersucht, inwieweit die Nutzung von Blockchain-Technologie und verteilten Speichersystemen im Verbund mit kooperativen Peer-to-Peer-Netzwerken sich hier als Lösung anbietet. Herausgekommen ist eine herunterladbare Anwendung, die ein normales Spieltempo sowie die Verwaltung von Echtgeld-Einsätzen mithilfe des Blockchain-Systems Ethereum ermöglicht.

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

Beim „Mental Poker“ ist durch kooperatives Verschlüsseln und Mischen der Karten gewährleistet, dass die Kartensätze für keinen einzelnen Spieler lesbar sind. Dabei kann jede Karte von einem, mehreren oder allen Spielern in der Gruppe „aufgedeckt“ werden. Das Protokoll funktioniert anhand von Kommunikationsverschlüsselung, wobei Karten in beliebiger Reihenfolge ver- bzw. entschlüsselt werden können. Der zugrunde liegende Algorithmus wird in Abschnitt 3.5.2 näher erläutert.

3.5.2 „Mental Poker“-Algorithmus mit zwei Durchgängen (Two-Pass Shuffle)

Drei Spieler – Peter, Annette und Thomas – sitzen zusammen an einem Pokertisch und spielen Texas Hold’em. Peter ist mit dem Kartengeben an der Reihe; er generiert auf seinem Rechner einen Satz von 52 Karten, die nur er sehen kann. Er verwendet einen Fisher-Yates-Algorithmus zum Mischen der Karten und verschlüsselt den Satz dann mit demselben Schlüssel für jede Karte, sodass er nur für ihn selbst lesbar ist. Diesen verschlüsselten Kartensatz gibt er dann an Annette weiter, die den Vorgang wiederholt: Sie mischt die Karten und verschlüsselt sie. Anschließend gibt sie den Kartensatz an Thomas weiter, der ihn nun seinerseits mischt und verschlüsselt.

Damit ist der Satz nun fertig gemischt, und die Karten befinden sich in einer Reihenfolge von 1 bis 52, die sich im Handverlauf nicht ändert. Thomas gibt den dreifach verschlüsselten Kartensatz an Peter weiter, der seine Verschlüsselung aufhebt und stattdessen jede einzelne Karte mit einem eigenen Schlüssel verschlüsselt: P1, P2 bis P52. Er gibt den Satz an Annette weiter, die ihrerseits ihre Verschlüsselung aufhebt und jede einzelne Karte mit einem eigenen Schlüssel verschlüsselt: A1, A2 bis A52. Anschließend gibt sie den Kartensatz an Thomas weiter, der den Vorgang ebenfalls wiederholt. Die ersten beiden Karten des Satzes werden Peter zugeteilt, der jedoch nur seinen eigenen Schlüssel für diese Karten hat. Daher verraten Annette und Thomas ihm ihre Schlüssel für die ersten beiden Karten – A1 und A2 bzw. T1 und T2 –, sodass Peter nun alle drei Schlüssel für seine eigenen Karten kennt. Damit sind seine Karten für ihn selbst lesbar, nicht aber für seine Mitspieler. Dieser Vorgang wird für jeden Spieler am Tisch wiederholt, sodass alle Spieler ihre eigenen Karten, nicht aber die Karten ihrer Mitspieler einsehen können.

Nachdem alle Spieler ihre jeweilige Spielentscheidung bekanntgegeben haben, wird der Flop gelegt. Der Flop besteht aus der siebten, achten und neunten Karte im Satz. Alle Spieler müssen ihre Schlüssel für diese drei Gemeinschaftskarten offenlegen, sodass sie von allen eingesehen werden können. Entsprechend geht es so lange weiter, bis am Ende der Hand dem Gewinner der Pott zugeschrieben wird und alle Mitspieler zur Bestätigung der Konsensbildung (siehe hierzu Abschnitt 4.2) das Ergebnis der Hand signieren. Dieses Ergebnis wird dann an die Ethereum-Blockchain übergeben, damit der Spielzustand für alle Spieler am Tisch aktualisiert werden kann. Dieses Verfahren wird in den Abbildungen 6 bis 9 veranschaulicht.

3.5.3 Verschlüsselung in zwei Runden: Mischen und Indizieren des Kartensatzes

Entsprechend dem Prinzip der sicheren Mehrparteienberechnung genügt es, wenn einer der Peers die Karten beim Mischen in eine zufällige Reihenfolge bringt. Solange jeder einzelne Spieler Vertrauen hat, dass sein eigener Rechner die Karten ordentlich gemischt bzw. in eine zufällige Reihenfolge gebracht hat, kann er darauf vertrauen, dass das Spiel fair ist.

Abbildung 6: Mischen und Verschlüsseln des Kartensatzes[17]

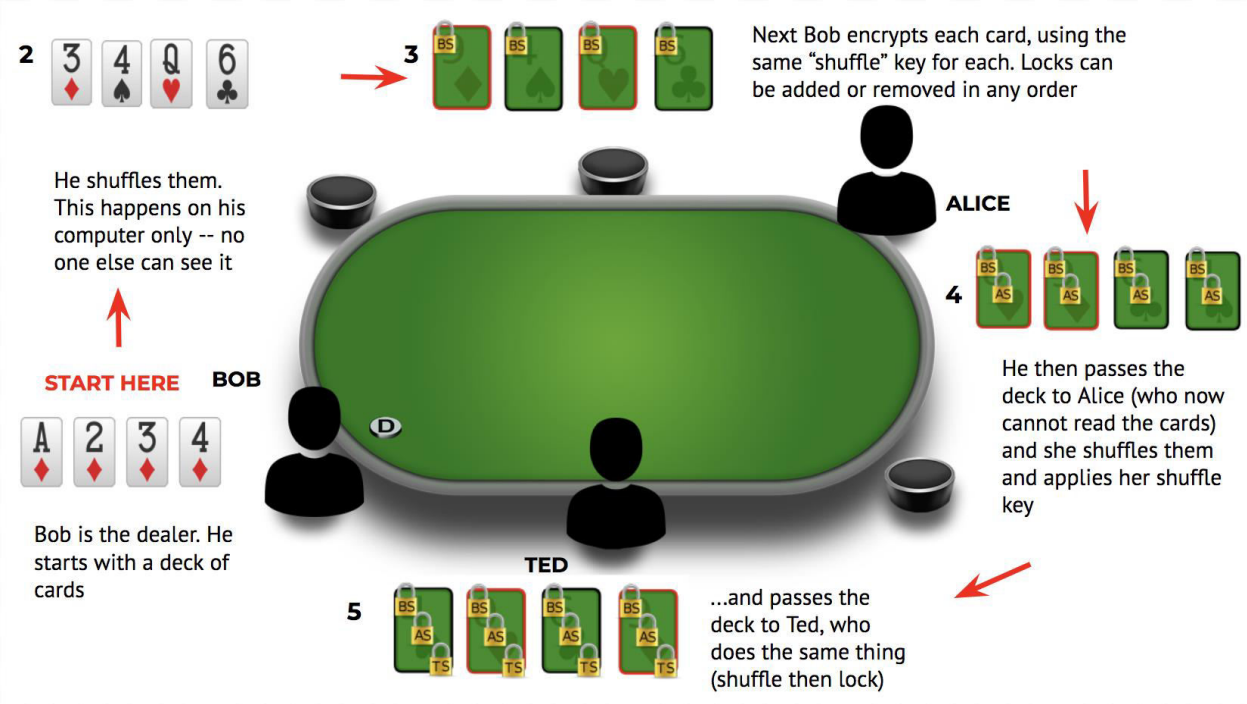
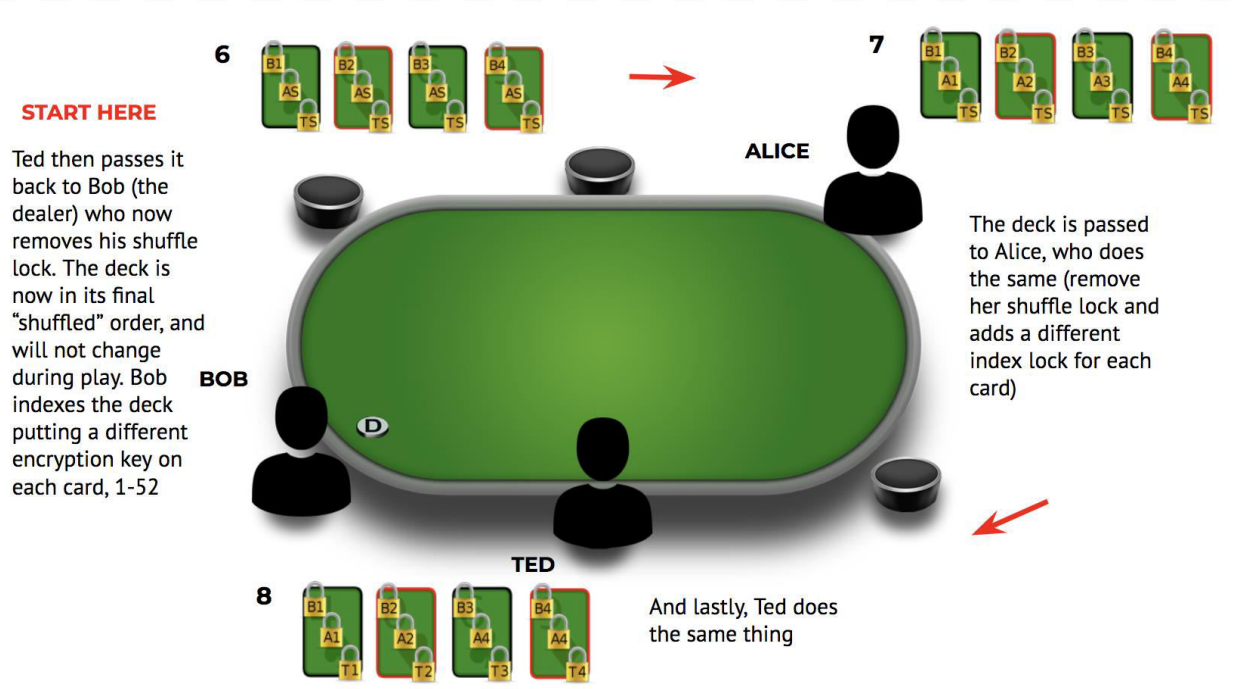


Abbildung 7: Indizierung des Kartensatzes

[17] Die vier Karten in den Abbildungen 6 und 7 sollen nicht Karten einzelner Spieler, sondern einen vollständigen Satz von 52 Karten darstellen



3.5.4 Entschlüsselung und Spielverlauf

Abbildung 8: Austausch von Schlüsseln zwischen den Spielern

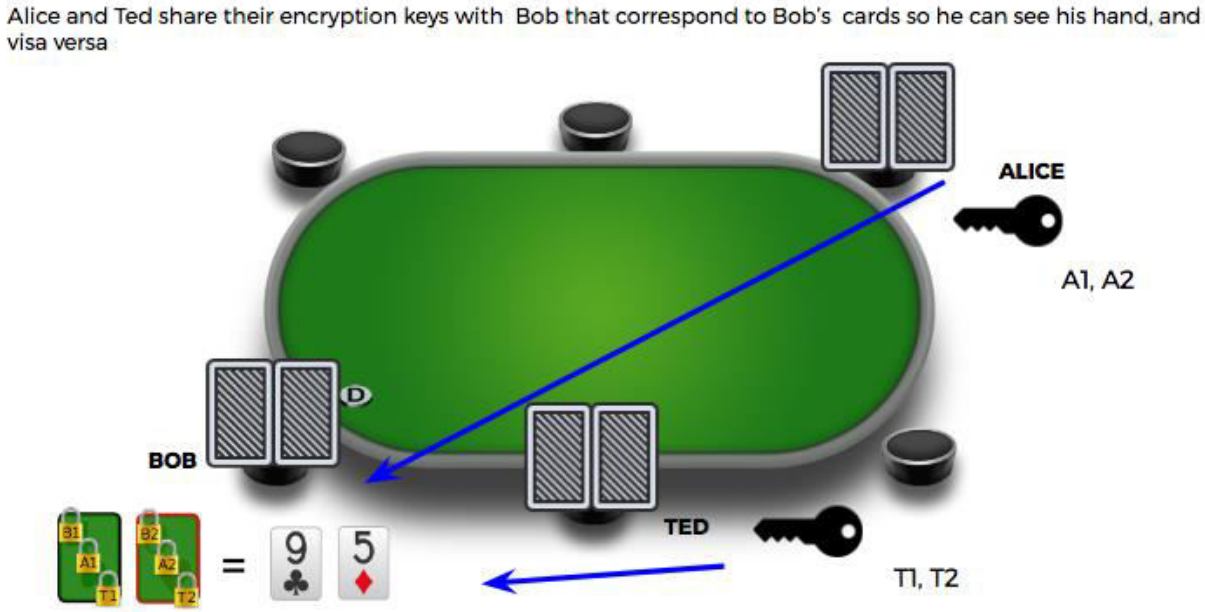


Abbildung 9: Gemeinschaftskarten[18]

[18] Analog werden die Turn- und die River-Karte jeweils nach Beendigung der Flop- bzw. Turn-Setzrunde aufgedeckt.

Dieser Vorgang läuft quasi hinter den Kulissen ab – aus Spielersicht unterscheidet sich das Spielgefühl auf der Virtue-Poker-Plattform nicht wesentlich von der Spielerfahrung, die sie von anderen Online-Plattformen kennen.

3.6 Peer-to-Peer-Messaging

3.6.1 P2P-Messaging zum Synchronisieren des Spiel-Clients

Das „Mental Poker"-Prinzip ermöglicht zwar die gemeinsame Nutzung eines Kartensatzes durch Spieler in einem Peer-to-Peer-Netzwerk – einschließlich Austeilen und Geheimhalten der Karten –, ohne dass ein zentraler Server erforderlich ist. Zur Bereitstellung eines praxistauglichen, verbraucher-orientierten Poker-Angebots sind darüber hinaus jedoch weitere Technologien notwendig.
Die herunterladbare clientseitige Spiel-Software besteht aus separaten Front-End- und Back-End-Prozessen, wobei das Back End dem lokalen Nutzer den jeweils aktuellen Spielzustand anzeigt sowie ggf. Eingaben annimmt und an das Back End weiterleitet, die dann von dort aus an die anderen am Spiel beteiligten Clients weitergegeben werden. Das Back End enthält die erforderliche Logik zur Anwendung der Spielregeln auf die Eingaben zu Ereignissen, die es vom Front End und von anderen erhält. Auf diese Weise wird gewährleistet, dass alle Clients denselben Code auf dieselben Daten anwenden.

3.6.2 Off-Chain-Transaktionen im Spielverlauf

Eine programmierbare Blockchain-Technologie wie Ethereum stellt eine fälschungssichere Datenspeicher-Lösung für Vorgänge bereit, die ansonsten allenfalls mithilfe eines Single-Server-Konzepts bewältigt werden könnten, wie etwa die Verwaltung der Spieler an einem bestimmten Tisch. Dadurch dass die Client-Software auf der Blockchain mit Smart Contracts interagieren kann, wird zudem die verteilte Verwaltung der

Spielmittel und Tischeinsätze sowie die fälschungssichere Dokumentation dieser Interaktionen möglich, wobei das Erfordernis einer vertrauenswürdigen dritten Partei wegfällt. Jedoch kann die Blockchain nicht in sämtlichen Aspekten des Spielverlaufs einen Server ersetzen, und zwar schon allein deshalb nicht, weil die Verteilung von Daten und Anweisungen von einer clientseitigen Anwendung über das Blockchain-Netzwerk im besten Fall mehrere Sekunden dauert. Zur Verwaltung von feingranularen Spielereignissen unterhalb der Handebene ist sie daher ungeeignet.

Spielereignisse, die schneller ausgeführt werden müssen, wie etwa die Wettvorgänge, müssen von der Client-Software selbst verwaltet werden – oder genauer gesagt, von der Software, die das Peer-to-Peer-Subnetz verwaltet, das von den Spielern an einem bestimmten Tisch gebildet wird. Durch Verwendung digitaler Signaturen kann jeder Client überprüfen, dass die bei ihm eingegangenen Nachrichten tatsächlich von dem angegebenen Absender stammen. Auf diese Weise werden Fälschungen verhindert. Durch Einsatz fehlertoleranter Methoden zur Konsensbildung wird sichergestellt, dass bei jedem einzelnen Schritt im Spielverlauf zwischen allen beteiligten Clients Einigkeit über alle Ereignisse besteht. Dadurch werden nicht nur Funktionsstörungen und Geräteausfälle, sondern auch byzantinische Fehler (absichtlich irreführende Informationen) erkannt.

Am Ende jeder Hand werden diese Konsensdaten, die digital von jeder clientseitigen Anwendung signiert wurden, zur Verarbeitung an die Blockchain übergeben. Die Clients selbst gehen zur nächsten Hand über. Streitigkeiten zwischen den am Spiel beteiligten Clients bzw. Peers werden von Schlichtern beigelegt (siehe Abschnitt 4.2).

3.7 IPFS: Hinterlegung von Spielprotokollen für Handverläufe

Zwecks der dauerhaften Dokumentation des tatsächlichen Spielverlaufs jeder einzelnen Hand müssen sowohl die signierten Nachrichten über Spielereignisse als auch die von der Blockchain bei der Verarbeitung des Handendes erfassten Zustandsinformationen gespeichert werden. Hierin liegt eine zweite Schwachstelle der aktuell verfügbaren Blockchain-Technologie: Die Speicherung umfangreicher Daten auf der Blockchain kann mit einem hohen Aufwand an Ressourcen verbunden sein, sodass sich die Hinterlegung dieser Protokolle auf der Blockchain als nicht praktikabel erweist.

Glücklicherweise stehen Technologien wie das Interplanetary File System (IPFS) zur Verfügung, die eigens zur Bereitstellung zuverlässiger verteilter Speichersysteme entwickelt wurden. Bevor am Ende einer Hand die Berichterstattung an die Blockchain erfolgt, übermittelt die Client-Software die protokollierten Daten an das IPFS, das diese mit einem eindeutig identifizierbaren Hash-Wert versieht, anhand dessen sie sich jederzeit wieder auffinden lassen. Dieser Hash-Wert wird gemeinsam mit den Spielstandsdaten an den Blockchain-Contract übergeben. Dabei ist in den Protokolldaten zu jeder Hand der Hash-Wert des Protokolls der vorherigen Hand enthalten. Somit kann durch Anforderung des letzten Hash-Werts von der Blockchain der gesamte protokollierte Verlauf des Spiels rekonstruiert werden. Singuläre Fehlerstellen, wie sie in verschiedenen Formen von zentralen Speichersystemen vorkommen, werden auf verteilten Speichersystemen vermieden.

4. Sicherheit beim Spielen

4.1 Betrugsmethoden beim Online-Poker

4.1.1 Absprache

Als Absprache wird die Kooperation zwischen zwei oder mehr Spielern an einem Tisch definiert, die Informationen austauschen und Kooperationsstrategien anwenden mit dem Ziel, sich einen Vorteil gegenüber anderen Spielern zu verschaffen.

4.1.2 Mehrfachkonten

Ein einziger Spieler kann sich an einem oder mehreren Computern mit mehreren Konten gleichzeitig am selben Spiel beteiligen und sich dadurch bei Turnieren oder Bargeldspielen einen unfairen Vorteil verschaffen.

4.1.3 Data-Mining

Spieler geben bisweilen Handverläufe, Spielernotizen und andere Daten über andere Spieler weiter. Solche Daten werden gesammelt und verschaffen den betreffenden Spielern einen Vorteil gegenüber ihren Mitspielern.

4.1.4 Poker Bots

Wie oben beschrieben, handelt es sich um Software-Programme, die ohne menschliche Beaufsichtigung an Pokertischen mitspielen können. Sie werden teils serienmäßig, teils als nutzerspezifische Sonderanfertigungen hergestellt.

4.1.5 Gemeinsame Kontonutzung (Account-Sharing)

Gemeinsame Kontonutzung bedeutet, dass zwei oder mehr Spieler dasselbe Konto verwenden, um sich unlautere Vorteile gegenüber der Poker-Plattform und anderen Mitspielern zu verschaffen. Dies gilt beispielsweise, wenn Poker-Plattformen etwa beim Rakeback höhere Anteile auszahlen, je öfter ein Spieler spielt bzw. je mehr er als Hausanteil einzahlt. Zudem kann es zu unlauteren Machenschaften gegenüber anderen Mitspielern kommen, indem beispielsweise ein Konto mitten im Turnier verkauft wird oder ein starker Spieler das Konto eines Spielers nutzt, der als schwächer bekannt ist.

4.2 Das Schlichter-System zum Bekämpfen von Betrug

Virtue hat ein Schlichter-System zur Bekämpfung von Absprachen und Betrug entwickelt. Schlichter sind nicht am Spiel beteiligte Schiedsrichter, die den Pokertischen nach dem Zufallsprinzip zugeteilt werden. Sie dienen der Sicherheit und dem Schutz der Spieler im Virtue-Poker-Netzwerk und werden für ihre Leistungen bezahlt. Schlichter sind als Validator Nodes im Virtue-Poker-Netzwerk zu verstehen, die jede Transaktion für jede Hand auf der Plattform signieren und Handverläufe zur Speicherung im IPFS hinterlegen. Schlichter werden automatisch nach einer bestimmten Anzahl von Händen rotiert.
Die oben beschriebenen Funktionen sind automatisiert; zum Betreiben eines Schlichter-Nodes ist keine manuelle Beaufsichtigung erforderlich.

4.2.1 Hauptaufgaben der Schlichter

Schlichter erfüllen im Virtue-Poker-Netzwerk drei Hauptaufgaben:

4.2.2.1 Schlichtung

In dem seltenen Fall, dass am Ende einer Hand oder eines Spiels zwischen den Peers an einem Tisch Uneinigkeit über den jeweiligen Spielstand oder -ausgang herrscht, legt ein Schlichter den Streit in Echtzeit bei und spricht den Pott dem Gewinner zu.

4.2.2.2 Datenfeed

Jeder Schlichter hinterlegt jeden einzelnen Spielvorgang in jeder Hand im IPFS, damit Handverläufe gespeichert werden können. Dies dient der Erfüllung regulatorischer Auflagen sowie der Unterstützung entscheidender Leistungen wie Aufdeckung von Absprachen, Bot-Erkennung und Identifizierung von Mehrfachkonten.

4.2.2.3 Teilweise Speicherung von Spieler-Schlüsseln

Das Problem des „ausgeschiedenen Spielers“ als Sonderfall innerhalb des „Mental Poker“-Protokolls tritt dann ein, wenn ein Spieler vor Beendigung der Hand aus dem Spiel ausscheidet. Dies ist insofern problematisch, als die Hand erst zu Ende ist, wenn alle Spieler ihre Schlüssel den anderen mitgeteilt haben, damit die Gemeinschaftskarten entschlüsselt werden können. Unter Anwendung des von Adi Shamir entwickelten „Secret Sharing“-Verfahrens lassen sich die Karten sämtlicher Mitspieler verschlüsseln und auf alle Spieler sowie den Schlichter aufteilen. Wenn ein Spieler aus beliebigem Grund ausscheidet, kann der Schlichter die entsprechenden Schlüsselteile von den übrigen Spielern anfordern und zur Entschlüsselung zusammensetzen, sodass die Hand beendet werden kann.

Die Aktivierung eines Schlichter-Nodes auf der Virtue-Poker-Plattform erfolgt durch Herunterladen des Schlichter-Clients auf einen Rechner, Öffnen der Anwendung und Aktivierung des Schlichters. Eine detallierte Beschreibung des Schlichter-Systems entnehmen Sie bitte Abschnitt 5.1.

5. VPP: Virtue Player Points

Virtue Player Points (VPP) haben innerhalb des Virtue-Poker-Netzwerks hauptsächlich drei Verwendungszwecke: (1) Sie können als Spielwährung verwendet werden. (2) Sie können als Pfand in einem als Schlichter-Registrierungsdatenbank bezeichneten Smart Contract eingesetzt werden, anhand dessen Nutzer innerhalb des Netzwerks Tokens einsetzen und Hände validieren können und dafür ein Honorar erhalten. (3) Sie können zur Teilnahme an Sonderturnieren eingesetzt werden.

5.1 Voraussetzungen für die Spielteilnahme als Schlichter

Dem Schlichter-Pool gehört eine begrenzte Anzahl von Nutzern an, die im Virtue-Poker-Netzwerk aktiv sind. Um als Schlichter einem Tisch zugewiesen zu werden, müssen Nutzer (a) VPP erwerben, (b) Tokens in der Schlichter-Registrierungsdatenbank einsetzen und (c) den Computer eingeschaltet sowie die Virtue-Poker-Anwendung geöffnet und auf *aktiv* gestellt haben.

5.1.1 Verfahren zur Überprüfung der Schlichtereingaben

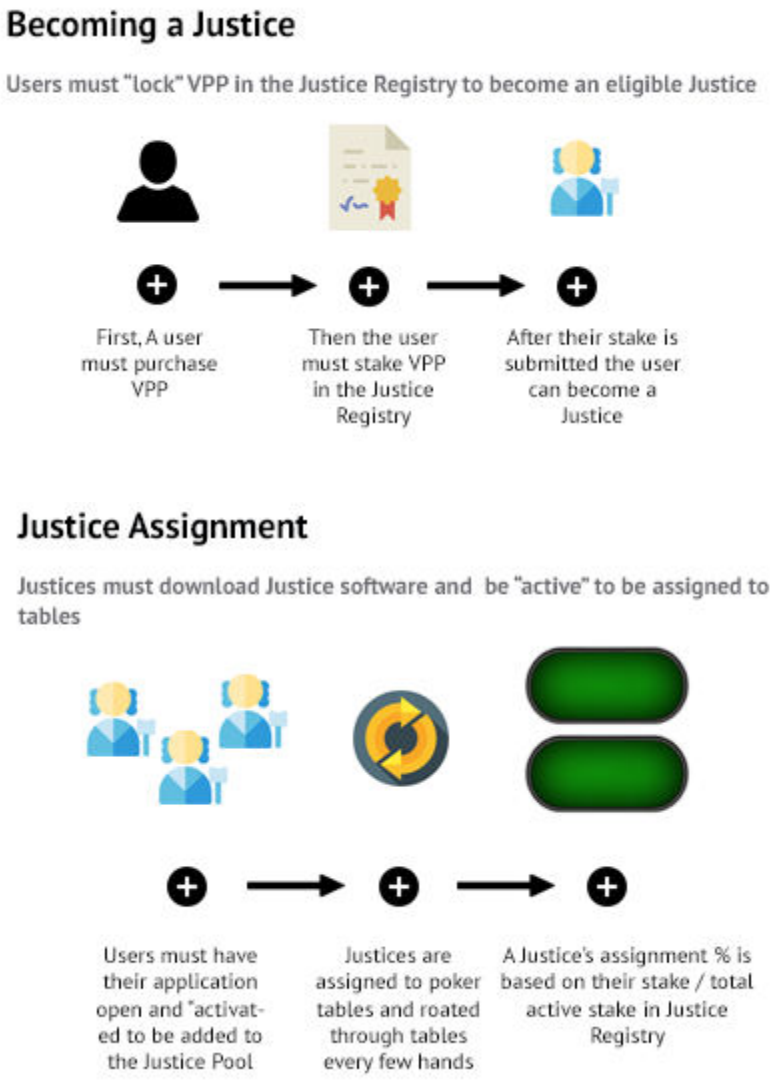
Eingaben von Schlichtern an das IPFS werden zunächst von einem Team aus Sicherheitsexperten geprüft. Dem Virtue-Poker-Team gehört ein Experte für Spielintegrität und -sicherheit an, der unser Entwicklungsteam beim Aufbau des Schlichter-Systems und Einsatz geeigneter Software-Programme zur Erkennung von Warnsignalen auf der Plattform unterstützt.

Betrugsvorwürfe können auf zwei unterschiedlichen Wegen bei dem für Sicherheit beim Spielen zuständige Team erhoben werden. Spieler können Beschwerden über verdächtige Vorgänge einreichen. Diese Beschwerden werden geprüft, um zu entscheiden, ob der Sachverhalt des Betrugs erfüllt ist. Darüber hinaus werden die von Schlichtern hinterlegten Daten ständig anhand von Algorithmen überwacht und sämtliche verdächtigen Vorgänge manuell überprüft. Wird ein Betrug festgestellt, so wird gegen den betreffenden Spieler eine Strafe verhängt. In schweren Fällen kann der Spieler auf Dauer von der Plattform ausgeschlossen werden.

5.1.2 Schlichter-Honorare

Die auf der Virtue-Poker-Plattform generierten Schlichter-Honorare werden zwischen den aktiven Schlichter-Nodes im Virtue-Poker-Netzwerk aufgeteilt. Die Gutschrift von Honoraren erfolgt in VPP und ETH. Das Schlichter-System wird in Abbildung 10 veranschaulicht.

Abbildung 10: Schlichter-System

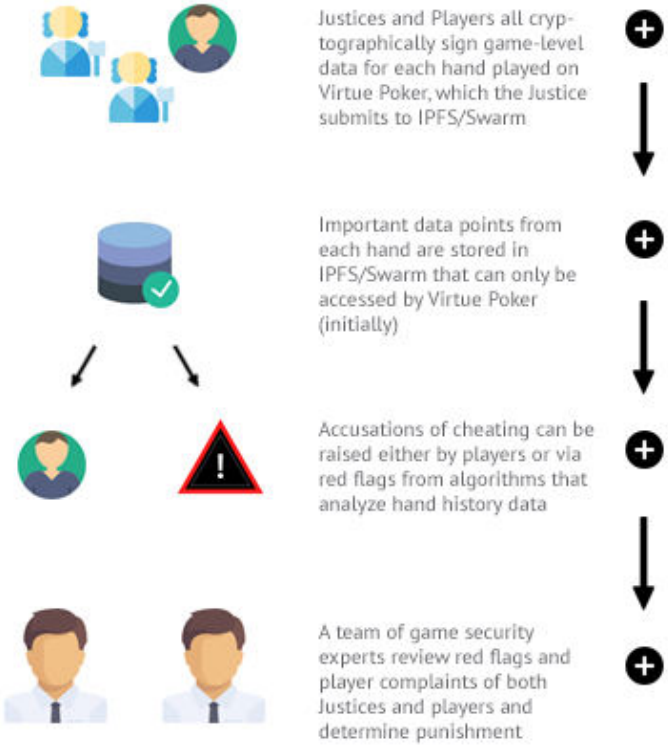


Justice Functions

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.



VIRTUE POKER

5.2 Spielwährung

Virtual Player Points (VPP) können als Spielwährung verwendet werden. Spieler können sich für die Teilnahme an Spielen entscheiden, die in VPP ausgeschrieben sind, um so ihren relativen Anteil an VPP im Verhältnis zu anderen Nutzern zu erhöhen.

5.3 Sonderturniere

Für bestimmte Turniere und Spiele ist der Einsatz von VPP erforderlich; Gewinne können in VPP oder ETH beansprucht werden. Insbesondere fallen darunter Turniere mit garantiertem Preispool, Freerolls und Sonder-Satellitenturniere.

6. Weitere Planung

6.1 Hauptaktivitäten

6.1.1 Plattformentwicklung

Das Team von Virtue Poker arbeitet bereits seit knapp drei Jahren an der Entwicklung unseres Systems. Der Aufbau einer Plattform im vollen Funktionsumfang wird einen Ausbau unseres Entwicklungsteams erforderlich machen. Virtue Poker plant die Einstellung von Entwicklern zur Verbesserung unseres P2P-Messaging-Backbone, Gestaltung individualisierbarer Benutzeroberflächen, Optimierung unserer Smart Contracts und Implementierung von Speicherfunktionen. Darüber hinaus soll die Koordination mit laufenden Ethereum-Infrastruktur-Projekten – hierzu zählen verteilte Speichersysteme, Identitätsverwaltung und Stable Coins – verstärkt werden.

6.1.2 Community-Wachstum

Virtue Poker wird mit etablierten Anbietern in den Wettbewerb treten, die über hohe Budgets verfügen und ausgefeilte Verfahren zur Kundenakquise entwickelt haben. Wir planen beträchtliche Ressourcen für den Auf- und Ausbau eines globalen Netzwerks für alle diejenigen aufzuwenden, die am Erfolg einer dezentralen Poker-Plattform interessiert sind. Konkret haben wir vor, unseren Nutzern mehr Mitspracherechte zuzugestehen, Turniere mit garantiertem Preispool und Freerolls auszurichten sowie durch Rakebacks, Datenanalyse und ähnliche Initiativen Vertrauen zu bilden.

6.1.3 Sponsorships und Öffentlichkeitsarbeit

Virtue Poker wird Poker-Foren, Websites, Blogs und Veranstaltungen sponsern, die bei Spielern beliebt sind. Zudem wird unser Team zur Vermittlung des Nutzenversprechens unserer Plattform an ein breites Publikum eine aggressive PR-Strategie verfolgen.

6.1.4 Rechtsbelange

Unserem Team stehen angesehene Anwaltskanzleien wie DLA Piper, ISOLAS und Ifrah Law, die sich auf einschlägige Rechtsfragen im Bereich Glücksspiel spezialisiert haben, als Rechtsberater zur Seite. Zudem halten wir bei der Umsetzung gesetzlicher und behördlicher Auflagen mit Aufsichtsbehörden in aller Welt Rücksprache. Durch den Erwerb einer Glücksspiellizenz im Vorfeld der Markteinführung soll sichergestellt werden, dass unsere Plattform sämtliche geltenden Compliance-Anforderungen erfüllt und die Spieler ausreichend geschützt sind.

6.2 Entwicklungsplan

6.2.1 Aktueller Stand

In den zwei Jahren seit der Erarbeitung des Konzepts für Virtue Poker im Mai 2015 wurde ein Prototyp entwickelt.

Unsere Anwendung wird seit ihrer Entwicklung wöchentlich getestet. Unser Team veranstaltet interne Spiele mit einer Implementierung des „Mental Poker“-Protokolls, die auf den Ethereum-Testnets läuft.

Bei der ersten Version von Virtue Poker handelt es sich um eine clientseitige Python-Anwendung, die auf dem Desktop der Nutzer läuft und für jede Tischinstanz einen individuellen Smart Contract erstellt. Unserem Team ist es gelungen, ein „Mental Poker“-Protokoll zum Kartenmischen sowie eine Spiel-Engine zu implementieren. Bei der Spiel-Engine handelt es sich um eine Zustandsmaschine, die über ein P2P-Messaging-Protokoll eine Verbindung zu anderen Spielern herstellt und sich in die Ethereum-Blockchain einhängt, sobald Spieler einen neuen Tisch anlegen bzw. einen bereits bestehenden Tisch auswählen. Aktuell bewältigt unsere Anwendung Spiele mit maximal sechs Spielern bei einer Geschwindigkeit von 70 bis 80 Händen pro Stunde. Das entspricht dem Standard der bisherigen Online-Poker-Netzwerke.

6.2.2 Weiterentwicklung

Das Kernteam von Virtue Poker steht bereits. Der weitere Auf- und Ausbau unseres Teams sowie der Virtue-Poker-Plattform soll im Wege der Eigenfinanzierung erfolgen. Unter anderem ist die Umgestaltung der Desktop-Anwendung zu einer Electron-Anwendung vorgesehen. Um den langfristigen Erfolg unserer Plattform zu gewährleisten, sind umfangreiche Testmaßnahmen erforderlich. Dabei muss sichergestellt werden, dass die Spiele den Kriterien der Fairness genügen, dass die zur Anmeldung und Identitätsprüfung angewandten Methoden robust genug sind, um Mehrfachkonten auf niedrigem Niveau sowie die Teilnahme Minderjähriger zu verhindern, und dass unser Mechanismus zur Datenspeicherung die Nachverfolgung von Datenpunkten im Rahmen der geltenden Compliance-Auflagen sowie der Betrugserkennung ermöglicht.

Verbesserung des P2P-Messaging-Backbone
Zur Ausführung unterschiedlicher Transportfunktionen kommen Plug-in-Implementierungen zum Einsatz, die bei laufendem Betrieb austauschbar sind. Die Verteilung von Nachrichten erfolgt mithilfe eines sehr einfach aufgebauten Message Exploders. Vor der kommerziellen Installation der Plattform soll noch ein robusterer Backbone eingebaut werden.

Schlichter-Implementierung
Dadurch dass im Beisein von einem oder mehreren Schlichtern gespielt wird, kann der Spielverlauf auf Peer-Ebene dauerhaft offline im IPFS archiviert werden. Damit ist eine wichtige Voraussetzung zur Erkennung von Absprachen oder Bot-Spielen erfüllt.
Ebenso lässt sich ggf. nachträglich nachweisen, dass bei dem betreffenden Spiel alles mit rechten Dingen zuging. Im Gegensatz zu anderen Konsensmechanismen, die für 51-Prozent-Attacken anfällig sind, wird durch Beisein eines Schlichters verhindert, dass zwei Spieler mit gehackten Anwendungen in einem Dreierspiel den dritten Mitspieler betrügen.

Front End in handelsüblicher Qualität
Noch bevor die Nutzertests in die erste Runde gehen, soll die grafische Oberfläche unserer aktuellen Anwendung neu gestaltet und eine Benutzeroberfläche für unsere Lobby entwickelt werden.

6.2.3 Erstes Quartal 2018

Identitätsverwaltung

Zunächst ist die Integration eines Identitätsprüfungssystem eines Fremdanbieters vorgesehen (Näheres dazu unter https://www.hooyu.com/). Im weiteren Verlauf unserer Zusammenarbeit mit Aufsichtsbehörden weltweit wollen wir die Vorteile von Anwendungen wie uPort thematisieren, die auf dem Prinzip der Self-Sovereign Identity beruhen. Auf Dauer ist die Umstellung unseres Anmeldeverfahrens auf eine dezentrale Lösung geplant.

Datenspeicherung
Schlichter-Nodes werden zur Erfassung und Speicherung des Spielverlaufs auf Hand-Ebene eingesetzt. Es ist vorgesehen, Handverläufe im IPFS zu hinterlegen und die entsprechenden Daten im Tisch-Contract mit einem Querverweis zu versehen. Für die Alpha-Version soll dabei zunächst ein zentraler Mechanismus zur Datenspeicherung zum Einsatz kommen.

6.2.4 Zweites Quartal 2018

Private Alpha-Testphase
Zwecks Fehlerbehebung und Einholen von Feedback zur Verbesserung der Benutzeroberfläche und -erfahrung wird eine private Testphase durchgeführt. Zur Teilnahme an der Alpha-Phase werden Nutzer eingeladen, die sich an der Token-Verkaufsaktion von Virtue Poker (Phase 1) beteiligt haben.

Vorab-Premiere
Virtue Poker plant die Ausrichtung einer Vorab-Premiere mit bekannten Pokerprofis aus der Online-Community sowie der Live-Szene. Es ist vorgesehen, diese Veranstaltung in Echtzeit auf Twitch zu streamen.

6.2.5 Zweites/Drittes Quartal 2018

Rakeback-Mechanismus
Abhängig von den Ergebnissen der laufenden Nutzertests ist die Implementierung eines tokenisierten Rakeback-Mechanismus mit VPP vorgesehen.

Ausbau der Kapazitäten für Turniere mit mehreren Tischen
Der Contract für Turniere mit mehreren Tischen verwaltet die Teilnahme bestimmter Tische am Turnier sowie die Zuweisung von Spielern an die jeweiligen Tische. Zudem werden darüber Verlauf und Ausgang des Turniers verwaltet – wer gewinnt und wie viel. Während des Spielverlaufs fungiert der Tisch auch hier als Einheit im P2P-Subnetz, kommuniziert aber darüber hinaus mit dem Contract für Turniere mit mehreren Tischen.

Eingeschränkte Freigabe von Virtue Poker (Öffentliche Beta-Version)
Mit der öffentlichen Beta-Version können Nutzer aus aller Welt Ein-Tisch- bzw. „Sit & Go“-Turniere und Bargeldspiele beginnen bzw. daran teilnehmen.

6.2.6 Viertes Quartal 2018

Turnier zur Markteinführung von Virtue Poker
Zur Markteinführung von Virtue Poker wird mindestens ein Turnier mit garantiertem Preispool ausgeschrieben, bei dem Nutzer aus aller Welt Gelegenheit erhalten, auf der Plattform zu spielen.

6.2.7 2019

Einbeziehung von Fremdbetreibern
Virtue Poker wird Fremdbetreibern und Lizenznehmern weltweit die Möglichkeit geben, eigene unternehmensspezifische Skins auf unserer Plattform zu entwickeln und unsere Infrastruktur zur

Entwicklung eigener Spiele zu nutzen. Dies wird uns eine schnellere Hochskalierung auf einen für Spieler attraktiven Liquiditätsgrad ermöglichen.

7. Team

Kernteam

Jim Berry, Lead Platform Developer: Jim Berry ist seit mittlerweile 30 Jahren als Softwareentwickler tätig und hat an den verschiedensten Projekten mitgewirkt: vom Bodensystem für das Hubble-Weltraumteleskop über die Applikation zur Verarbeitung der Forschungsdaten aus der Framingham-Herz-Studie bis hin zu Linux-Treibern für ein System zur Erfassung von Luftaufnahmen und der Installation von technologisch angemessenen E-Mail-Systemen für Entwicklungsländer im Südpazifik. Sein eigentlicher beruflicher Schwerpunkt jedoch ist die Arbeit an physischen Simulationen und Grafiken für Computerspiele – u. a. für MicroProse, Looking Glass Technologies und Electronic Arts.

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: Der kometenhafte Aufstieg von PokerStars vom unbekannten Startup zur größten Online-Poker-Plattform der Welt mit über 100 Millionen Spielern zählt zu den unbestrittenen Höhepunkten in Dan Goldmans über 20-jähriger Laufbahn als Spezialist für Online-Marketing. Vor dem Wechsel zu PokerStars leitete Goldman die Abteilung Marketing bei einem der größten Preisvergleichsportale bis zu dessen Übernahme durch Experian. Er gehörte dem Team an, das die objektorientierte Programmierung marktfähig machte und den Aufstieg von Digitalk vom Startup zum Branchenführer mit der Programmiersprache Smalltalk/V begleitete. Damit nicht genug, war Goldman in führender Rolle für die Entwicklung und Einführung einer Online-Glücksspielplattform für eins der größten Casinos in den USA verantwortlich.

Javier Franco Algarrada, Blockchain Development Team Lead: Javier Franco Algarrada bringt über 10-jährige Erfahrung als Softwareentwickler mit. Besonders gerne arbeitet er an Full-Stack-Anwendungen, bei denen er nicht nur verschiedene Technologien einsetzen, sondern sich auch aktiv in den gesamten Entwicklungszyklus des Produkts einbringen kann. Er hat bereits mehrere Fachprojekte erfolgreich geleitet und übernimmt nun die Leitung des für die Entwicklung von Virtue Poker zuständigen Teams. Franco Algarrada ist mittlerweile seit über sieben Jahren im Glücksspiel-Bereich tätig und hat an unterschiedlichen Produkten von Lotterien über virtuellen Sport, Casino-Spiele und Sportwetten

mitgewirkt. Technische Innovationen haben ihn schon immer fasziniert, und aus ebendiesem Interesse heraus wechselte er im vergangenen Jahr zur Blockchain-Technologie über. Franco Algarrada hat einen Bachelor-Abschluss in Computerwissenschaften und einen Master in Webentwicklung.

Catalin Dragu, Design: Catalin Dragu ist seit 2010 als Spezialist für Digital Design tätig. Aktuell arbeitet er gemeinsam mit ConsenSys an der Gestaltung spannender und ansprechender dezentraler Anwendungen. Er ist fest davon überzeugt, dass gutes Design der Seele gut tut, und bemüht sich entsprechend, den Endkunden ein Nutzererlebnis zu bieten, das so angenehm ist wie ein Spaziergang im Park.

Jose Diaz, Head of Product: Im Laufe seiner über 18-jährigen Tätigkeit in der Glücksspielbranche hat Jose Diaz als CTO, Leiter Produktentwicklung, Softwareentwickler und IT-Beauftragter vielfältige Erfahrung in den Bereichen Innovation und Unternehmensführung gesammelt. Er hat BWL und Computerwissenschaften studiert, verschiedene renommierte Projekte erfolgreich zum Abschluss gebracht und seine Kompetenz immer wieder durch die Planung neuer Entwicklungsstrategien für neue Plattformen, starke Teamführungsqualitäten und den Aufbau wichtiger Kundenbeziehungen unter Beweis gestellt. Für den Wechsel zu Virtue Poker war vor allem die Chance zur Nutzung innovativer Technologie ausschlaggebend.

Colum Higgins, Senior Product Manager: Colum Higgins kommt ursprünglich aus der Physik und promovierte Anfang der 1990er Jahre am CERN. Anschließend war er 10 Jahre lang in verschiedenen Fachpositionen in der Entwicklung von Hochleistungsrechnern, als Middleware-Berater für Enterprise sowie dreieinhalb Jahre lang als Gründer eines Tech-Startups und CTO tätig, setzte schließlich noch ein BWL-Studium drauf und wechselte 2003 nach China. Dort entwickelte er ein 3G-Vorführsystem für Ericsson und wirkte im Auftrag verschiedener Regionalregierungen und der Europäischen Union an Projekten zur Digitalisierung der Verwaltung mit. 2007 stieg Higgins bei Full Tilt Poker als Programmdirektor und Unternehmensanalyst ein. Er war federführend für die Umsetzung mehrerer Großprojekte wie der Neuprogrammierung des Spiel-Client, die Zulassung in Frankreich, die Einführung von Anfängertischen und Turniertickets verantwortlich.

Daniel Ortega, Back-End Developer: Daniel Ortega arbeitet seit 12 Jahren als Softwareentwickler. Vom Tiefbau bis zur Luftfahrt hat er bereits in den verschiedensten Branchen Erfahrung gesammelt und zwischendurch auch schon in der Glücksspielsparte Praxisluft geschnuppert. Ortega reizt immer wieder gerne die Grenzen seiner Wohlfühlzone aus und nutzt jede Chance, sich mit brandneuen Technologien zu beschäftigen.

Alvaro Rodríguez Villalba, Front-End Developer: Der Full-Stack-Javascript- und Android-Entwickler sammelte Erfahrung als Mitgründer des Startups Kultur, wo er für den Bereich Web- und Android-Entwicklung zuständig war. Unter anderem arbeitete er mehr als zwei Jahre lang am Aufbau einer Web-Anwendung zur Simulation von Satellitenverbindungen. Als freiberuflicher Entwickler baute er zudem mehrere JS-basierte Plattformen auf. Rodríguez Villalba absolvierte 2017 das „ConsenSys Academy“-Programm für Ethereum-Entwickler.

Lucas Cullen, Blockchain Platform Developer: Der Full-Stack- und Solidity-Entwickler Lucan Cullen kommt ursprünglich aus der Mathematik und arbeitete dann für Startups und Banken. Er kam 2011 erstmals mit Bitcoin in Kontakt, schürft seitdem begeistert mit und ist jederzeit gerne bereit, seine Mitmenschen von den Vorteilen der Kryptowährung zu überzeugen. Beim Projekt Ubin in Zusammenarbeit mit Accenture und der singapurischen Finanzaufsichtsbehörde konnte Cullen das Ethereum-Produkt Quorum von JP Morgan zum Einsatz bringen. Zuvor war er Inhaber und Geschäftsführer einer Software-Beratungsfirma, die Leistungen im Bereich Schulung und Softwareentwicklung für Bitcoin- und Blockchain-Projekte erbrachte. Er ist Organisator der Versammlungen der Bitcoin-Gemeinde im australischen Brisbane, sitzt im Vorstand von Blockchain Australian und ist Australiens Coloured-Coin-Botschafter.

7.2 Berater

Joseph Lubin: Joe Lubin hat in seiner bisherigen Laufbahn unterschiedliche Funktionen in den Bereichen Technologie und Finanzwesen bzw. an der Schnittstelle zwischen beiden ausgeübt. Sein Studium in den Fächern Elektronik und Computerwissenschaften an der Universität Princeton schloss er mit der Auszeichnung *cum laude* ab. Anschließend arbeitet er als Forschungsmitarbeiter im Robotics Lab der Universität und später bei Vision Applications. Softwareentwicklung, Finanzen und Kryptografie bildeten die Schwerpunkte seiner Arbeit bei Goldman Sachs, als Berater für eMagine bei dem IdenTrust-Projekt sowie als Gründer und Verwalter einer Reihe von Hedgefonds, die er in Zusammenarbeit mit einem Partner betrieb. Als Mitgründer des Ethereum-Projekts und der Softwareschmiede ConsenSys ist Lubin seit Januar 2014 an der Entwicklung der Ethereum-Blockchain beteiligt.

James Slazas: James Slazas bringt mehr als 15 Jahre Erfahrung in der Finanzbranche mit. Er war im Arbitragegeschäft mit Derivaten im Eigenhandel der Bank Lehman Brothers tätig und gründete dort einen Bereich für globales Risikomanagement zur Bewältigung der Risiko-Exposure durch hochvermögende Kunden in London, der Schweiz und Hongkong. Als Mitgründer eines Hedgefonds zur Verwaltung von Lebensversicherungspolicen sicherte er seinem Unternehmen in mehreren US-Bundesstaaten einen Status als bevorzugter Partner für die Einführung elektronischer Patientenakten und Abrechnungsleistungen für die Medicare- und Medicaid-Zentren sowie eine gemeinsame verbindliche Vereinbarung mit HCL America zur Bereitstellung von Verfahren zur Analyse von Daten zur Patientenunterstützung sowie Abrechnungsleistungen für medizinische Labore, Pflegeeinrichtungen, Privatpraxen und Krankenhäuser.

Patrick Berarducci: Patrick Berarducci ist Full-Stack-Softwareentwickler und arbeitet als Justitiar bei ConsenSys. Vor seinem Wechsel zu ConsenSys war er sieben Jahre lang bei der Kanzlei Sullivan & Cromwell LLP als Anwalt tätig und Mitgründer eines Startups im Bereich Gesundheitstechnik. Ganz besonders reizt ihn die Chance, seine vielfältigen Erfahrungen im juristischen, betriebswirtschaftlichen und IT-Bereich im Verbund mit Blockchain-Technologie zum Einsatz zu bringen und dadurch in Branchen, Märkten und Netzwerken kreative Störeffekte auszulösen.

Andrew Keys: Andrew Keys ist bei ConsenSys für die globale Geschäftsentwicklung zuständig. Aus seinen vorherigen Tätigkeiten als Aktienanalyst für die Investitionsbank UBS, Experte für den Vertrieb von Lebensversicherungsprodukten und Mitgründer eines auf Umsatzzyklus-Management spezialisierten Unternehmens bringt er Erfahrung in den Bereichen Kapitalmärkte, Technologie und Unternehmensführung sowie in der Arbeit mit Bitcoin und Ethereum mit. Die Förderung strategischer Technologie-Partnerschaften, Geschäftsentwicklung und Kommunikation bilden die Schwerpunkte seiner Arbeit bei ConsenSys. Darüber hinaus arbeitet der von ihm mitgegründete Unternehmensbereich ConsenSys Enterprise an der Entwicklung von Ethereum-Blockchain-Lösungen für Großkonzerne.

Robert Davidman: Robert Davidman war zuletzt als Interim-CMO beim Medienkonzern Ruby für die globale Marketing- und Digitalstrategie des innovativen Portfolios mit Marken wie Ashley Madison, Cougar Life und Established Men verantwortlich. Aktuell betreut er als Mitgründer und -inhaber der New Yorker Werbeagentur The Fearless Group die US- bzw. weltweite Marketingstrategie zahlreicher Spitzenmarken, darunter Kunden aus der Glücksspielbranche wie unter anderen Bwin.Party (PartyPoker), Pala Interactive (Palacasino.com, PalaPoker.com, Palabingousa.com), 888 Holdings (888.com), Lottoland.com. Seit 2001 hat Davidman als Marketing-Experte und Manager für verschiedene Online-Glücksspiel-Anbieter gearbeitet. Von 1999 bis 2001 leitete er bei Yahoo! die Abteilung International Broadcast Services und konnte im Rahmen seiner Tätigkeit die Streaming-Leistungen des Unternehmens außerhalb der USA und Kanadas in über 24 weitere Länder expandieren. Zuvor war Davidman von 1995 bis 1999 als 9. Mitarbeiter des Internetradiosenders Broadcast.com für die Vertriebs- und Marketingaktivitäten des Live-Streaming-Pioniers zuständig.

7.4 Team Virtue Poker

Phil Ivey: Phil Ivey ist mit 10 Turniersiegen gemeinsamer Zweiter unter den erfolgreichsten Spielern in der World Series of Poker und mit einem Gesamtverdienst von über 23 Millionen US-Dollar aus Live-Spielen Sechster in der Weltrangliste. Auch online zählt er mit einem Gesamtverdienst von über 10 Millionen Dollar zur absoluten Weltspitze. Dabei brilliert er in sämtlichen Formaten – in Turnieren ebenso wie in Bargeldspielen, im Live-Spiel genauso wie im Online-Spiel – und hält mit insgesamt neun Qualifikationen für den Final Table den Rekord für die meisten Finalteilnahmen bei der World Poker Tour. Im Zeitraum von 2002 bis 2009 erreichte Ivey viermal eine Platzierung unter den Top 25 im Main Event der World Series. 2017 wurde er ohne Gegenstimme in die WSOP Hall of Fame aufgenommen.

Dan Colman: Dan Colman erregte vor allem mit seinem Sieg über Daniel Negreanu beim Big One for One Drop (Mindesteinsatz: 1 Million US-Dollar) im Rahmen der World Series of Poker 2014 Aufmerksamkeit. Mit einem Gesamtverdienst von über 28 Millionen US-Dollar aus Live-Spielen belegt er in der Weltrangliste derzeit den 3. Platz.

Brian Rast: Brian Rast, der in der Online-Community besser als "tsarrast bekannt ist, konnte bislang drei Turniere in der World Series of Poker für sich entscheiden und steht dem Team von Virtue Poker nun als fachkundiger Berater zur Seite. Zu seinen weiteren Karriere-Höhepunkten zählt der Sieg beim mit 1.500 US-Dollar dotierten Pot-Limit Hold'em im Jahr 2011; außerdem ist er zweifacher Gewinner des

mit 50.000 US-Dollar dotierten Players Championship 2011 und 2016, wo er sich gegen Phil Hellmuth und Justin Bonomo durchsetzte. In der Weltrangliste liegt er mit einem Gesamtverdienst von über 20 Millionen US-Dollar aus Live-Spielen an 10. Stelle.

7.4 Rechtspartner

Ifrah Law PLLC (Rechtsberatung USA): Die Kanzlei Ifrah Law ist seit den Anfangszeiten der Branche auf Rechtsberatung im Bereich Online-Glücksspiel spezialisiert und zählt heute viele der größten einschlägigen Unternehmen und Branchenverbände zu ihren Mandanten. Sie war maßgeblich zahlreichen wichtigen Rechtsverfahren in diesem Bereich beteiligt. Unter anderem handelte Jeff Ifrah 2011 im Auftrag der Online-Anbieter Full Tilt Poker und PokerStars ein historisches Übereinkommen mit dem US-amerikanischen Justizministerium aus, das einen Meilenstein auf dem Weg zur Zulassung des Online-Glücksspiels in den USA darstellte. Ifrah Law wirkte zudem an der Schaffung gesetzlicher und behördlicher Rahmenwerke in Delaware, New Jersey und Nevada mit, den bislang einzigen US-Bundesstaaten, in denen Online-Glücksspiel zugelassen ist.

ISOLAS LLP (Rechtsberatung Gibraltar): ISOLAS ist eine Full-Service-Kanzlei mit Sitz in Gibraltar, die sich auf die Beratung internationaler Mandanten zur dortigen Rechtslage spezialisiert hat. Die 1892 gegründete Kanzlei, die jüngst ihr 125-jähriges Bestehen feiern konnte, ist nicht nur die älteste in Gibraltar, sondern auch eine der angesehensten und wurde für ihre exzellenten Leistungen zugunsten ihrer Mandanten bereits ausgezeichnet.

8. Anhang: Die Architektur von Virtue Poker

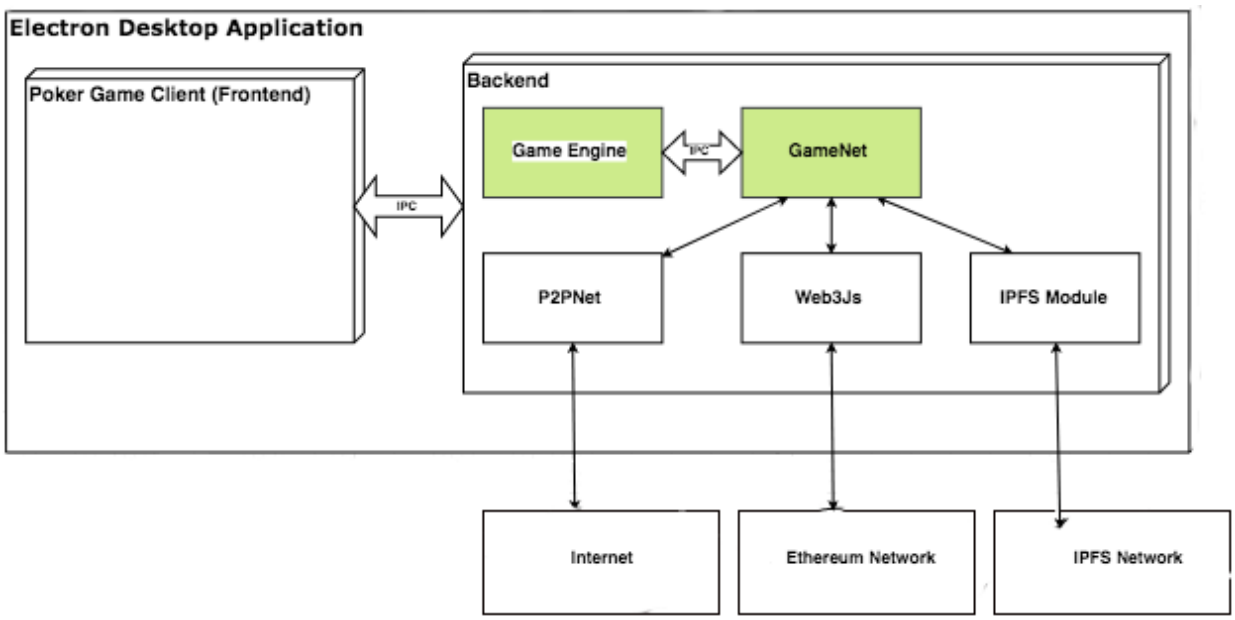
Virtue Poker befindet sich noch in der Entwicklung. Änderungen an den Angaben in diesem Abschnitt vorbehalten.

8.1 System-Architektur

Virtue Poker ist eine vollständig dezentrale Poker-Plattform. Dieses Ziel wird durch den Einsatz neuartiger Technologien wie Ethereum und IPFS sowie weiterer Lösungen realisiert.

Bei der Desktop-App von Virtue Poker handelt es sich um eine Electron-Anwendung für Desktop. Im Einzelnen besteht sie aus Spiel-Engine, clientseitiger Poker-Anwendung sowie der zur Kommunikation mit der Ethereum-Blockchain erforderlichen Infrastruktur und einem Peer-to-Peer-Subnetz für Spielinstanzen. Letzteres dient zur Unterstützung der Nachrichtenübermittlung mit geringen Latenzzeiten, die bei Online-Spielen mit menschlichen Teilnehmern erforderlich ist.

Abbildung 12: Architektur der Anwendung



8.1.1 Komponenten

Die Electron-Anwendung für Desktop besteht im Wesentlichen aus folgenden Komponenten:

- **Spiel-Engine:** Enthält die Spiellogik.
- **Ethereum:** Wird zum Hinterlegen von Spielparametern sowie für Treuhandleistungen, zur Berichterstattung über Spielergebnisse, tischübergreifenden Spielerverwaltung und Verwaltung von Schlichter-Contracts verwendet
- **GameNet:** Stellt eine einzige Komponente bereit, über die die Engine mit der Außenwelt kommuniziert
- **P2PNet:** Wird von GameNet zur Verwaltung eines spielinstanz-spezifischen P2P-Subnetz verwendet
- **Web3.js:** Die mit Ethereum kompatible JavaScript-API zur Implementierung von Kommunikation mit den Ethereum-Nodes
- **Electron (Desktop-Anwendung):** Plattformübergreifendes Programmiergerüst
- **Clientseitige Poker-Anwendung:** Der zum Spielen verwendete Client. Dabei handelt es sich um eine HTML5-Webanwendung, die mit dem Ökosystem von React programmiert wurde.
- **IPFS-Client:** Stellt Verbindung zum IPFS-Netzwerk her, um Spielprotokolle zu hinterlegen.

8.2 Spiel-Engine

8.2.1 Zustandsmaschine

Die Spiel-Engine bildet den Kern unserer Anwendung. Es handelt sich um eine Zustandsmaschine, die die Übergänge zwischen den einzelnen Zuständen im Spielverlauf steuert und die Spielregeln implementiert. In Abhängigkeit von den Interaktionen der Nutzer mit der Anwendung und den Netzwerk-Antworten löst die Spiel-Engine entsprechende Aktionen aus und geht zum nächsten Zustand über.

8.2.2: Vernetzter oder Offline-Status

Wenn ein Nutzer sich bei der Anwendung anmeldet, führt Virtue Poker folgenden Vorgang aus:

1. Die Anwendung ist nicht ans Netzwerk angeschlossen, wir befinden uns also im Offline-Zustand.
2. Der Nutzer gibt seine Zugangsdaten ein und meldet sich an.
3. Die Spiel-Engine empfängt die Eingaben und löst die Aktion zum Ausführen der Anmeldung aus.
4. Nach erfolgter Anmeldung geht die Spiel-Engine zur nächsten Aktion über und schickt eine entsprechende Nachricht an die Benutzeroberfläche.
5. Bei erfolgreicher Anmeldung geht der Nutzer zum vernetzten Zustand über.
6. Bei fehlgeschlagener Anmeldung bleibt der Nutzer im Offline-Zustand.

8.2.3: Lobbyzustände

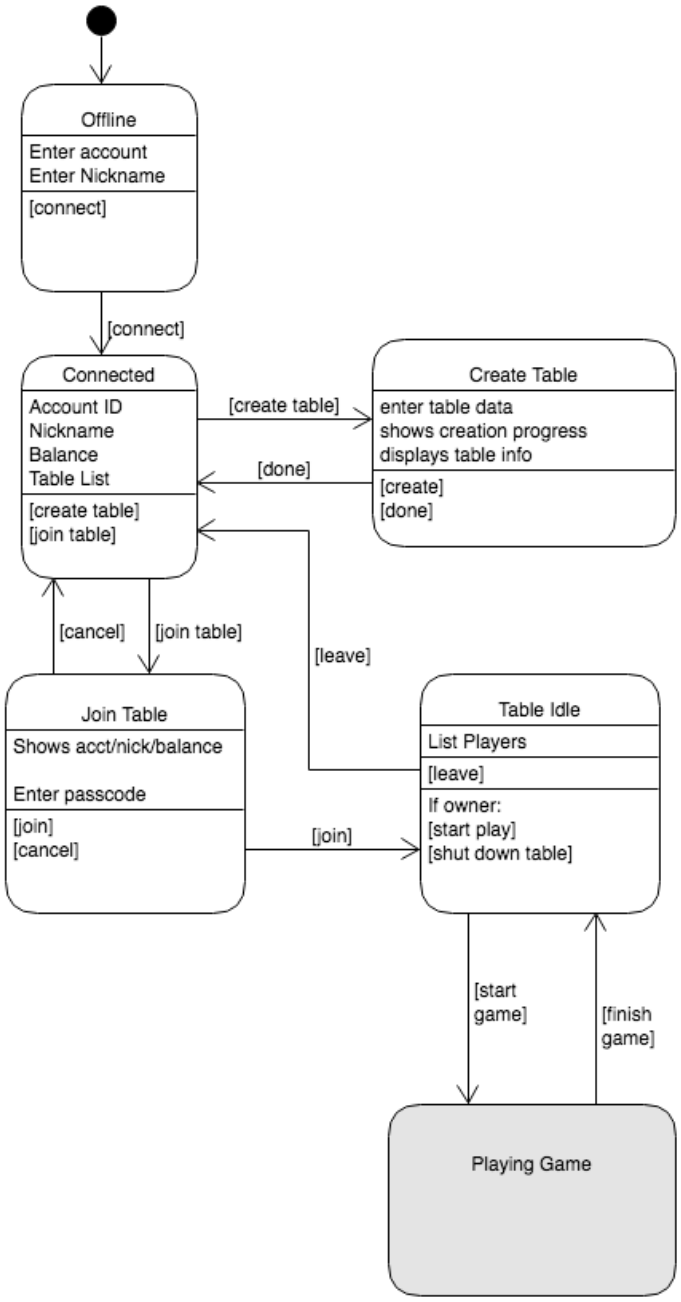
Die Zustände unserer Spiel-Engine lassen sich in zwei Kategorien einteilen:

- **Spielzustände:** Spielzustände im Verlauf eines Spiels.
- **Lobbyzustände:** Sämtliche Zustände, die sich nicht während des Spielverlaufs ereignen.

Es gibt folgende Lobbyzustände:

- **Offline:** Der Nutzer ist nicht angemeldet.
- **Vernetzt:** Der Nutzer hat sich angemeldet und kann einen neuen Tisch anlegen oder einen aktiven Tisch zur Spielteilnahme auswählen.
- **Neuer Tisch:** Der Nutzer legt einen Tisch an.
- **Tisch auswählen:** Der Nutzer wählt einen Tisch zur Spielteilnahme aus.
- **Wartezustand:** Der Nutzer wartet darauf, dass andere Mitglieder sich an den Tisch setzen, damit das Spiel beginnen kann.

Abbildung 13: Lobbyzustände



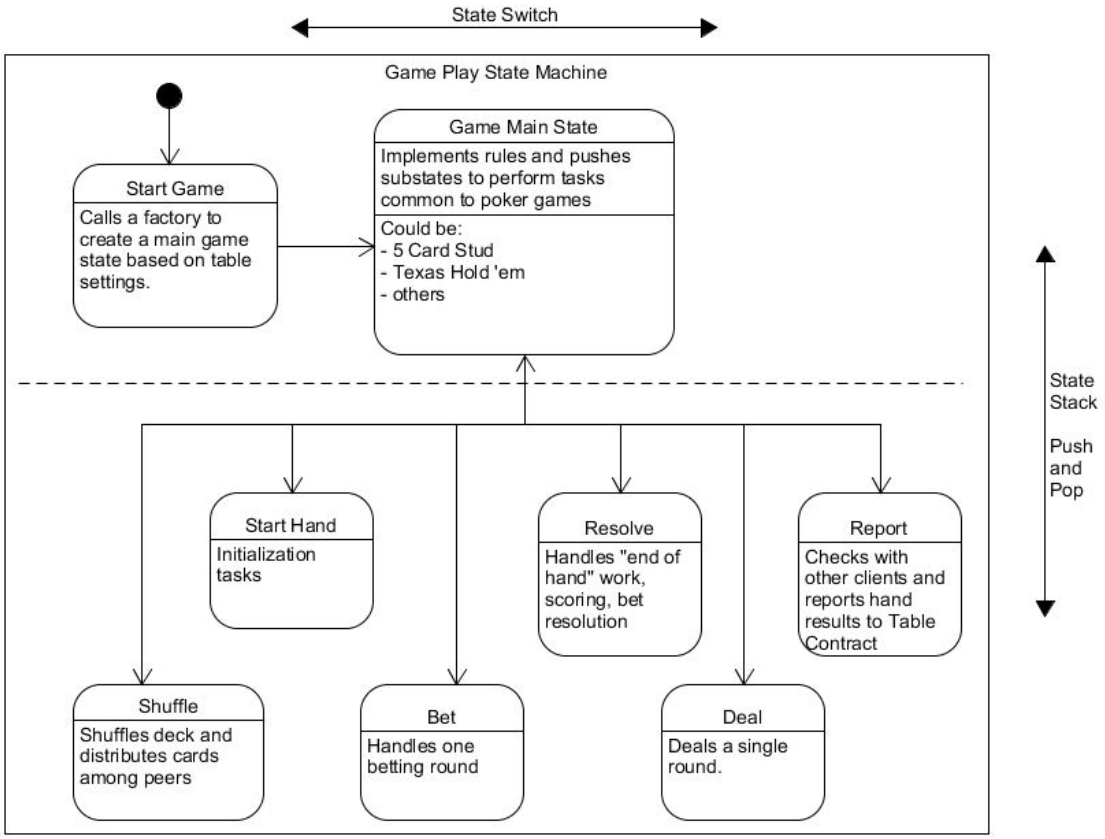
8.2.4: Spielzustände

Es gibt folgende Spielzustände:

- **On Deck:** Der Spieler wartet darauf, dass die Hand beginnt.
- **Hand beginnen:** Alle Spieler sind bereit, die Hand zu beginnen.
- **Karten mischen:** Der Kartensatz wird gemischt und verschlüsselt.

- **Karten geben:** Je nachdem, welches Spiel gespielt wird, erfolgt die Kartenausgabe in mehreren Runden. Beim Texas Hold'em etwa gibt es folgende Runden: Preflop, Flop, Turn und River.
- **Setzen:** Entsprechend dem aktuellen Spielzustand entscheidet der Spieler, ob er abwarten, wetten, aussteigen oder erhöhen will.
- **Überprüfen der Kartenausgabe:** Die Spiel-Engine gleicht die Kartenausgabe mit den Spielregeln ab und entscheidet, ob weitere Karten gegeben werden müssen.
- **Showdown:** Der Moment, wenn alle noch aktiven Hände entweder aufgedeckt oder weggeworfen werden.
- **Handende:** Der Ausgang der Hand wird angezeigt.
- **Bericht:** Die Ergebnisse der Hände werden an den Spiel- bzw. Tisch-Contract weitergeleitet und der Pott dem Gewinner zugesprochen.

Abbildung 14: Spielzustände



3.4 Ethereum Tisch-Contracts

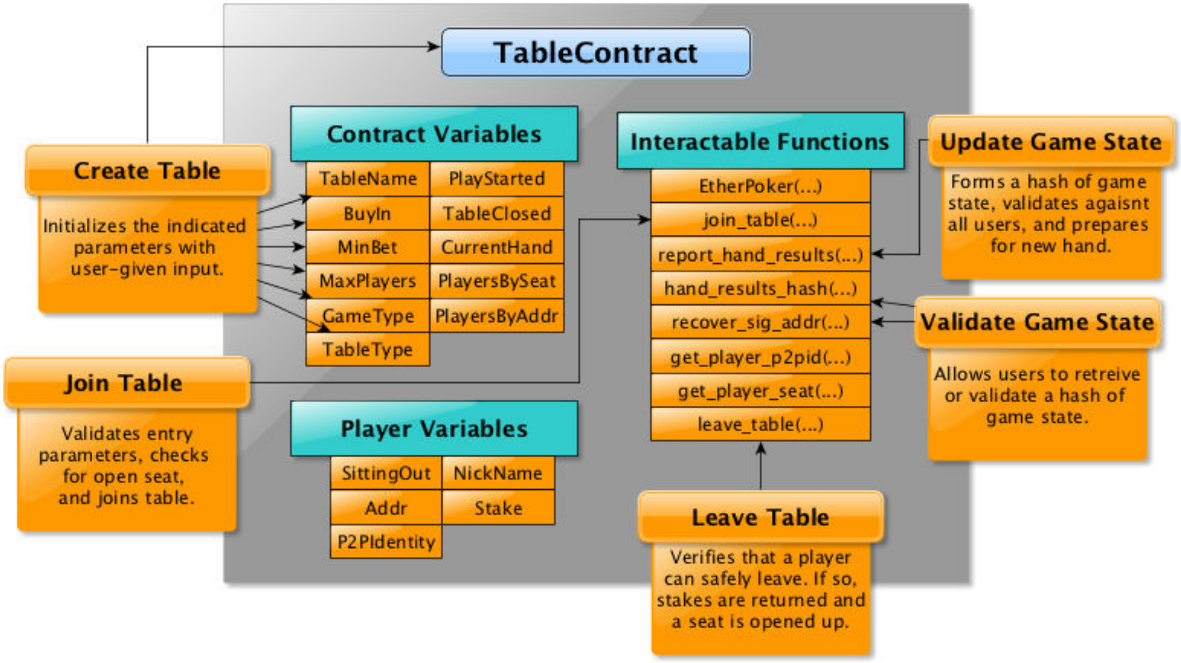
Ein Pokerspiel ausschließlich auf der Ethereum-Blockchain zu spielen, ist mit einem hohen Aufwand an Ressourcen und Zeit verbunden. Zur Gewährleistung eines reibungslosen Spielverlaufs werden Tisch-Contracts zur Spielerverwaltung und Überprüfung der Ergebnisse jeder Hand eingesetzt, sodass die Spiellogik außerhalb der Blockchain verwaltet werden kann.

8.3.1 Funktionen

VirtuePokerTable: Eröffnet den Pokertisch mit den angegebenen Parametern.
Join_table: Wählt einen Tisch zur Spielteilnahme aus, erstellt eine Spieler-Struktur anhand der eingegebenen Parameter und gibt bei Fehlern eine entsprechende Meldung aus.
Get_player_seat: Gibt die Platznummer des Nutzers aus, der die Nachricht geschickt hat, bzw. -1, wenn der Nutzer keine Platznummer hat.
Get_player_p2pid: Gibt die p2pid für die jeweilige Platznummer bzw. einen leeren String aus.
Hand_results_hash: Berechnet anhand der vom Nutzer eingegebenen Parameter einen sha3 hash.
Recover_sig_addr: Gibt die mit dem zum Signieren des Hashwerts Schlüsselpaar verknüpfte Adresse aus.
Report_hand_results: Überprüft, ob alle Spieler die Spieldaten signiert haben, und gibt ggf. eine Fehlermeldung aus.

Leave_table: Trennt die Verbindung zwischen Spieler und Platznummer und überweist die Gewinne des Spielers.

Abbildung 15: Variablen für den Tisch-Contract



8.4 GameNet

Das GameNet dient als Benutzeroberfläche zur Kommunikation unserer App. Dabei gibt es im Wesentlichen zwei Kommunikationsflüsse:

- Kommunikation mit anderen Spielern über P2PNet.
- Kommunikation mit dem Ethereum-Netzwerk über Web3.js

Ein Nutzer, der neu an einen Tisch kommt, interagiert beispielsweise mit dem Ethereum-Netzwerk.

Um seinen Spieleinsatz einzuzahlen, überweist er den entsprechenden Betrag aus seinem Wallet. Für die sichere Aufbewahrung der Geldmittel der Spieler ist ein zweiter wichtiger Bestandteil von GameNet zuständig, nämlich das Keystore-Modul.

8.4.1 KeyStore

Für das Wallet, in dem Sie Ihre Einsätze hinterlegen, gibt es zwei Schlüssel, einen öffentlichen und einen privaten:

- Der öffentliche Schlüssel ist die öffentliche Adresse, die zum Empfang von Auszahlungsbeträgen verwendet wird.
- Der private Schlüssel wird von Ihnen zum Einzahlen von Geldbeträgen verwendet.

Die Einsätze werden in einer Transaktion übermittelt, die mit dem privaten Schlüssel signiert wird. Dabei ist zu beachten, dass Ihre Geldmittel genauso sicher sind wie Ihr privater Schlüssel – wenn Sie einer anderen Person Ihren privaten Schlüssel mitteilen, kann diese Person auch auf Ihre Geldmittel zugreifen.

Unser Schlüsselspeicher verwendet die gleiche Schlüsselableitungsfunktion (scrypt) sowie die gleichen symmetrischen Chiffren (AES-128-CTR) und Nachrichtenauthentifizierungscodes wie geth, die offizielle Implementierung des Ethereum-Protokolls in Go.

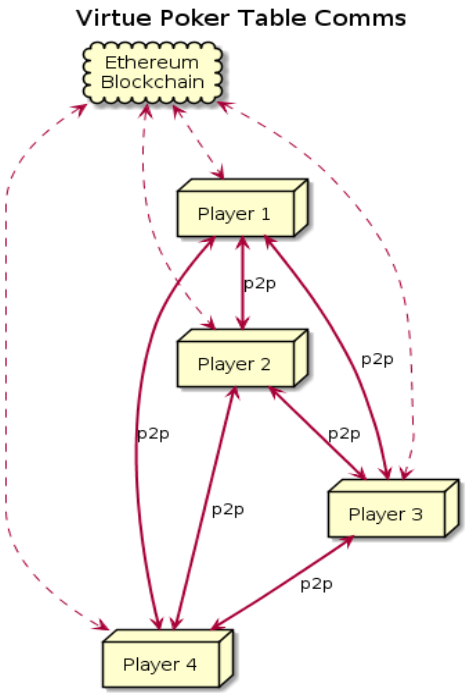
Ihre Schlüssel werden auf Ihrer Festplatte gespeichert und durch ein Passwort gesichert, das Sie zum Spielen auf Virtue Poker eingeben müssen.

8.5 P2PNet

Das P2PNet ist für sämtliche Kommunikationen zwischen den Nutzern zuständig, die nicht über das Ethereum-Netzwerk laufen. Im Kontext dezentraler Anwendungen werden diese Vorgänge als *off-chain* bezeichnet. Die Ressourcen des Ethereum-Netzwerks werden von sämtlichen dezentralen Anwendungen verwendet; zudem fallen für sämtliche Transaktionen über das Ethereum-Netzwerk Gaskosten an. Daher ist bei der Nutzung von dezentralen Anwendungen stets Effizienz geboten. In diesem Sinne sind wir bestrebt, sowohl die Größe unserer Contracts als auch die Übermittlung von Nachrichten über die Ethereum-Blockchain auf ein Minimum zu beschränken, um Betriebskosten zu sparen und den Spielverlauf zu beschleunigen.

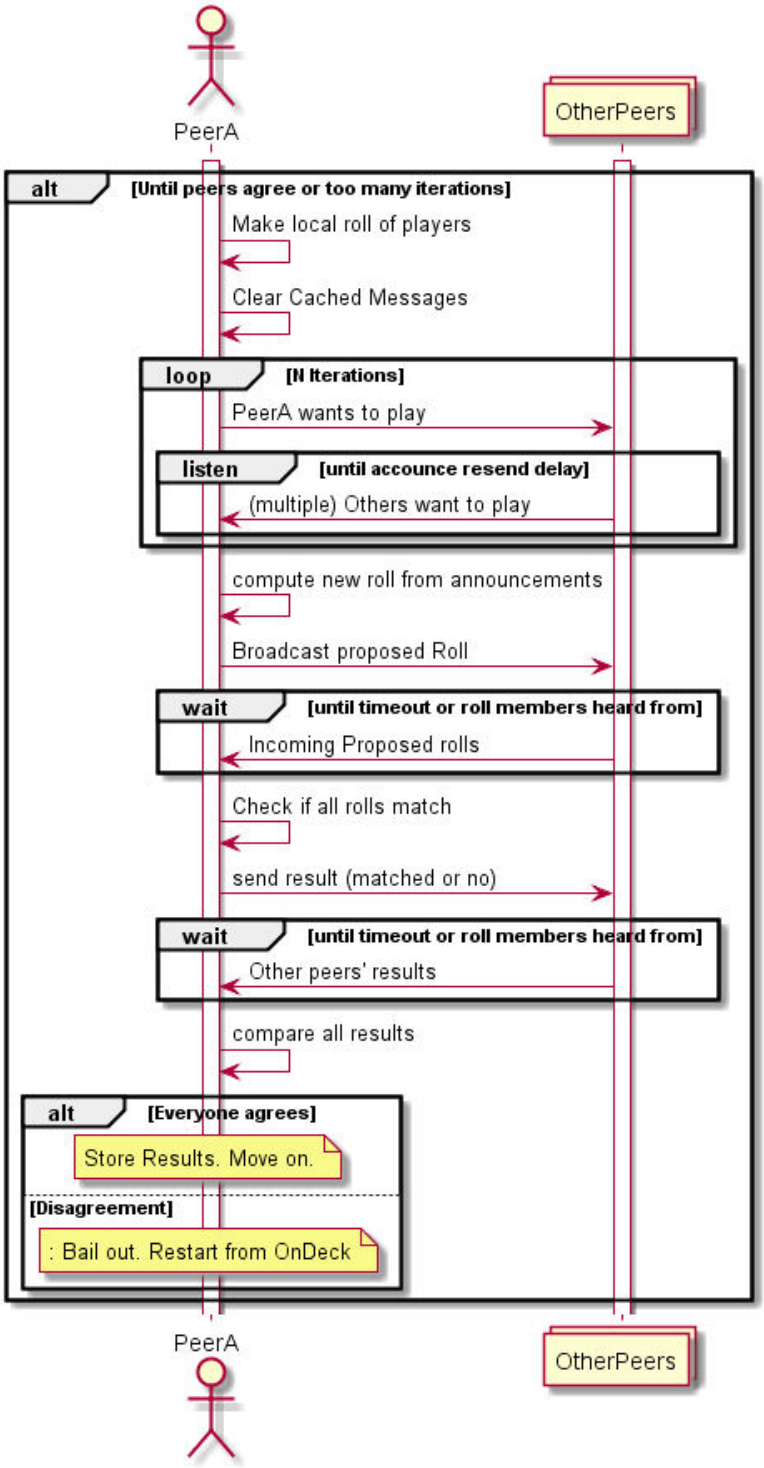
Unser P2PNet verwendet zwar keine Off-chain-Kanäle im eigentlichen Sinne, jedoch bilden sämtliche Daten (mit Ausnahme von Chat), die über P2PNet übertragen werden, Teil eines Off-chain-Subnetzes, in dem alle Spiel-Clients off-chain Einigung über den Spielvorgang erzielen. Dadurch kann die Blockchain zwar die Einigung als solche verifizieren, sie kann jedoch nicht jeden einzelnen Spielzug nachträglich überprüfen.

Abbildung 16: P2P-Kommunikation



Zu Beginn jeder Hand nehmen die Spieler am jeweiligen Tisch gleichzeitig einen „Roll Call“ vor, bei dem sie nach Nachrichten von allen anderen Spielern am selben Tisch schauen. Anschließend einigen sie sich darüber, wer an der nächsten Hand teilnimmt. Dieses Verfahren wird in Abbildung 17 veranschaulicht.

Abbildung 17: „Roll Call“



8.6 Web3.js

Web3.js ist die mit Ethereum kompatible JavaScript-API zur Implementierung des Protokolls Generic JSON RPC. Web3.js ist eine offizielle Programmbibliothek, die vom Ethereum-Team zur Verfügung gestellt wird. Wir verwenden Web3.js für folgende Aufgaben:

- **Contract kompilieren**: Vor der Kompilierung mit Web3.js werden unsere Contracts vorkompiliert und gründlich getestet. Die Kompilierung muss vor der Installation mit web3.js erfolgen.
- **Contract installieren**: Web3.js stellt eine einfache und sichere Javascript-API zur Installation der Contracts bereit.
- **Contract-Anruf**: Nach der erfolgten Installation wird jede Interaktion mit dem Contract als Anruf bezeichnet. Anrufe erfolgen ebenfalls über die web3.js-Schnittstelle.
- **Transaktionen**: Alle anderen Aktionen, die den Zugriff auf das Ethereum-Netzwerk erforderlich machen, werden über Web.js ausgeführt.

8.7 Electron

Unsere Desktop-Anwendung basiert auf Electron. Electron hat sich bereits bei früheren Ethereum-basierten Projekten bewährt, so etwa dem Mist Ethereum Wallet, Atom, Visual Studio Code und dem Jaxx Wallet. Electron ist ein von Github entwickeltes quelloffenes Programmiergerüst zum Aufbau nativer Anwendungen mithilfe von Web-Technologien wie JavaScript, HTML und CSS.
Bei der Entscheidung für Electron waren für uns folgende Kriterien ausschlaggebend:

1. **Es ist plattformübergreifend**: Man braucht den Code nur einmal zu schreiben und hat ein Produkt, das auf verschiedenen Plattformen funktioniert – in diesem Fall Windows, Mac und Linux.
2. **Es basiert auf Web-Technologien**: Wir können bei der Entwicklung unserer Anwendung die gleichen Technologien wie beim Aufbau von Websites verwenden und brauchen dafür keine auf bestimmte Plattformen spezialisierten Entwickler.
3. **Niedrigere Entwicklungskosten**: Wir können vielversprechenden Nachwuchsentwicklern eine Chance geben, die nicht unbedingt über plattformspezifische Fachkenntnisse verfügen, und sparen dadurch auch noch Kosten.
4. **Effizienzgewinne**: Anstatt Entwickler zur Programmierung spezieller Plattformen einzustellen, können wir unsere gesamten Ressourcen durch die Nutzung von Electron auf die Entwicklung eines Produkts konzentrieren, das auf verschiedenen Plattformen funktioniert.

8.7.1 Die Electron-Architektur

Die Architektur von Electron basiert auf:

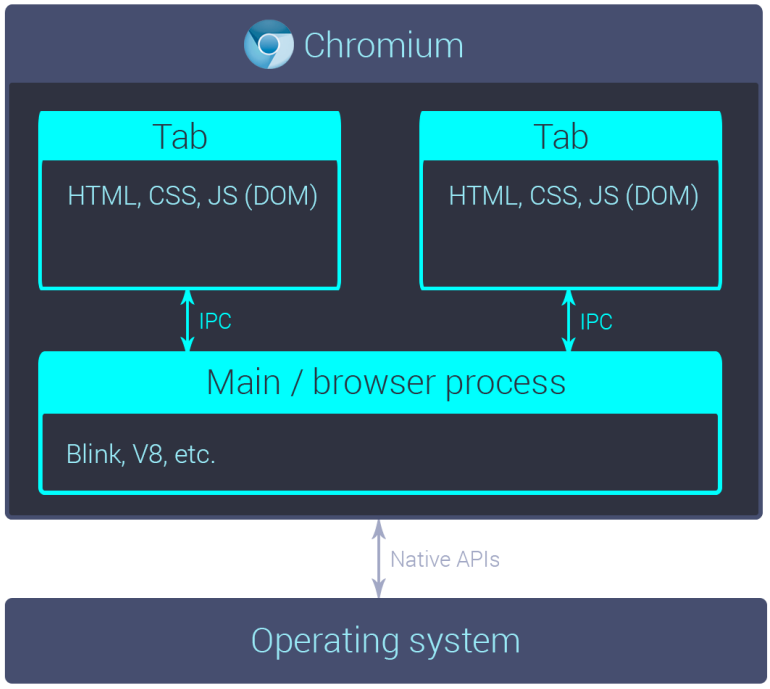
- **Chromium**: die Browser-Engine, die Google Chrome und Chrome OS zugrunde liegt. Durch ihre Verwendung können wir beim Aufbau unserer Anwendung Web-Technologien nutzen.
- **NodeJs:** Node.js ist eine Plattform zum Betrieb von Netzwerkanwendungen, die in der für Chrome/Chromium entwickelten JavaScript-Laufzeitumgebung „V8“ ausgeführt wird. Node.js ermöglicht den Zugriff auf das Dateiverwaltungssystem und weitere Ressourcen des Betriebssystems.

Jede neue Version von Electron basiert auf den jeweils aktuellen Versionen von Chromium und NodeJS. Bei Redaktionsschluss dieses Dokuments war Electron in der Version 1.6.11 mit folgenden Bestandteilen verfügbar:

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

Nähere Informationen zu Chromium finden Sie hier: https://electron.atom.io/

Abbildung 18: Chromium

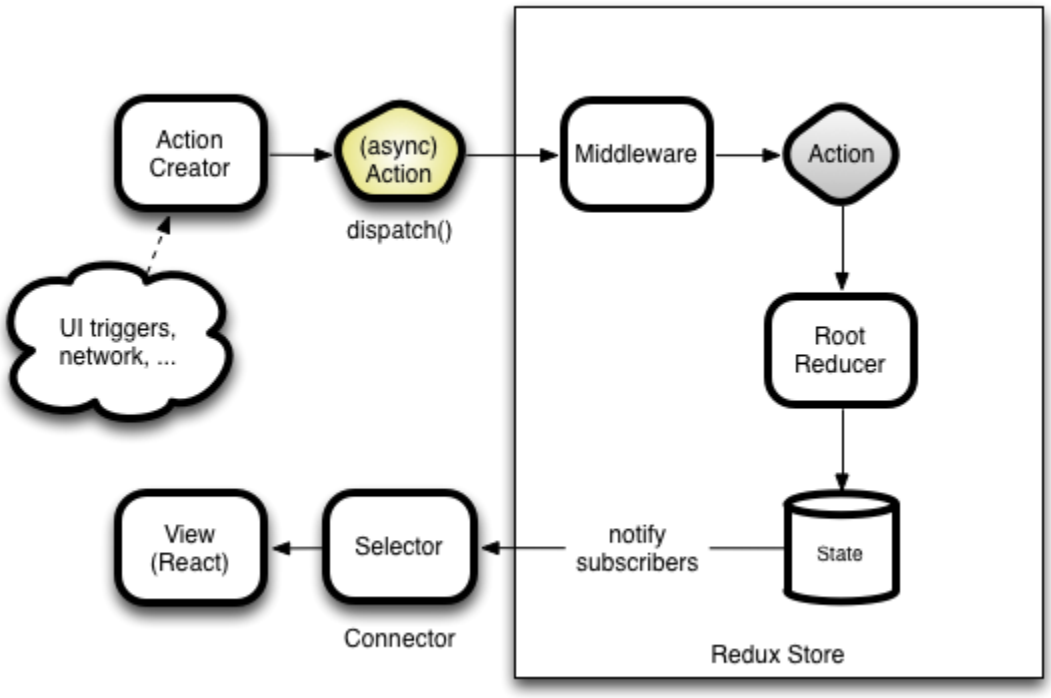


8.8 Pokerspiel-Client

8.8.1 Architektur des Spiel-Clients

Unsere clientseitige Spielanwendung wurde mit der Redux-Architektur von React entwickelt.

Abbildung 19: React



8.8.2 Spielverlauf

Die Benutzeroberfläche des Spiels besteht im Wesentlichen aus zwei Komponenten, die in unterschiedlichen Fenstern angezeigt werden:

- Lobby
- Tischspiel

Bei Spielbeginn befindet der Spieler sich in der Lobby und kann folgende Aktionen ausführen:

Anmelden: Der Nutzer meldet sich mit seinen Zugangsdaten bei der Anwendung an.
Neuer Spieltisch: Der Nutzer kann einen privaten bzw. öffentlichen Spieltisch neu anlegen.
Alle verfügbaren Tische anzeigen: In der Lobby werden sämtliche Tische angezeigt, die Nutzern aktuell zur Teilnahme an einem Spiel zur Auswahl stehen.
Aktives Spiel auswählen: Der Nutzer kann einen Spieltisch oder ein Spielturnier zur Teilnahme auswählen. **Wallet verwalten**: Der Nutzer kann sein virtuelles Poker-Wallet verwalten.

Ein Spiel spielen: Der Spieltisch öffnet sich in einem eigenen Fenster.
Mehrere Spiele gleichzeitig spielen: Der Nutzer kann an mehreren Spielen gleichzeitig teilnehmen.
