# SP8DE

## WHITE PAPER

Version 1.0: October 28, 2017

Version 2.0: December 15, 2017

Version 3.0: February 8, 2018

Version 4.0: February 14, 2018

# Contents

# Disclaimer

THE PURPOSE OF THE PRESENT WHITE PAPER IS INTRODUCTION OF SP8DE PROJECT TO POTENTIAL TOKEN HOLDERS IN VIEW OF UPCOMING TOKEN SALE. INFORMATION PROPOSED BELOW DOES NOT CONSTITUTE A PUBLIC OFFER. ITS ONLY PURPOSE IS TO PROVIDE RELEVANT AND SUFFICIENT INFORMATION TO POTENTIAL TOKEN HOLDERS. NOTHING IN THIS DOCUMENT MUST BE REGARDED AS ADVERTISING OF THE PRODUCT OR AN INVESTMENT OFFER. NOTHING IN THE DOCUMENT MUST BE REGARDED AS A SOLICITATION AND / OR PROPOSAL TO BUY ANY SECURITIES IN ANY JURISDICTION. THIS DOCUMENT DOES NOT FOLLOW ANY LAWS OR RIGHTS CONCERNING INVESTOR PROTECTION IN ANY JURISDICTION. SOME STATEMENTS, EVALUATIONS, AND FINANCIAL INFORMATION IN THE DOCUMENT ARE JUDGMENTS OF ITS AUTHORS. SUGGESTED JUDGMENTS OR INFORMATION MAY CONTAIN KNOWN AND UNKNOWN RISKS OR INACCURACIES, WHICH MAY LEAD TO EVENTS OR OUTCOMES WITH ECONOMIC EFFECTS. THE RUSSIAN LANGUAGE VERSION OF THIS DOCUMENT IS THE PRIMARY OFFICIAL SOURCE OF INFORMATION ON SPX TOKEN. INFORMATION IN THE DOCUMENT CAN BE SUBJECT TO INACCURACIES, GRAMMATIC AND SYNTACTIC ERRORS ORIGINATED FROM TRANSLATION TO OTHER LANGUAGES OR QUOTING ITS SECTIONS IN WRITING OR VERBAL FORM TO EXISTING AND POTENTIAL CLIENTS, PARTNERS, ETC. THE ACCURACY OF SUCH ALTERNATIVE COMMUNICATIONS CAN NOT BE GUARANTEED. IN THE EVENT OF DOUBT OR ANY INCONSISTENCY BETWEEN TRANSLATIONS, THE RUSSIAN LANGUAGE VERSION OF THIS DOCUMENT HAS PRIORITY AND IS THE PROPER SOURCE OF OFFICIAL INFORMATION. SP8DE SERVICE CANNOT BE USED TO ACQUIRE FOREIGN ASSETS AND / OR TO AVOID CONSEQUENCES OF UNLAWFUL ACTIONS WHICH ARE SUBJECT TO SUPERVISION BY FINANCIAL REGULATORS. THE ‘INVESTMENT’ TERM IN THIS DOCUMENT SHOULD BE UNDERSTOOD AS ACQUISITION OF TOKEN OR CRYPTOCURRENCY OFFERED IN TGE (Token Generation Event). THE ‘INVESTOR’ TERM SHOULD BE UNDERSTOOD AS A REAL OR POTENTIAL HOLDER OF A TOKEN OR CRYPTOCURRENCY. IF YOU ARE A CITIZEN OR RESIDENT (TAX OR OTHER) OF THE PEOPLE’S REPUBLIC OF CHINA OR THE UNITED STATES OF AMERICA, YOU DO NOT HAVE THE RIGHT TO PURCHASE OR HOLD SPX TOKENS.

# Introduction

Welcome to Sp8de, a blockchain-based platform capable of supplying unbiased public randomness for developing and running distributed casino applications. Sp8de is designed to suit the purposes of all the actors comprising the online casino landscape and as such represents the new breed of digital institutions, a distributed intermediary.

The spark that lit this project and continues to inspire us now, is that early blockchain and Bitcoin casinos simply didn't get it right. The Blockchain community was younger and wilder, ideals of distributed freedom were burning brighter… still, early adopters who applied blockchain technology to gambling promoted the wrong ideals; those undermining the image of decentralized casinos. Instead of promoting transparency and cost efficiency that characterize blockchain technology, they promoted anonymity and cyber anarchy. Instead of making the casino for everyone, they kept it to themselves.

By no means are we here to judge. Instead, we are here to change. We do not say that old ways are bad, but can prove that new ones are better. We hold faith in the decentralized future and appreciate the charm of gambling.

We soon realized that there is only a fragile wall of glass between the old centralized gambling and the future global distributed casino. This is it, a simple yet captivating idea. The future is here: **we can run a zero-house edge decentralized casino with close-to-zero transaction fees and provably fair random numbers feeding entropy into a myriad of Smart-Contract-based open source casino applications that can be developed by anyone who has a worthy idea by means of state-of-the art application-specific as well general-purpose programming languages.** "We can" was the silent voice of the idea. Now it is the marching echo of "we do".

As it frequently happens, technological progress made a massive leap forward that went unnoticed by the majority of human kind: people still prefer the traditional narrow-minded and boring online casinos that set draconian house edges and cannot be proven fair. Once again, no one has the right to judge: it is just an existential business need, produced by a dilapidated business model and an inch of greed.

Worse than this, however, is that even the enlightened ones, those chosen to witness the dawn of the distributed world *have noticed* a perfect fit between distributed consensus protocols and gambling applications, *have synthesized* them and… nothing. Some of these projects got infamous due to money laundering accusations, some have spoiled the beauty of the idea by running centralized online casinos and simply allowing for cryptocurrency deposits, others got their moments of fame during TGAs, today, however, few can recall even the names of these projects. Of course, there are some notable exceptions to this rule, but while succeeding locally all these projects have failed to create awareness. None of them has broadcasted the essential message: **"There is no glass wall; the future of gambling is now; we are better in every single quantifiable aspect; if quantifiable is not enough, we also have the powerful idea of the distributed future, while those who are stuck in the past have only a couple of servers and an unaudited poker protocol".**

We will do what no one has done before. Sp8de is a blockchain-based platform for developing distributed gambling applications. As a platform for gambling applications with self-respect, we are equipped with the protocol for generating fresh **unbiased public** randomness. As a team with some aspirations we have it **provably fair** and **completely decentralized.** We feel that it is important to be true to the spirit of the venture we embark upon: if blockchain is the universal and undisputed source of truth then it should also be the broadcast channel for randomness. We think that single points of failure should be perceived by anyone as just a relic of the past.

This feature, while setting us aside most starkly, is only a part of what we have to offer in terms of technological stack. In what follows we will dive deeper into the revolution we all are a part of and will explain in detail the best iGaming protocol the world has ever seen.

# Industry overview

In the European Union the online gambling industry grew nearly 19% from the first half of 2015 until the first half of 2016. The casino industry in particular generated over US$2 billion in revenues during this period. It is expected that until 2020 this number will reach US$2.25 billion per year representing about 12.5% revenue growth [1]. In the US for the period 2015 until 2016 online casino revenues increased by 24.4% and are expected to reach US$4 billion by 2020 [2]. The EU and the US are just a small part of the worldwide casino industry. Globally, the projections of the online casino show that for the period 2017-2025 the market will experience growth of about 130% reaching US$97 billion with cumulative annual growth rate of nearly 11%. Currently over 6 million adults are officially participating in gambling activities around the world with projections of reaching 10 million by 2020 [3].

Since inception, the blockchain technology was the subject of close attention by gambling enthusiasts. Recent news from The Merkle [4] show how popular online Bitcoin betting has become. In aggregate the wagers put on online Bitcoin casinos in February 2017 have reached nearly 3 Bitcoin per minute. The price of Bitcoin at the end of February was about US$1,200 while now it is US$5,900 (approximately 292% growth) which means that as of today almost US$715 million worth of Bitcoin was gambled in February alone.

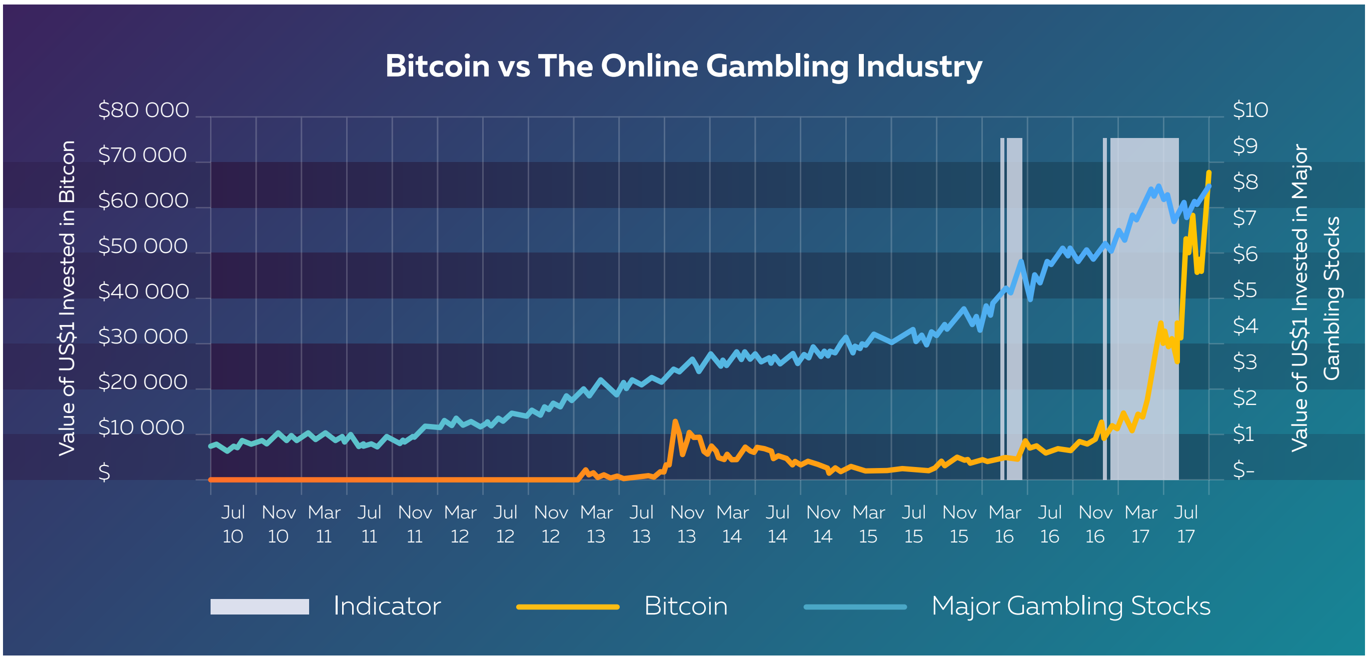


**Figure 1** The Online Gambling Companies and Bitcoin; Sources: Yahoo Finance and Coindesk.

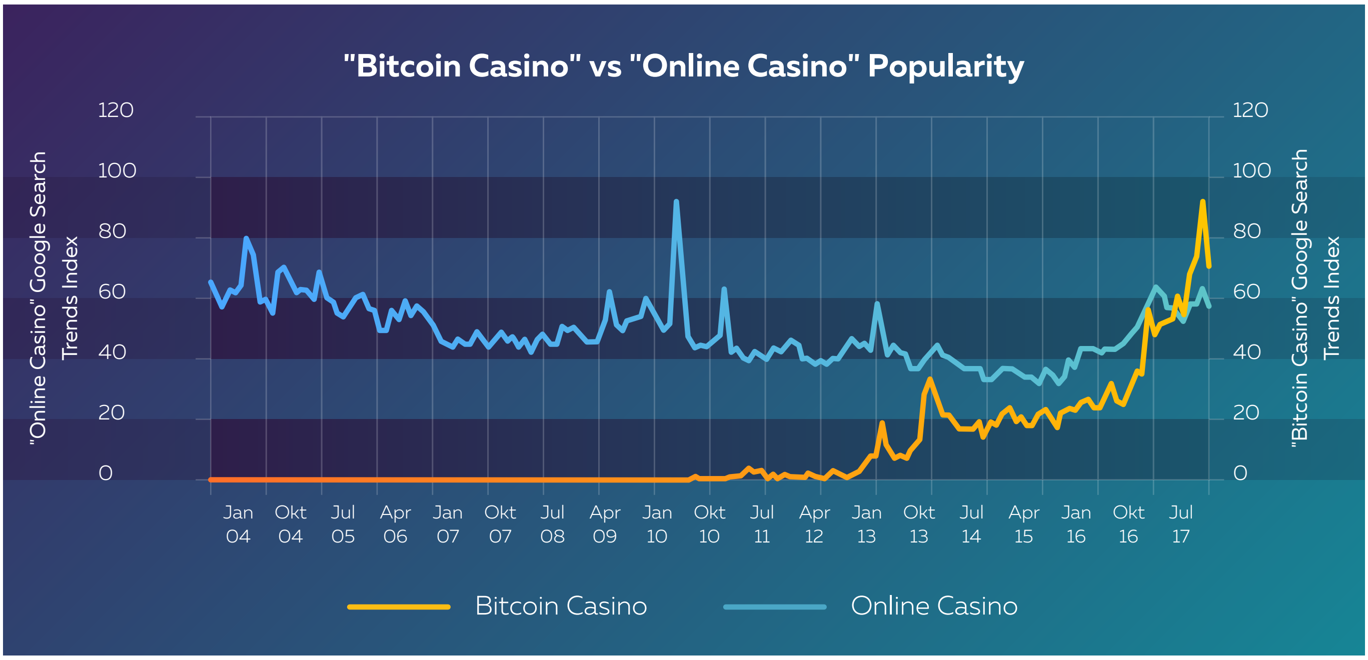


**Figure 2** Google Trends "Bitcoin Casino" vs "Online Casino"

In Figure 1 we show how an investment of US$1 would have developed from 2010 until 2017 if it was invested into the giants of the online gambling industry[1] [5] as compared to the same dollar being invested in Bitcoin. Apart from the fact that this investment in BTC would have provided US$70,502 as compared to only $US7.37 when invested in the index, one major observation can be made: the shaded areas show that as the Bitcoin blockchain technology was becoming more and more popular (that is the price of Bitcoin was rising) the traditional online casinos have also gained steam. However, when we look further in Figure 2 (Google Trends search for "Bitcoin Casino" and "Online Casino") we see that the popularity of online casinos has been relatively stable and slowly declining *since 2004*. Only since the beginning of 2016 when the Bitcoin casinos have started to gain wide popularity did the online casinos see slight increase in interest. In addition, the search "Bitcoin Casino" has skyrocketed since May 2017 when it surpassed the search term "Online Casinos". Furthermore, we know of the existence of at least ten relatively sound blockchain-driven casino projects that have entered the industry through a successful TGE and are still being developed. Although somewhat broad[2], this overview points out to an important pattern which holds a lot of relevance for the future of the gambling industry.

Currently, online casinos seem to be only weakly affected by the growth in the interest in Bitcoin gambling and the blockchain-based casinos that at the moment appear to at least complement traditional online gambling. However, this is happening at a staggering pace and the tendency shows a possibility of blockchain-based gambling taking over online casinos. If the current pace of technological advancement of the blockchain industry is sustained, soon there will be no benefits left for the consumers in the more traditional online casinos.

[1] To form this index, we create an equally-weighted portfolio of 888 Holdings, bet-at-home.com, GVC Holdings, Ladbrokes Coral Group, and MGM Resorts (although Bitcoin is traded during the weekends and holidays we only consider trading days).

[2] When replacing "Online Casino" with "Online Gambling" the results are similar. Also replacing "Bitcoin Casino" with "Blockchain Casino" does not alter our results significantly. The results of searching "Ethereum Casino" are also similar to those of searching "Blockchain Casino". Nevertheless, one has to consider that it is possible that people searching these keywords did not look for actual blockchain-based casino but rather that they want to gamble cryptocurrency such as Bitcoin.

# The Blockchain and the Casino

In what follows we describe a protocol for decentralized blockchain platform for developing casino applications with multiple unique features whose solid implementation is lacking in any of the currently existing projects in this space. The concept of decentralized consensus that lies at the heart of blockchain is based on the smart application of cryptography and game-theory. Combined, they create the economics of trust and hold immense potential for revolutionizing many classic industries.

This backbone of blockchain technology renders it an obvious candidate to consider in developing online gambling applications as, arguably, trust considerations and the need for transparency are - and always used to be - two major cornerstones of the gambling industry [6], [7], [8], [9]. In particular, **blockchain has the potential to provide transparency to all transactions, drastically reduce the house edge, nearly eliminate transaction costs, ensure anonymity of participants and ultimately, create the trust among players and other industry participants.** This rapidly evolving technological stack offers immense potential for improvements in the online gambling space, however, it also carries multiple new pitfalls that are scarcely (if at all) researched and poorly understood. To understand the benefits the blockchain brings, one needs to delve deep in the economics of casinos (the institutional viewpoint). Appreciating the challenges requires an overview of the mechanics of the blockchain technology.

So, why would applying blockchain to online gambling appeal to an average person?

## Economics of Gambling: An Institutional Perspective

While being driven throughout its long history by complex economic and sociological changes, the gambling industry has dramatically changed its competitive and institutional landscape – on the supply side it has changed remarkably little from the perspective of a person who wishes to try one’s luck. Indeed, it is still the same set of games that dominates the casino landscape, it is still the chance that defines one’s faith and these are still the classic transaction costs that interfere into the process, owing to the fact that the world we live in is not frictionless.

It follows that we can view the casinos from the perspective of institutional economics, a branch of economics studying the impact of institutions on the behavior of economic actors.

One of the major roles the financial institutions play, in modern economics, is economizing on transaction costs, thereby facilitating financial transactions that would otherwise be unfeasible. They also serve as escrows, notorious trusted third parties, who facilitate trust among the participants allowing them to enter into an exchange more efficiently than would otherwise be the case [10].

In this vein, casinos act as “gambling” intermediaries realizing the economies of scale, maintaining order and quality of service, thereby facilitating the “conditional” transactions – bets.

Let’s imagine the evolution of the gambling industry as a path towards reducing the transaction costs where innovative industry newcomers attempt to take a piece of the overall pie from the old incumbents by bringing gambling closer to the frictionless ideal.

In this vein, classic casinos reduce security and search costs, facilitate standardization by using chips and having house rules and, most importantly, realize economies of scale by bringing together people united by the shared desire to gamble. Following this line of reasoning, online casinos while performing the same functions as their classic brick-and-mortar counterparts, also facilitate convenience and economize on the travel costs on the side of players. The major reason for their existence, however, stems from their more lightweight cost structure that is characterized with virtually zero marginal cost of adding a new client. This translates into significantly lower overhead costs, results in smaller house edge and, therefore, smaller average wagers and larger average net gains on the side of the clients [11], [12].

The advent of the cryptocurrency casinos came as a result of their anonymity feature as well as absence of any regulatory oversight. As many other applications of the blockchain technology in its early days, the major considerations behind setting up casinos on the blockchain were idealistic, impractical or outright shady in nature. **The anonymity and laissez-faire regime, however, are not the features that fit best into our line of reasoning: indeed, the decentralized infrastructure does not imply any server maintenance costs: the protocol is autonomous; the bets are fair: the protocol code is public; its workings are imprinted into the immutable ledger forever and can always be verified by anyone.**

As a rule, once something new offers better ways for solving old problems, there always is a catch [13].

## The Mechanics and Issues of On-Chain Casinos

Summarizing, the blockchain revolution allows for greatly enhanced transparency and efficiency of transactions, levels the playing field for online game development and greatly reduces overhead costs erasing the necessity of maintaining relationships with trusted third parties, bringing the concept of online casinos to a completely new level.

While being clearly beneficial in some aspects, the *net* benefits of blockchain to the general public willing to put their hard-earned funds on stake are less clear-cut. The reason is that, unfortunately, while being *secure and trustless*, not a single blockchain protocol can compete in terms of *efficiency* with centralized systems, such as those that are used by the off-chain online casinos nowadays.

This imposes heavy burden on the user experience: one can imagine the winner's frustration caused by the necessity to wait for 10 minutes before knowing if the roulette round actually settled on the blockchain. Even a 10-second delay can be detrimental to user experience once certain types of online gambling applications are concerned[3].

Ordering of transactions is of paramount importance in a distributed ledger (the root of the double-spend problem). Unfortunately, simple time stamping cannot be used to achieve distributed consensus on the ordering of transactions in a decentralized peer-to-peer network. The blockchain protocols were created instead, offering a successful solution to the issue. However, decentralization always comes at a cost. Each block needs time to be mined and this creates inherent delays that are detrimental to user experience as far as casino applications are concerned[4]. Therefore, the first problem that needs to be resolved as efficiently as possible before online casinos can migrate on-chain is *transaction settlement times*.

The second inherent problems lie around *transaction fees*. Indeed, all the praised benefits of the decentralized payment networks, such as instant settlement and virtually absent transaction fees turn their back on those daring to employ them for micro-transactions. For example, currently the transaction fee to send ether on the

[3] For example, an online casino (NetEnt) has been heavily criticized by its community for having a delay of less than 300 milliseconds (0.3 seconds) in knowing whether they won or lost; and delaying the withdrawal of big winnings (e.g. jackpot) has been famous in the industry. A simple search in Google "online casino delay" yields nearly 1,000,000 results, indicating how prevalent delays in online casinos are and how frustrated the online gambling community is with them.

[4] This, of course, only applies once there is a fundamental limitation on the amount of games that can be played in every block. In currently existing applications, there indeed is such limitation – and it's 1. For as far as the block content is a required input for generating randomness, one game outcome is produced for every block.

native Ethereum blockchain is about US$0.351 and sometimes over US$1. Such fees are game stoppers in a literal sense when it comes to for example, 5-dollar bets [14], [15]. No one would accept *20% brute transaction fees* for a US$5 online bet. This problem is further exacerbated by the fact that most of the popular blockchains currently in existence are based on Proof-of-Work consensus protocols that are infamous for not scaling too well. This implies that soon we can and will witness situations where a gambler would have to either pay even higher transaction fees or experience large delays in settlement (see problem 1). It is also not clear, how to incorporate such choices on the level of the gaming application with more than one party involved. Furthermore, given that transaction fees on Ethereum or Bitcoin blockchains are paid in the underlying virtual currency, the cost of transaction is actually directly tied to the price of this currency.

This translates into a *proportional* increase in transaction costs. Therefore, an ideal solution for an on-chain casino would necessitate a protocol that can scale seamlessly and that would have low transaction fees. This is, however, far from being the end of the wish list when it comes to blockchain casino applications.

Here we have approached the cornerstone topic in on-chain casino design. The immanent importance of this topic can only be matched by the extent of controversy associated with it. Before delving deep into complexities of probability theory, let's summarize what has been said so far

a. The uprising of the casino industry from the early days of humanity until the very end of the XX century can be portrayed in standard outlines of economic theory: it has been a long quest towards erasing the transaction costs by the means of centralization and institutionalization of the gambling process.

b. The problems that have remained unresolved included poor transparency, high overheads incurred by casinos to maintain lucrative buildings and other required infrastructure that translated into high house edges; and, finally, the need to travel to a "physical" location.

c. An additional problem was that of inclusion: indeed, not everyone could participate in the development of new games. Some of these problems have been partially resolved by the slow migration of casinos online. Nevertheless, those of poor transparency and large house edges have also remained. In general, these are the problems that are inherent to the legacy financial system; the one based on intermediation and trust.

d. Therefore, it comes as no surprise that numerous projects have embraced the challenge to move the gambling process on-chain. This, however, turned out to be an ambitious aspiration with numerous pitfalls and seemingly unsurpassable technological barriers. While resolving the issue of inclusion, transparency (from the gambler's perspective) and excessive house edges, blockchain gambling exacerbated those of high transaction fees and anonymity. It also brought new challenges along with it: how do we resolve the issue of slow settlement?

e. Finally, we addressed the sinle most important problem: the generation of the *distributed randomness*.

Indeed, how does one generate provably random numbers on-chain? Overall, how one achieves provable randomness in applications where multiple parties are involved and the random number generated determines the distribution of the monetary gains and losses for those involved? An easy solution would be to use a local source of randomness, such as RAND() function in Microsoft Excel©. However, there is a problem with this approach that renders it inefficient: local sources of randomness can be easily subverted and thus, there is no easy way for all the parties to verify that the number provided by a party is the number actually generated.

What about public sources of randomness? For example, Random.org, NSA or NIST all serve to provide "pure" randomness which is sampled from various natural sources, such as quantum physics processes. While indeed being public and random, these sources of random numbers suffer from all those problems we inherit from the 'centralized' yesterday: any application, however distributed, relying on them automatically raises the 'single point of failure' red flag. Their outputs are susceptible to human errors, present an adversary with incentives to undermine their workings and finally, give malicious incentives to those running these protocols.

As always, when one is stuck being unable to find a theoretically convincing and practically appealing answer in the domain of centralized applications, the world of distributed consensus is the place to search for answers. There is no easy way to get distributed randomness: blockchain protocols are deterministic by nature and, do not have implementations of random number generation on the protocol level. But it wouldn't be blockchain if this was the final answer. The following 'solutions" have been proposed and implemented:

1. Most of the attempts to circumvent this limitation in the end still rely on fresh entropy provided by either the users themselves or random oracles that in turn can either be manipulated or have malicious incentives of their own. So, random oracles – off-chain – single point of failure – red flag.

2. Others opted for a different path and proposed using the block hash. While such protocol design is much more appealing from a theoretical viewpoint as it generates random numbers on-chain (no red flag), it has another major flaw: given sufficiently large monetary incentive miners with sizeable hashing power can manipulate the game outcome by not submitting the freshly mined block. Using timestamps and virtually any other block content falls victim to the same issue.

3. Commitment schemes: the most promising solution with two major drawbacks: huge computational overhead and possibility that a malicious player will not open the secret after learning the outcome of the game. In other words, these schemes lack guaranteed output delivery. Monetary disincentives can be introduced to punish malicious actors basically collateralizing the Smart Contract thereby forcing the output delivery. In theory it works just fine. In practice one ends up with a slow and terribly expensive *working* protocol with limited applicability.

As we will show, something that is effective but inefficient can always be improved, but not the other way around. Points 1 and 2 unfortunately belong to the latter category, but the situation with the commitment schemes is different.

The discussion so far has been quite abstract. A legitimate question is what does it all mean for the distributed gambling applications? Let's review the recent projects in this sphere that have received their part of public attention.

# Competitors' Review

A number of other projects utilizing the blockchain are entering the gambling industry by either aiming to create a platform for online casinos or by simply placing a specific game or a variety thereof on-chain. As noted above, among the issues which are solved by simply creating blockchain-powered versions of the games, three main problems remain yet unaddressed:

1. **Transaction Settlement Time:** it takes significantly longer to settle a transaction on-chain than off of it as each block requires time to be mined.

2. **Transaction Fees**: the fee for each transaction can become prohibitively high and preclude small bet sizes.

3. **Provably random**: the generation of randomness on-chain is a challenging as miners can see and modify block headers before everyone else.

DAO.Casino [18] introduces a decentralized system for the online gambling industry which consists of an automated value distribution protocol acting as mechanism of incentives based on Ethereum. The team has recently began developing Payment Channels to address the first two problems while addressing number three by the introduction of the Signidice algorithm (which is suitable only for two parties" games). It goes without saying that any casino protocol lacking good quality randomness that can be extended to any number of parties cannot serve as a backbone for the decentralized gambling industry.

BitPoker [19] propose a peer-to-peer protocol where no central actor has influence over the outcome of the game. They use Bitcoin and lightning network for transaction settling and blockchain for game state persistence. In the white paper of BitPoker (which is a project solely aimed at poker games) none of the aforementioned issues is explicitly addressed.

Edgeless [20] is built on the Ethereum blockchain and claim to be the first to create fully transparent and zero-house-edge decentralized casino. Edgeless" aspiring team aims to introduce a number of innovations in the industry of online casinos; however, their white paper also does not address the three notorious predicaments.

BitDice [21] is also based on Ethereum but aim to implement IOTA in the future to provide costless transactions. For now, the developers of BitDice claim that the move from Ruby to Elixir by Q1 of 2018 would reduce the betting latency from 20-40ms to 2-5ms, nevertheless, for now, transaction fees and the generation of randomness are not addressed in any meaningful way.

FunFair [22] is Ethereum based, can launch limitless number of online casinos, it is instant, claim to be ten times cheaper in terms of gas cost than other casinos, and propose an innovative way of RNG. FunFair's ambitious project aims to achieve zero latency between the time of user's interaction with the interface and the result, effectively eliminating the first issue. In addition, they pay attention also to both transaction fees and specifically target on-chain provably random number generation through the development of Fate Channels.

Table 1 below summarizes whether each of the projects addresses one or more of the three problems in a novel and effective way.

| | SETTLEMENT TIME | TRANSACTION FEES | RANDOMNESS |
|---|---|---|---|
| DAO.Casino | Payment Channels | Payment Channels | Not Addressed |
| BitPoker | Not Addressed | Not Addressed | Not Addressed |
| Edgeless | Not Addressed | Not Addressed | Not Addressed |
| BitDice | Move from Ruby to Elixir | IOTA (not implemented) | Not Addressed |
| FunFair | Fate Channels (not proven) | Fate Channels (not proven) | Fate Channels (not proven) |
| *Sp8de* | *Ouroboros (proven)* | *Ouroboros (proven)* | *Ouroboros (proven)* |

**Table 1** The solution to the three problems

The table above highlights that now as never one needs to appreciate the wisdom embedded in a "devil's in the detail" idiom: multimillion dollar casino projects who claim to revolutionize the multibillion dollar gambling industry do not appear to address the most fundamental problems this revolution creates. Any inquiring mind is recommended to briefly look at the history of the last century to see what a disaster any unplanned revolution is.

Sp8de is different: *details are our passion.*

# The Mechanics of Sp8de

Sp8de is the new-generation blockchain-based gaming platform aimed at all the participants of contemporary casino ecosystem. We call it "new-generation" as Sp8de satisfies all the aforementioned conditions of a 'proper' blockchain casino. We build Sp8de on top of the blockchain called Cardano [24]. The Cardano project itself is a monumental work that embraced the best practices and most far reaching innovations in the area of cryptocurrencies and packed them into a single state-of-art system. It is being developed and maintained by a large team comprised solely of PhDs in the field of programming and cryptography, and experienced engineers.

In what follows we will illustrate how Sp8de provides an environment for the design of gambling applications which are characterized with:

1. Close-to-absent transaction fees and Proof-of-Stake powered scalability that is beyond the reach of any other on-chain casino protocol currently in existence;
2. A mechanism to generate decentralized provenly uniform randomness at arbitrary time-spans;
3. Provides rich Smart Contract functionality that allows for creativity in game design that is bounded solely by the fantasy of the developer (and the demand for the resulting product of course);

Fairness of the outcome is essential for gambling; it is the core.

Sp8de utilizes Cardano to design its ecosystem and thereby solves the problems normally associated with the on-chain casinos described above. Here is how:

1. <u>Transaction fees and scalability:</u> the size of transaction fees is normally a function of the degree to which a given distributed system scales. Scalability can be defined as the relation between system resources and the number of nodes. Scalable systems gain in efficiency as new nodes join the network: BitTorrent and IOTA protocols are two prominent examples. Proof-of-Work based blockchain systems do not scale by construction: indeed, maintaining a common ledger implies *every* node possessing a *full* copy of this ledger. Without this condition, the security – most important property of such systems – is compromised. Therefore, there is no gain in efficiency when a new node joins the network. Ouroboros is a Proof-of-Stake protocol, meaning that at any given time, a trusted set of nodes maintain the integrity of the system. This protocol was shown in an experimental setting to be resistant to a handful of attacks that are known to plague other systems and are directly relevant to gambling protocols.

2. <u>Random number generation:</u> finally, Ouroboros, the POS protocol underlying Cardano blockchain in its workings fully relies upon generating unbiased (i.e. uniformly distributed) entropy. The beauty of the idea is that the blockchain itself serves as a broadcast channel: *the uniform randomness is generated on-chain*! For us, this is the crucial point, so let's elaborate on it further.

   POS systems are heavily dependent on the ability to generate good-quality randomness "to inject pure entropy into the system". Without it, the integrity of the protocol can be interrupted. This stems from the fact that if there is a way to manipulate the process of selecting an agent who is chosen to validate the next block, an adversary can bias the election process. This is the root of the infamous "Nothing-at-Stake" problem and invalidates the whole concept of POS-based distributed consensus protocols. Apart from provably random number generation, another pre-condition for the plausibility of POS protocols is that these numbers are actually delivered to everyone participating in the protocol. In other words, the delivery of uniform randomness has to be guaranteed on the protocol level. Hence, to be a valid concept, especially from a formal academic viewpoint, Ouroboros must have a mechanism for generating *and* broadcasting "good" randomness. Furthermore, to be scalable, the generation and verification processes must be computationally inexpensive.

Ouroboros solves these problems by embracing two well-known protocols from the field of distributed consensus: coin-tossing application of commitment schemes and verifiable secret sharing. Blending these two together produces a miracle: it creates a protocol for creating unbiased public randomness in a distributed adversarial setting with guaranteed output delivery. In layman terms, this means that Ouroboros:

a. Generates provably random numbers;

b. Guarantees that everyone will get them. Unchanged.

We will touch upon the topic of randomness again in the technical deep-dive below.

Apart from providing elegant solutions to the existential problems of on-chain casino protocols, Cardano offers a rich toolbox for solving several less critical issues:

3. <u>Flexible and finance application-tailored scripting language:</u> those who have experience with the Bitcoin scripting language know how draconian and inflexible it is, those who spent thousands of hours grinding through Solidity (the Ethereum scripting language), know how quickly it might become overly complex. Rigidity limits the number of applications; complexity limits the set of actors who are capable to work with the language and introduces larger scope for unintended errors and unnoticed bugs. To create a truly universal platform where those with bright ideas can compete for their share in the overall pie, one needs a simpler language whereby, simplicity would not come at the expense of the scope of application. Plutus is a general purpose Smart Contract language developed by IOHK and implemented in Cardano.

   The core idea is that any type of financial transaction can be decomposed into simpler ones. Therefore, all the wide variety of complex financial instruments is comprised of a much smaller set of "foundational elements" that create the entire transactional logic. Cardano is designed by matters of code and is set to follow best practices; its scripting language is tailored for financial applications: security and execution can be "extremely well understood".

   With a certain degree of abstraction, one can observe strong parallels between any financial derivative and most of the gambling applications: in essence these are just contracts between one or more parties where outcome is conditioned, in part, on a realization of a random variable. This leads us to conclude that Plutus is the best of kind natural fit for writing casino applications.

Cardano is scalable, secure, and complex yet elegant. The major takeaway is that designing a successful POS protocol requires solving the *same problems* that constrain the creation of provably fair on-chain casinos. With Cardano as a backbone, Sp8de is set to become the best of its kind.

Our claims don't require you to blindly trust us: all the results we rely on are proven with academic rigor and can be accessed by anyone on the ever-growing library of academic papers maintained by the IOHK foundation. Our competitors can appeal to the crowd stating that their protocol is unique, efficient and practically difficult to manipulate. Believing this implies having faith in their team: all the existing projects are either work-in-progress or completed, but centralized. All the results we rely upon are established with mathematical rigor and academic formalism by those for whom developing cryptography as a science is a profession, and state of the art code is an everyday tool.

# The Sp8de Protocol

Before delving deeper into the mechanics of the SP8DE protocol itself, we opt to give a brief overview of the Cardano blockchain and, in particular, the Ouroboros protocol that underpins it. As mentioned above, Ouroboros is the first provably secure POS protocol. All POS protocols rely heavily on the miner selection process whereby a participant is selected at random to sign a block of transactions. In essence it is a POW system without the anchor to the real world – that of processing power. A precondition for an effective POS protocol is the ability to select the next 'miner' (or minter using the POS jargon) randomly with the uniform probability which is proportional to one's stake in the system. The uniform nature of the probability distribution is an essential element: if it can be skewed or biased by any protocol participant, the security is compromised rendering the protocol useless.

At the heart of Ouroboros is the so-called Follow-The-Satoshi (FTS) procedure. Its essence is simple: assuming input of the uniform randomness, FTS is guaranteed to select a stakeholder with the uniform probability proportional to the number N of coins (or satoshis) one possess relative to the total number of coins in the system. In short, FTS does the job: it possess the qualities required to make an effective POS protocol. But, as always, there is a catch: FTS assumes input of 'proper' randomness. But where does it come from? Before answering this question, let us lead your through the mechanics of FTS procedure itself: it will prove useful later on.

The FTS proceeds along the following steps:

a. The fresh randomness is injected into the system;

b. It is used to 'pick' a single satoshi, the smallest unit of account in the system, an analogy to cent for US dollars;

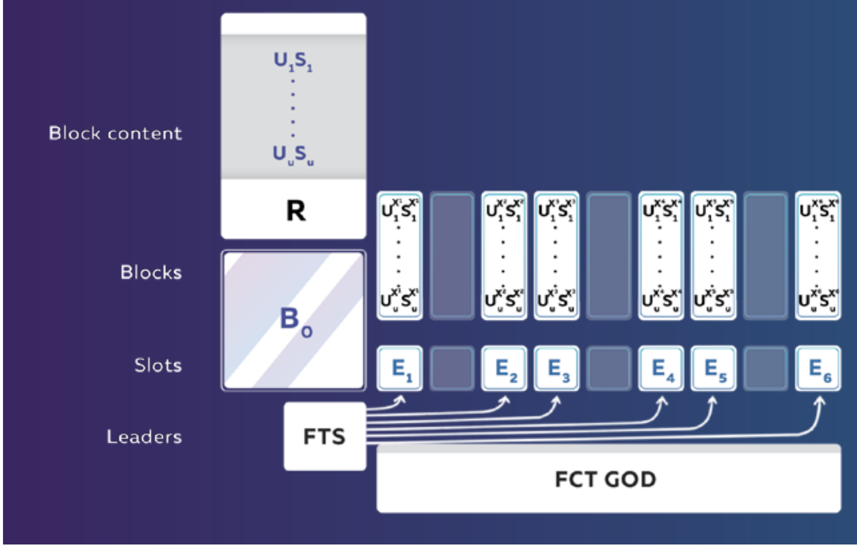
c. All satoshis have ids. The state of the protocol determines which user (determined by the wallet id) was the last one to hold the satoshi selected;

d. This user becomes the 'leader' or in other words is entitled to sign a block;

This simple procedure satisfied the required qualities of the protocol: assuming the input of unbiased randomness, it will select a stakeholder with the probability proportional to one's stake in the system. Injecting 'good' randomness into the protocol is another important concern. FTS assumes input of good randomness, but in order for the protocol to work this randomness needs to be generated on-chain. At this point it is important to highlight the similarity of the design challenge that faces the POS protocols and on-chain gambling applications: both of them require on-going inputs of unbiased distributed randomness.

Ouroboros employs the Fair Coin Tossing (FCT) procedure to generate randomness. This procedure is a known result in the field of academic and applied cryptography. It was first coined over 30 years ago and its mechanism is well studied and understood and is, thus, very efficient. The idea is that multiple entities participating in the protocol exchange 'messages' (the so-called commitments) that are encrypted by the sender and therefore are not known up-front by the receiver. When opened (by exchanging the keys) and combined, these messages produce an output that cannot be known a priori and neither can be manipulated by those participating.  One problem that remains is the possibility of one of the parties aborting the protocol by not sending the key to one's message. In the Ouroboros protocol this issue is solved by employing yet another protocol that is called Publicly Verifiable Secret Sharing (PVSS) PVSS basically ensures that (given the honest majority) the message is delivered to everyone participating even if a malicious party chooses not to share one's key. The combined procedure is called the Fair Coin Tossing protocol with Guaranteed Output Delivery (FCT GOD).

Armed with the PVSS and FCT machinery, Ouroboros protocol proceeds in steps: the minor steps are called slots and represent a spot in the protocol time whereby an elected leader has a chance of signing a block of transactions receiving the fee reward. The major steps are called epochs: these contain multiple slots and end with running of the FTS procedure. A stylized illustration of a single epoch is given in figure X:



$U_i$ – user id

$S_i$ – amount of funds (cum number of satoshis)

R` – random String for Epoch (prime is user to determine the epoch)

$E_n$ – user selected to sign the block in a given slot

$t_n$ – Transactoins in a given block (block content)

$st_n$ – state of the chain

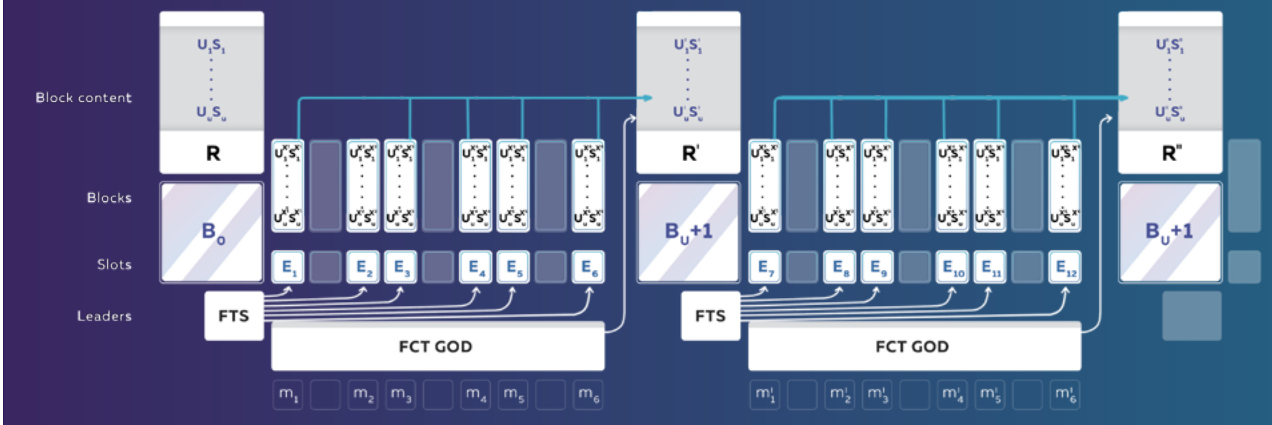
$B_n$ – block

FTS – Follow The Satoshi

GOD – Guaranteed Output Delievery

SIG – Signed by

The protocol is broken down into slots, slots contain blocks, and blocks contain transactions. The outcome of the FTS procedure determines all the slot leaders (those entitled to sign a block) for the following epoch. A stylized version of the multi-epoch protocol is illustrated below:



$U_i$ – user id

$S_i$ – amount of funds (cum number of satoshis)

R` – random String for Epoch (prime is user to determine the epoch)

$E_n$ – user selected to sign the block in a given slot

$t_n$ – Transactoins in a given block (block content)

$st_n$ – state of the chain

$B_n$ – block

FTS – Follow The Satoshi

GOD – Guaranteed Output Delievery

SIG – Signed by

At the beginning of every epoch the new distribution of stakes is determined from the blockchain state (the previous distribution along with all the signed transactions of the past epoch). Given that the distribution of tokens among stakeholders is taken from the past transaction history once it is set in stone at the end of every epoch, it is impossible to know upfront which satoshi will be chosen. The FCT GOD procedure is run in parallel with the protocol and is used to generate randomness for the next FST.
Being designed along these lines, Ouroboros is a blockchain protocol that makes the blockchain itself serve as a broadcast channel for randomness. By solving the problem of the POS protocols, Ouroboros simultaneously offers a unique toolbox for developing and running decentralized casino applications in an efficient and provably secure manner. The key words that are scattered over countless pages of academic papers written by the IOHK foundation are: ‘guaranteed’, ‘provably’ and ‘secure’. What else can one wish for when it comes to online gaming?

At the heart of Sp8de is the protocol that generates unbiased randomness at arbitrary frequencies: it synthesizes the workings of Ouroboros and Sp8de blockchain itself to generate entropy.

All the gambling applications on the Sp8de blockchain represent complex Smart Contracts that use SPX as their native currency. The outcomes of all the games on the Sp8de blockchain are conditioned upon the realizations of the coin tossing procedure that drives the Ouroboros protocol. The entire Sp8de ecosystem will flourish around these injections of entropy. The use of the seed will be application-specific. The mechanism will work as follows:

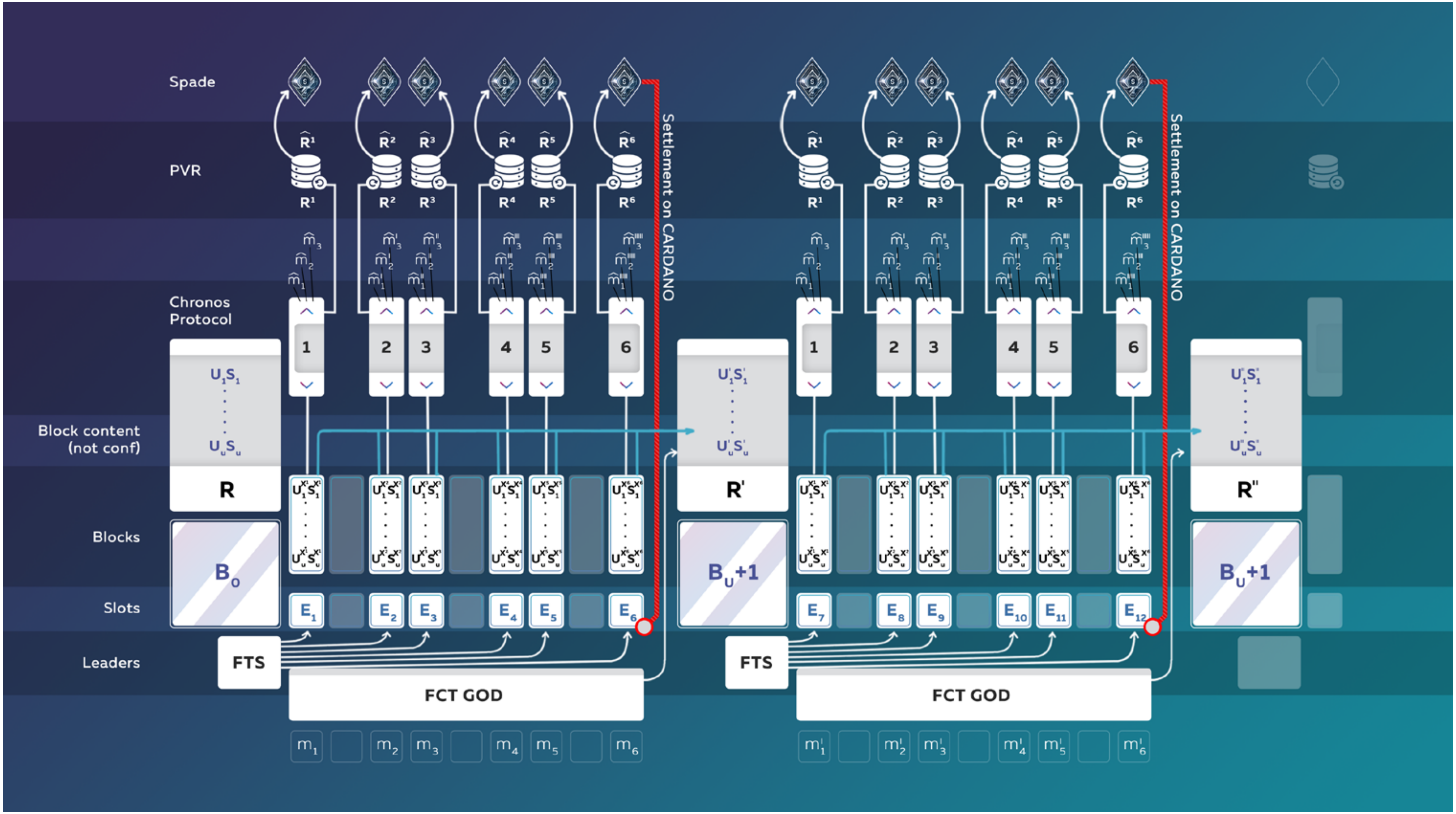
1. Cardano epoch begins with a fresh seed that derives from the distribution of coins among holders at the end of the previous epoch. This information rests on the public Cardano blockchain and is, thus verifiable by any interested party.

2. For every slot of the current epoch a coin tossing protocol with guaranteed output delivery is run facilitating the election of a slot leader. This protocol has the name: “Follow-the-Satoshi” or FTS for short. The essence of FTS is that, given a distribution of all the coins among all the coin holders, that is fixed at the beginning of an epoch and an injection of fresh randomness by the means of coin tossing routine, the protocol selects one leader for every slot of the current epoch. The random string that is used in the selection process is provided independently by the participants of the network through running the coin tossing protocol.

3. At this point an issue becomes apparent: fresh randomness is injected into the protocol only once for every epoch. It means that limiting ourselves to using only this randomness for determining the outcomes of Sp8de-based casino applications constrains us to running only one provably fair round every epoch. This is highly infrequent. This issue, if left unresolved, renders the whole concept of Sp8de obsolete. We can’t afford it.

   Therefore, here is our plan:

   a. Create a Smart Contract that constantly runs the Cardano native coin tossing protocol with guaranteed output delivery. Every time a particular block is “minted” on the native Cardano blockchain, the Smart Contract emits a random string that inherits all the “good” qualities of the Cardano’s native coin tossing protocol. The nodes participating in the protocol (those who actually commit and then open) represent all the online nodes having stake in the *Sp8de* blockchain. This ensures that computational overhead of running (already very efficient) SCRAPE protocol is significantly reduced: the number of shares that have to be verified is limited to Sp8de nodes only. In this way, we detach the leader selection process from the process of generating random numbers that we actually need: the coin distribution evolves on Cardano, while entropy is being created on Sp8de.



$U_i$ – user id

$S_i$ – amount of funds (cum number of satoshis)

R` – random String for Epoch (prime is user to determine the epoch)

$E_n$ – user selected to sign the block in a given slot

$t_n$ – Transactoins in a given block (block content)

$st_n$ – state of the chain

$B_n$ – block

FTS – Follow The Satoshi

GOD – Guaranteed Output Delievery

SIG – Signed by

b. By implementing this modification, we, however, expose Sp8de to other risks: on very short time intervals while new blocks on Cardano blockchain are not 'stable" an adversary can fork the chain if one is selected as a slot leader. While in the presence of honest majority, such actions can benefit an adversary only with a negligible probability on the native Cardano blockchain, the Sp8de chain is much more susceptible to these attacks as it relies on relatively smaller amounts of aggregated on-chain entropy (one block against one epoch). We resolve this issue by employing Verifiable Random Function (VRF) developed by IOHK team in their work on Ouroboros Praos. In a nutshell, given sufficient input entropy, VRF outputs an unpredictable value.

c. Now, even if we assume that a determined and highly sophisticated adversary by being present on both chains (Cardano and Sp8de) and being elected as a slot leader on the Cardano chain, wishes to make a malicious fork that would affect the results of the coin tossing procedure, the application of VRF, makes the results of any such manipulation unpredictable, thus useless.

d. Once the settlement issue is resolved, there remains nothing else that can be subverted by an adversary on Sp8de chain without the need to manipulate the overarching Ouroboros protocol that drives the Cardano blockchain. Indeed, the settlement of Sp8de transaction is done on Cardano, the randomness is provided by the changing Cardano stake distribution and local SCRAPE protocol that is run by Sp8de nodes. Any potential incentive to manipulate both chains is mitigated by the use of VRF.

With the Sp8de protocol set up and running, we can start actually deploying the applications that represent some gaming logic implemented using Cardano's smart contract scripting language. These applications run on Sp8de blockchain and get settled with every new heartbeat of the protocol or less frequently depending on the actual application.

The efficiency constraints are, of course, inevitable when it comes to application that would require extremely high-frequency outputs (such as once every 5 seconds). We cannot claim that all the issues with such applications will be resolved before the protocol is deployed. We can state, however, that Sp8de is in the best position to solve them.

# Token Distribution

## Sale

The entire token distribution will be 8,888,888,888 of which 3,655,555,558.4 (41.125%) will be in the form of token sale and 3,455,555,552 (38.875%) will be given as a jackpot to those who have participated in the "token sale" rounds. The remainder of the tokens 1,777,777,778 (20%) will be vested with the team for the purposes of marketing, advisory, and further development of the project (see the Token Proceeds Utilization section for further details on the use of the proceeds from the token distribution). There is a **one year vesting period** that applies to these tokens. From Table 2 it becomes clear that the SPX tokens received per ETH are decreasing after each sale while the tokens distributed are increasing following the Pre-Sale stage.

The token sale will take place in four rounds and the amounts in each round are as follows:

| PHASE | TOKENS DISTRIBUTED | SPX PER ETH | ETH |
|---|---|---|---|
| Pre-Sale | 888,888,888 | 98,888 | 8,989 |
| Sale I | 388,888,888 | 88,888 | 4,375 |
| Sale II | 585,858,585 | 78,888 | 7,426 |
| Sale III | 886,868,686 | 68,888 | 12,874 |
| Sale IV | 905,050,511 | 58,888 | 15,369 |
| Total | 3,655,555,558 | | 49,033 |

**Table 2** Token sale phases

## Jackpots

Everyone who participated in the token sale will be eligible to receive tokens during the jackpots. Table 3 outlines the jackpot distribution schedule:

| PHASE | TOKENS DISTRIBUTED |
|---|---|
| Jackpot I | 288,888,888 |
| Jackpot II | 388,888,888 |
| Jackpot III | 888,888,888 |
| Jackpot IV | 1,888,888,888 |
| Total | 3,455,555,552 |

**Table 3** Jackpot phases

# Distribution Schedule

The token distribution begins on Monday, January 08, 2018 and ends on Sunday, March 11, 2018 and is scheduled as in the manner illustrated in Table 4 below. The Pre-Sale lasts for 24 days while each Sale phase will be seven days followed by a Jackpot that is distributed entirely within a single day after every Sale. A graphical illustration of the entire SPX distribution can be seen in Figure 2 below.

| Phase | Begins on | Ends on | SPX |
|---|---|---|---|
| Pre-Sale | Monday, January 08, 2018 | Thursday, February 08, 2018 | 888,888,888 |
| Sale I | Thursday, February 08, 2018 | Wednesday, February 14, 2018 | 388,888,888 |
| Jackpot I | Thursday, February 15, 2018 | Thursday, February 15, 2018 | 288,888,888 |
| Sale II | Friday, February 16, 2018 | Thursday, February 22, 2018 | 585,858,585 |
| Jackpot II | Friday, February 23, 2018 | Friday, February 23, 2018 | 388,888,888 |
| Sale III | Saturday, February 24, 2018 | Friday, March 02, 2018 | 886,868,686 |
| Jackpot III | Saturday, March 03, 2018 | Saturday, March 03, 2018 | 888,888,888 |
| Sale IV | Sunday, March 04, 2018 | Saturday, March 10, 2018 | 905,050,511 |
| Jackpot IV | Sunday, March 11, 2018 | Sunday, March 11, 2018 | 1,888,888,888 |

**Table 4** Distribution schedule

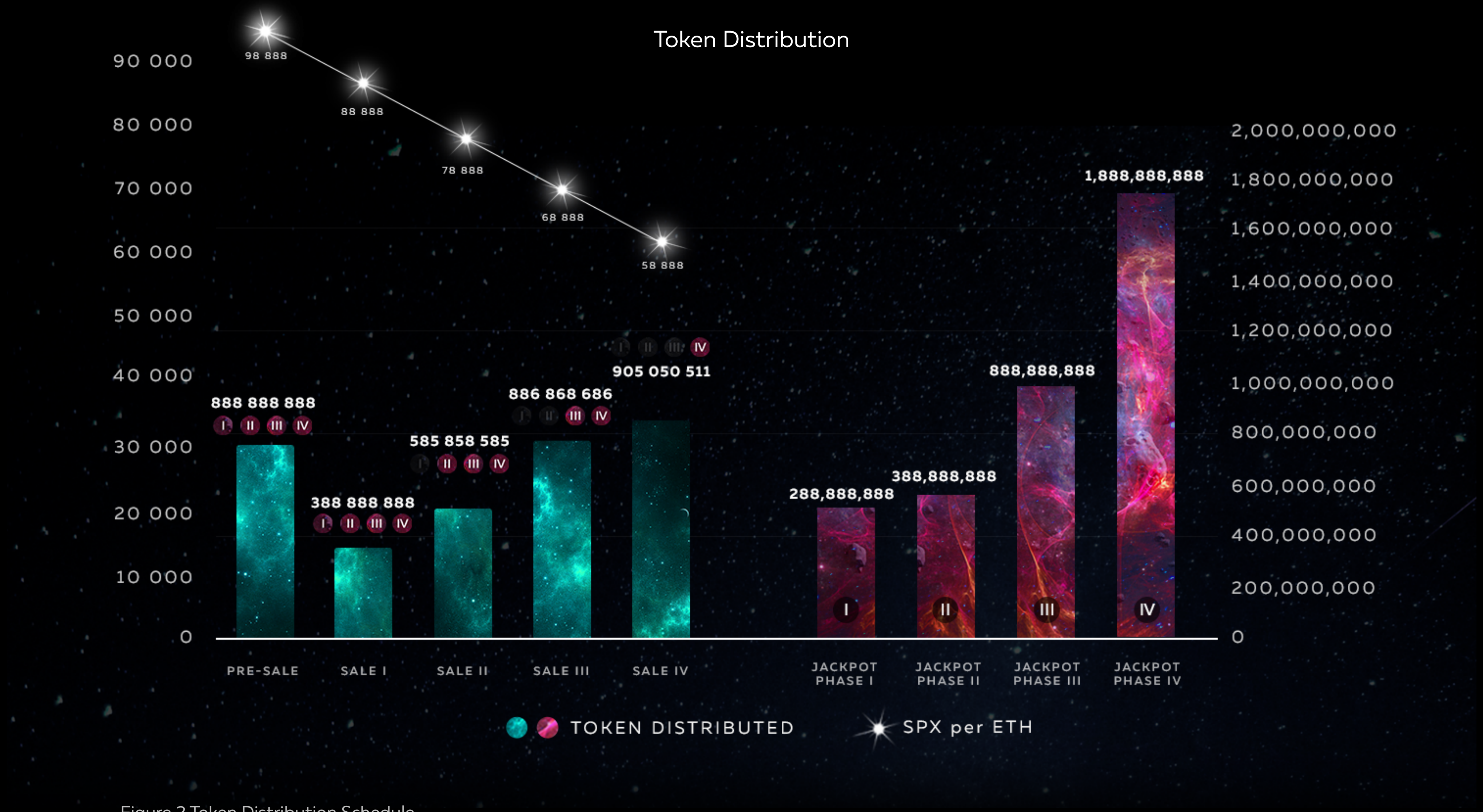
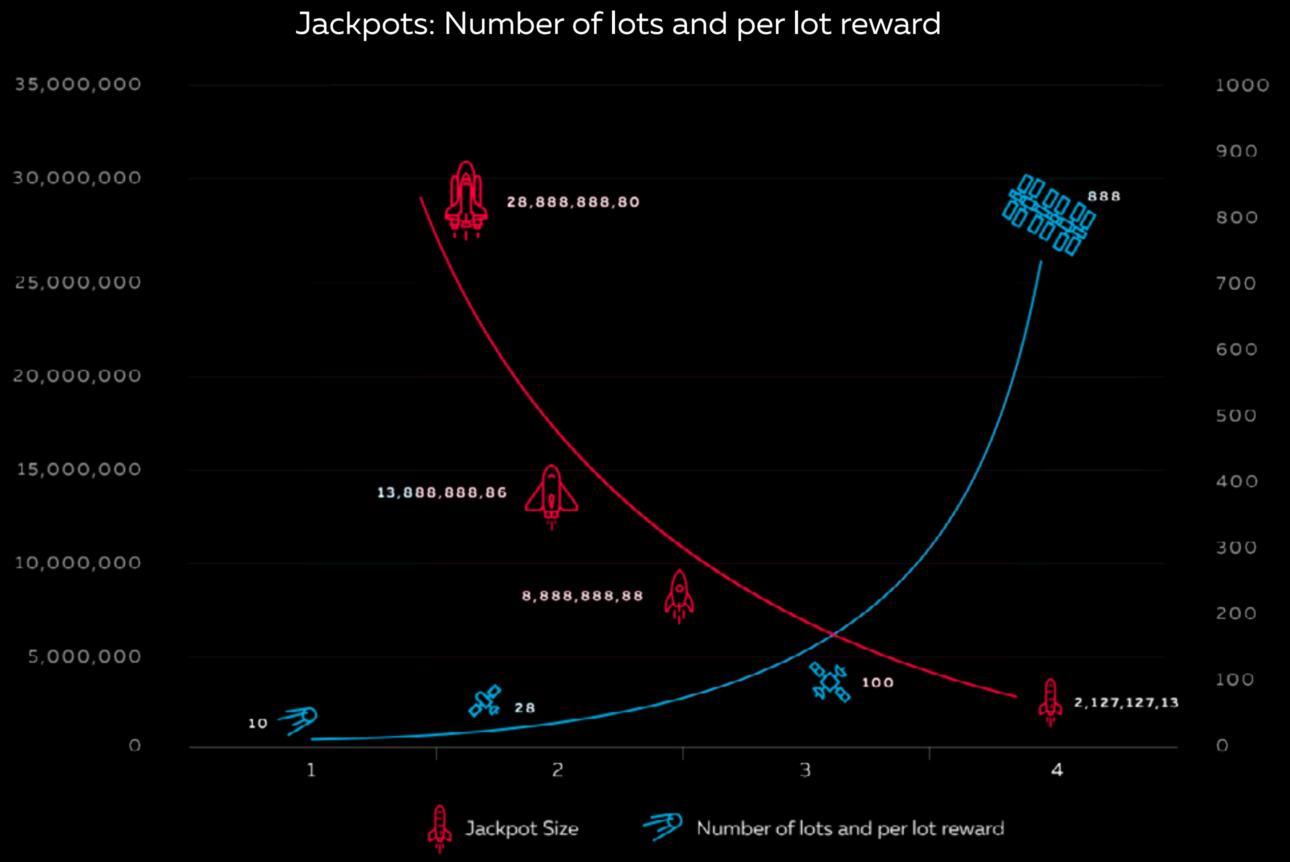


Figure 2 Token Distribution Schedule



Participants in the earlier jackpot rounds have small chance of winning large lot, while those participating later have higher c hance of winning, but are rewarded with smaller lots.

This shouldn't discourage late participation: the largest combined pool of prize tokens is played during the fourth jackpot round. In addition, earlier contributors participate in more jackpot rounds.

**Figure 4** Jackpots: Number of lots and per lot reward

So, those participating in the earlier jackpot rounds have small chance of winning large lot, while those participating later on have larger chance of winning, but are rewarded with smaller lots. In addition, earlier contributors participate in more jackpot rounds: e.g. sale I investors try their luck four times, while those entering at sale III can only participate in two jackpots. This shouldn't discourage late participation: the largest combined pool of prize tokens is played during the fourth jackpot round. For every lot we run a procedure which randomly selects one token out of those already issued. The holder of this token becomes the winner of the lot.

Each token being sold has a specific factor attached to it, the jackpot factor. The likelihood to win a lot is proportional to this factor. Mind, that jackpot factors are ordered: even within one sale round, earlier contribution is rewarded with more 'powerful' tokens. The distribution of these factors for every round is shown in the table below.

# How do the Jackpots work?

1. In essence, every Jackpot is an airdrop of tokens, however, with major modifications.
2. Every token sold during the preceding Sale rounds has a chance of winning a Jackpot during the subsequent Jackpot phases. For example, if you participated in the Pre-Sale then you have a chance to participate in all four Jackpot phases, but if you participated in Sale IV then you get to participate only in Jackpot IV.
3. Jackpots are large lots of SPX tokens that will be granted to a "lucky guy" – the owner of the token that will be chosen as a winner. So, any winner will get the entire lot. For example, there will be only 10 wallets (or less) who will win 28,888,888 SPX tokens during Jackpot I.
4. Jackpot tokens do not participate in the subsequent jackpots, so winning a jackpot does not increase one's chances of winning another one.
5. An important aspect of the jackpot campaign is the presence of Jackpot Factors attached to every token. This makes the game much more interesting and allows anyone to actually influence one's odds to win the Jackpot.

The factor is the probability multiplier. Without these factors, every token would have a probability ***$n^{-1}$ * α*** of winning one jackpot in a particular Jackpot phase; where ***n*** is the total number of tokens and ***α*** is a constant equal to the number of jackpots within every particular Jackpot phase. With factors, the formula changes to

$$\frac{\mathrm{F_j}}{\sum_{\mathrm{i=1}}^{\mathrm{I}} \mathrm{F_i n_i}} * \alpha, \mathrm{j} \in \mathrm{i}$$

where ***j*** is the factor of a token, ***i*** is the group of tokens, ***n*** – the number of tokens in the group.

Every group is defined as having some factor that every token within this group holds and a number of tokens that belong to this group. **For example**, if you participated in the Pre-Sale by getting 1,000,000 SPX and you got a multiplier of 88.8 (the maximum), then every single token that you hold has a 4.93 times higher chance of winning one or multiple of the jackpots during Jackpot phases I until IV, as compared to someone holding the same amount of tokens but with a factor 18.

The total probability of you winning the jackpot during Jackpot phases I until IV is calculated as follows:

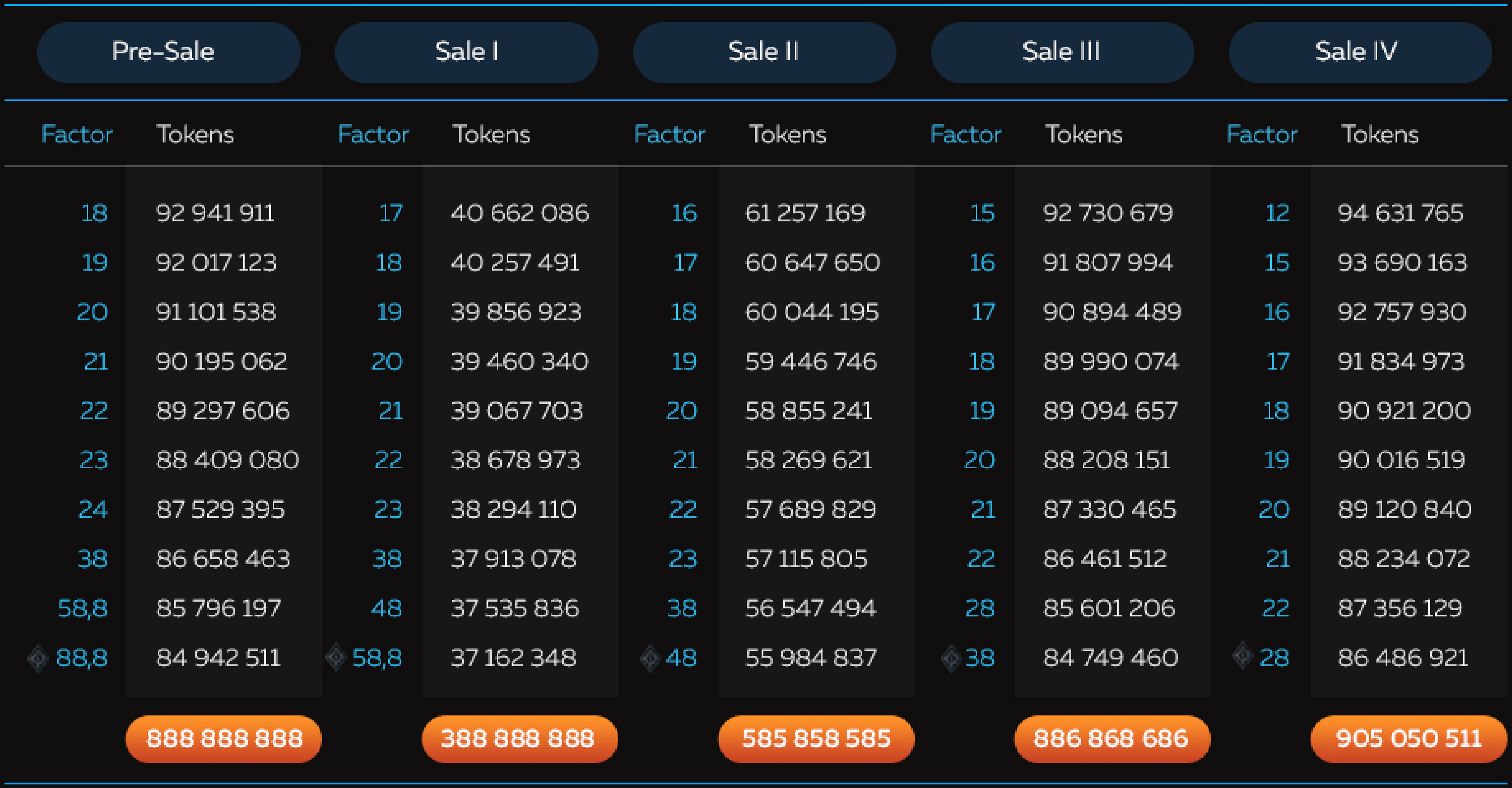
$$\frac{\sum_{\mathrm{j=1}}^{\mathrm{J}} \mathrm{F_j n_j}}{\sum_{\mathrm{i=1}}^{\mathrm{I}} \mathrm{F_i n_i}} * \alpha, \mathrm{j} \in \mathrm{i}$$

where ***j*** is a group id of tokens that you hold, ***n*** – the number within each group – therefore, a simple weighted probability. Of course, these numbers are different for every sale and jackpot round depending on how many tokens remain in the pools. **Following the logic of from the previous example**, the chance of winning a jackpot in Jackpot I with these parameters is equal to ~2.22%[1].

[1] (1,000,000*88.8)/(18* 92,941,911+...+88.8* 84,942,511+17* 40,662,086+...+58.8* 37,162,348)*10 = 0.022167377

# How Jackpots work?

The reader is referred to the Jackpots Mechanics paper for an overview of the Jackpots process.



| Pre-Sale | | Sale I | | Sale II | | Sale III | | Sale IV | |
|---|---|---|---|---|---|---|---|---|---|
| Factor | Tokens | Factor | Tokens | Factor | Tokens | Factor | Tokens | Factor | Tokens |
| 18 | 92 941 911 | 17 | 40 662 086 | 16 | 61 257 169 | 15 | 92 730 679 | 12 | 94 631 765 |
| 19 | 92 017 123 | 18 | 40 257 491 | 17 | 60 647 650 | 16 | 91 807 994 | 15 | 93 690 163 |
| 20 | 91 101 538 | 19 | 39 856 923 | 18 | 60 044 195 | 17 | 90 894 489 | 16 | 92 757 930 |
| 21 | 90 195 062 | 20 | 39 460 340 | 19 | 59 446 746 | 18 | 89 990 074 | 17 | 91 834 973 |
| 22 | 89 297 606 | 21 | 39 067 703 | 20 | 58 855 241 | 19 | 89 094 657 | 18 | 90 921 200 |
| 23 | 88 409 080 | 22 | 38 678 973 | 21 | 58 269 621 | 20 | 88 208 151 | 19 | 90 016 519 |
| 24 | 87 529 395 | 23 | 38 294 110 | 22 | 57 689 829 | 21 | 87 330 465 | 20 | 89 120 840 |
| 38 | 86 658 463 | 38 | 37 913 078 | 23 | 57 115 805 | 22 | 86 461 512 | 21 | 88 234 072 |
| 58,8 | 85 796 197 | 48 | 37 535 836 | 38 | 56 547 494 | 28 | 85 601 206 | 22 | 87 356 129 |
| 88,8 | 84 942 511 | 58,8 | 37 162 348 | 48 | 55 984 837 | 38 | 84 749 460 | 28 | 86 486 921 |
| | 888 888 888 | | 388 888 888 | | 585 858 585 | | 886 868 686 | | 905 050 511 |

Table 5 Token Sales' power (eligibility) for every Jackpot

**Table 5** Token Sales' power (eligibility) for every Jackpot

Let the game of chance begin.

# How jackpots work in practice?

1. Current jackpot phase (e.g. Sale I) ends at 9:00 AM (2018-02-14) UTC.

2. An additional half of an hour (until 9:30 AM) is given for all the 'late' transactions to settle. At 12:30 new SPX tokens are generated and distributed among the investors.Jackpots are large lots of SPX tokens that will be granted to a "lucky guy" – the owner of the token that will be chosen as a winner. So, any winner will get the entire lot. For example, there will be only 10 wallets (or less) who will win 28,888,888 SPX tokens during Jackpot I.

3. A list of transactions along with the factors and wallets of participating users is generated. The 'win' intervals are constructed taking into account the stake in the system and the factors. Additionally, we include the following variables: ETH addresses of participants, Start, End – the tokens participating in the jackpot.

   I. We calculate the Start, End for every user transaction. For example:

      a. $\mathrm{Start}(\mathrm{id}=1)=1;\ \mathrm{End}(\mathrm{id}=1)=\sum_{j=1}^{J}F_j n_j(\mathrm{id}=1)$

      b. $\mathrm{Start}(\mathrm{id}=2)=\mathrm{End}(\mathrm{id}=1)+1=\left(\sum_{j=1}^{J}F_j n_j(\mathrm{id}=1)\right)+1;\ \mathrm{End}(\mathrm{id}=2)=\sum_{j=1}^{J}F_j n_j(\mathrm{id}=2)$, in general:

      c. $\mathrm{Start}(\mathrm{id}=i)=\mathrm{End}(\mathrm{id}=i-1)+1=\left(\sum_{j=1}^{J}F_j n_j(\mathrm{id}=i-1)\right)+1;\ \mathrm{End}(\mathrm{id}=i)=\sum_{j=1}^{iJ}F_j n_j(\mathrm{id}=i)$

   II. Now, we relate the intervals in (I) to the user id's, effectively creating a list of the form: $\mathrm{ID}\ (\mathrm{id}=i), \mathrm{Start}(\mathrm{id}=i), \mathrm{End}(\mathrm{id}=i)$

1. Thereafter this list along with other relevant information is made public.

2. During the day of the jackpot (in this example, 2018-02-15), at 9:00 AM UTC the seed for generating random numbers is generated in the following way:

   a. We take the hash of the first slot with a block (not empty slot) confirmed after 9:00 AM UTC;

   b. We wait for the first block issued on the Bitcoin blockchain after the ADA block in 'a' to be confirmed and take its hash;

   c. We determine the number of the ETH block confirmed after the BTC block in 'b' and take the hash of the ETH block confirmed two blocks earlier;

   d. We concatenate the three hashes into one string:

$$H\left(ADA(n_t^{ADA})\right)+H\left(BTC(n_t^{BTC})\right)+H\left(ETH(n_{t-2}^{ETH})\right)$$

   where H is the hash, n – the number of the last block.

   e. We calculate the SHA-256 using the string in 'e' as the seed;

   f. We take the resulting 32-byte hash and turn it into an array of 8 integers which we will later use as the actual seed for generating random numbers

g. We put this seed into MT19937Generator and generate N random numbers in the range 1: MAX RANGE, where N is the number of jackpots, MAX RANGE is the weighted sum of the coins participating and their respective factors – basically the End parameter for the last participating id.

h. The prize distribution is made public, SPX are sent to the happy winners.

# Unpurchased Tokens Allocation

There is a possibility that some part of every token Sale will remain unpurchased. As illustrated in the table below the majority of the tokens that remain unsold will be automatically distributed among the Jackpots, increasing the number of tokens to be received by the participants in every Sale. If any tokens are allocated to the Sp8de Foundation they will be used for further development and promotion of the project.

| DISTRIBUTION OF UNPURCHASED TOKENS | | | | | |
|---|---|---|---|---|---|
| Phase | Foundation | Jackpot I | Jackpot II | Jackpot III | Jackpot IV |
| Pre-Sale | 30% | 30% | 20% | 20% | |
| Sale I | 20% | 15% | 40% | 25% | |
| Sale II* | 0% | | | | |
| Sale III* | 20% | | | | |
| Sale IV* | 30% | | | | |

**Table 6** Unpurchased tokens' distribution to the Jackpots

For example, if 10,000,000 SPX has not been purchased during the Pre-Sale phase then 3,000,000 SPX will be allocated to the Sp8de Foundation, another 3,000,000 SPX will be attributed towards Jackpot phase I; 2,000,000 SPX for Jackpot phase II; and the last 2,000,000 SPX for Jackpot phase III. These attributions will be made in equal amounts towards every of the jackpots within each of the Jackpot phases – i.e. during Jackpot I all of the jackpots will be increased by 300,000 SPX resulting in 29,188,888.80 SPX per jackpot. The same logic applies to the rest of the Jackpots and all unsold tokens.

The soft cap of the project is 4,500 ETH and hard cap is 31,000 ETH.

* To reward everyone in a reasonable manner we will distribute unsold tokens as follows: 100% of all unsold tokens during Sale II, 80% of all unsold tokens during Sale III, and 70% of all unsold tokens during sale IV to all participants in the Sp8de Pre-Sale and ICO. This will be done in proportion to the amount of their investment as percent of the total invesment amount fromall participants. All the tokens will be distributed after the ICO (March 11, 2018).

# Token Proceeds Utilization

The proceeds of the token sales as well as the tokens that remain in possession of the team will be used to promote and develop the project as outlined in the Road Map section of this paper. In the figure below, we show how the proceeds will be utilized. As we have shown earlier Sp8de is development intense, therefore we allocate the majority of the proceeds to development and operations as we believe that proper management and highly skilled developers are in the core of the success of this project. Furthermore, when needed the tokens allocated to the Sp8de Foundation and the team might be used for further promotion and as part of an incentives scheme.

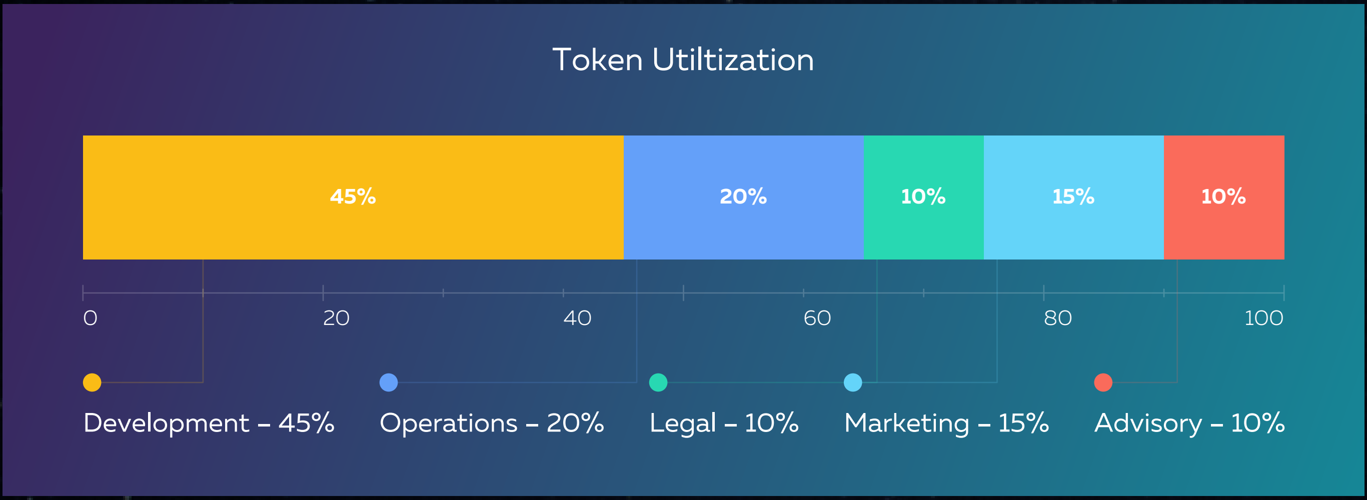


**Figure 5** Token utilization

## Crowdsale Proceeds Management

The funds raised during the Pre-Sale and the ICO will be held in the following cryptocurrencies and in the following proportions at the time of the conclusion of the ICO (March 11, 2018):

| Name | Ticker | Proportion |
|---|---|---|
| Bitcoin | BTC | 15% |
| Ethereum | ETH | 15% |
| Cardano | ADA | 40% |
| Ethereum Classic | ETC | 15% |
| Ripple | XRP | 15% |

**Table 6** Allocation of the funds collected

The distribution of the funds for development, marketing, operations, etc. will be done in these cryptocurrencies at the discretion of the team and these weights may not necessarily hold during the later stages of the Sp8de development.

# Team Board

### Alexey Kashirsky

*CEO & Co-Founder*

IT Mining Engineer graduate the Moscow State Mining University. MBA program of Mining Nitu «MISiS» Adviser to the General Director of NP «Miners of Russia» and an adviser to the Russian Academy of Natural Sciences, in the association «Industrial minerals»- an assistant to the president.

https://www.linkedin.com/in/alexey-kashirsky-166997b2/

### Mikhail Krapivnoi

*CIO & Co-Founder*

CIO & Co-founder ex Ceo of Man & Machine. A robotics research Company Multi Entrepreneur Champion in Online Poker and Chess Member of the AI Research Association Blockchain Evangelist and just a cool guy.

https://www.linkedin.com/in/mikhail-krapivnoi-1601a1142/

### Evgeny Borchers

*CVO & Co-Founder*

A visionary, experienced business expert focused on cryptocurrency investing, Fin-Tech, and affiliate marketing since 2013. Co-founder of a number of Fin-Tech projects, the most recent one of which DCEX, a digital currency exchange.

https://www.linkedin.com/in/evgeny-borchers-53906168/

### Alexander Baykiev

*CMO & Co-founder*

Responsible for the digital marketing, media communications, and creative content development to develop and sustain the brands of a number of businesses..

https://www.linkedin.com/in/alexander-baykiev-12654814b/

### Lyubomir Serafimov

*Chief Operating Officer*

Lyubomir headed the development of multiple cryptocurrency exchanges across Europe and US. His knowledge of the academic literature on market microstructure and its applications to liquidity provision are integral to Sp8de's token market availability while his knowledge of financial mathematics is essential to the technical design of the protocol.

https://www.linkedin.com/in/lserafimov/

### Mikhail Vakhrin

*Chief Business Development Officer*

Mikhail's experience in financial engineering and in devising complex algorithms are now fundamental to the technical design of the Sp8de protocol. Having raised funds in US and Europe, he is also an experienced entrepreneur and passionate speaker and is now strengthening the business relations for Sp8de.

https://www.linkedin.com/in/mikhail-vakhrin-a447b0129/

## Advisory Board

### Konstantin Katsev

*Blockchain Gambling Adviser*

Konstantin has over a decade of experience in marketing, web-development and entrepreneurship, as well as 2 years of productive work with blockchain-related infrastructure. He is currently involved in marketing and promoting the world's largest blockchain lottery platform, True Flip

https://www.linkedin.com/in/konstantin-katsev-881b3775/

### David Wainwright

*Blockchain Gambling Adviser*

An active investor & platform builder for over 20 years. Built and sold companies in over 20 countries including NetplayTV (Playtech), TelecomsTV (Oxygen8), HollywoodTV (Golden Race) and WHO Studios. Co-Founder of CryptoPad and founder of RealCasino and TheRedBox.

https://www.linkedin.com/in/davidwainwrightprofile/

### Artemy Zorin

*Graphics Design Adviser*

Interactive designer user interface and visual style for web and mobile applications. Visual design and branding manager, head of design department, «Yodiz» studio.

https://www.linkedin.com/in/temazorin/

### Alexandr Uglov

*Marketing Adviser*

Blockchain-evangelist and visionary. Has experience of staging in several projects C (SONM, Humaniq, etc). CEO of the Russian Media digital agency. Possesses 8 years of experience in Internet marketing and creating web services.

https://www.linkedin.com/in/uglovs/

# Advisory Board

### Norman Chou

*Strategic Business Adviser*

Norman Chou is a blockchain expert that brings 20 years plus of experience from the IT industry in Silicon Valley developing business partnerships globally. Not only has he surpassed his goals in enterprise sales year over year, he is a thought leader in Blockchain technologies. He has numerous engineering accreditations specializing in Business Marketing and Communications.

https://www.linkedin.com/in/normchou/

### Viv Anand

*Strategic Business Adviser*

Viv is a big believer in Blockchain technology and expects it to fundamentally change the way we live. He has a wealth of diverse work experiences including in corporate America (GE & McKinsey) and technology sales (Datalink, Nimble Storage & HPE).

https://www.linkedin.com/in/vivsf/

### Daniel Montaner

*Gambling Adviser*

World Champion Pro Gamer and Management/Consultant in eSports for teams such as compLexity, Evil Geniuses, and FaZe Clan. Voted Best Counter-Strike Player 2005 and North American Player of Decade.

https://www.linkedin.com/in/danielmontaner/

### Lantz Litchfield, Ph.D.

*Gaming Security Advisor*

Dr. Litchfield is a company executive and principal of a myriad of diverse professional service groups having extensive experience with a variety of organizations including Fortune-500 companies, government agencies, and military projects at the highest level of security covering industries such as Gaming, Internet e-commerce and dot-com start-ups. He holds a Ph.D. in Information Technology Management as well as the following computer security and IT certifications: CISSP, CSGE, CSGA, CSGI, CCSE+, CSE, CCSA, CCSI NG, NSI and NSA et al.

### Alexandr Malkov

*Legal Adviser*

Aleksandr is co-founder and CEO of Arbi (legal and escrow services for ICO), member of top 100 blockchain legal advisors in CIS, member of Expert Council on Digital Economy in the State Duma of the Russian Federation.

http://www.linkedin.com/in/александр-мальков/

# Advisory Board

### Dominikas Shpota

*Legal Adviser*

Dominikas is a Co-Founder and CFO of Arbi (legal and escrow services for ICO), serial Entrepreneur with a wide range of expertise: Cryptotrader, Financial Director of kpa.ru and Managing Partner of SB Burgers.

https://www.linkedin.com/in/dominikas-shpota-0108b538/

### Brian Krug

*Tech Business Development Advisor*

Brian brings an immense experience from a number of tech companies in California - he was a VP for over half a decade at Cisco, he is the founder and CIO at ITapp and currently Senior Director at ServiceNow.

https://www.linkedin.com/in/krugone/

### Andy Smith

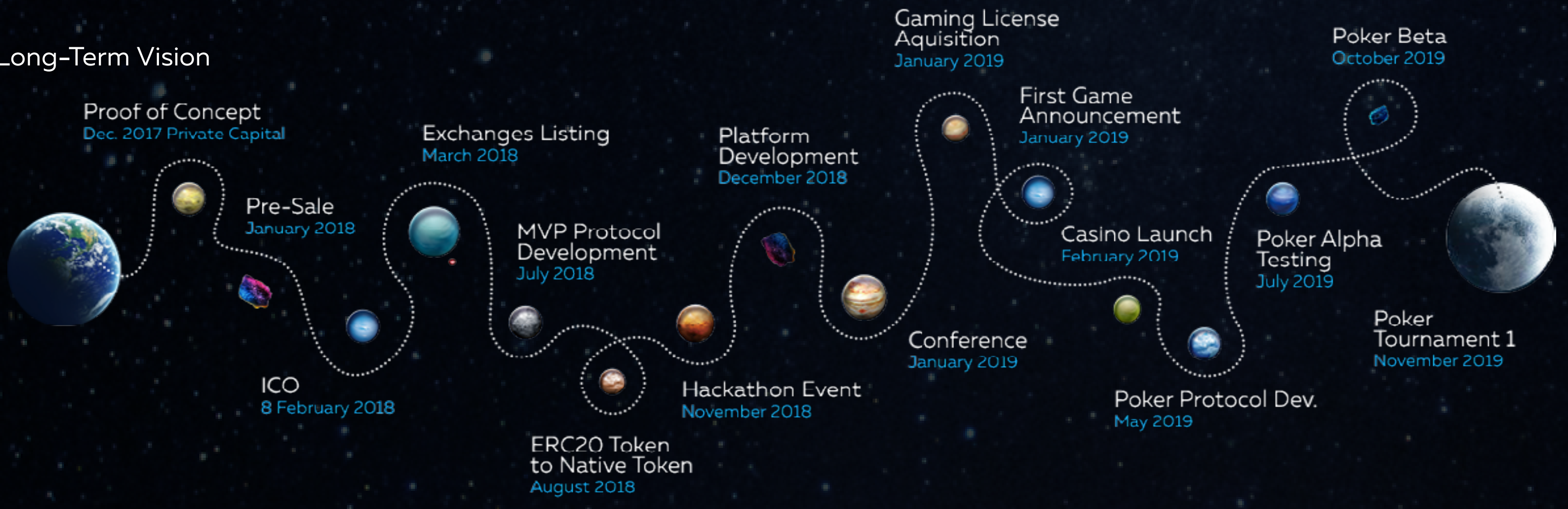
*Tech Entrepreneurship Advisor*

Tech marketer by experience, geek by destiny, Andy is General Partner of Center Electric, LLC where he invests in and helps grow early-stage companies as they build the Internet of Things (IoT). For the past 20 years he has served as an executive in the high-tech industry leading teams at Intel, Dolby Labs, BIGWORDS, LiquidWit, Analysis Group, Polaroid, Integral Inc. and PriceWaterhouseCoopers.

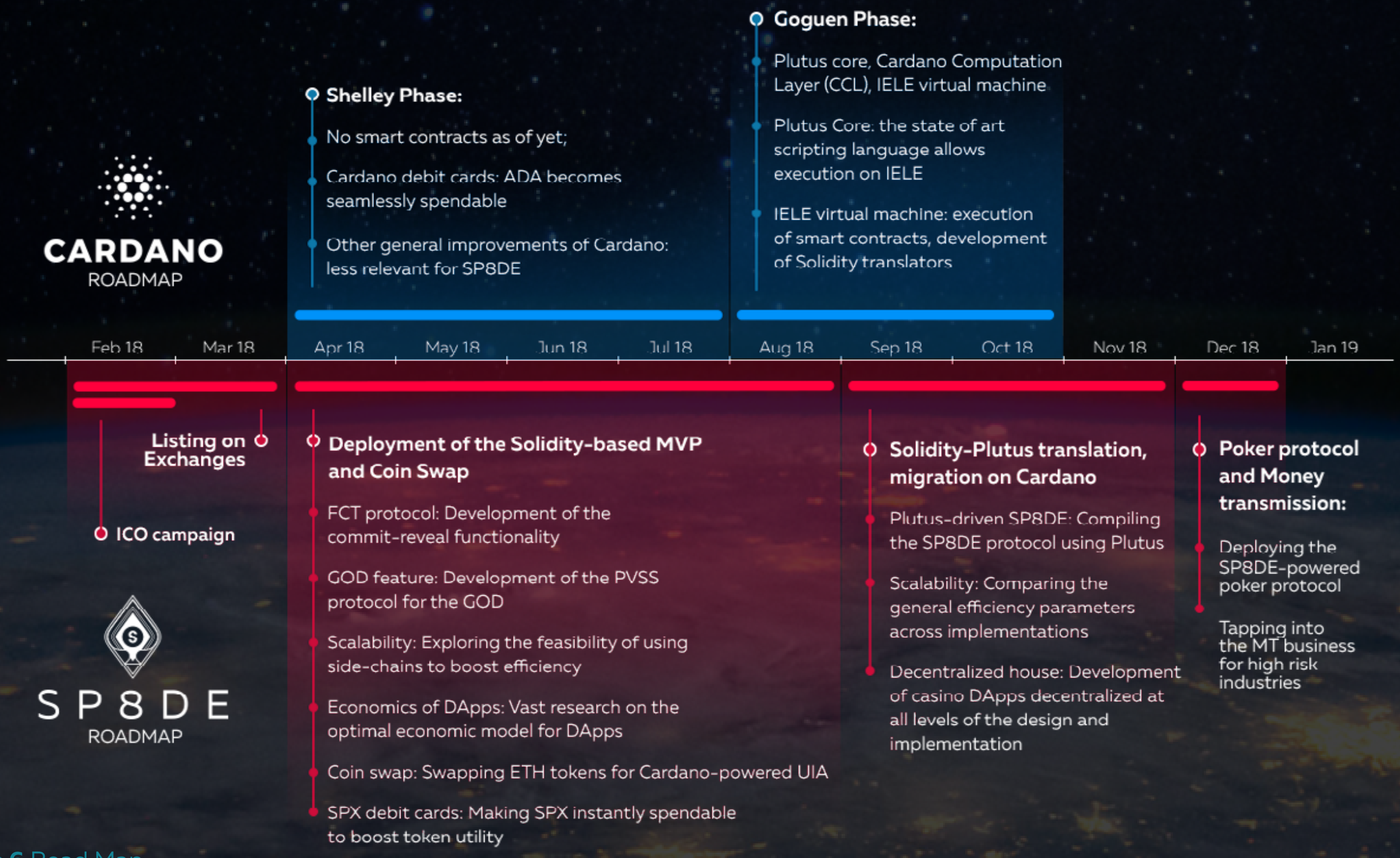
https://www.linkedin.com/in/andysmithlinkedin/

# Road Map

## The Long-Term Vision



## The One-Year-Ahead Road Map



**Shelley Phase:**

- No smart contracts as of yet;
- Cardano debit cards: ADA becomes seamlessly spendable
- Other general improvements of Cardano: less relevant for SP8DE

**Goguen Phase:**

- Plutus core, Cardano Computation Layer (CCL), IELE virtual machine
- Plutus Core: the state of art scripting language allows execution on IELE
- IELE virtual machine: execution of smart contracts, development of Solidity translators

**Listing on Exchanges**

**ICO campaign**

**Deployment of the Solidity-based MVP and Coin Swap**

- FCT protocol: Development of the commit-reveal functionality
- GOD feature: Development of the PVSS protocol for the GOD
- Scalability: Exploring the feasibility of using side-chains to boost efficiency
- Economics of DApps: Vast research on the optimal economic model for DApps
- Coin swap: Swapping ETH tokens for Cardano-powered UIA
- SPX debit cards: Making SPX instantly spendable to boost token utility

**Solidity-Plutus translation, migration on Cardano**

- Plutus-driven SP8DE: Compiling the SP8DE protocol using Plutus
- Scalability: Comparing the general efficiency parameters across implementations
- Decentralized house: Development of casino DApps decentralized at all levels of the design and implementation

**Poker protocol and Money transmission:**

- Deploying the SP8DE-powered poker protocol
- Tapping into the MT business for high risk industries

**Table 6** Road Map

## January 1, 2018 – March 31, 2018

### Conclusion of the ICO

The Sp8de ICO will be concluded on March 11, 2018 and Sp8de tokens will be moved to the respective wallets by March 16, 2018. We intend to hold the funds in multiple currencies to protect the project's funds against adverse idiosyncratic price movements (see the section on the ICO proceeds management).

### Listing on Exchanges

Until the end of March, 2018 collaboration with cryptocurrency exchanges will be initiated in order to list the Sp8de token on as many large exchanges as possible. We will try to avoid SPX being listed on small exchanges or exchanges with notorious reputation. An official announcement will be made on the Sp8de website with regard to the exchange on which the token is to be listed five business days prior to the listing event itself. Listing on exchanges will not end at this stage as it is a continuous process.

## April 1, 2018 – July 31, 2018

### Minimum Viable Product

During the Q2, 2018 major developments of the Cardano blockchain and fundamental expansions of the project's ecosystem are expected. In particular, the end of that quarter will see the release of most of the Shelley phase planned functionality enhancements and other related protocol improvements. For us, however, this will be only a small step towards realizing the ultimate potential of the Khronos protocol. The problem is that the delivery of promised Khronos functionality is contingent upon the completion of the Goguen phase of Cardano roadmap: IELE, Plutus and associated compilers are essential for building Khronos.

Therefore, instead of sitting and waiting for the required releases we will develop all the core functionality on Solidity using ETC blockchain as the base. There are multiple good reasons behind preferring ETC blockchain over any other solution existing on the market. The three major reasons are that:

1. Cardano and ETC have (at least partially) same user base, founders and community in general;
2. One of the priorities on Cardano's Goguen phase roadmap is to develop translators/compilers from Solidity and Plutus Core for IELE, the new-generation virtual machine that underpins the smart contract functionality. Solidity seems like an obvious candidate given this native support.
3. ETC is on average much less congested and thus significantly faster than the ETH network. The sidechain functionality that is being developed in Callisto initiative will also prove important for scalability that is essential for the SP8DE platform.

Using Solidity SP8DE team will develop the product with the minimum required functionality: a Fair Coin Tossing protocol with Guaranteed Output Delivery (FCT GOD) that is capable to output random numbers at high (not arbitrary) frequencies. Other significant functionality enhancements will be postponed until the next Roadmap Stage.

Summarizing, by the end of the MVP (II) stage of our roadmap, SP8DE will have a version of the SP8DE protocol implemented on Solidity with a narrower functionality and limited scalability. Yet, this version of the protocol will be ready to be compiled on IELE due to certain degree of compatibility between the systems.

Furthermore, this stage of our roadmap will see SP8DE exploring the design of the general decentralized house casino DApps. In particular, we will model the economic incentives of the decentralized house design. The decentralized house is among the most challenging and exciting theoretical and practical issues to be resolved by the SP8DE team. We will be having an entire blog thread dedicated solely to the game-theory and implementation challenges we will encounter. In fact, the decentralized house design implies having a novel market currently non-existent in the real world: the market for the gambling risk. The house edge serves as the 'price' of the risk of allowing passive execution of the bets. So, it's the price of betting against the average skill of gamers. As this line of reasoning illustrates, the potential for economic analysis of the incentive structure design of decentralized house applications is immense. During this stage of the roadmap we will be concerned exactly with this. The community involvement is of high importance for us: we are excited to hear feedback/ consider proposals, etc.

We will expand our team to include one or several professionals with economic/mathematical background(s) prior to getting started.

## Swap of the ERC20 Token to the Native SP8DE Token

We hope that by the end of July, 2018 Cardano will be sufficiently developed to incorporate the UIA functionality. Once this is done, we will issue our SPX tokens on Cardano and implement a 1:1 swap. From this moment onwards, the entire SP8DE infrastructure will be based on the Cardano blockchain.

## Parallel Development on Cardano

All along the way, we will have an entire task force dedicated solely to exploring the progress of the Cardano project. We will develop SP8DE in parallel with Cardano utilizing all the pieces of functionality available.

## Debit Cards

In Q2, 2018 Cardano is planning on introducing the debit cards that would make ADA, the native Cardano coin, spendable seamlessly anywhere. We will work on getting all the regulatory approvals and other compliance matters right to do the same for the SPX token. Allowing for the instant payments with SPX would make it truly a universal betting chip. We, however, expect severe regulatory issues as the payment processing industry is quite hostile in terms of compliance. Yet, we will do our best to make the SPX debit card dream come true as soon as possible.

## August 1, 2018 – December 31, 2018

### Deploying SP8DE on Cardano

This period will be marked with major developments on Cardano, basically making it a fully functional blockchain with smart contracts live and ready for deployment. The major milestones of the Goguen phase (the third phase of Cardano development timeline) are the development of Plutus Core, CCL (Cardano Computational Layer) and IELE, the Cardano virtual machine. Basically, at this point, the functionality for implementing SP8DE on Cardano will be ready on the Cardano side.

At this moment, we will migrate our code from Solidity to Plutus and deploy the MVP developed earlier on Cardano. This will mark the beginning of the development of the most complex and intricate parts of the SP8DE protocol, those that have to do with increasing the efficiency (i.e. increasing the output frequencies) beyond that of the underlying blockchain itself. Our aim is to be able to output thousands of random strings per second if needed. This is similar in essence to the problem faced by the decentralized exchanges: the decentralized order book can only be as efficient as the underlying blockchain itself. We will go beyond that.

### Using ETC blockchain and Solidity – build the decentralized house MVP

At this point, we will have the theoretical foundation for the economics for the decentralized house applications ready to turn into a working Solidity code. We assume that we will stick to Solidity to deploy the MVP. This, however, does not need to hold true and might change subject to the degree to which Cardano will be ready to accommodate the desired extent of smart contract flexibility.

So, basically, the aim of this would be to design an application (say, Black Jack) whereby anyone participating could become a part of the house. By diversifying (i.e. pooling the funds) the risk of every backer and allowing the house edge to be determined purely by the market, our goal is to find the equilibrium level of the house edge. If such design is actually possible, we hope to arrive at a product superior to any currently existing centralized solutions: the world of gambling without economic frictions.

## December 31, 2018 – and beyond

Going forward, our major goals will be to perfect the protocol and put all the connections that we will have established to their best use: the widespread adoption of the SP8DE protocol throughout the entire gaming (and other) industry. This adoption will inevitably lead SP8DE to become the quality standard, hopefully making any application that does not use it suspicious at best.

# Financial projections

The SP8DE venture itself is a BVI (British Virgin Islands)-incorporated entity with the classic set of features from the corporate world: while being crypto-powered and driven and we still have a balance sheet, income statement, strategic goals, banking relationships, and etc. But don't judge us too quickly for being not 100% sincere: our priority is witnessing how the Sp8de protocol thrives and receives mass adoption and today we still haven't figured out a way DAO can e.g. get a license.

A classic nature of business organization implies having to answer the classic set of questions that every start-up (that we essentially are) has to address, one of them being "what's your business model?" Narrowing down this question we end up having to lay down the revenue model and the cost structure of our venture. Intelligent management of these variables defines the venture success in the long-run.

## Revenue Sources

1. The ICO campaign: essentially a token sale event is a way of crowd funding whereby the product being distributed represents a claim on future use of software: a token is the right to use the blockchain, making use of the blockchain holds only as much utility as the functions that it provides, the problems that it solves – just like utility of using regular software. This is why from the accounting standpoint; money raised during the ICO can be classified as revenue (with some liability component to it). After subtracting all relevant expenses, the remainder is retained inside and used to develop the venture.

2. The transaction fees: we envision the SP8DE protocol as being a platform hosting a myriad of DApps (Decentralized Applications) of various nature and feeding entropy inside them via an API-like interface. In our design every transaction within the DApp (e.g. betting on zero in roulette) is a part of the transactional logic of the smart contract powering the DApp, so there will be no fees that need to be paid. The fees are only paid for transferring funds from a DApp to another DApp or in other words, every time when the actual settlement takes place on the blockchain itself. Every such fee will be distributed as follows:

$$\sum_{i=1}^{N} fees_i = \sum_{i=1}^{M} miner_i + \sum_{i=M}^{P} premium_i + \sum_{i=P}^{D} dev(?)_i + \sum_{i=D}^{N} f_i$$

   In other words, every transaction fee is divided between the miner's fee and premium, the fee for the developer who built the DApp and a small part that goes to the foundation for sustaining the SP8DE project. This latter part will be our major revenue driver in the long run and obviously scales proportionately with the popularity of the platform.

3. The marketing revenue: while being open-source, SP8DE will have all the attributes of a classic software developing startup: of course, we will have a website, blog, wiki, etc. We will monetize the traffic on these resources by advertising. Yet, we will abstain at all times from interrupting in any way the popularity equilibrium within our ecosystem: no DApps will get priority over others – only the crowd decides who thrives and prospers and who is left in the backwaters of history.

4. The SPX tokens: a large number of SPX tokens remain at our disposal. We will dispose of these whenever we see fit (after the 1-year founders' vesting period) thereby generating additional revenue streams.
5. Commissions for betting: we will disclose the nature of this revenue stream in a separate white paper to be released soon.

## Cost Structure

The development of Sp8de is not a standalone task that simply implies having a team of developers and a lead that would produce the protocol that will then magically create the revenue streams. On the contrary, while the expenses towards development are substantial, they will not materialize in value producing assets unless supported by a) proper advisory board that would serve to alleviate the penetration into the gambling market; b) marketing as well as listing on exchanges which will help the wide adoption of the protocol by popularizing and making available the SPX token; c) licensing and legal advice; and d) operations' department that would serve as a guiding force behind the allocation and structure of all expenses by making sure that even a penny is not spent unwisely

A classic nature of business organization implies having to answer the classic set of questions that every start-up (that we essentially are) has to address, one of them being "what's your business model?" Narrowing down this question we end up having to lay down the revenue model and the cost structure of our venture. Intelligent management of these variables defines the venture success in the long-run.

### Cost Structure

1. The development team: here, the costs in the beginning of the project are negligible to none, nevertheless as the revenue streams of the Sp8de project are driven, first and foremost, by the development of the platform for eSports betting and the Sp8de protocol, these costs will begin rising sharply once these activities begin. The objective is to begin with a small development team which will have an encompassing knowledge of all Sp8de products, which later will grow much larger and more segmented, specializing on the development of each of the Sp8de revenue drivers.
2. The advisory board: the spending on advisory are large in the beginning, this is due to the fact that the Sp8de project has to be placed properly within the market niches where the expenses for the development of the project will be most efficiently utilized to serve and/or create the customer needs.
3. Marketing team: the marketing team will work closely with the advisors in order to reach the markets for which the Sp8de development team is creating products, but also will work towards creation of new markets which is a relatively marketing-heavy task
4. Legal counsel: both the crypto space and its integration within the current online betting environment are both relatively young and weakly regulated. Nevertheless, as these industries mature and more sub-industries are created from their interconnections also the regulatory burden on all businesses in this sector will exacerbate.

5. Operations department: this department will take care of the day-to-day operations of the company but also the medium to long-term cost planning and revenue projections. As the company grows this department will become larger and more complex in terms of employees and their location and their management.

In what follows we will visualize and describe briefly the incurred and projected revenues and expenses for the period December 31, 2017 – January 31, 2019.

Breakdown of Expenses by Type and Percent of Total

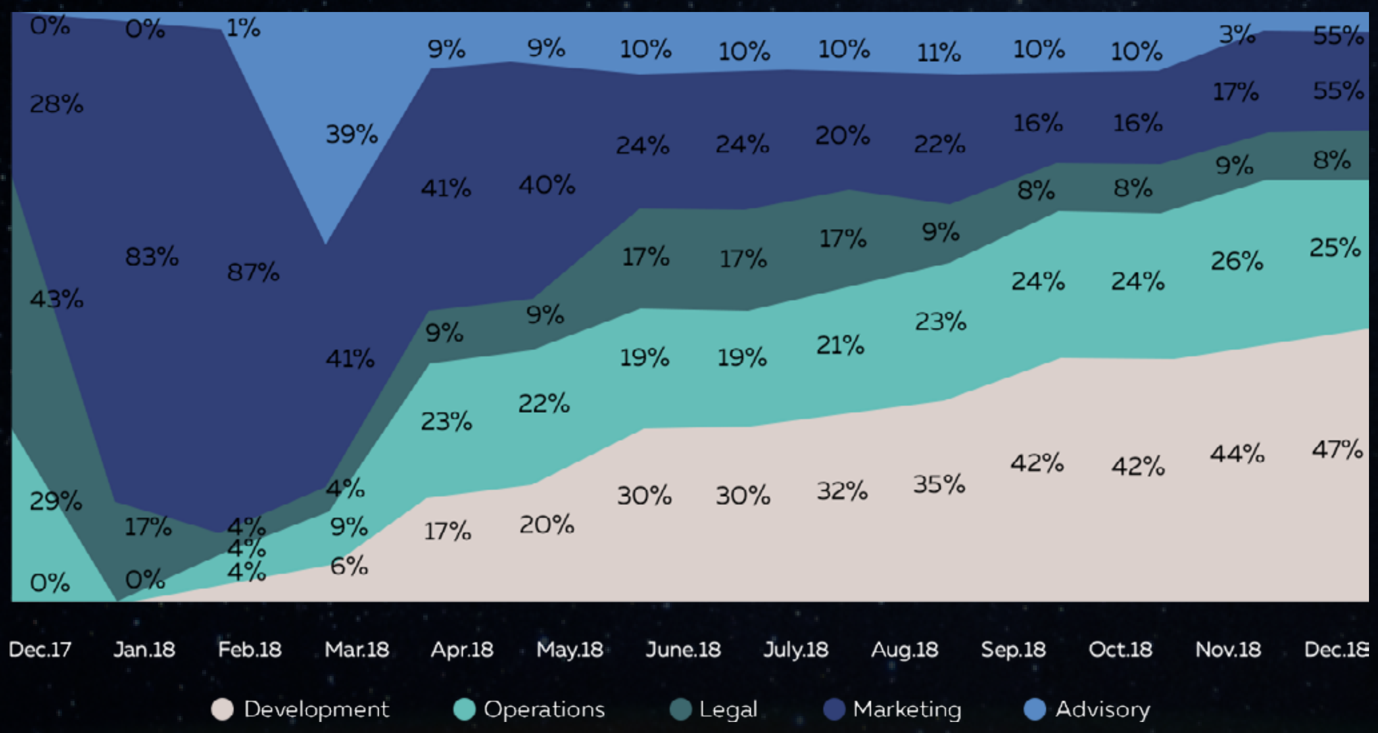


Figure 4 Expenses by type as percent of total

While marketing expenses are relatively large until May they will gradually decrease and the operating and development expenditures will continue to grow as Sp8de focuses on the development of the core product and the management of the company as a whole.

Legal expenses rise and then gradually fall as the main licenses are obtained, nevertheless these expenses may grow during 2019 along with those allocated for advisory. On the other hand, the allocation of funds towards marketing is expected to fall in time as stronger ties to the industry are established.

## Number of Employees by Function

The headcount will grow rapidly as the project enters the development phase in March, 2018 when the Operations department will add four new members – specialists for marketing, accounting, administration, and a one support. In addition, the development team will also grow in both headcount but also expenses as larger part of the budged is allocated for salaries for the developers as reflected in the previous figure.

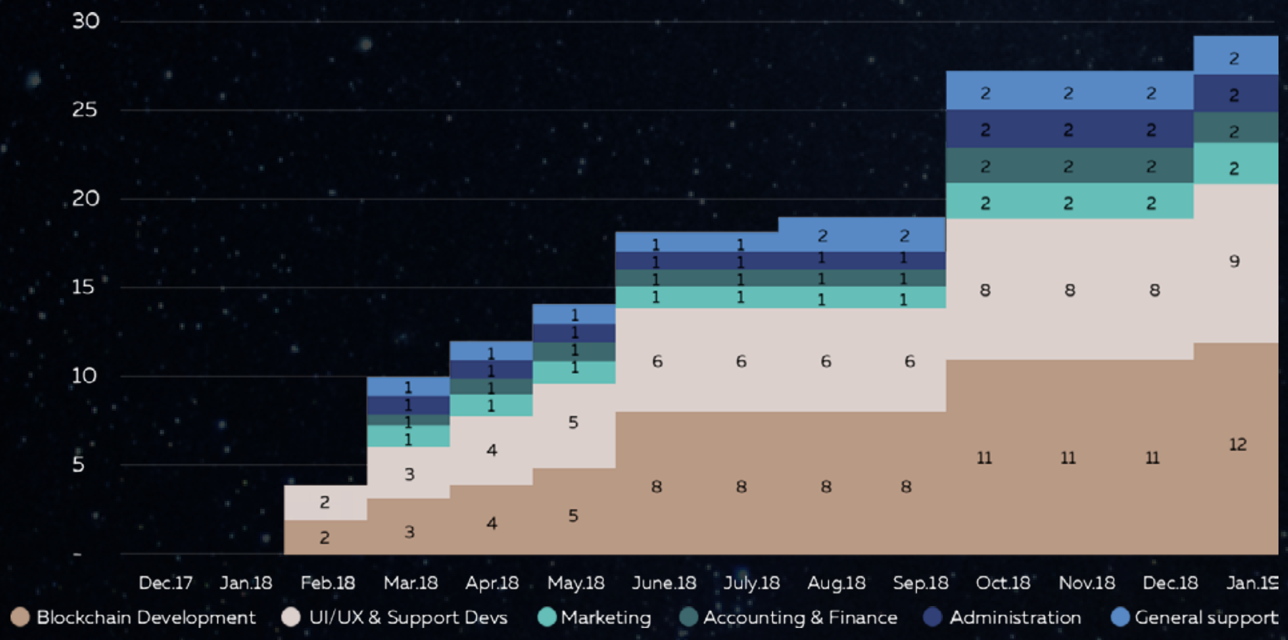


Figure 5 Number of employees by function

In the figures to the right, we show the net income of Sp8de when considering that 70%, 50%, and 20% of the ICO is complete. In these graphs we exclude the proceeds from the ICO as these "revenues" are one-time and do not represent the income generated by the operations of the company. The first revenue driver is that of the developed platform for eSports betting which is expected to become functional starting June, 2018. The reason for the slow growth of the revenues is that the market reach will be relatively weaker caused by weaker proportionately lower marketing and advisory expenses thought the period which. Break-even is expected to be reached by January, 2019 given that 50% of the funds are collected.

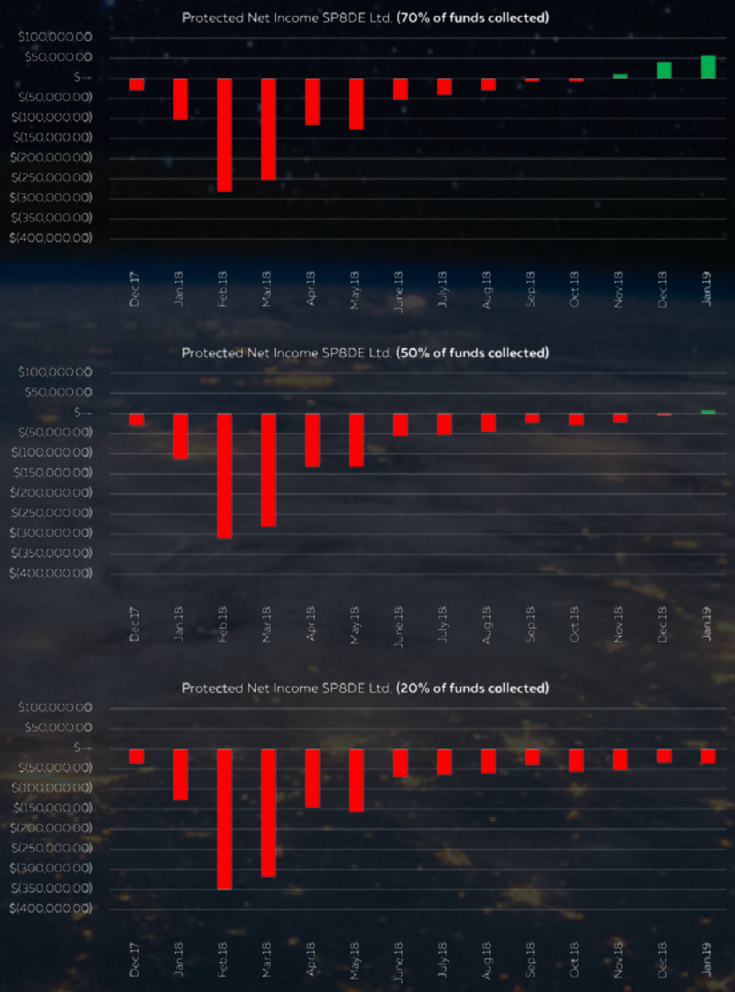


Figure 6 Scenarios of the projected net income of Sp8de in dependence with the amount collected during the Pre-Sale and the ICO

# References

1. EU gambling industry report by EGR Global can be found at: http://egr.global/wp-content/uploads/2017/02/001_EGRWhitePaper_2017.pdf

2. US gambling industry news at Best US Casinos: https://www.bestuscasinos.org/real-money/

3. Global gambling industry trends report: https://www.transparencymarketresearch.com/online-gambling-betting.html

4. Online Bitcoin casinos gambling: https://themerkle.com/bitcoin-casinos-recorded-us4000-worth-of-btc-being-wagered-every-minute-in-february-of-2017/

5. The top online casinos: http://markets.businessinsider.com/news/stocks/Global-Online-Gambling-Market-2017-2021-1002363954

6. Sfetcu (2014). Gaming in Online Casinos

7. Ethereum and casinos: https://cointelegraph.com/news/gaming-meets-ethereum-to-deliver-zero-house-edge-trust-to-online-casinos

8. Are online casinos rigged? https://www.casino.org/rigged-casino-guide/

9. Can blockchain technology improve online gambling transparency? http://www.osborneclarke.com/insights/can-blockchain-technology-improve-online-gambling-transparency/

10. Levine, Ross. “Finance and growth: theory and evidence.” Handbook of economic growth 1 (2005): 865-934.

11. Lucy Dewar, (2001) “Regulating Internet gambling: the net tightens on online casinos and bookmakers”, Aslib Proceedings, Vol. 53 Issue: 9, pp.353-367

12. Wood, Robert T., Robert J. Williams, and Paul K. Lawton. “Why do Internet gamblers prefer online versus land-based venues? Some preliminary findings and implications.” (2007).

13. Gainsbury Sally M. and Blaszczynski Alex. Gaming Law Review. September 2017, 21(7): 482-492. https://doi.org/10.1089/glr2.2017.2174

14. Can Ethereum casino games disrupt the online gaming industry? https://proofofsteak.com/can-ethereum-casino-games-disrupt-the-online-gaming-industry-ff36fa2bfa47

15. The average transaction cost of Ethereum: www.bitinfocharts.com

16. Bitcoin Washing and Casinos For High Rollers. http://structural-geology.org/bitcoin-casinos-and-cryptocurrency-laundering/

17. Using Bitcoin casinos to launder cash: https://www.casinopedia.org/news/the-mafias-latest-game-using-bitcoin-casinos-to-launder-cash

18. DAO. Casino white paper: https://github.com/DaoCasino/Whitepaper/blob/master/DAO.Casino%20WP.md

19. BitPoker white paper: http://www.bitpoker.io/pdf/White%20Paper_Bitpoker.pdf

20. Edgeless white paper: https://coss.io/documents/white-papers/edgeless.pdf

21. BitDice white paper: https://ico.bitdice.me/prospectus_en.pdf

22. FunFair technical and commercial white paper respectively: https://funfair.io/wp-content/uploads/2017/06/FunFair-Technical-White-Paper.pdf; https://funfair.io/wp-content/uploads/2017/06/FunFair-Commercial-White-Paper.pdf

23. Blum (1981) Coin flipping by Telephone: https://www.cs.cmu.edu/~mblum/research/pdf/coin/

24. About Cardano: Overview: https://whycardano.com/; Academic research: https://www.cardanohub.org/en/academic-papers/; All IOHK papers: https://iohk.io/research/papers/

# Appendix

The (partial) solution to the distributed randomness that is commonly used today was inspired by a problem posed and resolved by Blum in 1981: how can one ensure common uniformly distributed randomness in multiparty applications? [23] In other words: how can, say, two people being geographically distant and using only a phone, toss a coin and be sure that the outcome is fair? The answer on this question is quite technical (albeit intuitive) and is beyond the scope of this paper. The solution originally proposed by Bloom while being elegant, relies on the honest majority assumption. It is therefore susceptible to the 51% attack whereby an adversary can bias the output[5] or even prevent the honest parties from receiving any output at all.

By relying on Verifiable Secret Sharing (VSS) assuming an honest majority, random beacon is capable of providing a reliable source of good randomness and yet suffers from two main issues: firstly, the necessity of dealer-party interaction impedes scalability and secondly, only the actively participating parties can verify that the protocol was actually performed fairly (in the context of today's real-world, say blockchain, applications, this implies that off-line nodes, once online, cannot update their version of the chain in a trivial manner). The former issue can be resolved by applying non-interactive VSS, the latter, by using PVSS or Publicly Verifiable Secrete Sharing protocols. In the end, one needs to balance the scalability and security. While for the majority of applications the latter is preferred, for gambling applications where both, security and speed are important, it is less clear cut. The major issue with the PVSS lies in the way it handles the computational overhead: the number of computations required to verify n shares grows exponentially in n.

All about the scientific work carried out at Input-Output Hong Kong can be found in the URLs provided in [24].

[5] We deem, however, the possibility of the 51% attack negligible as is common in the blockchain applications.