UltraYOLO

Decentralized Lottery Protocol and DAO using Proof-of-Randomness

Table of Contents

Abstract

UltraYOLO project is a decentralized lottery protocol built with blockchain technology. The primary mission for this project is to create a platform to manage and run the world's largest international lottery. Our project introduces Proof-of-Randomness (PoR), which solves the issue of random number generation and miner attacks that plague existing lottery and gaming applications. Our protocol will involve a masternode network to ensure Proof-of-Randomness and to manage the health of the network as a DAO.

As our project matures, the DAO governance model for YOLO token holders should advance to a state of self regulation. The DAO model provides the organizational structure needed to determine rules and regulations of the lottery. On a technical level, the YOLO token provides the utility to run our Proof-of-Randomness with a percentage of the lottery profits used as incentive for running the network.

Our ICO will seek to raise 10,000 ETH primarily to finance the initial jackpot, technology development, and marketing costs. Our tokens (YOLO) will be issued at a rate of approximately 200,000 YOLO : 1 ETH, pegging each YOLO token at approximately $0.005.

The primary utility of YOLO tokens will be to run the lottery and for the distribution of funds to relevant stakeholders. YOLO token holders who have masternodes will be able to receive a percentage of all weekly ticket sales in return for running the lottery system.

The main focus of the UltraYOLO team is to ensure that this project becomes the largest global lottery in both user base and jackpot size. Current work is prioritized with user acquisition and technological advances. We also strive to provide consistent updates and plan to actively engage the community.

Overview

In this whitepaper, we shall go over the existing implementations of lotteries, analyze them, and propose a better system - the UltraYOLO Lottery. The UltraYOLO project shall address the limitations of existing lotteries and suggest the superior alternative of a decentralized blockchain lottery with DAO governance and Proof-of-Randomness.

The UltraYOLO project is a standardized, programmable ecosystem to facilitate on-demand, secure, and global access to the lottery. UltraYOLO presents a novel approach to lottery ticket sales, winner selection, and transparency.

1 Current State of Lottery Ecosystem

"Innovation and disruption are similar in that they both bring forth creative change. However, disruption differs from innovation in that it causes radical change in the way we behave and how we think. It displaces the status quo by supplanting existing technologies, industries, markets, or services and replacing them with different, usually more efficient, effective, and faster ones. This can create havoc as the disruptor tends to bring down those existing technologies, industries, markets, and services by making them obsolete."

- World Lottery Association, 2017

According to the World Lottery Association (WLA), the lottery industry is growing year over year and expected to top 350 billion USD in 2018. Lottery analysts forecast that the global lottery market will see growth of over nine percent per annum until 2021. Their research points to a number of areas that allow for this expansion, including relaxed regulations, the digitization of current offerings, and by them taking advantage of mobile and social media channels. [1]

But are these areas of expansion simply ways to extend the reach of current offerings and what happens when the limits of this reach have already been hit? We believe that for lotteries to thrive, we need to get creative about the game, take advantage of technology in innovative and interesting ways, and tap into what we know about the new player mindset. We need to be brave and honest, to gain the respect of a new audience, and even to find ways to entrust players themselves with the power of decentralization. [2]

The crypto lottery community is especially interested with the large market of young people familiar with new technologies. Recent studies done by VICE media show a decrease of traditional lottery playing among millenials and a opportunity for a newer replacement to establish itself. [3] By 2020, Millennials are expected to control between $19 trillion to $24 trillion of the global economy, and 48% play a favorite game at least once a week – yet they tend not to play the lottery in its current form.[4] In addition, millennial cryptocurrency adoption rates are set to reach 33% by the end of 2018 and to continue growing. [5] The UltraYOLO project sees an opportunity here to modernize lotteries with cryptocurrency.

The primary challenges existing lotteries face are their lack of digital convenience, lack of social media engagement, and antiquated gaming mechanics as compared with more addicting mobile games.[6] The UltraYOLO team will take on these challenges and succeed. By doing so, we expect to take the first mover advantage and achieve market dominance for years to come.

The lottery system is ripe for disruption and we believe the UltraYOLO project is the solution.

2 Outstanding Lottery Projects

In this section, different types of lottery projects are explored and discussed in terms of their pros and cons. The main attempts in the crypto lottery space have been SmartBillions and TrueFlip. The UltraYOLO team has studied the existing lottery projects and is confident that our product is technically superior and our implementation better.

2.1 SmartBillions

Their project currently is the most advanced lottery on the Ethereum blockchain. Positioned as a smart contract rather than a company or organization, development largely depends on the advances of Ethereum. Current development has stalled due to high gas prices and there is no roadmap for the interim. An audit of their smart contract shows serious design flaws with the main one being their choice of RNG coming from the Ethereum blockhash. Finally, their entire project does raise some concerns from our team, the main one being security and user acquisition. The UltraYOLO project is confident that we will reach multi billion dollar jackpot status before they do. [7]

2.2 TrueFlip

This project is a centralized lottery service.The lottery uses the Bitcoin blockhash as a source of randomness. In this scenario, possible attack vectors can be created from bitcoin miners colluding to influence the blockhash if the jackpot lottery prize vastly outweighs the bitcoin mining reward. Glancing through the TrueFlip github repo, their code shows a very amateur attempt of they determine their lottery winners. To sum it up, their entire open source codebase consists of an ICO contract, and 2 python scripts that output a CSV for presumably manual payout distribution.[8]

2.3 Other Ethereum Lotteries

There have been many attempts by smaller developers to create an ethereum lottery. However most attempts will ultimately fail for the following reasons: High gas costs and insufficient proof of randomness. [9,10,11]

	UltraYOLO	SmartBillions	True Flip	PowerBall
Structure	Decentralized	Decentralized	Centralized	Centralized
RNG Method	Proof-of-Randomness	Block Hash	Block Hash	Physical
Blockchain	UltraYOLO	Ethereum	Centralized	None
Jackpot Odds	1 : 2 985 984	1 : 16 777 216	1 : 49 578 984	1 : 292 201 338
House Edge	11.05%	13.85%	21.28%	>50%
Number Range	0-11	0-15	1-49 and 1-26	1-68 and 1-26

3 UltraYOLO Protocol Design Principles

The project team and community behind UltraYOLO project share a vision where the lottery industry will be decentralized and censorship-resistant. The following are the characteristics that the team believes an ideal lottery should exemplify from a technical standpoint:

3.1 Randomness

This is arguably the most important aspect for a successful lottery system. The UltraYOLO team defines randomness in **TWO** main aspects:

1. There needs to be enough **entropy** in the random number generated (RNG). The lottery result has to be random enough, not controlled by a single entity, and not predictable in any way.
2. The generated random number has to be **tamper-proof**. No party or middleman should be able to manipulate the random result of the lottery shift the odds in their favor.

Achieving this level of randomness is no small technical feat, and this is a huge flaw in most of the existing blockchain lottery implementations. We go more in depth in the following section on how our team will tackle this problem at a fundamental level by implementing Proof-of-Randomness.

3.2 Low Fees

Transaction fees are one of the largest roadblocks to wide adoption of blockchain technology. The Bitcoin network is plagued by high fees. Currently, as of January 2018, the fees associated with getting a transaction in the next Bitcoin block have been as high as $18. [12] These type of high fees have detracted Bitcoin from its original vision of being a "*A Peer-to-Peer Electronic Cash System*" [13] , even though PoW model has made Bitcoin a great store of monetary value, any lottery or gaming protocol cannot compromise with respect to high transaction fees. Such problems also exist in Ethereum, especially after the introduction of CryptoKitties. Arguably, the first widely used dApp, it sent the average fees of an Ethereum transaction skyrocketing from less than 0.50 USD to more than 4.00 USD [14] . As the *SteemIt* whitepaper best put it: "*Regardless of how rational the argument for the necessity of fees, users still hate the experience of being nickeled and dimed for everything that they do*" [15] . The most widely adopted lottery game needs to be able to process lottery tickets at a low price, with minimal to no transaction fees. The UltraYOLO project will ensure that there will be minimal to no transaction fees for lottery ticket purchases.

3.3 Anonymity

Part of the UltraYOLO lottery vision is privacy. Lucky winners of the lottery should be able to stay anonymous. A current issue many lottery winners face is that the sudden influx of money attracts unwanted attention. Our proposed solution is to introduce privacy measures to obfuscate jackpot transactions via a privacy algorithm "*you can verify the correctness of computations without having to execute them and you will not even learn what was executed*". [16] The lottery buying process and the payout distribution process should be fully anonymous much like payments in the popular privacy coins: *Monero* and *ZCash*.

3.4 Network Speed

Speed of confirmations will be increasingly important as UltraYOLO becomes more and more widely adopted. It is easier for a given network to have fast confirmations when there are few transactions. Much like the case for Ethereum and CryptoKitties, transaction speed drastically decreases when network burden increases. For UltraYOLO to become world's largest gaming/lottery system and be adopted by gaming establishments such as casinos, the network needs to be able to handle large sustained loads and large bursts of traffic.

Imagine a person buying a lottery ticket at a gas station or playing gambling game in a casino, he/she would want to know that their bet has been placed immediately upon their decision to purchase. How the team plans to handle transaction speed will also be addressed in sections below.

Low-fees, anonymity, randomness, and speed are the main technical challenges the UltraYOLO team seeks to address. The UltraYOLO project will also include features such as miner rewards (incentivising supporters of the project) and blockchain gaming protocols interactions (atomic swaps) in the mainnet release. Our focus on the technology is what sets the UltraYOLO project apart from other crypto lottery projects.

4 UltraYOLO Blockchain Architecture

4.1 UltraYOLO Network & Masternodes

The UltraYOLO network will consists of two types of nodes: light nodes and masternodes. Light nodes are the ones who make YOLO coin transactions such as buying the lottery ticket or simply sending coins to one another as a transfer of value. All of the transactions and random number generation will in turn be supported by the masternode network. In order to become a masternode, users will need to stake at least 200,000 YOLO tokens in the provided wallet client and register in the network. Note, the "masternodes" are much cheaper ($1000 with ICO price) than other given masternode system such as Dash and ZCoin. The UltraYOLO vision is to be a decentralized system with low barriers to entry. The masternodes provide two functionalities: verifying transactions on the network and generating random numbers. The technology that this mechanism depends on is called *"BLS Threshold Relay"*, first published by Boneh, Lynn, and Shacham *(BLS)*, professors from Stanford University. [17] BLS promises the signature scheme of each block also generates a random number that is completely unpredictable and verifiable. The masternode architecture will give UltraYOLO blockchain a fast block-time of 5 seconds per block since the masternodes are pre-selected and signature generation scheme will be quick.

4.2 Random Number Generation (RNG)

The Random Number Generation (RNG) Scheme is the most important aspect to a lottery protocol. After thoroughly comparing different random generating schemes, the UltraYOLO team has chosen the BLS threshold scheme as opposed to blockhash, oracles, or state (fate) channels type RNG schemes. A more comprehensive comparison will be given in the technical white paper. On a high level, using blockhash as a source of randomness popularized by

SmartBillions (Ethereum blockhash) and TrueFlip (Bitcoin blockhash), is the worst type of RNG scheme since they are very prone to miners colluding with one another if the lottery pot (or bet amount) becomes larger than the miner rewards. Oracles too can be very centralized, such as the Oraclize library. Finally, state (fate) channels, popularized by the FunFair project, are good for frequent microtransactions (such as the Bitcoin lightning network) between two parties since all transactions only require two on-chain transactions (one pledge transaction and one final state settlement transaction). If the two parties, however, only make one single transaction for example play one single game, the state channel is actually more costly. The BLS threshold signature scheme has a clear advantage in all regards is a clear winner in terms of randomness and being tamper-proof.

4.3 Proof-of-Randomness

"Random numbers should not be generated with a method chosen at random"

- Donald Knuth

Proof-of-Randomness comes from when all the a selected node group sign a given block and that signature is a deterministic and random number. This is pairing-based signature scheme is similar to the wide adopted RSA signature scheme. In RSA, there is a public key corresponding to a private key, blocks are signed by the miner's private key and verified using the miner's public key. In BLS signature, instead of a single private and public key pair, a group of private and public *key pair shares*, and each private key share can produce a *signature share.* If enough signature shares are collected, meaning enough nodes of the group validated on the block, the signature shares produce a collective signature that is publicly verifiable by the public key, grouped by the public key shares.
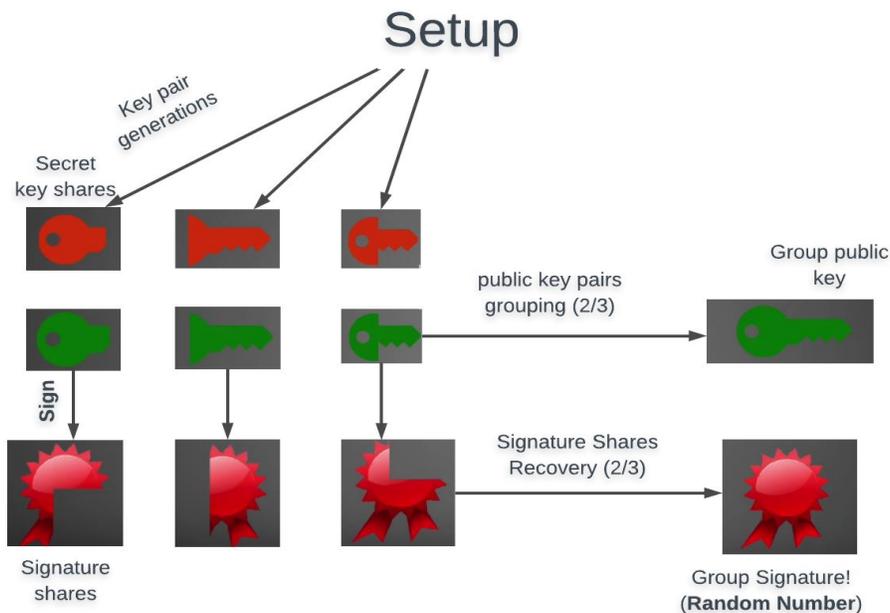
The collective signature is:

- **Unique and Deterministic**: A group of miners is identified by its threshold public key. The example in the chart uses a group of 3 nodes and if 2 is the threshold, any given 2 nodes will produce the same signature, which is a random number. Note this is for illustration - In reality, numbers will be more like group of 400 nodes with threshold of 200.

- **Publicly Verifiable**: The resulting signature can be validated by anyone who has the group's public key and block data. And that guarantees the group has reached the consensus and the random number was never tampered with.

The BLS Threshold Signature is the crown jewel when it comes to generating random numbers on the blockchain - every other RNG scheme fail in comparison. Fortunately, it has been proven through rigorous research by Stanford University [17] and an open-source implementation has been done by the Dfinity team. [18] The mathematical portion of BLS signature scheme will be explored more in depth in the technical white paper.

The UltraYolo team sees this innovation as a huge step forward in terms of blockchain technology.

4.4 Proof-of-Randomness vs Proof-of-Work vs Proof-of-Stake
This section will dive a bit deeper into how Proof-of-Randomness (PoR) with masternoding compares to other types of consensus protocols: Proof-of-Work (PoW), Proof-of-Stake (PoS).

PoW, first popularized by the Bitcoin blockchain, is the most familiar to the crypto community. A math puzzle and a race condition are generated for all the miners in the network to solve. The biggest problem with PoW is its wastefulness of resources. As quoted, *"Bitcoin could consume as much electricity as Denmark by 2020"*. [19] Besides this, PoW is said to have many other types of problems like selfish-mining, where a miner or miner-pool does not publish the valid solution in order to maintain a lead on the rest of the network.

PoS, first adopted by NXT blockchain and Peercoin Blockchain, and soon on Ethereum Casper, effectively solves these problems by pre-selecting miners based on the amount of stake they have in the network. Pre-selection of validators results in PoS being much faster than PoW. However, PoS also comes with it own problems such as the Nothing-at-Stake issue. The current incentive structure of PoS can promote bad behavior where validators sign each and every fork, since it reduces risk and there is no downside not to. On top of that, PoS does not have random number support built into the system.

PoR is designed natively as a lottery protocol, where random numbers are already integrated at the protocol level. PoR can be thought of as PoS with masternodes participating as validators of the blockchain in addition to the generator of random numbers.

	Proof-of-Work	Proof-of-Stake	Proof-of-Randomness
Fast Transactions	✗	✓	✓
Low-cost Transactions	✗	✓	✓
Built-in Random-Number-Generation	✗	✗	✓

PoW vs PoS vs PoR

4.5 YOLO Game Engine - An Autonomous Execution Environment

Previously, we discussed a reliable and fast source of random number generation guaranteed by BLS and a highly scalable blockchain guaranteed by masternodes. Now, we will introduce the YOLO Game Engine which is an escrow-like smart contract environment for trustless reward distribution.

At first, a smart contract platform will be utilized: Ethereum, being the most mature and functional smart contract platform to date, will be used for our proof of concept.

Here's exactly how it works:
After lottery tickets are purchased from the *ultrayolo.com* site, they (ticket number and player's wallet address) will be registered on the escrow contract in Ethereum until the lucky numbers for the week are revealed. After the lottery result is revealed, the escrow contract will be automatically invoked and rewards distributed to the winning wallet address stored on the contract. This contract will be publicly auditable by the entire UltraYOLO community. High gas prices and transaction fees will be mitigated by submitting lottery tickets in batches instead of one by one at no extra cost to lottery players.

Ethereum smart contracts will be a sufficient implementation for the initial lottery implementation, but the UltraYOLO team has far grander visions. Our team envisions a custom and dedicated smart-contract-like platform that natively integrates with the YOLO blockchain where multiple lottery and casino games can be hosted. EVM (Ethereum Virtual Machine) and other smart contract platforms (EOS, NEO) will be referenced for this task. This will become the ultimate game engine. It is designed to be fairly simple and light-weight for use specifically with games of chance. Developers and game designers will be able to use the YOLO Game Engine in their own projects. This will be further down the UltraYOLO development roadmap and will complete the UltraYOLO ecosystem.

4.6 Security Best Practices

"Code is Law" is a principle made popular by the Ethereum ecosystem. This paradigm states that smart contracts, once deployed to the Ethereum platform, are 100% final. There are designs to allow contract modification, but for the most part, contracts are an immutable self executing entity. That has led to multiple catastrophes in the past, such as the DAO hack, SmartBillions hack, and the Parity Wallet hack. UltraYOLO acknowledges that running the world's largest lottery will come with the responsibility of securing a huge jackpot and the team is well adept and prepared to take on the security challenges:

- **Blockchain Security Auditing**

This security of the UltraYOLO will come in two parts. First, the mathematically proven BLS signature scheme will guarantee the integrity of the blockchain. As described above, BLS signature scheme lacks the flaws that PoW (self-mining) or PoS (nothing-at-stake) do. In this aspect, our project will be a more secure blockchain with more advanced technology than the majority of outstanding blockchains. Second, the UltraYOLO blockchain will be governed and secured by masternodes and the UltraYOLO DAO. The weekly lottery outcome and fund distribution will be allocated (charities, social causes) and decided by the DAO. No single entity will be able to predict and tamper with the results.

- **Contract Security Auditing**

Both the ICO and gaming smart contracts will be heavily audited by authoritative agencies to ensure there are no loopholes and possible hacks like the DAO and SmartBillions contracts. UltraYOLO is blessed with a strong development team and all pieces of the contract will be modularized and easily testable, in contrary to the SmartBillions contract which is a monolithic contract prone to hacks.

- **Jackpot Cold Storage and Multi-Signature**

Due to the size of the UltraYOLO jackpot, the team has decided to err on the side of caution. Cold storage and Multi-Signature have proven to be very secure for storing large sums of funds. The UltraYOLO project will take on this approach to storing the jackpot when not in distribution mode. Only through consensus of the masternode network and DAO will jackpot funds be deposited or withdrawn from cold storage.

5.7 Development Vision

After the UltraYOLO masternode blockchain is deployed, the random number generation and 5-second block time will be huge assets for the gaming industry as a whole. Applications can be extended to games that require a random number: dice games, slot machines, etc. This type of integration will be even easier after the game engine is deployed and developers can roll out games natively. The UltraYOLO team has a grand vision of having partnerships with online games and even real-world casinos around the world and really become the "digital poker chips" of the blockchain era. The team chose the first application to be lottery since of its immediate possible impact and wide user adoption.

5 Decentralization and UltraYOLO DAO

The current governing body, the World Lottery Association (WLA) is an archaic organization that can be modernized with blockchain technology. Our project seeks to implement their structure in a decentralized manner. The purpose of the DAO will be to ensure the randomness of the lottery via our Proof of Randomness and to set industry standards for a decentralized crypto lottery. A large portion of our research will be to construct the technical infrastructure needed to build up a suitable DAO. For membership in the DAO, one only needs to control YOLO tokens, with more weight given to those with larger stakes.

Outline of the Online Gaming Regulatory Framework and relevant Industry Standards

Body / Entity	Document Type	Purpose	Examples
Regulatory Framework			
Legislature within the Gaming Jurisdiction	Gaming Law	Enables gaming activity Defines public policy Established the regulatory body	Gambling Control Act
Regulatory Body of the Gaming Jurisdiction	Gaming Regulations	Establishes the public policy framework	Lottery/ Online Gaming Regulations
	Technical Gaming Standards	Defines the requirements and specifications for a technical gaming solution, which if followed, ensure compliance with the regulations	Terminal, Gaming Device and Gaming Software Technical Specifications e.g. Alderney Standards and customized derivatives e.g. TGS5
	Minimum Internal Control Standards	Defines requirements for operational procedures which, if followed, ensure compliance with the regulations	Minimum Control Standards Internal Control Frameworks

6 YOLO Token Economics

6.1 Native Blockchain Token

YOLO token is the native token to the UltraYOLO blockchain. YOLO token will be first distributed as an ERC-20 token on the Ethereum blockchain, and will be ported over once the new blockchain is live. Users will be able to redeem the new YOLO coin using their ERC-20 tokens. This operation is much like the EOS token redemption process or any other blockchain that had their Initial Token Generation event on Ethereum. A more detailed description on the token transfer process will be published prior to the redemption date.

6.2 Total Supply

YOLO token will have a total supply of **4,000,000,000 tokens**

6.3 Initial Circulating Supply

YOLO token will have a Initial circulating supply of **2,000,000,000 tokens**

6.4 ICO Token Price

Initial token price target will be **$0.005**

6.5 Reserved Tokens

The 2 billion reserved tokens will be used for masternode rewards, airdrops and promotional events, bounty programs and even jackpot increases.

6.6 Exchanges

One core aspect of the UltraYOLO project is to build adoption of the lottery and our protocol. We see getting on the top exchanges as the best way to approach that. From our preliminary discussions with the exchanges, we will need to allocate funds to get listed. Below is the following roadmap on which exchanges we plan on listing first. We will start with the decentralized exchanges (DEX) and slowly move up to the larger ones, with the goal of listing on the top exchange, Binance. This will be a continuous process.

- **Decentralized Exchanges** - Immediately after crowdsale ends.
    - EtherDelta; RadarRelay
- **Low Volume Exchanges** - Within the first month of ICO completion
    - HitBTC; Coinexchange; Cryptopia; Mercatox
- **Asian Exchanges**
    - OKEX; Bibox; Huobi
- **Top Volume Exchanges**
    - Kucoin; Bittrex; Binance

7 Masternode Rewards

7.1 Masternode Setup

The masternode setup will be very easy. Users will simply need to download the provided wallet on Mac, Windows, or Linux and stake a deposit of at least 200,000 YOLO tokens. A VPS or server will then be needed to configured to send connect to the network and perform the masternode tasks. Our masternodes are inspired by DASH and should follow a similar setup.

7.3 Number of Masternodes

Given the numbers of tokens allocated during ICO and the masternode price of $1,000 it is estimated there will be between 2,500 to 5,000 masternodes in the UltraYOLO network

7.2 Masternode Rewards

Masternode rewards will be paid out on a weekly basis after the weekly lottery concludes. Masternode rewards will be 10% of the lottery proceeds of a given week. For example, if the lottery jackpot pays out a $2M in a given week, and 2,500 nodes are in the network, this would translate to $80 per node per week. In a given year, a node investment of $1,000 will generate a masternode reward of $4,160 at ICO price levels. At the time this paper's publication, the yield

would conservatively put YOLO token as a top 10 coin on the masternodes.pro.[20] This incentive should build a community of early masternode adopters for the UltraYOLO project[1].

8 Initial Lottery Mechanics

8.1 Lottery Tickets
Lottery tickets will consist of 6 digits each ranging from '1-12'. Each slot will have 12 possible options, with a grand total of 12^6 permutations. This is approximately 3 million total possible tickets and each ticket will be priced initially at 200 YOLO tokens (~ $1)

8.2 Lottery Design
The UltraYOLO lottery has the goal to be the most widely adopted lottery, and the initial lottery parameters favor a higher winning percentage at the cost of a smaller jackpot in order to build a consistent player base. The prizes range from **$4 - $1M** and each ticket has almost a **20%** chance of winning. An initial investment of $1 is likely to turn into $4 or even $1 million.

Suppose in a given week, the winning lottery number is: 1-8-3-8-7-12
- If a ticket matches all 6 digits, this means a lucky user purchased the ticket **1-8-3-8-7-12**, and is now a the lucky winner of the **$1M** grand prize.
- If a ticket matches 5 out of the 6 digits, e.g the ticket is: **1-8-3-8-2-12**, the player will receive a prize of **$5,000**
- If a ticket matches 4 out of the 6 digits, e.g **1-8-6-4-7-12**, he will receive a prize of **$100**
- Winners will receive prizes all the way down to 2 out of the 6 digit matches.

Ticket Number Hit	Win Odds 1 to:	Prize Value
6 out of 6	2,985,984	**$1M**
5 out of 6	45,242	$5,000
4 out of 6	1,645.4	$100
3 out of 6	112.1	$10
2 out of 6	13.6	$4

One good aspect about this lottery scheme is that the win odds are high. A given ticket has a **8.31%** chance of winning a substantial prize. These odds are much better than existing lotteries and should generate a large user base of interested players.

---

[1] Exact ROI number might fluctuate based on exactly weekly proceeds of lottery and number of masternodes in system. Numbers given here are based on $2M lottery proceeds and 2,500 masternodes

8.3 Future Lottery Designs

Our initial lottery design was designed to create as much winners as possible to build a reputation of fast and reputable payouts. Later editions of the lottery will provide a modified scheme with optimized parameters and a larger jackpot. For example, the next lottery in design will be a more traditional 6/49 lottery and will push for a large jackpot once the user base has been established.

8.4 Payout Schedule

To preserve the size of the jackpot and a stable token supply, UltraYOLO will distribute the top 3 largest prizes in installments. The lucky grand-prize winner will receive his $1 million in 50 weekly payments of $20,000, so after a lucky winner hits the grand prize, the winner will receive $20,000 for 50 weeks. The $5,000 prize will be distributed in 10 installments of $500. And the $100 prize will be distributed in 5 installments of $20. Distributing the prizes in this fashion will keep the lottery jackpot stable. Payouts will be pegged at the price of winning and in YOLO tokens.

In the situation that there are multiple winners, the payouts will be divided accordingly.

9 ICO Mechanics

9.1 Presale

To encourage early adopters, UltraYOLO is distributing 200 million YOLO tokens (10% of circulation supply) in a presale. In order to participate, **supporters are required to register on the official site**. Participants will be rewarded with a **bonus of 25%**, and **35%** if put in a larger amount. The presale is planned to take place on Feb. 1st, 2018 for the duration one week or until the 200 million tokens are sold out. **Only ETH will be accepted in this presale round.**

9.2 Public Sale

A public sale will be conducted shortly following the presale in Feb. 2018, with exact dates to be announced. The remaining circulation supply of 1800 million YOLO tokens will be distributed at a rate of $0.005 per token. There will be discounts for early participants in as well going down linearly as sales goes on. There will be exact details announced on a later date. Participants in this round will be required to register on the official site as well. The currencies accepted in this round will include: ETH, BTC, LTC and XLM to tailor to a wider public. Participants will need to provide an ERC-20 compatible wallet address if participating in currencies other than ETH.

9.3 Token Distribution

All YOLO tokens from the ICO will be distributed immediately after the public sale concludes, and will be tradable on EtherDelta, after which point team will be actively working on subsequent exchange listings.

10 Token Proceeds Utilization

40% Initial lottery bankroll
10% Reserve lottery bankroll

25% Marketing costs
25% Development costs

The structure above is designed for the long term success of the UltraYOLO project. Our main assets will be our technology and brand.

Our marketing efforts are primarily geared towards user acquisition costs in converting long term lottery buyers away from existing lotteries.

11 Bounty Program & Airdrops

10.1 Bounty Program

UltraYOLO team members are strong proponents on building a community behind this project. Planned bounty projects will include whitepaper translations and marketing support. Team is also planning an official meme contest and video for this project to spread awareness and generate hype. UltraYOLO team will allocate a total of **5% of overall YOLO tokens** to participants of the bounty program. Further details will be posted on the official site and ANN post on bitcointalk.

9.2 Airdrop
As periodic promotional events to the lottery, airdrops will be conducted to Ethereum address with a non-zero ETH balance and non-zero YOLO token balance or address who has participated in the lottery in the past. Users who receives the airdrops are encouraged to participate in the weekly lottery drawing and try their luck! Total of **5% of overall YOLO tokens** will be reserved for airdrops. Further details about the airdrops will be posted later.

12 Utility Mechanics

With the original intention of the lottery to generate funds to support social causes such as education and healthcare, the UltraYOLO project plans to do the same. Each YOLO token shall be a beneficiary of lottery proceeds. The intention being that a charity and for the YOLO token holder to donate at their own discretion. Further developments may amend allocations and technical specifications of the YOLO utility token.

Initial Utility Token Mechanics:
The YOLO token will have following properties:
1. Each YOLO token shall receive a percentage of jackpot earnings.
2. There will be both a universal allocation and an individual allocation based on the amount of YOLO tokens held.
3. The intention of YOLO token holders is that they should fund social organizations that have the intent of improving society.

Example groups and organizations to fund, examples taken from the Bitcoin Pineapple Fund [21]:
1. Watsi Project
2. The Water Project
3. Electronic Frontier Foundation (EFF)
4. OpenBSD
5. MAPs

Additional organizations can be added via future DAO proposals.

As the DAO governance gets developed, our vision is to have token holders vote on rules and regulations of the lottery. Separate proposals shall be provided to decide on lottery standards, jurisdiction and governance.

The regulatory framework and legal structure for the operation of the UltraYOLO project should be based on the lottery's conducting, managing and operating Internet or online gaming in accordance with the requirements of the laws within their respective jurisdiction, with the lottery incorporating best practices from around the world to ensure that the lottery's online gaming solution has a strong focus on responsible gaming, player protection, security of transactions and data privacy.

Planned issues of discussion and regulation depend will cover topics such as:
*   Legal regulations
*   Privacy concerns and procedures
*   Responsible gaming
*   Marketing procedures

13 Community Development

One of the largest challenges our project sees in the near term future will be user adoption. We are focused on Metcalfe's Law, which states that the value of a network is proportional to the number of users. Until our project becomes a global phenomena, we will focus on growth - How can we increase our Daily Active Users (DAU)

Our strategy is as follows:
1. Community Organic growth

2. Meme and Cultural development
3. Affiliate Program

Our affiliate model is based on the following principles:
1. We will provide the simplest user flow and the required resources to increase Conversion rates for our affiliates. Web, mobile, and offline methods
2. Lucrative initial commission structure for affiliates to build the brand.
3. A separate structure will be generated for affiliates to sell and register sub affiliates.
4. Multi sig wallet with the affiliate and the ticket sale to ensure veracity of sale.

Example Affiliate Commission Structure of Ticket Sales
1. 10% of the ticket sale will go to the affiliate
2. 90% of the ticket sale will go to the jackpot

In addition, 1% of all the lottery winnings will go to the affiliate.

Additional stipulations will be added to ensure genuine ticket sales. Our team will be actively working to determine the right affiliate incentive structures to prevent fraud.

By giving our affiliates the creativity to market our lottery, we hope to build up the network effects and brand ourselves in the largest global lottery on the blockchain.

14 Brand Development

The UltraYOLO project strongly believes in developing a high quality brand. Our philosophy and ultimate goal is to gain as many users as fast as possible to follow Metcalfe's Law of network effects. To achieve mass level adoptions, we are focused on user acquisition, lifetime value optimization, and brand marketing.

Our current marketing and brand philosophy is as follows:
- **Virality**: Our vision is to build the first truly global lottery. To achieve that goal, we strongly push for virality. Some may describe this as 'meme' potential. Following the success of Dogecoin and Pepecash from a virality point of view, our project hopes to achieve a portion of that level of success, at least in the initial stages.
- **Rebranding Possibility**: The current iteration of the UltraYOLO project is at its primary stages. At the point of more mainstream adoption, we will strongly consider rebranding. Similar projects we have seen that have done well after a rebrand is 'NEO', formerly known as Antshares. Another example is 'Dark Coin', now known as Dash. Both NEO and Dash are top 15 cryptocurrencies by market cap. We are not against a rebrand and view it as more the evolution of the product as it matures. Depending on how the project progress and the community feedback, we may take on a more professional name such as 'World Lottery DAO'.

15 Lottery Design and Mathematics

The UltraYOLO project will begin with a simple 6 ball draw lottery. Considerations for future lottery design will be taken from academic literature and optimized based on existing player statistics. Future modifications of the structure can be decided on via DAO governance.

From the "Handbook of Sports and Lottery Markets" (2008) [22] :

> Usually, a certain share, s_n, of the total prize money is reserved for the jackpot prize [claimed by the winner(s) who have "matched" all of the n numbered balls that are drawn from the N that are available] and the rest is allocated into separate prize pools, in predetermined shares s_{n-1}, s_{n-2}, and so on, to those who match n − 1, n − 2, and so on, balls. N and n determine the probabilities, p_n, p_{n-1}, and so on, of winning the n-ball, n − 1-ball, and so on, prize pools.
>
> The essence of our analysis is based on exploiting the variation in the shape of the prize distribution to explain sales variation over time.
>
> Lotto prize distributions are highly left skewed because almost all players lose their stakes, with a small proportion winning small prizes, and a very small proportion winning very large prizes. But when a rollover occurs, the size of the largest prize rises and so the degree of left skewness falls because the largest prize suddenly got larger.

The prize distribution shape is a factor that our team will be monitoring and developing. Existing crypto lottery projects are quite amateurish in design and disregard factors that sustain long term growth. Variables such as "Jackpot Fatigue" and "Cohort Segmentation" will be analyzed for further optimizations. [23]

Another factor for consideration will be finding the right parameters in the lottery design. Given that the cryptocurrency lotteries are in their infancy and player behavior is skewed towards risk takers, we will be actively measuring playing behavior to design the most optimal lottery.

As this project progresses, we will be dedicating more research into the effects of cryptocurrencies and lotteries.

16 Legal

Our team is currently in talks with our lawyers on the process of obtaining a online gambling license. Our excellent legal counsel is looking into ways to obtain license in offshore jurisdictions, as well as conduct any necessary research and other legal and compliance work that is required by a jurisdictional gambling control board. Current locations of interests are

Gibraltar, Isle of Man, or Malta. Licensing should be available by the time the lottery gains mainstream adoption.

Regarding the legal structure of this project, we are in the process of working through them and have been advised to withhold further statements until finalized by our legal team.

17 Project Roadmap

The project will have the following stages:

Lead Stage
- Distribute tokens
- Getting on initial exchanges such as Etherdelta
- V0 product with live lottery game on the Ethereum network with "V0 Proof-of-Randomness" and "V0 Masternodes"

Bronze Stage
- Developing the mainnet with Proof-of-Randomness
- Native Wallet Released with Masternode functionality enabled
- The initial community will be built and the markets for our coin will grow as we get on exchanges

Silver Stage
- Grow user adoption! We will be analyzing the how effective our customer acquisition is and will scale accordingly. This will be the main growth phase!
- Mobile apps. Offline cash methods. Affiliate distributors. User experience will be kept at the highest levels and designs will be sleek.

Gold Stage
- Sustainable levels of player base with the lottery running smoothly and at scale.
- The DAO will be refined a manner which would build a solid organization to maintain and grow the lottery

Important Dates
- Feb 9, 2018 : Pre-ICO Stage
- Feb, 2018: Prototype live
- March, 2018 : ICO Stage
- Q2, 2018 : Token appears on Exchanges
- Q3, 2018 : ERC-20 Token converts to Native Blockchain
- Q4, 2018 : Wallet Released and Masternodes live
- Q4, 2018 : Gambling license
- Jan, 2019 : Initial Lottery in alpha

- Q1, 2019 : Silver Stage begins. Focus on user acquisition
- Q1, 2020 : Gold Stage begins.

18 Team

We believe that our project stands up to scrutiny on both a technical and business level. We are confident that our vision of creating the world's largest decentralized lottery and new random protocol stands on its own regardless of how many ex-Google/Facebook/Amazon devs or how many ex-CEOs/PhDs/Vitaliks we have on our team. In the spirit of Satoshi Nakamoto and the cryptographic community, we would like to build a project that is greater than us and can evolve via the community. Thus the UltraYOLO project has decided to remain anonymous.

To give a better sense of the core team, we are a group of experienced technology professionals and academics from Silicon Valley and have esteemed professional reputations. We are a group of some of the brightest and innovative members of the cryptographic community. Most people in our positions would actually go the VC route by setting up a meeting on Sand Hill Road and undergo a Series A private sale consisting of multimillion dollar term sheets. However our team believes in the core democratic principles of equal opportunity participation. Thus the UltraYOLO project was born.

On the development side, our core lead has high level experience managing large codebases and is quickly becoming a top developer in blockchain technologies. We are actively developing in solidity and currently exploring alternate blockchains/technologies. Current focus has been rolling out our own blockchain, developing on top of Ethereum, and developing our Proof-of-Randomness algorithm.

On the business side, we have expert experience in marketing and user acquisition. We see adoption as our number 1 priority. With years of experience managing teams, the UltraYOLO project will be effectively managed with lean startup methodologies and rapid iterations. Many projects in the space have quite low quality teams by our standards and we see too many projects of questionable quality. Our team believes in having a strict integrity standard and hopes to build a reputation of trust.

Core Values

Responsibility
> The highest standards of community and social responsibility

Integrity
> Transparency and accountability

Professionalism
> Excellence in service to our members, to all stakeholders and in our performance

Innovation and Creativity

From an organizational standpoint, our vision of building a DAO involves building a community and should rely as little as possible on a centralized committee. The core members of the UltraYOLO project will work on developing the proper governance of lottery and the DAO.

After our ICO, we plan to expand the team. Main hires will be focused on development and QA of our protocol. In addition, we will be looking for additional statisticians/econometricians to manage and optimize lottery metrics.

Finally, we understand that many reading this may still uncertain in dealing with an anonymous team. To best alleviate those concerns, we are offering a line of communication with the team via Telegram and Discord. Find the latest updates there, talk to the UltraYOLO project leads, and the rest of the community.

References

[1] WLA Magazine Issue 47: https://www.world-lotteries.org/images/publications/wla-magazine/pdf/wla_mag_47.pdf

[2] WLA Magazine Issue 46: https://www.world-lotteries.org/images/publications/wla-magazine/pdf/wla_mag_46.pdf

[3] WLA Online Gaming for Lotteries: https://www.world-lotteries.org/images/stories/WLS2014_rome/docs/WLA_Online%20gaming%20for%20lotteries_19-November-2014.pdf

[4] Are Millennials Killing the Lottery Industry?, https://www.vice.com/en_us/article/a3kaza/are-millennials-killing-the-lottery-industry

[5] One in Three Millennials Will Own Cryptocurrency by the End of 2018, https://themerkle.com/one-in-three-millennials-will-own-cryptocurrency-by-the-end-of-2018/

[6] WLA Annual Report 2016: https://www.world-lotteries.org/images/publications/annual-reports/WLA_Annual-Report-2016.pdf

[7] Smart Billions Whitepaper, https://smartbillions.com/docs/SmartBillions_Smartpaper.pdf

[8] TrueFlip Whitepaper, https://fs.trueflip.io/TrueFlip_WP_1.1.pdf

[9] Edgeless Whitepaper, https://coss.io/documents/white-papers/edgeless.pdf

[10] Funfair Technical Whitepaper, https://funfair.io/wp-content/uploads/FunFair-Technical-White-Paper.pdf

[11] DAO.Casino Whitepaper, https://github.com/DaoCasino/Whitepaper/blob/master/DAO.Casino%20WP.md

[12] Bitcoin Fees Info https://bitcoinfees.info/

[13] The Bitcoin Whitepaper https://bitcoin.org/bitcoin.pdf

[14] Ethereum Transaction Fees https://bitinfocharts.com/comparison/ethereum-transactionfees.html

[15] The SteemIt whitepaper https://steem.io/SteemWhitePaper.pdf

[16] zkSNARKs in a nutshell https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/

[17] Dan Boneh; Ben Lynn & Hovav Shacham (2004). "Short Signatures from the Weil Pairing". Journal of Cryptology. 17: 297–319. doi:10.1007/s00145-004-0314-9

[18] Dfinity project https://dfinity.org/

[19] Bitcoin Could Consume as Much Electricity as Denmark by 2020, https://goo.gl/PfroXE

[20] Masternodes.pro https://masternodes.pro/

[21] The Pineapple Fund, https://pineapplefund.org/

[22] Handbook of Sports and Lottery Markets: https://doi.org/10.1016/B978-0-444-50744-0.50031-7

[23] Grossman, P.J. & Eckel, C.C. J Risk Uncertain (2015) 51: 195. https://doi.org/10.1007/s11166-015-9228-1

[24] CLOTFELTER C. T. & COOK P. J. (1989) "The Demand for Lottery products" NBER working paper 2928. http://www.nber.org/papers/w2928.pdf

[25] GARRETT T. A., SOBEL R. S. (1999) "Gamblers favor skewness, not risk: Further evidence from United States Lottery games" Economic Letters 63 85-90.

[26] KEARNEY M. S. (2002) "State Lotteries and Consumer Behavior" Document de travail Wellesley College.
[27] THALER R. H., ZIEMBA W. T. (1988) "Anomalies. Parimutuel Betting Markets: Racetracks and Lotteries" Journal of Economic Perspectives 2, 161- 174.
[28] WALKER I. (1998) "The Economic Analysis of lotteries" Economic Policy 27, 357-402.

Disclaimer

The token economy is relatively new and incredibly innovative. Tokens could be impacted by regulatory actions, including restrictions on ownership, use, or possession. Regulations or other circumstances may demand that the YOLO mechanics be altered in all or part. Therefore, UltraYOLO may revise mechanics to comply with regulatory requirements or other governmental or business obligations. Nevertheless, we believe our planned mechanics to be proper and likely in the final version.Contributors assume risk when participating in the ICO. UltraYOLO could be subject to attack, bugs, or operational errors, and other unforeseen problems could result in the loss of stored value. This whitepaper has been prepared by UltraYOLO team for the sole purpose of introducing the technical aspects of the UltraYOLO and its associated platform and underlying blockchain protocol. This document does not constitute any offer, solicitation, recommendation or invitation for, or in relation to, the securities of any company described herein. The white paper is not an offering document or prospectus, and is not intended to provide the basis of any investment decision or contract. The information presented in this whitepaper is of a technical engineering nature only, and has not been subject to independent audit, verification or analysis by any professional legal, accounting, engineering or financial advisers. The white paper does not purport to include information that a buyer of UltraYOLO might require to form any purchase decision, and, in particular, does not comprehensively address risks of the UltraYOLO, which are numerous and significant. UltraYOLO (along with its directors, officers and employees), does not assume any liability or responsibility whatsoever for the accuracy or completeness of information contained in this whitepaper, or for correcting any errors herein. Furthermore, should you choose to participate in the ICO or Pre-ICO sale of UltraYOLO, UltraYOLO does not assume any liability or responsibility whatsoever for any loss of market value of UltraYOLO. The content of this whitepaper is technically challenging and requires a high degree of familiarity with distributed ledger technology in order to comprehend the UltraYOLO and its associated engineering risks. Recipients of this document are encouraged to seek external advice, and are solely responsible for making their own assessment of the matters herein, including assessment of risks, and consulting their own technical and professional advisers.