I. Overview

Winchain is a blockchain-based underlying system developed by the Winchain Open Source Technology Foundation Team ("WOST team") from Singapore to support the operation of national-level lottery systems. With its in-depth blockchain technology know-how and unmatched industry exposure, the WOST Foundation team is trying to revolutionize the lottery industry through decentralized technology, and further develop the blockchain-based lottery technology into a new standard of underlying system behind lotteries around the world. Currently, an African country has decided to adopt the Winchain lottery underlying system in its national-level lottery operation, aiming to issue the world's first decentralized lottery ticket by 2019. Winchain is actively pushing its businesses in Africa, Asia and Europe along the One Belt and One Road corridor, some of the countries have expressed their interest to adopting the technology in its national lottery operation. The WOST Foundation team's vision is to become the world's leading lottery technology provider in the new age of cryptocurrency.

Today's blockchain applications are generally categorized as public blockchain and consortium blockchain. Although enjoys the optimal decentralized attribute, the public blockchain ("public-chain") is not appropriate for many practical application scenarios due to its slow transaction performance and high transaction costs. In the other end, the consortium blockchain ("consortium-chain") does have a huge advantage in terms of high transaction efficiency and low transaction cost, but the use of the consortium nodes in the consortium-chain falls short of the requirement of full data transparency. To address such imbalance, Winchain innovatively proposed a dual-chain mechanism (public-chain + consortium-chain) for the purpose of supporting new lottery business operations and new blockchain-based lottery games. The public-chain serves as the back bone of the node election and due to its openness, more people can participate the consortium-chain's node registration and bookkeeping process, and ultimately get rewarded. Such design not just encourages more participants to take part in the consortium-chain's ecosystem, but more importantly keeps the whole system much closer to a public-chain in terms of openness, transparency, and robustness. As the low-level technology platform, the consortium-chain is designed to support any nation's lottery operation and related lottery games, with benefits like instant transfer of digital assets at a very low cost. By combining the public and consortium blockchain networks together, the decentralized rights, bookkeeping, and transactions are carefully implemented in the ecosystem whilst decentralized lottery games can enjoy instantaneous performance on Winchain at a very low cost.

II. Challenges Faced by the Lottery and Gaming Industry

2.1 Background

Lottery can be traced back to the Roman Empire two thousand years ago when people started from playing raffles and later on, the lottery industry became popular in other counties and was gradually evolved into an modern industry with games, competition, recreation, and fundraising all being integrated together.

During the 1980s and 1990s, the lottery industry reached the stage of an explosive development and the lottery ticket sales witnessed a soaring growth all around the world. Lottery issuance became popular from developed nations to developing countries including Africa. To date, more than 150 countries have issued various lottery tickets, the lottery business has become the sixth largest industry in the world.

In January 2018, the World Lottery Association released the global lottery sales report in Basel, Switzerland. Statistics showing that compared with the same period of 2016, global lottery sales increased by 1.8% in 2017. The African lottery market has delivered a stronger performance with 5.6% growth in sales exceeding the Asia Pacific region, making it the fastest-growing region in the world. As one of Winchain's industry consultants, the World Lottery Association will assist Winchain to launching its innovative business operations globally.

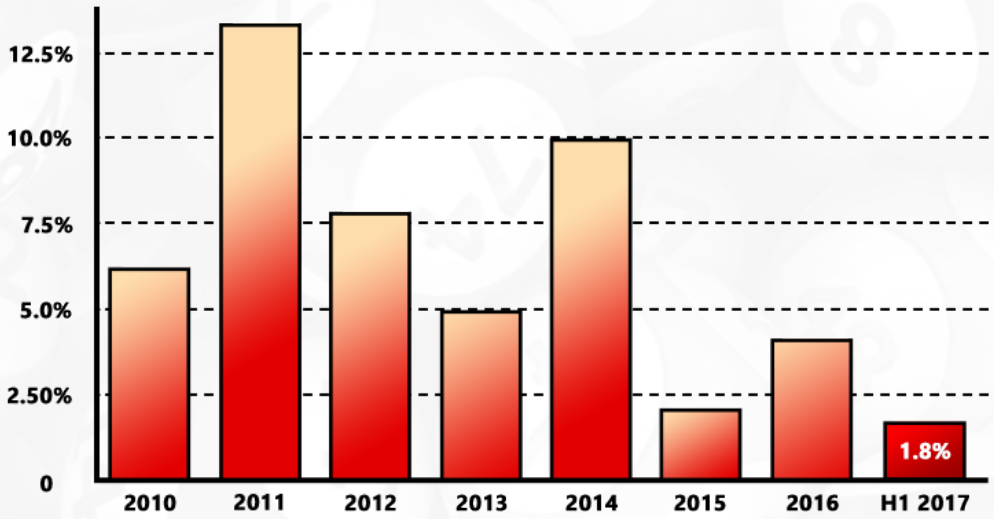


Figure 2-1 Growth Chart of Global Lottery Sales (2010~H1 2017)

As an emerging market, Africa is a place where lottery industry is growing rapidly and attracting attention from all over the world. Winchain's ecosystem partners are setting up operations in African countries since 2017 and have been granted the national lottery issuance and operation license in an African country. The progress of setup business operations in other countries of the African continent are also looking positive.

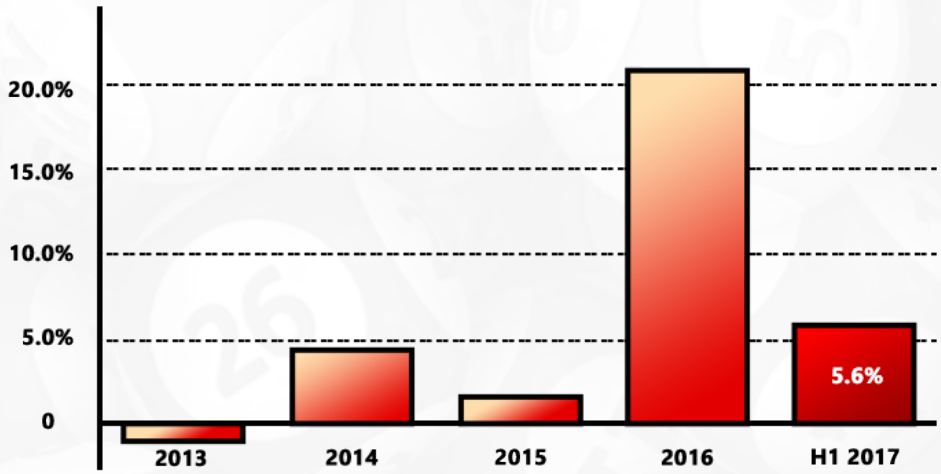


Figure 2-2 Growth Rate of Lottery Sales in Africa (2013~H1 2017)

2.2 Math and Operations Behind the Lottery Industry

2.2.1 The Laplace Probability Theory (Probability Equality Theory)

The Laplace probability theory is known as traditional probability theory. If a random experiment contains a limited number of unit events and each of them has the equal probability to take place, the probability **P (A)** of the event **A** in the event space **S** shall be:

The sample space of the random experiment **E** (the aggregate consisting of all basic results of the random event **E** is the sample space of **E**) is set to **Ω**. Each of events **A** corresponding to **E** is given a real number **P(A)**, which shall meet the generally acknowledged truth as follows:

1) Non-negative: **P(A)⩾0**;

2) Standard: **P(Ω)=1**;

3) Countable (complete) additivity: a number of incompatible but countable infinite events **A1**, **A2**..., **An**..., then **P(A1UA2UA3---)=P(A1)+P(A1)+---**

So, the real number **P(A)** is called as the probability of the event **A**.

For example, if we assume that, in a random experiment for casting two coins at the same time, both coins show the surface of character is called event **A**, so the probability of the event **A** should be calculated as follows:

S={(character, character), (character, number), (number, character), (number, number)}

As defined therein, the probability of **A** is 1/4. And because people don't know whether the coins are "perfect", such as, whether the coins are made perfectly even, and the center of gravity is exactly located in the positive center. Nevertheless, the traditional probability theory is widely applied to determine the probability value of events in practice, which is theoretically evidenced by "it is concluded that two events have the equal probability value as long as no sufficient argumentation can prove the probability of an event is greater than that of another event".

The statistical definition of probability theory is:

When the number of occurrences of the random event **A** in **n** repeated experiments is set to **nA**, the frequency **nA/n** swings around a value **p** steadily if the number of experiments **n** is large and the amplitude of swing becomes smaller as the number of experiments **n** is increasing, so the number **p** is the probability of the random event **A**, expressed as **P(A)=p**.

2.2.2 Types of Lotteries

Currently, lotteries can be generally categorized into the following three types:

1) **Probability Games (Lotto)**

   Powerball, Union Lotto, 6/49, 3D, 5D, Seven Stars, 5/22, etc.

2) **Guessing Games**

   Football Lottery, Basketball Lottery, China Football Lotteries, Virtual Gaming Quiz, etc.

3) **Instant Games**

   Scratchie, Quick Draw, etc.

2.2.3 Operating Model

The lottery industry around the world are currently operated under three models:

1) **Sale by Proxy (entrusted by the government)**

   Taking France as an example, the French Government established the French National Games Group, a lottery issuing company supervised by the Ministry of Budget, Public Accounts and Civil Administration of France on behalf of the French Government.

   Unlike France, in Spain, national lotteries are operated by Spanish La Primitiva under the supervision by the Ministry of Finance and the Economy (a government institution whose major staff are civil servants).

   All US lottery operators operating as a lottery institution or lottery company under the state governments' rules and regulations. The United States does not have a unified national lottery and lottery issuance is determined by each state. Lottery legislation is legislated in state level and the state governor designates several members to form the lottery committee. The use of public welfare fund raised by the sale of lottery tickets is managed by the fund management committee according to relevant state laws.

2) **Enterprise Contracting**

The National Lottery in the UK is a typical example of this model. Such lottery tickets are approved for issuance by the British Parliament, raise funds for public welfare undertakings, and issue business licenses to the successful bidders in the form of open tendering.

3) **Licensing**

In many countries in Europe, according to their national needs, the government has issued lottery licenses. The license holders include both state-owned companies and private enterprises.

2.3 Challenges Faced by the Lottery Industry

The greatest challenges faced by today's lottery industry is always security, transparency, and efficiency. In general, the lottery betting, drawing and prize claiming process usually operated like this:

There are many problems exist in such process:

1) Lottery players need to buy lottery tickets at sales outlets, the sale of the lottery ticket is constrained by the geographically availability of the sales outlets;

2) When betting, the lottery buyers and sales outlets are prone to disputes over the printed number selections;

3) The drawing process needs to be conducted in the presence of third-party notaries and the credibility of winning numbers is subject to, and endorsed by the reputation of the third-party notaries;

4) The prize calculation is completed in a concentrated central system, so the creditability of the amount of the prize is also subject to, and endorsed by the reputation of the third-party notaries;

5) The guarantee of payment and commissions to the lottery winners and sales outlets are endorsed by the government at a national or state level;

6) All data is backed up on an independent hard disk before the result is made public under the supervision of the notary, that is, the security of all data being saved is also rely on the endorsement from the third-party notary.

Next, let's look at the centralized IT system generally adopted by the lottery industry corresponding to the operating flow illustrated previously:

Such centralized IT system has the following vulnerabilities:

1) Lottery buyers may argue the printed lottery numbers are inconsistent with those they originally selected. That is, the centralized IT system is unable to curb the acts of disavowal;

2) It is impossible to completely avoid the collusion of insiders and notaries from modifying the winning results;

3) It is possible that the notary was bribed by players;

4) Insiders may have an opportunity to alter the data when or before it is being sealed;

5) The computation of prizes is not transparent;

6) The data may be altered if the servers are attacked by hackers.

In addition, in the circulation of lottery tickets consumption, the lottery operator usually sits on the center or top-level of the hierarchy, tickets are issued to lottery players via agencies, the whole operation is centralized in multiple levels. The opaque and centralized nature of such operation resulted the credibility of issuing subjects, winning subjects, issuing subject matter and operating rules are all in question, because it is unable to make each element of the circulation transparent, fair and fully trusted under the system.

2.4 What is the Blockchain?

2.4.1 Blockchain Overview

The blockchain technology is an innovative application of modern computing technologies including distributed data storage, peer-to-peer network, consensus mechanism, and data encryption. To be specific, the blockchain technology is a new distributed computing architecture which validates and stores data through a chain-like data structure, it enables trustless nodes to generate and update data through distributed consensus, and guarantees safe access and transmission of data by means of data encryption, data are operated on the blockchain by the use of the smart contracts written with automated scripting language.

Broadly speaking, blockchain is a highly-reliable distributed data storage system maintained by multiple parties without a centralized authority. Key characteristics of the blockchain include: first, all the parties on the network can participate in bookkeeping; second, multiple participants independently validate the information without a centralized authority; third, blocks created are cryptographically sealed in the chain, this means that it is impossible to delete or alter already created blocks.

In practice, blockchain-based systems can enable sharing, consensus, and mutual responsibility of information among all participants, so as to help businesses getting away from the constraint of traditional bindings or relying on the endorsement from a third-party, parties can exchange the value directly without the middle man. Such characteristics of blockchain can effectively reduce transaction costs, improve transaction efficiency and consistency. Meanwhile, the blockchain is also able to protect data privacy while making information public available, safeguard individual's interests but also enjoy the benefit of consensus based mutual decisions.

2.4.2 Characteristics of Blockchain Applications

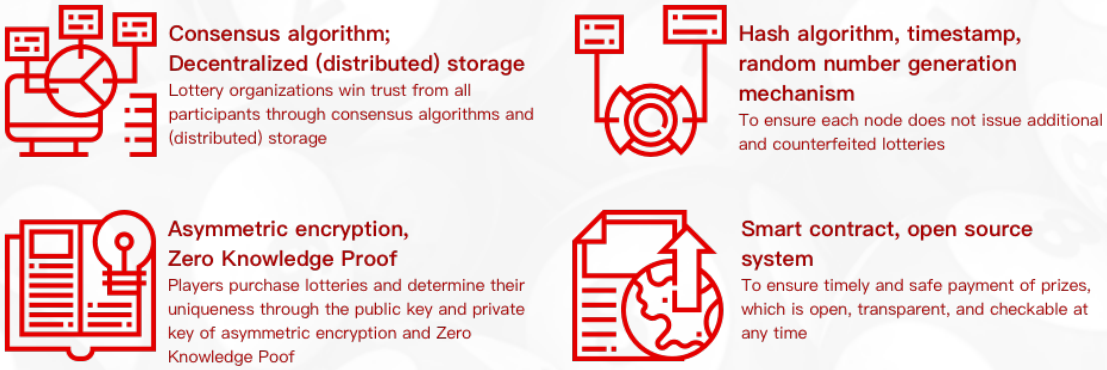


Figure 2-3 Characteristics of the Blockchain Applications

At present, the concept of blockchain has aroused a wide range of attention in every industry, because it revolutionized the information-based Internet into a value-based Internet by converting the computable information into trusted value. This allows the blockchain technology to be increasingly adopted by the highly trusted business applications through the disruption of the traditional centralized information technology architecture.

To be specific, the characteristics of blockchain technology in all aspects of its applications are summarized as follows:

1) Use of the blockchain system: Information and data generated through various encryption techniques cannot be disavowed or falsified;

2) Operation of the blockchain system: The system is operated and managed in accordance with the provisioning of smart contracts are free from control by any centralized authority;

3) Development of the blockchain system: All designs and source codes are open sourced and transparent to the public scrutiny, in which case the developers are less likely to hide the back door;

4) The blockchain is divided into the public blockchain, private blockchain, and consortium blockchain according to the rules of node access.

2.5 Revolution of the Lottery Industry Impacted by Blockchain

The blockchain's innate technological advantage happens to be the principle capability that is urgently needed for the future development of the lottery industry. It should be noted that the application of blockchain technology in the lottery industry should adopt a "license" based model and it will make the lottery operations securer, more transparent and more efficient.

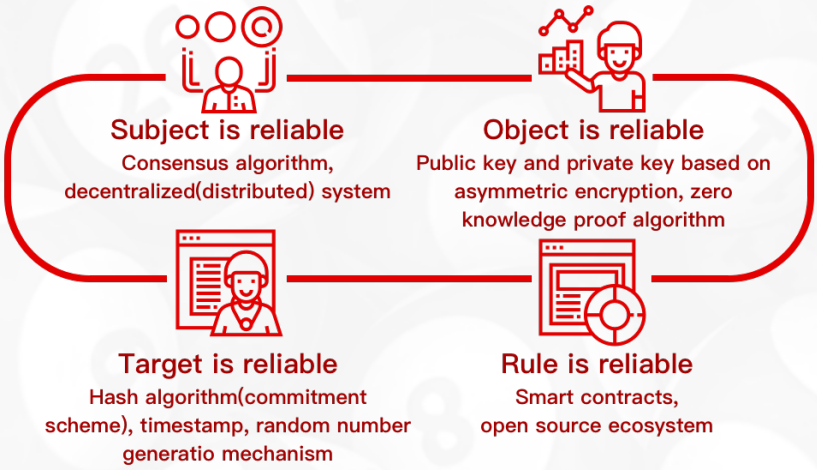


Figure 2-4 Blockchain Matches the Lottery Industry

2.5.1 The Application of Blockchain Technology Will Make Lottery Safer Than Ever

Taking the existing operating model of a national-level lottery operator as an example, because the blockchain technology itself is trusted, we can setup a consortium-chain connecting provincial sales outlets, central issuing agencies, national and provincial supervisory authorities, and local notary agencies all together, and safe-keeping all or part of the original data generated from various lottery games in the ledger in a real-time fashion in accordance with various lottery regulatory requirements.

In aspect of data storage, the application of blockchain technology can realize a barrier-free, error-free and non-interventional identification and verification system as well as information sharing, it also secures the reliable, error-free and automated running of the rule based lottery operation defined by the lottery industry. For example, the decentralized consensus network can secure the credibility of the lottery issuers (sellers); the use of public-private key and zero-knowledge proof under asymmetric cryptography algorithm can secure the credibility and identity of the lottery players; the application of hash algorithm, timestamp and random number generation mechanism can secure the credibility of the lottery tickets (either in the electronic form, or digital fingerprint of a traditional lottery ticket).

2.5.2 Blockchain Technology Enriches the Lottery Games

Along with today's rapid development of mobile Internet and other new communication technologies, new digital channels dominated by smartphones have gradually captured the consumers' attention along with the rise of new interactive games mainly distributed via digital channels. Unfortunately, today's lottery games developed under the traditional IT system are not equipped into such change. In the other hand, the outbreak of private lottery games along with the rapid development of the Internet, indicating that consumer demands in this aspect are not been well served yet.

If a public blockchain participated by all does exist, and all transaction data can flow in the ledger in a fair fashion, under such as system the social lottery games which is not possible under current system can be developed, whereby the participants can interact with each other fairly, so the game can be far more interesting. To summarize, the blockchain technology can introduce social games, virtual games and many others into the lottery space and help to unleash a wide range of new possibilities for the development of new lottery operations.

2.5.3 Blockchain-based Lottery System Will Achieve Complete Fairness and Transparency

As a nation's social welfare development projects, countries across the world raise billions of dollars of capital through lotteries each year. However, centralized lottery system has issues like non-transparency, susceptible to manipulation etc. Although endorsed by a country or national government's credibility, it is undeniable that the fairness of lottery operations is still doubted by many lottery players.

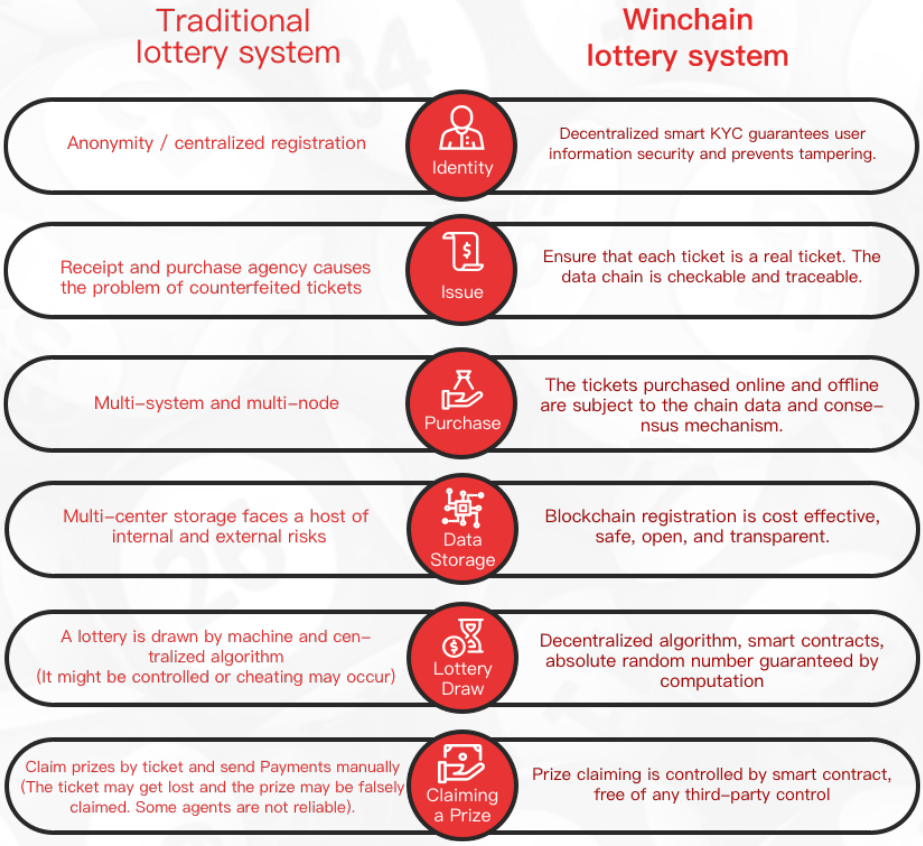


Figure 2-5 Comparison of Winchain and Traditional Lottery System

The blockchain technology and the benefit of decentralization it brings, if applied appropriately, can allow anyone with a blockchain wallet to issue his own lotteries in accordance with the laws and regulations, so as to raising public funds and taxes for the benefit of the country. The winning numbers are calculated on the basis of the smart contracts, no party can control or forgery the results. On the other hand, the lottery game's source code is open sourced which allows anyone to inspect which means it is impossible for the lottery operator himself to predict or set the winning numbers in advance without being caught. Such design improves the fairness of the system as the data is open accessible and hold by the participants who can perform all-around supervision before and after. In addition to this, the supervision and notarization authorities can also perform their duties even better, thus fix the problems of traditional lottery system such as centrally controlled by someone and always being criticized of non-transparent.

The blockchain technology is destined to change today's lottery distribution system, and may contribute to the qualitative change of the traditional lottery system, so as to bring the complete fairness and transparency into the industry.

2.5.4 Blockchain Technology Democratizes the Access to Lottery Issuance

Traditional lottery tickets can be purchased only in local currency due to geographical limitations. However, digital currencies, or cryptocurrencies can be stored anywhere in the world, which mean players can play blockchain-based lottery games from anywhere in the world as long as they have access to the Internet, even in areas where the banking facility is not accessible.

For example, we generate the lottery contracts containing lottery wallet address using the contract generation module of the wallet application, write the lottery contracts into the ledger as transaction data, and issue the lottery contracts through the running of the wallet. After the player put his bets on the targeted lottery contracts, he will then cash the reward through the cashing module of the wallet if he wins. We could even achieve the automatic reward payment through the development of corresponding smart contracts. The blockchain technology will make lottery issuance much more efficient and convenient.

Winchain is competing against the International Gaming Technology (IGT) from the US, IGT is a lottery system service provider and operator with an annual income of over $30 billion. IGT provides technical services on lottery system to many countries in the world. However, it is generally believed that a decentralized lottery system will become the new standard due to its superiority in terms of cost, efficiency, security and public credibility. The foundation of the Winchain project is the answer to the industry's needs in recognition of the team's in-depth blockchain technology knowhow and unmatched industry exposure.

III. Winchain System Architecture

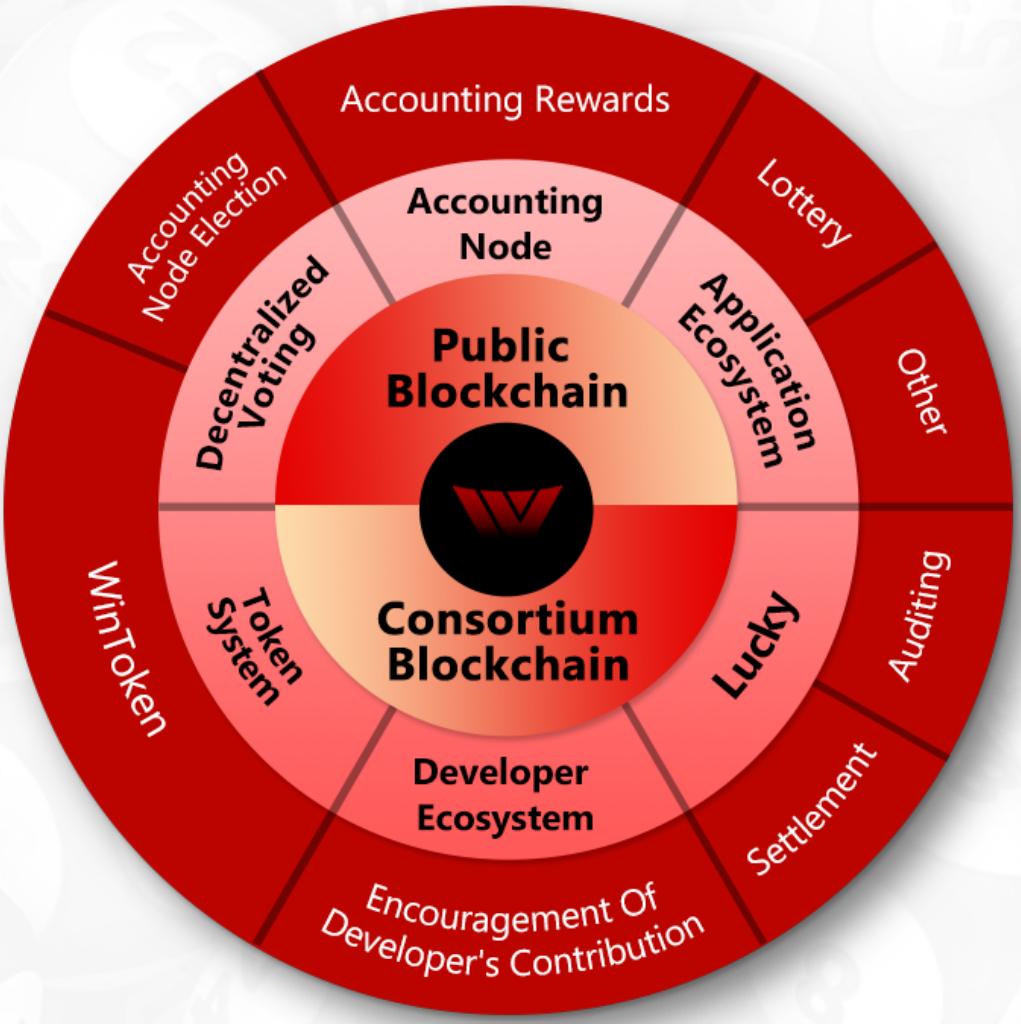


Figure 3-1 Winchain Dual-chain Framework

3.1 Smart KYC Account Management System

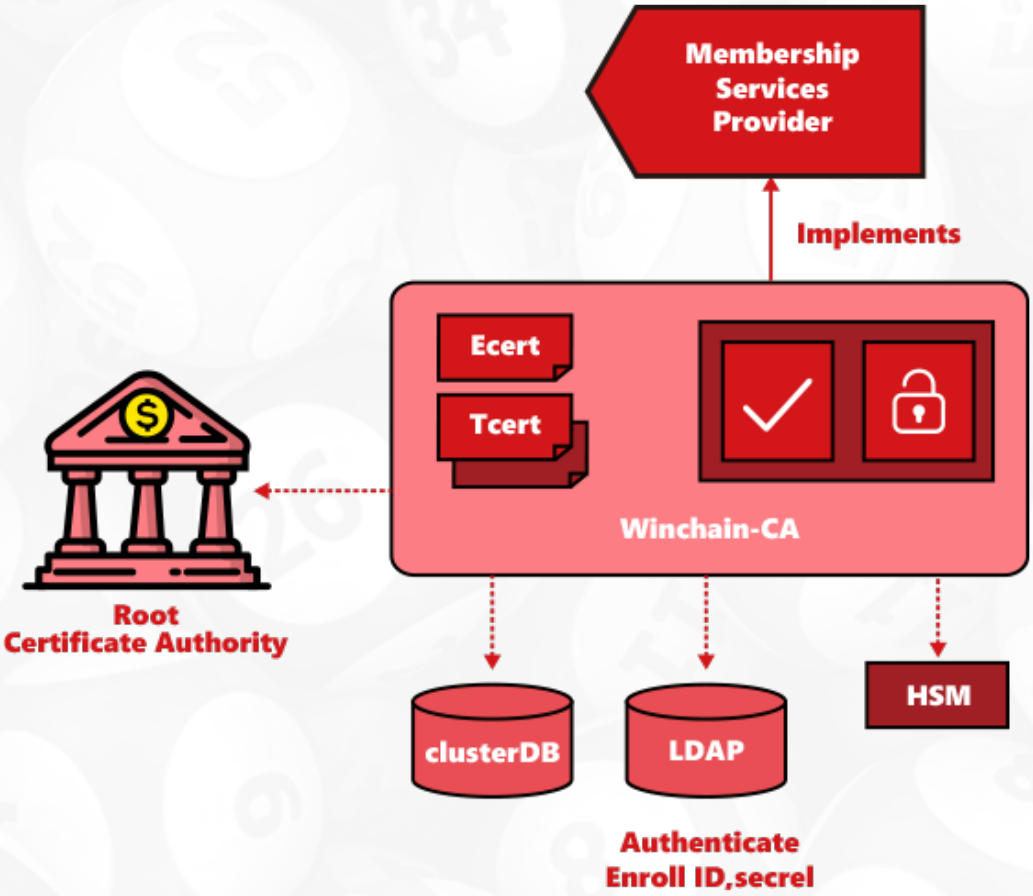


Figure 3-2 Digital Certificate Issuing System

3.1.1 Decentralized User Account System

Account is the passport and identification of a user in the Internet world. Traditionally, the information of user accounts is stored in a centralized server, whose security and credibility are the key to the security of the user accounts. However, it is highly possible that the centralized server can be hacked and user information could be stolen and exposed at any time. Meanwhile, the safety of the user accounts is dependent on the service providers who own the centralized server, the service providers are also facing risks due to various threats driven by politics, economy, competition, profit and many other factors. In the lottery system, due to the diversity of user accounts (including real name lottery, semi-real name lottery, and anonymous lottery etc.), lottery player's identity verification, customer data storage, as well as authentication and confidentiality of lottery winners have imposed strong demands for security, flexibility, confidentiality and anti-fraud of the user account.

What's most important of blockchain technology is its decentralized architecture that autonomously delegates the responsibility of account management to users themselves. Unlike the centralized account system which totally relies on the central server to process and store user information and identities, Smart KYC account management system keeps these into the blockchain network where user identities and information are fully controlled by the users themselves. The decentralized account system hands the job of the user identification over to the blockchain network. The blockchain network's nodes located all over the world safeguard the security for the whole system. There is no special authoritative node exists in the system and every node is treated equally. As the equitable "centralized service providers", the smart contracts replace the traditional centralized service providers and realize the open and fair "autonomy" of decentralization organizations.

By creating a unique token address on the blockchain and using the address as the exclusive marking of user identity and asset ownership, every asset registered on the blockchain has the unique property of asset ownership. Only the private key holder possesses the usage right and ownership of the assets. The digital signature helps achieve the possession and transfer functions of identity acquisition, identity authentication and asset ownership of users.

3.1.2 Trusted Identity Authentication

There exist various problems throughout the process of lottery consumption, i.e., loss of lottery tickets, ownership of lottery tickets bought by proxy, safety of cashing in, and so forth. The root cause rests with the incredibility of user identification, so the uniqueness of matching between user account and identity need to be further enhanced.

Smart KYC system carry out the process of user identification over the blockchain and takes the token address as the only identity and asset identification of a user. The uniqueness validation will be conducted upon the consumption and cashing in of the lottery. Controlled by the smart contract, no intermediary agent participates in user verification and asset transfer validation. This realizes the credibility verification of user identity throughout the whole lifecycle of the lottery consumption.

3.1.3 Multi-Scenario Support

Winchain is a national blockchain-based lottery system adopted by an African country at first. As different countries have different policies and regulations and there are many different lotteries, the requirements for user identity vary from country to country. The Winchain Smart KYC system is a complete smart user identification system. Whilst ensuring the security and reliability of user identity and authentication through the blockchain technology, Winchain can also meet versatile demands from various countries for identity authentication.

On the other hand, the lottery tickets can also be traded by lottery players themselves. After buying lottery tickets, the tickets held by the lottery players will be treated as assets on the blockchain, whereby the player can transfer his/her tickets to others through virtual asset trading and get the transaction registered on the blockchain. This ensures the reliability, security, and anonymity of digital asset transfer.

3.2 Blockchain-based Data Management System

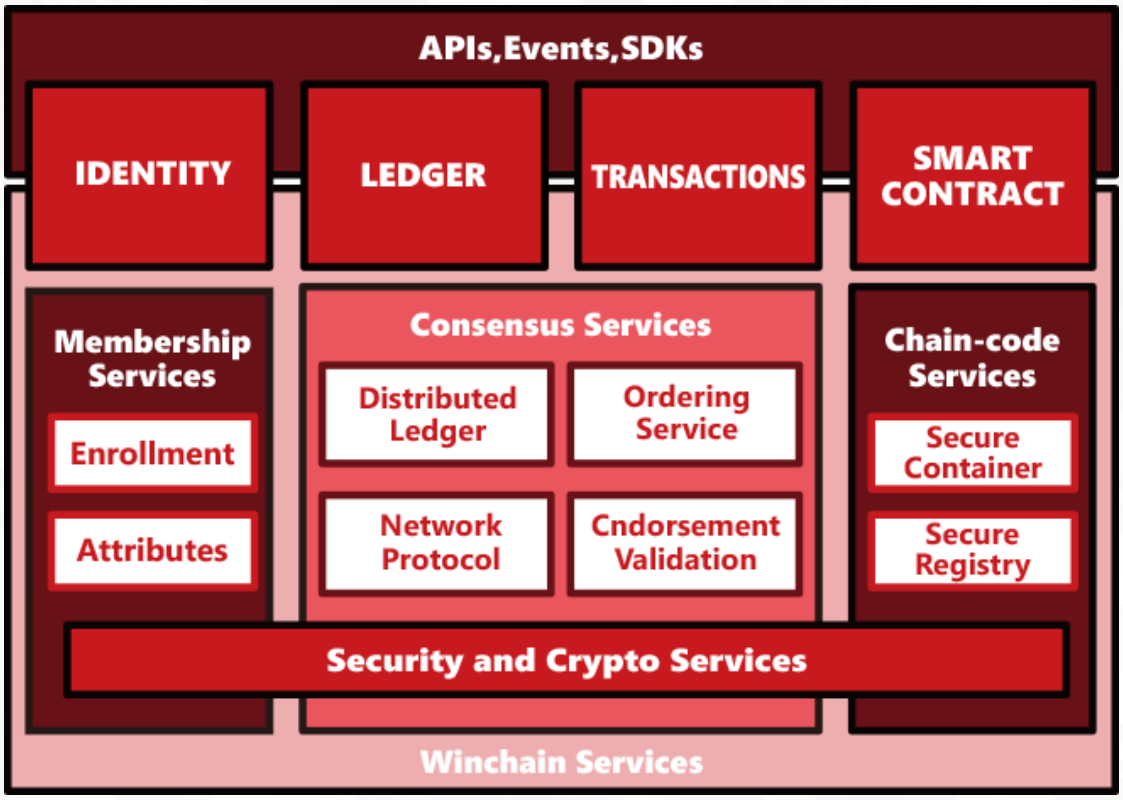


Figure 3-3 System Modules

3.2.1 WinData Lottery Data Storage Management

In a Winchain lottery system, users can instantaneously view their records on the blockchain network after buying lottery tickets. The purchase records are recorded in the blockchain network, and therefore cannot be falsified or denied. Both Winchain's official platform and its partner's platforms provide the blockchain data enquiry functions. Users can trade via the platforms or directly on the blockchain, thus ensuring the fairness and security of the lottery sale.

The lottery data storage management system based on blockchain is the core system of Winchain at the stage of buying lottery tickets. Based on this system, all countries and corresponding Winchain service providers do NOT need to care about the right of ticket issuing and storing, what they only need to do is just to provide the data enquiry functions for users by calling the public blockchain data of the Winchain network. In this way, they can save huge costs for system development and trust building, and focus their energy on lottery sales and lottery game itself.

3.2.2 WinSell Sales Data Decenralized Storage System

The classical lottery sales channel involves numerous multi-level agencies and channel management organizations, and the whole chain including a complicated structure made of regional agents, subagents, point of sale terminal, notarization terminal, settlement terminal, etc. Each level need to make a lot of effort on sales and trust building, and take a slice of share from the lottery's sales revenue. In different countries, about 40~70% of lottery sales revenue goes to branches and sub-branches no matter whether they are welfare lotteries or sports lotteries. The actual profit of the national operator has been reduced significantly, not to mention the fund contributed public welfare are also largely discounted.

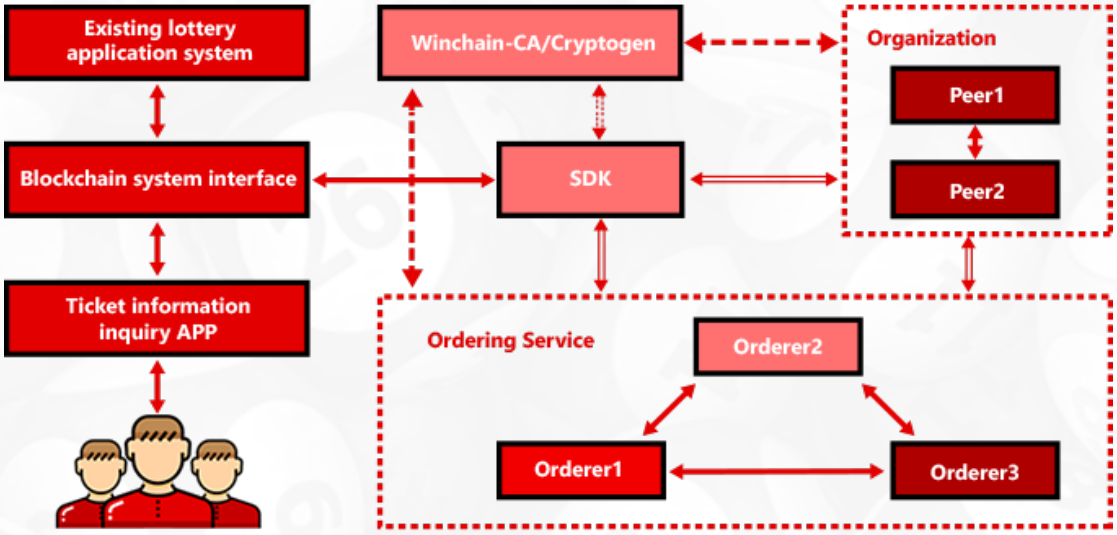


Figure 3-4 Lottery Token Application

With the sales data stored on the Winchain, two innovations are made:

Under traditional process, daily sales data will be burned into a CD. A number of notaries from different departments will copy the data to the CD and save the backups at the notary public office, regional lottery sale center and supervisory authority, in order to preventing insiders from modifying the database, and preventing outsiders from malicious operation taking advantage of system loopholes. Such process is very inefficient and requires a lot of human resources. Meanwhile, it hardly achieves the purpose of building complete trust as the risks were simply transferred from lottery institutions to notary public offices. Many cases also indicated that this procedure is not secure enough.

WinSell sales data decentralized storage system provides a decentralized bookkeeping system for joint bookkeeping, it removes the necessity of tedious manual works for trust building. In addition, the system can avoid human errors and system related risks. Public, transparent and decentralized ledger system can guarantee the security and absolute credibility in the course of sales data (evidence) storage.

3.2.3 WinPri Prize Management

Under traditional practice, prizes are claimed offline or via a centralized prize distribution network. Prizes are stored in a central location and claimed after the system verification is complete. Manual verifications are involved when issues like tickets were stolen, miss or forgotten to claiming prizes arise. Such process intensifies potential risks and disputes over the cashing in step, and reduces the efficiency of prize claiming. Meanwhile, the existence of multi-hierarchy organizations taking a portion of the prize also reduce the system's transparency. Trust building has been the most important issue in the lottery industry ever since.

WinPri prize settlement system will save lottery ticket's purchase records in the blockchain and connect to other distributed ledgers of the system, including user identity and results from the oracle. After receives the lottery drawing results, WinPri's smart contract of settlement will automatically settle the prizes, and release the prizes to the winner's identy address on the blockchain instantaneously. This process is free from control of any centralized body or third-party agencies, thereby ensuring that the cashing process is absolutely open, fair and transparent.

3.3 Transaction Processing System and Oracle

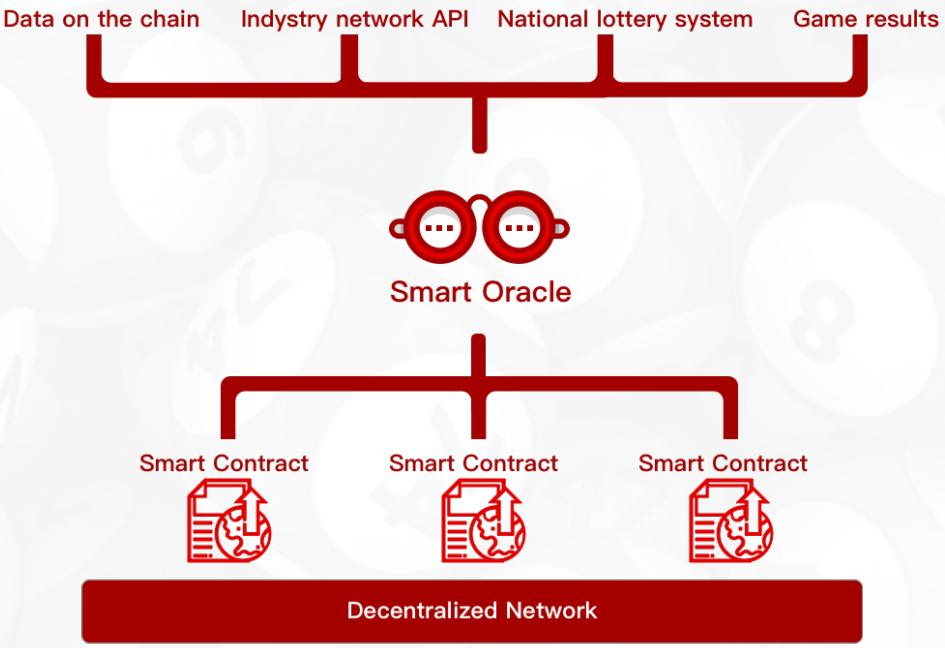


Figure 3-5 Winchain Oracle

3.3.1 Absolute Random Number for the Lottery Draw

The absolute random number generation has always been an interesting topic in the technical field. There are many programs can generate the pseudo-random numbers, however, in theory, these programs can be hacked or modified because they were based on a centralized system. For the online lottery in particular, players have concerns about the security and reliability of its random number generation all the time.

The emergency of the blockchain technology brings us a new way of thinking in terms of how to generate random numbers. The Bitcoin network and many other decentralized networks secure the operation of the whole network via distributed bookkeeping. Once the network reaches a certain level along with the increasing number of its nodes, the whole network will establish a very stable security. The existence of multiple bookkeeping nodes guarantees the fairness of the whole network unless someone established absolute control over the network's overall computing power. Since the Bitcoin network is quite mature and in a very large scale, we developed a unique mechanism to generate the absolute random number relied on the robustness and decentralized nature of Bitcoin's blockchain network. This practice can be calculated with different, but transparent algorithms according to the hash value of Bitcoin's blocks minable in a period of time in the future, so an absolute random number can be generated from the Bitcoin network and can thus provide absolute random factor for various lottery games. The transparent random number generated under various rules can be obtained through a random factor, therefore secures the absolute fairness and transparency of the lottery draws.

3.3.2 Decentralized Oracle Under Multi-point Tendency

For those traditional lotteries and sports lotteries such as the football lottery for the World Cup, the prize must be drawn according to external information. The smart contract cannot execute the contractual contents and handle the work automatically until the match results are made available, this requires an Oracle who connects the real world and the virtual world, and provide data for the blockchain in order to secure the operation of the smart contract. However, a single oracle may get its data from untrusted sources. To find a optimal solution for the lottery industry and guarantee the accuracy and reliability of external information, we propose a mechanism of decentralized oracle under the multi-point tendency. The source data of oracle is retrieved from multiple credible nodes, and through the token incentive mechanism, users of the Winchain network choose volunteers to participate in the judgment. When some credible nodes showing different results, the participants will perform a multi-party verification. This practice of multi-point data plus multi-point verification can ensure the security and reliability of data coming from the oracle, which is very important to the openness and transparency of any lottery system.

3.4 Developer Ecosystem

As a national-level decentralized lottery system, the developer ecosystem is an important part of Winchain. The strong support from developers is conducive to the development of the Winchain ecosystem. As time goes by, the traditional lottery games gradually show that they can't cope with the ever-growing demands from lottery players who are desperately looking for better games and better way of playing.

Under the blockchain network, developer ecosystem becomes more open and diversified. As an open, national-level, and blockchain-based lottery technology platform providing open applications, multiple ways of playing for any country, lottery operator, and individual player to choose from, is one of Winchain's primary works.

By deep collaborating with lottery operators from multiple countries, new lottery games are expected by every lottery operator in the industry. The decentralization and transparency brought by the blockchain technology are warmly welcomed in the lottery industry and almost all countries are investing on researching how blockchain can be applied in the lottery industry, and the revolutionary changes in the lottery industry are broadly expected.

3.4.1 A Platform for New Lottery Games

In addition to traditional lottery games, the blockchain-based game lotteries constitute an integral part of Winchain and enjoy the incomparable advantages of transparency, openness, and fairness. The traditional lottery games can be directly migrated to Winchain ecosystem. The developers are also encouraged to provide various new games, especially the those blockchain-based lottery games.

The decentralized Winchain system provides the blockchain-based lottery system and it's technical services to many countries and its lottery operators. Any game migrated to Winchain have an opportunity to serve tens of millions of international players, the developers can therefore benefit from generous returns from a large base of global players.

Winchain will provide a complete and user-friendly API interface for game developers to take advantage of a billion dollar lottery market by developing games on the Winchain.

3.4.2 Access Token

Lottery games, as a kind of game of chance, have diversified rules. Each game must go through system auditing and then be given access to the corresponding interfaces. Many games require a preset prize or base prize due to different game rules.

The access token is a basic mechanism of Winchain developer ecosystem. Developers are authorized to use the interfaces and submit new games only if they have purchased WosToken and put it into custody. After the code review and inspection is past, the games will be made available to the official channels and tens of millions of lottery players all over the world.

3.4.3 Incentive Mechanism

For those games connected to the Winchain, developers can set the proportion of returns using smart contract, and get returns from the sale of the lottery games accordingly. Winchain encourages developers to jointly develop the secured, transparent, reliable and decentralized lottery game platform supporting multiple ways of game play.

3.5 Winchain Ecosystem

3.5.1 Blockchain Revolutionize Lottery's Control and Operation

Unlike traditional operating model of lottery games which has multiple levels, multiple networks, multi-sectoral coordination and manual operation, Winchain provides a efficient and flexible control and operation mechanism, to support the underlying technology architectures of lottery consumption, recording, evidence, drawing and claiming. Meanwhile, it is also compatible with different games and organization's management models, in order to be easily accepted by different lottery operations from different countries.

3.5.2 New Lottery Games and its Open Ecosystem Will Reform the Industry

As mentioned above, the global lottery industry is expecting new technologies to bring new form of games, in hope of further expanding the new ways of playing lottery games and attracting the players' attentions while enhancing the transparency and fairness of the lottery industry. Winchain lottery game platform is an underlying technology system which encourages developers to develop games in a decentralized manner, share profits based on the smart contract and promote the technology base for the industry jointly, and eventually make the whole industry grow enormously.

On the other hand, the technical revolution brought by the blockchain creates more possibilities for the lottery industry. The brand-new blockchain-based lottery games to be developed with the blockchain technology will bring more surprises to the industry.

3.5.3 Supported Scenarios

Figure 3-6 Application Scenarios of Winchain

Winchain's decentralized lottery underlying system supports several application scenarios, including:

"Classical lotteries"

1) Probability games (Lotto): Powerball, Union Lotto, Lotto 6aus49, 3D, 5D, Seven Stars, 5/22, etc.;

2) Sports lotteries: e.g., quizzes of football and basketball events, E-quiz, etc.;

3) Chess games: Texas hold'em Poker, etc.

"New blockchain-based games": e.g., the transparent and fair virtual asset lottery integrated into various blockchain-based games such as Crypto Kitties.

In combination with existing partners and industry resources, and based on our accumulated expertise in the blockchain technology, we are fully convinced to gradually develop Winchain into an international leading service provider of blockchain-based lottery technology. The blockchain-based lottery technology will certainly become a new generation of standards for lottery underlying technology replacing the traditional lottery systems of all countries.

3.5.4 Big Data

Blockchain-based lottery is characterized by its openness, transparency, diversified rules and comprehensive data. Parties in the Winchain network can view and share lottery sale data, participating status of the games, and service usage conditions in various places. Collaborating with teams from various countries, Winchain will conduct the big data analysis using artificial intelligence, to optimize the lottery operation, adjust lottery playing rules accordingly, and further improves the superiority of the blockchain-based lottery system.

3.5.5 Public Welfare

Lottery has been always closely related to the public welfare and it comes with the property of taking social responsibilities. The utilization of fund raised by traditional public welfare are always been criticized of its transparency . Winchain will include a decentralized public fund utilization platform, through which the lottery operators from various countries can enjoy an open and transparent utilization of fund from public welfare lottery thanks for the blockchain technology, so to indeed make the best use of every capital been raised.

IV. The Winchain Open Source Technology Foundation

4.1 Introduction

Winchain Open Source Technology Foundation Limited ("Winchain Foundation") is an independent legal entity registered in Singapore. It is team up by senior experts from the lottery industry and blockchain technology field. Winchain Foundation's vision is to promote the application of blockchain technology into the lottery industry through developing the blockchain-based open source underlying lottery system with partners around the world.

The Winchain system is a dual-chain based lottery technology platform composed of Public Blockchain and Consortium Blockchain including features like lottery tickets issuing system, data storage system, token system, lottery drawing system, prize claiming system, smart contract system, and open lottery gaming platform. By establishing a decentralized lottery system and introducing decentralization, unmodified data, system stability, smart contracts and other features into the lottery ecosystem, Winchain is committed to helping lottery operators and lottery system providers around the world to develop Winchain–based lottery system according to individual needs of each partners, and ultimately contribute to the prosperity of the global lottery industry.

Winchain Foundation will coordinate industry resources around the world to accelerate the development of this open, transparent, safe and stable blockchain-based underlying lottery system into a new world standard. In this case, more decentralized lottery games can be developed so the value of blockchain technology will be realized in the lottery industry. Winchain Foundation will create a brand-new blockchain-based lottery gaming ecosystem and it will be far more efficient and transparent than any other solutions envisaged by human society in the past.

Figure 4-1 Winchain Organizational Structure

Short-term Goals：

- In April 2018, Winchain will establish the Blockchain Lottery Research Institute joined by the China Welfare Lottery Issuing and Management Center, the Sports Lottery Management Center of China, and many industry experts to promoting the application of blockchain technologies into the lottery industry.
- In 2018, Winchain will join the Winchain Eco-Country Lottery Company in Africa to try to connect the first national blockchain lottery system.
- By 2018, Winchain will collaborate with 3~5 companies to land the blockchain-based lottery system in different countries. Winchain is committed to develop the new world standard in the lottery industry and push the whole industry towards a fair, open and more efficient place.
- At the beginning of 2019, Winchain will complete the application of the national blockchain lottery system and issue the world's first blockchain lottery.
- By 2019, Winchain will setup blockchain-based lottery systems in 5~10 countries and complete the development of blockchain-based lottery gaming platform with developers and companies in the ecosystem. Accordingly, Winchain could provide various new lottery games to lottery operators from different countries and further improve and finetune the blockchain-based lottery system.

4.2 The Winchain Ecosystem

Winchain Open Source Technology Foundation

Winchain Foundation is a non-profit organization registered in Singapore. As the main operating entity, Winchain Foundation is commissioned to promote and supervise the development of Winchain ecosystem, to coordinate industry resources from other countries, and to boost and facilitate the openness and transparency of the blockchain-based lottery underlying technology to be accepted as the industry standard of all countries, so to unleash the real value of the blockchain technology.

Victory Game Challenge

The Silicon Valley based Victory Game Challenge is the main operating company of Winchain. The company is team up by senior blockchain technology experts and business experts from the lottery industry, it provides new blockchain-based lottery underlying technology and services to a global customer base from its subsidiary offices around the world. Winchain will develop the global service market of the new lottery technology and create the trillion-dollar ecosystem from its strong Silicon Valley based R&D operations.

Blockchain-based Lottery Research Institutes

Winchain will roll out the establishment of blockchain-based lottery research institutes in collaboration with relevant government agencies of the country it operates. The research institutes will conduct researches on how to best combine the lottery industry with the blockchain technology in its hosting country, so as to make localized improvement and joint efforts to promote the evolution of local lottery industry towards an open, transparent and fair blockchain-based world.

Subsidiary Companies and Global Business Operations

As an underlying blockchain-based lottery system, Winchain aiming to promote the blockchain-based lottery business around the world through replacing or upgrading existed centralized system but still follow the laws and regulations of every hosting country. As of today, Winchain has already set-up a subsidiary company in an African country, Africa to provide the national-level lottery business integration services for African countries, the subsidiary company has obtained the only lottery operating license of the country and its blockchain-based lottery system is expected to be launched in 2018. Meanwhile, the set-up of subsidiary offices in Angola, Southeast Asia and other countries are in the pipeline.

V.Dual-chain Mechanism and Issuance Policy

With many years of lottery technology development experiences, Winchain team is fully aware of the challenges faced by today's centralized lottery system, including the huge loss of trust and revenues due to issues like fake lottery tickets, ticketing issuance failure, cheating during the sale of the ticket; and various mistrusts. Since early 2017, Winchain started applying the blockchain technology into the lottery system and conducted research on the decentralized blockchain technology and the use of its distributed storage, open, transparent and tamper-resistant characterizes in the lottery system. After comparison of public blockchain, consortium blockchain, and private blockchain, it is concluded that the public-chain is best in terms of decentralization but not friendly for high-current transaction applications (such as instant lottery games) and the transaction costs are high; the consortium-chain is better in terms of high-current transaction support and cost, but its consortium nodes still fall short of the requirements of complete openness and transparent of data; the private-chain is even worse than the consortium-chain in terms of collaborating under a trustless environment.

Based on extensive experiments and testing, the team decides to use the dual-chain model of "public blockchain plus consortium blockchain" to support the lottery system. The public-chain serves as the base of the bookkeeper election mechanism. Because public-chain is complete open, more people can participate in the node registration and bookkeeping of the consortium-chain and get their rewards accordingly; the consortium-chain functions as the underlying technology platform of the lottery system. Winchain develops a complete suite of decentralized blockchain-based lottery underlying business platform on the top of the consortium-chain, to support the lottery business operations and its surrounding ecosystem around the world. By combining the public and consortium blockchain networks together, the decentralization of rights, bookkeeping, and transactions are well achieved on the ecosystem whilst decentralized lottery games can enjoy instantaneous performance on Winchain at a very low cost.

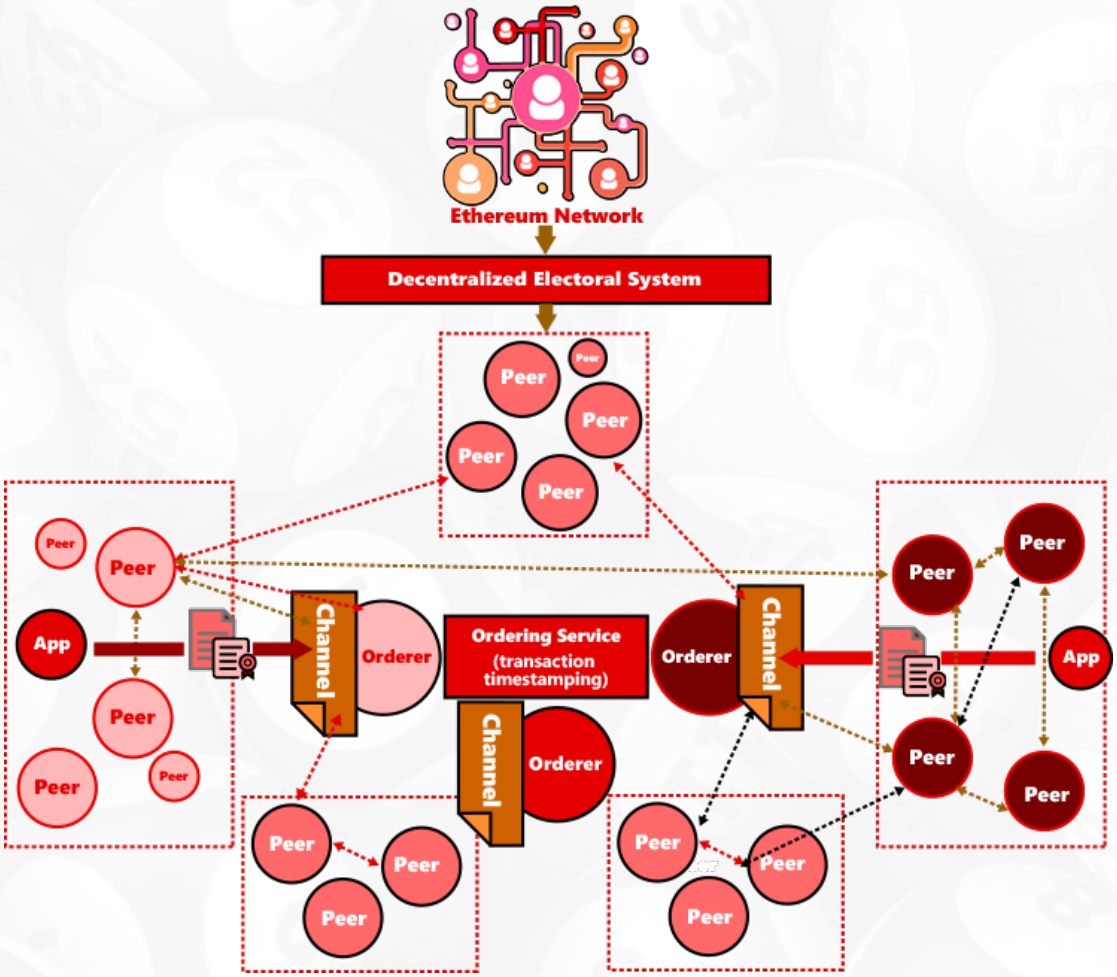


Figure 5-1 Dual-chain Mechanism

5.1 Dual Tokens

5.1.1 WosToken

As the access token of the Winchain system, the evidence of Winchain's rewards, and the base for bookkeeping node's election, WosToken will be listed and available for trading on tier-1 cryptocurrency exchanges.

Access Token

Winchain enables social organizations and government bodies to establish their lottery operations easily. To access the Winchain system, they must hold and put a certain amount of WosToken to custody, which will serve as the access token for lottery operation and bonus pool deposit. This amount of WosToken (been hold and put into custody) will participate the system's incentive (awarding) program.

Decentralized Voting Rights

Winchain innovatively develops the dual-chain system based on its research of blockchain technology for over a year. After reviewed a great number of blockchain projects, Winchain believed such design should benefit most from the decentralization of bookkeeping, equity sharing, and maximum efficiency. Winchain elects a great number of distributed nodes to keep the ledger through decentralized voting on the public-chain, so as to secure the robustness and security of the system. In addition to joint bookkeeping with national government agencies and partners, the Winchain network adopts an electoral bookkeeping approach. Through the WinElc management system, both consortium nodes and other community leaders can be elected as Lucky's management node. The robustness and integrity of the Winchain system is achieved through distributed ledger system, ensure the safe operation of the decentralized system, and making a fee.

On the other hand, Winchain is a decentralized community. Token holders have the right to discuss and vote on major system issues. According to the percentage of their ownership on WosToken, members of the community can perform decentralized voting and comment on major community issues, game evaluation and selection, and system program settings etc. Winchain will provide decentralized voting and decentralized commentary to facilitate the user's exercise of rights.

5.1.2 Lucky

Winchain combines the consortium ledger with the Ethereum ledger. In addition to the joint bookkeeping with government agencies and partners in various countries, the Winchain network adopts the method of electoral bookkeeping, through the WinElc management system to become the system's bookkeeping node and enjoy the incentives from the bookkeeping work.

As the super exchange center of valuable assets and digital assets, government agencies are responsible for joint auditing and relevant asset management. A constant exchange rate of 1 Lucky = 1 US$ is set and distributed on the blockchain network which provides exchange services to facilitate the purchase and exchange of lottery tickets on the Winchain.

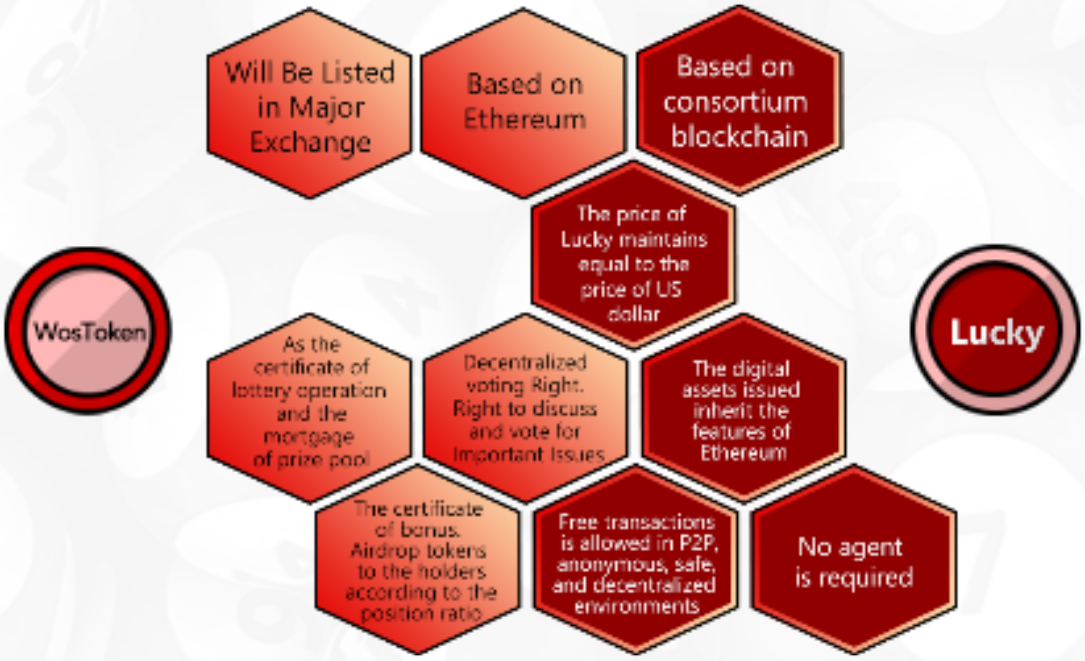


Figure 5-2 Characteristics of Winchain Token

5.2 The Value of WosToken

5.2.1 Bookkeeping Fee

Winchain Foundation will regularly launch decentralized voting via its WinElc system to elect joint bookkeeping nodes on the public-chain. The elected address owner will have the joint bookkeeping right on Winchain, jointly operate the bookkeeping nodes on the consortium-chain, and get rewards of bookkeeping fees for all transactions in the system during its tenure. With the popularization of Winchain in various countries and the growth of its users, the bookkeeping nodes will obtain a very good bookkeeping fee as return; the Winchain Foundation will regularly roll out the decentralized election of joint bookkeeping nodes and publish the details of the nodes in a timely manner, assign bookkeeping rights, synchronize data, and work with community members to safeguard and maintain the fairness and robustness of the Winchain system.

5.2.2 Access Decentralized Lottery Games

Winchain's dual-chain system can not only plug into traditional lottery system and make the whole lottery business running on the blockchain, but also support the complete WosToken-sustained blockchain-based lottery developer ecosystem. Smart contract based lottery system developed for Winchain, and blockchain-based lottery games developed by Winchain's ecosystem partners, all support WosToken holders to directly purchase and exchange lottery tickets using WosToken (subject to individual country's regulation). We firmly believe the blockchain-based lottery is the future of the industry and the increasing demands from players of new decentralized lottery games will significantly increase WosToken's value.

5.2.3 Developer Ecosystem Rewards

The developer ecosystem is an important component of the Winchain platform. Developing decentralized lottery games with Winchain's open API requires developers to submit and put a certain amount of WosToken in custody. This mechanism not only enables developers to write a national level lottery game and get rewarded from its issuance on a national lottery operating platform, but also promote the circulation of WosToken and its use, which is significant in terms of the value proposition for the Winchain ecosystem.

5.2.4 Luckywin Lottery System

Luckywin is a blockchain-based public lottery system designed to encourage users and developers to develop, elect and compete in the lottery games. As a testnet for the lottery games, those best lottery games with best performance and popularity will be recommended to national states and become the national-level lottery games by joining the lucky network. The goal is to develop Luckywin into the largest lottery pool and the most active lottery game developers' community in the world.

The 6aus49 lottery ("Powerwin"), a basic lottery game based on Luckywin will be introduced. Initially, Winchain will airdrop the equities of lottery number selection to WosToken holders according to the number of WosToken hold by them individually.

Source of the lottery pool

From the start, the lottery pool will be initiated with 100 million WosToken. Pool nodes will be setup on both Powerwin and Lucky networks, the bookkeeping fees will be collected into the lottery pool automatically to stimulate Powerwin's operation.

Later on, the revenue collected from user purchasing lottery tickets will also contributes to the lottery pool directly.

The official rules of the airdrop is related to the amount of WosToken hold by Winchain users. The detailed rules are as follows: monitoring the amount of WosToken held by each individual Winchain users. If a user's amount of WosToken exceeds a designated value (i.e., 1000), the user will be rewarded with airdrop. Meanwhile, the number of 6aus49 lottery tickets obtained through the airdrop will not only be related to the amount of the users' WosToken but also depend upon how long he holds his WosToken.

Random Number Generation

The random numbers can be generated through a number of ways. For example:

(1) Oracle scheme: monitoring seven transaction hashes generated through BTC network during the lottery drawing, and then taking the figures obtained through hash mode 49 as the random numbers. The random numbers generated each time will be transmitted to the smart contract through Oracle. After the lottery drawing, the smart contract will automatically transfer the prizes to the winning addresses.

(2) Absolute random numbers: The random number algorithm will be programmed into the smart contract and the random numbers will be generated after the lottery drawing. After the lottery drawing, the smart contract will distribute prizes automatically.

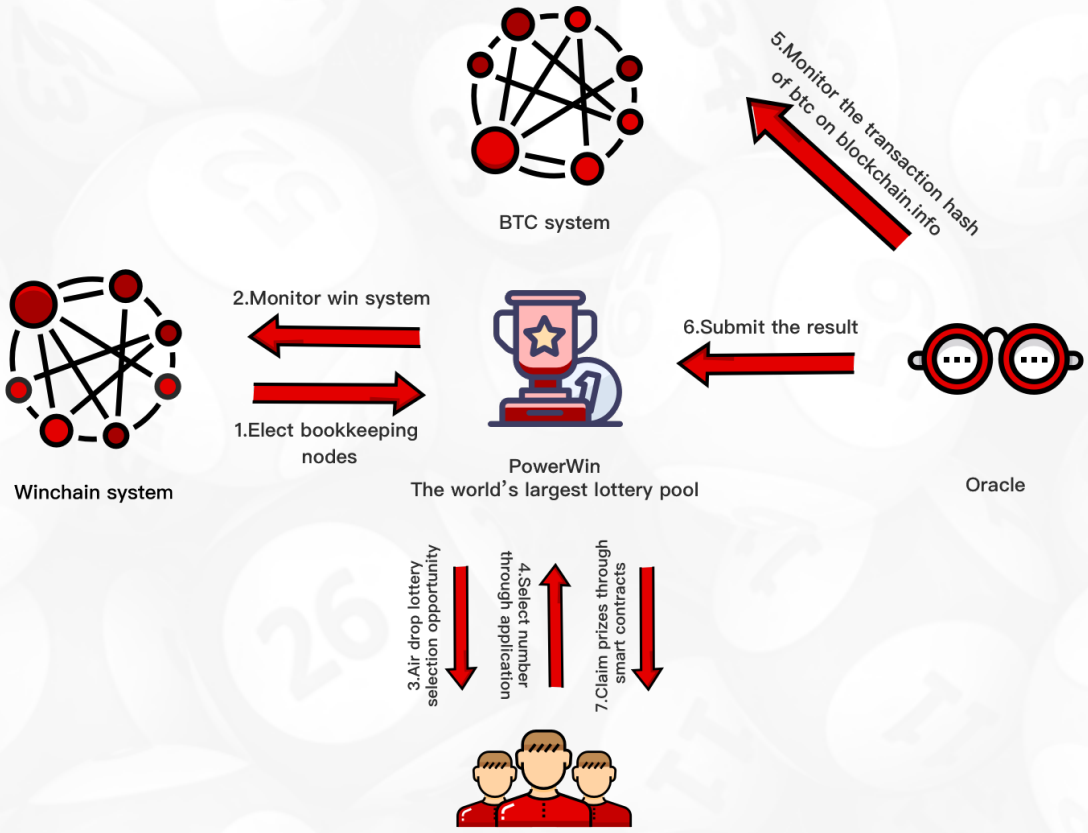


Figure 5-3 Oracle Scheme

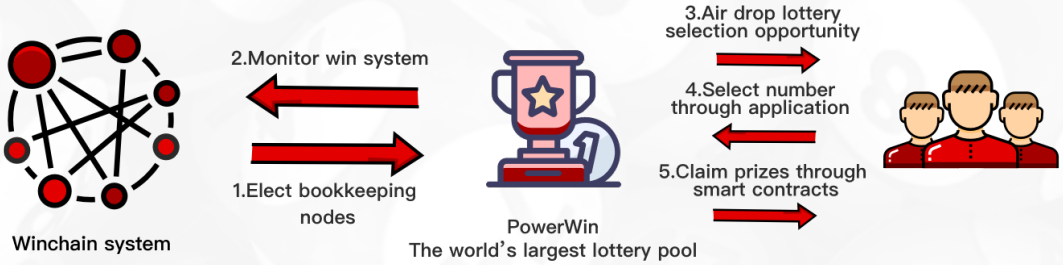


Figure 5-4 Random Number Generation Plan

5.3 Token Issuance Policy

5.3.1 WosToken

As the cryptocurrency of the decentralized global lottery market, WosToken's total supply is 21 billion pieces, of which the convertible amount is 10.5 billion pieces (50% of total supply); and among the remaining 10.5 billion pieces (50% of total supply), 15% of them are reserved for team incentives, 15% are reserved for marketing， business development， and node incentives, 10% are reserved for community support, and 10% are reserved for the developer ecosystem.

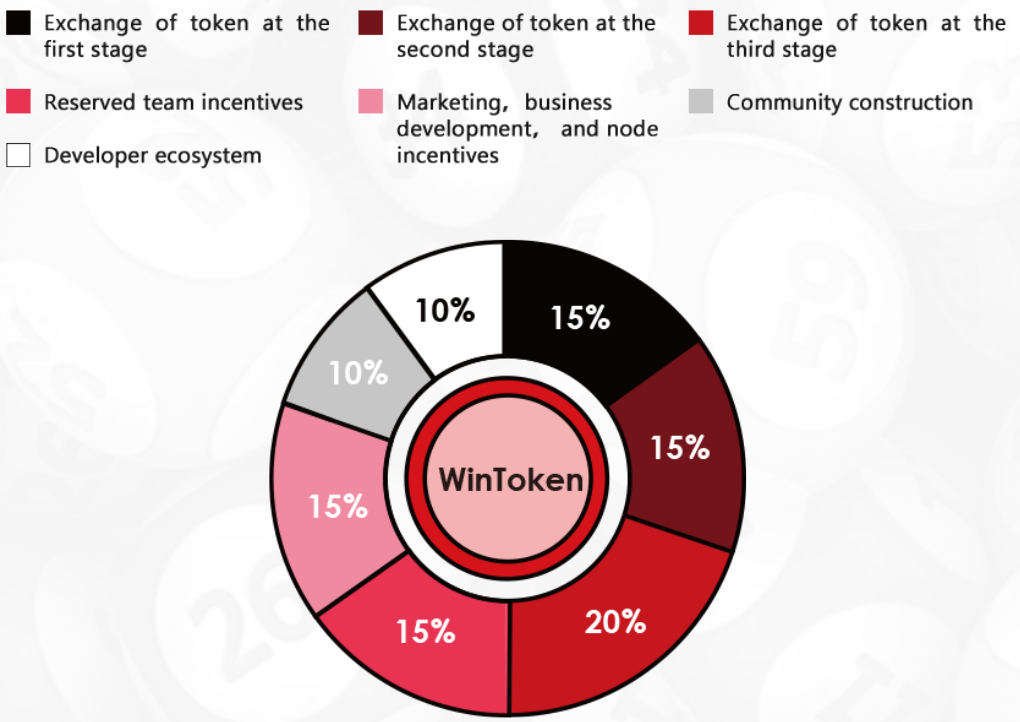


Figure 5-5 Pie Chart of WosToken Distribution

The blockchain industry is a little mixed with dragon and fishes jumbled together. With the experienced team and its industry resources, Winchain will join hands with ecosystem partners to launch the national-level decentralized lottery system in various countries. Winchain will issue tokens in three stages and at each stage, the community members will see the material progress of Winchain in the global lottery market, including the progress of its ecosystem projects. Winchain's goal is to develop the first killer application in the whole blockchain world on the lottery industry, the one needed the blockchain technology most.

Stage 1: February 2018

Key milestone: Winchain's ecosystem partner obtains the lottery operating license for the national blockchain-based lottery in an African country. The team has started the work on building the lottery system on the Winchain.


Aceitem, V. Exas, os nossos respeitosos cumprimentos.

Maputo, aos 16 de Junho de 2017
Chefe de Depto de Licenciamento, Estudos e Controlo

Gertrudes Tigo

Figure 5-6 National Lottery Operating License for A Country in Africa

Winchain will initiate its first token issuance. No more than 20% of all token supply will be released (including 15% issued to the public, a total 3.15 billion pieces, to raise no more than 15,000 ETH and 5% as the gifts for cornerstone investors). The first issuance will target cornerstone investors and private equity investment firms. The raised fund will be used for market development, system development, lottery operating licenses, business development, community incentives, personnel expenditure, legal expenditures and other expenditures.

Stage 2: Pending

Key milestone: To jointly establish the Asian Blockchain-based Lottery Research Institute and promote blockchain technology, especially Winchain and the recognition of its advantages on the lottery industry, the world's first national blockchain-based lottery will be issued in this stage (The original plan was September 2018, but the time for issuing lottery tickets was affected because of the adjustment of the online plan of the relevant African countries. Therefore, the fundraising time will be adjusted accordingly).

The second token issuance will release 15% of total supply, involving 3.15 billion pieces (30% of total supply including the initial offering) targeting the private equity investment firms and qualified investors. During the offering period:

a) If the raised amount fails to reach the soft top at 50,000 ETH, the fund-raising is deemed to fail, whereby the ETH raised at stage 2 will be returned and 15% of token involved in stage 2 will be destroyed completely.

b) The fund-raising is deemed to succeed if the amount reaches the soft top at 50,000ETH.

c) When the raised amount exceeds the soft top at 50,000ETH, the amount calculated by **a* (b/c)** will be granted to the investors. (**a** refers to the release amount of WosToken at stage 2, the amount of **a** is 15% of WosToken's total supply; **b** represents the ETH invested by the qualified investors; **c** means the total amount of ETH raised thereof)

Stage 3: Around Mid-2019

Key milestone: Partners from all countries in the Winchain ecosystem will obtain the lottery operation and issuance licenses of at least five countries, and starts deployment of Winchain based block-chain lottery operating system; the number of new lottery games contributed by Winchain developer ecosystem will exceed 50; the amount of lotteries to be sold and issued through the Winchain system will exceed US$1 billion in equivalent each year, which will create a very promising future for the Winchain ecosystem.

The third token issuance will involve 20% of token for public exchange, involving 4.2 billion pieces (up to 50% of total supply, the WosToken issuance will end up now) targeting qualified investors. If during the period of fund-raising:

a) The raised amount fails to reach the soft top at 100,000ETH, the fund-raising is deemed to fail, whereby the ETH of investors at the third stage will be returned and 20% of token involved will be destroyed completely.

b) The fund-raising is deemed to succeed if the amount reaches the soft top at 100,000ETH.

c) When the raised amount exceeds the soft top at 100,000ETH, the amount of WosToken calculated by **a* (b/c)** will be granted to the investors. (**a** refers to the release amount of WosToken at the second stage, namely 20% of WosToken; **b** represents the ETH invested by the qualified investors; **c** means the total amount of ETH raised thereof)

5.3.2 Lucky

Lucky is based on the consortium-chain, issued by government agencies and departments. When needed, users can buy Lucky directly at relevant application scenarios. Digital tokens are released strictly in proportion to the assets at a ratio of (1:1) stored on the Ethereum network. The released digital assets inherit the characteristics of Ethereum network and can be freely traded in an anonymous, safe and decentralized P2P environment. Meanwhile, Lucky acting as exchange between valuable assets and digital tokens at a 1:1 exchange rate, so as to safeguard the value of the digital token.

Like the Linked Exchange Rate System, Lucky use the US dollar as the statutory currency of reserves, Lucky will be issued strictly according to the number of reserves at a proportion of 1:1 on the Ethereum network. Which means one additional Lucky can be issued when and only when the reserve is increased by one dollar.

Meanwhile, users can also redeem US dollars via the redemption gateway of Lucky at the same exchange rate, and the redeemed Lucky will be destroyed, so as to keep the price of Lucky in line with US dollars at the fixed exchange rate of 1:1.

Characteristics of Lucky: Lucky is open and transparent, has strong public credibility with regular auditing from government agencies without the need of any intermediaries. In a certain country in Africa, Lucky is used by the blockchain-based lottery operator as the only token for lottery sales and the use of Lucky making sure the open and transparency of lottery ticket sales and lottery prize claim.

VI. Team and Consultants

6.1 Team members

Team up with the world's leading lottery system development team and blockchain technology development team, the Winchain Team has distinctive advantage in high-concurrent system design, application of blockchain technology in the lottery industry, the operating of lottery games and lottery business in various countries, and in-depth understanding of the lottery industry including the use of industry resources. The Winchain Team has expanded its operations to a number of countries in Africa and Southeast Asia. In 2018, Winchain will operate the national-level blockchain-based lottery system in at least two countries. The team's vision is to develop the Winchain system into the new standard of Internet based lottery system, covering more countries and delivering brilliant results in the global lottery industry.

6.2 Founder team

Forrest Nie

Forrest Nie is a team member of Winchain. Forrest obtained his Bachelor's degree from the Department of Geophysics at Peking University and Master's degree from Chinese Academy of Sciences. Peter was the core architect of China Welfare Lottery System and he is the leading expert in the lottery system development area in China. Forrest served as a technical expert in Institute of Software, Chinese Academy of Sciences and project manager of Business-intelligence of Oriental Nations Corporation Ltd.

Adam Zhang

Adam Zhang is a team member of Winchain. Adam served as a senior manager in a well-known Internet company O2O. He has rich experience in O2O resource integration and business development.

John Niu

John Niu is a team member of Winchain, John also serves as Management Partner, Director, Investment Committee Member of Chinagrowth Capital, and CEO of Chinagrowth digital. John once worked in CITIC Securities Jinshi Investment and has over 20 years of financial investment experience with rich experience in global asset allocation. Good at market value management, cross-border mergers and acquisitions, fund management, asset trading and so on, the assets under management and mergers and acquisitions exceeded RMB 40 billion.

Emílio Jacinto (Mozambique)

Emílio Jacinto is a team member of Winchain. Emílio also serves as the HR manager and Assistant to the General Manager of Mozambique Beneficial Lottery.
Emílio is proficient in English and Portuguese and is responsible for Winchain's business development in Mozambique and other African countries.

Xing Jin（London）

Xing Jin is a team member of Winchain. Xing is an experienced software architect with more than 20 years in IT industry and software development. Xing also serves as CTO of Power X, a UK based block-chain startup in the field of energy exchange.

Bob Lu (Sydney)

Bob Lu is a team member of Winchain. Bob is a seasoned internet expert and a blockchain technology enthusiast with 18 years of experiences in start-ups, software engineering, product management and go-to-market across UK, China, Brazil, and Australia. Bob also serves as an advisor for the TrustNote Foundation, an Australia based blockchain technology startup.

6.3 Core team

Peter Zhong (Silicon Valley)

Peter Zhong is a team member of Winchain, Peter obtained his master's degree in computer science at the University of Silicon Valley and has 20 years of experience in Linux development. Peter served as the CEO of Linuxlab, CTO of WebKomputing, and Vice President of Silicon Valley Business Association.

Vivienne Liu

Vivienne is the COO of Winchain, who takes the responsibility of Winchain's marketing and public relations. Vivienne obtained her bachelor degree in Tsinghua University. She founded YIDIANER in 2012, which is one of the earliest online art trading platforms in China. Then, she founded Next Buy industrial manufacturing platform in 2014, which was acquired by Qihoo 360. In addition, she used to be elected by Forbes 30 Under 30(China) and Forbes 30 Under 30(Asia) for outstanding entrepreneurs successively.

6.4 Consultants and Early Investors

DKB FUND

Vancoin Capital

Tianan Capital

OK Blockchain Capital

LONGLINK FUND

Zipper

LINKVC

Fun&Fast Camps Incubator

F2POOL

JIU XIAO ZI BEN

ROOTSCAP

Andrew Gu
Danhua Venture Capital

Yang Xiangyang
from Resources Investment

Wang Jipeng
the partner of Oriza Holdings

He Jia
the partner of Nanshan Capital

Huachuang Digital

Hash Capital

BLOCKWORLD

6.5 Industry Consultants

World Lottery Association

Asia Pacific Lottery Association

Asia Pacific Association for Gambling Studies

Chen Haiping
deputy director of LRCC

Su Guojing
founder of China Lottery Industry Salon

Han Dawei
Yao Capital

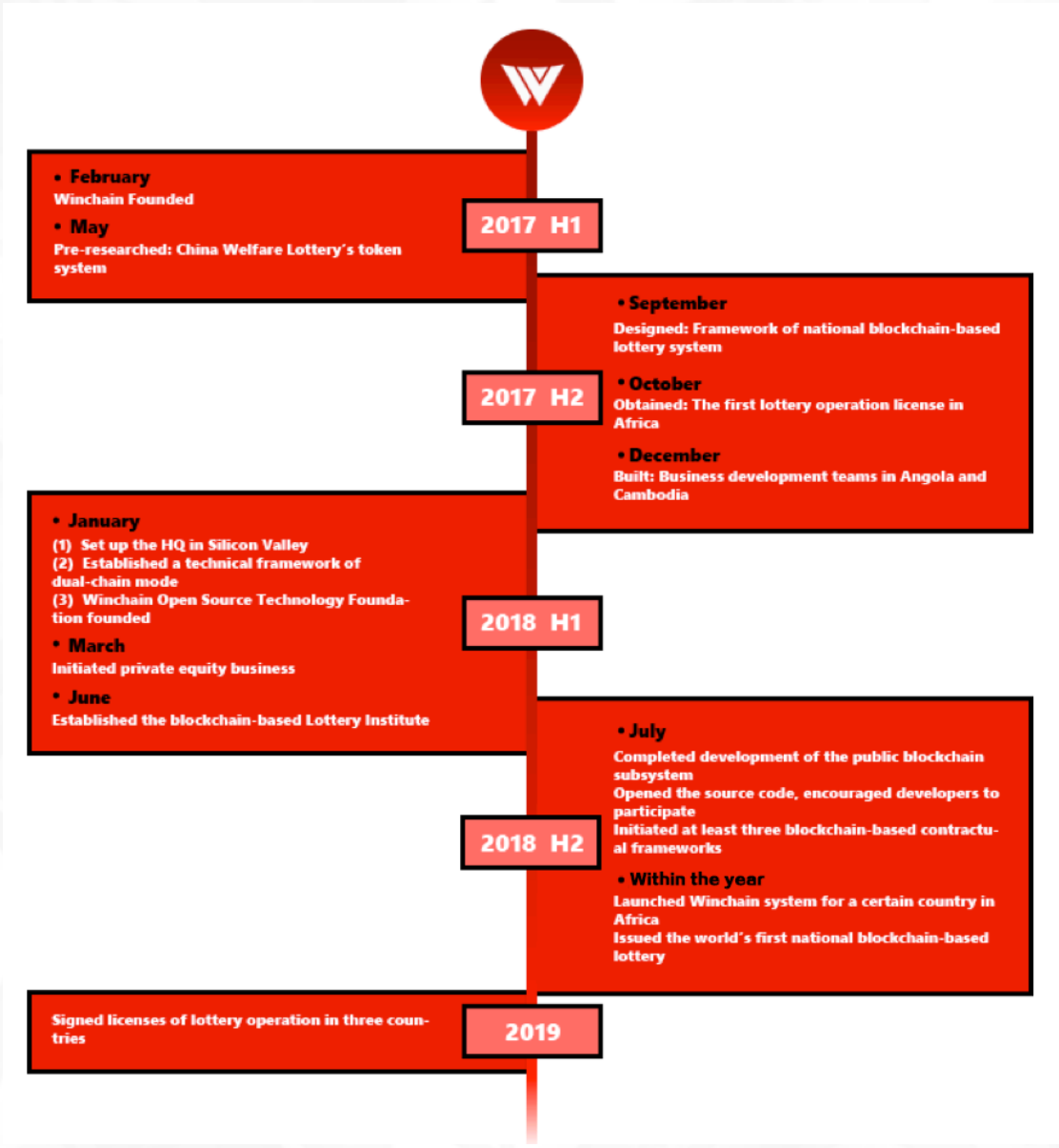
6.6 Proposed Partners

Beijing Zhongcai Printing Co., Ltd.

China Sports Lottery Technology Group

Hong Kong Jockey Club Business Development Co., Ltd.

VII. Winchain Roadmap



VIII.Summary

The global sales of lottery continue to grow, but the lottery operators and service providers still facing various challenges, especially the trust between the players and the operators as well as the problems of transparency and fairness. Global lottery operators are desperately looking for the most credible solutions and when decentralized blockchain technology emerges as a new disruptor of today's centralized system, lottery operators realize that they will have to embrace the blockchain technology sooner or later. As the forerunner of the blockchain-based lottery system, Winchain will join hands with global lottery operators to explore the full potential of the brand-new lottery games empowered by the cutting edge blockchain technology.

IX. Legal Affairs and Risk Disclosure

9.1 The legal structure of the Winchain project

Winchain Foundation Limited ("Winchain Open Source Technology Foundation") is a non-profit organization registered in Singapore to facilitate the Winchain project. As an independent legal entity, Winchain Open Source Technology Foundation is fully charged to build a team to develop the blockchain-based lottery system and its applications. However, Winchain is operated and used by the autonomous Winchain community in which Winchain Open Source Technology Foundation can only make suggestions on its governance, just like any other members in the community, Winchain Foundation does not have any superior power than other members.

The Winchain Open Source Technology Foundation sells WosTokens that are intended to run on and be used on the Winchain platform. WosToken functions as settlement units for users to use the Winchain service. Once sold, there will be no commitment to re-purchase or redeem them. As a virtual commodity, WosToken is neither a security nor a speculative investment vehicle. Winchain Foundation does not guarantee WosToken's intrinsic value or any return. WosToken does not represent any real-world assets or rights (such shares, voting rights of the Winchain Open Source Technology Foundation). WosToken's typical audience is technical experts familiar with digital tokens and blockchain technology.

The income from the sale of WosToken by the Winchain Open Source Technology Foundation will be freely used by the Winchain Foundation. It will be mainly used for technology development, marketing, legal compliance, financial compliance, business development etc.

Winchain's lottery operating platform is a fully decentralized platform built on Ethereum, anyone in the world can access it through the consumption of WosToken, regardless of his geographic location. The Winchain itself does not have a physical entity and it has nothing to do with the territory and statutory currency of any country or region.

9.2 Disclaimer

Except as expressly set forth in this whitepaper, the Winchain Open Source Technology Foundation makes no representation or warranty regarding Winchain or WosToken (especially for its merchantability and specific features). Anyone involved in WosToken's sales plan and the purchase of WosToken are based on their own knowledge of Winchain, WosToken and this whitepaper. All participants will accept WosToken as they are once the Winchain project is launched, regardless of their technical specifications, parameters, performance, or features. The Winchain Open Source Technology Foundation explicitly disclaims and refuses to assume the following responsibilities:

(1) Anyone who violates any country's anti-money laundering law, anti-terrorism financing law, or any other regulatory requirements when purchasing the WosToken;

(2) Any person who purchases WosToken in breach of any statement, warranty, obligation, commitment or other requirements specified herein, and the resulting failure to pay or fail to withdraw the WosToken;

(3) The abandonment of the sale plan of WosToken for any reason;

(4) The failure or abandonment of Winchain development, and the resulting failure to deliver WosToken thereof;

(5) Delay or postponement of Winchain development, and failure to meet the previously disclosed agenda;

(6) Errors, discrepancies, defects or other problems of the Winchain's source code;

(7) Failure, collapse, breakdown, rollback or hard fork of the Winchain system or the Ethereum blockchain;

(8) Failure of Winchain or WosToken to implement any special features or the feature implemented does not fit for any specific purposes;

(9) The use of the funds raised through WosToken sale;

(10) Failure to disclose the full information of the Winchain development in a timely manner;

(11) Any participant has leaked, lost or damaged the digital token, or the private key of the wallet (especially the private key of the WosToken wallet in use);

(12) Breach of contract, infringement, collapse, slander, termination or suspension of service, fraud, misuse, misconduct, error, negligence, bankruptcy, liquidation, dissolution or out of business of the third-party crowdfunding platform used by Winchain;

(13) Any discrepancy, conflict or contradiction of the contents agreed between any person, the third-party crowdfunding platform, and the contents of this whitepaper;

(14) Anyone trading or speculating on WosToken;

(15) Listing or delisting of WosToken on any cryptocurrency exchange;

(16) WosToken is classified or deemed as a currency, securities, commercial draft, negotiable bill, investment product, or other thing by any government, quasi-government agency, competent authority, or public agency, so that it is prohibited, regulated, or restricted by the law;

(17) Any risk factors disclosed in this white paper, and any damages, losses, claims, liabilities, penalties, costs, or other negative effects associated with, resulting from, or concomitant with such risk factors.

9.3 Risk Statement

The Winchain Open Source Technology Foundation holds true that numerous risks exist in the development, maintenance and operating of the Winchain system, many of them are beyond the control of the Winchain Open Source Technology Foundation. In addition to the other content described in this whitepaper, each WosToken buyer should also peruse, understand and carefully consider the following risks. Each WosToken buyer should pay special attention to the fact that the Winchain Open Source Technology Foundation is established in Singapore, but both Winchain and WosToken exist only in the online virtual space and do not have any tangible presence, and therefore do not belong to or involve any particular country. All buyers have fully understood and agreed to accept the following risks.

(1) Inadequate provision of information

As of the publication date of this whitepaper, Winchain is still at the stage of development, for which its concepts, consensus mechanism, algorithms, codes and other technical details and parameters may be updated and changed frequently from time to time. Despite containing the latest information of Winchain, this whitepaper is not absolute complete, Winchain Open Source Technology Foundation will from time to time making changes and updates for specific purposes. Winchain Open Source Technology Foundation is unable and not obliged to, at all times, notify participants of each detail during the development of Winchain (including its progress and expected milestone, whether or not postponed); and therefore does not necessarily give buyers prompt and full access to Winchain's information in a timely manner during the development of Winchain. It is inevitable and rational that the information disclosure is insufficient.

(2) Regulatory measures

Digital tokens are being or may be supervised by the authorities of various countries. Winchain Open Source Technology Foundation may from time to time receive inquiries, notices, warnings, orders or rulings from one or more governing authorities, and may even be ordered to suspend or terminate the development of Winchain. The development, marketing, promotion or other aspects of Winchain may therefore be seriously affected, hindered or terminated. As regulatory policies may change at any time, the existing regulatory permission or tolerance for Winchain in any country may only be temporary. In various countries, WosToken may be defined as a virtual commodity, digital asset, and even securities or currencies at any time. Therefore, according to local regulatory requirements in certain countries, WosToken may be prohibited from trading or holding.

(3) Cryptography

Cryptography is constantly evolving and it cannot guarantee absolute security at all times. Advances in cryptography (such as password cracking) or other technological advances (such as the invention of quantum computers) may pose dangers to cryptographic-based systems including Winchain. This may result in the theft, stolen, vanished, destroyed or depreciated or devaluation of WosToken held by any person. To a reasonable extent, the Winchain Foundation will prepare itself for preventive or remedial measures to upgrade Winchain's underlying protocol to address any progress in cryptography and, where appropriate, incorporate new and reasonable security measures. The future of cryptography and security innovation cannot be foreseen, and the Winchain Open Source Technology Foundation will make every possible effort to accommodate the constant changes in cryptography and security space.

(4) Failure or abandonment of development

Winchain is still in its development phase, not a finished product that is ready-to-release. Due to the technical complexity of the Winchain system, the Winchain Open Source Technology Foundation may face unpredictable and/or insuperable difficulties from time to time. Therefore, the development of Winchain may fail or be abandoned at any time (for example due to lack of funds) for any reason. Failure to develop or abandon will result in WosToken not being delivered to any buyer of its token issuance program.

(5) Theft of fund

There may be attempts to steal funds received by the Winchain Open Source Technology Foundation (including those that have been converted into fiat currency). Such theft or theft attempts may affect the Winchain Open Source Technology Foundation's ability to fund Winchain development. Although the Winchain Open Source Technology Foundation will adopt cutting-edge technology solutions to protect crowdfunded funds, some cybercrimes are still difficult to be completely prevented.

(6) Defects in source code

Nobody can guarantee that the source code of Winchain is completely flawless. The source code may have some defects, errors, discrepancies and bugs, all of which may prevent users from using specific functions, disclose user information or result in other damages. Such defects will certainly threaten the serviceability, steadiness and/or security of Winchain, and therefore deliver negative impacts on the value of WosToken. The open source code is based on transparency to facilitate identification and problem resolution of code originating from the community. The Winchain Open Source Technology Foundation will work closely with the Winchain community to continuously improve, optimize and improve the source code of Winchain.

(7) Permissionless, distributed and self-governed ledger

In today's blockchain projects, there are three popular types of distributed ledgers, namely, permissionless ledger, consortium ledger, and private ledger. Winchain's underlying ledger is permissionless, which means that it can be freely accessed and used by anyone without restriction of access. Although Winchain was initially developed by the Winchain Open Source Technology Foundation, it is not owned, operated, or controlled by the Winchain Open Source Technology Foundation. The spontaneously formed Winchain community is completely open, not centrally governed by any one, and accessible by the public without any barriers to entry. It is composed of users, fans, developers, WosToken holders and other participants worldwide, most of these people have no relationship with the Winchain Open Source Technology Foundation. With respect to the maintenance, governance, and even evolution of Winchain, the community will be decentralized and autonomous. The Winchain Open Source Technology Foundation is just an active member of the community in equal status with other people. There is no supreme or arbitrary power been given to Winchain Foundation, even if it had previously made hard works and contributions to the birth of Winchain. Therefore, after Winchain is released, how it governs and how it would eventually evolve is not dominated by the Winchain Open Source Technology Foundation.

(8) Source code upgrade

Winchain's source code is open source and may be updated, modified or changed by any member of the Winchain community from time to time. No one can anticipate or guarantee the exact result of an upgrade, amendment, modification or change. Therefore, any upgrades, corrections, modifications, or changes may result in unpredictable or unexpected results that can have a material adverse effect on Winchain's operation or WosToken's value.

(9) Security vulnerability

The Winchain platform is based on open source software and is a distributed permissionless ledger. Although the Winchain Open Source Technology Foundation will make every possible effort to maintain Winchain's system security, anyone may intentionally or unintentionally bring vulnerabilities or defects into Winchain's core infrastructure elements that the Winchain Open Source Technology Foundation is not able to take safety measures to prevent or remedy. This may eventually lead to the loss of the participant's WosToken or other digital tokens.

(10) Distributed Denial of Service (DDoS) Attack

Ethereum is designed as a permissionless ledger. As a result, Ethereum may suffer from the so called “Distributed Denial of Service” (DDoS) cyber-attacks from time to time. This attack may cause the Winchain system to be negatively impacted, stagnated or paralyzed, and as a result, transactions on top of it will be delayed or being delayed of written into Ethereum blocks, or even temporarily unavailable.

(11) Insufficient processing capacity

The rapid development of Winchain will be accompanied by a sharp increase in trading volume and demand for processing capacity. If the demand for processing power exceeds the load that can be provided by the nodes within the Ethernet blockchain network, the Winchain network may collapse and/or stagnate, and may generate fraudulent or erroneous transactions such as "double spending". In the worst case, WosToken held by anyone may be lost, and the reversal or even fork of the Ethereum blockchain may be triggered. The aftermath of these events will undermine Winchain's usability, stability and security, and the value of WosToken.

(12) Unauthorized claim for sale of WosToken

Any person who obtains the buyer's registered email or registered account access rights by decrypting or cracking the WosToken buyer's password will be able to maliciously obtain the buyer’s WosToken for sale. Therefore, the WosToken for sale purchased by the purchaser may be mistakenly sent to any person who claims WosToken through the registered email or registered account of the purchaser, and such sending is irrevocable and irreversible. Each WosToken purchaser should take measures such as the followings to properly maintain the security of its registered email or registered account: (i) use a high security password; (ii) not open or reply to any fraudulent email; and (iii) strictly protect the confidentiality of secret or personal information.

(13) Private key of the WosToken wallet

The loss or corruption of the private key necessary to acquiring WosToken is irreversible. WosToken is accessible and operated only by having a local or online WosToken wallet with a unique public-private key pair. Each purchaser should keep its WosToken wallet’s private key in safe. If a WinToekn buyer's private key is lost, missing, leaked, damaged or stolen, neither the Winchain Open Source Technology Foundation nor any other person can help the buyer to obtain or retrieve the WosToken.

(14) Popularity

The value of WosToken largely depends on the popularity of the Winchain system. Winchain does not anticipate that it will be popular, in vogue or widely used in a short period after its launch. In the worst case, Winchain may even be marginalized for a long time, attracting only a small group of users. In contrast, a large portion of WosToken demand may be speculative. The lack of users may lead to fluctuations in the price of WosToken, which will affect the long-term development of Winchain. When such price fluctuations occur, the Winchain Open Source Technology Foundation does not (and does not have the responsibility to) stabilize or influence the market price of WosToken.

(15) Liquidity

WosToken is neither a currency issued by any individual, entity, central bank or national, supranational or quasi-national government organization, nor it is supported by any hard assets or any other credits. WosToken's circulation and trading in the market is not the responsibility or pursuit of the Winchain Open Source Technology Foundation. WosToken's transaction is based only on the consensus reached by the relevant market participants on its value. No one is obliged to redeem or purchase any WosToken from its holder, nor does any person guarantee to any degree the liquidity or market price of the WosToken at any time. If the WosToken holder wants to transfer WosToken, the WosToken holder needs to find one or more buyers who are interested in buying at a mutually agreed price. This process can be very costly, time consuming, and ultimately unsuccessful. In addition, there may be no cryptocurrency exchange or other market for public trading of WosToken.

(16) Price fluctuations

When trading in the open market, crypto tokens usually fluctuate in price. Price shocks often occur in very short period. The price may be quoted in Bitcoin, Ethereum, U.S. Dollar, or other statutory currency. This price volatility may be caused by market forces (including speculative trading), changes in regulatory policies, technological innovations, the accessibility to the cryptocurrency exchanges, and other objective factors, which also reflect changes in the supply-demand balance. Whether or not there is a secondary market for WosToken transactions, the Winchain Open Source Technology Foundation assumes no responsibility for any secondary market WosToken transactions. Therefore, the Winchain Open Source Technology Foundation has no obligation to stabilize the price fluctuations of WosToken and is not concerned about it. The risk involved in the transaction price of WosToken must be borne by the WosToken traders themselves.

(17) Competition

Winchain's underlying protocol is based on open source software. No one claims copyright or other intellectual property rights over the source code. Therefore, anyone may legally copy, duplicate, reproduce, design, modify, upgrade, improve, recode, reprogram, or otherwise utilize Winchain's source code and/or underlying protocols in an attempt to develop a competitive protocol, software, systems, virtual platforms, or virtual machines to compete with Winchain, or even overtake or replace Winchain. The Winchain Open Source Technology Foundation cannot control this. In addition, there already exists and there will be many more competing blockchain-based platforms to compete with Winchain. The Winchain Open Source Technology Foundation cannot eliminate, prevent, limit or reduce such competitive efforts aimed at competing with Winchain or replacing Winchain under any circumstances.