HCTN

HCTN
WHITE PAPER

Preface

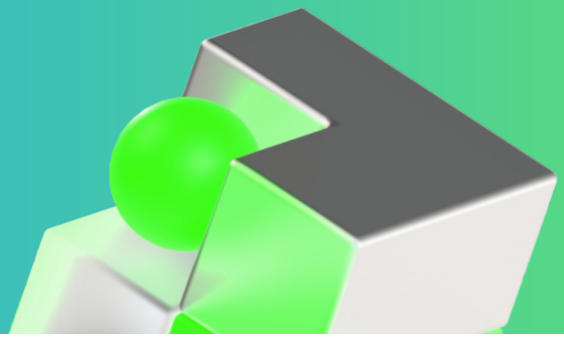
The rapid development of the Internet has made the flow of information very efficient , thus promoting the development of human society . However, on the other hand , the privacy issue has become more serious because of the rapid development of the Internet. As the next generation of value Internet , blockchain was once considered a very good tool for protecting privacy , but everyone soon discovered that in the current major blockchain networks , once the digital wallet address and its owner's personal information are matched , all account information and transaction information of the wallet owner will be visible in the entire network and cannot be eliminated , which will lead to more serious problems than privacy leaks on the Internet. For this reason, cryptography and top technical experts in the blockchain industry are making unremitting efforts . Several teams in the industry have developed some special virtual currencies that protect privacy . This type of virtual currency is called "anonymous currency" . The more famous digital currencies in the industry include ZCash (ZEC) and Monero. (XMR) , Dash (DASH) , etc. These digital currencies that have adopted certain privacy protection have obtained very high circulation market value based on their huge market demand , and are ranked among the top 20 virtual currencies in the world , indicating that privacy protection is a very strong demand for the blockchain industry.

Smart contracts are computer protocols designed to disseminate, verify or execute contracts in an information-based manner . The invention of smart contracts makes the implementation of blockchain technology more feasible. However, the frustrating situation is that none of the blockchain systems currently in operation around the world support encryption protection for smart contracts . The use scenarios of existing privacy protection mechanisms have been greatly reduced due to this technical limitation. If anonymous blockchain systems that do not support smart contracts, such as Cash and Monero, are privacy protection solutions 1.0 , in order to allow the solution to be implemented in more industries and application scenarios , privacy protection solutions 2.0 that support smart contracts are highly anticipated.

It is undeniable that the anonymous blockchain system that supports smart contracts has a very high technical threshold . Only a handful of teams in the world are working hard for it . Now HCT has officially released its products to the world . HCT's R&D team (referred to as the "HCT team") is also the only team in the world that can propose a complete solution to this problem and has completed major engineering research and development work. Not only that , the HCT team did not regard the successful development of a privacy-protected blockchain system that supports smart contracts as the end point of the privacy protection solution for decentralized applications . In order to make the widespread implementation of privacy-protected decentralized applications feasible , the HCT team not only considered protecting the privacy of DApp users' accounts, the privacy of related tokens (Tokens) and the private data transmission process , but also fully considered the privacy protection strategy that was previously restricted by the various transport layer protocols during the data transmission process of the blockchain system , and even included data privacy protection in the scenario of the combination of decentralized applications and Internet applications.

CONTENTS

01
Industry status analysis



In recent years, technology has continuously reshaped our economy and life, as well as the world. Brand-new financial network technologies have emerged from the bottom, and blockchain has become a focus of world attention. The birth of blockchain is quite legendary, and the series of products it has triggered: digital currency, smart contracts, distributed governance, etc. have inspired changes in various industries in the global field.

1.1 Current status of the financial industry

In recent years, with the continuous deepening of financial reform and opening up, the market environment facing the financial industry has improved greatly. Especially since several financial crises, governments at all levels have placed financial security and stable development in a very important position, adopted a number of management measures, strengthened their own construction, and prevented financial risks, and have made great progress.

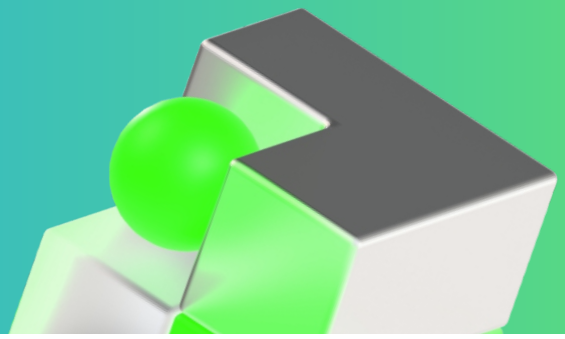
1.2 Digital transformation

Following the three industrial revolutions of mechanization, electrification, and digitization, mankind has ushered in the fourth industrial revolution, which is also called the digital economy. The digital economy refers to the new generation of information technology, such as the Internet, cloud computing, big data, artificial intelligence, blockchain, and 5G, as the engine. The new round of financial industry revolution brought about by the digital economy will disintegrate and reconstruct the global financial industry value chain, and ultimately change the business model and value model of the traditional financial industry.

1.3 Wealth is being reorganized

In the context of the digital economy era, digital technology innovation and application innovation continue to emerge, the critical point of digitalization in the financial derivatives industry is constantly being disintegrated, 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 traditional economic and social fields. More and more world economic activities are taking place in the digital space. The digital economy can provide a continuous source of power for corporate development and effectively promote the transformation and upgrading of traditional industries. The digital economy is changing the way the financial and financial derivatives industries operate, with banks as the internal infiltration and influence, bringing subversive changes to traditional financial models and formats, and is gradually changing the value chain shaped based on traditional models. The digital transformation of the traditional financial industry by digital technology not only strengthens the cross-industry collaboration between banks and the service industry, but also blurs the boundaries between the traditional financial industry, thereby deeply integrating the added value of the financial industry, manufacturing industry and more service industries under the digital economy.

01
Industry status analysis

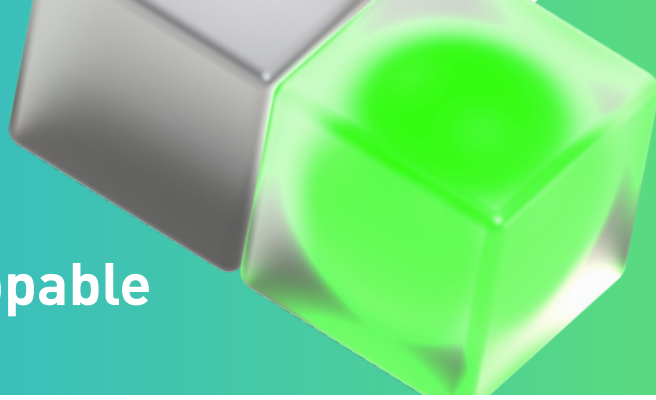


1.4 Digital Economy Era

The future is a digital era. Without the support of blockchain technology, the goal of digital economy will not be achieved. Blockchain allows all tangible assets to be processed digitally. Blockchain can establish a multi-party trusted collaboration model at low cost in an untrustworthy competitive environment, build a new transaction order and value system, and provide many solutions for the digital economy.

02

The digital economy is unstoppable



Blockchain is one of the most revolutionary emerging technologies in the current information technology field. Through the joint accounting of multiple nodes in the network, data (blocks) are connected in series (chain) in chronological order to form a transaction record that is traceable in chronological order and cannot be tampered with. The essence of blockchain is a value network. It realizes the circulation of value without any third party through distributed ledgers, consensus mechanisms, cryptography, peer-to-peer networks, smart contracts and other mechanisms.

Nowadays, the craze for blockchain technology development and application has swept all walks of life and has become one of the hottest and most watched information technologies. Compared with information technologies such as big data, cloud computing, and artificial intelligence, the characteristics of blockchain such as "decentralization", "immutability", and "openness and transparency" seem to be more likely to become a solution to people's vision of future technology.

The significant advantages of blockchain applications are to optimize business processes, reduce operating costs, and improve collaborative efficiency. These advantages have gradually emerged in many fields. The significance of blockchain technology is not only reflected in the technical level, but also in its transformation of social organizational forms and collaborative methods. Grasping blockchain technology and industry can bring major development opportunities to the social economy.

blockchain has empowered all industries around the world and provided a new data sharing system .

The digital economy will reshape the world, and humanity is entering 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, and makes electronic credential services more reliable, efficient, and secure, solving the following four problems:

1) It can effectively identify the authenticity of electronic credentials without worrying about 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 enterprises and users with a safe and reliable acquisition channel
3) Solve the trust bottleneck faced by the data storage industry and help business development;
4) By recording electronic credential summaries, circulation records, etc., electronic credentials can be traced to meet the needs of business supervision and review.

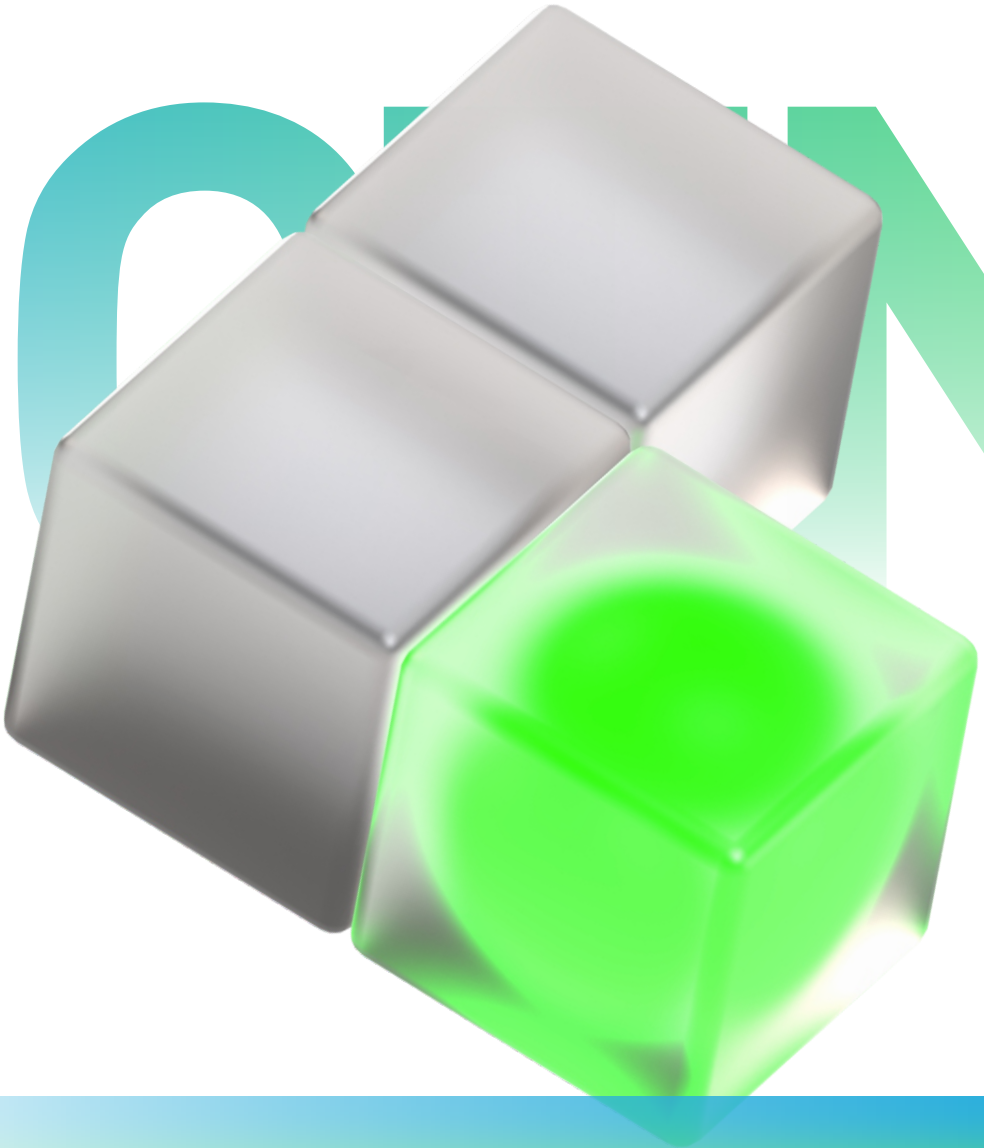
02

The digital economy is unstoppable

The future is a digital age, but without the support of blockchain technology, the goal of digital economy will not be achieved. Blockchain allows all tangible assets to be processed digitally. Blockchain can establish a multi-party trusted collaboration model at low cost in an untrustworthy competitive environment, build a new transaction order and value system, and provide many solutions for the digital economy.

HCT Alliance Chain : A new data sharing system in an anonymous world

The digital economy will reshape the world, and data privacy protection has become a top priority. Humanity is entering a new era. Only by building a secure and reliable data sharing system based on blockchain encryption technology can we meet the new era and challenges together . The HCT alliance chain will bring new ideas to the digital economy era.



03

Introduction to HCT

HCT is the world's first blockchain system that truly implements privacy protection with Turing-complete smart contracts. Compared with existing blockchain privacy protection technologies, HCT can not only achieve privacy protection for account information and transaction information, but also privacy protection for Turing-complete smart contract input and output. In addition, developers can also issue anonymous digital assets (Tokens) based on smart contracts on the HCT -Chain, and the communication information with smart contracts will also be protected by privacy and security.

HCT has redesigned the blockchain structure and various underlying protocols, making privacy-protected Turing-complete smart contracts a reality. Not only does it provide privacy protection measures for a wider range of application scenarios, but it also uses advanced NIZK cryptography algorithms to further increase the difficulty of attacking user privacy data. In addition, it improves the practicality of the current NIZK encryption algorithm, greatly reduces the memory resources required, and improves computing efficiency. In addition, compared with the mainstream anonymous blockchain systems on the market, HCT's support for Turing-complete smart contracts and privacy protection measures for its related decentralized applications have greatly generalized its usage scenarios.

By building a shared network of machine trust, we can solve problems such as data access, encrypted transmission, sharing, trusted transactions, and storage. We can achieve the safe chain-up of data and assets in various industries around the world, promote more industry individuals to join the alliance, conduct data integration, maximize data value, and jointly create a digital economy alliance with borderless data circulation, open value sharing, and industrial collaborative innovation.

1. HCT Alliance Chain Purpose:

Fairness, justice, openness, co-creation, sharing and win-win

2. The original intention of HCT alliance chain :

Everything is digitized. Through blockchain distributed data storage, we unite individuals, enterprises, and institutions around the world to achieve data and asset storage on the chain and create a massive database.

Data assetization. Through encrypted storage and peer-to-peer transactions, data rights are privatized and public use is made available, and digital assets can be circulated without barriers in the form of tokens.

Asset sharing. Build a secure and reliable digital economic alliance, optimize resource allocation within the alliance, reduce resource integration costs, improve efficiency, stimulate social productivity, and jointly build a DT value ecosystem.

03

Introduction to HCT

3. HCT Alliance Chain Advantages:

TPS is modularized, with a minimum of 3,000. The TPS function is made into a module, and different modules are built for different applications. The lowest TPS in traceability and evidence storage is 3,000 , and it can reach 62,000 in the logistics tracking scenario .

tens of millions of traffic , 20 countries and regions including Southeast Asia, China, South Korea, and Australia were launched simultaneously to create a global digital economy alliance.

4. Technical features of HCT alliance chain

Low cost and high efficiency

The public, secure, and low-cost HCT blockchain private cloud service has high availability, security, and hyper-converged platform deployment capabilities.

Highly compatible

HCT standardizes and modularizes the underlying complex technical system and heterogeneous systems, is compatible with various consensus algorithms, encryption algorithms and interactive protocols, and can achieve cross-platform, cross-chain and cross-application data interaction and sharing.

Open Intelligence

HCT is committed to building an open platform. Users do not need to pay attention to the underlying implementation details of the blockchain. By calling simple interfaces, they can create blockchains and various applications with a low threshold, thereby allowing the financial derivatives industry to focus more on the realization of business logic.

Safe and reliable

HCT 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 reliable, thereby ensuring the continued stability and security of the entire network.

On-chain anonymity

HCT will create a completely anonymous and open on-chain ecosystem, where user transactions and account information can be anonymous on the chain. The data in ordinary transactions are encrypted, and non-transaction parties cannot know the source, destination, asset type, amount and other details.

High practicality

HCT hides transaction data, it does not include all information in its scope, as this is uneconomical and inefficient. HCT will take into account users' existing usage habits and pain points and conduct phased research and development.

03

Introduction to HCT

5. HCT Alliance Chain Goals

the HCT alliance chain is to build a digital economic alliance with borderless data circulation, open value sharing, and industry collaborative innovation. Using cutting-edge technologies such as blockchain, big data, the Internet of Things, and AI, we can achieve the safe chaining of data and assets in various industries around the world, promote the integration of industrial data, connect physical value through massive data, create a global value Internet, and achieve the integration of the "five flows" of business flow, capital flow, information flow, logistics, and user flow, so that all entities within the alliance can create greater value and jointly build an open, shared, collaboratively innovative, and continuously cyclical digital economic alliance ecosystem.

Share data and create profits in the ecosystem!

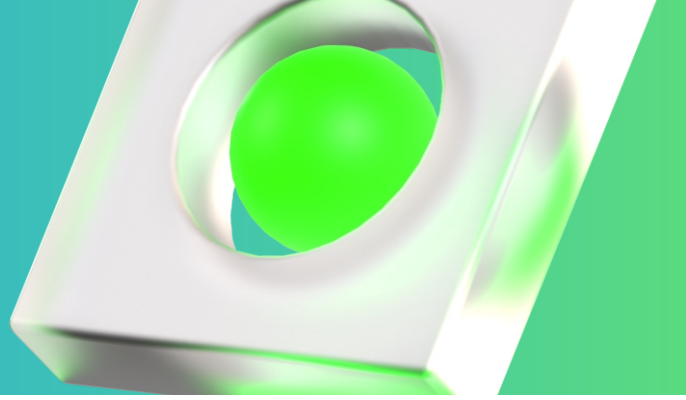
The HCT Alliance Chain not only provides a secure and reliable data sharing technology platform, but also unites multiple industry organizations to jointly build a data highland.

Create a digital economic alliance with borderless circulation, integrated sharing, and collaborative innovation, and play an important role in digital traceability, digital upgrades, digital finance, etc. It can be said that the HCT alliance chain will open an era of data sharing in which rights and interests are privatized, use is public, and digital can play an infinite value in the form of distributed nodes !

In the future, the Internet environment will change from relying on authority and system to gradually relying on technology to achieve trust, and the application of trusted electronic certificates based on blockchain will truly guarantee the legitimate rights and interests of all parties involved in the business, and help to completely realize paperless certificates. HCT takes financial industry data as the starting point, and attracts more institutional individuals and industries to join the alliance with the advantages of openness and sharing, creating the core component of the next generation of value Internet architecture, becoming an important entrance connecting the virtual and real worlds, and comprehensively building the key infrastructure for the digital transformation of the economy and society.

04

Ecology and Application



HCT alliance chain is suitable for scenarios where multiple parties participate and need to establish trust. Through the trusted data of blockchain, multiple parties can improve the transparency and sharing of information, thereby simplifying the business model, reducing the trust cost under the traditional model, and improving efficiency. The application scenarios of blockchain are very broad. Based on the characteristics of blockchain decentralization and shared trusted ledgers, from the perspective of building an industrial ecology, we can jump out of the way of thinking that only looks at problems from our own perspective and combine our own business scenarios to discover more potential business opportunities.

HCT focuses on blockchain + industrial development, ecological construction, and multi-chain integration. It applies Datong blockchain technology in various fields and continuously connects more digital economy participants, including individuals, entrepreneurial projects/enterprises, regulatory agencies, banks, venture capital institutions, etc. With the help of cutting-edge technologies such as AI, big data, cloud computing, 5G, and the Internet of Things, it digitally transforms industrial resources, accurately matches and widely circulates them, realizes the digital upgrade of the real industry, and creates a digital economy platform with borderless data circulation, open value sharing, and industrial collaborative innovation.

Ecological application:

finance

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

Payment

Small amount payment, B2B international remittance, tax declaration and statistics, personal authentication (KYC), anti-money laundering (AML)

Consumer Industry

Sharing economy, supply chain management, drug tracking, agricultural food certification, logistics management

Insurance

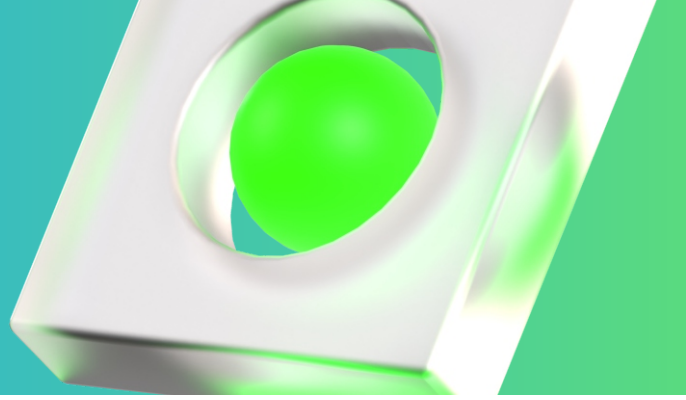
Claims filing, claims processing and management, fraud monitoring, telematics and ratings, digital authentication

media

Digital copyright certification, art certification, advertising, real statistics of ad clicks, and sales of genuine assets

04

Ecology and Application



Underlying Assets

Diamonds, designer brands, car rental and sales, home mortgages, land ownership, physical asset digitization

Medical Aesthetics

Product traceability, account registration, file chain, distributed storage, comparison and confirmation of ownership, token transaction, comprehensive credit value

social contact

Social interaction is a key part of the crypto world. The success or failure of a project depends on the community and network system they create. The emergence of HCT allows users to gain an in-depth understanding of their investment results and the status of their implementation, and through HCT , it breaks down the trust barriers between users' transactions and communications.

Big Data Applications

Big data is the most strategically significant core capability of smart networks and smart terminals in the future. There are two main aspects of big data applications in the future: community ecological big data based on open ledgers and collaborative networks to provide relevant information services for exchanges and community users; and quantitative investment support and risk control focusing on individuals (smart terminals).

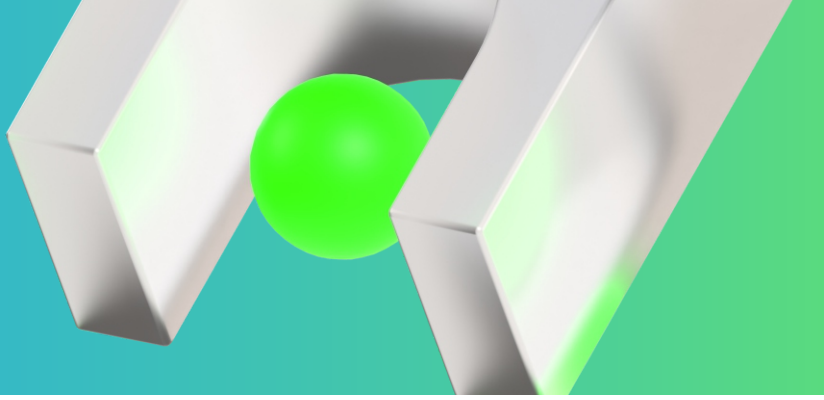
Social Management

Voting, vehicle registration, welfare distribution, copyright protection, education and certification

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

05

HCT technology



HCT supports deployment and expansion based on private cloud and public cloud; supports controllable authorized access to nodes , supports multiple encryption algorithms, and multiple consensus algorithms; supports high-performance autonomous smart contract engines , provides governance and operation and maintenance support for blockchain systems, and can monitor the operating status of the entire network in real time.

Security of HCT Alliance Chain

1. DPOS model

Security is our main concern in designing the HCT Alliance Chain. The HCT Alliance Chain uses the so-called "provably secure DPOS blockchain protocol". This algorithm has the following five characteristics, making it a very secure DPOS model.

First, the model focuses on durability and liveness, two formal properties of a healthy transaction ledger. Durability means that once some node in the system declares a transaction "stable", the rest of the nodes (if queried and responding truthfully) will also report it as stable. Stability is understood here as a predicate that is parameterized by some security parameter k and affects the certainty with which a property holds. (e.g., "more than k blocks deep.") Liveness guarantees that once a genuinely generated transaction is presented to the network nodes for a sufficient number of time, say u time steps, it will become stable. The combination of liveness and durability guarantees a healthy transaction ledger, in the sense that genuinely generated transactions are taken and made constant.

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

This prevents so-called grinding attacks, distinguishing our approach from other previous solutions. Furthermore, our approach is unique in that the system ignores rounds of stake modifications. Instead, the current set of stakeholders is recorded at regular intervals, called epochs; at each such interval, a secure multi-party computation occurs, using the blockchain itself as a broadcast channel. Specifically, in each epoch, a set of randomly selected stakeholders forms a committee and is then responsible for executing the coin-flipping protocol. The outcome of this protocol determines the next set of stakeholders to execute the protocol in the next epoch, as well as the results of all first elections in that epoch.

05
HCT technology

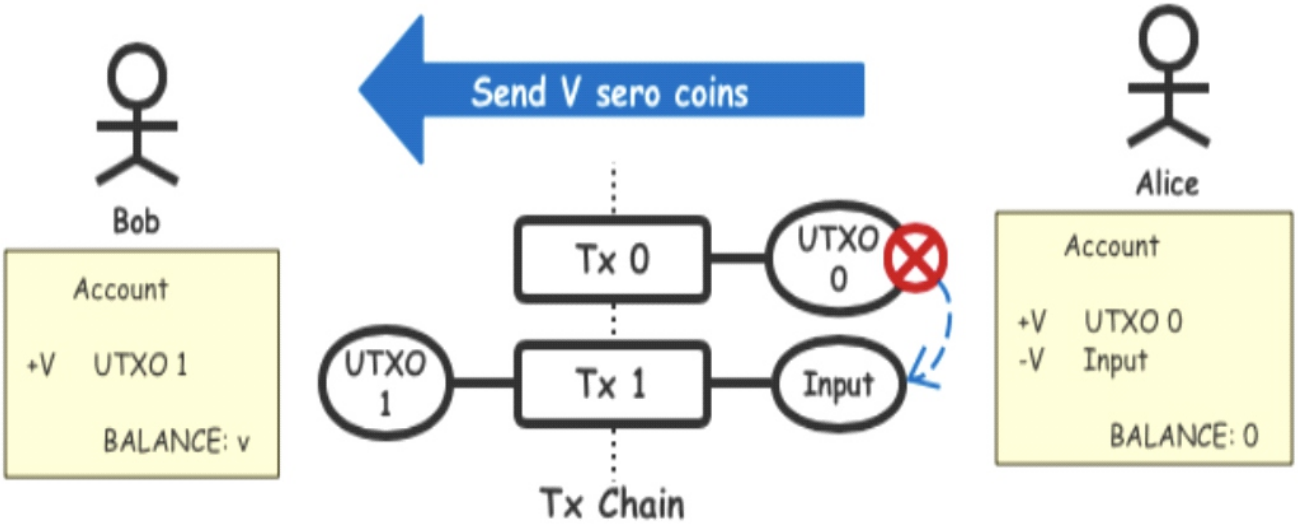
2、Technical Architecture

HCT Anonymous Token Issuance Principle

HCT is the world's first privacy blockchain system that supports Turing-complete smart contracts. Since it supports smart contracts, it is certainly not a simple smart contract + anonymous currency. HCT deeply integrates the advantages of both: the openness of smart contracts and the closedness of privacy systems. With the support of these two features, HCT's smart contracts have very exciting features and can do some magical things.

2.1 UTXO and ACCOUNT

Readers who understand the composition of blockchain should know that blockchain is a distributed ledger, each ledger contains multiple transactions Tx, and each transaction contains multiple records. The smallest unit of the ledger is a record, and each account records the inflow or outflow of assets in an account. However, from the actual implementation method, according to the different ways of recording asset outflows, the blockchain system has evolved into two different accounting implementations, which we call UTXO mode and ACCOUNT mode. These two modes correspond to the modes of Bitcoin and Ethereum respectively. HCT adopts a more complex hybrid mode.



05

HCT technology

As shown in the figure above, there are two types of records in the UTXO mode. For the transaction initiator, they are Input and Output. The Output is the unspent output (UTXO) in the eyes of the transaction recipient, until the transaction recipient initiates another transaction and specifies an Input to invalidate the UTXO. The records in the transaction always link various inputs and outputs. In this mode, ACCOUNT is not required as a status summary.

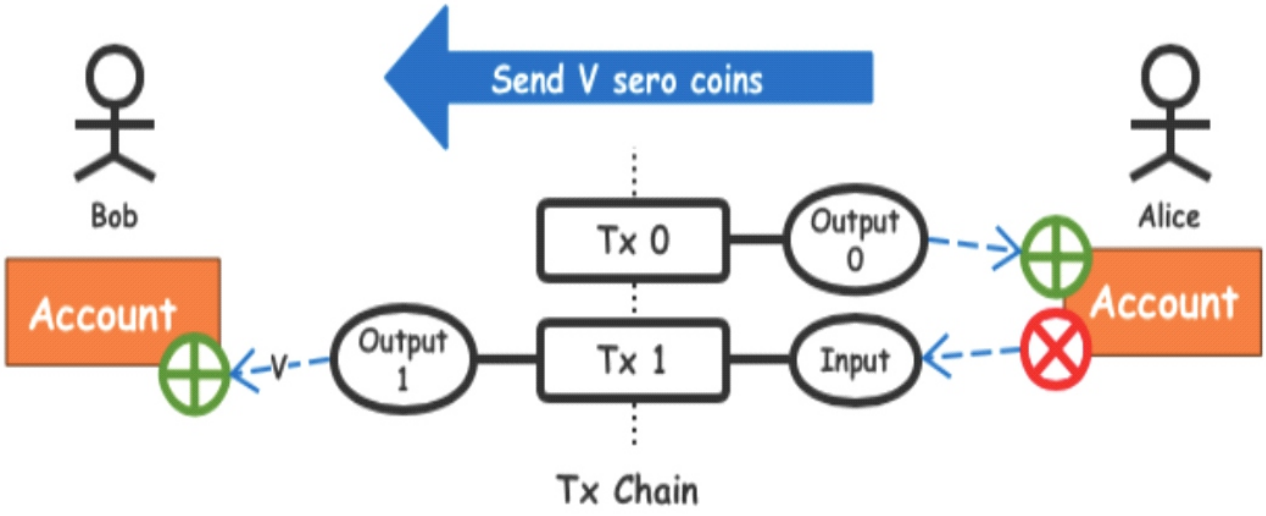
For example, in the figure above, Alice has previously received a transaction Tx 0, which has an output UTXO 0, and UTXO 0 contains V HCT coins. Her account can record [+V HCT , BALANCE=V]. Later, she transferred these V HCT coins to Bob, so she generated a transaction Tx 1, which has an input that invalidates UTXO 0, so Alice's ACCOUNT should record [-V HCT , BALANCE=0]. As for Bob, he added a UTXO 1 worth V HCT . If the previous BALANCE of his ACCOUNT was 0, his account can record [+V HCT , BALANCE=V].

This pattern has two advantages:

In the UTXO model, each transaction is independent of each other, which means that as long as the double-spending problem can be handled properly, transactions under one account can be processed in parallel, and the capabilities of multi-core CPUs can be fully utilized.

UTXO is essentially a form of record based on history, which is both a process and a result. Therefore, it has great advantages in some applications that require the generation of witness proofs. This is why blockchain systems with privacy features are basically UTXO models.

ACCOUNT-based transactions



05

HCT technology

Previously, the UTXO model mentioned that each account can generate a temporary ACCOUNT as a status summary. In the UTXO model, this account is temporary and not necessary. In the ACCOUNT model, each asset inflow and outflow record in the transaction references ACCOUNT instead of UTXO. Recording Input means increasing the assets of this ACCOUNT, while recording Output means reducing the assets of an account. In this model, the ACCOUNT entity is necessary. Without this ACCOUNT, all records are meaningless.

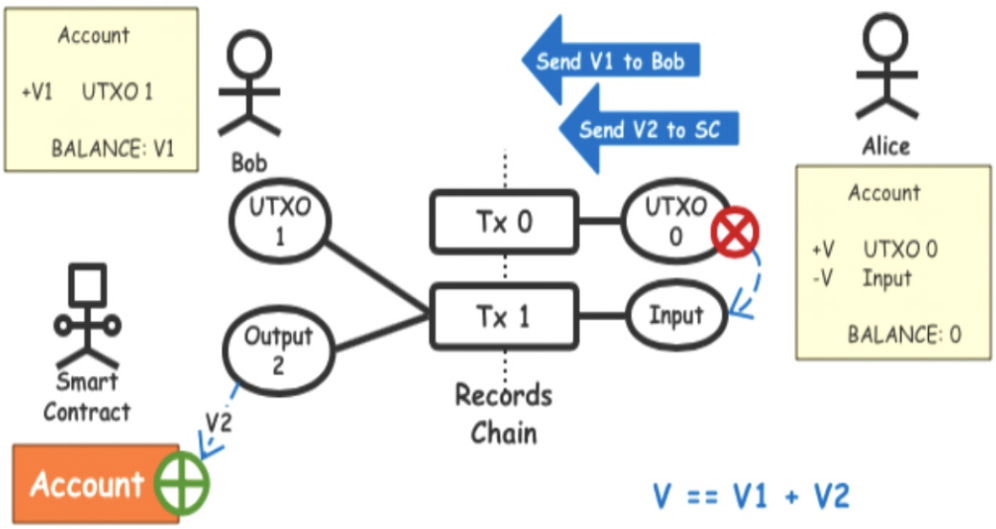
Same as above, for example, Alice has received a transaction Tx 0 before, which has an output Output 0 with an asset value of V HCT , and her ACCOUNT will increase by V HCT . At this time, she wants to transfer V HCT coins to Bob, so she initiates a transaction, the Input of the transaction points to her ACCOUNT, the value is V HCT coins, and Output 1 points to Bob's ACCOUNT, the value is also V HCT coins, then when this transaction is processed by the system, the assets in both parties' ACCOUNT will be directly added or subtracted. In this mode, Alice cannot distinguish whether the Input is the HCT coins input by Output 0 or the HCT coins that have been stored in the ACCOUNT before .

The ACCOUNT mode also has two advantages

The ACCOUNT mode directly increases or decreases the assets in a separate account, and only one record is needed to increase or decrease any number of assets in an account. Therefore, the size of the generated record is much smaller than the record generated by UTXO under the same circumstances.

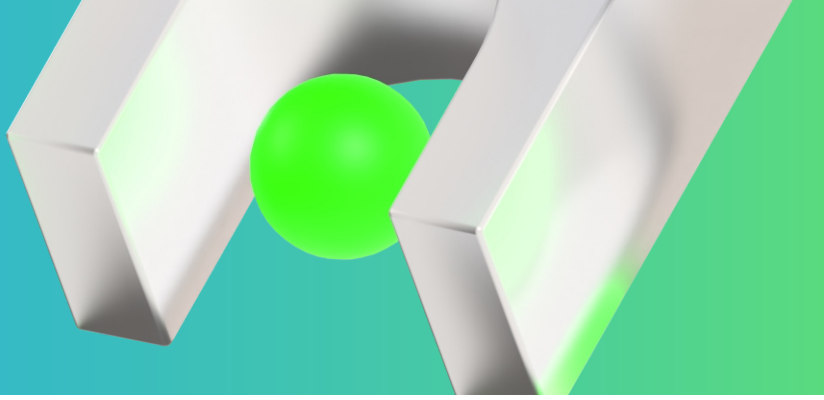
The ACCOUNT model is essentially state-based. Input and Output are processes, and ACCOUNT is the result. Therefore, it is naturally easy to introduce Turing machines. This is why blockchain systems that support Turing-complete smart contracts mostly adopt the ACCOUNT model.

Hybrid Model of HCT



05

HCT technology



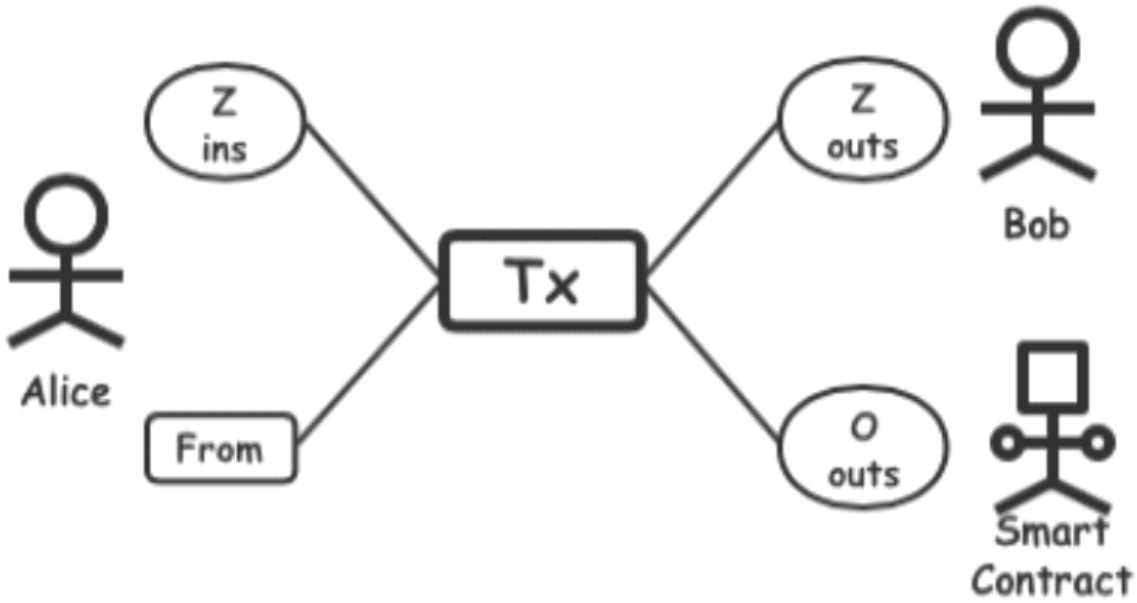
HCT uses a mixture of UTXO and ACCOUNT modes, using the UTXO mode where privacy protection is needed and the ACCOUNT mode where smart contracts need to be run. HCT seamlessly integrates these two modes through transactions, consensus, and the Pedersen Commitment algorithm, enabling smart contracts to perform amazing functions.

2.2 Anonymous transaction structure

In the BetaNet network, ordinary transactions of HCT are mandatory anonymous. Because if any non-anonymous transactions are allowed, the privacy and security of users who want to use the anonymous function will not be guaranteed in related transactions. In addition, if you want to publicize your assets and other information, it is recommended to use smart contracts to disclose some information to a limited extent.

At the time of MainNet release, HCT achieved a balance between privacy and generation speed by selecting a privacy level.

Transaction Tx

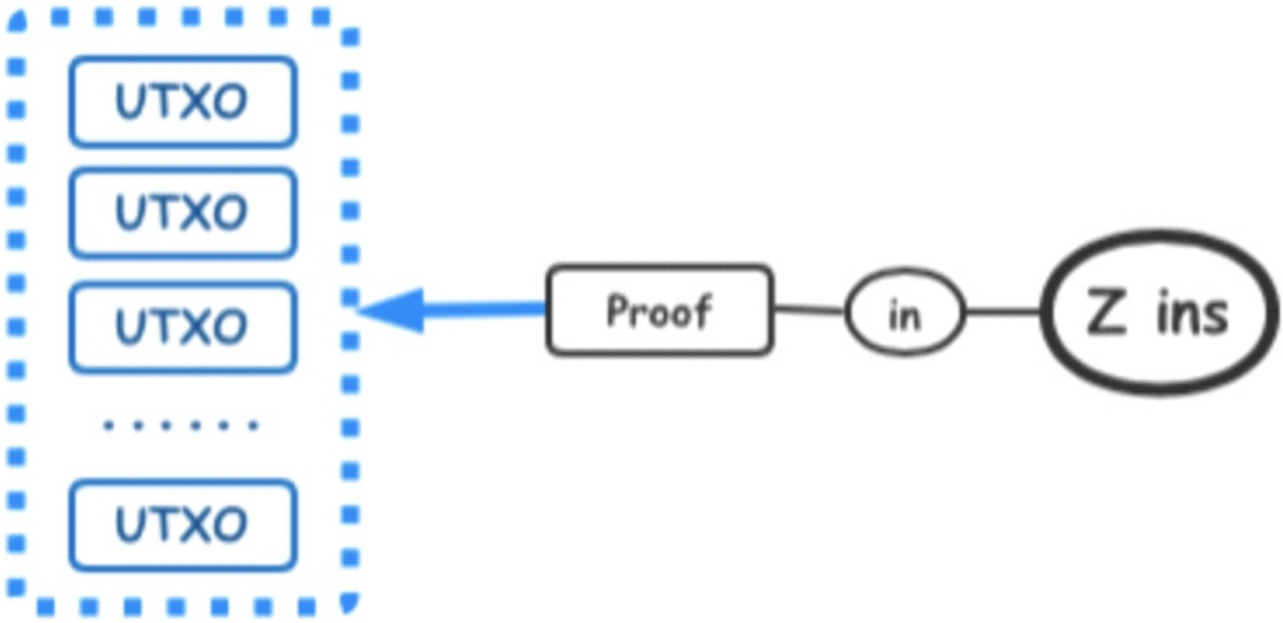


HCT 's anonymous transaction Tx has an anonymous input set Z ins, an anonymous output set Z outs, a normal output set O outs, and a temporary address called From. Z ins is completely anonymous, so that third-party observers cannot know the source and content. Z outs is a completely anonymous UTXO, and only the recipient can view and use its content. The content carried by O outs is not hidden, and it points to two recipients: one is to point to the smart contract address, and the other is to point to a temporary address. From represents the sender of the transaction, which is also a temporary address. Therefore, the entire Tx cannot make people determine who the real user is, and the information such as the assets carried in it is also hidden to the greatest extent.

05

HCT technology

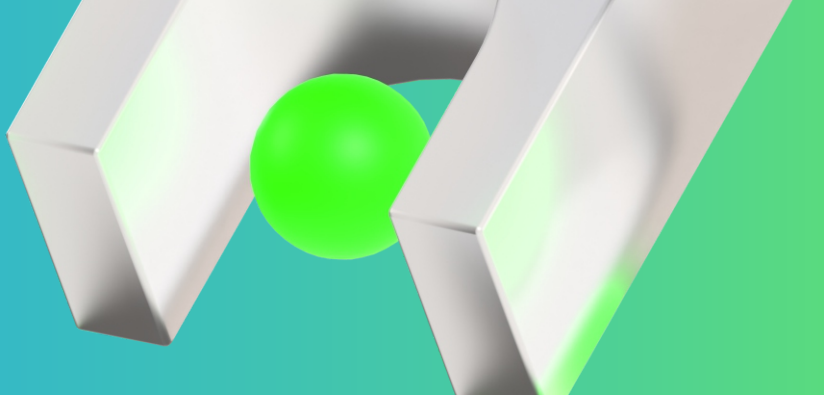
Input Z ins



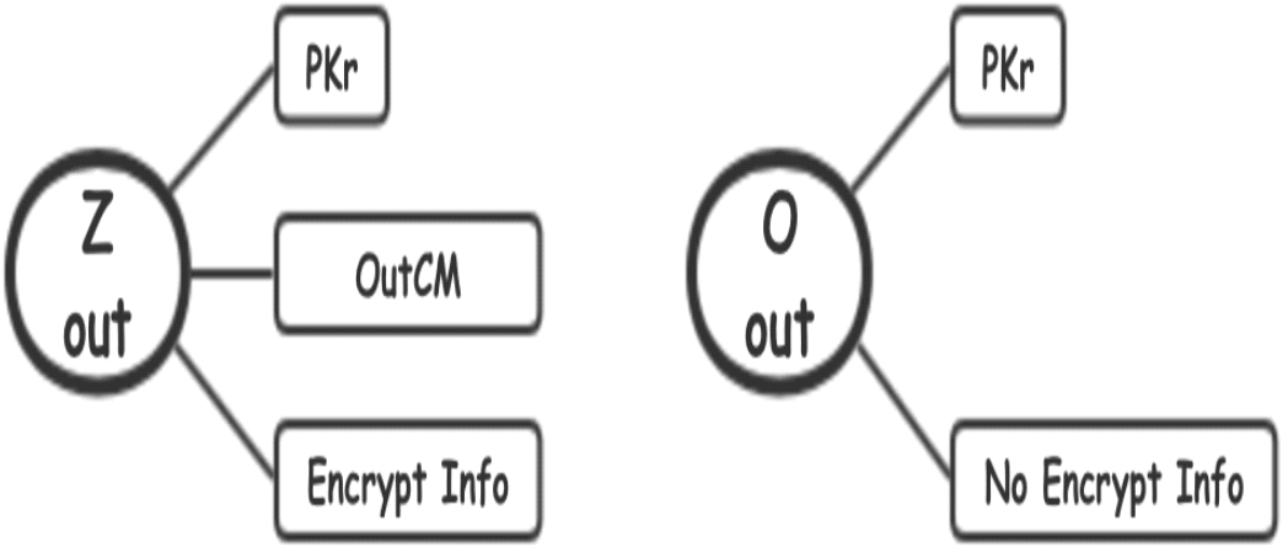
In the input set Z ins of the HCT transaction, each input is anonymous, including the ID of the source UTXO and the asset information carried. Each input is generated by a Proof using zero-knowledge proof ZKP, pointing to a specific UTXO hidden in a huge UTXO sequence. This sequence is part of the HCT history, and all the detailed information is hidden by the Proof. Without knowing the detailed information, the verifier can confirm whether the input is legal through the Proof. This method is very similar to the ring signature, but the size of our Proof itself is much smaller than that of the ring signature, and under the zero-knowledge proof, the range of the set used to hide the UTXO is much larger than that of the ring signature.

05

HCT technology



Two different outputs outs



The outputs contained in HCT transactions are divided into two forms, zero-knowledge output Z out and ordinary output O out.

Z out

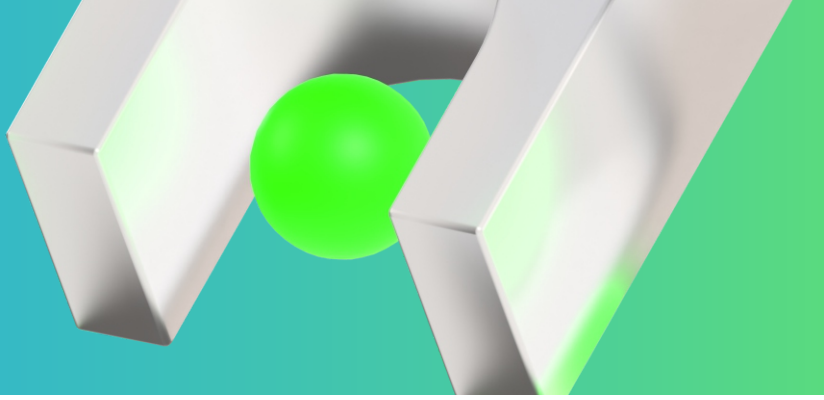
Z out points to the temporary address PKr, and only the recipient can decrypt the identity of the temporary address. Since each temporary address is different, no third party can identify the direction of Z out. Z out also carries the encrypted information of the asset Encrypt Info, which can only be decrypted by the recipient's private key. OutCM is an output commitment, and only the two parties of the transaction can reproduce the calculation process of OutCM. OutCM plays a vital role in proving that "Z out is referenced by ins".

O out

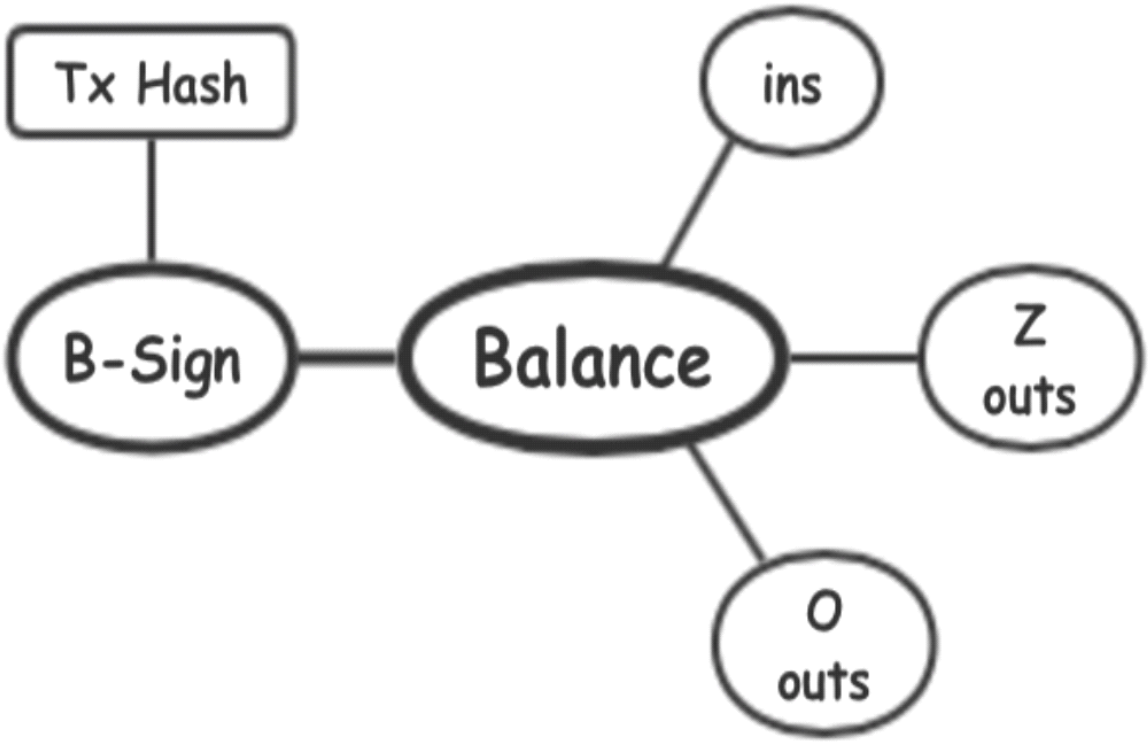
There are two forms of PKr pointed to by O out. One is initiated by a smart contract and points to the temporary address of a normal account. The other is initiated by a normal account and points to the address of a smart contract. Due to the randomness of the temporary address, the third party cannot know the identity of the recipient, and the asset information carried by O out is public.

05

HCT technology



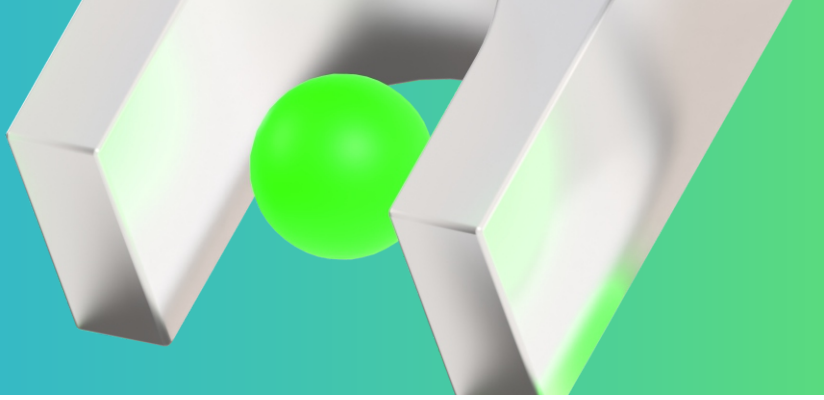
Balance of input and output



Tx packages ins, Z outs, and O outs together. How can we prevent malicious attackers from tampering with the data and ensure the security of assets? We introduce perdesen commitment. Its homomorphic encryption feature allows the verifier to confirm that the Balance must be balanced, that is, the input is equal to the output, without knowing the details of the information.

In addition, in order to prevent malicious attackers from tampering with O outs, we use the random characteristics of perdesen commitment to sign Tx Hash with the random part of Balance. In this way, each input and output can be calculated independently and then packaged together through B-Sign.

05
HCT technology



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. At this time, the temporary address From is the place where the output resources are received. From is determined when the transaction is generated and is only used once. Except for the sender of the transaction, no one else can locate the identity of the sender.

3. The principle of issuing anonymous tokens

Token Assets

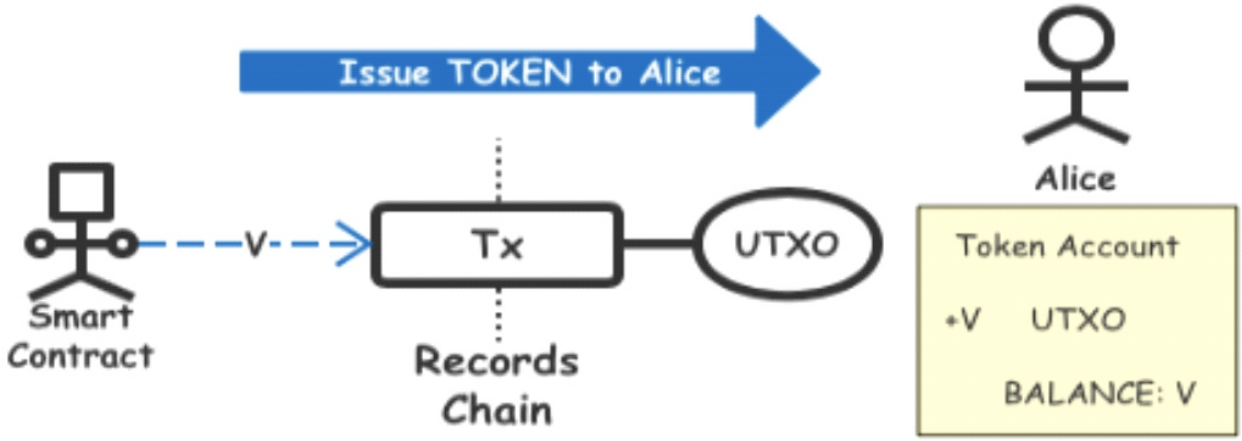
Token, also known as "homogeneous token", is a form of asset recognized within the HCT system. Tokens of the same type can be divided and mixed at will, specifically, they are called "coins". As the first currency of the HCT system, HCT coin is essentially a token. For token assets, except for the handling fee that can only be paid in HCT coins, they are treated the same within the HCT system, and their privacy and security are ensured by consensus.

Different from the Token concept in Ethereum, the Token in Ethereum is just a symbol recorded inside the smart contract, while ETH is the Token asset that actually runs inside Ethereum.

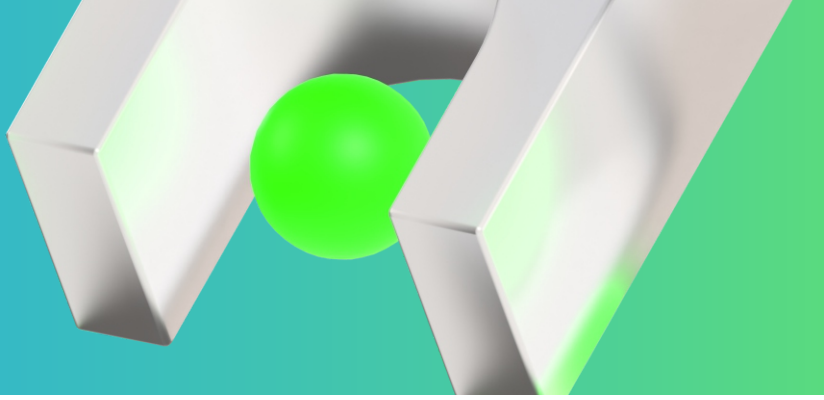
Coin Name

Each token has a currency name. After the HCT system is initialized, there is only one registered currency name HCT by default . When a smart contract issues an anonymous token, a globally unique string must be registered with the HCT system as the currency name of the token. The currency name can greatly improve the readability of your issued assets.

Anonymous Token Assets



05
HCT technology



HCT 's smart contract has a very powerful function, which is that it can issue anonymous tokens at will. Of course, the premise is that you need a coin name that has never been registered. Once the anonymous token is successfully issued, the smart contract can send the token to the temporary address PKr of a normal account in the form of a normal transaction. At this time, these sent tokens will be separated from the smart contract account in the form of UTXO, and like HCT coins, enter the user's personal account, thereby being protected by HCT 's privacy mechanism.

HCT coins is achieved by miners. The process is similar to the mechanism of issuing anonymous tokens by smart contracts. It is a built-in token issuance function of HCT .

3. Smart Contracts

Smart contracts are an extensibility function provided by the chain, but for security reasons, contracts will not be registered 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.

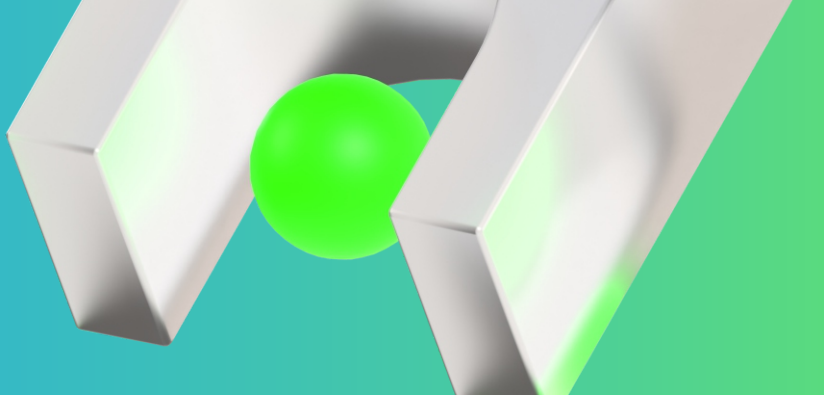
HCT uses the Docker container solution to provide an isolated and secure environment. Smart contracts run in Docker containers and can be isolated from the chain system, ensuring the security of contract execution. Users can use the G0 language to write smart contracts according to HCT technical documents. The Docker container solution can provide good system compatibility.
HCT will implement a custom lightweight virtual machine solution, in which smart contracts are executed to ensure isolation from on-chain data and avoid security risks. At the same time, it is more efficient than the Docker container solution, supports controlled I0, and has rich built-in microservice interfaces. Relying on the research institute's test platform, during the design and development process, HCT will introduce a smart contract security testing system, provide testing tools to detect security vulnerabilities in smart contracts, and help users discover and solve security issues in contracts.

After the entire ecosystem is perfected, there will be more demands, and more contract templates can be provided on the chain. These functions do not require changes to the underlying chain, but only require registration of new contracts.

(1) Virtual Machine

Smart contracts on the chain are developed using Turing-complete languages. The syntax can be adapted to support Lua, C#, etc. The results of virtual machine execution are recorded on the chain, and there is no need for all nodes to run virtual machines, reducing the load on the entire blockchain network.

05
HCT technology



(2) Contract

In systems like Ethereum, contracts can be registered and called at will. This is very beneficial for scalability and experimentation. However, in our storage system, we support any contract, but you need to have certain permissions to register it on the chain. This limits the types of contracts to a certain extent, but it is controlled for the stability of the entire network and the future development direction. At the same time, for the new contracts that need to be added in the future development, its scalability and flexibility are not affected at all.

4 Network Service

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

Each node uses P2P network technology to organize the network and supports dynamic joining and exiting of multiple nodes. The joining and exiting of nodes are controlled by permission management, and newly joined nodes need to be unanimously agreed by existing nodes to succeed.

5 Permission Management

Permission management is responsible for the management of the permissions of all nodes participating in HCT, and different permissions are granted to different nodes. In addition, the permission management module is also responsible for the access and read and write permissions of HCT, and only authorized users can access the data on the chain.

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

6 Security Mechanism

The design of HCT needs to fully consider the security requirements of the enterprise level, adopt encryption mechanisms that meet national and international standards, and have corresponding security measures in the implementation and deployment of servers. Block and chain structure, hash algorithm, asymmetric encryption and signature algorithm all support national secret algorithms.

HCT uses the PKI-based certificate system to perform node identity authentication. The CA server manages the issuance and destruction of certificates. Nodes use digital certificates for verification and encryption and decryption to prevent security issues caused by events such as repeated use of node certificates, repeated node logins, and node exits.

05
HCT technology

Currently supported cryptographic algorithms are:

HCT has implemented the Raft and PBFT consensus algorithms.
Raft is a distributed consistency algorithm based on Paxos . It has a simple structure and the same functions and performance as Paxos. In the scenario of consortium chain, HCT has modified and implemented Raft to adapt to the blockchain, which can ensure the consistency of the system when half of the nodes fail.
PBFT is a Byzantine fault-tolerant algorithm that can tolerate f Byzantine nodes when the number of nodes is not less than n=3f+1, but due to its low communication efficiency, it will be improved on this basis in the future.
In addition, the HCT research team is studying a scalable Byzantine fault-tolerant algorithm that can dynamically adjust the algorithm according to the network environment and security situation, and can improve tps without reducing fault tolerance through multi-node parallelism.

06
Release plan

6.1 Issuance Rules

The total number of HCT issued is 110 million , and the mother coin is 10 million . All HCTs were produced through POC hard disk mining in the early stage . It is a digital asset used by users to settle accounts and use on the HCT chain, and an important medium for communication between all parties. It is an indispensable part of the entire ecosystem.

6.2 Allocation Mechanism:

45% is used for dividends for coin holders; 50% is used for mining rewards; and 5% goes into the total dividend pool.

6.3 Coin holding income

Holding a certain amount of HCT can participate in the coin holding dividend, and the minimum holding amount can be adjusted dynamically; dividends are distributed proportionally according to the coin holding ranking; the total number is 1.1 billion, with 10 million in the first phase, a monthly increase of 10 % in the first year, 9 % in the next year , 7% in the next year, 6 % in the fourth year , and 5 % in the fifth year , until all 1.1 billion coins are issued.

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

M is the HCT holding ranking, and those holding the same amount of HCT are ranked uniformly. W is the total HCT issuance in the country, and A is the user's coin holding income on that day.

6.4 Mining Rewards and Promotional Benefits

In the early stage , HCT is produced through POC hard disk mining. Users can use it for circulation or wallet holding. 50% of the total daily output is used for computing power calculation. The calculation formula is as follows:

06

Release plan

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

HCT is issued daily , 50% of which is automatically allocated based on the proportion of the linked user group to the total computing power.

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

the total issuance of P_{max} HCT coins in the entire network , P is the number of HCT coins at the maximum intervention point , and P is the ordinary intervention (the team performance of ordinary access, if it is less than 10,000, is multiplied by 10 to calculate the promotion computing power, and the excess is not multiplied by 10).

07

Future plans

HCT Alliance Chain believes that under the new economic model of blockchain , by breaking through the barriers of countries, regions, languages, and circulation , HCT will help the data-centric digital light economy to achieve rapid development. To create an innovative economy . Building a communal digital economic alliance will open up data resources in various industries around the world , change the productivity relationship of all roles in the business model through the alliance ecology , and better promote the global development of the digital economic alliance with the support of the foundation .

Off-chain computing and homomorphic encryption smart contracts

In fact, homomorphic encryption of smart contracts has entered the substantive development stage . We have found a way to balance data security (a mechanism that can completely isolate sensitive data from the computer) and performance through on-chain and off-chain computing , and we plan to complete this work within 6 months.

Wallets and other ecological applications HCT 's decentralized wallet application is also currently under development and is scheduled to be officially released before March 2019. Since HCT supports developers to issue their own tokens , HCT 's wallet will support the management of HCT 's own tokens and all developers' tokens issued based on HCT .

The latest consensus mechanism

We will release a new consensus mechanism IMU -Random in a certain version within one year . It is a consensus mechanism that combines the latest PBFT theory and VRF algorithm design to achieve a balance between fairness and efficiency.

The Three Swordsmen of Privacy

HCT has two brothers , Alien Protocol and Castrol Protocol. The former provides a distributed DNS system that achieves stable network operation and information transmission through automatic addressing , while the latter implements encrypted privacy protection for node addresses . The trinity forms a complete decentralized application privacy protection solution.

Secure Multi-Party Computation

In many cases , data proof needs to be combined with existing centralized data sources , which can also be off-chain data sources . Currently , the strategy to solve the above problems is to assume that there is a trusted service provider or a trusted third party. However, in the current volatile and malicious environment , this is extremely risky . In the face of this problem , the general secure multi-party computing problem is solvable. HCT will also consider introducing secure multi-party computing (SMC) in the future to achieve extensive support for off-chain data under the premise of privacy protection .

07

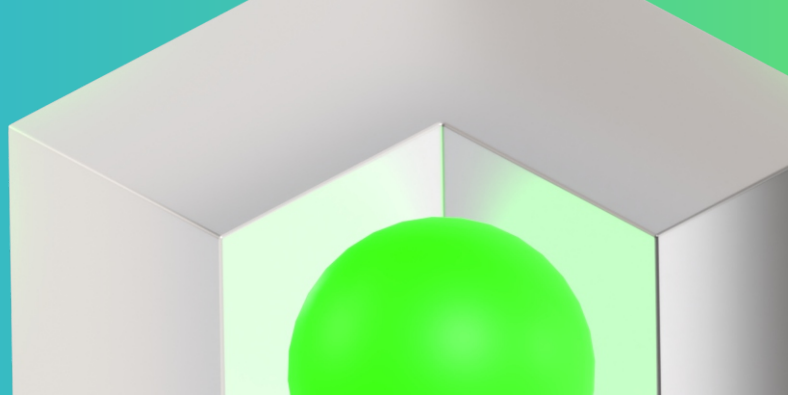
Future plans

Multi-chain system

The multi-chain system is the scalability solution for HCT . HCT will use a mechanism similar to Ethereum Plasma to perform horizontal performance expansion based on the multi-chain system. The multi-chain parallel computing mechanism similar to Plasma can enable HCT to reach an extremely high level of state updates per second (possibly billions). This will enable HCT to replace the current centralized cluster in terms of performance , giving HCT the prospect of handling various privacy-related decentralized applications around the world.

08

Development Plan



March 20 , 2020

Team building project preparation and launch

June 20 , 2020

White Paper Release Initial construction of the main chain

August 20 , 2020

Core technology research and development Main chain construction completed

September 20 , 2020

Wallet Development Mainnet Testing

20 November 20

The construction of the digital source platform is completed

January 20-21

Improve the digital economy alliance system

March 20-21

Tourism, real estate, and shopping mall circulation

August 20-21

Rich application scenarios Tracing application implementation

December 20-21

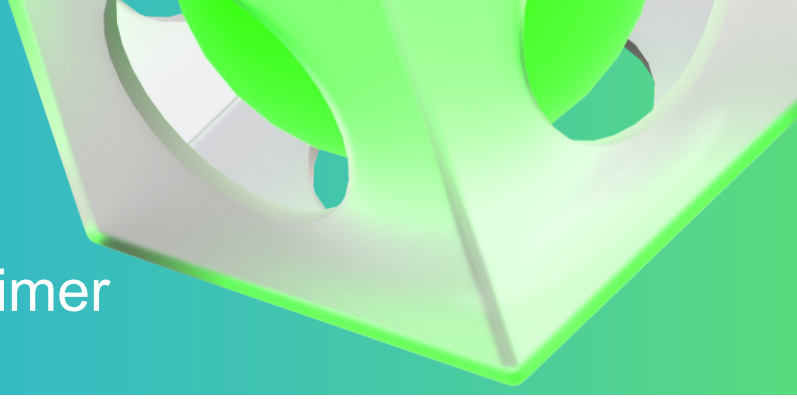
Global reach Ecosystem expansion

2022

Ecological iteration

09

Risk Warning and Disclaimer



1. Risk Warning

(1) Risks related to judicial supervision

Blockchain technology has become the main subject of regulation in major countries around the world. If the regulatory body intervenes or exerts influence, the application or token may be affected. For example, if the law restricts the use and sale of electronic tokens, the token may be restricted, hindered or even terminate the development of the application.

(2) Risk of lack of attention for the app

There is a possibility that platform applications are not used by a large number of individuals or organizations, which means that the public is not sufficiently interested in developing and growing these related distributed applications. Such a lack of interest may have a negative impact on tokens and applications.

(3) Risks of competitive expansion

There is a certain degree of competition among blockchain tokens. If a stronger competitor emerges in the industry, it will inevitably be affected.

(4) Risk that related applications or products fail to meet expected standards

The platform itself may undergo major changes during the development phase before the official release, or the market may undergo major changes before the release, causing the platform to fail to meet the expected requirements in terms of functionality or technology. Or due to incorrect analysis, the platform's application or token functionality may fail to meet expectations.

(5) Risk of Cracking

The technology currently used cannot be cracked, but if cryptography develops rapidly or computer computing speed improves rapidly, such as the development of quantum computers, it may bring the risk of cracking and lead to the loss of tokens.

(6) Other notes

Please fully understand the development plan of the operating platform and the relevant risks of the blockchain industry, otherwise it is not recommended to participate in this investment. If you invest, it means that you confirm that you have fully understood and recognized the terms and conditions in the details.

09

Risk Warning and Disclaimer

2. Disclaimer

This document is only used to convey information and does not constitute any opinions on the purchase and sale of this project. The above information or analysis does not constitute a reference for investment decision-making. This document does not constitute any investment advice, investment intention or abetment of investment.

This document does not constitute or be construed as providing any buying or selling behavior, nor is it a contract or commitment of any form.

Relevant potential users need to clearly understand the risks of this project. Once investors participate in the investment, they will be deemed to understand and accept the risks of the project and be willing to personally bear all corresponding results or consequences.

The operation team is not responsible for any direct or indirect losses caused by participating in this project .