YOOBA

Decentralized blockchain-based e-commerce system

Ye Song (flyye) (fly31318@gmail.com flyye@yooba.org)

2018.3.13

Home：https://yooba.org Email：yooba@yooba.org

table of Contents

1 Origin....2
2 . Yooba usage scene....3
2.1 Share/sell/discover goods and services anytime, anywhere....3
2.2 Supermarket platform....4
2.3 Supply chain....4
2.4 Insurance....4
2.5 Storage, artificial intelligence, etc....5
3 Yooba Design idea....5
3.1 Nature....5
3.2 Demand....5
3.3 Blockchain introduction....5
3.4 Yooba key part....6
3.4.1 Account system....6
3.4.2 Private....10
3.4.3 DPOS....11
3.4.4 Storage....11
4 Community Development Plan....12
5 Token distribution....12
6 Token status and disclaimer....13
7 Notice....14

1 Origin

The appearance of the Internet has caused a drastic change in people's lives.People's lives are getting richer and more convenient.Using the Internet to meet daily needs has become the habit of most people. Nowadays, clothes, furniture, snacks, books, games, cars, rooms, etc. almost all physical objects or virtual objects can be obtained on the Internet, and even many services can only be obtained through the Internet.There are numerous sites, large and small, and the services provided are all-inclusive.Also,there have been some problems and contradictions in the development process.

As a consumer, users need to register on multiple different websites, provide different levels of personal information, and need to remember multiple accounts and passwords. The service experience and quality provided by different service providers are not the same.The protection awareness and measures of user information from

different service providers are also very different.User data may leak in one place and cause multiple leaks.The user's data is leaked or the user's data is used for what purpose. In these situations, the user has little control or even no knowledge.

As service providers, due to data competition, resource competition, and user competition, data oligarchs and resource oligarchs have gradually emerged.These oligarchs have absorbed more and more scope just like tornados and gradually formed industry leaders and rule makers. They make it difficult for newcomers to enter or expand.And ultimately affect the user's service experience and service diversity.

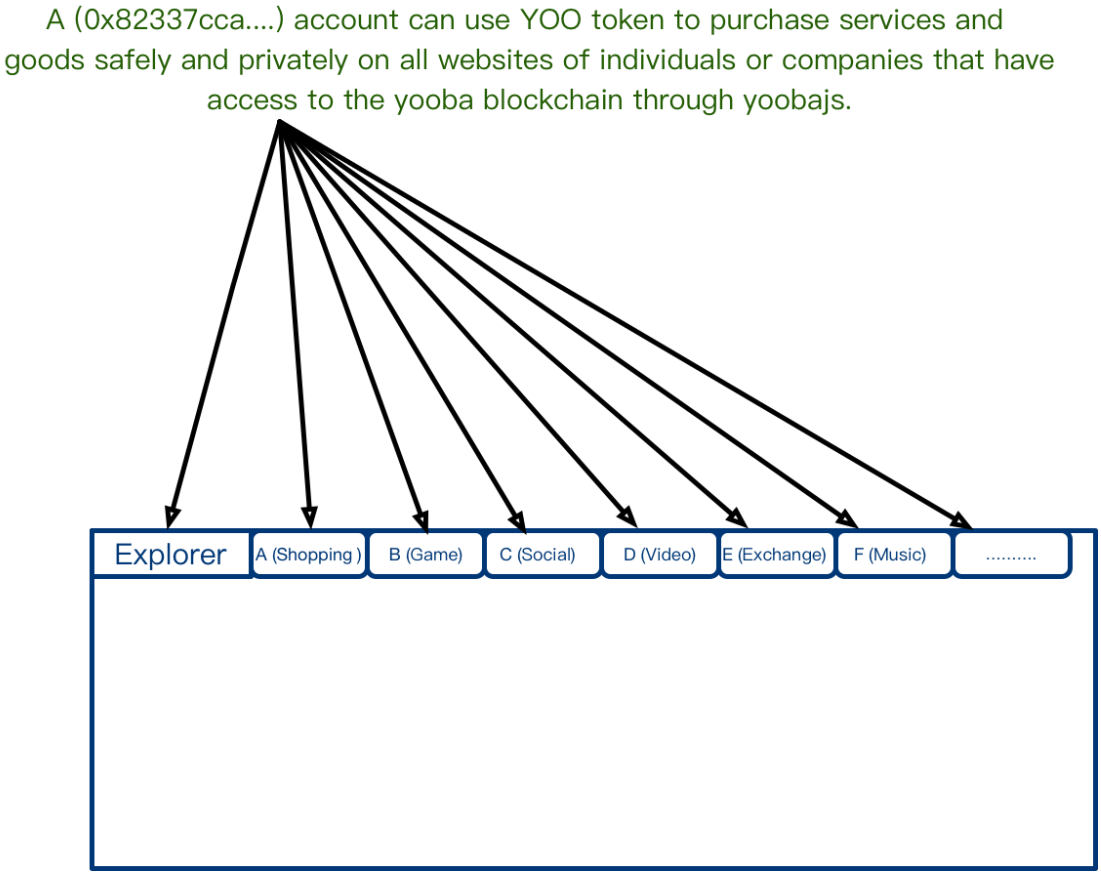
Yooba is a solution to the above problems. Yooba is committed to allowing all consumers to conduct global consumption security, privacy, freedom, and convenience , through one account; and is committed to establishing a global, decentralized, transparent, fair, and dynamic business platform. Of course this is an experiment. It may be successful or it may fail.

2 . Yooba usage scene

Yooba is a blockchain system for shopping only. Although she can apply in all aspects, Yooba's research, development and maintenance only focus on commercial scenarios and future related to goods and services. The following is a brief list of some of the application cases.

2.1 Share/sell/discover goods and services anytime, anywhere

Any user or company can upload their own products (including regular merchandise, artwork, second-hand items, etc.) or services (including virtual products such as knowledge and music) through the App or pc wallet. Some main websites can collect and classify the products or services they are interested in through yooba to form various types of service websites. Users only need one Yooba account, and once they log in (browser plug-in login), they will be able to access all websites that access Yooba services. As shown below



2.2 Supermarket platform

A principal or platform with a strong reputation can establish a large platform or a large supermarket on Yooba, and choose his trusted or controlled small company or individual on Yooba to pull into his shop. They established a virtual organizational relationship through Yooba. In this way, various complicated forms of business organization can be formed.

2.3 Supply chain

From small toys to large cars, all of their components can be found in Yooba. Anyone can choose the most cost-effective component they need on Yooba in a fair and transparent manner. Yooba has a complete record of supply and demand in the supply chain. And their trading history.

2.4 Insurance

Different business scenarios have different risks and different security policies. Insurance is a basic service in Yooba (accessed by different service providers) and it is

also a big business.

2.5 Storage, artificial intelligence, etc.

Yooba's large number of commodity data, transaction data, etc. have put forward higher demands and broader prospects for storage, big data analysis, and artificial intelligence. Any company entity or individual can fairly acquire Yooba products, public transaction records, users, stores and other visible data to develop their own businesses and provide services on Yooba or elsewhere.

3 Yooba Design idea

3.1 Nature

Yooba's essence is a blockchain. Her goal is to allow all consumers to conduct global consumption security, privacy, freedom, and convenience , through one account; to establish a global, decentralized, transparent, fair, and dynamic business platform. So its design, community development, and application promotion will all focus on this goal.

3.2 Demand

- High performance: tens or even millions of transactions per second to meet the global user shopping experience
- Low latency: Confirmation speed in seconds, improving trading experience
- Big Storage: Huge storage space for rich goods and services
- High scalability: Different transaction processes and rules required for various commodity trading scenarios, free access to third-party services, and networks. Meet various business models
- Decentralization: The conflicts of interests among sellers, service providers, and commercial entities are obvious. They need fair and transparent mechanisms to maintain, and there is no middleman control.
- Security, Privacy: Great Protection of User Privacy and Property Security

3.3 Blockchain introduction

Blockchain originated from Bitcoin, and its decentralized, distributed, demediated, non-reformable, and programmable features have great power of subversion for all

walks of life. The core of the blockchain is decentralization. Multiple peer nodes jointly maintain and develop this public ledger. It is difficult or impossible for any node or middleman to control an open, well-operated blockchain network based on its own interests.

Blockchain is great, and its emergence has its inevitability. Fairness, justice, freedom, and individuality are often pursued by people as faith or ideal in the long river of humanity. Blockchain decentralization, irreversibility, DAO and other characteristics reflect these characteristics to a certain extent, and satisfy most people's internal needs.

3.4 Yooba key part

Yooba does not plan to implement its own blockchain system from scratch. Of course, doing so also has its advantages, but our resources such as manpower and material resources are limited. We chose to stand on the shoulders of giants. We chose Ethereum, which has a relatively mature technology and application in the current blockchain world (and thanks to Ethereum for their efforts and contributions to the world of blockchain). Yooba will transform it to meet its own needs and goals. Of course, we do not intend to live in the shadow of Ethereum for a long time. We do not want the development of Yooba to be limited to the development of Ethereum (after all, our goals are different). Yooba will step by step improve or even replace the core components of Ethereum, as long as it does not adapt to the development of Yooba, we will do so, of course, we will do our best to ensure Yooba’s compatibility. Yooba will gradually form its own complete technical system, in order to maximize support for its own development scene.

3.4.1 Account system

Yooba is for shopping and for business. According to its application scenario, Yooba has 3 types of accounts: Account, Store, Contract. However, compared with Ethereum Yooba, it expanded the account structure and capabilities to fit Yooba's application scenario.

Account

```
type Account struct{
    address
    balance
    homepage
    score
    goodsurl
```

```
    historyurl
    ordersurl
    ...
    ...
    ...
}
```

Account is a basic type of account for Yooba. Most consumer account types are Accounts. Account can perform normal transactions, create smart contracts, vote, upload goods/services, downline goods/services, buy/sell goods/services. From the Account structure above, you can see that in addition to the balance attribute, Account in Yooba also introduces homepage, score, goodsroot, historyurl, and ordersurl. Give a brief introduction below.

- ✧ homepage for Account personal or shop homepage. This home page defaults to https://explorer.yooba.org/address/Account.address but the user can customize this address (eg his own official website).
- ✧ score credit. This score is calculated from the transaction history of Account on Yooba, and is synchronized across the entire network. Score initial value of 5 points, out of 10 points, the lowest 0 points. Score affects the user's trust in their products and services, thereby affecting the popularity of the services provided by users on Yooba. It also affects what services users can enjoy on Yooba. For example, a service provider imposes restrictions on the smart contracts that it provides services for: Only Accounts with a score greater than 7 have the right to purchase this service. Score specific computer system will not be implemented in the initial version of Yooba. The value is 5 before it is implemented. Do not rule out the use of existing history as a way to initialize the score when a version of Score is implemented.
- ✧ goodsroot is the hash root of the Account product information. It can be used to check if the product is updated and to retrieve the list of products stored on the IPFS.
- ✧ historyurl and orderurl are generated automatically based on Account.address. Use them to retrieve Account's merchandise transaction history information and Account's order information. This information is also stored on IPFS. Historical records and orders need to be viewed by an authorized account. The specific authorization mechanism is implemented using smart contracts.

Contract

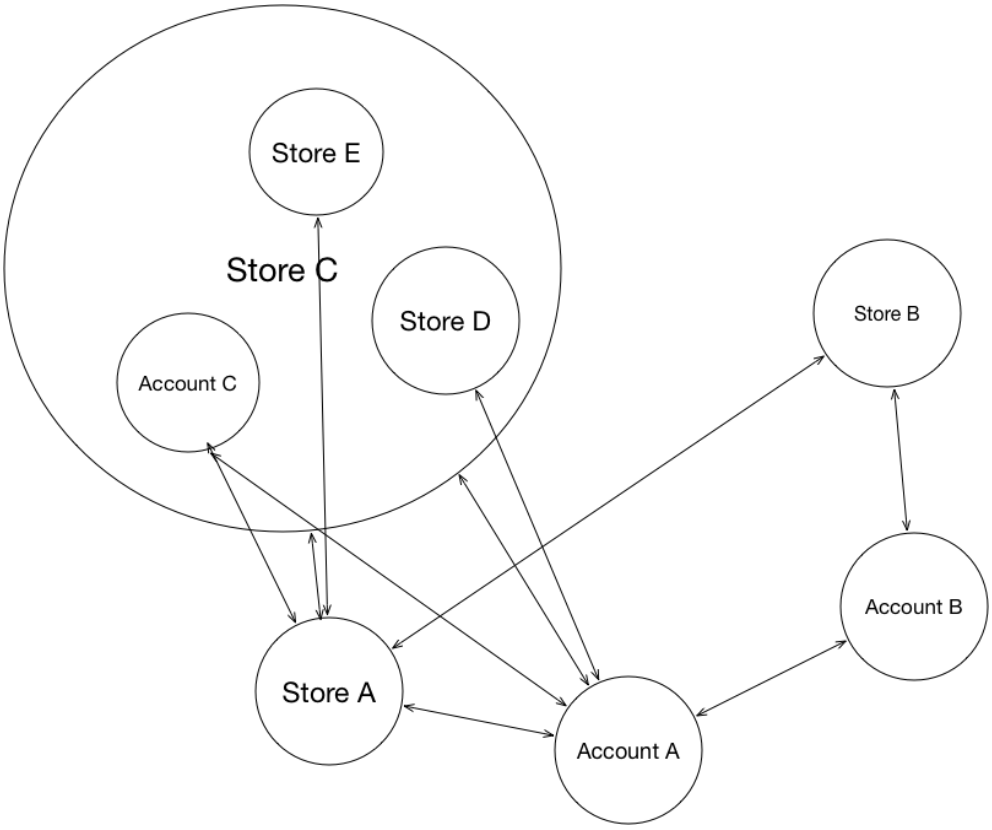
Contract is a smart contract. Smart contracts are a collection of codes that accomplish a specific function. It can run on each node's virtual machine. Since the language for

writing Contract is Turing complete, Contract can implement a very large number of unique applications and functions, as long as the imagination is rich enough. At Ethereum, Contract is widely used in the issuance of tokens. Of course, the smart contract in Yooba is not mainly used for this, it can be used as a pre-condition or post-condition of the transaction to ensure the smooth progress of the transaction. It can also be bought and sold in the form of goods as a carrier for a wide range of virtual products. Such as coins, limited-time products (image products, knowledge products), insurance, instant services and so on. Privacy in Yooba's business is also provided by smart contracts (more on that later).

Store

Stores are everywhere in real life. In Yooba, the location of the Store is equally important. Account is like an individual in life. Store is like a real shop, a company, etc. The reason why the Store and Account are separated is that the meaning of the Store in Yooba is much different from that of the Account, and in the follow-up upgrade of Yooba, the Store often brings new features to meet the continuous development and improvement of the system.

In addition to the basic functions of the Account, the Store can be nested within each other. Just like real big supermarkets have many suppliers of goods. In Yooba, Store is included in other Stores to form a large Store. Let's talk about why we design such a feature!



We all know that the role of trust in trading is very important. Nor mally, the regular seller does not care who the buyer is. As long as the money is received, it will provide services or goods. The buyer often requires more knowledge of the goods and the seller to be able to hand over the money. Usually the buyer wants to protect privacy as much as possible, and the seller wants to promote its own brand as much as possible. The buyer's fundamental appeal is to hand over the money to buy a good product, and the lesser the person who knows his real name, gender, age, identity ID, phone number, what to buy, etc., the better. On Yooba users only need to enter the correct parameters into the product contract. Then according to the commodity price, transfer the corresponding token to Account/Store to obtain the corresponding goods or services. The seller only knows someone bought his product, and where the product is sent or which account receives the product. Other information about buyers does not need to be known at all. So the seller is usually willing to inform their users of their information. However, buyers generally do not trust undisclosed individuals or unknown small groups. In the absence of third-party guarantees, users who are cautious are generally not going to buy their products. So even if there are a lot of personal Account uploaded products, it is still an adventure for ordinary users to buy their products. Because the user may have given the money, but could not receive the product and could not find the merchant (part of the information provided by the merchant is false). But there are always some users willing to buy their products. Such as business acquaintances, after confirming their identity through the line, willing to trade with the city offline users, users willing to risk rare products. We hope that a wider range of users can enjoy Yooba's services. Yooba offers Store account types to provide better services and attract a wider range of users and businesses as much as possible.

Assume a very well-known brand, create a Store account through the Yooba client, and upload their own product. Then on its own official website (trusted place), it accesses the Yooba service through Yoobajs, logs in to its Yooba Store account, and can display the products in its Store account on its official website (of course, the display page needs to be customized), so that users can use Yoo token to buy their products very confident because their official website is trustworthy. This way to promote, users can log in to the browser Yooba plug-in, browse where (game site, music site, video site, shopping site, etc.) to use the token to buy on the line, do not need to log in other exposed privacy account, Buy more convenient and faster.

Let's assume another scenario. Another well-known shopping site wants to add more products and build a big platform. These large platform-type stores can also allow many local trusted individuals and small stores to join. These large stores can have their own authentication mechanisms for small stores within their own platforms. They have the responsibility and obligation to screen their service providers to protect the interests of users. Because the external users see a large store, they will be charged according to the contract a fee for the merchant within the platform. In addition, these large stores can introduce service providers such as insurance to increase their

credibility.

These large-scale service providers, insurance, logistics, and contracts represent certain trust agencies. In this way, in a decentralized system, through various credible links, relatively reliable stores, trusted service providers, and trusted steps, etc., step by step to enhance transaction credibility, to better serve users. And these relative reliable points are not the only points in the relative domain, so they will not lead to a regional centering. And each point is in a competitive relationship that helps provide better service.

3.4.2 Private

Privacy has always been one of the features that users are very concerned about. Assets, transaction records, personal information, etc. are very important to the user. Because this information is mastered, the user's consumption habits, behavioral characteristics, etc. are grasped. No one wants to be completely exposed to another person, let alone to the public. Personal data should be mastered by individuals. No third party can guarantee 100% data security and do not abuse data. We should hold our own things in our own hands.

The technologies used in the field of cryptocurrency to ensure privacy and apply widely include zero-knowledge proof (zk-SNARKs) and ring sign (Ring Signatures). The corresponding well-known projects are Zcash and Monero.

- Ring Signatures is a digital signature that can be signed by someone in a user group with its private key. But don't expose who is signing. That is to say, the public key cannot be bound to the signature. The greater the number of public keys participating in the ring sign, the higher the privacy. Of course, the greater the cost.
- zk-SNARKs allow the prover to prove to the verifier that his statement is true, and this proof does not reveal any information beyond the validity of the statement itself. The use of zero-knowledge proofs guarantees that information such as the parties to the transaction and the transactions will not be disclosed.

From the above we see that zk-SNRKs have a higher level of privacy. However, generating zero-knowledge proofs is very resource intensive. At present, it takes about 40 seconds to generate a proof on a relatively good performance of the RAM 3G~4G. This obviously limits its application on mobile phones. In contrast, ring signing has a higher performance and experience. However, according to the zcash blog introduction zcash sapling upgrade will greatly reduce the resources and time required for zero-knowledge proof generation (time will be reduced to second, memory is reduced to about 40M). Therefore, zero-knowledge proofs will play a greater role in the future on the mobile side.

Most cryptocurrencies such as Zcash and Monero are privacy protections implemented at the bottom of the blockchain. Ethereum is already exploring and implementing smart contract layer privacy protection mechanisms. Yooba chose privacy protection at the smart contract layer for greater freedom and broader application scenarios. Yooba will implement and provide a variety of privacy protection smart contracts as a basic module for users to choose from, including ring sign and zero-knowledge proof.

3.4.3 DPOS

Yooba is born for shopping. This transaction includes not only transactions between tokens, but also transactions of various physical and virtual goods. This puts high demands on the processing capabilities of the system and requires very low confirmation delays and very low transaction costs. Yooba chose DPOS, a consensus algorithm that satisfies these requirements (does not rule out subsequent updates to better algorithms). All accounts with YOO token have a proportional vote for selecting which trusted nodes to use as the accounting nodes. Compared to POS, the DPOS reduces the possibility of users with large voting rights directly involved in evildoing. It also decentralizes and reduces their rights and makes the entire system more decentralized.

Yooba's witness amount is 31. Yooba's first round of elections elected 51 initial witness , and then randomly choose 31 out of 51 as the winner of this round as the witness.

3.4.4 Storage

When Yooba develops to a certain stage, it will become a world-class shopping platform and trading platform. Many of the information, including pictures, product descriptions, and exchange information during the transaction, are current or personally related, and the amount of data is enormous. This data should not be permanently stored or stored on the global blockchain. But where should so much information be stored? Where can we not only ensure the security of product information, but also ensure that the data will be found when needed? Here we look at the swarm of ethereum. Swarm is an excellent distributed storage solution. It uses a small percentage of the space (or cloud space) on which the swarm node occupies the nodes on each node for storage. All these small spaces make up a huge space. But swarm has its limitations. The appearance and disappearance of swarm nodes are frequent changes. Within a short period of time, there may be thousands of old nodes disappearing and tens of thousands of new nodes appearing, and frequent data updates and migrations will occur. In addition swarm is not suitable for storing large data, swarm will split the data or file into chunk storage, and each chunk can store up to 4104 bytes of data. Swarm is mainly used to store contract code and blockchain data.

Due to the large amount of data related to commodity information in Yooba, and the relatively large volume of individual files, it is not appropriate to do frequent migrations. Users can save costs by going offline at any time. We use IPFS as Yooba's main data storage method.

IPFS is a content-addressable, versioned, peer-to-peer hypermedia distributed storage and transmission protocol.The attributes of Account, goodsroo, historyurl, and orderurl, are the IPFS addresses. The user's data is encrypted on the IPFS. Only authorized users can access and parse the data. Users need to pay for the storage space they use (YOO payment). Specific rates are dynamically changing. Storage service providers can also join in to provide stable storage services and get paid. The space used by the user will be released when the amount of arrears reaches a certain amount. Of course, users can also delete some products to reduce storage and save money.

4 Community Development Plan

Yooba's growth must rely on the strong support of the community. In order to avoid the concentration of tokens, to attract attention, and to stimulate the rapid development of the project, Yooba will take 20% of the tokens for airdrops. It is expected that 100,000 to 200,000 users will have Yooba when airdrops are completed. This gave Yooba a strong initial motivation.

We will develop a very detailed development plan. It is easy for every developer who is interested and able to contribute to Yooba to participate in the development of Yooba. At the same time, these contributors will also receive a clear Yooba token in return. And the earlier, the greater the amount of these returns.

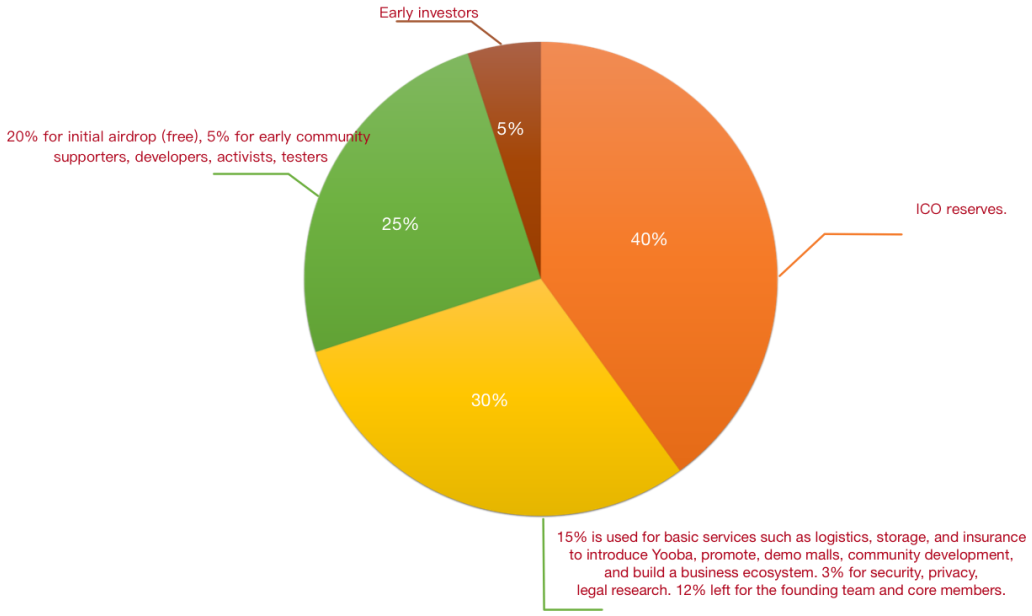
We will also continue to attract Yooba's contributors to the Yooba team as Yooba develops.

Yooba will establish a foundation organization and will be responsible for the development, maintenance, promotion, and ecosystem development of Yooba.

5 Token distribution

The symbol for Yooba token is YOO.YOO is the basic currency used for trading in Yooba. The total supply is 10 billion.

The following figure is its distribution chart.



Explanation:

- The green part is 25% early issued, and 20% of them are airdropped and randomly distributed free of charge to the Ethereum Account with more than 0.01ETH (priority) (thanks to Ethereum).The amount of airdrop is 2 billion, and about 200,000 addresses can get 10,000 Yoo. It will be distributed before December 31, 2018, and the specific information will be distributed on the official website or Yooba social media. The other 5% was used for initial incentives for Yooba development, promotion, testing, and community enthusiasts.
- 40% for ICO reservation.
- 5% for early investors.
- 30% is reserved for the community, ecological construction, founding team, scientific research, etc. Of these, 15% is left for ecological construction and community. 3% is reserved for research projects such as security, privacy, and law. 12% is left to the founding team and core developers.
- Inflation rate: 0.5% to 5%. The specific mechanism will be given later.

6 Token status and disclaimer

Yooba Token (YOO) is used as Yoko System's internal commodity trading medium.

Yooba Token (YOO) is not Yooba's stock. You do not have the right to receive a bonus for project income when Yooba organizes development. No right to share project capital.

Yooba does not guarantee the security of the transactions on Yooba, nor does it

guarantee that the goods on Yooba are not false or defective. Although we will do our best. Yooba will not bear the loss caused by the user's failure to trade on Yooba and fraudulent transactions. Due to the high degree of freedom and privacy of Yooba, as well as some imperfections in the system, it has certain trading risks and users need to take their own risks.

Yooba does not assume responsibility for the products and services it sells and stores in compliance with local or international legal regulations, nor does the executor assume the responsibility. Because it is decentralized and globalized, we cannot guarantee that every commodity on it will comply with each regional law. Yooba is a global system involved in maintenance and management. We will do our best to protect our consumers. We will try our best to advise our users to only provide services that meet the requirements of regional laws. We will provide some functional components that allow consumers and service providers to filter goods and services, but Yooba does not guarantee that it will be the best.

7 Notice

This white paper will be updated when there are significant additions or changes.