XOTTO
white paper

February 2017

WARRIOR DEVELOPMENTS LTD.

Contents

Abstract

The white paper describes the features of a decentralised blockchain lottery XOTTO, implemented on the Ethereum blockchain.

From the technical point of view, the XOTTO lottery is transparent and fair thanks to the blockchain technology, which represents the core of the lottery’s structure. Such an approach to transparency has all the chances to disrupt the existing gambling industry rules.

At the same time, the design of the lottery is very simple from the player’s viewpoint, which solves the major problem in the online gambling such as money withdrawals. With the cryptocurrency VEROS serving as a fuel for XOTTO, purchasing a lottery ticket is made easy and fast. The winner’s awards are delivered to a player’s Ethereum digital wallet simultaneously in VEROS.

The underlying technologies such as distributed ledger, the decentralised platform Ethereum and crypto-token VEROS have proven to be the most suitable and efficient solutions to the aforementioned issues (fairness, transparency, withdrawals) that the online gambling industry is challenged with.

Keywords: blockchain gambling, cryptocurrency, Ethereum, online lottery, XOTTO, VEROS.

Introduction

The spread of the blockchain technology throughout many spheres (fintech, IT, insurance, auditing, banking, real estate, etc.), which traditionally used to be centralised, has caused a tremendous transformation in these industries. The same is true about gambling, which has partially moved from the physical casinos to online gambling websites, and is now taking a step further from centralisation towards de-centralisation.

Digital currencies gained a lot of popularity on gambling websites as an alternative payment method, allowing players to deposit their funds to the online casino in a fast and secure way. However, cryptocurrencies alone could not help the industry to solve all of its current problems, especially when it comes to fairness, transparency and withdrawing funds. Thanks to the blockchain a new approach to gambling has been discovered.

Among thousands of applications of the blockchain technology gambling is one of those capable of changing the rules of the industry forever. For the first time in the history of gambling the blockchain technology allowed the industry players to witness transparency, which hasn’t been there before.

The key elements for transparency within the blockchain structure are smart contracts. Being introduced in 1994 by Nick Szabo smart contracts only existed as a concept up until recently. With the invention of Ethereum, designed specifically to implement smart contracts, the perception of the concept has changed. So far, Ethereum is the first and most well-known implementer of smart contracts, and is one of the leading decentralised platforms.

With regard to the XOTTO lottery, presented in this white paper, we are addressing the aforementioned major problems of the gaming industry: fairness, transparency and reclamation of awards. We are convinced that all three of these problems can be successfully solved by means of the technologies that are already known: decentralised platforms (e.g. Ethereum), distributed ledgers (e.g. the blockchain) and crypto-tokens (e.g. VEROS). The utilisation of these technologies in a lottery game does not imply any complexity, which we will demonstrate by outlining the mechanics of the XOTTO lottery.

The Impact of Blockchain Gambling On The Industry

Ethereum has proposed a new model of transparency, in which the blockchain is the game changer. In the gambling world, because of the blockchain, the players do not have to trust their funds to the game operator anymore, as no individual within this framework can hold the funds. This produces a direct effect on the reputation of casinos, which can now use smart contracts as a proof of reputation. Apart from transparency, lower transaction costs and anonymity are a valuable asset gained from using crypto-tokens on the blockchain-based gambling platforms.

From the auditability perspective the blockchain records data, which can easily be tracked by game providers and players, thus increasing the level of trust between the two parties. Just like in banking, the blockchain can prevent frauds, reward players and facilitate auditing, leaving no space for ‘black boxes’ within the industry. Potentially, thanks to the security features of the blockchain, online games can become unhackable and uncheatable.

Having experienced fair and transparent gambling, the players will start demanding more of it from non-blockchain online casinos, causing an immense transformation in the market. The current centralised structure of online casinos will be replaced by blockchains and decentralisation.

The future of the blockchain gambling is seen in prediction markets, which can identify trends and forecast outcomes of certain matters and events by means of specifically designed software applications named oracles. In prediction markets the blockchain will serve as an instrument to reduce risks via smart contracts. On the blockchain, the funds will remain safe and locked until an outcome in a prediction market is confirmed. Within this structure enhanced security can be achieved through multi-signature solutions and complex smart contracts, allowing to keep the funds on the blockchain inaccessible until a certain event takes place, triggering the release of the funds.

Thanks to the blockchain technology the gambling we are so used to will stop existing very soon, being replaced by a more fair openly accessible structure, in which the possibility of a fraud is next to nothing. Both parties involved into the gaming process on the blockchain (the game operators and the players) can benefit from this new way of interaction online. The absence of the old bulky structures within gambling will leave more space for creativity and will enhance the positive user experience.

What is XOTTO?

XOTTO is a blockchain-based lottery application in which players are required to guess the numbers that will be drawn from a transparent lottery machine. In decentralized gambling the blockchain performs a function of a lottery machine, and is also transparent for all the players.

The rules of the XOTTO lottery are very simple: players select 6 numbers from 1 to 49, enter an email address to receive notifications about the jackpot and purchase the ticket. The Mark Six lottery machine has the shape of the cylinder, which can be rotated so that the numbers can be randomised. Once the winning numbers are selected (which happens automatically), the person who entered the matching numbers receives the jackpot to exactly the same digital wallet address, from which the ticket price has been paid.

The entire XOTTO lottery platform is built on the Ethereum blockchain. This means that all tickets are verified on the blockchain as well. Such a transparent structure helps to confirm that the person actually owns the ticket. The jackpot funds are also stored in a single digital wallet and are auditable by any user.

By purchasing tickets players are sending digital money to a smart contract, which means that they are actually playing with a smart-contract application - that exactly describes what XOTTO is. On the Ethereum blockchain smart contracts act autonomously as entities, that is, the lottery participant plays versus a smart contract or the code. There is no place for a third party in this interaction: the code cannot be controlled by anything or anyone in this decentralised peer-to-peer network.

In terms of features the XOTTO lottery is:

- **decentralised:** Similarly to the entire Ethereum blockchain, on which XOTTO is based, there is no single person or entity in control of the system or the smart contract;
- **autonomous:** The process of drawing the winning numbers and transferring the reward to the winner happens automatically, like in the case of a self-executing smart contract. The player doesn’t have to go through lengthy registration and verification processes, he/she just sends the money from

purchasing the lottery ticket directly into the Jackpot wallet. The prize is automatically allocated to the winning player, so that the claiming is no longer needed.

- **fair:** The XOTTO lottery is transparent by design, as it makes use of the blockchain technology at its core. Everyone can access the data stored on the blockchain, but no single entity can bring changes to it. There is zero chance of fraud caused by the players or the XOTTO operator.

The Blockchain Specifics

In XOTTO lottery the payment (pay-ins and pay-outs) is done using the VEROS (VRS) cryptocurrency, and all transactions can be monitored on the blockchain. There is a number of other functions, which can be performed on the blockchain. These functions are outlined below.

According to the rules, the winning ticket receives the prize immediately, with funds (pay-outs) being automatically sent to the wallet, from which the ticket was purchased.

All tickets in XOTTO lottery are non-refundable and non-transferable, which means that if a player changes his/her mind before, after or during the game the ticket cost will not be returned

The jackpot can be viewed publicly on the blockchain placed onto a single Ethereum address. The size of the jackpot is determined by the total cost of the sold tickets. The payment to the winner is processed automatically from the jackpot wallet to the winner's wallet

The total amount of purchased tickets and the numbers selected by the player are automatically verified on the blockchain. This means that any ticket can be viewed and confirmed by anyone.

The 8-hour buffer is required before the numbers selected by the Mark Six lottery inside the blockchain application can be submitted within the XOTTO system.

Transparency

The common feature of the blockchain lotteries is enhanced transparency, which is an inherent characteristic of the blockchain as such. In the case of XOTTO functioning as a smart-contract, which is uninterruptible and is out of the game operator's control, the blockchain serves as a decentralised display of the following actions within the lottery:

- the automatic payouts to the winners' VEROS digital wallets;
- openly viewing and confirming all the tickets on the blockchain;
- the verification of purchased tickets added to the smart-contract;
- the verification of the jackpot on the blockchain viewable as a digital wallet address.

Restricted by the way smart contracts are created, the XOTTO game operator has no power to influence the process of selecting numbers. The operator cannot decide who the winner is going to be, as the winning ticket is selected automatically based on the drawn numbers. The operator does not determine to which wallet the prize will be sent, because this process is also completely automated and defined by the smart contract.

XOTTO as a Smart Contract

Smart contracts are considered to be the technology of the future functioning hand-in-hand with the blockchain. Just like the blockchain has once become an inevitable part of cryptocurrencies, smart contracts are now bound to be implemented into blockchains. The reason why smart contracts gained so much popularity is their compatibility with a wide range of devices and machines.

Smart contracts can hold information about commodities and property on the blockchain and thus transfer value in all kind of forms, other than just cryptocurrencies. Smart contracts are designed to assign rules and conditions to these commodities, they can also check whether all participants are following the rules or not. Thanks to the code smart contracts are unbreakable. Just like many cryptocurrencies and the blockchain itself, smart contracts are decentralised, transparent and easily accessible for anybody to view. The aforementioned features make smart contracts a promising technology with a bright future.

What decentralised platforms (e.g. Ethereum) are trying to reach with smart contracts is easier and faster achievable consensus, decentralised autonomous arbitration and automatic execution. In the near future these functions will be accomplished by decentralised autonomous organisations (DAOs), which are currently being designed by Ethereum, BitShares, Ripple, etc. So smart contracts are only an initial stage in ambitious plan to make the world more decentralised.

On behalf of the XOTTO lottery developers we were inspired by the idea of decentralisation and autonomous execution of actions on the blockchain. We also didn't want to lag behind the newest technologies, so the choice of smart contacts as the underlying technology for XOTTO was the natural one.

The code defines rules, under which smart contracts trigger specific events. For example, when the drawn lottery numbers match the numbers in a player's ticket, the prize is awarded. There is no place for additional third parties in this interaction and the entire process of the game is made in the most transparent manner possible. This autonomous interaction brings benefits to both parties involved into the game: **the game operator** does not have to look after the funds himself anymore, he can also rest assured that no frauds will occur; **the player** knows that when he wins, the smart contract will make sure that the award is delivered automatically to his own wallet.

VEROS Tokens

VEROS (VRS) is a cryptocurrency built on Ethereum, a blockchain-based distributed computing platform that runs smart contracts. VEROS has 8 digits after the decimal point (e.g. 0.12345678 VRS).

Ethereum serves as an abstract foundational layer, on which all the features required for the optimal functioning of VEROS are implemented. These functions are accomplished by smart contracts, deployed and processed by the entire network. By means of the entire Ethereum infrastructure, which allows validating transactions and adding new blocks to the blockchain, the possibility of attacks on the coin is minimised. The main reason to use the blockchain technology in the development of VEROS was providing a decentralised, stable and secure infrastructure, guaranteeing equal rights to access it to all of the parties involved.

VEROS can store and process digital transactions in a secure and transparent way. The token works as a blockchain application on the Ethereum platform, following the cryptocurrency standards prescribed by Ethereum at the deployment phase, namely the Proof-of-Work (PoW) function.

Smart contracts on the Ethereum blockchain are used to validate and protect certain rules regarding the distribution, management and ownership of coins. These contracts are enforced by the Ethereum network and cannot be invalidated or changed by any individual, organisation, entity or user.

The main advantage of VEROS is its suitability for the unbanked individuals, who are excluded from the banking industry due to economical hardships. With VEROS these individuals can use financial services for their daily transactional operations on the equal terms with the ‘banked’ individuals. VEROS users can send and receive transactions online and offline, exchange VEROS to FIAT money, shop with VEROS and buy XOTTO lottery tickets. VEROS tokens are sent and received by individuals in a fast and easy manner, which eliminates any third-party interventions typical for the traditional bank transfers.

Lottery Tickets

All XOTTO tickets are stored on the blockchain alongside with the selected numbers and ticket orders/ wallet addresses. By means of the Ethereum Explorer (a 3rd Party) any player can check all the tickets sold for the current jackpot.

All tickets have a fixed price in VEROS.

The ticket allows the player to select six (in some cases seven) numbers from the span of 1 to 49.

The XOTTO lottery website (xotto.org) is equipped with a ticket verification system, which acts as an explorer for the Ethereum contract.

XOTTO is based on a new Ethereum contract linked to the existing VEROS smart contract. The source code of the contract is open source.

The XOTTO lottery ticket can be purchased with VEROS at xotto.org. All prizes and the jackpot are offered in VEROS.

All tickets in XOTTO lottery are non-refundable and non-transferable, which means that if a player changes his/her mind before, after or during the game the ticket cost will not be returned.

XOTTO Shares

Xotto.org has its own jackpot funded from the amount of sold tickets.

The jackpot is shared between all winners with following categories:

- 6 matching: 70%
- 5 matching: 13%
- 4 matching: 5%
- 3 matching: 2%
- House commission: 10%

The operator always charges the commission from any amount of the winnings.

If no winning ticket has been drawn, the jackpot is awarded in the next draw.

The jackpot increases until all the prizes are won. This will lead to a huge jackpot overtime, attracting wider audiences.

Payouts

Apart from the majority of online casinos, in which players are supposed to claim their winnings after the game and, basically, rely on the will of the game operator. With blockchain gambling the rules have changed in the player’s favor.

XOTTO is one of the lotteries, which supports this idea and does not intent to cause any inconvenience to its customers. This is why the winning players are not required to request a payout, instead they receive the payments for their winning tickets automatically. The payout is automatically sent to the address, from which the XOTTO lottery ticket was bought.

The problem of prize reclamation has been the sore point of the gambling industry for years. Nowadays it is not an issue anymore due to the blockchain technology and its transparency-enhancing features. These features make blockchain gambling platforms more advantageous compared to other online casinos, and XOTTO is not an exception.

Results

The drawing occurs three times a week: on Tuesday, Thursday, Saturday or Sunday at 9:30 pm (Hong Kong time). The XOTTO players will be informed about the draws via email if they choose prior to purchasing tickets.

Architecture

XOTTO is organised as an application, which makes use of the Ethereum Smart Contracts (also implemented in VEROS) to allow users to buy lottery tickets. The action flow of the application is as follows:

1. The lottery draws 6 random numbers from 1 to 49.
2. The numbers are retrieved, then shown on the XOTTO website where users can check them.
3. The winning numbers are added to a smart contract, which then indicates the winning tickets. The users can track this process.

4. The smart contract, based on the jackpot, executes a VEROS transaction from the jackpot wallet to the winners' wallets.
5. If there is no winner, then the jackpot is kept in the jackpot wallet, and the tickets sold for the next draw are added to the reported jackpot wallet.

Conclusion

The white paper demonstrated how the major problems of the gambling industry can be addressed in a new way by means of the blockchain technology. On the example of the XOTTO lottery we have revealed how the issues such as fairness, transparency and fund withdrawals can be easily dealt with. The distributed ledger technology on the Ethereum platform fuelled with crypto-tokens has proved to be an essential part of the solution.

We anticipate that the popularity of online gambling will increase thanks to the blockchain technology, changing the rules in favor of the players and the game providers. What was formerly viewed as risk is now becoming a matter of transparency, through which the trust between the participants of the game is increased.

Bitcoin was among the earliest technologies, which has changed the way people spend money in the internet. Ethereum has increased the transparency of not only payments, but also all kinds of data exchange between two or more parties on the blockchain. VEROS is providing the unbanked individuals with a possibility to interact in the global economy, while XOTTO brings more fun and ease to cryptocurrency users. Thus, the entertainment and the generous rewards are organically imbedded into the framework of the XOTTO lottery delivering a unique experience to its customers.

References

VEROS white paper, 2016: https://veros.org/white-paper.pdf

Ethereum website: https://www.ethereum.org/

How Can The Blockchain Technology Impact The Gaming Industry, 2016: http://blockchain-finance.com/2016/06/21/how-can-blockchain-technology-impact-the-gambling-industry/

Gambling Industry - How Blockchain Can Make It More Transparent, 2016: http://fintechnews.ch/blockchain_bitcoin/transparent-gambling-blockchain-gambling-industry-how-blockchain-can-make-it-more-transparent/3844/

Online Gambling Industry - Worth Some 40$ Billion - Firing Up For Blockchain, 2016: http://www.the-blockchain.com/2016/11/26/online-gambling-industry-worth-40-billion-firing-blockchain/

What Will Be The Impact Of Blockchain On The Gambling Industry?: https://cms.gamcrowd.com/images/uploads/reportpreviews/sample_report_final_11.11.16.pdf

Zero-Collateral Lotteries in Blockchain and Ethereum, 2016: https://pdfs.semanticscholar.org/69c5/e9f976687ac6862fb583cdfb36f4650f4d36.pdf

Gaming Self-Contained Provably Fair Smart Contract Casinos, 2016: http://www.ledgerjournal.org/ojs/index.php/ledger/article/view/29/53

CoinDesk Smart Contracts Report, 2016: http://www.coindesk.com/blockchain-bitcoin-smart-contracts-report/

Blockchain Technology And Applications From A Technical Perspective, 2016: http://www.the-blockchain.com/docs/UNICREDIT%20-%20Blockchain-Technology-and-Applications-from-a-Financial-Perspective.pdf

Distributed Ledger Technology: Beyond Block Chain, 2016: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Appendix: Definitions

Blockchain is a distributed database used to create a digital ledger of transactions and to share it among a distributed network of computers. Cryptography allows each participant of the network to access and manage the ledger in a securely. No central authority here is needed. Each blockchain record (block) contains a timestamp and a link to the previous one comprising a chain.

Cryptocurrency is a medium of exchange, which makes use of cryptography to secure transactions and to control the creation of additional currency units. The development of cryptocurrency has been actively growing in the past decade, thus offering a broad range of transactional possibilities to both users and organizations.

Decentralisation is the process of distributing power, authority and/or responsibility from a single administrative center to subordinate or quasi-independent organizations and/or the private sector. The main advantage of the technology is the facilitation of complex procedures within a bureaucratic system speeding up the decision-making process.

Decentralized application (dapp) is a type of software shapes as a set of smart contracts and code ruling them. DAPPs are designed to exist in the Internet independently from the control of any single entity. There are many similarities between dAPPs and traditional web applications. Unlike a traditional web application, a dAPP has no centralized server. Instead of a server there is a blockchain. DAPPs can be built into the blockchain, just like various altcoins. In fact, dAPPs are compatible with many various applications and technologies.

Decentralized autonomous organization (DAO) is one of the most novel and disruptive applications of the blockchain technology representing a new form of legal structure, in which management and control is carried out by smart contracts.

Distributed ledger technology (DLT), a synonym of the blockchain technology, is a consensus of replicated, shared and synchronized digital data, geographically spread across multiple sites, countries and/or institutions. A distributed ledger immediately reflects the changes made by any participant in all copies of the ledger, and is very efficient. The full potential of distributed ledgers is attained when the other applications are layered on top of them (e.g. smart contracts).

Ethereum is a decentralised blockchain-based computing platform for applications such as smart contracts. The Ethereum blockchain is very advanced, which allows it to stay immune to frauds, hacks, censorship, etc. Thus, building applications on top of Ethereum is extremely safe thanks to its decentralized network protecting the blockchain.

Oracle is a piece of software, hardware or a human agent that can illuminate and authenticate the real world events, submitting this data to a distributed ledger to be used in smart contracts and to resolve disputes.

Prediction market is an exchange market designed to trade on the outcome of events. In a prediction market the crowd's opinion on the outcome of events can be detected.

Proof-of-work (PoW) is a function allowing the nodes in the blockchain network to reach consensus about the entries to the blockchain. This function requires users to perform a degree of work, or computer power solving mathematical puzzles, in order to participate. The first node to find a correct solution to the puzzle is rewarded with cryptocurrency (e.g bitcoin, ether). The other participants confirm that the solution is correct (reach consensus), which leads to the creation of a new block.

Smart contracts are contracts on the blockchain with terms recorded in computer language; they can be automatically processed by computer systems and perform functions such as value distribution, data storage, interaction with other contracts, etc. Using smart contracts has proved to be efficient both economically and functionally.

The **unbanked** individuals are people who do not own a bank account and/or do not have access to the traditional financial system due to economic hardships.

VEROS is a cryptocurrency functioning on the Ethereum platform, specifically designed for online payments, exchanges and purchases by means of smart contracts.