SPL/T

A transparent Ethereum lottery platform which contributes to the growth of a cryptocurrency index fund.

Michael Somerville, Eric Somerville, Antonio Sou, Vadim Mansurov, Milan Stanojevic

Draft Version 0.1

March 2017

Overview

The blockchain has great potential to disrupt and improve a vast multitude of centralized services and organizations around the world. The crowd funding and lottery and gaming spaces are ones that will be upended by transparent trustless DApps running on the blockchain. We believe SPL/T has the capability to be major contributor to this coming improvement.

SPL/T will be a decentralized, transparent 80/20 draw. Users will purchase chances to win 80% of the total ticket sales while 20% of the funds, less the cost of maintenance and management will be invested by the company into an indexed cryptocurrency fund. 50% of the fund's growth in the market is then distributed to the SPL/T coin owners on a quarterly basis. Further profit could be realized through the setup of SPL/T multi draw platform allowing for other organizations seeking to raise capital to set up their own transparent draw. Profit from these draws would be applied to the SPL/T Fund.
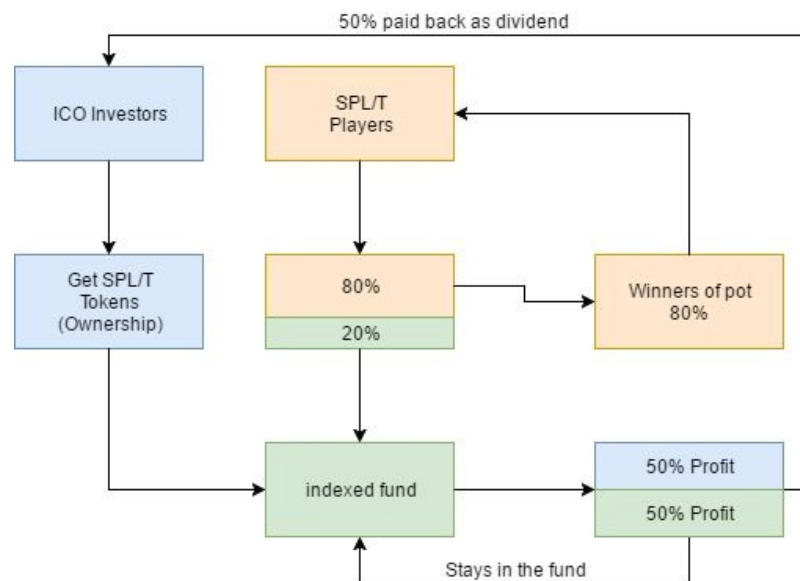
SPL/T Draw Breakdown

The concept for SPL/T is very simple. Sell a bunch of tickets each week. At the end of each week, select a user at random and award them 80% of the sales.

Ticket sales and paying out winnings are trivial with an Ethereum smart contract. The difficult part is randomly selecting a winner. This is difficult in an environment where we do not wish to necessarily trust the miners who execute the code for the Smart Contract.

Getting a Random Number

The concept for SPL/T is very simple. Sell a bunch of tickets each week. At the end of each week, select a user at random and award them 80% of the sales.

Ticket sales and paying out winnings are trivial with an Ethereum smart contract. The difficult part is randomly selecting a winner. This is difficult in an environment where you cannot necessarily trust the miners who execute the code for the Smart Contract.

Getting a Random Number

Our solution will use a future block hash from the Bitcoin Blockchain. There are many vulnerabilities with this, but SPL/T uses an approach to mitigate all points of abuse without relying on a central authority.

1. Using http://www.oraclize.it, we can query information for the required headers for that week
2. We use the first block hash after noon on Sunday to determine the winner by mapping the block hash to a ticket number
3. To prevent putting trust in Oraclize, we will verify the block hashes within the smart contract. We will evaluate 17 consecutive blocks, one before noon and 16 after noon

For example, block #462209 has a hash of:

00000000000000000504747c04b3ec42571d0a5be1dbbad8ec261c37860fd49

Which consists of 64 hex digits. Due to the **difficulty** of the blockchain, this hash will always have leading zeros. We will base our algorithm off the last 32 digits which will remain random for any foreseeable difficulty, and results in more than than $3x10^{38}$ possibilities. As a sense of scale, this is roughly all the bacteria cells on Earth, times a million.

We will sell the number of tickets equivalent to the value of 80% of 12.5 bitcoin, each ticket will cost 0.001 Ether. This means that the maximum pot will never surpass the value of a mined bitcoin, making it not worthwhile for Bitcoin miners to manipulate the system by discarding a Bitcoin block if the outcome for a SPL/T draw is unfavourable to them. (Discarding an unfavourable block will only give the miner another random draw at the SPL/T lottery, and doesn't guarantee a win).

Verifying the Source

SPL/T gets the Blockchain header information from Oraclize, but will verify the headers within the smart contract to eliminate the possibility of manipulation by Oraclize. The contract will verify the last block before noon on Sunday, and the first 16 blocks after noon on Sunday (for a total of 17 consecutive blocks). The first block after noon will be used to determine the winner.

In order for Oraclize to affect the outcome, they'll have to either:
● find a block hash with the exact same **Previous Hash** value as one of the legitimate blocks that day

- add 16 blocks to a legitimate block

There's no incentive for them to do this because they could put that work towards mining actual Bitcoins and get a higher return. The contract will verify the timestamp of each block header to ensure that it was created during that day, and ensure the difficulty is at least 500,000,000,000. Even if the difficulty doubles every 6 months, it will still not be worthwhile to manipulate a draw after 2 years. See the link below for difficulty trends.

https://blockchain.info/charts/difficulty?timespan=all

Picking the Winner

Each ticket will be assigned a range of winning sequences from the 32 hex digits. The $3x10^{38}$ possible values will be divided evenly among the tickets sold. Due to remainders, the early ticket purchasers may have 1 more sequence than the later ticket purchasers. This increases their probability of winning by 1 in $3x10^{38}$, which we deem negligible.

A new pot will automatically start at midnight on Monday, UTC time. Ticket sales will be allowed Monday through Saturday. Ticket sales will be rejected on Sunday, and the first block hash mined after noon that day will be used to determine the winner. This is a simple way to ensure that ticket sales do not overlap with any block hashes that are used in determining a winner.

Cost of Processing

Oraclize charges $0.01 per blockchain header retrieved, resulting in $0.17 per draw.
The Gas used for processing should be negligible for purchasing tickets. Retrieving and verifying the blockchain headers will be a heavier computation, but should also be negligible since this only needs to be carried out once per week.
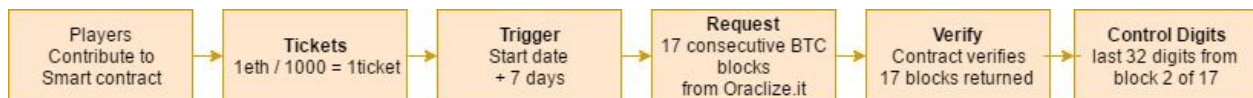
SPL/T Multi Draw Platform

After the successful development and launch of the SPL/T Draw a web portal will be developed allowing users to develop their own draw. Those looking to raise funds for projects, charitable causes or the like will have an easy to use interface which will allow them to launch a "50 50 type draw" wherein they will collect 30 percent of the contributions to the draw 20 percent of the contributions will flow to the SPL/T Fund and the remaining 50 go to the winner of the draw. The party generating the draw will be able to simply fill in description fields for who they are, their reason for raising funds, input the destination wallet and launch the draw page. By allowing users to generate separate draws, SPL/T will gain the promotional capability of their social networks and reach a much larger number of people. .

SPL/T Cryptocurrency Index Fund

Initially, funds portioned from the SPL/T Draw will be invested using Iconomi in the ICNX coin. Upon the release of a decentralized investment platform (i.e Melonport) funds will be moved to where our management team will oversee a portfolio of crypto assets. The portfolio will contain a balance of established entities in the crypto space and start up ICO's and DApps as identified by the management team.

SPL/T Fund Operating Costs

Prior to transfer to the fund, platform transaction costs are to be deducted from the SPL/T 20% earnings when contributing to the SPL/T fund. Additionally, operating costs of SPL/T Platform such as smart contract gas price, and fund management transaction costs will be deducted prior to deposit within the fund. When paying out the quarterly growth, the platform transaction costs will also be deducted.

Token Presale

The SPL/T token initial distribution will be in the form of a pre-sale. SPL/T will issue 100 million SPL/T tokens X days after the crowdfunding campaign successfully ends. SPL/T tokens represent a Proof-of-Membership in a fund which grants access to a share of 50% of fund growth quarterly, executed by an Ethereum smart contract. The remainder of the funds growth after fees are left in the fund, allowing the Net Asset Value (NAV) of a token to increase over time. SPL/T tokens also represent 100 % ownership of the SPL/T platform, which adds to the fund through its take on the 80/20 draw again increasing the value of the SPL/T token. SPL/T token ownership entitles its possessor to participate in SPL/T platform related voting.

The SPL/T token will have a hard cap that, when reached, will immediately disable additional sales. The cap will be measured in Ether and set in the token sale smart contract to a value approximately equal to $5 million USD based on the ETH/USD price at the start of the token sale. If $500 000 USD are not pledged by the end of the token sale, funds will be returned minus transaction fees.

Contributions will be held by a smart contract until end of the offering date or when maximum funds reached. At the end of the sale, SPL/T Token distribution will be 80% to the contributors of the ICO and the founding team will receive the additional 20% allocation of SPL/T Tokens. This founding team allocation is subject to a 24 month holding period. These tokens will serve as a long-term incentive for the SPL/T founding team.

Marketing Strategy

Initial marketing investment will focus most intensely on online cryptocurrency publications. These ads will target those who are invested and interested in the blockchain space. Further advertising will be done

throughout social media platforms targeting those with an interest in the online gambling sector in order to highlight the inherent advantages a blockchain based lottery has over the conventional online counterparts. Lastly, we will seek to promote the Multi Draw Platform to those who seek to raise funds online via crowd sourcing sites both in the cryptocurrency and traditional web space.(Weifund, Indigogo, KickStarter, GoFundMe)

ICO Fund Distribution

40% development of SPL/T platform
25% fund
15% marketing
15% legal
5% or capped at 52K for 1K a week early draw seed

ICO funds will be distributed as follows: 40% will be put towards the development and implementation of the SPL/T platform. 25% of the money raised will seed the index fund. 15% will go to the marketing of SPL/T to encourage the use of the 80/20 draw. 15% will be allocated for legal consultation to ensure SPL/T is compliant with the appropriate laws and regulations. 5% will be allocated to early draw seeding, this, however is capped at $52 000 USD to seed the draws with $1000 USD a week for the first year. If the cap is hit the remainder of the portion will be allocated to the fund.

Bonuses

Token Sale Bonuses

10% first 10 000eth

7.5% next 20 000eth

5% next 20 000 eth

2.5% next 20 000 eth

Roadmap

Concept Development

Technical Roundtable

White Paper Release

Launch ICO

Legal Compliance / Gaming License Acquired

Launch SPL/T

SPL/T Multi-Draw Platform Development