Victory Protocol

A protocol for running decentralized lottery games.

Lightpaper 0.1

November 21st, 2018

This document contains 10 pages.

Contents:

Why lottery?

Gambling is one of the oldest human activities. There are artifacts supporting this claim which are dated back to the Paleolithic period. Gambling houses were widespread in ancient China, dice from 3000 BC were found in areas belonging to Mesopotamia.

In recent times, we are seeing an extreme effort from governments to regulate, centralize, and even nationalize all aspects of gambling, especially lottery games. A notable example is Israel where most forms of gambling are illegal, but the state runs 2 national lottery games.

It should be obvious how the core principles of the blockchain can be applied to lottery:

- **Distributed Database** - since every party to the blockchain has access to the entire database and its history, there is no need for a central entity to provide control, regulation and oversight.
- **Peer-to-Peer Transmission** - by default, all nodes, wallets, and other parties have unlimited options to establish peer-to-peer relations - regardless of their physical location. Thus, participation cannot be subject to

artificial limitations such as geo-IP blocking or blocking on a national level of domain names, etc.

- **Irreversible Records** - which allows a proper blockchain to replace the need for licensing and technical oversight of the game operators.
- **Computational Logic** - all lottery games will run as smart contracts subject to core mathematical principles thus eliminating any human-centric "weak spots" in the design and implementation. Specifications are TBA after private testnet has been launched.

What is Victory Protocol?

Victory Protocol is designed with the objective of providing a blockchain platform for running decentralized games of chance which follow a predefined logic enforced by smart contracts.While the exact technical aspects of the protocol are still under final consideration and early development, these principles are considered corner-stone by the developers:

- **Scarcity**. The native currency of the blockchain will be deflationary by definition. It will be minted instantly at the start of the swap event and will have a finite number. Once all tokens are minted, there is no option for creating additional ones.
- **Consensus.** We have chosen to address the Byzantine generals' problem by implementing a DPoS consensus mechanism. While recognizing the obvious scalability issues, we believe that this disadvantage can be solved by electing a different number of delegates on each vote. The exact number will depend on factors such as network activity, median transaction size, etc.
- **Collateralization**. All game operators will be forced to lock assets before running a game of chance. Bad actors

will lose some or all collateral. Said collateral will be distributed fairly to all game participants who were exposed to the fraud attempt.

- **Inclusiveness**. The only requirement for interacting with the blockchain is ownership of its native currency. Everyone can participate without discrimination of any kind. Anonymization techniques will be implemented to prevent as many kinds of fencing as possible.
- **True Randomization**. It is paramount to declare and verify a method of true randomization, either by using advanced pseudo-generation or by harvesting sources of natural entropy. Having a viable randomization mechanism to which all dAPPs adhere is a cornerstone in running fair games of chance.
- **Immutable Reputation Records**. All game operators will be subjected to a rule-based ratings protocol and all historic events pertaining to this will be added to the blockchain thus allowing unrestricted access of all parties to all data.
- **Governance**. The team does not wish to retain creative control of the protocol and its implementation on the blockchain. While the team (or any other interested party) can suggest new protocol implementations, it will be up to the community (or token holders) to decide on

whether to accept or deny the proposal. For example, both a poker game and a lottery draw require interaction with a tamper-proof randomization generator. Thus, adding a poker dAPP to the blockchain will *not* require protocol modification. However, a dAPP running a game of chance using a different method (like utilizing atmospheric noise in different areas or measuring cosmic ray emission) will require a "hard-fork" of some kind. The given example is generic and does not encompass all possible protocol modifications.

Once a stable and self-sustaining mainnet is achieved, additional services can be implemented to the blockchain. A few examples would be:

- **DEX** - A DEX will allow for seamless exchange between LOTTO and major cryptocurrency/ FIAT pairings in a decentralized and anonymous environment.
- **Sidechains** - Sidechains can arbitrarily employ specific protocols as long as they are compatible in principle with Victory Protocol. For example, a draw game adheres to a logic which is different than that of a poker game.

- **Anonymized Interaction** - This can be achieved by deploying a TOR layer of protocol interraction on a node level.
- **Asset Tokenization** - Allowing games of chance to distribute physical goods to the winners.
- **Stand-alone wallets**. Initially, access to mainnet will be provided through a Metamask-esque browser extension which also serves as a wallet. Future development will undoubtedly allow for development of wallets as stand-alone applications for all OS. To prevent application congestion, one wallet will allow interaction with all games on the blockchain.

What is Victory Token (VIC)?

Victory Token (VIC) is an ERC-20 token which is crucial in the incoming swap for LOTTO. VIC has a total supply of 1 trillion. The team owns 10% of the total supply. 10% were sold to interested parties. Both the team and the investors' tokens are locked until mainnet launch. The remaining 80% of VIC will be airdropped to our community at several stages. Stage 1 was completed on 11/18.

Once mainnet is launched to the satisfaction of the team and the community, VIC will be swapped for LOTTO. After this event, VIC will lose all purpose or relation to the blockchain. Swap conditions are TBD and will be announced shortly before the event.

What is LOTTO?

LOTTO is the native currency of the blockchain. All blockchain interactions require the transaction and/ or burning LOTTO. LOTTO is designed with deflation in mind. The total supply of LOTTO is TBD. LOTTO will be divisible up to 18 decimal numbers.

The only way of acquiring LOTTO is by holding VIC at the time of the swap. We have chosen neither to pre-mint nor to pre-sell LOTTO. We believe that blockchain should not be wealth-centric and everyone should have equal opportunity at launch. Since acquiring VIC can be achieved simply by actively participating in our airdrops and community initiatives, there might be a ladder-system distribution during the swap event.

There are staking, locking, and burning mechanisms which will be applied to different use cases. Let's look at three examples.

Alice wants to take part in a lottery game on the blockchain. Since the protocol enforces the use of the native currency for blockchain interaction, Alice will need to acquire some LOTTO to place a bet. She can either receive some from a friend or purchase LOTTO from an exchange. Whenever Alice interacts with the blockchain, a percentage of the

transaction will be sent to a burn address and another percentage will be distributed amongst stakers.

Bob has enough LOTTO - much more than he wants to gamble. Bob has 2 options for generating passive income - he can stake his tokens (thus locking them and taking them out of circulation) or lend them to other players. Bob’s profit from staking or lending will be deducted with a burn amount and a staker’s fee.

Samar wants to run a game of chance. Samar will need to acquire enough LOTTO to deploy a smart contract on the blockchain and to provide a collateral for the game. Distributed profits will see, again, a 2-part deduction (as explained above).

--- The end ---