blockdraw

Decentralized Peer-to-Peer Casino Platform

WHITEPAPER V1.4 (DRAFT)

Business class security and Integrity combined with the verifiability and trustless capability of the blockchain.

- An Important Notice to all Token Sale Participants
- Read this document in its entirety before taking any action.
- Acknowledge the non-regulated nature of purchasing Ethereum utility tokens.
- Accept a high degree of risk in relying on forward-looking statements, the viability of the business, and the future of Ethereum Draw utility tokens.
- Consult an expert if you are in any doubt about the contents of this document.
- You will be required to agree to the Blockdraw Terms and Conditions before participating in any Sale of Draw utility tokens.

1. OVERVIEW

Blockdraw technologies LTD ("Blockdraw") is focused on developing distributed ledger (e.g. blockchain) online casino solutions, with an emphasis on peer-to-peer, banque vs. player games. Put more simply, Blockdraw is working toward building a decentralized casino betting exchange, allowing anyone to function as the casino or as a Player (when we use the term banque or banquier, we are referring to players who are playing the role of the casino).

The online gambling market is projected to grow to $59.79B by 2020 and has nearly tripled since 2009[1]. The largest regions of growth continue to be in Asia, particularly in China. Online casino revenues are estimated to make up 24% of total revenues[2]. Blockdraw believes that distributed ledger technologies will eventually be widely adopted by online casinos and sports books as the technology matures and players become more accustomed to using the technology.

The rapid growth in online casino games has brought many innovations, but one of the many complaints from gamblers continues to centre around fraud and payment issues where either operators refuse to pay winning bets either by claiming regulatory issues, or that fraud or cheating has occurred (often without proof). Or, the casino itself goes bankrupt, leaving player funds lost forever. Other issues centre around questions related to fairness of the random outcomes. Blockchain casinos offer the promise of many changes, which can make them fraud proof and provide instantaneous payments in a trusting environment where players should always get paid their winnings or have their funds returned.

Regardless of the format, today's online gambling games suffer from several problems: (a) the random number drawing can be compromised ("fair draw problem"); (b) the player, or her agent, must trust the website operator to pay

[1] https://www.statista.com/statistics/270728/market-volume-of-online-gaming-worldwide/

[2] https://www.statista.com/statistics/248655/segmentation-of-online-gambling-market/

winnings; (c) expensive administration and advertising costs eat into the gambling return to players; (d) a fair distribution of winnings can be slow or corrupted; (e) provider's financial conditions are rarely known and can go bankrupt leaving player funds lost; (f) betting lacks customization and (g) the player cannot participate as the "casino."

Distributed ledger and blockchain technologies used along with existing technologies (peer-to-peer, IPFS, crypto logical random number processes, such as "Mental Poker," etc.) can resolve these challenges.

Blockdraw is designing a peer-to-peer blockchain casino based on the Ethereum platform. Our partially open sourced smart contract games will revolutionize online casino gambling in several ways. A significant innovation is that anyone can be a player or a casino banquier playing on the Blockdraw platform, which is backed by a token ecosystem that assures payment to players (using our Draw tokens). We plan to begin by offering a suite of digital equivalents to Baccarat, Blackjack, Mahjong, Sic Bo, Pai Gow, and Pai Gow Poker, but we will later add all traditional games. We believe that there is currently no blockchain product that has the verifiability, performance, audit (for regulatory purposes), decentralization, and provably fair results that Blockdraw will offer. We have combined the best of all currently available technologies including leveraging the best of what Ethereum offers while discarding the worst.

1.1. THE VIP OPPORTUNITY

Blockdraw believes that the single largest opportunity in online gambling, which is yet unrealized, exists in creating VIP (including very high stakes) focused blockchain casino card games. For the first time ever, Blockdraw will produce a platform that allows players to face a player banque (or banquier). All players choose between being the passive casino (banquiers) with an edge or a regular player. If an individual is willing to "lay" betting action passively through Blockdraw's platform,

then they will be able to function as the “casino.” Because of the opportunities that distributed ledger technology creates, Blockdraw will be able to offer fair games with a token system and software that assures high stakes gamblers will get paid when they win, that games are verifiably fair, and that Blockdraw (or a malicious third party) cannot manipulate the results. There are virtually no general access online casinos that cater to the serious ($1,000 up to $1,000,000/hand) VIP player since online casinos are satisfied with small wagers and have a low volatility of gaming results – assuring profitability. The facts are that in extreme stakes games, a casino can take serious financial drawdowns, but with Blockdraw, stakes will be limited only to the size of the banker’s Draw token wallets – players could wipe out a banker, but not the platform! And we expect to allow anyone to spectate high stakes “head’s-up” games where players try to wipe out bankers.

We believe that through our partners, we can attract the serious top 5% of the gambling elite to our token ecosystem by offering a place where the serious high stakes gambler can play for massive stakes and be assured an instant payout.

1.2. THE BUSINESS MODEL

Blockdraw is creating a robust business model designed to incentivize other providers with existing customer bases to drive traffic to the network. The Blockdraw network motivates partners to cooperate as part of a larger network. Users will experience a well-rounded selection of games and environments along with incentives to own and acquire the Draw tokens.

Imagine a banquier who wishes to banque a $10K/hand game of Baccarat where it may be necessary for a banquier to post as much as 20-50X the bankroll of the player. While it is true the market for very high-end gambling is very small, presently this market is underserved by many online providers. Blockdraw plans to disrupt this market entirely by attracting the kind of high stakes players found in the best casinos in Macau and Las Vegas. Our mathematicians have run simulations for our

games to determine the size of a banker's wallet required to support a given table limit for each of our games. At the very least, a banker will need to match the combined capital of all players at a table. Heads up play will be allowed where players can risk breaking the bank, in much the same way heads up action occurs in online Poker.

In addition to our technological advances, our most important tool behind the Blockdraw platform is the DRAW digital utility token.

All activity within the Blockdraw network centres around the DRAW token, including the collection of fees from users, providing collaterals for games by banquiers, and paying tokens to winning players. DRAW is the centre and the critical driver of a sustainable economy whose price is set during the initial coin offering ("ICO").

We believe that when the Blockdraw network features are combined, they create a powerful force to drive the price of DRAW higher over time.

Blockdraw was founded by industry veterans from the online gambling and financial markets with strong backgrounds in regulatory compliance in both sectors. The company has hired out both gambling development and blockchain teams. Both the token and the platform have been well thought out to maximize value to Draw token holders.

2. MISSION STATEMENT

Blockdraw's mission is to create the world's most entertaining, secure, and trusted blockchain online decentralized peer-to-peer premium casinos. Our mission is to become the world leader in decentralized VIP gaming, creating fun, exciting, and innovative games and game designs.

2.1. OUR PHILOSOPHY

We live in an exciting time right now because of blockchain technologies. They enable us to perform provably fair transactions without a trusted third party in an openly verifiable way. Cryptocurrency is just one of the major implementations of blockchains, and talented visionaries are finding amazing ways to apply them in new areas. Many technocrats are filled with a revolutionary zeal to replace central authorities like banks and governments and create a citizen empowered world.

We have a different mindset. We're not out to topple governments with cutting-edge tech; we want to work with and within existing systems to help improve them. We want to give everyone new options they didn't have before, and that includes not only citizens but also policy makers in business and administration. Innovative technology is compelling, and we're doing cool stuff. Our LEAP system is designed to meet the needs of individuals, investors, businesses, and regulators. And our cryptographically secure "Mental Poker" algorithm is the most advanced ever theorized. Extended from the work of Phillipe Golle, our non-shuffling algorithm enables trustless peer-to-peer decentralized gameplay and employs random number generation that Blockdraw will have tested and certified by a reputable testing authority.

But great technology alone isn't enough.

For a venture to succeed, it also needs to have a sound business model. That entails providing value to customers, being profitable, and building community. This is the first bar where many ICOs (and revolutions) fail. Just because a technology is modern doesn't mean it meets our needs better, can be monetized, or generates goodwill. We have a realistic plan for building a successful company that comes from our years of executive experience.

Combining technology with business is a potent mix, yet we feel we can do still more. At a basic level, running a business means finding ways to make money by providing value. But curating a utility token involves more than traditional business requires: we must also attend to the token economy. People should only in invest in tokens because of their utility value.

3. INTRODUCTION

3.1. CASINO GAMES

Casino games are found in virtually every country in the world and are usually available online either legally (regulated), illegally, or in a regulatory limbo form (called “grey”). Technologies like the blockchain are already bringing these opportunities to the masses. As the proliferation of cryptocurrencies increases, new ideas will emerge to improve online gambling. Many public and some private companies offer direct access to online casinos for fiat currencies, some regulated and some unregulated; but in all cases, there is little transparency regarding random number security, creditworthiness of the casino, jurisdiction where player funds are held, and many other important details players should be concerned about. Virtually no online casino has the ability, let alone the incentive, to provide high stakes ($1000+/hand or more) games such as those offered in terrestrial casinos in Las Vegas or Macau. The future of current blockchain currencies is uncertain, but the probably of a nation state eventually using distributed ledger technology for all their currencies is only a matter of time. If this happens, Blockdraw will be in the driver’s seat to offer casino solutions. In the meantime, legal or grey market opportunities exist for online blockchain casinos that are significant.

3.2. CHALLENGES

The transaction value of current blockchain technology limits the ability of developers to bring casinos totally online to the blockchain, but this is changing quickly. Using state channels in Ethereum, some games can be moved closer to full decentralization, but while the technology may exist, it remains very immature and has vert real security challenges. Nevertheless, blockchain and other technologies can still be used to solve many critical issues, such as the fair draw problem, player

payment guarantees, and peer-to-peer gambling. Blockdraw created an optimal solution to address the current problems facing Ethereum.

3.3. MARKET SIZE

The market potential for blockchain casinos growth is likely tremendous; as the proliferation of cryptocurrencies has increased, the number of Bitcoin casinos has exploded. Many of these casinos still function like fiat casinos, since smart contracts are not always used. The larger commercial companies are selectively accepting cryptocurrencies, but not using the technology to its potential, These companies seem to be waiting to acquire this technology from a future company. Some of the better bitcoin casinos offer the latest technology in “provably fair” games, but still lack the possibilities available in smart contracts under Ethereum. Blockdraw believes that Ethereum based VIP casinos using Ethereum smart contracts represent a significant market opportunity.

4. DEFINED TERMS

Player: is a regular player who places bets on games as she would in any casino. Players using Blockdraw may however also be able to negotiate some game rules to minimize the edge that Banquiers get from traditional games.

Banquiers: Are players who Banque (accept the same financial risk as a casino) all Blockdraw games, they are passive players who receive bets – they cannot place bets. Banquiers also have the option of acting in an automated fashion (using standard game rules, e.g. hit on 16 or stand on 17 in the case of Blackjack) or by making their own decisions in the game (e.g. hit on 17 if they want).

Blockdraw Network: is the total network including all games (Blockdraw or third parties), the software, revenue sharing agreements, and all smart contracts are operated by Blockdraw.

Blockdraw Platform: is the software including the server software, app software and smart contract software, and all intellectual property needed to operate Blockdraw's software.

Blockdraw ecosystem: represents everyone involved in the system, including players, Draw tokens, the platform, and the network.

5. THE DRAW TOKEN

The Blockdraw ecosystem uses an open source cryptographic token named “Draw” (the Draw token) which is fractionally divisible, transferrable (either directly or through an exchange), and fungible.

5.1. PURPOSE AND USE

The Draw token is an integral part of the Blockdraw platform and a fundamental driver for the Blockdraw ecosystem. All activity within the ecosystem is driven using the Draw token including the fact that:

- Users are required to purchase Draw to participate in Draw games, collateral and guarantees are held in Draw, and winnings and wagers are paid and collected in Draw;
- Platform fees are paid in Draw by Banquiers to Blockdraw;
- Banquiers must post Draw to smart contracts that run Draw games equal to at least the cumulative amount of player capital being staked;
- Revenue share (earned from the gaming margin) will be paid in Draw to affiliates who drive traffic to Blockdraw games.

In short, users must purchase Draw token(s) to participate in Blockdraw games and any winnings are held by Blockdraw curated smart contracts payable in Draw tokens.

5.2. TECHNOLOGY

Draw is an ERC20-compatable utility token over the Live Ethereum blockchain which itself has become an industry standard for issuing custom digital assets.

Utilizing Ethereum ensures global compatibility with the entire Ethereum ecosystem including wallets, exchanges, and other development tools. But perhaps most important, and a key factor for BlockDraw's integration with Ethereum is the ability to program smart contracts that allow for a decentralized economy where trust is maximized for participants:

- Users make payments to Ethereum smart contracts which hold and distribute users funds;
- These same smart contacts guarantee winnings in Draw tokens either through holding funds within the smart contract or receiving payments from wallets set-up to guarantee payments to users;
- Decentralized smart contracts settle final gaming transactions (once posted) and funds can be accessed globally from the world-wide web;
- The entire process is recorded on an Ethereum chain.

Blockdraw technology maximizes decentralization (given the constraints) and works towards minimizing the degree/capacity to which the user in the system (e.g. players or banquiers) must trust another (e.g. game provider) to enforce some specific properties (e.g. fairness).

Blockdraw's casino platform effectively operates similarly to a betting exchange offering peer-to-peer gambling for casino games.

5.3. MAINSTREAMING BLOCKDRAW GAMES

Due to the technical requirements of the blockchain we accept that mainstreaming blockchain games can be a difficult process unless there are proper incentives. However, our corporate strategy envisages both a push and pull methodology. We intend to specifically target the VIP player market in Asia and partner with large Asian junket operators who we can incentivize to bring high stakes players to the platform.

Our founders' experience in financial markets and online gambling from a development and regulatory standpoint makes us well positioned to understand how to mainstream games through:

- Marketing, promotion, and advertising
- Testing game design to create games people love to play
- Maintaining internal regulatory compliance until regulation is possible or needed

5.4. SUSTAINING THE DRAW ECOSYSTEM

For a utility token to be successful and maintain value, it must have the following qualities:

- Utilized in a product or service that people want to use and trust (demand)
- Incentives for users to try the product
- Incentives for developers to improve the product
- Incentives for operators to market and promote Draw utility tokens and its games
- Adequate scale to create trading liquidity or cache value among Draw owners
- A limited supply

We have put a great deal of thought into our Draw token pool. Draw tokens will be utilized within Blockdraw games at the outset. Additionally, we will also set aside a small portion of our Draw token pool to incentivize large junket style operators who routinely court high stakes players. We have intentionally created a large token pool so that we can provide incentives to users and promoters of the product. Our game designs will be tested and improved over time to ensure we provide the market with what consumers demand. While we will write our token contract to allow for future

token destruction (to provide future flexibility), we do not plan to create a typical destruction mechanism from game play.

6. THE DRAW ECOSYSTEM

Blockdraw aims to build a long term global decentralized gaming network for card games other than Poker. We think that the basic infrastructure requires some hybrid solutions until blockchain networks mature further; but for now, the blockchain offers significant advantages to the online gambling industry. Our business model assumes that Bankers (acting as a casino for individual games) will market Blockdraw products for revenue, drawing VIP players to the system for its ability to offer large stakes play, and also that Blockdraw will generate revenue from licensing royalty and platform fees.

6.1. BANQUIER ROLES

Blockdraw provides a platform for players to wager against banquiers in a trusted peer-to-peer network:

- Bring high stakes games using Draw tokens;
- Bring traffic to the Blockdraw network and build demand for Draw utility tokens through customer adoptions of the Blockdraw app;
- Provide either Draw tokens for smart contract collateral (or obtain loans from Blockdraw);
- Provide direct client access to the Blockdraw network though the Blockdraw app;

6.2. BLOCKDRAW'S ROLE

Blockdraw is the official creator of both the Blockdraw Platform and the Draw utility tokens and is solely focused on releasing Ethereum based gaming solutions:

- Create and curate the Draw token ecosystem;

- Provide casino games to the platform and possibly the availability of third party game offerings;
- Create technology that will allow players and bankers to communicate and message each other;
- Offer games that have flexible betting limits or other game rules that can be adjusted to change the percentage return to the player;
- Define the models for bankers and players to use the Blockdraw Platform of games;
- Create incentives for bankers to provide and market the Blockdraw app;
- Develop, protect, and create all the technology required for bankers and players to use the technology;
- Create a Platform that is scalable, networkable, and flexible to allow for broad development possibilities;
- Promote the Blockdraw Platform to all interested stakeholders.

Blockdraw Technologies Ltd. is incorporated as a for-profit company in Gibraltar. Blockdraw's revenues are expected to come from licensing, royalty fees, platform fees, revenue sharing, and consulting services associated with its assets.

6.3. GAMES

Blockdraw will create its own games for the network but may allow in the future the ability to add other providers' games.

6.4. THE SYNERGIES OF THE BLOCKDRAW ECOSYSTEM

Blockdraw is building a powerful ecosystem designed to create benefits for all who share in the network, from players, to bankers to Blockdraw, all gaining in a synergistic process that creates win-win opportunities for all involved.

Synergy defined:[3]

"**Noun, plural synergies.** The interaction of elements that when combined produce a total effect that is greater than the sum of the individual elements, contributions.; synergism."

6.4.1.PLAYERS BENEFITS IN THE BLOCKDRAW ECOSYSTEM

- Provably fair games, with known returns to players and transparent verifiable results;
- Global access;
- Blockchain technology guarantees players trustless outcomes

6.4.2.BANQUIER'S BENEFITS IN THE BLOCKDRAW ECOSYSTEM

- Access to a global, diverse, new, and exciting network to bring VIP players to high stakes games;
- Financial opportunities to earn Draw tokens from incentive programs offered to banquiers that drive traffic to the platform;
- Brand recognition associated with Blockdraw
- Earn the financial mathematical game "edge" that would traditionally go to a casino.

6.4.3.DRAW TOKEN HOLDER BENEFITS IN THE BLOCKDRAW ECOSYSTEM

- By creating a synergy of benefits, we expand the possibilities for Draw usage and increase the chances for a Pull Marketing strategy to benefit Draw Token holders;

[3] http://www.dictionary.com/browse/synergy

- We are creating a platform that will offer games and an incentive system that has the potential to create significant demand for Draw tokens;

Our synergistic process increases the chances of adoption of the Blockdraw platform by creating opportunities for others to share in the success of Draw. We believe that we have created an alignment of interests between the Draw utility token holders and Blockdraw so that our success is their success.

7. THE BLOCKDRAW PLATFORM AND NETWORK

The Blockdraw ecosystem seeks as its goal the development of a decentralized betting exchange gaming platform focused on casino games.

Gambling games generate two key types of revenue, gross gambling revenue, which represents the total amount wagered, and net gambling revenue which represents the difference between the gross gambling revenue and winnings from gambling paid to players (the gross profit before administrative expenses). Online gambling operators have enormous basic costs in terms of developers, offices, hardware, security, customer service, and administrative costs. Decentralization is widely believed to remove many of these costs; and, while this may be true, some of the platform and network operator's costs will always remain. Blockdraw believes that largest benefit of decentralization is that it allows smaller start-ups to compete efficiently with larger multinational online gaming businesses, because decentralization replaces or significantly reduces many costs. Acceptance and development of the Draw token creates opportunities to raise additional capital for expansion.

Nevertheless, it is important for Blockdraw to have partners to expand its network, promote its games, and to refresh its gaming library to keep players coming to visit and play on the Blockdraw platform. Ultimately this creates the need for financial incentives.

7.1. SMART CONTRACT ESCROW MECHANISM

Blockdraw uses decentralized Live Ethereum smart contracts to escrow player funds. Our game play system (see LEAP below) functions like an Ethereum state

channel, in that all activity is played using our decentralized app and settled later when a player chooses to exit the platform. Blockdraw smart contracts may also have payment algorithms for paying revenue share fees to Blockdraw and affiliate smart contracts wallets on the Live blockchain.

7.2. REVENUE SHARING SYSTEM

Blockdraw plans to create a revenue sharing system for affiliates to drive traffic to the Blockdraw network. The exact amount that each party shares is negotiated with Blockdraw and depends on numerous factors, but there are standard traditions already in place within the traditional online market that will likely dictate some of the terms that Blockdraw will negotiate. We do not believe it's appropriate to publicly disclose our payment model in full, since this is a new scheme for the blockchain industry.

8. THE BLOCKDRAW TECHNOLOGIES AND APPLICATION

Our goal is to build the world's best decentralized peer-to-peer casino application. More specifically, we have designed a system that is:

- *Peer-to-peer* – Decentralized gameplay that is proven cryptographically secure
- *Trustless* – Still works even assuming no participant can be trusted
- *Reliable* – Guaranteed to payout to winners, using Ethereum-based Draw tokens
- *Verifiable* – Structured so that games can be proven to be played correctly and fairly
- *Performant* – Is smooth and fun to play, avoiding technical slowdowns
- *Efficient* – Effectively accomplishes function with minimal cost and resources
- *Compliant* – Meets legal and regulatory requirements for gambling apps
- *Secure* – Protected against known threats, both internal and external

Blockchain-based solutions offer the first four qualities but struggle to meet the last four. Server-based solutions offer the latter four qualities, but often fail the first four.

[As an important aside: the word "server" is something of a taboo in the cryptocurrency community, and it shouldn't be. After all, blockchains and other open technologies are run on servers. The contention isn't with servers *per se*, but with the opaque implementations historically done on them that force users to relinquish control over their own assets. It makes more sense to weigh the advantages and disadvantages of each technology class, than to discard the

benefits of server architectures just because they haven't been properly utilized up to now.]

Let's take a look at each technology in more detail and highlight their limitations.

8.1. ANALYSIS OF AVAILABLE TECHNOLOGIES

Blockchains are ideal for their original intended purpose, which is to record financial transactions in a decentralized, open, and provably verifiable way. Efforts to extend those advantages into other areas have met with practical problems. Ethereum suffers from several issues, shared among blockchains in general (though with different specific values):

- Typical blockchain throughputs are around hundreds of transactions per minute, which is insufficient to handle even a modest gaming volume. Hundreds of concurrent users can easily saturate a single blockchain. Games often have thousands of users playing at any given time; popular ones can peak in the tens of thousands.
- Under typical load a block confirmation takes an excess of 10 seconds, while heavy loads can sometimes reach near 30 seconds. [4] This latency is incurred for every transaction involving the live blockchain. Such delay mars the user experience, causing unnecessary frustration with game play. Furthermore, because of finality cascades, the probability that a transaction will fail to register on the blockchain increases with network congestion.
- Ethereum currently only supports transaction fees in Ethereum (aka "gas"), requiring users to maintain a standing ETH balance. At the time of this writing, *gas cost* ranged from $.10 to $.30 USD per transaction;[5] a single game might incur dozens of transactions (say, one for each bet or

[4] https://etherscan.io/chart/blocktime

[5] https://ethgasstation.info/

confirmation). This racks up an unacceptable burden on players, as well as making it more difficult for an app to compete against “free” alternatives.

- Publicly viewable Ethereum smart contracts are susceptible to manipulation and attack. A notorious example of this is the Decentralized Autonomous Organization (DAO) hack. A venture capital fund in cryptocurrency had approximately $50M USD stolen from it because of a coding error in their smart contract. [6] The DAO hack was such a seismic event it split the community into two camps, resulting in a fork called Ethereum Classic. [7]
- Proof-of-work blockchains are hideously inefficient. Because of the competition of servers to mine the next block, each new block created wastes the energy of the efforts of all the losing servers competing for that block. This results in rampant energy consumption and inflated transaction costs.[8] The prevailing blockchain model is unsustainable, from both environmental and economic perspectives. Alternate models like proof-of-stake attempt to address these issues but have yet to see adoption because of a lack of incontrovertible proof they are secure. [9]
- Cryptocurrencies are *difficult to regulate* in the first place, let alone well. Their distributed nature makes even the determination of jurisdiction a thorny problem. While the utopian ideal of a citizen-empowered world is appealing, the sobering reality is that cryptocurrencies have enabled just as much undesirable crime and insurrection as desirable borderless commerce. [10] The future of successful cryptocurrency-backed business lies in cooperation with

[6] https://en.wikipedia.org/wiki/The_DAO_(organization)

[7] https://en.wikipedia.org/wiki/Ethereum_Classic

[8] https://www.welivesecurity.com/2017/12/12/cryptocurrency-kilowatt-hours-counting-costs/

[9] https://en.wikipedia.org/wiki/Proof-of-stake

[10] https://www.washingtontimes.com/news/2017/aug/10/bitcoin-value-surge-sign-of-criminal-activity/

regulatory authorities and achieving both community acceptance and legal legitimacy. [11]

Classic client-server architectures usually offer fast, efficient performance, comply with local laws, and afford a baseline level of security. For non-sensitive content distribution like public websites, they are a perfect fit. But for sensitive and / or financial applications (gambling in particular) they can raise red flags:

- A fundamental problem with most designs is that they presume the operator is trustworthy and can function as a *trusted third party*. Under regular conditions this may be true, but when large sums of money are involved this has routinely been proven false. There are many documented cases of game-rigging, collusion, etc. that involve server access. [12] It is noteworthy that cheating most often originates from rogue employees or owners. Thus, a system must be trustless: users must be protected from shady businesses, companies must be protected from unscrupulous individuals, and all peers must be protected from one another.
- Internal operation is typically opaque to external users. This makes it difficult if not impossible to ensure verifiability or reliability. Going hand in hand with trust, this is another major concern with classic server implementations.
- Static servers are susceptible to several well-known attacks. [13] Data centres are in the business of protecting servers from these kinds of attacks and are swift to remove vulnerabilities as they become known. Note that most of the concerns arise from a single, fixed location. A central location permits traffic-based attacks that are less feasible in a more distributed system.
- One server can present a single point of failure. This can be compensated for by server farms and other redundant setups. Note that a service failure can occur through means both innocent (say, eventual hardware breakdown) and

[11] https://www.inc.com/will-yakowicz/startups-law-enforcement-agencies-catch-criminals-who-use-cryptocurrency.html

[12] https://www.casino.org/rigged-casino-guide/

[13] https://technet.microsoft.com/en-us/library/cc959354.aspx

malicious (say, a denial of service attack). A less severe but related phenomenon is system overload: when capacity is exceeded processing takes a noticeable hit.

- Central accounting as a failure bears special mention; it's not precisely a server feature but is often implemented using them. Systems that require users to deposit funds into game accounts are susceptible to fraud. In 2013, the founder of Full Tilt Poker pled guilty to embezzling money in a Ponzi scheme using player accounts. [14] Other high-profile cases like Absolute Poker were prosecuted. [15] PKR Poker (a UKGC regulated company) recently failed, and players would have lost over $2M in their user accounts if PokerStars hadn't bailed them out. [16] Moreover, central accounting also exposes a company to risk. Shady players can use the time differential of fund clearing, multi-posting, credit card chargeback, and other tricks to launder both fake and dirty money through online sites maintaining financial user accounts. Taken altogether, this emphasizes the need to comply with regulations intended to protect consumers and businesses alike.

A simple way to summarize the division between blockchains and servers are the open-source and proprietary code perspectives. Blockchains were designed with a transparent community in mind, while servers were designed with business protection in mind. Both of these are important features to retain, and each technology has pros and cons. What we want is a way to fuse the strengths of each approach, preserving all the advantages while removing all the disadvantages.

In order to get the best of all possible worlds, our solution must be a quantum LEAP.

---

[14] https://indiancountrymedianetwork.com/news/business/founder-of-full-tilt-poker-pleads-guilty-to-fraud-in-federal-court/

[15] https://www.digitaltrends.com/computing/pokerstars-full-tilt-absolute-poker-busted-for-fraud-money-laundering-in-fbi-crackdown/

[16] https://calvinayre.com/2017/07/06/poker/pokerstars-rescues-pkr-players/

8.2. LEAP ARCHITECTURE SOLUTION[17]

There are four distinct communities that we wish to service well:

- **Players** – These are people who want to sit down, have fun, and gamble safely. They are interested in aspects like user experience, performance, convenience, and reliability. Most players are satisfied with a reasonable assurance that everything is on the up and up, usually achieved by an examination and endorsement by a trusted authority.

[17] US Provisional Patient Pending

- **Banquiers** – These are parties who are willing to invest large sums to become their own online casino. They are interested in aspects like verifiability, security, rates of return, and asset protection. They need to know the precise implementation in sufficient detail to make an informed decision. [Banquier comes from the French for banker.]
- **Businesses** – These are organizations interested in conducting their enterprise online by harnessing the latest technologies. They are interested in aspects like cost, IP protection, efficiency, and risk factors. They demand that solutions perform as advertised, giving them a competitive edge in their markets while safeguarding their trade secrets and business practices.
- **Regulators** – These are legislators interested in protecting society by ensuring minimum quality standards are met. They are interested in aspects like leverage, accountability, controls, and forensics. They require that practices could potentially stand up in court, successfully prosecute criminal activity, and effectively curtail harmful operations.

Note these communities aren't mutually exclusive. For example, we expect a significant overlap between players and Banquiers. One combination is particularly noteworthy, namely Banquiers with a business mindset effectively view Blockdraw as an investment vehicle. We are dedicated to ensuring that investment in Draw Tokens yields dividends. Our business strategy includes cultivating the token economy as well as creating stable services and profitable products.

Many of the desires of these diverse communities overlap, but there are two specific areas where they come into conflict. The first is transparency vs. opacity. Generally speaking, players have the greatest stake in complete transparency, while businesses need tighter access control; Banquiers and regulators fall somewhere in between.

There are legitimate and justifiable reasons to prevent public dissemination of sensitive information. Thus, we must make a subtle distinction between *desirable confidentiality* and undesirable secrecy. Also observe that most sensitive information is timely: usually, knowing something today is more valuable than knowing it tomorrow.

Another area of seeming disagreement is centralization. Generally speaking, crypto-communities comprising players, Banquiers, et al. want full peer-to-peer decentralization, while businesses and regulators want more centralized architectures. But upon closer inspection it turns out this really isn't a contention at all. Businesses and regulators don't desire centralization, they want to perform their functions well and so far only monolithic solutions have worked. Given the rise of outsourcing and remote workers, businesses have accepted the premise of decentralized business processes. And most regulators would be amenable to any solution that enabled them to stop more criminal activity, whether it was centralized or not. They simply haven't been shown a viable decentralized model yet.

Until now.

Our LEAP solution has four distinct blockchains: *Live*, *Execution*, *Audit*, and *Performance*. Each of these is based on the Ethereum blockchain and can run smart contracts. However, the parameters of each are tuned for its particular function. Let's describe each in detail (though not in letter order):

- Live – This is the live, public Ethereum blockchain as we know it. It costs gas, has slow transactions, is inefficient, and possesses vulnerabilities; it also has fully open verifiability, proof-of-work integrity, and is the ultimate ledger for ETH accounts and Draw Tokens. We maintain smart contracts on the Live chain that are limited to fiscal accounting, harnessing its forte: decentralized peer-to-peer transactions. This chain will mostly be used by Banquiers to track their finances.

- The Live chain exists on thousands of servers run by independent miners around the world. The remaining chains (PEA) live on a different, smaller network of managed servers; locations are chosen strategically to maximize coverage and minimize latency. Initially, Blockdraw will manage this network, and then hand it off to a strategic partner like a Content Delivery Network (CDN). (As we will see later, who manages these servers is actually less important than who controls the Live chain servers.) The following chains do not cost gas, are more efficient, remove vulnerabilities, and enable new features.

- **Performance** – This is a low-latency highly responsive chain that is used in real-time during gameplay. It records information like bets, consensus data, random outcomes, player choices, and everything else needed to reconstruct an entire game. The Performance chain is read-only viewable to the public at large; we will provide an explorer that allows anyone to check information on it in a manner that doesn't impair its high-performance nature. This chain is of most interest to players, both during play for its snappy speed, and afterwards for game analysis.

  Note that our performance chain is not like previous incarnations that have already been tried. It is not a cached local copy of the Live chain used to increase

performance; all chains are unique, and the Live and Performance chains are not the same. It's not a private chain, because we're making it fully public. Even though we restrict access to authorized clients, it's not a permissioned chain, either. [18] Those chain experiments failed because they were unable to offer segmenting and confidentiality, which we can provide.

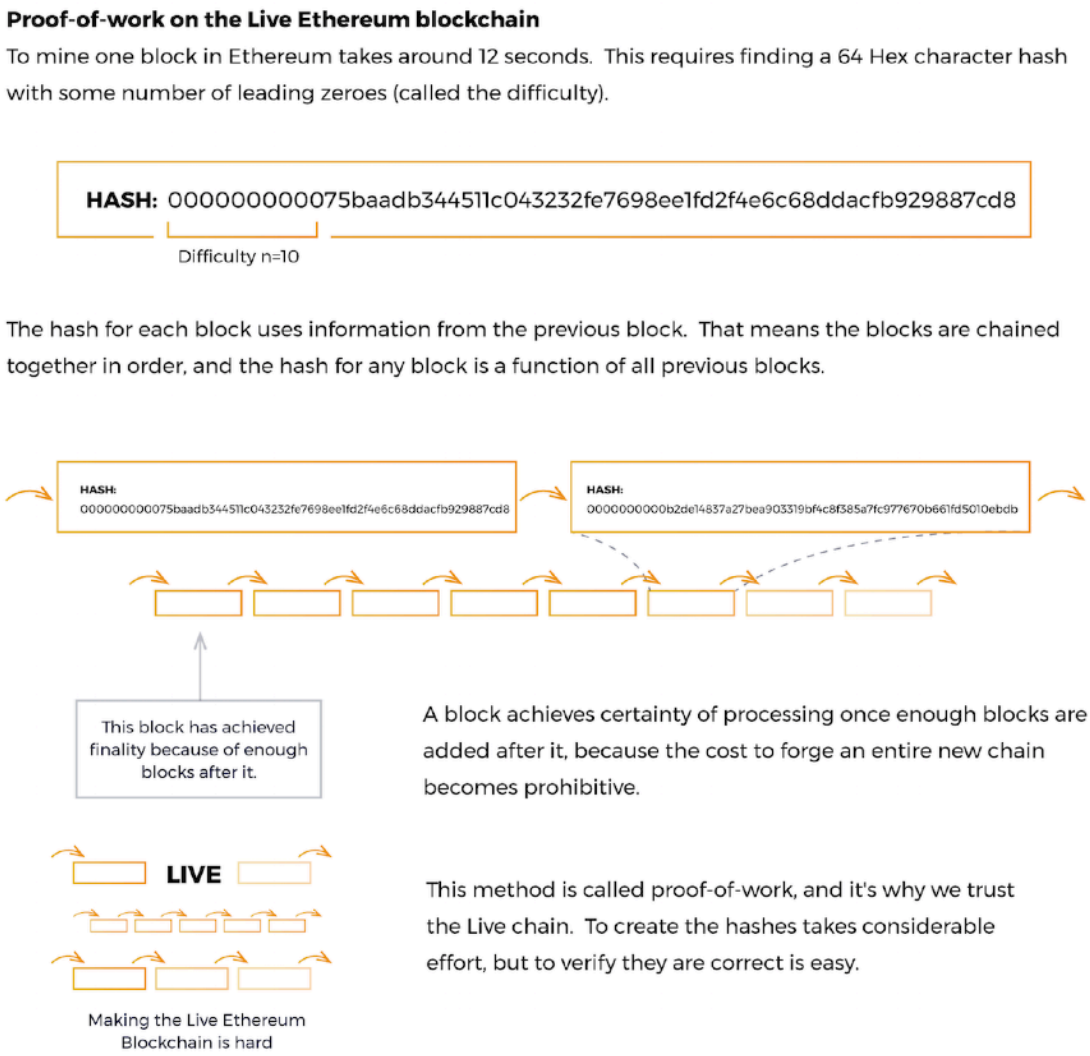
- **Execution** – This is a low-latency chain that is used in real-time during play. It runs the smart contracts used by a game in a secure execution context. It contains things like: game logic, game accounting, user accounting, etc. This chain is not viewable from the outside world and isn't even reachable externally. Smart contracts on the Execution chain only accept calls from the Performance chain. This chain is of the most interest to businesses, as it protects their business practices from scrutiny while still enabling them to function.

  This methodology is called encapsulation and is a well-accepted technique in programming. Since the functions are on the Performance chain, we've publicly committed to an Application Programming Interface (API). [19] But because the actual code that runs is on the Execution chain, we've preserved information hiding and modularity. This shields us from the vulnerabilities present in the Live chain, conforms to best coding practices, and creates a place to protect confidential programs and IP.

- **Audit** – This chain gathers together all digital forensics surrounding online activity in one place. In addition to logging, its smart contracts provide alerts, red flagging, and account protection. It contains things like: IP and MAC addresses, byzantine behaviours, hardware hashes, access logs, and changelogs. This chain has the provenance that a regulator would need to audit our compliance, or a criminal prosecutor would require in order to establish case facts. As such, it is

[18] https://www.coindesk.com/private-blockchains-gone/

[19] https://en.wikipedia.org/wiki/Application_programming_interface



custom designed for regulators, and only accessible via legal compulsion through proper channels.

The PEA chains are fundamentally different than the Live chain. The Live Ethereum blockchain (LEB) was constructed under the assumptions that a) servers mustcompete with one another using Proof-of-Work, and, b) trust can only be determined by consensus. It is this combination that gives the LEB its powerful integrity; however, it also incurs costly inefficiency. The PEA chains are designed with the assumptions that a) the servers can cooperate with one another and b) trust can be transferred from the LEB. This allows for simplification of their mining,

Notary stamp integrity of the LEAP system

To mine one block on our PEA chains has no difficulty (n = 0). It can be done as fast as the computer can process it, which gives our system high performance.

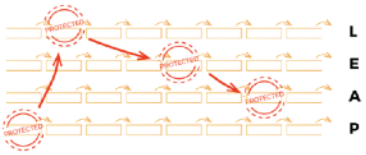
HASH: 9ax7b3252r15860e5f2d2634878bdaa80dd6f31de314ee2f785f5eda3a2bfd76

No difficulty n=0

Making a Performance, Execution or Audit chain is easy

That means PEA has no proof-of-work; it would be easy to generate another chain. Instead, we prove our integrity using a block hash in a notary stamp we place on the Live chain.

This irrevocably commits the state of our chain, because to generate any hash is easy, but to generate a specific hash is virtually impossible. Once the stamp is public, we can't create a forgery.



To further increase integrity, our chains notary stamp each other. That means we have verifiability and create a forensics trail that can establish impeccable provenance.

LEAP as a system offers a feature that one blockchain alone can't: proof that can legally stand up in court. This is of great interest to regulators, legislators, and businesses.

consensus, and communication protocols that lead to dramatic increases in performance. Thus, we need to demonstrate how we inherit trust from the Live chain.

We use *cross-hashing notarization* similar to Komodo and their delayed Proof-of-Work. [20] Whenever a LEAP chain accesses another chain, it supplies a notary stamp comprising, in *addition* to the transaction data:

- The sequential block number of the latest consensus block of the originating chain
- The blockchain hash of that block
- The unique chain ID of the originating chain
- The unique user ID of the requestor, encrypted

This notary stamp is infeasible to forge, as it requires producing one specific SHA hash from among 2256 hashes. Once accepted by the Live chain, all blocks on the PEA chain prior to the stamp can be considered irrevocable.

Our improvement on Komodo is to not only notarize the PEA chains to the Live chain, but also to each another. This gives the LEAP system much greater integrity than an individual blockchain could provide. The cross-fertilization also means that we can use the same proof of correctness as HashGraph [21], and the calculation of parameters is the same as for any blockchain. In summary: cross-hashing notarization inherits the same trust, finality, and verifiability as the Live Ethereum blockchain, while providing greater performance, efficiency, and integrity. We get this at minimal gas cost overhead, since we only notary stamp in accounting transactions to the Live chain we had to perform anyway. Thus, LEAP verifiability is provably *independent of who manages the PEA servers*.

This has a fortuitous side effect in terms of scalability. With a single Proof-of-Work blockchain, the difficulty must increase with number of servers added, and the overall system becomes less efficient. Our LEAP solution is reasonably insensitive to scale. Additional servers add lower latency and more resources but are balanced by greater network and consensus requirements. Notary stamps themselves have

[20] https://www.komodoplatform.com/en/technology/whitepapers/2018-01-13-Komodo-White-Paper-Full.pdf

[21] http://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

negligible impact on performance, as values are known at the time of transaction. They cost no calculation, only minor storage.

To the dyed-in-the-wool open-source community, the deliberate shielding of the Execution chain is perhaps the least palatable aspect of the architecture. But the unfortunate reality is that the public exposure of smart contracts on Ethereum is insecure. Early on Bitcoin tried using its Script language as smart contracts, but the feature was repeatedly exploited. Eventually Bitcoin was forced to give up and remove the vulnerability. Ethereum is in a similar state, with the advent of tools like Porosity [22] being the harbinger of ready reverse-engineering of smart contract byte-code. The fundamental problem is developers continue to mistake cryptographic integrity for *executional security*; blockchains possess the former but not the latter. These are not abstract, philosophical concerns. The DAO hack cost $50M USD. The Parity Wallet hacks cost over $150M USD. [23] At a certain point, enough money will be lost where the Ethereum designers must concede public smart contracts are flawed.

There are two ways in which we offer assurance even into the “hidden” Execution chain. The Performance chain rapidly varies as games are played, but the Execution chain only changes on software updates. That means the hashes on the Execution chain are like code version numbers, except more binding. These are cross-hashed with the Performance chain regularly, uniquely identifying which code revision ran which exact game.

Furthermore, our goal is confidentiality, not opacity. Thus, we regularly prune each of the PEA chains and upload the pruned tail into an *open* format like Inter-Planetary File System (**IPFS**). IPFS creates a permanent and decentralized method of storing and sharing files through a content-addressable, peer-to-peer hypermedia distribution protocol. The practical reality for code is that only the last couple major versions need to be protected; older versions can be harmlessly

[22] https://github.com/comaeio/porosity

[23] https://medium.com/@Pr0Ger/another-parity-wallet-hack-explained-847ca46a2e1c

“declassified” so to speak. Other rules apply to other chains; to illustrate, we may not legally be able to reveal portions of the Audit chain if they are being used in a court case. The eventual goal is total transparency ,while still retaining contemporary confidentiality and cooperative compliance. This is precisely the model employed by the United States government as set forth in the Freedom of Information Act. [24]

At this point we’ve established that the architecture is sound, meets all our design criteria, and satisfies several diverse communities simultaneously. We’ve additionally compensated for some known weaknesses, such as the distributed network of LEAP servers having greater integrity than a single blockchain and greater security than a single server.

But what about the gameplay itself? How can we play peer-to-peer games without any party trusting any other? Fortunately, this problem has already been elegantly solved. Blockdraw is not only on the forefront of technology creation, but we also employ the most advanced algorithms.

8.3. BLOCKDRAW’S NON-SHUFFLING MENTAL POKER ALGORITHM

Traditionally, online card-playing games closely mimic what occurs in real-life. The first step is usually to shuffle a deck of cards, then to deal according to the rules of the game, and then play. In real-life, the shuffling presents a potential exploit, because dealers can cheat. They can stack the deck, float cards, bottom deal, top deal, and more. There’s no way to prevent this kind of skilled cheating, so the accepted practice is to rotate the dealer to even out any advantage gained.

Online gambling has a similar pitfall. The first step is shuffling the deck, an expensive computer operation. But that gives the dealer an unfair advantage, because their program now knows the contents of the deck. Two approaches are common. The first is to treat the dealer as a trusted third party, which fails when they aren’t. The second is to use an encrypted shuffle to hide the cards from the

[24] https://www.foia.gov/

dealer, but this creates even more computational overhead. Ideally, what we want is a way to deal cards that is fair and efficient.

That's what the *Golle* algorithm does. [25] In 2005, at the Palo Alto Research Center, Phillippe Golle created a fully decentralized peer-to-peer method to deal cards that is significantly more efficient than extant Mental Poker algorithms. [26] The essential innovation is: rather than shuffle a whole deck up front, we randomly choose a card each time one is needed. The cards are encrypted in such a way that:

- The back of each card uniquely identifies the front. Anyone can be shown all the card backs and verify all the cards are there.
- No one knows which card is which. But since the backs are distinguishable, we can easily tell when cards are different. (or the same, see collisions below)
- A card front can only be revealed when all peers cooperate. This is done by sharing a joint key distributed among the group of peers.

To be even more precise, the Golle algorithm doesn't select a card from a deck. It chooses a random number between 0 and r-1 from among r = 52 outcomes, and we can interpret the numbers {0, 1, … , r-1} as being distinct cards. Moreover, we can choose any integer r > 1 we want. That means Golle works for *all games of chance*, not just card games. We can pick a Chinese tile, spin a wheel, flips coins, and roll dice using the same method. This covers all popular casino games, including but not limited to: Baccarat, Blackjack, Poker, PaiGow Poker, PaiGow, Mahjong, Sic Bow, Craps, Roulette, and Slot Machines.

The only subtlety is that there are two different games of chance: independent trials and alphabet depletion. Rolling dice is easy because we don't need to know the previous rolls. But once a card is dealt or a (unique) tile is chosen, it can't be used again. Golle calls this handling a *collision*, and the solution is easy: just randomly deal again. This incurs extra computation when it happens, but since the number of

[25] http://crypto.stanford.edu/~pgolle/papers/poker.pdf

[26] https://www.revolvy.com/main/index.php?s=Mental%20poker

cards dealt is small compared to the deck size, this is a minor issue. Even accounting for collisions the overall cost is still much smaller than whole-deck shuffling: Golle uses 2-4 times less modular exponentiations than the second best runner up, which does full shuffling using mix-networks. [27]

Let's examine the algorithm in more detail. Golle needs a few supporting pieces to work properly, all of which are well known and have reference implementations:

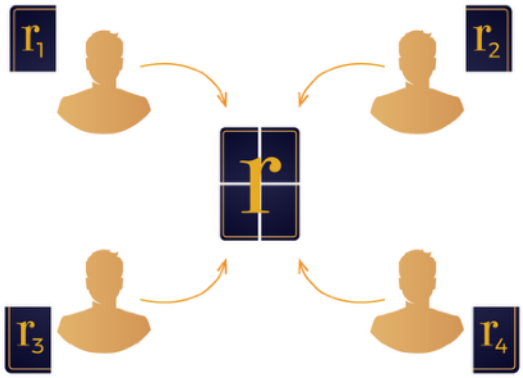
- **Secure** communication **protocol**. The peers need to be able to interact with each other without anyone else eavesdropping. There are a wide variety of equivalent choices here; we'll be using *RFC 4419*. [28]
- **Homomorphic encryption**. If E(r) is the encrypted ciphertext of plaintext r, this means that $E(r_1)\ E(r_2) = E(r_1 + r_2)$. Several options are available; we use *El Gamal*[29], which was also chosen in the Golle paper.
- **Distributed private key**. Let p be the number of players. We need a private key $k = k_1 + k_2 + \ldots + k_p$ jointly held so that each player i only has the part k_i. The clear winner here is the *Pedersen Protocol*. [30] (not to be confused with Chaum-Pedersen, another cryptographic tool)

[27] http://www.arijuels.com/wp-content/uploads/2013/09/JJ99b.pdf

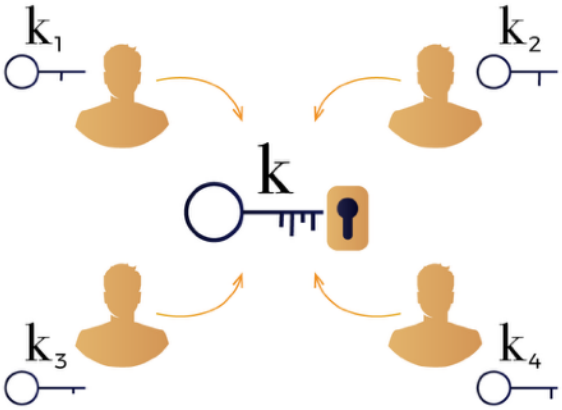
[28] https://tools.ietf.org/html/rfc4419

[29] https://en.wikipedia.org/wiki/ElGamal_encryption

[30] https://www.cryptoworkshop.com/ximix/lib/exe/fetch.php?media=pedersen.pdf



Each player chooses a random number $\mathbf{r}_i$. The group adds them all together securely to determine which random card **r** is dealt. No one can manipulate the outcome.



Each player has one piece $\mathbf{k}_i$ of a private key **k**. To reveal a card, all players must cooperate together. No one can see a card they aren't supposed to see, before the rules say they can see it.

We must integrate these three features together to reveal a card. We need the entire joint key k to decrypt a card. Each player contributes their piece k_i, secretly encrypted into $E(k_i)$. Then all the pieces are combined homomorphically

$$E(k_1)\ E(k_2)\ \ldots\ E(k_p) = E(k_1 + k_2 + \ldots + k_p) = E(k)$$

into E(k), which is then used to unveil the card. The magic of the algorithm is that all this can be done without anyone ever revealing the ki; only the ciphertexts need be used. For a face up card, everyone securely shares their E(ki) with all other players, so everyone can independently calculate the card. For a card shown only to one player, every other player securely tells them their E(ki), so only they can see what their own card is.

Choosing a card at random uses exactly the same process, with all the k_i replaced by r_i. Everyone randomly chooses a number r_i in {0, 1, ... , r-1}, we add the results using homomorphism, and take a final number modulus 52 to ensure we are in the correct range. So altogether, we can only randomly choose the card as a group, and

only reveal the cards as a group. Thus, every peer is guaranteed their participation is necessary and consequential.

The Golle algorithm is logically correct but isn't practically robust. We've made significant improvements to account for real-world situations like network congestion and player timeouts, as well as shored up common exploits like false testimony and buffer overruns. We've further extended the theory by proving the probability distribution function, which was provided for in the original paper. And, we have made other proprietary improvements that significantly extend the technology. We can prove that as long as there is one honest player (using the algorithm as intended) the deck will be fair (random outcomes are equi-probable). All our improvements and their proofs of correctness will be released in a separate paper.

The Golle algorithm is a perfect match for our intended usage. It enables us to create any casino game of chance in a fair, decentralized way. Even more serendipitously, it generates exactly the information needed to provide airtight verification. This dovetails nicely with our LEAP architecture. To illustrate, the initial step in Golle is generating all the card backs (which are the encryptions E(0), E(1), ..., to E(r-1)). Every player sees this set before play begins, so they may verify all cards are present. Thus, it is safe to publicly post to the Performance chain. From that point forward, our application has created a binding commitment to a fair game; there's no way that we (or any other player) can alter the deck. Similar binding commitments and consensus data are published each card draw and player action, making it possible to reconstruct the entire game, and impossible for anyone (us included) to later deny or spoof what happened. This reconstruction can be done without reference to implementation, which is another reason why the code on the *Execution chain is ultimately superfluous to verification*.

We've now got a good sense of the technologies, architecture, and algorithms used that prove Blockdraw is verifiably secure and fair. So, what will the games actually be like?

8.4. APPLICATION DETAILS

The application runs on several *platforms*. Initially we will deploy applications in Windows and Mac. Then we'll create mobile applications in Android and IOS. Eventually we want to also support Linux and HTML5 compliant browsers. The latter requires we iron out certain security issues involved, some of which are beyond our ability to control.

The application has basic *wallet* functionality. It prominently displays the Draw balance, has a transaction history, and can perform simple transactions. It has buy-in and cash-out features to convert to different fiat money and other cryptocurrencies. This is primarily for user convenience. Since the Draw Token is ERC20 compliant [31], it is already compatible with all major existing wallets and exchanges. Players are free to use what they prefer.

8.5. CROUPIER TABLE MANAGER

The application logic is run in conjunction with the LEAP servers. Two areas bear special mention. The first piece of logic is Croupiers. Croupiers manage table operations and play in the "house position" in certain games. A croupier at a roulette wheel handles bids and spins the wheel, while a croupier at a blackjack table has their own hand players compete against. Croupiers may make play decisions that influence game play when they are involved in the game. The decision algorithms for croupiers are well known, like a Blackjack dealer always hitting on a soft 17 or below.

Initially, our Croupier will be automated. They are an added extra peer in the Golle algorithm who is the guaranteed honest player that keeps the deck fair. This Croupier is still a peer in Golle even if they do not participate in the game and make no play decisions. Eventually, we want the Croupier to be our in-game call support mechanism employing an actual person who combines the roles of referee,

[31] https://theethereum.wiki/w/index.php/ERC20_Token_Standard

arbitrator, and troubleshooter. This staff would be able to resolve support issues for games in progress, as if a pit boss was called to a casino table in real life. If a player calls for a human supervisor, normal play is put on hold and the app enters a Resolution Mode. Then our support staff can chat with everyone at the table, review the hand history and administrative logs, determine whether technical problems or misplay occurred, and make a determination what the fair resolution should be. The need for this intervention should be rare, but if it does happen, we want to immediately provide the human touch.

Blockdraw always tries to match players with banquiers where possible, but sometimes a player won't be able to find a suitable banquier table. In order to ensure that players can always find a table to play at, Blockdraw serves as the default banquier. These fallback tables are run by automated Croupiers and offer the standard limits and play found in real-world casinos. Banquiers may use automated Croupiers to earn tokens on their stake automatically, or to play the house position at their own table themselves. The former option enables running many tables simultaneously, while the latter is only one table at a time. Banquiers make all decisions for their table(s), and will eventually be able to customize all settings.

Player-banked casinos and the croupiers handling them are a vital component to our business and token strategies. Croupiers functions will include sophisticated analysis tools that enable banquiers to calculate expected earnings given the parameters of their table(s).

8.6. RANDOM NUMBER GENERATION

The second piece of logic is *Random Number Generation* (RNG). Every peer in Golle needs to be able to generate a random number, which when combined with everyone else's number, determines the next card dealt. That means we need RNG for the Croupier as well as each client application. A significant benefit of the Golle

algorithm is that each peer can force the deck draw to be fair by randomly choosing their own number, independent of the choices of every other peer. One honest player keeps the deck fair, without the need for a trusted third party. Many common RNG algorithms and approaches are considered acceptable; we'll use software RNG on the client app and more sophisticated hardware RNG for the Croupier. Blockdraw follows the standard industry practice and will have its RNG certified by an independent agency.

Note that making non-random choices requires subverting the client RNG using memory hackers or reverse-engineering the app itself. So in practical terms, this means that if a player uses our app as intended without actively cheat hacking, they are protected against those trying to fix the deck. One of the many beauties of the Golle algorithm is that because every peer is independently choosing a random number, no subset of peers can manipulate the outcome. The Croupier assures that all the players can't collude together, and that even if some are actively hacking their client apps, the deck still remains fair. Furthermore, each player can separately guarantee the same thing: as long as they play honestly, outcomes are provably random.

8.7. EXAMPLE INITIAL USER EXPERIENCE

Alice has heard from Bob how fun gambling on Blockdraw is, so she's decided to check it out. After downloading the game, she logs in and takes a look around.

[Behind the scenes Blockdraw has already performed several checks to validate that Alice is legally able to gamble in her locale. For example, certain age verification is done to ensure that she isn't an underage minor. Other Know-Your-Customer checks are performed as well, like blacklisted jurisdictions, banning compliance, self-exclusion, and fraud checks.]

Hey, she already has an invitation from Bob waiting for her! When she clicks on it she reads the little information blurb and discovers, wow, she can do a lot more

than just play with Banquier Bob. She can also spectate high-roller events, as well as keep abreast of the top ranking players for each game.

Spectation is an important part of the casino experience. People like watching players gambling for high stakes almost as much as they like gambling themselves.]

She wants to play a game with Bob, so first she loads in some Draw Tokens into the game. She buys 1000 Draw. She accepts the invite to play Baccarat at Banquier Bob's Table. He's currently backing another game, so she watches that match until he's done.

[The table selection screen has a variety of options to help players find, filter, and highlight tables. There are many other ways to matchmake Banquiers and players, like invitations.]

The two of them pair up head-to-head at Bob's table.

[Behind the scenes a great deal happens. Smart contracts on the Live and Performance chains have negotiated an escrow of Alice and Bob's Draw tokens. Both have implicitly agreed to pay tokens if they lose a game, and are guaranteed to gain tokens when they win. This costs real gas, which is covered individually. This only needs to be done once—the first time a player or Banquier plays a game during a single session; they may also voluntarily choose longer durations to stake their funds, and thereby avoid excess gas costs.]

They have a fun and exciting time playing.

[In the background, every card draw and choice by any player, Banquier, or dealer is recorded to the Performance chain. At each step, smart contracts ensure that every bet is backed by a financial surety to pay. These smart contracts reside on the PEA servers, and thus do not cost gas. Blockdraw absorbs the expense of running the servers.]

They play for a while and then leave the table.

[The smart contracts finalize all accounting and ensure the Live chain is updated with the correct information. Payments are made directly from the escrowing smart

contract, without passing through an intermediate account owned by Blockdraw. Losers cover gas costs, deducted from the funds they send. Overhead payments are made directly to Blockdraw, such as a table rake, croupier service fee, or percentage of winnings, depending on the specific game and the prevailing customary structure. All remaining escrowed funds are returned to the player's token address, which costs real gas. Thus, a typical play session incurs two Ethereum gas fees: to start playing, and to stop playing.]

Alice had fun. She chats with Bob for a little bit before calling it a night and logging off.

[Final security checks run to ensure Alice's funds are now completely her own again. Blockdraw checks for potential zombie escrows and other states that might have occurred due to esoteric errors. For players, tokens are escrowed while they are logged on. For Banquiers, those using croupiers can explicitly authorize us to continue managing their tokens after they have logged out. Croupiers are rented for fixed periods of time in advance, and after that time expires, we perform similar integrity checks as for players. As another failsafe, a hard coded 24-hour non-activity return is put into all smart contracts. Thus, funds always revert to owner control and aren't kept by a Blockdraw account.]

8.8. BLOCKDRAW INNOVATIONS

8.8.1.BUSINESS-CLASS SECURITY, CONFIDENTIALITY AND INTEGRITY

Blockdraw's innovation was to recognize the benefits of all available technologies and fuse the best pieces into a custom-made process. We took the security and speed of servers and combined them with the integrity and confidentiality that the blockchain affords to create a solution that is superior to traditional state channels. Public smart contracts are simply not secure; monthly hacks have demonstrated this point and serious business leaders can see this, but the community still wants

the verifiability and trustless capability the blockchain affords. It turned out that the solution was available: LEAP! By marrying the best of the blockchain with the best of traditional server architecture we created a world class platform and used the blockchain for all its intended purposes.

8.8.2.IMPECCABLE CHAIN OF CUSTODY

Businesses don't just require security, regulators demand it; they also demand audit trails and secure random number generation. Since we operate card by card, dice toss by toss, or spin by spin, we record everything live on our audit chain. Not only that—everything we do can be recorded on-chain. We are able to offer regulators, data analysts, or business leaders unprecedented records securely on our blockchain.

8.8.3.SOFTWARE SDKS

Moreover, we aren't the only ones seeking answers to the hard problems of combining verifiability with performance. So, we will structure our technologies into Software Development Kits and turnkey solutions that game developers, online businesses, and industry regulators could all benefit from. That means anyone can license our tech to run games, business contracts, or proof-of-compliance, resting easy that the underlying platform is confidential, scalable, and secure and still highly verifiable. And the Ethereum community gets a high-performance blockchain system that doesn't slow down the live Ethereum network.

8.9. MILESTONES AND PLANS

Here are the expected phases of our product development, along with specific deliverables. We include relevant business and operational goals we'll need to achieve in order to meet our milestones.

8.9.1.MILESTONE 1: COMPLIANCE DEMO (MARCH 2018)

This is a working proof-of-concept necessary to comply with certain financial regulations. It enables US investors to participate in the ICO.

The highlights of this first demo version are:

- A functional game supporting Baccarat
- Deployable on at least one platform
- Basic user authentication and sessioning
- Uses all peer-to-peer crypto-technology, specifically the Golle algorithm
- Supports Test and Live modes (Test is for demonstration, Live uses real coins)
- Uses smart contracts on Live chain for escrow and summary accounting (Live mode)
- Uses smart contracts on Performance chain for betting and hand accounting
- Single PEA server operational
- Simple automated Croupier managed by Blockdraw
- Uses server code and logs in lieu of Execution and Audit chains

8.9.2.MILESTONE 2: ALPHA PROTOTYPE (Q3 2018)

During this phase we expand the development team and build out both our product and our operations. The primary product goal is to upgrade the compliance demo to a stable application, refactoring it to professional coding standards. The

operations goal is to create at least three independently functioning working groups.

The highlights of the alpha version are (over and above what's in the demo):

- Deployed on more platforms: Windows, Mac and possibly Linux
- Full user authentication, including Know-Your-Customer checks
- Uses smart contracts on Execution chain for game logic and business practices
- Multiple PEA servers operational in disparate physical locations
- More sophisticated Croupier
- Banquier Tables, Basic Limit Settings
- Uses server logs in lieu of Audit chain

Draw Token holders may request access to the alpha prototype. The alpha is intended to certify our progress and enable community feedback. **The alpha should not be used for serious gambling**. The incomplete implementation may have security holes. *Users assume all risk of playing the alpha in Live mode, including loss of coins due to bugs.*

8.9.3.MILESTONE 3: BETA GAMES (Q1 2019)

Once our product becomes stable enough for fully Live play, we graduate to beta status by removing Test mode. At this point most of the core application features are implemented, and our operations should be smooth. Our personnel plan at this stage is to attract top tier executive and management talent.

The highlights of the beta are (over and above what's in the alpha):

- At least five casino games: Baccarat + 4 others TBD
- Deployed to Android, IOS, Windows, and Mac
- Full LEAP system, cross-hashing, blockchain explorer, and integrity checkers

- Multiple PEA servers operated by strategic partner
- Real-time chat and communication in-game
- Automated and Human Croupier, Table Visiting, Resolution Mode
- Table search, sophisticated Matchmaking, full-fledged Banquier Tables
- Full Croupiers, including customizations, statistics, and play histories
- Fault Tolerance against network problems and byzantine behaviours
- Software Development Kit (SDK) for building Draw Token enabled games

All Draw Token holders will be issued beta keys and are encouraged to play under real gaming conditions. **The beta should not be used for high stakes play**. All security features will be implemented, but there is still a lingering possibility of undiscovered bugs.

8.9.4.MILESTONE 4: PRODUCTION RELEASE (Q3 2019)

We've now reached confidence that our products are ready for the big leagues. Our focus at this time is mostly external. We want to raise awareness through marketing, branding, and advertising; attract users (both players and Banquiers) and build community relations; and attentively nurture the token economy.

The highlights of the release are (over and above the beta):

- Customer support system, including quality control feedback cycles
- Watch lists and Social Media integration
- Spectators, Watch Mode, Table Privacy and Publicity Settings
- Platform-specific application integrity protection(s)
- Events, Leagues, Ladders, and Ratings

Since Banquiers can now declare the parameters of play at their own tables, people are free and able to play precisely how they want to. Have fun!

8.10. FUTURE VISIONS

Most of 2019 will be spent ensuring the growth and stability of the platform. During the same time, we will take steps to assist active and satisfied communities involved who believe in the Draw token. After our financial footing is secure, it's time to think bigger.

Here are some more projects we'd like to undertake:

- **Expand casino game offerings**. Once we've proven the model with a few games, it makes sense to apply it to all remaining casino games. The SDK makes the process of creating new games much easier.
- **Attract game developers**. The SDK enables new strategies by empowering game developers to use our mature infrastructure. This means they could create casino games on their own or incorporate Draw tokens into their existing non-casino games.
- **Partner with casinos**. We have the cutting-edge know-how to build peer-to-peer casino applications. Existing casinos have years of experience, brand recognition, and established networks. The combination has tremendous potential.
- **Create business solutions**. The LEAP system has many features attractive to turnkey businesses. In particular, it is well matched to business-to-business interactions where the protocols for negotiation, decision, and sale are well established.

At the beginning, we must perforce spend all our effort tactically to secure our success.

But success is only the beginning.

9. BLOCKDRAW GAMES

All of Blockdraw's lottery games will be guaranteed by Draw tokens in smart contracts provided by Draw or its B2C partners. Every game will have adequate funding available within the smart contract to meet winners' demands with a statistical chance not to exceed 5+ standard deviations of outcomes using a normal probability. A portion of Blockdraw's gaming margin is used to fund ongoing smart contracts so that they will always stay adequately funded as described above (eg. The Blockdraw Platform and Network).

9.1. CASINO GAMES

9.1.1.BACCARAT

Baccarat is a card game consisting of multi decks of playing cards, usually six (but the number of decks is statistically insignificant). The game usually allows 9 participant spots against a single participant draw. Each card has its own value, with face cards having a value of zero and Aces equal to 1. The game pits a player against a banker (not to be confused with a real casino banker). The classic game of "Punto Banco" has specific drawing rules that require both player and banker to act depending on the initial card drawn to each party. The object of the game is for one player to win with the highest numerical count, the maximum being a natural 9 (drawn with the first two cards). Several variations of Baccarat will be offered, some of which will allow participants to make their own decisions. The game has a side bet allowing anyone to bet on a "tie" between the banker participant and the player participant that traditionally pays 9 for 1.

9.1.2.BLACKJACK

Blackjack is one of the world's most popular games and has specific drawing rules. The game usually pits up to 7 players against the casino's hand. The casino draws last and his cards are usually not shown until the end of the game, forcing the players to act without knowing the casino's hand. The object is to get the highest hand up to 21; but, if you exceed 21 before the casino reveals its hand, you automatically lose. The game is traditionally multi-deck since card counting theoretically can give a player an advantage over the casino. Even where single deck Blackjack is still played the game is usually reshuffled before the end of the deck, often based on the dealers count. Face cards are worth 10, Aces are worth either 1 or 11. There are several side bet options and various opportunities to split cards for additional wagering opportunities.[32]

9.1.3.MAHJONG

Mahjong is a Chinese tile game consisting of either 136 or 144 tiles. There are 16 rounds in a game with a winner after each round. Blockdraw will focus on the 136-tile version. Blockdraw believes that it will be one of the first to offer this game on the blockchain to the Asian marketplace.[33]

9.1.4.SIC BOW

Sic Bo, meaning "dice pair" is an *ancient* Chinese gambling dice game. The game pits participants against the casino to bet on specific dice rolls. Like craps it offers many types of bets. The game is widely played in Asia.[34]

---

[32] https://en.wikipedia.org/wiki/Blackjack

[33] https://www.thoughtco.com/how-to-play-mahjong-687535

[34] https://wizardofodds.com/games/sic-bo/

9.1.5.PAI GOW & PAI GOW POKER

Pai gow is a Chinese gambling game, played with a set of 32 Chinese dominoes.[35]The name "pai gow" is loosely translated as "make nine" or "card nine". This reflects the fact that, with a few high-scoring exceptions, the maximum score for a hand is nine. The value of a hand is determined by adding up the total number of dots on its two tiles and dropping the 10s digit.

“Pai gow poker is a version of pai gow that it is played with playing cards bearing poker hand values, instead of pai gow's Chinese dominoes. The game is played with a standard 52-card deck, plus a single joker. It is played on a table set for six players, plus the dealer. Each player attempts to defeat the banker (who may be the casino dealer, one of the other players at the table, or a player acting in tandem with the dealer as co-bankers).”[36] The game is played in Asia, but is more popular in the US.

9.2.GAME DESIGN MATTERS

Game design is a critical component to a successful casino platform.

The entire experience of online gaming is a combination of users experiencing the game they enjoy the most. It’s not widely understood by individuals outside of the industry, but gaming is user dependent, game type dependent, and supplier dependent. This is to say that players get into the habit of playing one or at maximum two types of their favourite games, played by their favourite company in their favourite type of game. A Pokerstars poker player will generally only play at PokerStars and he may even play only Texas Hold’em (if this is his favourite game). Sure, skilled operators can entice him to play blackjack, roulette, or baccarat occasionally, but he will continually come back to play his favourite game – that’s where the vast amount of his gambling will take place. Venture capital companies

[35] https://en.wikipedia.org/wiki/Pai_gow

[36] https://en.wikipedia.org/wiki/Pai_gow_poker

experimented (and discovered this fact) with great losses in trying to take popular social slot games played in the US and market them into the UK as real money games. It turned out those same social slot games that are popular in the US were a bust in the UK real money online slot market. The lesson here is to KNOW your customer and understand what types of games he likes and why—data is important. Blockchain games are new and exciting and will draw new users to them out of curiosity alone, but for sure, operators need to take design into consideration and study what is working in each of these sectors. Blockdraw will take its game design seriously and will study which games work and will continually crunch the data on its live games over time.

9.3.FUTURE GAMES

9.3.1.CRAPS

Craps is a dice game in which the players make wagers on the outcome of the roll, or a series of rolls, from a pair of dice; like some other games, players can wager against other participants but the casino retains an edge due to the payoffs provided to winning participants on either side of the outcome. The game offers several side bets including individual payoffs for specific dice rolls.[37]

9.3.2.ROULETTE

Roulette is a casino game named after the French word which means “little wheel.” Participants may choose to place bets on single numbers, various groupings of numbers, or the colors red or black, whether the number is odd or even, or if the numbers are high (19–36) or low (1–18). The game is based on a wheel which has

[37] https://en.wikipedia.org/wiki/Craps

numbers 0-36 alternating between red and black, with either a single green 0 or sometimes also a double 00.[38]

9.3.3.PACHINKO

Pachinko is a Japanese arcade game that usual involves gambling and has similarities to slot machines.[39]

9.3.4.BRIDGE

The cryptographic process used is excellent for all card games, but betting on Bridge in a decentralized peer-to-peer man is a future addition to the app that we are very excited about – we think Bridge could be our biggest surprise, but we want to clear the most popular gambling games before adding Bridge to the app. Moreover, we could consider creating Bridge tournaments, possibly even sanctioned ones – the addition of IPFS as a record of all the games is perfect for proving masters points.

9.3.5.POKER

The cryptographic process used for creating random shuffles in Blockdraw is one that was originally developed for Poker (but unlike other variations of Mental Poker, it also happens to be useful for other games). As a result, adding Poker to the platform would be an easy adjustment.. Given the fact that other apps are being developed to focus on Poker, and that the industry is very specific (thus requiring an entirely different marketing model), for the time being we are not considering adding it to the platform. Part of the reason for us delaying Poker is we want to fully

[38] https://en.wikipedia.org/wiki/Roulette

[39] https://en.wikipedia.org/wiki/Pachinko

develop our Banquiers so that they can also function as Justices and handle in game help queries. As a result, we intend to add poker on our roadmap after the initial development of our app is created. We believe that Blockdraw's version of Poker will not only be the best application available in the market, but the most scalable and robust. None of our competitors have the capabilities we are designing.

10. PRODUCT VISUALIZATIONS


blockdraw
SMALL
BIG
ANY TRIPLE
TWO DICE
ONE
TWO
THREE
FOUR
FIVE
SIX
50
100
500
blockdraw
Player
Banqueir
Bishop
REBET
NEW BET


blockdraw
Balance
126,466
Win
0,00
Bet
20,000
Limit
20-1,000
SMALL
BIG
ANY TRIPLE
TWO DICE
ONE
TWO
THREE
FOUR
FIVE
SIX
1:1 ON ONE DICE
2:1 ON ONE DICE
3:1 ON ONE DICE
Bishop
+750
Bishop
+25
LOBBY
X
25
50
100
500
1000
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod?
SAY SOMETHING...
Send
CLOSE CHAT


blockdraw
Balance
126,466
Win
0,00
Bet
20,000
Limit
20-1,000
Tie Limit
120
Round
7
Player
Banqueir
Bishop
+750
Bishop
+25
Open chat
3 New messages
Score board
CLOSE SCORE BOARD
REBET
NEW BET
LOBBY
X
25
50
100
500
1000
LOL
SAY SOMETHING...
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod?
Send
CLOSE CHAT


blockdraw
Balance
126,466
TABLE
GAME
TYPE
BANK
STAKES
PLAYERS
TABLE NAME
BACCARAT
PUNTO BANKO
3
1000K
1K-5K
5-10
New Table
SELECT GAME
SELECT STAKE
HIDE FULL TABLES
SHOW HEADS UP
MEASSAGE BOARD
Player
Sed ut perspiciatis unde omnis iste natus sit voluptatem accusantium
Privecy Policy
Terms
More
Help


blockdraw
Balance
Win
Bet
Limit
Tie Limit
Round
126,466
0.00
20,000
20-1,000
120
7
LOBBY
RESET
NEW BET
DOUBLE
HIT
STAND

11. COMPETITION ANALYSIS

During 2017, there were several notable gambling ICOs launched which compare to Blockdraw in several different ways. While none of the following are perfect competitors, many feature similar characteristics and nuances that make them competitive to Blockdraw. We believe that gambling ICOs represent some of the biggest opportunities in the distributed ledger space. Currently, no major public or serious fiat commercial gambling company has entered the space, so we believe that as time goes by the opportunities for acquisitions or adoption by commercial fiat based acquirers will increase. It's critical to understand that Blockdraw's technology was designed to serve a broader range of users as well. We believe in the future of Ethereum, but as businessmen we understand that we live in a real world where there are real world concerns that businessmen, regulators, and legislators must come to grips with. Hence, we designed our software not just as technology enthusiasts, but as technology enthusiasts with real-world business experience (and gaming) in mind!

11.1. STOX

Stox is building a decentralized prediction market. It was also an early adopter of the Bancor protocol, but since then, its offering hasn't proven to stabilize the currency. There are several other players in this space, but Stox has been an early development leader. That being said, prediction markets are unproven; these products have been available in fiat form for at least a decade and adoption by the public has been slow. In some ways, however, the platform works like a betting exchange, which is like Blockdraw, with the key difference being Blockdraw's focus on traditional casino games. The similarities stop there and Stox's focus is clearly on creating prediction markets that may also push the barrier of financial investment products, such as futures contracts traded on traditional fiat exchanges, like the

Chicago Mercantile Exchange. The platform is being developed in concert with an existing development team that has some experience in financial markets and an existing website that has purportedly millions of subscribers; what is unclear is whether any of these users are adequate targets for the Stox platform. Stox is claiming that this customer base is one of its strongest selling points to distribute the platform.

11.2.FUNFAIR

Funfair is built around a team that founded and operated PKR poker[40]. The owners have proven experience in the gambling space and have developed gambling games in the past; PKR was successful in acquiring hundreds of thousands of users. The actual FunFair product was developed prior to launch and runs state channels using Ethereum, which allows users the ability to launch their own casino. Like Blockdraw it offers a provably fair RNG. While it shares a competitive position of being a casino product, the biggest difference is that this product allows users to create their own casino and doesn't currently offer the ability to create decentralized gambling in the same form as Blockdraw. Since its smart contracts operate in the wild, FunFair has not presented a clear explanation of how it will operate in the regulated or real world; we can't claim to have solved that issue totally either, but we designed our platform with those needs specifically in mind. Finally, FunFair runs on the live blockchain with all its inherent issues, while Blockdraw runs exclusively on Ethereum blockchains in real time using a native decentralized application with security and confidentially built-in.

Blockdraw believes that there is a real future for businesses who need security, but who still want to offer the same sort of verifiability that is afforded on the live blockchain.

[40] https://calvinayre.com/2017/07/06/poker/pokerstars-rescues-pkr-players/

11.3.VIRTU.POKER

Virtu Poker hasn't launched as an ICO, but like Blockdraw it is an exciting offering that is certain to be a significant launch in 2018. Virtu Poker is a Concensys Ltd offering, which is a major social influencer in the Ethereum space. That being said, the entire Poker market is already dominated by Pokerstars and it is no longer a growing segment of gambling space; however, there are likely opportunities for an Ethereum player to enter this highly competitive space, in much the same way Blockdraw will compete in the highly competitive fiat casino market place. The sole difference here is that the global casino market is still growing, where the global poker market is stagnant or declining. Given the Concensys Ltd backing it is highly likely that the product is being built by an experienced and credible Ethereum team. However, unlike Blockdraw and FunFair, the team has little to no experience in internet gambling, relying heavily on celebrity poker names as advisors. Because of the technical team's prowess, the app purports to offer some new ideas including the introduction of Mental Poker for card shuffling and IPFS for recording hand histories. Like Stox it has introduced a mechanism to handle disputes. There is no indication that Virtu Poker has solved many of the security and performance issues associated with a full on-chain experience – moreover they "hint" that their process will not function like a pure state channel (although in the developer world, the entire concept of what is and what isn't a state channel is still highly debated).

11.4.BLOCKDRAW

Blockdraw is regularly reviewing the competitive landscape. As of early 2019, we do not believe that any single competitor either has the technical prowess, management capabilities, or experience to create a globally successful brand, product and blockchain casino from scratch. Only Blockdraw is working on building the world's most secure, performant, and regulated decentralized peer-to-peer pure blockchain betting exchange in the world. Unlike many of the other gambling

offerings it is managed by a team with significant entrepreneurial, gambling, and regulatory experience. Not only is Blockdraw's peer-to-peer idea unique among casino related gambling offerings in the blockchain space, it has clearly articulated its regulatory plan, target market, and has a team experienced in gambling regulation and internet gambling. No other offering runs entirely on-chain Ethereum and offers the scalability, security, performance, and verifiability packaged in an on-chain offering. All of this is only possible using our LEAP solution.

The following table summarizes key differences among the platforms:

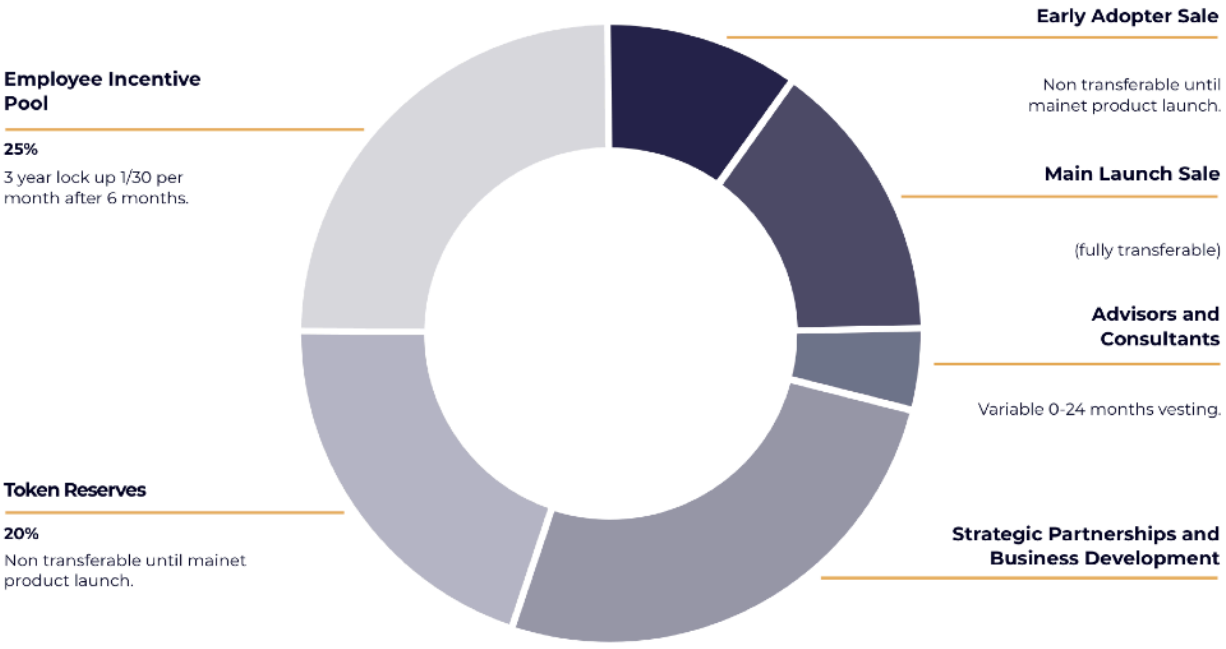
Feature	BLOCKDRAW	STOX	FUNFAIR	VIRTUE POKER
All funds held by smart contract	✓	✓	✓	✓
Vision for decentralized gambling platform	✓	✓	✓	✓
Known business plan to promote growth	✓	✓	✓	✓
Cryptographic random outcome	✓	N/A	✓	✓
High-performance scaleable platform	✓	✗	✓	✓
Mechanism for inherent token appreciation	✓	✗	✓	✗
Management with gambling experience	✓	✗	✓	✗
Executive regulatory experience	✓	✗	✗	✗
Defined regulatory and compliance plans	✓	✗	✗	✗
Audit trail with impeccable provenance	✓	✗	✗	✗
Multiple revenue streams reducing investor risk	✓	✗	✗	✗

12. TOKEN ISSUANCE

12.1. TOKEN SALE SUMMARY

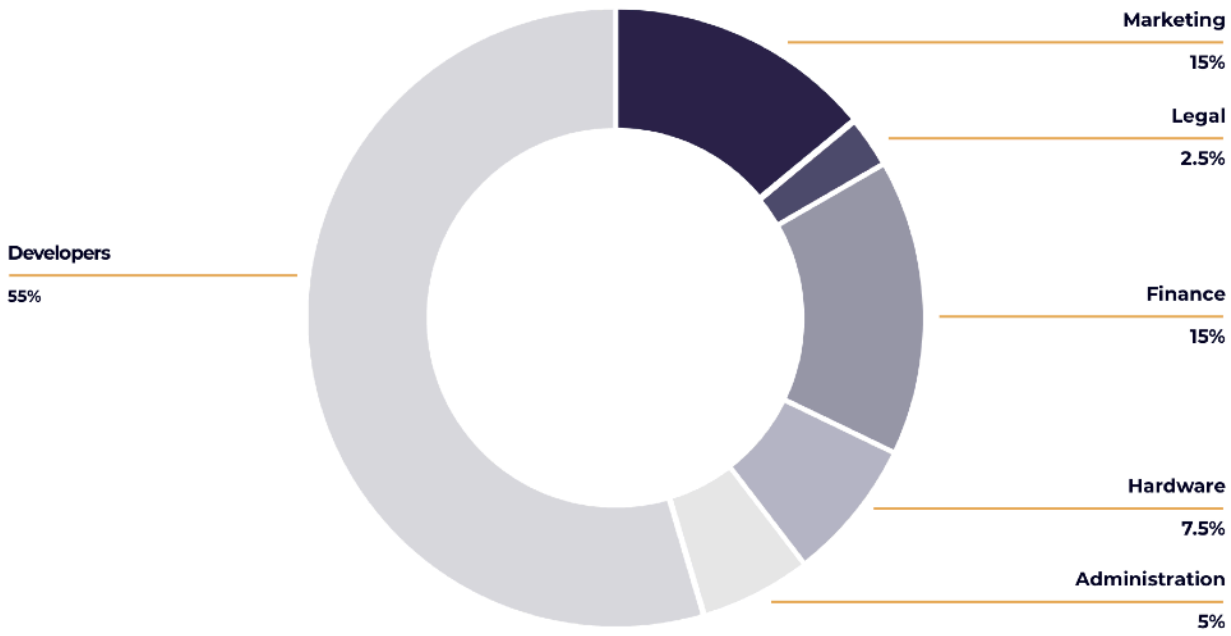
To finance Blockdraw's roadmap, Blockdraw will conduct utility token sale(s). Blockdraw will create a total maximum supply of two billions tokens (2,000,000,000). No other tokens will ever be created. We intend to split the maximum supply in the following manner:

- 30% of the total maximum supply will be allocated for sale to Participants.
- 29% of the total maximum supply will be allocated as incentives to related Blockdraw Parties, including but not limited to Founders, Advisors, and Employees.
- 20% of the total maximum supply is allocated to token reserves.
- 21% of the total maximum supply is allocated for strategic partnerships and business development which includes processes to ensure that table games are offered by banquiers.



Details of the token sale(s) will be announced directly on the Blockdraw website prior to the sale(s). Blockdraw will issue tokens through the Blockdraw Token Trust or a related entity.

12.2.BUDGETED UTILITY TOKEN SALE FUNDING PROCEEDS BREAKDOWN



Development: Creating the code base that will be the Blockdraw platform is our biggest cost, which is primarily composed of disbursements to unrelated service providers, Blockdraw founders or employees, and for costs associated with various non-development service providers (including but not limited to intellectual property management). Development costs and disbursements will be managed by a related group entity that acts as a development service provider.

Hardware: hardware includes local equipment and cloud servers / dedicated racks and everything we need to run our business; anything related to the technology.

Finance: All costs associated with fundraising, funding the ICO, listing on exchanges, banking and financial intermediary costs.

Marketing: We will use our marketing budget to promote our brand, our tokens, and our platform.

The expected breakdown of the Token sale proceeds may be altered as the project progresses. Blockdraw may also use some of the proceeds from the various pools described above to make additional investments that it believes are in the best interest of the Company.

12.3.ABOUT BLOCKDRAW FINANCIAL PROJECTIONS

Blockdraw anticipates operating at a loss for the foreseeable future; we see little point in publishing projections of future revenue which is difficult to predict. Moreover, we believe it is critical to create a war chest for the possible collapse in the funding markets which we see as inevitable in the boom and bust world of technology. We believe that during busts it's critical to have financial firepower available to make investments when others are struggling. As a result, we prefer to over raise, than to under raise.

Our founders also are stern believers in a strong financial function with budgeting for any business involved in gaming. You can rest assured we will know how much we spend on everything. We have a budget for platform development, but with such a project we also realize that a larger amount might be necessary to build our app/server side software/servers/etc. We also keep in mind that we have a longer-term eye to the future of both Ethereum and other blockchain technologies which will allow Blockdraw to be among the future winners in our market. We understand

the need for investment in our staff, our people, founders, and our technology, and as a result, we intend to do our best to be around for the long term.

A great deal of funding will be used to develop and brand the app (and the Company) as described in this paper and to make Blockdraw highly competitive in the market.

13. TEAM AND ADVISORS

13.1. FOUNDING MANAGEMENT TEAM

Blockdraw's management team has a long history of working in the gambling space.

Darin Oliver, Founder and President

Darin has over 30 years of experience in finance working in senior institutional sales and trading roles with UBS, Bear Stearns, Drexel Burnham Lambert, and Société Générale in Paris, Tokyo, and Chicago. He graduated with a BA from the University of Kentucky and attended graduate school at the University of Chicago in finance (MBA studies). He has owned his own SEC/FINRA regulated Broker Dealer in Boston. In 2009, his firm (led by Fairhaven Capital and later North Bridge Venture Partners) took over the 2000 stock automated marketing business from the failed BMLS. Darin packaged the transaction and won the stalking horse bid to acquire the assets. He has a long history in technology and managed the software team that recovered and rebooted the trading system (which incorporated new innovations into automated market making). He first became involved in gaming from his involvement in the harness racing business, where he worked as a groom, trainer, and later owner throughout the East Coast and Midwestern US campaigning grand circuit trotters and pacers. From 2012-2015, he was Deputy Director of Licensing at the Alderney Gambling and Control Commission ("AGCC") where he oversaw licensing and investigations of a significant number of offshore regulated gaming companies.

Konstantinos Despotakis, Founder and COO

A gambling compliance and AML/CFT professional, Konstantinos has worked for over eight years as a Deputy Director Compliance at the AGCC.

An Industrial Engineer by training, with post-graduate studies in Management Science and Energy & Resources, Mr. Despotakis worked in project management and consulting until 2004 (M.Sc. Imperial College of Science and Technology, University of London, PhD, University of California, Berkeley). Dr. Despotakis then moved to the eGambling sector in 2004, originally as the CEO of an Alderney operated eGambling lottery provider and operator, eventually moving in Oct 2009 to the AGCC.

13.2.DEVELOPMENT TEAM

Kim Lumbard, Blockdraw's Cryptology Expert

Kim graduated with honors in Applied Mathematics from the California Institute of Technology, where he later taught Information Theory. He is an expert in cryptography, discrete mathematics, and prime number theory. He has worked for National Labs in the United States, including JPL and MIT Lincoln Labs, and has performed classified research for the US government. Near the turn of the millennium, he made the leap from academia into business. He participated in three successful startups, and was co-founder and CTO of QIXO, the world's first travel aggregator to search consolidator databases. Kim is also a huge gamesman.

Denys Oliinyk, Blockchain Expert

Denys started programming professionally more than 15 years ago and since then has founded a solid software development company that has proven to be a reliable outsourcing service provider in the gambling industry. As a founder and lead system architect at Melior Games, he constantly tracks the fast-growing and dynamic technology ecosystem, which has allowed him to see the importance of blockchain development and master all of its aspects.

Olga Zadereshchenko, Project Coordinator

Olga has more than 6 years of experience in coordinating various IT projects and a proven track record of successful deliveries of gambling projects. Making sure that development goes in a right direction is what Olga does best.

Vyacheslav Rumyantsev, Blockchain Developer

Starting as a Unity developer, Vyacheslav has rapidly extended his expertise in order to master all major areas of gambling projects. After a few years of working with blockchain projects, he continues to grow as a smart contracts and solidity expert.

Vladyslav Ternovoy, Blockchain Developer

Vladyslav is an experienced full stack developer and blockchain enthusiast whose interest in blockchain began when bitcoin was not as popular as it is now.

Vaclav Marcenkevič, UI/UX Designer

Vaclav is among the most talented and experienced graphic designers in Lithuania. Through years of creating designs for various gambling games, he has become an expert in turning simple UI into high-end artwork.

Paulius Slivinskas, Senior Digital Art Director / UX Designer

Paulius is a UI/UX designer and digital art director with 9 years of presence in the advertising industry. He is focused on designing effective and memorable products which are based on user insights and tailored specifically for them. His task is to roll out the red carpet for high value users and create an engaging digital experience. Paulius believes in trying new ideas rather than sticking with ordinary “yesterday” style designs.

13.3.LEGAL ADVISORS

Vincent Oliver, Blockdraw US Corporate Legal Advisor

Vincent is a gaming lawyer who has over 30 years of experience in gambling practicing in California. He is a life master bridge player and has sat at the final table of two World Series of Poker Omaha tournaments. Vincent advises cardrooms and casinos in California on regulatory matters. He began his career playing Bridge and Poker at the highest levels and worked in card rooms while earning his law degree.

Sam Quinn, Blockdraw Offshore Corporate Legal Advisor

Sam is a qualified lawyer in Western Australia, England, and Wales and for the past decade has worked as the general counsel to a natural resources venture capital group called the Dragon Group (where he continues to work in a part-time capacity). Sam is also a director and company secretary of several UK-listed companies. Prior to this, Sam worked as a lawyer for several leading international law firms based in Western Australia and London. Sam also holds a Certificate in Corporate Finance and a Certificate in Securities from the London Securities and Investment Institute. Sam graduated from the University of Western Australia in 1999 with a Bachelor of Law and Bachelor of Arts.

13.4.US LEGAL COUNSEL

Ifrah Law has represented iGaming clients since the inception of the industry, and now represents many of the largest iGaming companies and industry associations around the world.

13.5. BRITISH VIRGIN ISLANDS (OFFSHORE) LEGAL COUNSEL

Appleby is a leading offshore law firm with around 470 people, including 60 partners, operating from 10 offices around the globe.

13.6.ADVISORS

Executive Director of the Alderney Gambling & Control Commission.

André Wilsenach

André is the Executive Director of International Center for Gaming Regulation, established in partnership between UNLV's International Gaming Institute (IGI) and the William S. Boyd School of Law.

In 2002 he was appointed Executive Director of the Alderney Gambling Control Commission where he regulated the eGambling industry there until January of 2016.

In his capacity as a gaming regulator André was instrumental in promoting regulatory best practices around the world. He was the keynote speaker at the first international eGambling Summit held in the United Kingdom in 2006. He gave testimony to the Financial Services Committee of the US House of Representatives concerning the introduction of the Internet Gambling Regulations Enforcement Act, 2007. He was a keynote speaker at the American Gaming Association's 2008 Global Gaming Summit in Las Vegas, and in 2012 gave testimony to the UK Culture, Media and Sport Select Committee regarding their new regulatory framework.

André is a former President of the International Association of Gaming Regulators and is an active member of the International Masters of Gaming Law and the International Association of Gaming Advisors.

Jieho Lee

Jieho Lee is a founding member of Knighted Ventures and has served as Co-Managing Partner since 2012. Previous to Knighted Ventures, Jieho Lee was head of International Business Development at POM Wonderful (a division of Roll Global) where he oversaw development and marketing for the Asia Territories. Lee also served as General Partner at Blue Horizon Capital, where he co-led an investment strategy team focusing on acquisitions in the business information sector. Before Blue Horizon, Lee co-founded Gemini Enterprises, a consulting firm focusing on risk management initiatives; there he oversaw ERM operations for companies such as the Dole Food Company, Ducommun Incorporated and Pacific Union Bank.

Lee also pursued a career in the entertainment field: writing, producing and directing commercial productions for clients such as Ralph Lauren, Victoria's Secret, and Tommy Hilfiger. He wrote and directed the feature film "The Air I Breathe" (starring Forest Whitaker, Emile Hirsch, Andy Garcia, Brendan Fraser, Kevin Bacon, John Cho and Sarah Michelle Gellar) and oversaw development and production of several other projects for Lionsgate Films.

Lee received a double degree in College of Letters and Cinema Studies at Wesleyan University, and an MBA from Harvard Business School. He resides in Beverly Hills with his wife, South Korean film actress Min Kim.

Sergey Portnov

Sergey is the CEO of Pairmatch, a major eastern European sports bookmaker with offices throughout Eastern Europe.

Nikita Izmaylov

Nikita is the COO of Pairmatch, a major eastern European sports bookmaker with offices throughout Eastern Europe.

Ivan Starodub

Ivan is a technology professional focusing on solving complex business challenges with the use of technology, research, and creative thinking. He is inspired by blockchain as a mechanism to create trustworthy solutions for untrusted environments.

14. RISK FACTORS & DISCLOSURES

The following are some of the risk factors that buyers of Draw tokens should consider carefully in the Draw utility token sale created by Blockdraw ("the Group"):

- The Group may not achieve the projected token sale and may not have adequate funds to execute its future business plans;
- Certain statements found on the Group's website, documents, and other oral and written statements made from time to time are considered "forward-looking statements" which may describe strategies, goals, outlook, or other non-historical matters, as well as project revenues, income, returns, or other financial measures. These statements are only predictions and involve known and unknown risks, uncertainties, and other factors that may cause our actual results to differ materially from those expressed or implied by such forward-looking statements. Given these uncertainties, you should not place undue reliance on these forward-looking statements. Forward-looking statements speak only as of the date on which they are made, and we undertake no obligation to update or revise any forward-looking statements.
- The digital currency market is highly volatile, speculative, and Draw tokens may be difficult to trade and even become illiquid (or untradeable). There is no guarantee, nor should there be an assumption that token purchasers will ever be able to trade their tokens for another digital currency or a fiat currency now or in the future;
- The DRAW token may not gain the adequate acceptance that the Group envisions. Events outside the digital currency markets may impact the value of Draw in ways the Group cannot yet imagine, but may include regulatory,

international tax laws and treaties, or laws against digital currencies or utility tokens;

- While online gambling is currently legal in some jurisdictions, the status of blockchain casinos remains uncertain, and it may be difficult to license Blockdraw's products in white or grey jurisdictions;
- The Group's software is complex and the technologies of the blockchain are new; numerous scenarios could result that impact both blockchain technology and our software that render it useless; moreover, due to technical or other challenges we may never be able to fully develop our software as planned or discussed in this paper;
- Our management team is newly created and has not previously worked together, hence their ability to produce results is untested;
- Competition may produce superior products that limit the business potential of the Group's software;
- International laws and regulations may render DRAW trading impossible;
- The use of DRAW tokens may come under the scrutiny of governmental institutions;
- The token may be deemed a security either by the jurisdiction of the token sale or another jurisdiction which could impact the Groups legal or regulatory status negatively;
- The ownership of Draw tokens may fall under new and unpredicted taxation laws that will erode Draw benefits;
- The Group will make every effort to code audit our smart contracts, now and into the future, but since the introduction of both Ethereum and Bitcoin, numerous hacks have occurred that have included coding errors in wallets, security breaches at websites, and outright theft by employees. The risks of losses of Blockdraw's ETH or Draw tokens in smart contracts and wallets are significant and a major breach could damage the reputation of Blockdraw or

even impact on the finances of Blockdraw in such a way to prevent it from continuing to operate, if such a large enough breach were to occur;

- The Group cannot provide any tax advice on how various jurisdictions will tax or treat the taxation of profits and losses from the purchase and sale of tokens, or how your local jurisdiction will treat taxation issues from tokens issued in another jurisdiction. Due to the unregulated nature of tokens, there are a multitude of tax issues that are unknown at the present and may only emerge when regulation becomes more understood;
- The Group cannot be held responsible for unintentional errors of omission from our website or other documents; our materials cannot fully describe our complete business plans and is subject to change without notice. We are not responsible to notify you of changes to our whitepapers, business plans, or other plans in the future;
- There is no certainty that the Group's software will obtain a patent for its processes, although the Group will attempt to do so;
- Despite our best attempts to maintain security, the Ethereum network is new and a still emerging technology. We may become vulnerable to known or unknown attacks on our software which may cause financial losses or damage our reputation;
- It is expected that you will review and read our AML/CFT Policy, website Terms of Use, Privacy Policy, and our Whitepapers before acquiring Draw Tokens;
- You must read and agree to the Blockdraw Terms and Conditions, which contain, among other important information, a more complete set of risk disclosures.

Blockdraw retains the right to change its plans, roadmaps, corporate structure, investments, software, to pivot the business in any way, or to make any material corporate decision it wishes including changing the use of its funds/proceeds

raised from any future utility token sale at any time without any notice to token holders. A utility token purchase does not grant any rights to purchasers in respect to ownership or equity in Blockdraw Issuer Limited, Blockdraw Token Trust, Blockdraw Capital Limited, Blockdraw Technologies, LLLC their parents, subsidiaries, affiliates or any of its technologies, assets, or intellectual property. See our sale terms and conditions for complete details.

15. REGULATORY STRATEGY

The purposes of regulation in gambling is to ensure both the suitability and financial stability of the operator (including reviewing professionalism), protect society from abuse (underage players, money laundering, and addictive gambling), provide for fairness and transparency in game play (security of player data and the platform, testing of game algorithms and disclosure of returns to players), and require that adequate business systems are in place to monitor and control ongoing operations and compliance. Effective regulation ensures that these factors are built into an operator's systems. Smart contracts and decentralization normally do not play well with many real world demands. There are real challenges to ensuring that problem gambling is checked since a user can create a new wallet or identity at any time; unless well monitored, with blockchain tokens, underage players could theoretically play undetected. On the other hand, blockchain solutions solve many problems currently inherent within the analog world, like global access, guaranteed payments and built in financial controls that are simply not possible without blockchain. It was with these obstacles in mind that Blockdraw developed its LEAP technology, which uses the best of all available technologies to create a platform that can not only be decentralized but also has regulatory oversight build into the system (see our technology section). We will run our business from day one in line with standards required by regulatory bodies and when needed, will seek regulation for our offerings.

15.1. KYC AND RELATED ISSUES

The disruptive nature of the blockchain does not remove real world regulations and laws; while smaller operations may escape these, realistically without proper age verification and KYC or fraud detection, your business model simply will not be allowed to operate. Additional tools for self-exclusion and IP location (and related

tools) are critical. There are a lot of tools for these systems being developed, but in the meantime, we plan to incorporate and to build industry standard capabilities into our platform so that we will be able to control underage gambling, fraud, and manage black listed markets.

15.2.REGULATED AND NON-REGULATED MARKETS

We are going to approach regulation cautiously. Our gaming product will certainly need licensing in some jurisdictions and hence we will undergo the required processes in order to gain a license when needed, or have our operators do so. We may initially operate in grey or unregulated markets, which should not be underestimated in their ability to deliver significant revenues. But as each year passes less of the world is unregulated, so we will likely use these markets to test and hone the product. Longer term, we realistically understand the importance of pursuing international licenses in the major jurisdictions that allow online gambling.

16. EXCHANGE LISTINGS

At the appropriate time, Blockdraw will enter into consultation with several exchanges to accept Draw tokens for trading so that users that did not participate in our token sales will be able to purchase tokens for use on the platform. We will notify utility token participants either by email or on the website's blogs when Draw tokens are tradable and on which exchanges.

17. DOCUMENT REVISION HISTORY

EACH NEW BLOCKDRAW WHITEPAPER, LIGHT PAPER, OR TECHNICAL FAQS (THE "WHITEPAPERS") REVISION CONTAINS THE ENTIRE CURRENT UNDERSTANDINGS WITH RESPECT TO THE MATTERS COVERED BY THE WHITEPAPERS. All prior or contemporaneous writings in any of the whitepapers with respect to the subject matter covered hereof and all other such commitments, agreements and writings shall have no further force or effect. Blockdraw is under no obligation to inform readers of any changes to its whitepapers and urges readers to check for revisions from time to time.

Revision	Author	Date	Status and Description
1.0	Administrator	Feb 6, 2018	Initial Draft Whitepaper
1.1	Administrator	Feb 12, 2018	Updated section 14 (bios, added advisors), some minor edits to sections 12, 13, 15, and added sec 18.

Revision	Author	Date	Status and Description
1.2	Administrator	March 12, 2018	Editing changes, added offshore and US Legal. Clarified role of Draw utility token.
1.3	Administrator	April 15, 2018	Editing changes, discussion on Poker, added Draw Token Sale details
1.4	Administrator	April 19, 2018	Clarifications to Golle Algo, editing milestones