Quanta

White paper

The establishment of blockchain-based gaming alternatives has been a recognized possibility for nearly a decade already. Few decentralized gaming projects, however, have truly taken into account the implications of government regulation. Everyday, innovative projects are being shuttered by regulators, largely due to their founders' hubris with regards to the law.

v. 1.0.2
September, 2018

www.quanta.im

NOTICE:

THIS WHITEPAPER IS NOT A SOLICITATION TO INVEST. QNTU HAS NOT BEEN SOLD BY QUANTA AND THERE WILL NOT BE AN INITIAL TOKEN OFFERING. TOKENS ARE DISTRIBUTED BASED ON A LOYALTY SCHEME DETERMINED BY QUANTA. THE TOKENS ARE TRADABLE AS THEY CONSIST OF AN ERC20 ETHEREUM TOKEN. QUANTA DOES NOT MAKE ANY REPRESENTATION WHATSOEVER ABOUT THE FUTURE PRICE OR WORTH OF THE QNTU TOKEN. YOU PURCHASE THE TOKEN IN THE SECONDARY MARKET AT YOUR OWN RISK. TO LEARN MORE ABOUT THE RISKS OF PURCHASING TOKENS PLEASE READ HERE WARNING FROM UK FCA. FURTHERMORE WE DO NOT MAKE ANY REPRESENTATION AS TO WHETHER THE QNTU TOKEN IS OR NOT A SECURITY. ACCORDING TO THE LAWS OF THE ISLE OF MAN FROM WHICH THE QNTU TOKEN IS ISSUED THE TOKEN IS NOT DEFINED AS A SECURITY. YOU ARE RESPONSIBLE FOR ENSURING THAT YOU ARE LEGALLY ENTITLED TO PURCHASE THE TOKEN FROM A THIRD PARTY AND THAT SUCH DOING DOES NOT BREACH ANY LOCAL LAW IN YOUR JURISDICTION OR OTHERWISE. IF YOU RESELL A QNTU TOKEN YOU ARE RESPONSIBLE FOR ENSURING THAT THE BUYER IS AWARE OF THE QNTU TOKEN TERMS AND THAT THEY HAVE AGREED TO THE SAME. PLEASE NOTE: QUANTA IS NOT SELLING QNTU TOKENS UNDER ANY CIRCUMSTANCES SO IF YOU PURCHASE A TOKEN IT CAN ONLY BE FROM A THIRD PARTY OR AS AS PART OF A QUANTA LOYALTY SCHEME.

Quanta

Table of Contents

Executive Summary

The establishment of blockchain-based gaming alternatives has been a recognized possibility for nearly a decade already. Few decentralized gaming projects, however, have truly taken into account the implications of government regulation. Everyday, innovative projects are being shuttered by regulators, largely due to their founders' hubris with regards to the law.

The Quanta lottery, founded by experts in both 'fintech' and 'regtech,' is the first decentralized gaming organization that succeeds at combining advanced decentralization techniques - such as smart-contract powered random number generation (RNG) - with business practices that are compliant with government regulation.

Quanta's primary technical innovation lies in the manner by which lottery winners will be selected - the Ethereum-powered RNG protocol referred to as 'RANDAO.' This RANDAO feature has been thoroughly tested by NMI, and has received a remote gaming operator's license in the Isle of Man. This makes Quanta *the first legally operating blockchain lottery anywhere in the world.*

It is expected that Quanta will solve many issues currently faced within the lottery industry worldwide. As a platform, Quanta will form the basis of an entire ecosystem, with the lottery at its core. A system of cryptotokens will enable secure interactions and transactions between Quanta participants, including advertisers (affiliates), white label licensees, RANDAO participants, players, and other community members.

In terms of vision, Quanta's goal is to provide universal access to fair lottery services, whether this be for entertainment purposes or for charity. This document is intended to elaborate on this vision, and to make readers aware of the true humanitarian potential for the lottery.

Unit 1: Introduction

According to the Merriam-Webster dictionary, a lottery can be defined as “a drawing of lots in which prizes are distributed to the winners among persons buying a chance.” Whether or not a lottery can be described as a form of gambling is up for debate, but the fact that it is a type of business is indisputable, be it run by a private, public, or decentralized organization.

As a business, the lottery is composed of a number of key processes:

- Random Number Generation (RNG): In the vast majority of cases, lottery winners are selected by matching the number on their ticket with another number, randomly generated by the lottery organization using some kind of software.
- Ticket Sales: The means by which lottery tickets are advertised and sold.
- Budgeting: The determination of the size of the prize pool and the amount of funds directed back to the lottery organization
- Prize Delivery: The determination of the size of the prizes and the means by which they are delivered to winners.
- Compliance with regulation as well as local cultural practices in the region of the lottery’s operation.

1.1 The Case for Lottery Decentralization

In the forthcoming subunit, it will be argued that each and every one of these processes can be benefitted by decentralization, be it through blockchain integration or other methods.

Random Number Generation

Since the advent of the large-scale lottery, many techniques have been invented to determine the winner in the most fair way possible. The first significant attempt at RNG with a computational device for lottery purposes was made by the UK government in the late 1950s, and since that time protocols for this purpose have consistently grown more sophisticated.

While RNG is on its own an effective means by which to ensure fair winner selection, its implementation by centralized organizations has not proven itself invulnerable manipulation. In 2010, for example, a former employee of the US Multi-State Lottery Association managed to install software that manipulated the random number generator. The perpetrator managed to win a $14.3 million jackpot.

By carrying out RNG protocols on a distributed ledger, the entire process can be made visible to network participants. With integration of blockchain technology, inherent transparency can absolutely eliminate manipulation.

Ticket Sales

Five years ago, in 2013, the size of the online lottery market was already estimated to have a total revenue of $34 billion. As the industry grows, more and more online advertising is being carried out selling tickets for these lotteries. As the number of genuine ads, the number of scams grow as well - and this is a big problem. Usually carried out as “advance-fee fraud,” notable examples of lottery scams include the El Gordo Sweepstake, The UK National Lottery scam, and the Australian Lotto Inc scam.

By integrating blockchain technology into the lottery, two key things can be accomplished in terms of the sale of tickets: First, potential players will be able to determine if lottery tickets are genuine by looking up the smart contract code and examining the transactions. Second, by advertising using a decentralized system of affiliate advertising, the lottery can keep advertisements for their tickets under their control. In the event that an affiliate carries out a practice that may defraud the ticket purchaser, the decentralized lottery can banish the affiliate from its platform and eliminate the possibility for them to earn by advertising the lottery ever again.

Budgeting

The lottery as an institution has been well-recognized as a potential means by which to distribute charity - or at least to direct money to a good cause - while providing an exciting form of entertainment for the common man. In the United States, for example, it is usually the case that lottery revenue is directed to public schools.

Forever exists the worry, however, that funds that are meant to go to a good cause fail to actually go there. When all the transactions that a lottery organization carries out are recorded on the blockchain, the community can keep track of how closely management holds to its budgeting promises.

Prize Distribution

In traditional lotteries only around 45-60% of revenue is returned to players as prizes. Taxes generally take 25-40% of revenue, while 15% generally goes back to the managing organization to cover operational costs and be saved as capital.

With blockchain integration, most business processes can be automated, thereby reducing costs. In this way, the prize pool can be expanded, and a greater percentage of total revenue can be directed towards charitable causes.

Compliance with Government Regulations and Cultural Norms

A decentralized organizational structure can truly enable success for a transnational lottery platform. With decentralized management, experts in legal compliance from regions all over the world can be installed as consultants to help the lottery get accepted by local governments. A long list of countries are not adverse to online lotteries, but just require said lotteries to obtain official permission to operate. Local participants in the decentralized organization can help to obtain this permission.

Additionally, local consultants can help adjust the platform to local cultural norms, and even to the language. The way various cultures conceive of lotteries varies drastically around the world, and it is essential to enlist the help of locals in every market. Decentralized management provides a means by which to recruit and reward these locals as members of the community.

---

www.gbgc.com/publications/global-gambling-report/

www.scamwatch.gov.au/types-of-scams/unexpected-winnings/unexpected-prize-lottery-scams

www.money.cnn.com/2016/01/13/news/powerball-education/index.html

1.2 A World First

Having already been found to be compliant with gaming regulation in the Isle of Man, Quanta has become the world's first legally operating blockchain lottery. A decentralized organization built both to generate revenue and to contribute to charitable pursuits, Quanta has set the following objectives for itself:

- Develop a fully automatized and decentralized solution to RNG Manipulation
- Fully decentralize the ticket selling process using smart contracts and a unique system of purposeful affiliate marketing.
- Set a prize pool starting at 70% of revenue, and work to increase up to 85% in the long run.
- Build a global community of experts, as well as regular people, dedicated to making Quanta a viable - and legally compliant - business everywhere in the world.

www.quantaplc.im/wp-content/uploads/2017/11/pdf.pdf

Unit 2: The Lottery

2.1 The port of entry: thewallet

The port of entry for the Quanta lottery is the secure cryptocurrency wallet, which will enable users to participate on the platform in various ways.

- RANDAO participation (Winner selection)
- Lottery participation - Ticket purchase
- Receive affiliate rewards
- Cryptocurrency exchange (long-term)

The Quanta wallet will be released for download to iOS, Android, Windows, and Mac.

2.2 The Quanta Core: RANDAO

The core process of any lottery is the means by which winners are selected. The RANDAO random number generation protocol has been developed to decentralize this process. RANDAO is a type of decentralized autonomous organization (DAO) that makes use of community participation to generate random numbers. The RANDAO is governed by a smart contract that outlines participation rules. As a protocol, RANDAO comprises three stages that are automated using smart contract code.

Community participation is enabled by the following Quanta software products:

- Quanta KYC Webportal: Potential participants must provide the necessary information to achieve KYC level 3.
- Randao Admin Webportal: User interface utilized by administration personnel, elected by the Quanta PLC to administer the RANDAO protocol.
- Quanta Game Wallet: User interface utilized by community members, wishing to participate in the RANDAO protocol.
- Operation Manager Tool: User interface utilized by Quanta personnel, elected by the Quanta PLC to reward community members, participating in the RANDAO protocol.

RANDAO is a three stage protocol that can be also described as a five step process for the various participants.

Step 1: Preparation

Members of the community (RANDAO players), reach KYC level 3 and make a small ETH token, while Quanta administrators deposit reward payout tokens to an escrow wallet held by a third party organization.

Step 2: RANDAO Initiation

The lottery manager and operator each initialize the RANDAO protocol using the admin webportal The process starts only with the input of both participants.

Step 3, Stage 1: The Commit Stage

RANDAO community participants have their KYC level checked and deposit verified. When the minimum number of players for RANDAO have entered the “game,” the next phase is initiated. If not, the entire protocol is restarted and deposits are returned to game wallets.

Step 4, Stage 2: The RevealStage

The deposits made by community participants create hashing numbers which will henceforth be referred to as the “reveal number.” The operator or manager also submits a reveal number. Together these numbers are processed to create a final number, which can be used to calculate the lottery prize.

Step 5, Stage 3: The End Stage

The final number is sent to all wallets that had participated in the RANDAO protocol. The lottery manager sends rewards to community participants’ game wallets using the operation manager tool.

Note: RANDAO participants on the Quanta platform will have had to make a pledge in QNTU tokens prior to participating in the protocol. See section 3.2 for more information.

For a technical description of the RANDAO protocol, see appendix A.

2.3 Lottery Ticket Sales

Decentralized affiliate marketing

The vast majority of new Quanta lottery players will be referred to the platform via affiliate marketing. Affiliates will earn rewards for every ticket sale that results from a player following a referral link.

Affiliate payouts will be automated using smart contract code. See appendix C, section 1 for more details.

2.4 Revenue Distribution

A preliminary sketch of how ticket revenue will be divided is as follows:

Prize pool: 70-79% will be paid out to lottery winners (prize pool)

Ticket sale smart contract commissions: 1-10%

Royalty payments to QNTR token holders: 5%

Quanta's operational costs: up to 15%

The team has set the following two long-term goals in terms of ticket revenue distribution:

- 85% of revenue going towards the prize pool.
- Operational costs taking up less than 10% of revenue

Additional notes:

- Ethereum gas costs are estimated on a case by case basis.
- Exact rates for ticket sale commissions and royalty payments are subject to change.

The intention is to automate the revenue distribution process as much as possible. See appendix C, section 2 for more details.

2.5 The Prize Pool

The Quanta lottery will will have five prize tiers:

- Jackpot (1 winner) - 55% of prize pool
- 1st Prize (3 winners) - 5% of prize pool each
- 2nd Prize (5 winners) - 2% of prize pool each
- 3rd Prize (10 winners) - 1% of prize pool each
- 4th Prize - # of tickets sold = prize pool in dollars divided by 3 times the round's ticket price in ETH.

For a technical description of how winners are divided into tiers, see appendix B - "Game rules."

Upon winning, winners are notified automatically. Prizes, however, must be manually claimed. In the event that a prize is left unclaimed for 180 days it will be donated to a charitable organization of the Quanta PLC's choice. This process will be automated using a smart contract. See appendix C, section 3 for more details.

Unit 3: The Quanta Token System

3.1 Introduction to the Token System

The Quanta lottery is supported by a token economy. The lottery and the token system are two separate entities that supplement one another.

The Quanta token system includes two blockchain-emitted assets:

1. QNTU is the utility token of the Quanta ecosystem that the various participants will be able to “put up” as a pledge. QNTU forms the basis of an internal economy that ensures the security of the network.

2. QNTR tokens provide token holders with the right to access royalties from the Quanta lottery system.

Neither tokens are connected in any which way. They exist with separate purposes in mind.

3.2 The Quanta Utility Token (QNTU)

QNTU as a facilitator of honest community participation

As was described in Unit 2, Quanta aims to decentralize all aspects of the lottery. Community participation is essential for the following processes of the Quanta’s decentralized lottery:

- Ethereum gas costs are estimated on a case by case basis.
- Exact rates for ticket sale commissions and royalty payments are subject to change.

While registry on the distributed ledger will make these processes transparent, it does not provide full security for the system. It is for this reason that the Quanta team has developed the QNTU token.

The QNTU token will not be available for direct sale.

Token Concept

The QNTU token functions as a pledge that community members must “put up” before they may begin participation. In the event that the participant breaches the terms of use laid out by Quanta, the pledge made in QNTU is forfeited to the Quanta PLC.

Community participants required to make a QNTU pledge in order to participate:

- RANDAO Players: The QNTU pledge is deposited prior to the KYC procedure.
- Affiliate Marketers: The QNTU pledge raises the affiliate marketer to a level above that of a bounty participant. The QNTU pledge means the affiliate marketer will receive a commission in the currency used in the lottery (ETH).

Non-community participants required to make a QNTU pledge in order to participate:

- White Label Licensees: The QNTU pledge is a mechanism by which whitelabel businesses can be kept in check. If the terms of use are breached and the pledge lost by the white label licensee, that lottery business can no longer function.
- Experts and Consultants: The QNTU pledge ensures that regional legal, business, and advertising experts devote themselves to compliance with local laws, as well as to honest practices in general.

Membership Values

All QNTU pledge “values” will be expressed in USD. We expect a large amount of the supply at any given time to be pledged and held in smart-contracts.

Issuance and Token Allocation

QNTU is issued by the Quanta PLC as an ERC-20 ethereum based token, and unlike many new utility tokens, will not be distributed during a token sale. Instead, there will be a token generation event, during which tokens will be distributed in the following manner:

120 Billion QNTU tokens to be issued. Distribution will be in the following manner:

- 18% - Early Distribution Program: Lottery Mining system. When a user purchases a lottery ticket from Quanta Technology then the user ‘mines’ QNTU from this allocation. Mining distribution expected to take place over the months of February, March and April 2018
- 2% - Token distribution in person at major industry events and conferences over the months of February, March and April 2018 for Quanta Members
- 40.47% - Quanta Membership Programme Account (Supporter Members/ Affiliate Members/ Community Members/ Player Members). Distribution of these tokens to Members based on loyalty and rewards mechanisms only. Quanta membership Account is not part of the market circulation of the token; the tokens are earned based on the actions of the Members
- 15% - Quanta PLC allocation (locked token account. Locked for 24 months)
- 15% - Quanta PLC allocation unlocked tokens. If balance of unlocked tokens of Quanta plc exceeds 33.33% of tokens in circulation in market then the excess will be transferred to locked balance account of Quanta plc
- 9.53% - Airdrop to early supporters of Quanta project

QNTU and Lottery Players

A player of the Quanta lottery does not need to pledge QNTU in order to play. They may however be eligible for the Quanta Player Loyalty Scheme, where players receive ‘cashback’ in QNTU. This loyalty scheme will be provided to player members from time to time.

QNTU as a reward and entry point for Bounty Participants

Bounty participants are not excluded from the Quanta platform. They can work as affiliates, advertising the sale of lottery tickets, in exchange for a QNTU reward. Eventually, bounty participants can earn enough QNTU to make a token pledge and become affiliates, thereby becoming able to earn cryptocurrency commissions.

The purpose of this reward system for bounty participants is to encourage highly motivated advertisement of lottery tickets, while staying within the bounds of the Quanta terms of use.

3.2 The Quanta Royalty Token (QNTR)

The Quanta royalty token serves a different purpose than the utility token. QNTR tokens will be sold during various token sales, with the intention of raising the funds necessary to expand the lottery to newjurisdictions.

The Royalty Smart Contract

5% of the lottery pool received by Quanta Technology Limited will be distributed to QNTR holders as royalties. This will be done automatically via a smart contract.

Token Registration

QNTR is an ERC-20/ KYC token. This means that the token can only be transferred from verified users. Verified users have to be verified by the Quanta PLC (Quanta plc is in the process of transferring administration of the Quanta protocol to the Quanta PLC over the course of 2018).

The Quanta wallet will serve as a port of entry for this KYC procedure.

- 120 billion tokens
- Currently distributed:
    - 9.53% distributed to early supporters (already distributed)
    - 2.87% Quanta PLC
- Locked and held by Quanta PLC:
    - 2.6% (locked for 12 months)
    - 25% (locked for 30 months)
    - 60% (long-term lock)

*However if supply in market circulation is more than 33.33% then Quanta plc to transfer to locked balance.

Note: QNTR is not classified in the country of issuance as a security. However outside most likely will be considered a security and, as a result, users may not be able to access QNT-R if it is restricted by law in their jurisdiction.

Unit 4: The Quanta Organization

4.1 Quanta's Structure: Approaching Decentralization

The organizational structure of the Quanta ecosystem aims at decentralization. Currently, the structure manifests itself in the following way:

- Quanta PLC acts as the holding company at the current moment. Outstanding tokens will be relegated to this company during the initial phases of Quanta setup and operation.
- Quanta Technology is an organization that is held by Quanta PLC. This organization runs the lottery and issues both QNTR and QNTU tokens.
- Preparations are underway to transfer ownership of both tokens' smart contracts to the Quanta PLC which is currently in the process of being set up.

4.2 Team

Konstantinos Farris

Chief Technology Officer

Konstantinos had a prosperous twenty-eight-year career in the gaming industry including twenty years at Intralot, the Greek giant company with more than 5000 employees and one of the biggest technology supplier and operator in the global gaming industry. At Intralot, Konstantinos was the Group CTO and Executive Committee member responsible for the management of the Group Technology Division with more than 350 IT experts.

Steven Ormond-Smith

Chief Financial Officer

Steven is a Fellow Member of Association of Chartered Certified Accountants (FCCA) and is the Founder and Managing Director of Ormco PLC – a company providing accounting, corporate structuring and outsourcing services. Steven has over 20 years' experience, with extensive experience in fiduciary services, fund administration and fund accounting. Before founding Ormco, Steven was a Senior Fund Accountant for 4 years, managing the finance function for a number of companies listed on the London Stock Exchange. He has also worked for two of the Big Four accounting firms. Steven is an experienced director, and is currently a non-executive of several companies.

Adam Vaziri

Chief Regulatory Officer

Adam is a blockchain lawyer and founder of London and Hong-Kong based Diacle, which assists blockchain & fintech projects with compliance. Adam is a tireless blockchain entrepreneur and 'bitcoin pioneer' as labeled by Bitcoin Magazine. He is now in his third term as director of the UKDCA, which lobbied for and achieved the most favourable regulatory environment for cryptocurrency in the world. Since 2014, Adam has run bitlegal.io – a global tracker for blockchain law that was featured by CNN and The Washington Post.

In conjunction with HackCoin, he hosted the first suite of blockchain hackathons across the world in the UK, India, HK and Malaysia. Adam is a member of Chain-Finance.com which provides dedicated news/ events about the blockchain financial services industry.

Lee Hills

Chief Operating Officer

Lee is a founder of SolutionsHub, a company that develops start-ups for small and medium-sized enterprises and offers business consulting, planning, and strategy support services. Since 2009, he has successfully provided consultations and multi-jurisdictional licensing services for eGaming companies while being a key advisor to dozens of licensed and non-licensed gaming companies globally. He was instrumental in obtaining licenses for a number of unprecedented business models and the first ever sub-license. Subsequently, Lee has widened the scope of his technological expertise into the Blockchain and FinTech sectors.

Advisors

Harmen Brenninkmeijer

Advisor

Harmen Brenninkmeijer (Advisor) founded Dynamic Partners together with several international gaming industry veterans in 2015. He was VP Strategic Markets for Inspired Gaming Group (INGG); founder and CEO of Octavian Global Technologies, a USD $90MM casino technology supplier with over 35k networked Electronic Gaming Machines and operations in 10+ countries. Before founding Octavian, Harmen partnered with the Gauselman Group to establish Avalon Casino Management, which developed, owned and operated the Grand Casino in Hungary, Magic Casino in Northern Cyprus and the Playboy Casino on the island of Rhodes.

Hans Lombardo

Advisor

Hans Lombardo (Advisor) is co-founder of Chain of Things, an integrated hardware service startup related to blockchain technology and IoT (internet of things). He is also the current manager of the company's Marketing and Communications department. As a tech journalist in the late 1990s, Lombardo interviewed such industry luminaries as Jack Ma (CEO of Alibaba), Jerry Yang (Yahoo! founder), Richard Li of PCG and Vinton Cerf (also known as one of the fathers of the internet).

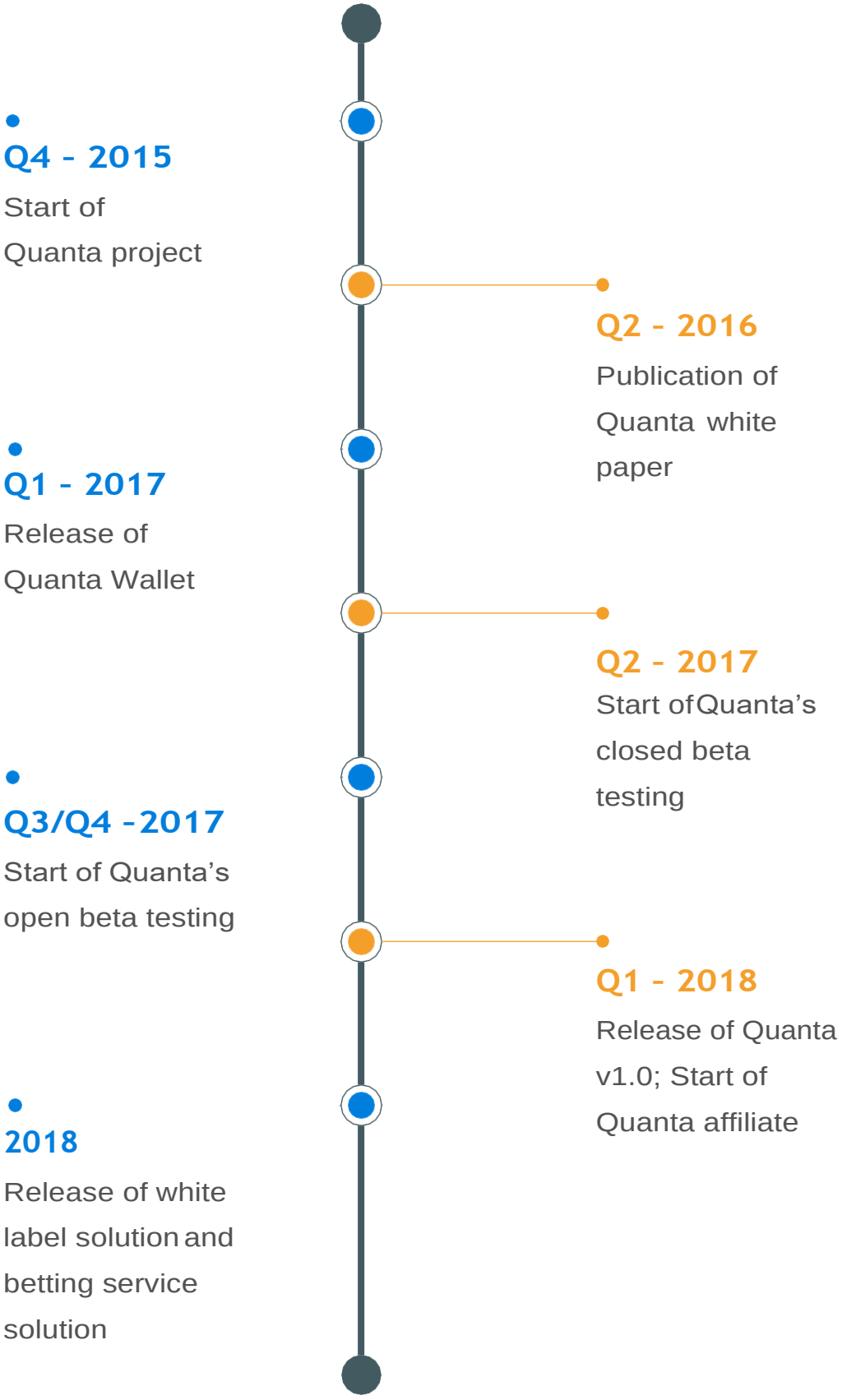
Lombardo later provided due diligence support for internet.com's venture capital fund in Asia, investing in a number of internet startups in China. He has extensive experience in the internet industry as a whole, including an editorial position at Internet World Magazine.

Pawel Kuskowski

Advisor

Pawel Kuskowski is an entrepreneur and regulatory AML/ CFT and compliance thought leader. Pawel is the former Global Head of AML/ CFT/ Sanction Functions at major international banks, with over 14 years experience in the Financial Sector. He is also an innovator in the application of blockchain technology in the financial industry. A recognized leader in compliance and anti-money laundering, with extensive experience conducting global projects for international financial institutions and cooperating with supervisory authorities, Pawel is also the Chairman of the Compliance Association of Poland.

4.3 Roadmap


Q4 - 2015
Start of Quanta project
Q2 - 2016
Publication of Quanta white paper
Q1 - 2017
Release of Quanta Wallet
Q2 - 2017
Start of Quanta's closed beta testing
Q3/Q4 -2017
Start of Quanta's open beta testing
Q1 - 2018
Release of Quanta v1.0; Start of Quanta affiliate
2018
Release of white label solution and betting service solution

Appendices

Appendix A: Technical description of the RANDAO protocol

Part 1 of this appendix discusses what a RANDAO is and how it functions in general terms.

Part 2 gives a brief overview of the particularities of Quanta's RANDAO.

Part 1: The Basic Randao

A RANDAO is a type of DAO, or 'decentralized autonomous organization.' The participation in a RANDAO is dependent on the creation of a smart contract, in which the rules of the 'game' and encoded. The purpose of the RANDAO - the random DAO - is to generate a random number in such a way that excludes internal and external manipulation.

Step 1

To begin the process of generating a random number, the user needs to send a transaction to contract K with a pledge of X ETH within a limited timeframe. This is sent with the result of sha3(s), s the being the secret number generated by the walet.

Step 2

When this is complete, and provided the sha3(s) has been submitted and accepted, then the next step is to send the number 's' to contract K. Contract K will verify that s is in fact a valid number be running it with sha3 and contrasting the new result with the already sent data.

Step 3

Provided it is accepted, s will be used as a seed in the random number generation process.

Once all secret numbers have been submitted, collected, and verified, contract K will generate a random number using the function f(s1,s2,…,sn). The output of the function will be written to contract K and all other contracts that had requested the random number will receive this output as well.

Following this, contract K will send back the pledge to the participant, dividing any profit equally as a bonus for each participant. This profit is generated by fees paid by other contracts that utilize the generated random number.

Anti-manipulation rules

The random number generator incorporates several rules that are designed to make sure it operates efficiently and avoids potential manipulation. These rules are.

If multiple sha3(s)s are submitted at once, the first one received is the only one accepted.

There is a minimum number of participants, if this number is not reached within the limited period of time, the random number will not be generated.

If an sha3(s) is sent and accepted by the contract, s will be revealed in step 2. It cannot remain hidden.

Should the user fail to reveal s during step 2 of the process, his X ETH sent in step 1 will be surrendered and no recompensation will be provided.

Further if one of more is not revealed in step 2, the random number generation will fail. All confiscated ETH will be split equally among other participants who did reveal their s in step 2. The fees paid by other contracts will be returned.

The Random Number Generation cycle is short and 20 cycles per hour are easily possible. If one cycle returns a profit rate of 0.001%, monthly profit could be estimated at 0.00001 x 20 x 24 x 30 (profit rate per cycle, hourly cycles, 24 hours, 30 days). Resulting in a monthly return of 14.4%.

Using this 14.4% monthly return we can calculate the costs.

Let N = number of users, G = the ‘gas price, C = the gas used internally by the contract,
R the number of requests, P = the call price in Ethereum.
Running costs = N * 3 * 500 * G - C
Income = R * P
Money received per participant = (RP – 1500n * G – C)/N

Current gas price = 10 szabo. Contract consumption estimation = 1500n gas. Estimate of net income is therefore: RP/ N – 0.03 ETH.

If the RNG has 10 participants with a pledge of 1000 ETH, the minimum income would be over 0.001% at 0.4 ETH. There is, therefore, only a single RNG request with a service price of 0.4 ETH. Should it be requested 10 times, the prime remains the same at 0.04 ETH for each.

Part 2: The Quanta RANDAO

RANDAOs, as with other smart contract protocols, are not impervious to manipulation and other security concerns. It is for this reason that the Quanta RANDAO has implemented the following requirements and procedures:

- KYC verification as a condition of RANDAO participation (appendix B)
- QNTU token Pledge as a condition of RANDAO participation (unit 3.1).
- A two-sided structure (Quanta's unique protocol is outlined in unit 2.2): Inclusion of the lottery administration as a participant reduces the chance that some external group can collaborate to drive a particular number through the RANDAO system.

Appendix B: Game Rules

1 Our Services

RANDAOs, as with other smart contract protocols, are not impervious to manipulation and other security concerns. It is for this reason that the Quanta RANDAO has implemented the following requirements and procedures:

a. Be 18 years old or the minimum age for gambling in the country where you are located, whichever is the greater;

b. Register your Ethereum wallet address that you will use to send Ether in order to buy a lottery ticket (Sending Address).

c. Once you registered, you can not change the following information: full name, email, display name, date of birth and Ethereum address in the Account Profile (Profile).

Ether is the name of the currency used within Ethereum blockchain network. We will hereafter use ETH for Ether in this document.

2 Account Profile (Profile)

In order to verify the Account Profile (Profile), you need to go through further verification process ‘KYC 3' in which you provide:

a. Colored scan of your official identification document

b. A photo of yourself holding the official identification document

c. A picture of your proof of current address (such as credit card statement, bank statement). It must be original in English (has to be issued within last three months).

Once sending the above document to be verified by QTL, you cannot change any information in your Profile. If you have passed KYC3 then you will be informed.

3 Your Account

You are only entitled to open one account with QTL (Your Account). Duplicate accounts constitutes a breach of these terms.

You warrant that the details you provide in relation to Your Account relate to you, are accurate and up to date. You warrant that you: control and are the legal and genuine owner of any ETH you send to us and any Ethereum address you register with us; that the funds are not derived from any illegal source.

We will take all measures at our disposal and as provided by the law, including but not limited to cooperating with investigatory bodies, if we identify any breaches by you of these warranties. In case of a breach of our terms, a ban of your Account and/or even a loss of ETH you have spent for tickets and/or restriction to service access including tickets history will be applied.

4 Using the Services

Each draw runs sequentially. We do not run multiple lotteries in parallel. You will be able to see the current lottery on the Sites (Current Lottery).

All lottery tickets are priced in ETH and the payment is only received in ETH. The price of each lottery ticket is set in ETH equivalent of USD1.00 at the time of each lottery draw's start.

You will see a QR code that contains our lottery ticket public selling address (Selling Address). If you use the QR code, the ticket price will be shown USD1.00

Please pay into the Selling Address to order 1 or a number of lottery tickets (Lottery Order).

There is a maximum of 30 tickets that can be purchased with one Lottery Order. Any overpayments for tickets will be refunded.

A valid Lottery Order is only made when the Selling Address has received cleared funds which for now is 6 confirmations on the Ethereum network.

If we accept your Lottery Order you will see your ticket numbers for each ticket that you have purchased (Ticket Number) in the Account Profile (Profile).

The Ticket Number is randomly allocated to you. You do not choose your own Ticket Number.

Through the Profile interface you will see all the tickets you have purchased during the Current Lottery and previous lotteries.

5 Selling Period

There is a minimum threshold of 1,000 tickets for each lottery that must be met (Minimum Threshold). Once the Minimum Threshold has been met then the lottery will commence: for 7 days and then expire or will expire when the number of tickets sold reaches the maximum threshold of 50,000 tickets (the Expiry Time).

6 Prize Pool

The Current Lottery Prize Pool is displayed on our Sites. For convenience we display this in US Dollars but it is held in ETH. The US Dollar value of the Lottery Pool may fluctuate based on exchange rate changes between US Dollars and ETH which we will set, and will be final. From the Final Number the lottery system will determine the allocation of the Prize Pool to the winning ticket numbers.

6.1 Ticket Sales

70% of the tickets sold represents the prize pool (Prize Pool).

6.2 Ticket Sales

55% of the Prize Pool is the Jackpot. The Jackpot is only available if the last digit of the Final Number is one of ‘8’, ‘0’, 1’, ‘3’. Due to hexadecimal nature of the Final Number that makes 25% chance (4 possible outcomes out of 16: from 0 to f) of the Jackpot occurring in each lottery draw.

If there is a Jackpot winner, 90% of Jackpot prize pool is paid to the winner, 10% is added to the next Jackpot prize pool. If it is not available then the Jackpot will roll-over to the next Jackpot prize pool.

Jackpot Transfer Rule: the Jackpot will rollover 04 (four) times. If Jackpot does not occur within 4 consecutive draw, then it must occur on the following draw , the 5th draw of the lottery.

6.3 Other Prizes

15% of the Prize Pool is for the 1st prize of which there are 3 potential winning ticket numbers

10% of the Prize Pool is for the 2nd prize of which there are 5 potential winning ticket numbers

10% of the Prize Pool is for the 3rd prize of which there are 10 potential winning ticket numbers

10% of the Prize Pool is for the 4th prize of which is based on the number of tickets

The 4th prize (is a fixed formula) = 3 * ticket price of the current draw (in ETH) Total of 4th prize winning ticket numbers (q*) = Prize pool (4th) / 4th prize

7 Randao Process (RNG)

All participants' random reveal number(s), plus operator's reveal number and operation manager's reveal number (operatorReveal) are collected to generate Randao Final Number (see Randao Process diagram). We combine all reveal numbers to generate Randao Final Number by using XOR operator : 'bitwise exclusive or' operator ^ (see more in Solidity documentation: http://solidity.readthedocs.io/en/develop/types.html)c.random ^= c.operatorReveal;

8 Winning Tickets Selection

Randao produces Randao Final Number after Randao process is completed.

All winning tickets are selected by using this Randao Final Number. To select winning tickets, the lottery smart contract uses MOD operation and SHA3 as below: MOD is Modulo operation that always produces a single result. SHA3 is a cryptographic hash function that converts any large number into a consistent 256-bits one that is thus suited for matching to ticket numbersFinal number (1) = SHA3(Randao Final Number)

The formula for deciding the jackpot winning ticket is below:

If the last digit of the Final number (1) which was produced by “SHA3 of Randao Final Number” s ‘0’, ‘1’, ‘3’ or ‘8’, there is a Jackpot prize in this draw of lottery.Jackpot ticket number = Final number (1) MOD number of tickets sold.

The formula for deciding the winning tickets of “1st prize” is below:

Whether there is a Jackpot prize or not in the draw, the Lottery contract always uses the formula as below to calculate Final number (2)
Final number (2) = SHA3(Final number (1))
“1st prize Ticket number” = Final number (2) MOD number of tickets sold If the “1st prize Ticket number” is identical to “Jackpot Ticket number”, the “1st prize Ticket number” is determined by repeating the calculation formula as below until getting a unique “1st prize Ticket number”
"final number (3) =SHA3(Final number (2)) 1st prize Ticket number = Final number (3) MOD number of tickets sold The formula for deciding the winning tickets of 2nd prize to 4th prize is the same formula for deciding 1st prize:"

Final number (i) =(SHA3(Previous Final number))“The next prize Ticket number” = Final number (i) MOD number of tickets sold If the “The next prize Ticket number” is identical to any “Previous Winning Ticket number”, the “The next prize Ticket number” is determined by repeating the calculation formula as below until getting a unique winning ticket number.
Final number (i+1) = (SHA3(Final number (i))

The next prize Ticket number = Final number (i+1) MOD number of tickets sold

9 Official Results

The official results of the lottery are published on the Ethereum blockchain and on the Sites. You agree that those results are final. Once the results are public on our Sites, we consider that date is the announcement date

10 Payment of Prizes

If you have won a prize then you will be notified via the Profile. You must make a claim in order to receive the prize.

Any delay on your part may result in expiration of the prize (which is 180 days from the announcement date). Once you make a claim request, all winnings up that point will be processed simultaneously. If your claimed prize plus the total of ETH you have claimed in the current month has the value of USD200.00 or less OR you have already completed KYC level 3, your claim will be reviewed and approved by QTL.

After approval has been received your prize will be transferred to your winning ETH address immediately. An email will be sent to you in order to confirm your user details prior to the payment being made if the prize is more than USD200.00 (two hundred U.S. Dollars), then you will need to go through additional verification ‘KYC3’ before we can pay the prize to you. This will involve you signing into your account and uploading a photo of your official identification document, a photo of you with the identification document and a picture of your proof of current address (has to be within last three months).

If you have already passed KYC3, then you will be informed. Once you have passed KYC3, you will receive the prize due to you once you have clicked the 'claim winnings' box in your user profile. If you do not pass KYC3 within the period of 180 days from the announcement date then those prizes will be forfeited and passed to donation pool.

11 Details

You warrant that the details you provide are accurate.

You are responsible for keeping your details up to date. If you failed to pass our KYC3 procedures as requested it may result in the blocking of your account and not being able to claim the prize. If you provide details to us but we are unable to accept you as a user of the website for any reason, we will notify you of this. In this situation you acknowledge and agree that we may retain your details for a reasonable period of time in case circumstances change and we are subsequently able to create an account for you.

We only pay prizes to the Ethereum address you registered with us. We will not be liable for paying the prize to your registered account if you no longer has access to that account.

12 Typing Errors

We take no responsibility for typing errors on your part in submitting a Lottery Order. Please note that Ethereum transactions are irreversible.

13 Technology

In order to participate in the QTL Lottery you need to have an Ethereum wallet. You are responsible for the management of your wallet and the private keys for your wallet.

14 Sending Address

We register your sending address on our system. If you send ETH to a Selling Address from a non-registered account we will refund those funds and you will not be able to purchase a ticket.

15 Self-Exclusion

QTL believes in responsible gambling. See our page on how to Self-Exclude or Self-Limit. If you Self-Exclude and try to pay for a ticket your account will be suspended and funds will be returned.

16 Transaction Costs

We do not pay for transaction costs in making refunds. All refunds are minus the transactions fees incurred in making the payment.