ZXTH WHITEPAPER

Contents

1.Background of the project

1.1 Introduction of blockchain technology

Blockchain is currently the most attractive technlogy. It integrates computer technology such as distributed data storage, point-to-point transmission, consensus mechanism and encryption algorithm. It is considered to be another subversive innovation in the Internet era. Because of its huge breakthroughs in data storage and information transmission, it is likely to fundamentally change the existing economic and financial operation mode, and may even cause a new technological innovation and industrial change on a global scale.

Blockchain is a chained data structure that combines data blocks in a chronological order in a sequential manner, and cryptographically guaranteed immutable distributed ledgers. The essence of the blockchain is a distributed accounting system, and the encrypted digital assets (such as Bitcoin) are assets or currencies that exist in digital form on this system. These encrypted digital assets are just a representation of accounting. The blockchain is a set of distributed, encrypted, and trusted accounting systems and clearing systems at its bottom.

Blockchain technology is considered to be the next generation of disruptive core technologies after steam engines, electricity, and the Internet. If the steam engine releases people's productivity, electricity solves people's basic needs of life, and the Internet completely changes the way information is transmitted, then the blockchain, as a machine for constructing trust, will completely change the way human values are transmitted.

In the past, relying on credibility, relying on centuries-old stores, authoritative institutions, etc., blockchain utilization technology has established a new way of trust, which can be quantified, from a technical point of view, so the blockchain becomes the next trust. The core revolutionary feature of the blockchain is to change the credit mechanism that has lagged behind for thousands ofyears

As defined in the EConomist magazine, blockchain is a machine of trust. It will redefine the production relationship and make the entire ecosystem more credible. Decentralization and distributed correspondence, data and computing are done by distributed nodes, without centralized organizations, avoiding dependence on central institutions, and risks to the entire system due to the risk of central institutions. Another benefit of distributed system is that if one of the nodes fails, it does not affect the overall functionality of the system

1.2 Avantages of blockchain

1. Decentralization

the next trust. The core revolutionary feature of the blockchain is to change the credit mechanism that has lagged behind for thousands ofyears.

As defined in the EConomist magazine, blockchain is a machine of trust. It will redefine the production relationship and make the entire ecosystem more credible.

Decentralization and distributed correspondence, data and computing are done by distributed nodes, without centralized organizations, avoiding dependence on central institutions, and risks to the entire system due to the risk of central institutions. Another benefit of distributed system is that if one of the nodes fails, it does not affect the overall functionality of the system

2. Trust and transparency

The successful application of cryptography and consensus mechanisms has enabled the underlying system to support trust issues, even without a central authentication system, to ensure the success of peer-to-peer transactions. All nodes in the system can be traded without trust, because the operation of the database and the entire system is open and transparent, and nodes cannot deceive each other within the rules and time frame of the system.

3. Openness

Data formats, data content, data exchange protocols, contracts, and even the underlying blockchain system are all open, and anyone can develop applications and query data within established rules of the system. This allows the entire ecosystem to optimize the blockchain system. Anyone can query blockchain data and develop related applications through a public interface, so the entire system information is highly transparent. In addition, private information can be stored encrypted to ensure privacy is not compromised.

4. Information cannot be tampered

The blockchain information is distributed storage, and each node has complete block data. Any node that modifies the data needs to be recognized by more than of the nodes. This mechanism makes the information almost impossible to be tampered. Modifications to the database on a single node are not valid for the entire system, so the data stability and reliability of the blockchain is extremely high.

5. Anonymity

The cryptographic algorithm and the digital wallet ensure the anonymity of the transaction, and the information in the system cannot be associated with the specific personal information. Since the exchange between the nodes follows a fixed algorithm, the counterparty does not need to open the identity to let the other party generate trust. It is very helpful for the accumulation of credit.

Block-chains are divided into public chains, private chains, and consortium chains. The public chain is mainly used in the Internet environment. Consortium blockchain is mainly aiming to solve

the needs of traditional enterprise application blockchain technology. In addition to the basic characteristics of the block-chain, ZXTH has increased the ability to be semi-centralized, enabling traditional enterprises to embrace block-chain technology. The demand for supply chain traceability can be better supported by a consortium blockchain.

1.3 Global sourcing industry

Problems we are so

Trust is one of the main problems in global sourcing. There are several reasons behind this lack of trust. First of all, when two actors are involved in a cross-border trade, most of the time they are from countries with different cultural background. This cultural gap is often the source of misunderstanding in business situation. The language difference is also another important reason of miscommunication. For instance, a French buyer who is buying products from a Chinese factory, will face lots of challenges to communicate and exchange information about products that he wants to manufacture. The problem in sourcing is that with several little miscommunications, we could have tremendous quality issues.

Another issue that brings mistrust in global sourcing, is legal systems in each country. When an international places an order to a supplier, it is very difficult to enforce purchasing contracts. In order to be able to have purchasing contracts that are well written, buyers must use local lawyers order to draft

contracts following the local laws and regulations of the supplier's country. For instance, if an international buyer does not have a branch in China and write a purchasing contract in English with a Chinese supplier, that contract has no legal value in China. Therefore, in most cases, if there is a quality problem for a particular order, buyers won't be able to becompensated.

Last but not least, international payrnents bring another layer of rnistrust in the relationship between buyers and suppliers. If a buyer and supplier decide to use letter of credit (LC) as the payment method of a particular order, risks related to late delivery and bad quality are more controlled. However, LCS are expansive for both buyers and suppliers and it takes more time to process and get cash in the supplier's account.

The most common way is to use T/T payment, but this type of payment does not guarantee most of the terms of the purchase contract.

2. ZXTH and Usage Blockchain

2.1 Features

In the following sections we will explain different features of blockchain that ZXTH will implement. We have carefully analyzed each feature in order to be able to apply in real world business situations

2.1.1 Smart contracts

A smart contract is an agreement or set of rules that govern a business transaction; it's stored on the blockchain and is executed automatically as part of a transaction. Smart contracts may have many contractual clauses that could be made partially or fully self-executing, self-enforcing, or both. Their purpose is to provide security superior to traditional contract law while reducing the costs and delays associated with traditional contracts. Smart contracts eliminate the hassles and delays inherent in contracts by building the contract into the transaction. Through smart contracts, the blockchain establishes the conditions under which a transaction or asset exchange can occur. No more fæxing or emailing documents back and forth for review, revision, and signatures.
We have conducted in-depth interviews with experts in the field of global sourcing in order to translate current sourcing processes into algorithms. Then using these algorithms we are able to

create smart contracts. The most challenging part is to be able to define general terms for our smart contracts. Because some companies might have slightly different processes, therefore our smart contracts might not completely fit their current situations. However whenever one wants to

standardize the industry, a general process has to be defined. That is why we intend to become the standard of smart contract in the field of global sourcing.
We have divided the sourcing process in six different stages. Each stage is translated into one smart contract. Later in this white paper six algorithms that are being used to write smart contracts will be explained.

2.1.2 Oracles and last mile problem

Everything from property ownership to 2nancial instruments to family arrangements can now be implemented as a piece of code on a publicly verifiable shared ledger knov,m as a blockchain. This code is "smart" in many ways : it is selfexecuting, modular, and able to drastically lower the transaction costs associated with contracts . However it is less adept in its ability to receive and verify information from the outside world. For example, an insurance contract can be programmed to pay a car owmer some amount if their car is damaged, but it cannot independently assess such damage. This gap between the offline world and its digital representation is called "last mile" problem. That is why it is important to have trusted intermediaries called "oracles" to effectively bridge the last mile between a digital record and a physical individual, business, device, or event

An oracle, in the context of blockchains and smart contracts, is an agent that 2nds and veri2es real world occurrences and submits this information to a blockchain to be used by smart contracts. This agent can be software, hardware, or human
There are several types of oracles. A software based oracle could be programmed to search for and parse text for information, but may suffer from difficulty with information categorization and resolution of ambiguous events. Such oracles will likely find to be most immediately applicable to the verification of events happening on other blockchains. Hardware oracles will likely involve submitting sensor data and will 2nd application in the Internet of Things. Human oracles are likely to be the dominant form in the near future as they can independently view or research an event outcome.
In supply chain, the problem of last mile is very important because a large part of the process is done offline and controlled by third-party agents (quality inspectors, freight forwarders, shipping companies...). Today, most of the process is still paper based and little information is digitized. We do not aim to digitize the whole process alone because this involves government agencies, customs

and banks, Several large banks such as HSBC and JP Morgan have already started the digitization process of international trade. In addition, several ports have started to develop electric B /L (bill of lading).

ZXTH will be one of the major players in the transformation of international trade, because once the whole process is digitized, our smart contracts will become the standard in the industry.

2.2 Introduction of ZXTH

2.2.1 The Solution

ZXTH is a collaborative and decentralized solution for global sourcing. It combines the power of a trusted social network with audited and validated transaction data to provide you with a comprehensive global sourcing solution.

ZXTH brings trust and transparency to international trade by introducing some innovative features in procurement, such as geolocation and supplier groups, dedicated instant messaging tools, block-chain-based smart contract and machine learning-based buyers and suppliers. The matching system between.

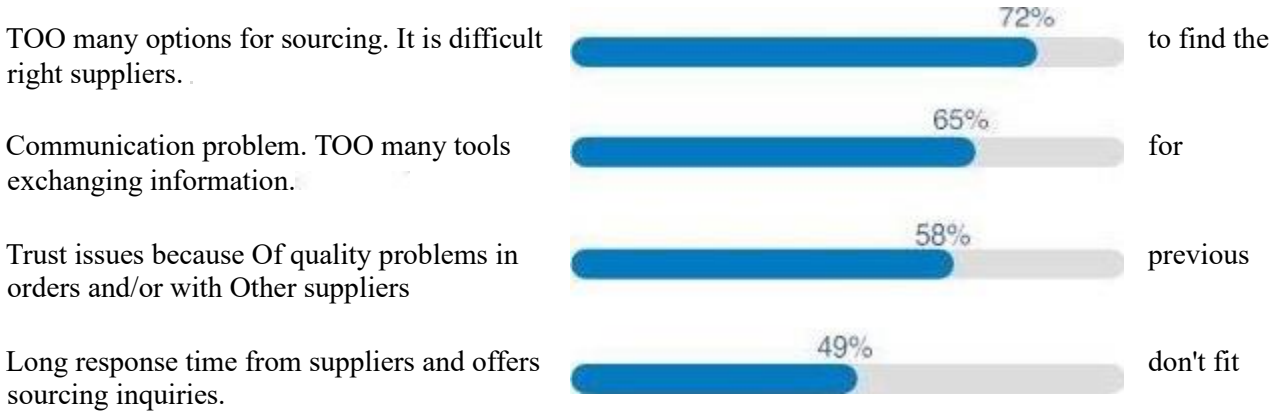
Our open platform is available to any trader and manufacturer to discover new leads and monitor the entire trading chain, while ZXTH +, our white label service, allows large purchases of

ZXTH + allows them to protect their data, improve communication with suppliers, better communicate across departments, and increase supplier transparency to optimize and accelerate their procurement processes.

2.2.2 Problems that ZXTH is solving

Trust is one of the main issues in global sourcing. There are several reasons behind the lack of trust. First, when two participants participate in cross-border trade, most of the time they come from countries with different cultural backgrounds. This cultural gap is often the source of misunderstandings in the corporate situation. Language differences are another important reason for miscommunication For example, French buyers who buy products from Chinese factories face many challenges in communicating and exchanging information about the products they want to manufacture. The problem with procurement is that we may encounter huge quality problems due to somemisunderstandings.

Another problem that brings mistrust to global procurement is the legal system of each country. When the international order is placed with the supplier, it is difficult to execute the purchase contract. In order to be able to enter into a reasonable purchase contract, the buyer must use a local attorney to draft the contract in accordance with the laws and regulations of the country in which the supplier is located. For example, if an international buyer does not have a branch in China and signs an English purchase contract with a Chinese supplier, the contract has no legal value in China. Therefore, in most cases, if there is a quality problem with a particular order, the buyer will not be able to obtain compensation.



Last but not least, international payments create another level of distrust in the relationship between the buyer and the supplier. If the buyer and supplier decide to use the Letter of Credit (L/C) as the payment method for a particular order, the risks associated with delayed delivery and poor quality will be more controlled. However, It is extensive for both buyers and suppliers and requires more time to process and get cash in the supplier's account. The most common way is to use T/T (Telegraphic Transfer) payment, but this payment method does not guarantee most of the terms of the purchase contract.

Our vision for using blockchain technology for this issue is to create a very userfriendly solution. Because the target users of our solutions are not very technical users. In fact, in the procurement industry, people still use excel files, and in some countries they still use fax machines to send quotes to each other. As a result, our solution intelligently hides the blockchain technology of users who may not understand the benefits of this technology. That is why we have to show them real results in their business. One of the most difficult challenges of the block-chain is to find real business use cases and make them user friendly enough for companies to adopt it.

That is why the development of our solution is done in several stages. First, we developed a mobile and web application to improve communication and information exchange between international buyers and suppliers. Currently, we are developing a procurement management tool that made it easier for buyers and suppliers to manage their orders. This procurement management tool will feature smart contracts on back-end in order to trace all the orders between buyers and suppliers.

2.3 Our goal

By implementing blockchain technology into our solution, we are aiming to bring more trust and transparency in international trade. Using smart contracts will bring the following advantages for our users:

1. More transparency from suppliers
2. More trust between international buyers and suppliers.
3. Providing a background check of suppliers
4. Keeping trace of business transactions
5. Easier order management

Easier conflict management between buyers and suppliers in case of late delivery, late payment, quality issues...

international trade.

Building a trust index of suppliers and buyers based on all orders.

In order to build the trust index of buyers and suppliers, we use qualitative and quantitative data. Then using these data, we have created a correlation formula and define different weights for each coefficient. We have conducted a survey among 200 buyers in order to evaluate weights of each coefficient.

We get qualitative data from the rating system that is already available in our mobile app. This feature allows buyers to rate suppliers based on their previous businesses. The issue with this type of rating (that is the most common type of rating in most of the platforms) is its authenticity. Therefore we put a lower weight for this coefficient in our correlation formula. Another type of qualitative data comes from the "crowd-verification" feature that we have developed in ZXTH . This feature allows buyers and quality inspectors to verify the location of suppliers.

Quantitative data are gathered through smart contracts. Buyers and suppliers will use our order management tools that implements smart contracts. We can trace all the issues that could occur during an order execution such as late payment, late delivery, bad quality... By putting weight for each issue, we have defined the trust index that we call ZIX (ZXTH+INDEX).

2.3.1 Decentralized Business Environment

We believe that decentralization is the only way for sourcing companies to reduce their costs and accelerate their processes. But in order to be able to decentralize a business process, we must implement the platform that provides trust and transparency. Blockchain per definition is the protocol of trust. That is why we have used this technology in order to decentralize the global sourcing process.

ZXTH allows all the stakeholders of international trade to interact with smart contracts in order to record immutable data on blockchain. In this environment, reputation is very important, that is why buyers and suppliers will have to perform well in order to keep a high ZXTH.

Creating a decentralized ecosystem will allow the acceleration of the processes. Currently each step of global sourcing is controlled and verified by agents. These stakeholders can be part of sourcing office or third-party service companies. In both cases, the cost of verification is high and it takes long time.

ZXTH Token (ZXTH)

ZXTH is the utility token of ZXTH that will be used in our application for dedicated services. The use ZXTH will allow us to reduce the cost of networking and to create value for the ZXTH holders. ZXTH token economy has been designed in order to maximize the usage of the utility token in the ecosystem of ZXTH .

Planned uses of token:

1. Node providers staking their tokens and gettingrewards for participating in transaction confirmations
2.Rewarding Oracles ("Crowd verifiers", Quality inspectors...)
3.Purchasing premium services at a discounted price

Token Issuance Model

Ticker Symbol and logo : ZXTH
Token Background: ERC20
Total Token Issued: 21,000,000 ZXTH
Smart Contract Token : 0xF9933cb5f0397bf020Bb950C307e30dd8f62080f

Token Distribution and use of funds

Token Selfdrop Program	54%
Reserve Fund	5%
Team and Founders	20%
Board Advisors	10%
Airdrop	6%
Marketing and Bounty	5%

Listing Exchange	40%
Building App Dev	12%
Marketing & Promotion	20%
Legal & Regulation	10%
Operational & Administration	8%
Contingency	4%
Partners	6%

ZXTH data model and storage Trading Structure

The state is the atomic unit of information in ZXTH . The state does not change: either a circulation ("unexpended") state, or a state of being consumed ("has been spent") that is no longer valid. The trade consumes zero or more states (inputs) and creates zero or more new states (outputs) Since the state cannot exist outside of the transaction that created it, the state is consumed or not, which can beidentified by the identifier of the transaction that created it and its index in the transaction output list.

The transaction consists of the following components:

Enter a (hash, output index) pair that points to the state of the transaction consumption.

The output state each state itself is a new state, a contract that defines the conversion function it allows, and finally a notary is specified for the state.
The attachment transaction specifies a list of hash values for a sorted zip file.The last transaction of each zip file contains code, data, certificates, or auxiliary documentation.The contract code has permission to use the contents of the attachment when checking the validity of the transaction.

Directing an input state allows for multiple output states.For example, an asset can be issued, transferred to a new owmer on the ledger, or withdrav,m from the ledger after being redeemed by the owmer and no longer needs to be tracked.An instruction is essentially a parameter passed to the contract that specifies more of the required information (such as data from the display service) that is available from the checked state.Each instruction has a list of associated public keys.Similar to the status, the instructions are all object graphs.

The set of signatures required for a signed transaction is equivalent to the union of the public keys of all instructions.

A type transaction can be a general type of transaction or a change of a notary' stransaction.The validation rules are different for each transaction type.

If a timestamp is provided, then a timestamp defines the time range in which the transaction can be considered to have occurred.This will be discussed in more detail below.

A summary of the text on the specific behavior of the transaction, checked by the transaction related smart contract. This domain is very useful for secure signature devices.

Since the signature is added at the end of the transaction and the transaction is identified by the hash used for the signature, the scalability of the signature does not become an issue. There is no need to use hashes to identify transactions including signature information. Signatures can be generated and checked in parallel, and they are not directly exposed to contract code. In fact, the contract checks if the set of public keys specified by the directive is appropriate, because the transaction is valid only if each public key listed in each directive has a matching signature. The structure of the public key is opaque. As a result, the flexibility of the algorithm is preserved: the new signature algorithm does not need to adjust the code of the smart contract itself when deployed

Example: In the image above, we can see an example of a cash issuance transaction. The transaction (bottom left) contains o inputs, and an output, the newly issued cash status. The cash status (upper right extension) contains some important information: 1) details of the cash being issued - total, currency, issuer, owmer, etc., 2) contract code whose verify() function is responsible for the issue The transaction and the future consumption of the transaction in this state are verified, 3) a hash containing the documents of important legal provisions, which provides a basic legal regulatory environment for the behavior of this state and its contract code.

The transaction also contains an order indicating that the purpose of the transaction is to issue cash. The directive also specifies a public key. The check function of the cash status is responsible for checking that the public key specified by the order belongs to the party of the transaction, and these parties need to provide their owm signature to make the transaction valid. In this case, it means:

The verify() ftmction must check that the acknowledgment directive specifies a public key that corresponds to the issuer of the cash status

The ZXTH framework is responsible for checking that the transaction has been signed by the public key listed in all instructions. In this way, the verify() function only needs to ensure that all parties that need to be signed have been specified by the Composite Key.

The term "public key" in the above description actually refers to a composite key. composite key is a tree whose leaves are regular cryptographic public keys with algorithmic identifiers. The nodes in the tree also specify the weight of each of its children and the weighted threshold it must reach. The validity of a signature set can be confirmed in such a way that from the bottom up through the tree, the weights of all

keys with valid signatures are summed and compared to the threshold. By using weights and thresholds, you can code a wide variety of situations, including Boolean expressions using and and or.

Composite keys can be used in a variety of scenarios. For example, an asset can be under the control of a 2 composite key: one key belongs to one user and the other belongs to an independent risk analysis system. When the transaction appears suspicious, such as transferring too much value in a short time window, the risk analysis system will refuse to sign the transaction. Another example involves coding the collaboration structure into a key, allowing cfo to sign a large transaction on its owm, but its subordinates need to be signed together. Composite keys are also useful for notary offices. Each participant in a distributed notary is represented by a leaf of the tree, and a specific threshold setting can make the signature of the entire group still valid if some participants are offline or refuse to sign.

Although there are already threshold signature schemes that can accurately generate composite keys and signatures, in order to allow different algorithms to be used to mix keys, we have chosen a low spatial efficiency displayformat. In this way, in the process of phasing out the old algorithm and adopting the new algorithm, it is not necessary to require all participants in the group to upgrade at the same time.

Timestamp

The transaction timestamp specifies a [start, end] time window that can be determined to be in the window. The reason that the timestamp is represented in the form of a window is that there is no exact point in time in the distributed system, but only a large number of clocks that do not have synchronicity. This is not only influenced by the laws of physics, but also because of the nature of shared transactions—especially if the signature of a transaction requires multiple authorizations, the process of constructing a joint transaction can last for hours or

It is worth noting that the purpose of the transaction timestamp is to satisfy the logical coercion of the smart contract code and to convey the position of the transaction on the timeline to the contract code. Although the same timestamp may be used for other purposes, such as regulatory reporting or event sequencing on the user interface, there is no requirement to use timestamps like that, and although the time observed with other participants is not accurate Matching, using locally observed timestamps is sometimes a better option. Or, ifyou need a precise point on the timeline and this point must be recognized by multiple participants, you can agree to use the middle point of the time window. Although this does not accurately correspond to an event (such as a keystroke or a verbal agreement), this method will still be useful.

The timestamp window can be open to communicate that a transaction occurs earlier than a specific time or later than a specific time, but it does not matter how long it is early or late.Such usage is similar to the nLockT field of a bitcoin transaction, which specifies a constraint that occurs after...

The timestamp is checked by a notary service. Since the participants of the notary service do not have a precisely synchronized clock, it is unpredictable whether a transaction submitted at the boundary of a given time window is considered valid at the instant of submission. However, from the perspective of other observers, the signature of the notary office is decisive: if a transaction has the signature of a notary, the transaction is assumed to have occurred within a giventime.

Reference clock. In order to use a relatively narrow time window when the transaction is under full control of a single participant, the notary office is expected to synchronize with the atomic clock of the US Naval Observatory. The precise feed of the atomic clock can be obtained from GPS satellites. Note that the Java timeline used by Huptex is expressed in UTC time, and the leap second is included in the last 1000 seconds of the day, so each day contains exactly 86,400 seconds. Special attention needs to be paid to ensure that the leap second counter changes in GPS are handled correctly so that they are synchronized with Java time. When setting the time window of the transaction, you must pay attention to the delay of network propagation between the user and the notary service and the internal communication of the notary service.

Data storage Merkel hash tree

The Merkel hash tree is used to construct an efficient audit proof. Its input is a list of data items whose hash values are hashed as the leaf nodes of the Merkel tree. Its output is the root node of the tree

The hash value. Given an ordered list of n inputs: $D[n]=(d_0,d_1,\ldots,d_{n-1})$, the corresponding Merkel Tree Hash (MTH) is defined as follows: $MTH()$=sha 0 MTH({do})=sha(oxoolldo)

1«nS2k represents a sublist of do to elements of list D, indicating two bit strings before and after the connection.

Merkel-Patricia Tree

In some scenarios of the ontology network, we need to quickly prove the final result of a certain entity after multiple transactions are generated, such as proving the identity status of an entity. If Merkel certification is used, each history will be required. The transaction is proved one by one, and the use of Merkle Patricia Tree (MPT) [20] can greatly improve efficiency.MPT is a combination of Patricia tree [21] and Merkel tree,

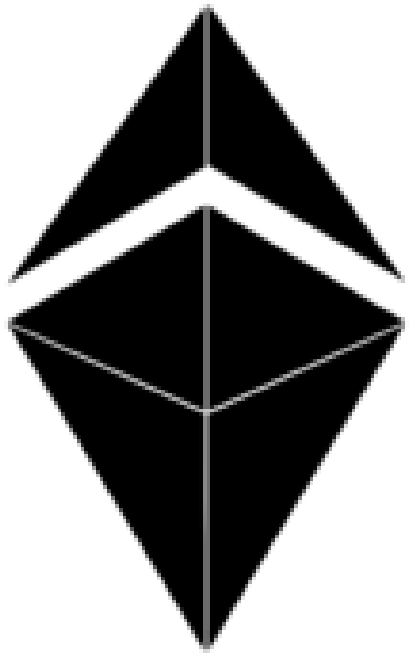
including the mapping of key values, providing a cryptographicbased, self-checking

tamper-resistant data structure with certainty and efficiency. And security features:

1. Certainty. When looking up data, the same key value will find the same result and have the same root hash;

2. Efficient: When the data changes, the new tree root can be quickly calculated without recalculating the whole tree. The time complexity of inserting, searching and deleting data is controlled at O (log2n);

3. Security. When an attacker maliciously creates a large number of transactions, initiates a dos attack, and attempts to manipulate the depth of the tree, the defined depth of the tree will make the attack impossible



END V1.0.0