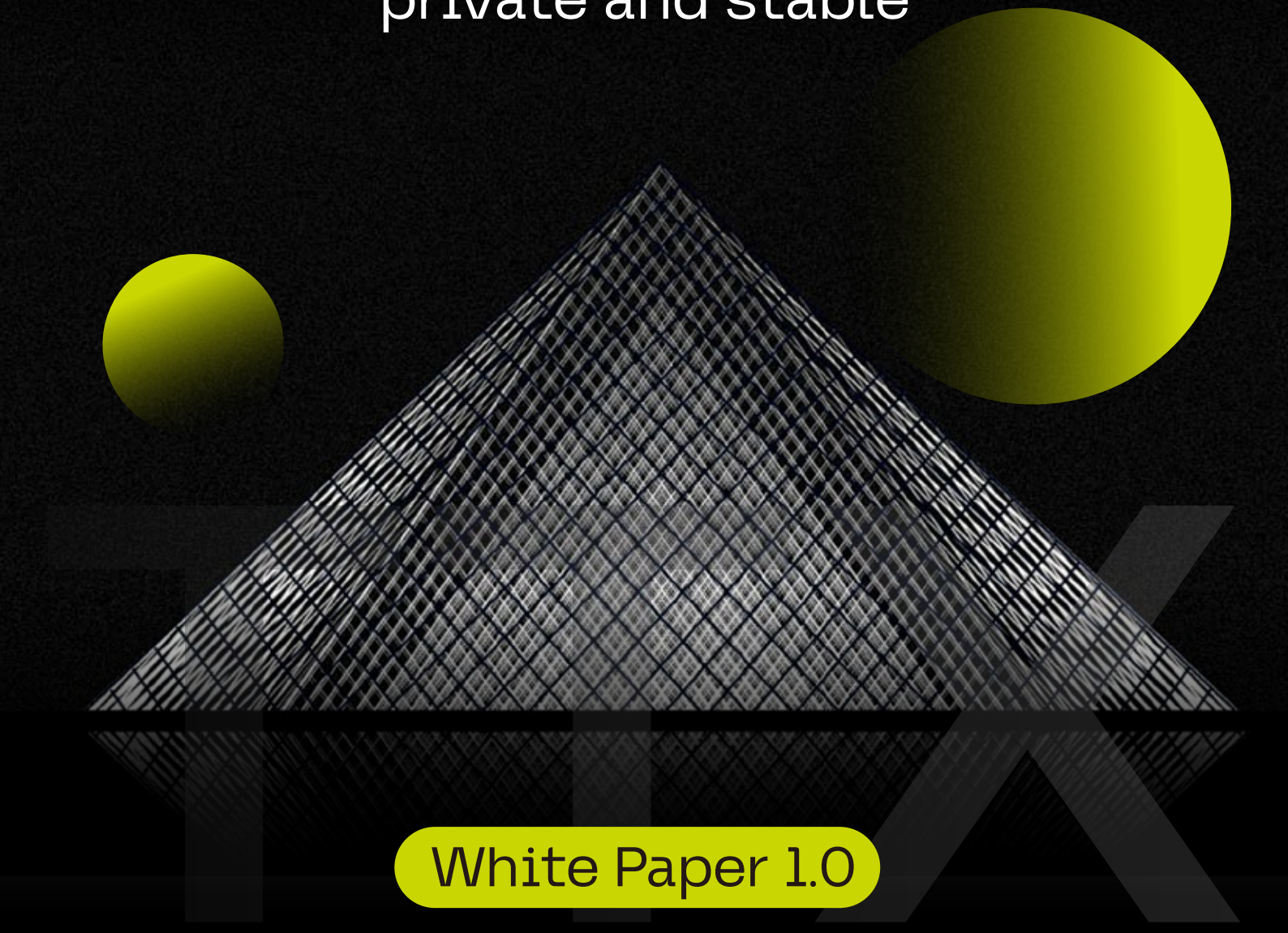
TTX

Constructing on-chain anonymization spaces

Making distributed applications truly secure private and stable



White Paper 1.0

Preamble

The rapid development of the Internet has made the flow of information very efficient, thus promoting the development of human society, but on the other hand, the privacy problem has also become more serious precisely because of the rapid development of the Internet. Blockchain, as the next-generation Internet of value, was once considered a very good tool for protecting privacy, but it was soon discovered that in the current major blockchain networks, once the address of a digital wallet corresponds to the personal information of its owner, all the account information and transaction information of the wallet's owner will be visible and impossible to eliminate throughout the entire network, which will lead to even more serious problems than the Internet's privacy leakage. This will lead to more serious problems than the privacy leakage of the Internet. Cryptography and top technologists in the blockchain industry have been working tirelessly on this issue, and several teams in the industry have developed special virtual currencies to protect privacy, which are called "anonymous coins", and some of the more famous digital currencies in the industry include Zero Coin (ZCash), Monero (ZCash (ZEC), Monero (XMR), Dash (DASH), etc. These digital currencies with certain privacy protection have gained a very high circulating market capitalization based on their huge market demand, and are ranked among the world's top 20 virtual currencies, which indicates that privacy protection is a very strong demand for the blockchain industry.

The invention of smart contracts, which are computerized protocols designed to informally disseminate, validate, or enforce contracts, has made the implementation of blockchain technology more feasible. However, it is frustrating that none of the blockchain systems currently in operation around the world support the cryptographic protection of smart contracts, and existing privacy protection mechanisms are greatly reduced in their scope of application by this technological limitation. If the anonymous blockchain systems that do not support smart

contracts, such as Cash and Monroe Coin, are the privacy protection solution 1.0, the smart contract-enabled privacy protection solution 2.0 is highly anticipated in order to enable the solution to be implemented in more industries and application scenarios.

It is undeniable that the anonymous blockchain system supporting smart contracts has a very high technological threshold, and only a handful of teams in the world are working hard on it, and now TTX is officially launching its products globally, and the R&D team of TTX ("TTX Team") is the only team in the world that can put forward a complete solution and has completed the major engineering research and development work on this issue. The TTX R&D team ("TTX Team") is currently the only team in the world that can propose a complete solution to this problem and has already completed the major engineering work. In addition, TTX Team does not consider the successful development of a privacy-preserving blockchain system that supports smart contracts as the end of the privacy-protecting solution for decentralized applications. In order to make the widespread implementation of privacy-protecting decentralized applications feasible, the TTX Team not only considers the protection of the privacy of accounts of users of DApps, the privacy of related tokens and the privacy of the process of transferring private data, but also fully takes into consideration the privacy of the user's accounts in the blockchain, and the privacy of the process of transferring private data in the blockchain. At the same time, the TTX team has fully considered the privacy protection strategy during the data transmission process of the blockchain system, which was previously restricted by the protocols of the various transmission layers, and even included the data privacy protection under the scenario of combining decentralized applications and Internet applications.

TTX

CATALOGS

Constructing on-chain anonymization spaces

Making distributed applications
truly secure private and stable

1 Analysis of the current state of the industry

In recent years, technology has continued to reshape our economies and lives as well as transform the world, with brand new financial networking technologies bursting out from the bottom, and blockchain becoming a world-famous focal point. The birth of blockchain is quite legendary, and the series of products it triggered: digital currencies, smart contracts, distributed governance, etc. have inspired various industry changes in the global field.

1.1. Status of the financial sector

In recent years, with the deepening of financial reform and opening-up, the market environment faced by the financial industry has improved considerably, especially since several financial crises, and governments at all levels have placed financial security and sound development in a very important position, taking a number of management measures, strengthening their own construction, preventing financial risks, and making great progress.

1.2 Digital transformation

Following the three industrial revolutions of mechanization, electrification and digitization, mankind has ushered in the fourth industrial revolution, which is also known as the digital economy. Digital economy refers to the new generation of information technology such as the Internet, cloud computing, big data, artificial intelligence, blockchain, 5G and so on as the engine. The new round of financial industry revolution brought by digital economy disintegrates and reconstructs the global financial industry value chain, and ultimately changes the business model as well as the value model of the traditional financial industry.

1.3 Wealth is being reorganized

In the context of the digital economy era, digital technological innovations and application innovations continue to emerge, the digitalization tipping point of the financial derivatives industry continues to be dismantled, and a new round of major industrial changes is restructuring social wealth. The digital economy is the result of the deep integration of digital technology and the traditional fields of economy and society, and more and more of the world's economic activities are taking place in the digital space. Digital economy can provide constant power for enterprise development, and can effectively promote the transformation and upgrading of traditional industries. The digital economy is changing the way of operation of the financial and financial derivative industries, with banks as the internal and external penetration impact, bringing disruptive changes to the traditional financial model and industry, and is step by step changing the value chain shaped based on the traditional model. The digital transformation of the traditional financial industry by digital technology has not only led to increasing cross-industry collaboration between banks and the service industry, but also to the blurring of the boundaries between the traditional financial industry, thus leading to the deep integration of the financial industry, the manufacturing industry and more value-added in the service industry under the digital economy.

1.4 The digital economy era

The future is a digital age, and without blockchain technology to back it up, the goals of the digital economy will not be realized. Blockchain allows all tangible assets to be digitally processed. Blockchain can establish a collaborative model of multi-party trust at low cost in an untrustworthy competitive environment, build a new type of transaction order and value system, and provide many solutions for the digital economy.

2 The unstoppable era of the digital economy

Blockchain is one of the most revolutionary emerging technologies in the field of information technology. By means of joint bookkeeping by multiple nodes in the network, data (blocks) are linked (chained) in chronological order to form a chronologically traceable and tamper-proof transaction record. The essence of blockchain is a value network, which realizes the circulation of value without any third party through distributed ledger, consensus mechanism, cryptography and peer-to-peer network, smart contract and other mechanisms.

Nowadays, the development and application of blockchain technology has swept through all walks of life, and has become one of the hottest and most popular information technologies. Compared with big data, cloud computing, artificial intelligence and other information technologies, blockchain seems to be a better solution for people's vision of the future of science and technology, with such characteristics as "decentralization", "tamperproof", "open and transparent" and so on. Compared with other information technologies such as big data, cloud computing and artificial intelligence, blockchain's features such as "decentralization", "non-tampering" and "openness and transparency" seem to be the solutions people envision for the future of technology.

The significant advantages of blockchain applications lie in optimizing business processes, reducing operating costs and enhancing collaboration efficiency, and these advantages have gradually emerged in many fields. The significance of blockchain technology is not only embodied in the technical level, but also in its change of social organization and collaboration, and grasping blockchain technology and industry can bring significant development opportunities for the social economy.

The emergence of blockchain has empowered all industries globally and provided a new system of data sharing.

The digital economy will reshape the world and mankind is crossing into a new era. Only by building a data sharing system can we meet the new era and challenges together.

Blockchain technology provides a reliable way to establish trust, reduces the cost of mutual trust, makes credentials electronic services more credible, efficient and secure, and solves the following four problems:

1) It can effectively identify the authenticity of electronic credentials without fear of malicious tampering or forgery.
2) The third-party hosting model can effectively reduce the cost of enterprise system construction and operation and maintenance, and the way of querying and obtaining electronic credentials from a credible third party provides a safe and reliable access channel for enterprises and users.
3)Solving the trust bottleneck faced by the data storage industry helps business; and
4) To record the summary of electronic credentials, flow records and other ways to make electronic credentials traceable, to meet the needs of business regulation and review.

The future is digital, but without blockchain technology to back it up, digital economy goals will not be realized. Blockchain allows all tangible assets to be digitally processed. Blockchain can establish a collaborative model of multi-party trust at low cost in an untrustworthy competitive environment, build a new type of transaction order and value system, and provide many solutions for the digital economy.

TTX Alliance Chain: A New Data Sharing System in an Anonymous World

The digital economy will reshape the world, data privacy protection has become a top priority, mankind is crossing into a new era, only to build a secure and trustworthy data sharing system based on blockchain cryptography technology under the blockchain, in order to meet the new era and challenges together, the TTX alliance chain will bring a brand new idea for the era of digital economy.

3 Introduction to TTX

TTX is the world's first blockchain system that truly realizes the privacy protection of Turing-complete smart contracts. Compared with the existing blockchain privacy protection technology, TTX not only realizes the privacy protection of account information and transaction information, but also realizes the privacy protection of Turing-complete smart contracts' inputs and outputs, and in addition, the developers can issue anonymous digital assets (Token) based on the smart contracts on TTX-Chain. In addition, developers can also issue anonymous digital assets (Token) based on smart contracts on TTX-Chain, and the communication information with smart contracts will also be protected by privacy and security.

TTX has redesigned the blockchain structure and various underlying protocols to make privacy-protecting Turing-complete smart contracts a reality, which not only enables a wider range of application scenarios to obtain privacy protection measures, but also further improves the difficulty of attacking the privacy of user data because of its advanced NIZK cryptography algorithm. In addition, it improves the practicality of the current NIZK encryption algorithm, greatly reduces the memory resources it needs to consume, and improves computational efficiency. In addition, compared to the mainstream anonymous blockchain systems on the market, TTX's support for Turing's complete smart contracts and privacy protection measures for its related decentralized applications have greatly generalized its usage scenarios.

By building a sharing network of machine trust, solving the problems of data access, encrypted transmission, sharing, credible transaction, storage, etc., realizing the safe up-linking of data and assets of various industries around the globe, promoting more industrial individuals to join the alliance for data fusion, maximizing the value of data, and jointly building a digital economic alliance with borderless circulation of data, open sharing of value, and collaborative innovation of industries.

1. TTX Affiliate Chain Purpose:

Fair, just, open, co-creation, sharing, win-win situation

2. TTX Union Chain Initialization:

Everything is data-enabled. Through the blockchain distributed data storage, unite global individuals, enterprises and institutions to realize data and assets on the chain storage, and create a massive database.

Data Assetization. Through encrypted storage and peer-to-peer transactions, data rights and interests are privatized and the use of public, in the form of Token, to realize the unimpeded circulation of digital assets.

Asset Sharing. Construct a secure and trustworthy digital economy alliance, realize the optimal allocation of resources within the alliance, reduce the cost of resource integration, improve efficiency, stimulate social productivity, and build a DT value ecosystem.

3. TTX affiliate chain advantage:

TPS modularization, the minimum of 3,000, the TPS function to make a module, different applications to build different modules. In the traceability and authentication, the minimum TPS is 3,000, and in the logistics tracking scenario, it can be up to 62,000.

Ten million flow community consensus, Southeast Asia, China, South Korea, Australia and other 20 countries and regions synchronized launch, to create a global coverage of the digital economy alliance.

4、TTX alliance chain technology characteristics

Low cost and high efficiency

The public, secure, and low-cost TTX blockchain private cloud service features high availability, security, and ultra-aggregated platform deployment.

highly compatible

TTX has standardized and modularized the design of the underlying complex technical system and heterogeneous systems, and is compatible with all kinds of consensus algorithms, encryption algorithms and interaction protocols, so as to realize cross-platform, cross-chain and cross-application data interaction and sharing.

open intelligence

TTX is committed to creating an open platform where users do not need to pay attention to the details of the underlying implementation of the blockchain, and can create blockchain and various applications with low threshold by calling simple interfaces, which in turn enables the financial derivatives industry to focus more on the realization of business logic.

safe and trustworthy

TTX provides a powerful smart contract platform and integrates a variety of cryptography to encrypt the transmission and storage of transaction information, making the data more authentic and trustworthy, thus guaranteeing the continuous stability and security of the entire network.

Chained Anonymous

TTX will create a completely anonymous and public on-chain ecosystem where user transactions and account information can be anonymized on the chain. The data in ordinary transactions are encrypted, and details such as source, destination, asset type, amount, etc. cannot be known to non-transacting parties.

high utility

While TTX hides transaction data, it does not include all information, which would be uneconomical and operationally inefficient, and is developed in phases, taking into account users' existing habits and pain points.

5. TTX Alliance Chain Objectives

The ultimate goal of TTX Alliance Chain is to build a digital economy alliance with borderless circulation of data, open sharing of value and collaborative innovation of industries. Utilizing blockchain, big data, IoT, AI and other cutting-edge technologies, it realizes the safe uploading of data and assets from various industries around the world, promotes the integration of industrial data, connects physical value through massive data, creates a global value internet, and realizes the unity of the "five streams" of business flow, capital flow, information flow, logistics, and user flow, so as to enable the subjects within the alliance to create greater value, and jointly To build a digital economy alliance ecosystem of open sharing, collaborative innovation and sustainable circulation.

Sharing data, ecological profit generation!

TTX alliance chain not only provides a technical platform for safe and credible data sharing, but also unites several industry organizations to jointly build a data highland.

TTX Alliance Chain will create a digital economy alliance with borderless circulation, integration and sharing, and collaborative innovation, and play an important role in the fields of digital traceability, digital upgrading, and digital finance. It can be said that TTX alliance chain will open an era of data sharing in which rights and interests are privatized, use is publicized, and unlimited value of digital can be exerted by the way of distributed nodes!

In the future, the Internet environment will change from relying on authority and system to gradually relying on technology to reach trust, and the application of trustworthy electronic credentials based on blockchain will enable the legitimate rights and interests of all parties involved in business to be truly guaranteed, and help to completely realize the paperlessness of credentials.TTX takes the data of the financial industry as the starting point, and attracts more organizations, individuals and industries to join the alliance with the advantage of openness and sharing, to build the next-generation Internet of value. TTX will be the core component of the next-generation value Internet architecture, become an important portal connecting the virtual and real worlds, and comprehensively construct the key infrastructure for the digital transformation of the economy and society.

4 Ecology and Applications

TTX Coalition Chain is suitable for scenarios where multiple parties are involved and trust needs to be established between them. The trusted data of blockchain between multiple parties improves the transparency and sharing of information, thus simplifying the business model, reducing the cost of trust under the traditional model and improving efficiency.

Blockchain has a wide range of application scenarios. Based on the characteristics of blockchain's disintermediation and shared trusted ledger, from the perspective of building an industrial ecosystem, we can jump out of the mindset of looking at the problem only from our own point of view, and discover more potential business opportunities by combining our own business scenarios.

TTX takes blockchain+industry development, ecological construction, and multi-chain integration as its focus, Cosmos blockchain technology application in various fields, and continuously links more digital economy participants, including individuals, entrepreneurial projects/enterprises, regulators, banks, venture capital institutions, etc., and digitally converts industrial resources with the help of cutting-edge technologies, such as AI, big data, cloud computing, 5G, and the Internet of Things, to accurately collate, widely It will realize the digitalization and upgrading of the real industry, and create a digital economy platform with borderless circulation of data, open sharing of value, and collaborative innovation of the industry.

Eco-Apps:

financial

Trading area, wealth management, derivatives trading, collateral management, supply chain finance

disbursement

Micro-payments, B2B international remittances, tax reporting and statistics, personal identification (KYC), anti-money laundering (AML)

consumer sector

Sharing economy, supply chain management, drug tracking, agri-food certification, logistics management

be bound to

Claims filing, claims processing and management, fraud monitoring, telematics and rating, digital authentication

media, esp. news media

Digital rights certification, art certification, advertisement placement, real statistics of advertisement clicks, sales of licensed assets

underlying asset

Diamonds, designer brands, car rental and sales, home mortgages, land ownership, digitization of real assets

medical cosmetology

Product traceability, account registration, file uploading, distributed storage, comparative authentication, token trading, comprehensive credit value

socialize

Social interaction is a key part of the crypto world, the sinking and floating of the project is determined by the community and network system they create, the emergence of TTX can allow users to deeply understand the results of their investment and the state of the landing application, through TTX to break the user transaction in the communication of the trust barriers.

Big Data Applications

Big data is the most strategic core ability of intelligent network and intelligent terminal in the future. The future application of big data is mainly in two aspects: community ecological big data based on open ledger and collaborative network, providing relevant information services for the exchange and community users; and quantitative investment support and risk control focusing on individuals (intelligent terminals).

social management

Voting, vehicle registration, benefit distribution, copyright protection, education and accreditation

As a blockchain + infrastructure provider in the era of digital economy, TTX will integrate big data, cloud computing, 5G, AI, IoT and other high-tech to reach the "protocol layer of blockchain solutions", and build a huge integrated ecosystem for industrial chains in different fields.

Technology Applications;

Technology + Underlying Network - Creating an Automated Operating Layer

TTX uses blockchain distributed ledger to structure the identity authentication management hierarchy system from the bottom, signing the multiple signature registration binding management of dual private keys to satisfy the decentralized regulation of decentralized network and the governmental accessibility commercial grade regulation requirements. In order to meet the commercial demand, TTX uses credit consensus mechanism to allow more merchants and users to participate in it, and issues universal digital currency TTX COIN to realize the data transaction and circulation within the system.

App+Protocol Middle - Creating a digital management layer

TTX smart contract upgrades the application chain with blockchain technology at the application level to realize the barrier-free circulation of business flow, logistics, information flow, capital flow and user flow in the digital era. Taking user demand as the core, it realizes the flattening, communityization and sharing of data, shortens the transaction links from upstream brands, downstream terminals to consumers, and reduces social duplication. Super 3000's ODPS data system can realize the integration and linkage of each link - helping brands to cover terminals, helping terminals to purchase from upstream directly through the platform, and realizing the interconnection of individual platforms.

Ecology + Open Services - Building an Intelligent Decision-Making Layer

TTX is an open alliance platform system that supports the government, third-party organizations and all third parties in the upstream, midstream and downstream of the supply chain to carry out commercial application development on this basis, and provides intelligent decision-making through intelligent analysis of data by means of AI, big data, cloud computing, 5G, and the Internet of Things, in order to promote the long-term growth of the real economy, as well as to promote the combination of finance and the real economy, to reduce the financial risks, and to create a multi-center, digital economy platform that is distributed according to labor, value contribution, and fair distribution of benefits.

TTX

5 TTX technology

TTX supports deployment and expansion based on private and public clouds; supports node-controllable authorization access, multiple encryption algorithms, multiple consensus algorithms; supports high-performance autonomous smart contract engine, provides governance and operation and maintenance support for blockchain system, and can conduct real-time monitoring of the operation status of the entire network.

TTX Alliance Chain Security

1. DPOS model

Security was our main concern in designing the TTX Coalition Chain, which uses the so-called "provably secure DPOS blockchain protocol". The algorithm has the following five properties that make it a very secure DPOS model.

First, the model focuses on persistence and activity, two formal properties of a healthy transaction ledger. Persistence means that once a node of the system declares a transaction as "stable", the rest of the nodes (if queried and responding truthfully) will also report it as stable. Here, stability will be understood as a predicate that will be parameterized by some security parameter k, and affect the certainty of property holdings. (e.g., "more than k blocks deep".) Activity guarantees that a real generated transaction will be stable once it is made available to a network node with enough time, say u time steps. The combination of activity and persistence guarantees a healthy transaction ledger, in the sense of taking a real generated transaction and making it constant.

Second, we describe a new DPOS-based blockchain protocol. Our protocol assumes that participants are free to create accounts, receive and make payments, and that these rights change over time. We utilize a very simple, secure, multi-party implementation of the voting protocol to achieve randomness in the first election process.

This prevents so-called grinding attacks and distinguishes our approach from other previous solutions. Furthermore, the uniqueness of our approach lies in the fact that the system ignores round after round of ley modifications. Instead, the current population of stakes is recorded at regular intervals, called epochs; at each such interval, a secure multi-party computation occurs, utilizing the blockchain itself as the broadcast channel. Specifically, in each epoch, a group of randomly selected libertarians forms a committee, which is then responsible for executing a coin-flip protocol. The outcome of that protocol determines the next set of stakeholders to execute the protocol in the next epoch, as well as the outcome of all first elections in that epoch.

2、technical architecture

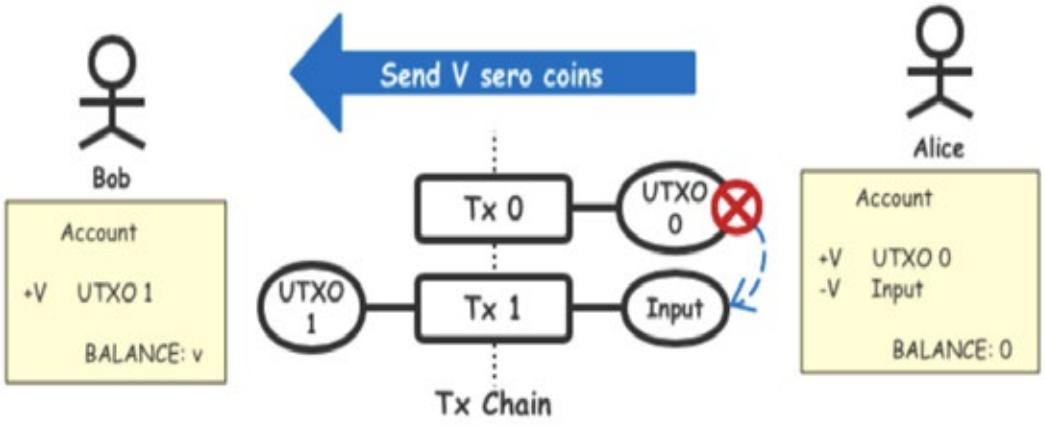
TTX Anonymous Token Issuance Principle

TTX is the world's first privacy blockchain system to support Turing-complete smart contracts. since it supports smart contracts, of course, it can't be a simple smart contract + anonymous coins. tTX deeply integrates the advantages of the two: the openness of the smart contract, the closedness of privacy system. With the support of these two features, TTX's smart contracts have very exciting characteristics and can do some amazing things.

2.1, UTXO and ACCOUNT

Readers who understand what constitutes a blockchain should know that a blockchain is a distributed ledger, each of which contains multiple transactions Tx, and each of which in turn contains multiple records. The smallest unit of the ledger is the record, each of which records the inflow or outflow of an account's assets. However, in terms of the actual implementation, depending on the way the asset outflow is recorded, the blockchain system has evolved two different bookkeeping implementations, which we call the UTXO mode and the ACCOUNT mode, respectively. These two modes correspond to the Bitcoin and Ether modes, respectively. TTX, on the other hand, uses a more complex hybrid model.

UTXO-based transactions



As shown above, there are two types of records in the UTXO mode, Input and Output for the transaction initiator, and this Output is the Unspent Output (UTXO) in the view of the transaction receiver until the transaction receiver initiates another transaction and specifies an Input to nullify this UTXO. The records in the transaction are always linking the various Inputs and Outputs. In this model, ACCOUNT is not required as a state summary.

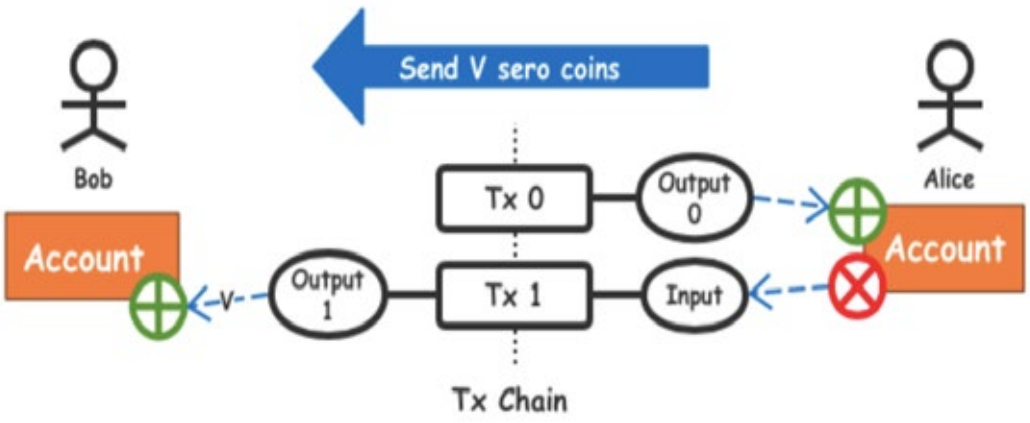
For example, in the above figure, Alice has previously received a transaction Tx 0, this transaction has an Output UTXO 0, there are V TTX coins in UTXO 0, she can record [+V TTX, BALANCE=V] on her account. And later she transfers these V TTX coins to Bob, then she generates a transaction Tx 1, this transaction has an Input to nullify UTXO 0, then Alice's ACCOUNT should record [-V TTX, BALANCE=0]. As for Bob, he then adds a UTXO 1 with a value of V TTX, and if his ACCOUNT was preceded by a BALANCE of 0, it can record [+V TTX, BALANCE=V] on its account.

This model has two advantages:

UTXO mode each transaction is independent of each other, which means that as long as you can deal with the problem of double spending, transactions under one account can be processed in parallel, and you can fully apply the power of multi-core CPUs.

UTXO is essentially a history-based form of recording, both the process and the result, and therefore has a very strong advantage in some applications where witness proofs need to be generated. This is why blockchain systems with privacy features are basically UTXO models.

ACCOUNT-based trading



Previously the UTXO mode talked about how each account can generate a temporary ACCOUNT as a status summary, and in the UTXO mode, this account is temporary, not required. Whereas in the ACCOUNT mode, each asset inflow and outflow record in a transaction references an ACCOUNT instead of a UTXO, and the record Input indicates an increase in the assets of this ACCOUNT, while the record Output indicates a decrease in the assets of an account. In this mode, the ACCOUNT entity is required, without this ACCOUNT, all records are meaningless.

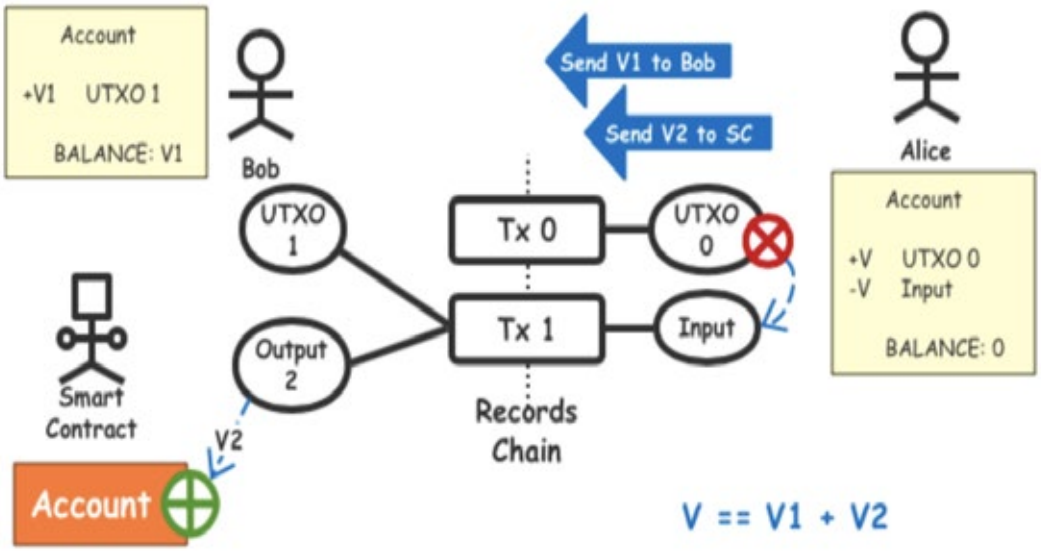
As above, for example, Alice has previously received a transaction Tx 0, which has an output Output 0 with an asset value of V TTX, and her ACCOUNT will be increased by V TTX. At this point, she wants to transfer V TTX coins to Bob, so she initiates a transaction with an Input pointing to her ACCOUNT valued at V TTX coins, and an Output 1 pointing to Bob's ACCOUNT also valued at V TTX coins, then this transaction will be processed by the system by directly adding or subtracting the assets of both parties. Output 1 points to Bob's ACCOUNT, which is also worth V TTX coins, and the transaction is processed by the system by adding or subtracting assets from both parties' ACCOUNTs. In this mode, Alice cannot distinguish whether this Input is using the TTX coins entered by Output 0 or the TTX coins that have been previously stored in ACCOUNT.

ACCOUNT mode also has two advantages

The ACCOUNT mode directly adds or subtracts assets from a separate account, and can add or subtract any number of assets from an account with only one record. As a result, the size of the records generated is much smaller than those generated by UTXO in the same situation.

The ACCOUNT model is essentially state-based, with Input and Output being the process and ACCOUNT being the result, so it is naturally easy to introduce Turing machines into the mix, which is why blockchain systems that support Turing-complete smart contracts mostly use the ACCOUNT model.

Mixing Modes for TTX



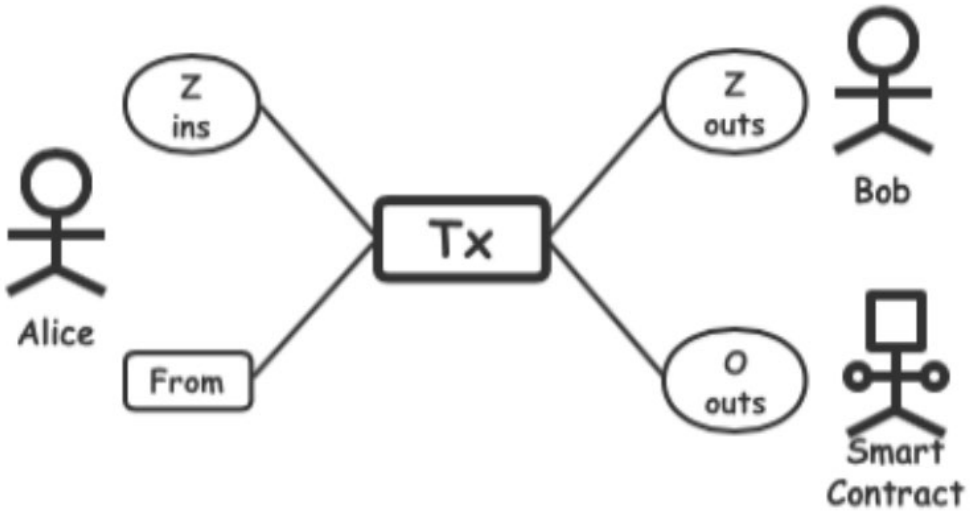
TTX applies a hybrid of the UTXO and ACCOUNT modes, using the UTXO mode where it needs to support privacy protection and the ACCOUNT mode where it needs to run a smart contract.TTX seamlessly integrates the two modes through transactions, consensus, and the Pedersen Commitment algorithm, enabling smart contracts to perform surprisingly well in terms of their capabilities.

2.2. Anonymous transaction structures

In the BetaNet network, anonymity is mandatory for normal TTX transactions. This is because if arbitrary non-anonymous transactions can be allowed, the privacy and security of users who want to use the anonymity feature will not be guaranteed in the associated transactions. In addition, if one wants to publicize information such as one's assets, it is recommended to use a smart contract to disclose some of the information in a limited way.

At the time of the MainNet release, TTX obtained a balance between privacy and generation speed by choosing a privacy level.

Trading Tx

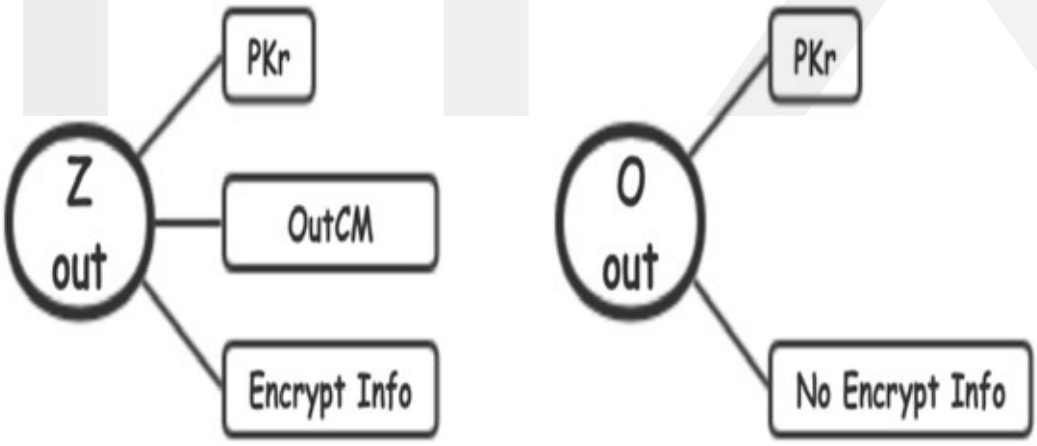


The anonymous transaction Tx of TTX has an anonymous input set Z ins, an anonymous output set Z outs, a common output set O outs, and a staging address named From. Z ins is completely anonymous, making the source and content unavailable to third-party observers, Z outs is a completely anonymous UTXO, and only the receiver can view and use its content, and O outs carries non-hidden content, and it points to the recipient in one of two ways: either to a smart contract address or to a staging address. from represents the transaction sender, which is also a staging address. Therefore, the entire Tx does not allow anyone to determine who the real user is, and the information carried in it, such as assets, is also hidden to the greatest extent possible.

Input Z ins

In the set of inputs to a TTX transaction, Z ins, each input is anonymized, including the Id of the source UTXO as well as information about the assets carried. Each input points to a specific certain UTXO that is hidden in a huge sequence of UTXOs that are part of the TTX history by employing a Proof that is generated by the Zero Knowledge Proof ZKP, and all the detail information is hidden by the Proof. Without knowing the details, the verifier can confirm that the input is legitimate through the Proof. This approach is very similar to ring signatures, but the size of our Proof itself is much smaller than ring signatures, and the range of sets used to hide UTXOs under zero-knowledge proofs is also much larger than ring signatures.

Two different outputs outs



The outputs included in the TTX transaction are of two forms, the zero-knowledge output Z out and the ordinary output O out.

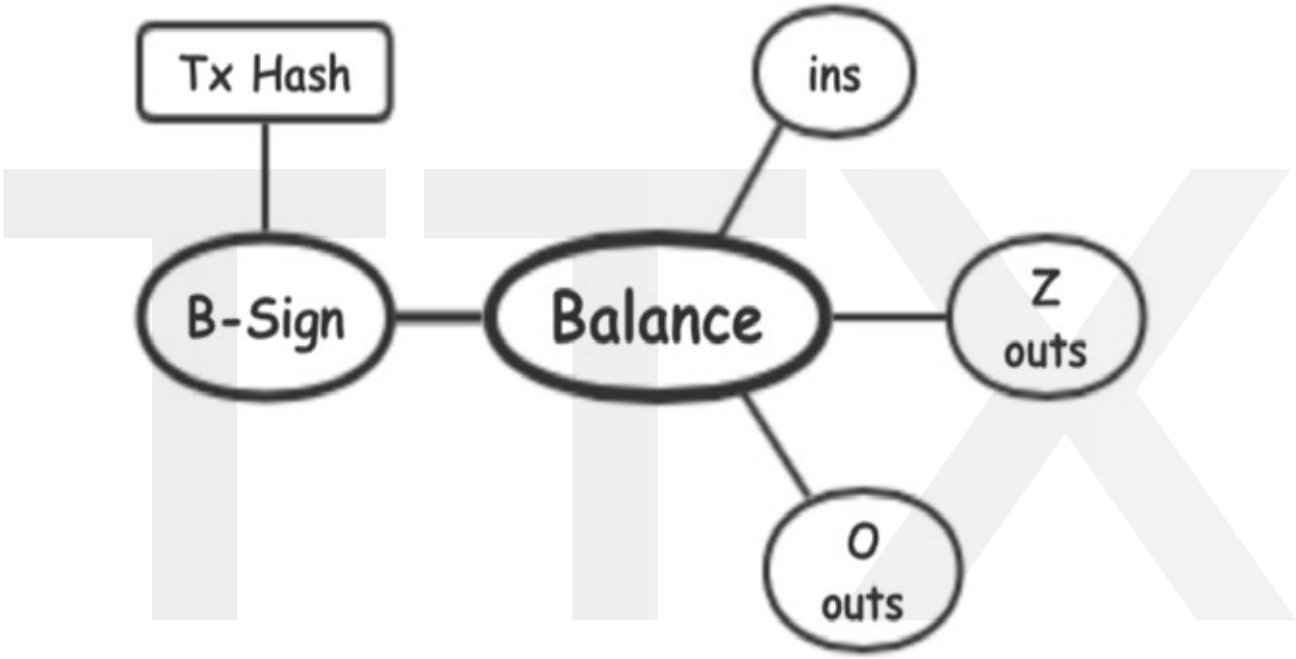
Z out

Z out points to the staging address PKr, which can only be decrypted for identity by the recipient. Since every staging address is different, no third party can recognize where Z out is pointing. z out also carries Encrypt Info, the encrypted information of the asset, which can only be decrypted by the person who holds the recipient's private key. The OutCM is an output promise, and only the two parties to the transaction can reproduce the computation of the OutCM, which plays a crucial role in proving that "Z out is referenced by ins".

O out

There are two forms of PKr that O out points to, one is initiated by the smart contract and points to the general account's staging address. The other is initiated by an ordinary account and points to the address of the smart contract. Due to the randomness of the staging address, the third party has no way of knowing the identity of the recipient, and the asset information carried by O out is public.

Balance of inputs and outputs Balance



Tx pack ins, Z outs, and O outs together, how to prevent malicious attackers from tampering with the data inside and secure the assets, we do so by introducing perdesen commitment, whose homomorphic encryption property allows the verifier to confirm that Balance must be balanced, i.e., input equals output, without knowing the details of the message.

In addition, to prevent the tampering of O outs by malicious attackers, we utilize the random nature of perdesen commitment to sign the Tx Hash with the random part of Balance. In this way, each input and output can be computed independently and then packed together by B-Sign.

Transaction Sender From

When the output of a transaction is directed to a smart contract, the smart contract sometimes needs to output resources to a given account according to the rules written. The From address is the place where the output resources will be taken. from is determined when the transaction is generated, and is only used once, so that no one can locate the sender except the sender of the transaction.

III. Principles of issuing anonymous Token

Token Assets

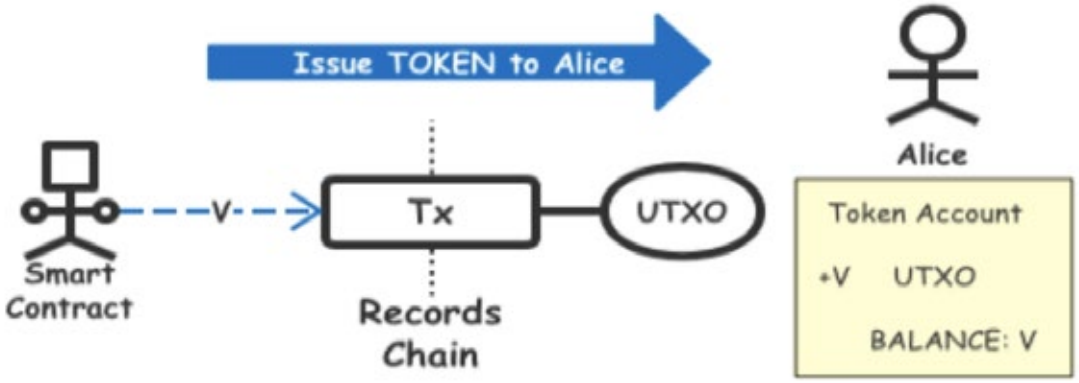
Token, also known as "homogenization pass", is a form of asset recognized by the TTX system, and the same type of token can be divided and mixed in any way. The same type of Token can be arbitrarily divided and mixed, specifically the so-called "coins". TTX Coin, as the first coin of the TTX system, is essentially a Token, and Token assets are treated the same way within the TTX system, except for the handling fee that can only be paid in TTX Coin, which is guaranteed by consensus. Token assets are treated in the same way within the TTX system, and their privacy and security are ensured by consensus.

Unlike the concept of Token in Ether, which is just a symbol recorded inside a smart contract, ETH is the real Token asset running inside Ether.

name of coin

Each Token has a coin name, and after the TTX system is initialized, there is only one registered coin name TTX by default. when a smart contract issues an anonymous Token, it must register a globally unique string with the TTX system as the coin name for that Token. Coin names can greatly improve the readability of your issued assets.

Anonymous Token Assets



TTX's smart contract has a very powerful feature that allows it to issue anonymous tokens as often as it likes, provided you have a coin name that has never been registered before. Once the anonymous Token is issued, the smart contract can send the Token in the form of an ordinary transaction to a common account's temporary storage address PKr, at which point these sent Token will be detached from the smart contract account in the form of UTXO, and, like TTX coins, enter the user's personal account, thus being protected by TTX's privacy mechanism.

The issuance of TTX coins is realized by miners, and the process is similar to the mechanism of issuing anonymous Token by smart contract, which is the built-in Token issuance function of TTX.

3. Smart Contracts

rt contract is an extended function provided by the chain, but for security reasons, it will not register contracts arbitrarily. The chain will provide some contract templates to provide basic management functions for uploading and downloading files. The client must access the file through the contract.

TTX adopts the Docker container program to provide an isolated security environment. Smart contracts run in Docker containers, which can be isolated from the chain system to ensure the security of contract execution. Users can use G0 language to write smart contracts according to TTX technical documents, and the Docker container solution can provide good system compatibility.

TTX will realize a customized lightweight virtual machine solution, and the smart contract will be executed in the virtual machine, which ensures the isolation of data from the chain and avoids security risks. Meanwhile, it is more efficient than Docker container solution, supports controlled I0, and has built-in rich microservice interfaces. Relying on the testing platform of the research institute, TTX will introduce a smart contract security testing system during the design and development process, provide testing tools to detect security vulnerabilities in smart contracts, and help users find and solve security problems in contracts.

After the whole ecosystem is perfected, there will be more demands, and the chain can provide more contract templates, and all these functions do not need to change the underlying chain, but only need to register new contracts.

(1) Virtual machines

On-chain smart contracts are developed using Turing's complete language. The syntax can be adapted to support Lua, C#, and other languages. The results of virtual machine execution are recorded on the chain, eliminating the need for all nodes to run virtual machines and reducing the load on the entire blockchain network.

(2) Contracts

Within a system like Ether, contracts can be registered and invoked at will. This is a great benefit for scalability and experimentation. However, within our storage system, we support arbitrary contracts, but they require certain permissions to register on the chain. To a certain extent, it limits the types of contracts, but it is controlled for the stability of the whole network, as well as for the direction of future development. At the same time, for the future development of the need to add new contracts, its scalability and flexibility has not been affected in any way.

4. Network Services

TTX supports peer-to-peer P2P communication based on the TCP/UDP communication protocol. Node roles can be customized and extended according to usage, separating nodes that do not participate in consensus but only store or read data to share the query burden of the main network.

Each node uses P2P network technology to organize the network, supporting dynamic joining and exiting of multiple nodes. The joining and exiting of nodes are controlled by privilege management, and new nodes need to be unanimously agreed by the existing nodes before they can be successful.

5. Permission Management

Privilege management is responsible for managing the privileges of all nodes participating in the TTX, and different privileges are granted to different nodes. In addition, the permission management module is also responsible for the access, read and write permissions of TTX, and the data on the chain can only be accessed by authorized users.

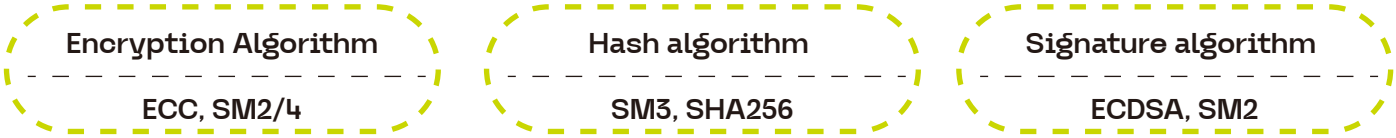
Based on the consideration of anonymous verification of data among nodes, the TTX R&D team is developing zero-knowledge and ring-signature algorithms, which will be online in the subsequent versions.

6. Security Mechanism

The design of TTX requires full consideration of enterprise-level security requirements, using encryption mechanisms that comply with national and international standards, and there are corresponding security measures in the deployment of server implementation. The block and chain structure, hash algorithm, asymmetric encryption and signature algorithm all support the state secret algorithm.

TTX PKI-based certificate system does node authentication, CA server manages the issuance and destruction of certificates, and nodes use digital certificates for authentication and encryption/decryption, preventing security problems caused by events such as repeated use of node certificates, repeated login of nodes, and node exit.

Currently supported cryptographic algorithms are.



TTX has implemented Raft and PBFT consensus algorithms.

Raft is a distributed consistency algorithm implemented on the basis of Paxos, with a simple structure and the same function and performance as Paxos. In the scenario of coalition chain, TTX has modified and implemented Raft to adapt to the blockchain, which can ensure the consistency of the system in the case of half of the nodes failing.

PBFT is a Byzantine fault-tolerant algorithm, which is able to tolerate f Byzantine nodes when the number of nodes is not less than n=3f+1. However, due to its low communication efficiency, it will be subsequently improved on this basis.

In addition, the TTX research team is working on a scalable Byzantine fault-tolerant algorithm, which can dynamically adjust the algorithm according to the network environment and security situation, and can improve the tps without decreasing the fault-tolerance through multi-node parallelism.

6 Distribution program

6.1 Issuance rules

The total number of TTX issued is 1.1 billion coins, with 10 million mother coins, and all of the TTX are produced through POC hard disk mining in the early stage. And as a user in the TTX chain settlement bookkeeping and the use of digital assets, as an important medium of communication between all parties, is an indispensable and important part of the entire ecology.

6.2 Distribution mechanism

45% goes to dividends on coin holdings; 50% goes to mining incentives; and 5% goes to the total dividend pool.

6.3 Gain on holding

Holding a certain amount of TTX can participate in the dividends of holding coins, the minimum holding amount can be dynamically adjusted; proportional dividends according to the ranking of holding coins; a total of 1.1 billion coins, the first 10 million coins, the first year of the monthly growth of 10%, followed by one year of the monthly growth of 9%, and then one year of the monthly growth of 7%, the fourth year of the annual growth of 6%, and the fifth year of the monthly growth of 5% until 1.1 billion coins have been issued.

$$A_i = \frac{M_i}{M_1 + M_2 + M_3 + \ldots + M_n} \times \frac{W}{2}$$

M is the ranking of TTX holdings, those holding the same number of TTX are ranked uniformly, W is the total number of TTX issued in the country at that time, and A is the gain from that user's holdings on that day.

6.4 Mining Rewards and Promotion Benefits

In the first period, TTX is produced through POC hard disk mining, which can be used by users for circulation or wallet holding, and 50% of the total daily output is used for arithmetic calculations with the following

$$B_i = \frac{X_i}{X_1 + X_2 + X_3 + \ldots + X_n} \times \frac{W}{2}$$

formula:

Daily new TTX releases, of which 50% are automatically allocated based on the proportion of the total computing power of the linked user base

$$Ai = \sqrt[3]{P_{max}} + P1 + P2 + P3 + \ldots\ldots Pn$$

X is the propagation power of the user point, W is the total amount of TTX coins issued in the whole network at that time, P_{max} is the number of TTX coins at the maximum intervention point, and P is the ordinary intervention (the performance of the team with ordinary access is multiplied by 10 for those below 10,000 to calculate the promotion arithmetic, and not multiplied by 10 for those beyond).

7 Future plans

TTX alliance chain believes that under the new economic model of blockchain, breaking through the barriers of country, region, language and circulation, TTX will help the data-centered digital light economy United Illumination to achieve off-speed development. To create an innovative economy. To build a shareable digital economy alliance, it will open up the data resources of various industries around the world, change the productivity relationship of all players in the business model through the alliance ecology, and better promote the globalization of the digital economy alliance with the support of the Foundation.

Off-chain computing and homomorphic cryptographic smart contracts

In fact homomorphic encryption for smart contracts is already in the substantial development phase, and we have found a way to balance data security (a mechanism that can be oriented towards computers leaving sensitive data behind) with performance through on-chain and off-chain computation, and plan to complete this work within 6 months.

Wallet and other eco-applications TTX's decentralized wallet application is also currently under development and is scheduled to be officially released by 20193. Due to TTX's support for developers to issue their own Token, TTX's wallet will support the management of TTX's own Token as well as the cryptocurrency assets of all developers based on the Token issued by TTX.

Latest consensus mechanisms

We will release a new consensus mechanism, TTX- Random, in some version within 1 year, which combines the latest PBFT theory and VRF algorithm to design a consensus mechanism that can relatively balance the fairness and efficiency.

The Three Musketeers of Privacy

TTX has two brothers, Alien Protoco and Castrol Protoco, the former provides a distributed DNS system to realize the stable operation of the network and information transmission through automatic addressing, and the latter achieves cryptographic privacy protection for the addresses of nodes, forming a complete decentralized privacy protection scheme for applications. protection program.

Secure Multi-Party Computing

In many cases, the proof of data needs to be combined with an existing centralized data source, which can also be an off-chain data source. Currently, the strategy for solving the above problem is to assume that there is a trusted service provider or to assume the existence of a trusted third party. However, in the current volatile and malicious environment, this is extremely risky, and in the face of this problem, the generalized Secure Multi-Party Computing problem can be solved.TTX will also consider introducing Secure Multi-Party Computing (SMC) in the future, so as to achieve broad support for off-chain data under the premise of privacy protection.

multichain chain system

Multi-chain system is the scalability solution for TTX, which will be scaled horizontally based on a multi-chain system using a mechanism similar to Ether Plasma. The Plasma-like multi-chain parallel computing mechanism will enable TTX to reach an extremely high level of state updates per second (possibly billions). This will enable TTX to replace the current centralized clusters in terms of performance, and give TTX the prospect of handling all kinds of privacy-related decentralized applications around the world.

8 Development Plan

- March 2020 Team building Project preparation launch
- June 2020 White paper released Initial construction of the main chain
- August 2020 Core technology research and development Main chain construction completed
- September 2020 Wallet development Mainnet testing
- November 2020 Completion of the construction of the digital source platform
- January 2021 Improvement of the Digital Economy Coalition system
- March 2021 Tourism, real estate, mall circulation on the ground
- August 2021 Enriching application scenarios Traceability applications on the ground
- December 2021 Radiant Global Eco-Expansion
- 2022 Ecological Iteration

9 Risk Warning and Disclaimer

1. Risk Alert

(1) Risks related to judicial supervision

Blockchain technology has become a major subject of regulation in every major country in the world, and applications or tokens may be affected by regulatory bodies if they intervene or exert influence. For example, if decrees restrict the use and sale of electronic tokens, tokens may be restricted, hindered or even terminate the development of applications.

(2) Risk of lack of attention to the application

The possibility exists that platform applications are not being used by a large number of individuals or organizations, which means that there is not enough public interest in developing and growing these relevant distributed applications, and such a lack of interest could have a negative impact on tokens and applications.

(3) Risk of competitive expansion

There is a certain amount of competition between blockchain tokens, and assuming a stronger rival emerges in the industry, it will inevitably suffer.

(4) Risk that the relevant application or product does not meet the expected standards

The platform itself may undergo major changes during the development phase before the release of the official version, or the market may undergo huge changes before the release, causing the platform to fall short of expectations in terms of functionality or technology. Or, due to incorrect analysis, the platform's applications or tokens fail to meet expectations.

(5) Risk of cracking

The techniques currently used cannot be cracked, but assuming cryptography advances rapidly, or computer computing speeds advance rapidly, such as the development of quantum computers, there may be a risk of cracking, leading to the loss of tokens.

(6) Other notes

Please fully understand the development plan of the operating platform as well as be clear about the risks associated with the blockchain industry, otherwise it is not recommended to participate in this investment, if you make an investment, it means that you confirm that you have fully understood and recognized the terms and conditions in the bylaws.

2. Disclaimer

This document is for informational purposes only and does not constitute an opinion regarding the purchase or sale of this program. The above information or analysis does not constitute a reference for investment decisions. This document does not constitute any investment advice, investment intention or abetting investment.

This document does not constitute, nor is it to be construed as, an offer to buy or sell, nor is it a contract or commitment of any kind.

Relevant intended users need to clearly understand the risks of the project, once investors participate in the investment that is to say that they understand and accept the risks of the project, and are willing to personally bear all the corresponding results or consequences.

The Operations Team shall not be liable for any direct or indirect damages resulting from participation in and as a result of this program.