Graycoin Cash (GCH) White Paper on Block chain

Gresham laboratory

1. catalogue

2. Introduction

The concept of block chain (Blockchain) originated in Bitcoin, dating back to late 2008, when a mysterious man named Nakamoto first proposed the concept of block chain. Since 2009, a variety of Bitcoin-like digital currencies have emerged, allowing the value of the block chain to be widely recognized, and Bitcoin has pioneered a decentralization of cryptographic currencies. Since then, some block-chain platforms have worked hard to support operationally decentralized applications, and more entrepreneurs and developers have been trying to promote the technology to support a wider range of applications on a single blockchain platform.

The feasibility and safety of block chain technology have been fully verified by many years of application. It has been found that the significance of block-chain is to build a more reliable Internet system to fundamentally solve the problem of fraud and rent-seeking in value exchange and transfer. More and more people believe that with the spread of blockchain technology, the digital economy will become more credible and economic society will become more just and transparent.

Block chain technology from 1.0 digital assets "speculation" era to the combination of digital assets and intelligent contract 2.0 era, 2018 is a block chain technology to the 3.0 era of the rapid development of block chain and related industries. Marks the beginning of human beings to build a true trust in the Internet.

The everywhere value exchange brought by block chain technology makes the society form a world of value interconnection with seamless connection of many kinds of devices. The block chain makes the economy not only the circulation of money, the Internet is not only the flow of information, but also further promote the effective allocation and circulation of information, money and value, so that the internal friction of human resources is minimized. Become a truly decentralized organization.

Further studies have found that the blockchain technology has a powerful ability to "reduce costs", can simplify the process, reduce some unnecessary transaction costs and institutional costs. Block chain 3.0 is a combination of real economy and real industry, and it is also the combination of industry chain entity and Internet, which promotes the application value of block chain.

The world is stepping into the "block chain economy era". In the next 3-5 years, blockchain technology will be prominent in many areas, such as the Internet of things, financial transactions, network security, public records, and so on, and will significantly improve the service flow in these areas. Even overturning traditional business models in these areas has huge potential for future development. Globally, the application of the blockchain industry has accelerated, permeating and spreading from digital money to non-financial areas, merging with innovation in various industries, further reconciling conflicts between technology and regulation, and continuously optimizing technical solutions and performance. As an emerging species, block chain is playing a great role in its existence.

Block chain technology is an opportunity for everyone in the world. Block chain will redefine the world.

3. On block chain

3.1. Brief introduction of Block chain

3.1.1. What is a block chain?

Block chain is a new application mode of distributed data storage, point-to-point transmission, consensus mechanism, encryption algorithm and so on. It is a series of data blocks associated with cryptography. Each block contains the information of a network transaction, which is used to verify the validity of its information (anti-counterfeiting) and to generate the next block.

In a narrow sense, it is a kind of chain data structure which combines the data blocks in order according to the time sequence, and can not be tampered with and unforgeable by cryptography.

Broadly speaking, block chain technology is the use of block chain data structure to verify and store data, use distributed node consensus algorithm to generate and update data, use cryptography to ensure the security of data transmission and access, and to use an intelligent contract composed of automated script code to program and operate a new type of data. Fabric infrastructure and computing.

The idea of block-chain technology has prompted us to rethink how to create transactions, store data, and exchange assets. It is the starting point of a great change.

3.1.2. Block chain development history

The concept of block chain is first proposed by <Bitcoin: A Peer-to-Peer Electronic Cash System> published in the bitcoin forum by Satoshi Nakamoto at the end of 2008. In this paper, block chain technology is the basic technology to construct the data structure of bitcoin and the encrypted transmission of transaction information. The technology realizes the mining and exchange of bitcoin. First, the model of processing information with the aid of third parties has an inherent weakness between point and point lack of trust. Households will ask customers for completely unnecessary information, but they will still be unable to avoid certain acts of fraud. Second, the existence of intermediary organizations will increase transaction costs and limit the minimum scale of transactions that are actually feasible. Third, Digital signature itself can solve the problem of electronic currency identity, and if third party support is needed to prevent double consumption, the system will lose value. Based on the above three existing problems, Nakamoto created Bitcoin based on block chain technology.

Compared with the development of the Internet, the block-chain technology we see today has actually gone through a long historical evolution. It dates back to the Byzantine Generals problem raised by Leslie Lamport in 1982. The Byzantine General problem is a virtual model to explain the consistency problem. Byzantium was the capital of ancient eastern Rome, and, because of its vast territory, the general of the guard had to deliver messages by messenger to reach an agreed decision. But because there may be traitors among generals, these defected generals may Will send the wrong message, interfere with everyone's decision.

The Byzantine question was raised to solve the problem of how loyal generals could reach an agreement in such a situation. This problem has evolved into the field of computers, where different computers communicate to reach agreement on the Internet. In the actual process, some computers may be wrong and some computers may be attacked by hackers. How to ensure that computers on the network agree on something is the problem to be solved by this theoretical model.

Byzantine problem is the basis of consensus mechanism in block chain technology. It is precisely because of this theoretical basis that the block chain technology has a scientific basis for development.

Before Bitcoin, the block chain had evolved for generations, including e-Casho HashCasho B-money and other related digital currencies. This period belongs to the development stage of digital money.

E-Cash was proposed in 1983 as a digital payment system, but it failed because of centralization.

In 1997, HashCash was a digital currency using Poof of Work (PoW), and was widely used in digital currency.

B-money proposed in 1998 is the first decentralized digital monetary system, but unfortunately no concrete implementation has been proposed.

It was not until January 2009 that Bitcoin was introduced into the world, and a truly decentralized, open-account digital money system was introduced, which officially opened the development of blockchain technology.

After the advent of bitcoin, the block-chain technology behind it began to attract attention.

However, the application of block chain technology is restricted by the reason that Bitcoin itself is based on script development. The increasing demand for application development based on block chain has spawned the exploration of intelligent contracts by many Niuren.

Vitalik Buterin's Ethernet workshop, EOS of Daniel Larimer are all the research and exploration of the block chain technology in intelligent contract, PressOne is even more so.

Block chains have evolved from encrypted money, digital money to smart contracts, and will move toward more sophisticated smart contracts.

With the development of block chain technology, the difficulty of application development based on block chain will be reduced, and the innovation in the field of block chain will be accelerated and the integration with the Internet will be accelerated.

Block chain technology can be used not only for digital money, but also for more extensive use. The application of monetary scope is called block chain 1, which mainly solves the centralization of money and payment means.

When Bitcoin was created, Nakamoto considered making it programmable to support a variety of transaction types.

Starting with this, blockchain technology extends beyond digital currency, and blockchain 2.0 can be used to register, recognize and transfer various types of assets and contracts, such as financial transactions, public records, private records, etc. Thus more macro to the entire market decentralization.

Block chain 3.0 goes further beyond the economy and can be used to distribute increasingly automated physical and human resources around the world, promoting large-scale collaboration in the fields of science, education, health, e-commerce, community, entertainment, and so on.

3.1.3. Evolution of Block chain

- Block chain 1.0-Digital currency

It is a digital currency application represented by bit currency , and its scene includes payment , circulation and other monetary functions .

- Block chain 2.0- Digital assets and Intelligent contracts

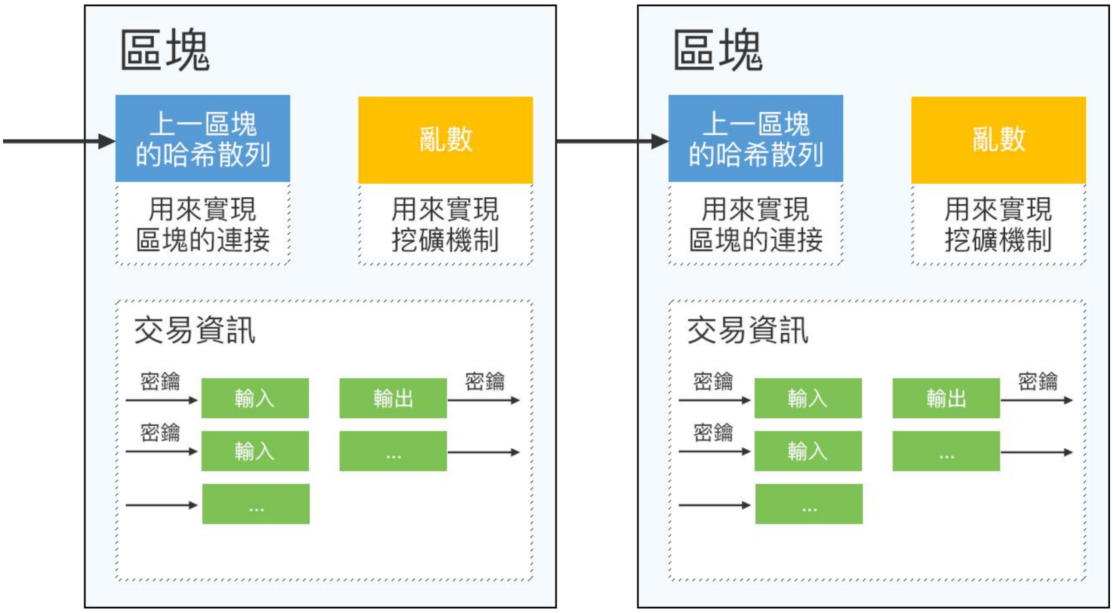
It is a combination of digital money and smart contracts that optimizes the broader scenarios and processes of finance.

- Block chain 3 - IFMChain, block chain links to mobile terminals formally.

Application beyond the financial field, block chain formally linked mobile terminals, to provide decentralized solutions for various industries.

3.1.4. Block chain core technology

1. Block chain link



As the name implies, a block chain is a chain of blocks. Each block is divided into two parts: the block head and the block body (including transaction data). The block header includes the hash PrevHashvalue (also known as hash) of the previous block used to implement the block link and the random number noncede used to calculate the difficulty of mining. The hash value of the former block is actually the hash value of the head of the previous block, and the rule of calculating random numbers determines which miner can obtain the right to record the block.

2. consensus mechanism

Block chain is born with bitcoin and is the basic technology architecture of bitcoin. Block chain can be understood as an internet-based decentralized accounting system. A decentralized digital money system such as Bitcoin requires consistency in the accounting of honest nodes without a central node, which requires a block chain to complete. Therefore, the core of blockchain technology is a consensus mechanism to reach a consensus on the legitimacy of transactions between individuals without central control and among individuals with no mutual trust basis.

At present, there are four kinds of consensus mechanisms in block chain, distributed consistency algorithm.

3. Unlock script

Script is an important technology for automatic verification and execution of contracts in block chain. Every output of every transaction is strictly not to an address, but to a script. A script is like a set of rules that constrain how the receiver can spend the assets locked on the output.

Verification of the legitimacy of transactions also relies on scripts. It currently relies on two types of scripts: lock script and unlock script. Locking script is a condition added to the output transaction, implemented by a script language, located in the output of the transaction. The unlock script corresponds to the lock script, and only if the requirements of the lock script are met, can the corresponding assets on the script be spent in the input of the transaction. Many flexible conditions can be expressed through scripting languages. The script is interpreted by a "virtual machine" similar to our programming world, which distributes every node in a block chain network.

4. rules of transactions

he transaction of block chain is the basic unit of block, and it is also the actual valid content of block chain record. A block-chain transaction can be a transfer or other transactions such as the deployment of a smart contract.

In the case of Bitcoin, a transaction is a payment transfer. Its trading rules are as follows:

1) the input and output of the transaction cannot be empty.

2) for each input to the transaction, the transaction is rejected if its corresponding UTXO output can be found in the current trading pool. Because the current pool is a transaction that is not recorded in the block chain, each input to the transaction should come from the confirmed UTXO. If found in the current trading pool, it is double-flower trading.

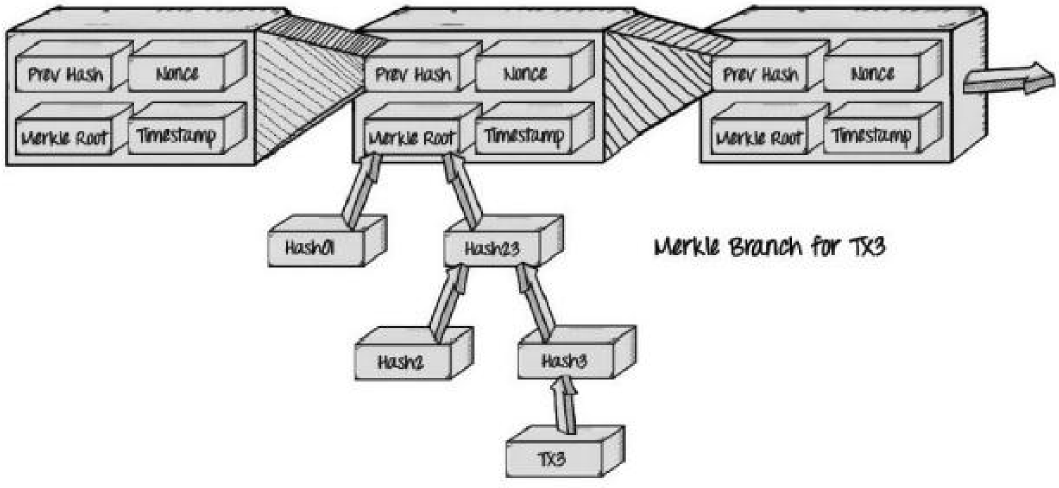
3) for each input in the transaction, the corresponding output must be UTXO.

4) each input unlocking scriptmust work with the corresponding output locking scriptto verify the transaction compliance.

5. Transaction priority

The priority of block chain transactions is determined by the block chain protocol rules. For Bitcoin, the priority that a transaction is contained in a block is determined by the time the transaction is broadcast to the network and the size of the transaction amount. As the time for trading to broadcast to the network grows, the chain age of the transaction increases, the priority of the transaction is increased, and eventually the transaction is included in the block. For Ethernet, the priority of the transaction is also related to the transaction cost that the publisher of the transaction is willing to pay. The higher the transaction cost the publisher is willing to pay, the higher the priority of the transaction being included in the block.

6. Merkle proof



The original application of the Merkle certification is Bitcoin system, which was described and created by Satoshi Nakamotoi Nakamotoi in 2009. The bitcoin block chain uses Merkle certificates to store transactions in each block. It also makes it easy to verify that the transaction is included in a particular block.

7. RLP

RLP(Recursive Length prefix (recursive length prefix encoding) is one of the main encoding methods of object serialization in Ethereum, which aims to encode sequences of arbitrary nested binary data.

3.1.5. Block chain classification

Public Block chain (PublicBlockChains)

The public block chain means that any individual or group in the world can send a transaction, and the transaction can be confirmed effectively by the block chain, and anyone can participate in its consensus process. The public block chain is the earliest block chain and the most widely used block chain. The virtual digital currency of each bitcoins series is based on the public block chain. There is only one block chain corresponding to this currency in the world.

Joint (industry) block chain (ConsortiumBlockChains)

Industry block chain: multiple pre-selected nodes are designated as bookkeepers within a group, and the generation of each block is decided by all pre-selected nodes (pre-selected nodes participate in the consensus process, other access nodes can participate in transactions, But don't ask about the bookkeeping process (essentially managed bookkeeping, just become distributed bookkeeping, how many nodes are preselected, How to determine the bookkeeper of each block becomes the main risk point of the block chain, and anyone else can use the block chain open API to make a qualified query.

Private Block chain

Private block chain: only use block chain general ledger technology to account, can be a company, can be an individual, exclusive access to the block chain write, This chain is no different from other distributed storage schemes. (Dec2015) the conservative giants (traditional finance) want to experiment with private block chains, while public chain applications such as bitcoin are industrialized, and private chain applications are still groping.

3.1.6. Block chain feature

decentration

Because of the distributed accounting and storage, there is no centralized hardware or management organization, and the rights and obligations of any node are equal. The data blocks in the system are maintained by the nodes with maintenance function in the whole system.

Thanks to the decentralization of the block chain, Bitcoin also has a decentralization feature.

open

The system is open, except the private information of the transaction parties is encrypted, the block chain data is open to all, anyone can query the block chain data and develop related applications through the public interface, so the whole system information is highly transparent.

Autonomy

Block chains use consensus-based specifications and protocols (such as a set of open and transparent algorithms) that allow all nodes throughout the system to freely and securely exchange data in a discredited environment. So that the trust in "people" changed to trust in the machine, any human intervention does not work.

Information cannot be tampered with

Once the information is validated and added to the block chain, it is permanently stored, and unless more than 51% of the nodes in the system can be controlled at the same time, changes to the database on a single node are invalid. Therefore, the block chain data stability and reliability is extremely high.

anonymity

Because the exchange between nodes follows a fixed algorithm, there is no need for trust in their data interaction (the procedural rules in the block chain will determine whether the activity is valid or not, so the counterparty does not have to let the other party generate trust by means of public identity. It is very helpful to the accumulation of credit.

3.2. Block chain prospect

3.2.1. Block chain application requirements

Nowadays, many people question how much real value the block chain has in addition to speculation and speculation. The technology is too slow to be applied on a large scale. The first generation technology often can not bring about the impact change, must wait until the second generation or the third generation technology. The adoption of technology often takes this process. The only difference of block chain is that its iterative process has received a lot of attention. In the long run, block chains can make many industries more automated, transparent and decentralized, and it is only a matter of time before the chain matures.

Many organizations and institutions are now working on block-chain applications, a good blockchain application, or decentralization, to be more universal, with the following requirements:

1) large user support capacity

As an excellent application, it can support at least one million level users. Whether it is centralization or decentralization, it must have strong multi-user support ability. If the decentralized application wants to be accepted by the mainstream users, it must have the ability to support millions of users, so it needs to be large enough to expand the capacity of the decentralized application.

For example, large apps such as Facebook Uber, as we know it, must have the technology to handle tens of millions of active users, or the app won't work properly, and how can it be called a good app. The same is true for block-chain applications, where future applications, whether for payment transactions or social applications, need to have the ability to support large numbers of users, and it is important to have a platform that can handle a large number of users. Currently, the number of users in block-chain applications is relatively small, so which application has a strong scalability is an important part of the future development.

Free application experience

The whole application platform or operating system should have the ability to support the development of free application software and provide a good user experience to the user. Even if there are many benefits of decentralized applications, users cannot be forced to pay for them.

Most of the time, application developers should provide free service to users flexibly, when users can use the platform without paying money, the number of applications developed on this platform is bound to grow. At the same time, the free block-chain platform will naturally get more user attention. When there are enough users, developers and related businesses can create more profit models.

3) simple and convenient system renewal ability

The whole block chain application platform should provide sufficient degree of freedom for participating developers. Update the decentralized application at the right time according to their ideas and needs. Or let individuals choose the time they want to update according to their own needs.

If bug needs to be addressed in an application, the developer should not affect the entire underlying operating system when patching. In addition, block-chain-based applications naturally need to be able to support software upgrades when performing functional iterations. When a block chain underlying platform encounters bug, it should have the ability to correct errors from bug.

4) low latency

The application of block chain or decentralization should not only have the ability to run smoothly, but also have low delay.

The longer the delay, the more the user experience will be affected, and the decline of the user experience will seriously affect and reduce the market competitiveness of the application.

5) powerful serial performance

A good block chain application should choose to focus more on serial or parallel capabilities based on specific application scenarios. For example, an exchange, such as an exchange, often needs to handle a large number of serial operations. In this scenario, a good block chain architecture needs to have strong string performance, accompanied by intelligent parallel processing capabilities.

6) Intelligent parallel performance

A block - chain application operating platform has the ability to synchronize operations based on its de - centralized applications so that a reasonable amount of computation can be allocated to save time . Also , large - scale applications are required to divide workloads between multiple CPUs and computers .

3.2.2. The future of the block chain

The blockchain technology originated from the virtual currency. Since 2009, the virtual currency has risen in the global scope, and the blockchain technology has come into people's view step by step. At present, governments, industry and academia all over the world pay close attention to the application and development of block chain.

Trend 1: block chain industry application accelerates from digital currency to non-financial sector penetration and diffusion

Block chain technology as a universal technology, from digital currency accelerated penetration into other areas, and a variety of industry innovation fusion. The future application of block chain will be driven by two camps. On the one hand, IT camp, from information sharing, to establish credit at low cost as the core, gradually covering digital assets and other fields. On the other hand, the encrypted money camp proceeds from the currency, gradually advances to the asset side management, the depository security domain, and diffuses to the credit information and the general information sharing class application.

Trend 2: enterprise Application is the main Battlefield of Block chain, Alliance chain / Private chain will become the mainstream Direction

At present, the actual application of the enterprises in the field of digital money is a virtual economy. We think that the future block chain application will take off the virtual reality, more traditional enterprises use the block chain technology to reduce the cost, improve the cooperation efficiency and stimulate the real economic growth, which is the main battlefield of the future block chain application.

Unlike the public chain, in enterprise applications, more attention is given to blockchain control, regulatory compliance, performance, security, and so on. Therefore, alliance chain and private chain, the strong management of block chain deployment mode, is more suitable for enterprises to use in the application landing, is the mainstream technology direction of enterprise applications.

Trend 3: application of diverse technology solutions, block chain performance will be continuously optimized

In the future, the application of block chain will develop from single to multiple. Bill, payment, insurance, supply chain and other applications, in real-time, high concurrency, delay and throughput and other dimensions will be highly differentiated. This will spawn a variety of technical solutions. Block chain technology is still far from being finalized, and will continue to evolve in the future, consensus algorithm, service segmentation, processing methods, organizational forms and other technical aspects of the space to improve efficiency.

Trend 4: closer integration of block chains with cloud computing BaaS is expected to become a public trust infrastructure

Cloud computing is the trend of the times. The combination of block chain and cloud is also an inevitable trend. There are two models for the combination of block chain and cloud, one is block chain in cloud, the other is block chain in cloud. The latter, Blockchain-as-a-ServiceBlockchain-as-a-Service, refers to the provision of block chains directly to users by cloud service providers. In the future, more and more cloud service enterprises will integrate block chain technology into the ecological environment of cloud computing. By providing BaaS function, the deployment cost of enterprise application block chain can be effectively reduced, and the initial threshold of innovation and entrepreneurship will be lowered.

Trend 5: block chain security issues are becoming increasingly prominent, security protection needs technical and management overall considerations

The block chain system is almost perfect in mathematical principle. It has the advantages of open and transparent, difficult to tamper, reliable encryption, DDoS attack prevention and so on. However, its security is still restricted by infrastructure, system design, operation management, privacy protection and technical update iteration. In order to ensure the safety of application, we need to consider the overall situation of technology and management, strengthen basic research and overall protection in the future.

Trend VI: increased demand for block chains across chains and the importance of connectivity

As block chain application deepens, payment settlement, logistics traceability, medical records, authentication and other areas of enterprise or industry, will establish their own block chain systems. In the future, it is an inevitable trend to cooperate and interoperate across chains among these block-chain systems. Cross-chain technology is the key to the realization of value Internet in block chain, and interworking of block chain will become more and more important.

Trend 7: block chain competition is becoming increasingly fierce, patent competition has become an important area of competition

With the increase of the participants, the competition of block chain will be more and more intense, the competition is omnidirectional, including technology, mode, patent and so on. In the future, companies will strengthen the layout of blockchain patents. Since 2014, the number of blockchain patent applications has exploded. Blockchain patents are mainly distributed in the United States in North America, the United Kingdom in Europe, China and South Korea in Asia and will maintain this pattern in the future. The patent gap between China and the United States is narrowing, and China's filing volume in 2016 has surpassed that of the United States. It can be predicted that the future of the block chain patent competition will become increasingly fierce.

Trend 8: block chain investment continues to be hot, and the accumulated risk in the crowdfunding model is worth paying attention to

Block chain has become a hot spot in the pursuit of capital market. Future investments will continue the rising trend of 2018-2020. Unlike other tech financing models, a blockchain model has emerged, known as Initial Coin offering, a crowdfunding approach for startups to raise money on behalf of money. The share of global escrow crowdfunding has accounted for 48% of the total volume of venture capital related to the block chain. In 2017, the share of global token crowdfunding has accounted for 49.5% of the total volume of venture capital related to the block chain. Important channels. It is expected that more than 300 ICO cases will appear in 2018-2020 years. With the rise of the number of currencies, its lack of audit, huge fluctuation in value, and the risk of being on the edge of supervision will increase. It is worth paying attention to.

Trend 9 : There is a conflict between block chain technology and supervision , but the contradiction is expected to be further reconciled

The decentralization, disintermediation and anonymity of block chain are incompatible with the traditional enterprise management and government supervision system. But there should also be an opportunity for regulation by the blockchain. In the future, companies will actively cater to regulatory needs, actively build in regulatory requirements in technical solutions and mode design, not only to achieve compliance operation, but also to significantly reduce the cost of regulatory compliance. We also believe that in the future, regulators around the world will embrace blockchain, a new regulatory technology to improve the effectiveness of government regulation.

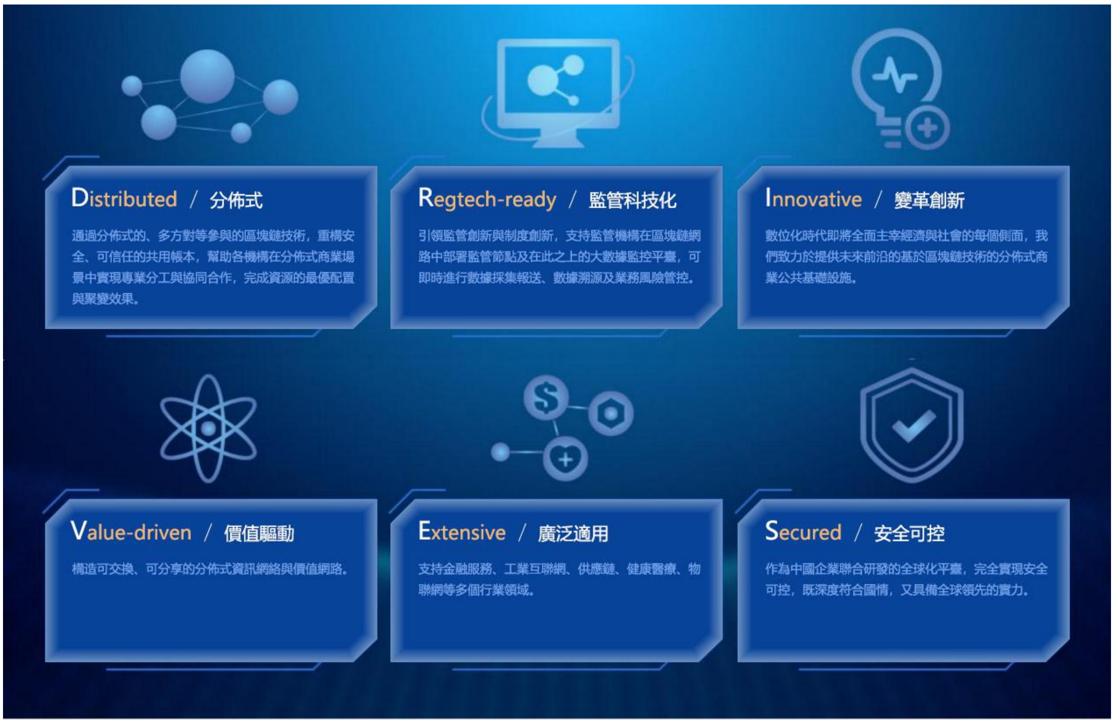
Trend # 10: trustworthiness is the core requirement of block chains, and the importance of standard specifications is becoming increasingly prominent

In the future value transfer network based on block chain, we will completely use algorithms and software to build trust base, but this is far from enough. In the future, the standard of block chain will be based on the user's point of view, business oriented, from the dimensions of intelligent contract, consensus mechanism, private key security, authority management, etc., to standardize the technology and governance of the block chain, and to enhance the credibility of the block chain. Gives weight to trust in the block chain.

4. About Gresham.

4.1. About Gresham's lab.

Gresham Labs, the burgeoning global digital currency lab, supports a variety of digital currency transactions, such as Bitcoin BTCU / Wright Coin / ETHU / ZEC), high-speed matchmaking engines, a full range of funds security, and an extremely fast charging experience. To provide the most secure, convenient and professional digital asset services for global digital currency lovers, we have been committed to the creation of the most professional digital asset trading experimental and practical platform. Gresham Labs follows the following six values:



Distributed / 分佈式

通過分佈式的、多方對等參與的區塊鏈技術，重構安全、可信任的共用帳本，幫助各機構在分佈式商業場景中實現專業分工與協同合作，完成資源的最優配置與聚變效果。

Regtech-ready / 監管科技化

引領監管創新與制度創新，支持監管機構在區塊鏈網路中部署監管節點及在此之上的大數據監控平臺，可即時進行數據採集報送、數據溯源及業務風險管控。

Innovative / 變革創新

數位化時代即將全面主宰經濟與社會的每個側面，我們致力於提供未來前沿的基於區塊鏈技術的分佈式商業公共基礎設施。

Value-driven / 價值驅動

構造可交換、可分享的分佈式資訊網絡與價值網路。

Extensive / 廣泛適用

支持金融服務、工業互聯網、供應鏈、健康醫療、物聯網等多個行業領域。

Secured / 安全可控

作為中國企業聯合研發的全球化平臺，完全實現安全可控，既深度符合國情，又具備全球領先的實力。

4.2. What's Graycoin Cash?

Graycoin Cash is on the basis of ripple's RTXP agreement and the centering of bitcoin. The digital currency developed by block chain technology is the central currency of Graycoin Cash global digital currency application ecology.

Graycoin Cash will become the core information source of the industrial chain, the value chain and the ecological chain in the ecosystem, as well as the core information source of the large data center of the applied ecological block chain in the future. With the insight generated by the data, Graycoin Cash application ecology will accurately match the two sides of the transaction, achieve intelligent matchmaking, significantly increase the transaction rate, and reduce transaction costs.

Graycoin Cash acts as the ecological internal financial hub or center to promote internal capital transfer and centralized management, further evolves and extends Graycoin Cash system to industrial chains, value chains and ecology, and cooperates with various financial institutions and physical industries. Build the application ecology of "block chain + financial industry consumption".

4.3. The characteristics of Graycoin Cash

Block chain bottom technology

Block chain bottom technology, with decentralized, open and transparent, safe and reliable, open consensus and other characteristics.

Owning entity applied ecology

Based on Graycoin Cash system, a huge block chain digital monetary ecology is established, which is connected with a variety of entities around the world.

Ecocentric currency

Graycoin Cash, as the central ecological currency, links the RMB with other currencies (other digital currency, French currency and digital assets), exchange, circulation channel, is the lubricant running through the whole ecology, and its own value is incalculable.

Incremental issuance

Establish rules with wisdom contract, daily additional issue, regular attenuation.

4.4. Graycoin Cash wallet

Wallet is the main access to Graycoin Cash, storage and exchange between the various currencies within the platform.

A Graycoin Cash wallet support:

- There is an address like this: Ox9CJAWyB4rj91VRWn96DkukG4bwdtyTh1 / Ox', plus 32-bit hexadecimal characters); the address contains a check code. Make sure that typing errors are unlikely.

- Collecting income from mining;

- Collection of promotional income

- Exchange with the balance of the wallet
- All currencies rolled out within the platform

4.5. Graycoin Cash account

An account is an entity in Graycoin Cash account. Usually, people have an account that holds their Graycoin Cash loan records, IOU, trust paths and trust relations with other accounts. Anyone who knows the secret key of an account can authorize the purse to initiate a transaction (that is, to have a private key. " Everything has the account.

A Graycoin Cash account:

- ✓ Holding Graycoin Cash transaction balance
- ✓ May hold a promissory note issued by another account)
- ✓ You can set up a trust in another account (usually a gate Gateway) (this account can issue you currency promissory notes)
- ✓ Can hang orders, money exchange wallet balance, trust amount, payment is public information.
- ✓ No one can know who the wallet is for.
- ✓ Each Graycoin Cash account has an address for other wallets that:
- ✓ Send the balance of the other account to the account

- ✓ Extension of the trust line to the account

4.6. Graycoin Cash issue plan

Constant circulation: 600 million

Issue time: 6 years

Pre-digging: Graycoin Cashcoin (Graycoin) is officially released three years after Gracin's lab pre-dug 3000 pieces, or 5%, over three years.

Graycoin Cash will be circulated in the block chain application scene created by different types of laboratories.

4.6.1. Issue plan

- ✧ Issue time: 3 months, issue number: 6 million

- ✧ Second phase: 8 months of issuance, with a monthly increase of 18% in money holding and promotion awards

- ✧ Third issue: one year and two months, with a 14% monthly increase in money holding and promotion awards

- ✧ Fourth issue: one year and eight months, with a monthly increase of 10% in money holding and promotion awards

- ✧ Fifth issue: one year and eight months, with a monthly increase of 6% in money holding and promotion awards

4.6.2. Revenue calculation

The main role of the server is to calculate the number of platform coins that each user can receive on a daily basis, based on the actual formula, as follows:

Interest on currency:

Formula: earnings per day (daily circulation / total number of users holding money) (number of coins held on that day / total amount of money held at all nodes / total amount of money held at all nodes / total amount of money held by all nodes / total amount of money held by all nodes / total amount of money held by all nodes / total amount of money held by all nodes)

Computational formula of C or by Di: United Mi× CF weight of 1000 M_1 plus plus plus M M behavior of M_4 * PCF..

Formula: C: number of GCH issued on the day

U: number of all coin-holding members

Mi: number of coins held by members on the day

CFC: force value for the day

Di: interest on money held on the same day

M / M / M / M: all currency holdings

PCF: force value of the issuance plan

Case of Coin-holding income:

Assuming that there are only 10, 000 users in the world, with a total holding capacity of 1, 000, 000 GCHs, Gracin Labs issues 500, 000 GCHs on the same day, and I hold 5, 000 GCHs in accordance with the first issue force value 6000, I have 5, 0001GCHs, so I have calculated power values according to the maximum of 100, the substitution formula can be obtained

Di=(50000/10000)*(50001*(100/1000)/1000000)*6000=150.003GCH

4.6.3. Extension income

Calculation formula (Chinese description: day promotion income = user point promotion / all user points promotion power) (daily circulation volume per second)

Official: computational Bi by Xi gets X $_1$ behavior of X plus plus plus X X $_4$ +...) C. Times. 2, C CF 1000 config

Formula: C: number of platform coins issued on that day

Bii: promotion proceeds for the day

Xii: popularizing calculation power

X X X: the Promotion of every Wallet

CFC: force value for the day

4.6.4. User point generalization power

Official: computational Xi by Pmax potential 1 / 3)+(P $_1$ plus plus plus P P behavior of P $_4$ teacup.

The formula shows that the calculation force should be generalized.

Pmax / 1 / 3: maximum popularizing power is cubic.

P: all user outreach

Calculation value interval delineation：

Currency holding range	Bottom value	Capping force value
1-500	10	15
501-3000	15	40
3001-10000	40	60
10001-20000	60	70
20001-50000	70	85
50001+	85	100

Value delineation of the calculation force of the issue plan：

Issue cycle	Calculated force value
1	6000
2	5500
3	5000
4	4500
5	4000

4.7. The characteristics of Graycoin Cash issuance Mechanism

4.7.1. decentration

Graycoin Cash is a digital currency, there is no central issuer, the decentralized Graycoin Cash on a pro rata basis, so there is no payment.

4.7.2. Equitable benefit

Graycoin Cash is the first digital currency that truly feeds back the value of money to value creators! Through Gray's innovative cash issuing algorithm, the right to issue money is distributed to the holders and promoters of the currency, so as to realize the fair monetary system in which the value creators get the value.

4.7.3. Preservation and appreciation

Gray's total cash limit is 600 million, and the money software background is closed-loop locked and can never issue additional money. Solved the inflation problem, let the currency keep value, appreciate.

4.7.4. Withdrawals at any time

There is no closed period, collaborative market dealmaking, can withdraw the principal and interest at any time.

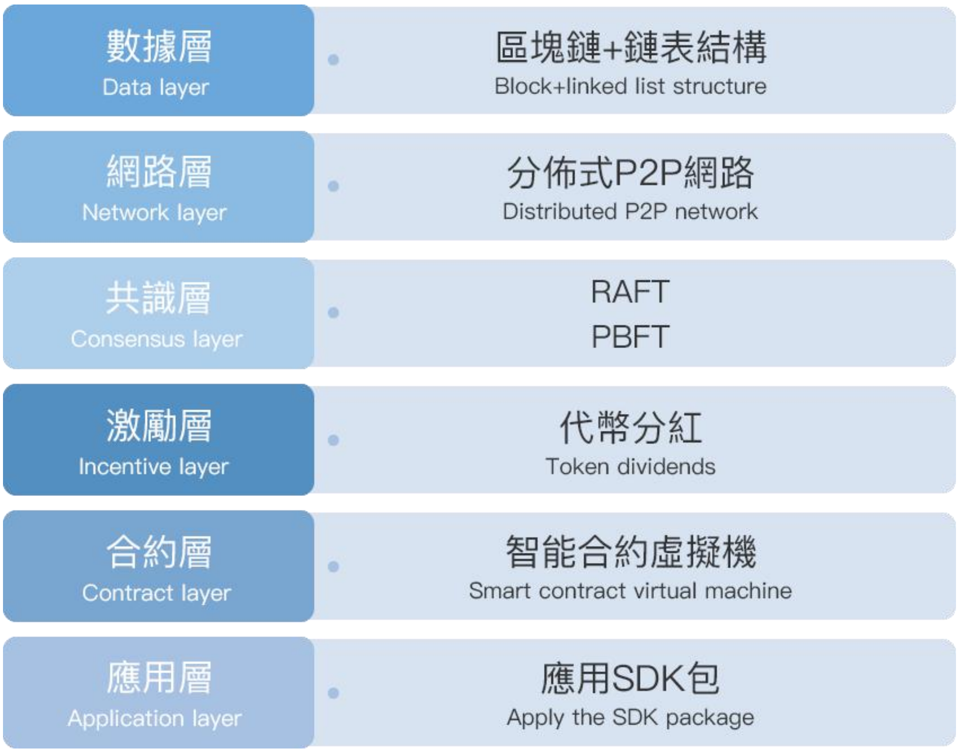
4.7.5. Global distribution

The larger the volume, the higher the value and stability, so that the holder and the promoter gain higher profits, and then urge the promoter to make more efforts to promote, so that the holder is willing to invest more, forming a virtuous circle.

5. About Graycoin Cash system.

5.1. system architecture

Graycoin Cash architecture consists of six layers: data layer, network layer, consensus layer, incentive layer, contract layer and application.



數據層 Data layer	區塊鏈+鏈表結構 Block+linked list structure
網路層 Network layer	分佈式P2P網路 Distributed P2P network
共識層 Consensus layer	RAFT PBFT
激勵層 Incentive layer	代幣分紅 Token dividends
合約層 Contract layer	智能合約虛擬機 Smart contract virtual machine
應用層 Application layer	應用SDK包 Apply the SDK package

5.1.1. Data Layer

Based on the high redundancy storage mechanism of block chain, block chain storage has a certain impact on the expansibility and performance of block chain. Graycoin Cash framework is designed with multi-level node system. According to different node applications, there are different storage strategies (distributed bookkeeping: accounting node: Graycoin Cash core role, entrusted by the BST holder to participate in the consensus mechanism, manufacturing blocks. All-node: responsible for preserving the complete data, but not participating in the consensus, listening and relaying transactions. Ordinary users directly through the interface or user access, do not save data. The advantage of a multilevel node system is that it is not desirable that all nodes be involved in accounting (mining), store complete data, relay transactions. Because not all nodes have the same demand, they all want to keep the complete data. Graycoin Cash design makes the whole system have a clear division of roles, professional nodes do professional things, not only save energy but also improve the efficiency of the whole system.

5.1.2. network layer

P2P protocol supports data transmission and signaling exchange among nodes in block chain network. It is an important communication guarantee for data distribution or consensus mechanism. Graycoin Cash system supports many P2P protocols. The configuration of communication mechanism and serialization mechanism requires flexible protocol usage according to different scenarios. In terms of communication security, we can flexibly support secure communication protocols such as HTTPS / TLS / TLS / WSS secure Web sockets. We can extend the support for OAuth on the platform application external service interface. Authentication integration.

5.1.3. Consensus layer

Graycoin Cash selection PoW (workload proof) and PoS (equity proof) consensus algorithm is a Byzantine fault tolerant consensus algorithm based on bookkeeper vote. It has the characteristics of high performance and high consistency, and is suitable for financial payment. Digital transaction data is generated frequently, and has high real-time accounting requirements of the weak center upper application. Because of the setting of accounting rules, the traditional block chain needs to reach a certain number of block confirmation to complete the chain confirmation in a certain probability. That is to say, when the block is added to the block, it can guarantee 100% that it will be this chain in the future. There's always a tiny possibility of being overturned. . Basic needs to six blocks 99.999999% of the confirmed transactions. In this mode, the final transaction is weak, so it is not suitable for the digital upper application of financial payment such as digital asset trading platform. DBFT consensus algorithm can keep block consistency well. This consensus algorithm selects bookkeepers according to the proportion of rights and interests, and then achieves consensus by Byzantine fault-tolerant algorithm between bookkeepers. Has a certain endorsement and letter, so basically more than a third of the accounting node collusion to do evil, even if this happens, we can use cryptographic evidence to run things Take evidence after the pursuit of responsibility.

The advantages of this approach are:

Professional bookkeeper;

Can tolerate any kind of error;

(3) bookkeeping is done by many people. Each block is final and does not bifurcate.

4) the reliability of the algorithm is proved by strict mathematics.

The core of the dBFT mechanism is to ensure that the system is final and not forked, so it is very suitable for the digital application of financial payment.

5.1.3.1.PoW (workload proof)

Work proof (Proof of Work), through calculation to guess a value (nonce), to solve the prescribed hash problem (from hashcash). Guarantee that within a period of time, only a few legal proposals appear in the system.

At the same time, the small number of legal proposals will be broadcast on the network, and the users receiving the verification will be based on the calculation of the longest chain that it considers to continue the problem. Therefore, there may be a chain branching (Fork) in the system, but in the end, there will be a chain that becomes the longest chain.

The problem of hash is irreversible, so there is no effective algorithm to solve it except for violent computation. On the other hand, if the nonceils are obtained, the corresponding computational power is paid in probability. Who has more computational power, the more likely he is to solve the problem first. When we master more than half of the whole network, we can control the direction of the chain in the network from the probability. This is also the origin of the so-called 51% attack.

People who take part in the PoW competition will pay a lot of economic cost (hardware, electricity, maintenance, etc.).

By the time the lucky ones are calculated, these costs will all be sunk. This also guarantees that if someone vandalism, it will have to pay a lot of economic costs. There are also designs that attempt to match the calculation power of a certain percentage into the next round.

There is a very intuitive example of why this economic game model ensures the uniqueness of the longest chain in the system.

The supermarket needs to line up for payment, and there may be people out of line to jump in line. The supermarket manager checks the line to see if the longest line is legal and requeues illegal forks. As long as most people are not stupid, they will consciously line up in the longest queue.

5.1.3.2.Pos (proof of interest)

Proof-of-rights was proposed in 2013 and was first implemented in the Peercoin system, similar to the real-life shareholder mechanism.

The principle is to bet against a legitimate block for interest and transaction fees on mortgaged capital through a margin (a valuable item such as a token, an asset, a reputation, etc.). The more margin you provide proof, for example, through money transfers, the more likely you will be to have the right to account. A legitimate bookkeeper can earn a profit.

PoS is an attempt to solve the problem that a lot of resources are wasted in PoW. The malicious participant will have the risk that the margin will be forfeited, that is, the loss of economic benefits. In general, for PoS, need to master more than the resources of the entire network, it is possible to determine the final outcome. It's also easy to understand that three people vote, the first two vote for one side, and a third party vote will determine the final result.

PoS also has some improved algorithms, including an enabling equity certification mechanism, in which shareholders vote to elect a board of directors so that board members have the right to keep accounts.

5.1.4. Excitation layer

Twenty percent of Graycoin Cash tokens are used for consensus rewards. Because Graycoin

Cash has a unique consensus mechanism and its performance is not affected by the number of nodes, there is no upper limit on the consensus nodes of Graycoin Cash, and it is dynamically issued. Anyone can join in at any time to earn an award.

5.1.5. Contract layer

For each intelligent contract, run the entire life cycle management of the financial assets as a necklace, complete and controllable process management for the submission, deployment, use, and write-off of the intelligent contract, And integrate the authority management mechanism to the intelligent contract operation mechanism for comprehensive security management. Integrity and risk control systems in the Internet finance industry are set up under Graycoin Cash intelligence contract, including P2P, crowdfunding, private equity, and Internet finance accessories. For example, forward contracts, block chain intelligence contracts, signing by both parties, and future designated deadlines for the sale of assets on the same day.

5.1.6. application layer

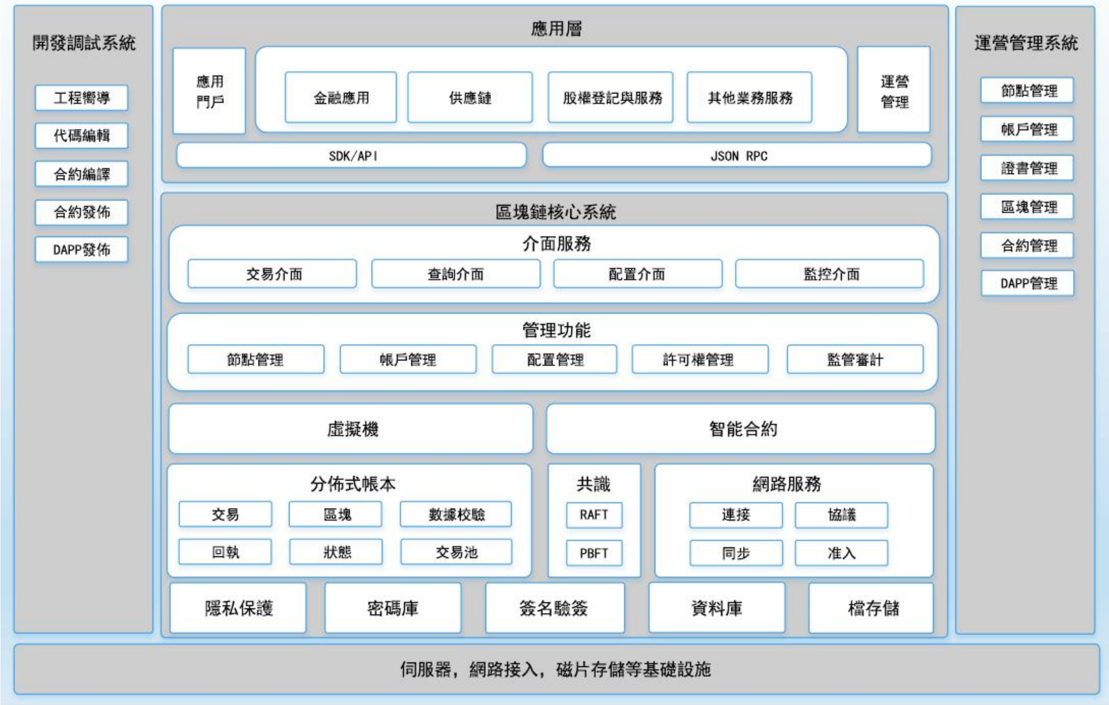
The application layer will provide general transaction protocol, support multilingual integration and function extension. At present, C#, JavaScriptPython PHP and other multi-languages have been supported. At present, a universal financial integrity protocol has been developed and completed. In fact, this protocol is not only applied to the integrity protocol of interconnected finance.

5.2. Platform technical characteristics

Unlike the traditional centralized business model, the development of the distributed business model needs to be carried by the new generation of data exchange infrastructure.

Graycoin Cash platform is a complete blockchain technology platform designed for large-scale distributed commerce, which has supported a number of distributed business scenarios in banks, equity markets and supply chains. As a new generation of commercial data exchange infrastructure, the current version of the Graycoin Cash platform already has some leading technical

features.



5.2.1. function

Has the perfect commercial application function and the ease of use, promotes the application landing practice.

Support flexible user account management function and implement alliance with role and privilege model

Chain participant management

Support for flexible configuration changes to all nodes across the network at the same time, configuration data retention High consistency.

Based on SDK, interface and intelligent contract, it can develop all kinds of business applications quickly. It will support many languages to write intelligent contract, and make the business development process more in line with enterprise software development conventions.

Supports packet multi-copy storage of files and holds hash of files in the block chain

Value and related addressing information to improve the efficiency of block chain storage and network synchronization.

5.2.2. function (of a machine, etc.)

It has high transaction throughput and low delay, can be expanded parallel, and can support massive services.

The transaction process and communication process are optimized to enhance the node processing capacity.

Implementation of an efficient consensus algorithm system, using plug-in design to support optimized

PBFT and RAFT consensus algorithm.

With parallel computing architecture, can be parallel expansion, to meet the needs of massive services.

5.2.3. safe

Multi-level, comprehensive safety protection to meet high safety standards.

The communication layer, user data and other modules are protected by high intensity encryption.

Many cryptographic algorithms are supported, including privacy protection algorithms based on cryptography.

Provide security best practices to secure the entire network.

5.2.4. administer

Has the standard management way, guarantees the business legal compliance, the system steady operation

CA system based on the identity authentication, with node access control mechanism.

Provide functional interface for regulatory audit and support access to regulatory audit

Support comprehensive monitoring of block chain indicators to ensure operational quality

Support the grayscale upgrade of the whole network to ensure the maintainability of the large-scale commercial network.

5.3. Platform technical route

The technical form in the field of block chain is still developing rapidly. The following technical characteristics are listed as the key research object by Graycoin Cash platform, which has been continuously invested in research and development.

5.3.1. Multi-chain and cross-chain

Depending on the requirements of business functions, privacy protection, data isolation, or performance capacity expansion, multiple independent chains work in parallel. Chains and chains can interact through cross-chain services, such as sending transactions, querying transaction results, Read configuration data, etc. Cross-chain interaction is currently the focus of research in the field of block chain, in security, fraud prevention, data consistency, efficiency and other aspects need to be further explored. Including:

To achieve parallel and cross-chain consensus and improve the efficiency of consensus;

The combined signature is used to replace the transaction execution for block verification, so as to reduce the number of transaction execution.

Cross-chain communication and data validation, cross-chain security transactions, cross-chain reconciliation.

5.3.2. Distributed storage

In the current implementation of block chain, each node stores the whole amount of block chain data. The data redundancy is high, and the data capacity is affected by the single machine storage hardware. In the mass service, if we need to store the data for a long period of time, The amount of data is generally not the capacity of a single server.

The block chain data is usually stored on the physical hard disk of this node based on the file system and does not provide a cross-network storage structure by using a file-type local database such as level db. In the organization with high data security requirements, the data is generally stored in the security area isolated from the external network to ensure the security of the data. At the same time, these organizations have established mature data storage and maintenance programs to ensure the high availability, scalability, portability and maintainability of data storage services at the infrastructure level, and integrate with systems such as big data's platform. Using the scheme of distributed data storage, the capacity and dimension of data can be considered synthetically. Protection, security, support the use of existing enterprise level distributed storage solutions, such as data warehouses, database clusters and other storage block chain data.

5.3.3. Privacy protection

Although block chain technology has some anonymity, both the address and the amount of money can be traced back, for some industry applications such as financial applications, there is a clear lack of privacy. Therefore, Graycoin Cash platform considers the following data to carry on the thorough encryption processing.

Transaction identity anonymity: completely anonymous double (multi-party) addresses in a transaction, satisfying one secret at a time, unforgeable, unrelated and traceable.

Transaction data encryption: encrypted transmission and storage of transaction data.

Account status encryption: encrypts transfers and stores account status data.

For the above encrypted data, meet the following requirements:

The interested party (counterparty , regulator) has the right to see the plaintext data

Other participants have no right to see plaintext data, but they must be able to verify the authenticity of ciphertext data

The Graycoin Cash platform plans to achieve multiple levels of privacy protection:

Identity anonymity: group signature is used for identity anonymity, and the supervisor can track the identity of the user.

Data Privacy Protection: an additive homomorphic encryption algorithm has been implemented on client and smart contracts, with plans to add zero knowledge proof to prove the correctness of encrypted data (e.g. whether account balance data is sufficient for payment)

Fine-grained privilege control: multilevel access control based on attribute encryption algorithm and proxy authorization cipher algorithm to control privacy access to encrypted data.

5.3.4. Token system

The chain token system has many applications, from subcurrencies representing assets such as US dollars or gold to corporate stocks, individual tokens representing smart assets, secure and unforgeable coupons, Even token systems that have nothing to do with traditional values are used to reward points. It is surprising how easy it is to implement a token system in Gracin's lab. The key point is to understand that all currencies or token systems are essentially a database with the following operations: subtract X units from A and add X units to B, The prerequisite is that there are at least X units and 2 units prior to the transaction.) the transaction is approved by A. Real To implement a token system is to implement such logic into a contract.

The basic code of implementing a token system in Java language is as follows:

```
from = msg.sender

to = msg.data[0]

value = msg.data[1]

if    contract.storage[from] >= value

contract.storage[from] = contract.storage[from] value

contract.storage[to] = contract.storage[to] + value
```

This is essentially a minimization of the state transition function of the "banking system" that will be further described in this article. Additional code needs to be added to provide the ability to distribute money at the initial and other edge situations, ideally by adding a function that allows other contracts to query the balance of an address. That's enough. In theory, a token system based on Gracin Labs as a subcurrency may include an important function that a Bitcoin-based chain dollar lacks: the ability to pay transaction costs directly with this currency. The way to achieve this capability is to maintain a Graycoin Cash account in the contract for the purpose of issuing The supplier pays the transaction fees by collecting the internal currency used to act as the transaction cost and auctioning them out in a running auction. The contract continues to fund the Graycoin Cash account. So users need to use Graycoin Cash to "activate" their accounts, but once the accounts have Graycoin Cash, it will be reused because Each contract will be recharged for each contract

5.3.5. Virtual machine optimization

The Graycoin Cash platform plans to support higher performance virtual machines and more mainstream development languages in the next release. Plan to support JVM Virtual Machine and Java development language.

5.3.6. Trusted information management

The "prophecy" solution makes it possible for blockchain smart contracts to access real-world uncertain data, such as asset prices, currency exchange rates, stock indices, and so on. The mechanism of economic incentive and game is used to make the uncertain external information into the block chain intelligent contract, so that the execution of the intelligent contract can rely on the real world data to carry out the related business process. A specific consensus mechanism is used to judge the certainty of submitting information so that the informed person can submit the real world data information based on the block chain digital identity driven by economic interests. A certain penalty mechanism also ensures that the information is deterministic and accurate. The property direction converges.

5.4. DAPP (decentralized application)

5.4.1. brief introduction

Decentralized applications are applications running on P2P networks rather than on a separate computer, or DApps has existed since the advent of P2P networks. It is designed to exist on the Internet in a way that is not controlled by any single entity, so DApp is a more reliable and secure system for storing and managing any type of data.

5.4.2. characteristic

The design of the open DAPP system is open and transparent, the open transparency is the basis of the whole DAPP system, the organization of a dark box operation can not be used as the DAPP, now the open source spirit of software becomes a typical example of openness;

Denaturalization, no Sinochem and the organization can control the entire DAPP, this feature determines the similarity, deChinalization ensures the life of the DAPP system;

The governance DAPP system can participate, the participants are companies or units of the DAPP system, and promote the development of DAPP. The sending of participants ensures the transport of DAPP;

The value DAPP system must be of value, such as the international payment of the currency system, anonymous transactions, tax avoidance, value storage, non-freezing, and non-regulatory characteristics, which determine the DAPP system.

The profitability of the

The participants of the for-profit DAPP are rewarded for the development of the DAPP system, and the profitability is determined by the value of the DAPP.

Similarity, even if only some DAPP nodes can still operate and develop normally, and the destruction of some unit nodes will not affect the development of DAPP.

• democracy, the changes in the DAPP system need to be voted on by the overwhelming majority of the units, which determines that DAPP must be a democratic voting system.。

5.5. Asymmetric encryption algorithm

Asymmetric encryption algorithm is a key security method.

Asymmetric encryption algorithm requires two keys: public key (public key) and private key (private key). If the data is encrypted with the public key, only the corresponding private key can be decrypted; if the data is encrypted with the private key, the data can be decrypted only with the corresponding public key. Because encryption and decryption use two different keys, this algorithm is called asymmetric encryption. The basic process of asymmetric encryption algorithm to realize the exchange of confidential information is: party A generates a pair of keys and takes one of them as a public secret The key is made public to other parties; Party B who obtains the public key uses the key to encrypt the confidential information before sending it to Party A; Party A decrypts the encrypted information with another special key kept by Party A.

On the other hand, Party A may sign the confidential information with Party B's public key and send it to Party B.

Party A can use its private key to decrypt any information encrypted by its public key. Asymmetric encryption algorithm is more secure, it eliminates the need for end-user key exchange.

The characteristics of asymmetric cryptosystem are: the intensity of the algorithm is complex, and the security depends on the algorithm and the key. However, because of the complexity of the algorithm, the speed of encryption and decryption is not as fast as that of symmetric encryption and decryption. There is only one key in symmetric cryptosystem, and it is not public. If you want to decrypt, you must let the other party know the key. Therefore, to ensure the security of the key is to ensure the security of the key. There are two kinds of keys in the asymmetric key system, one of which is public, so that the key of the other party can be transmitted without the need of the symmetric cipher. It's a lot more secure.。

5.6. term

Bitcoin: Bitcoin, the digital money technology initiated by Nakamoto.

Blockchain: block chain, a cryptographic and trusted information storage and processing technology.

Chain code: code that runs in advance on the block chain (state machine).

DAO:Decentralized Autonomous organization, distributed autonomous organization based on block chain

The loose crowdfunding group associated with smart contracts.

Distributed Ledger: distributed bookkeeping, a centralized bookkeeping platform that we all approve of.

DLT:Distributed Ledger Technology.

DTCC:Depository Trust and Clearing Corporation, Depository and Clearing Corporation, the world's largest back-office provider of financial transactions.

Fintech : Financial Technology , financial - related (information) technology .

Hash: hash algorithm that maps binary values of arbitrary length to shorter fixed-length binary values.

Lightning Network: lightning network, a technology for increasing transaction throughput through an off-chain micro-payment channel.

Noncec: a cryptographic term that represents a temporary value, mostly a random string.

P 2P: a point-to-point communication network in which all nodes are equal and there is no central control mechanism.

PoW:Proof of work, workload proof, under the premise of a certain difficult to solve a SHA256 hash question

Title

Smart contract: intelligent contract that runs on the block chain in advance of the contract;

Sybil attack: a few nodes masquerade as a large number of nodes by forgery or embezzlement, and then destroy the distributed system.

SWIFT:Society for Worldwide Interbank Financial Telecommunications, Global Bank Financial Telecommunications Association, operates the World Financial message Network, service banks and financial institutions.

Mining: through violent attempts to find a string, the hash value after it is added to a set of transaction information conforms to certain rules (for example, the prefix includes several zeros), and the person who finds it can claim that the new block has been found. And get a systematic reward for Graycoin Cash.

Miner: a person or organization involved in mining.

Miner: equipment specially designed for bitcoin mining, including GPU, dedicated chips, etc.

Mine pool: a team-based approach to mine digging and allocation of bitcoins.

The depth of the market: transactions that have not been concluded, measuring the stability of the exchange rate after the market bears a large amount of trading.

Turing completeness: the function of a machine or device that can be used to simulate a Turing machine (the embryonic form of a modern general-purpose computer).。

6. Application scene

6.1. Application planning

Gracin is committed to the development of a third blockchain ecosystem outside Bitcoin and Ethernet Square, expanding the application boundaries and technical boundaries of blockchain technology so that the value of blockchain technology can be felt by ordinary Internet users. In Graycoin Cash system, peer-to-peer value transfer can be achieved through the value transfer protocol (RTXP), under which a multi-industry (financial, e-commerce, physical, social, consumer, and social) system can be constructed to support multiple industries. A decentralized industrial circulation platform。

6.2. application area

6.2.1. Online shopping mall

Taking the block chain as the bottom technology, the properties of decentralization and non-tampering are realized, and the current electronic commerce and block chain technology are combined in depth fusion. Through block-chain technology to create high-quality commodities, the realization of national income, supervision by the whole people. In addition, Greshin offers smart contracts, multi-signature, digital currency trading, smart customer service, and other seamless services, allowing more businesses and customers to have innovative experience and services.

B2B2C Multi-user Mall system

To help enterprises to create a variety of B2B2C profit model, the best choice for multi-merchant-based e-commerce.

Member management system

Using data to help you better understand customers, care for customers, a variety of marketing means to improve the rate of purchase, increase revenue.

New retail management system for O2O stores

Open online leisure integration, create a new type of customer-led stores online contact customers, promote multiple store consumption.

Solutions:

Small enterprise financing difficulties, user loan difficulties, is an important factor in the emergence of e-commerce finance, Graycoin Cash for providers to supply online supply settlement system, and to small enterprises and individual users to provide financial services products, the use of service products convenient, innovative point, financing for small and medium enterprises and individuals, loans, loans. Business. It also provides suppliers and electronic business platforms firmly tied together, and can also provide users with sustainable and effective financial services.

digital cash

A distributed accounting system that allows users to grade and distribute digital assets, title vouchers, integrals, etc., and transfers, pays and trades on a point-to-point basis

[自]intelligent management

Commodity data, inventory, order, on-line and offline integrated management, easy docking each platform, matching the solution for the entire business chain, reasonable application in the form of business, industry and popular e-commerce.

Open and transparent

All environments in the supply chain, including production and processing, will be uploaded to the underlying Gray Lab in the form of photos and videos, and users will check the information at all times to verify what the business is saying.

Advantages:

The Russian data on the block chain can not be tampered with, which is beneficial to the traceability of the commodity, and the establishment of credit cost can be reduced by using the platform established by the block chain.

Provincial trust cost

The application of block-chain makes it possible for businesses that are not in a centralized market to invest a lot of effort, manpower and advertising budget to build trust in the e-commerce industry.

Management system optimization

Prevent commodity information and the possibility of tampering in the process of transportation, once there is a problem, you can easily find out in which link the problem, clear up the related responsibilities.

Data authenticity

Applicable to the distributed accounting model, which records every transaction with tamper proof, and maintains the authenticity of the information on the global network, preventing information from being unequal in the process of purchase as a result of activities such as brushing orders

Decentralized payment

Helps to reduce the cost of reconciliation between financial institutions and the cost of dispute resolution, thereby significantly increasing the processing speed and efficiency of payment operations

6.2.2. Game platform

The game industry is a huge industry . At present , the global game player has more than 1 billion people , the industry has a breakthrough of $ 8 billion . But for players , the player ' s interests are hard to guarantee . It is said that the player ' s interests are hard to guarantee . It is said that the player ' s interests are hard to guarantee . It is said that the player ' s interests are hard to guarantee . Unlike traditional online games , end games , etc . , block chain games are distributed in a publicly transparent block chain , not only unique . And once owned by you , it is your personal asset . and cannot be copied , modified or destroyed by any person unless the person is in custody or has a problem with the exchange on which the block chain belongs .

Advantages:

Data authenticity

Block chain has uniqueness , security and non - tamper proof technical support

Decentralized payment

Helps to reduce the cost of reconciliation between financial institutions and the cost of dispute resolution, thereby significantly increasing the processing speed and efficiency of payment operations

Asset sharing

Player role information as personal "assets" in multiple game world circulation, block chain game in the digital assets can be in accordance with a certain protocol to achieve cross-platform circulation, This is very different from the traditional network game closed system, many block chain game products can form a consensus game alliance chain, so as to achieve the circulation of various game assets and user sharing, This ability is undoubtedly to activate and amplify the value of the digital assets of the blockchain game

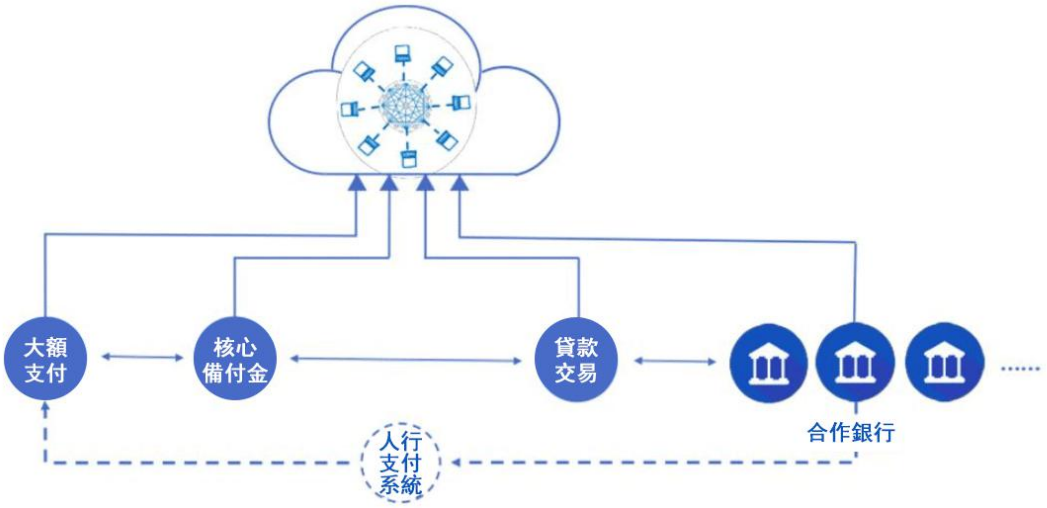
Grange Labs GCH) Entertainment can be open to all games via the platform API. GCHG's quick and convenient payment system and intelligent mechanism of intelligent contract can realize the transaction and distribution of props, so that online entertainment in the payment chain has the advantages of encrypted virtual property, decentralized payment, free exchange of props, and so on. Independent settlement, independent operation, protection of players, fairness, and no change in the original game system will all be unique to the online entertainment in the payment chain as distinct from the traditional system。

6.2.3. Financial industry

By using the block chain network, the traditional financial institutions, foreign exchange market makers and liquidity providers are added to the payment network and become payment gateways. Through the payment gateway, the flow of digital assets on the block chain can be connected with the legal tender in reality, and the legal currency can be converted into the digital assets in the block chain, which is convenient for subsequent payment transfer. The network connector in the block chain payment network can connect the traditional market maker, exchange trip, import line and so on, abandon the intermediate transaction link, and realize the point to point fast and low cost payment.

According to the current traditional network payment architecture, the transaction flow of cross-border payment is deeply analyzed, and the block is combined in this paper.

The characteristics of chain Technology and the Construction of Cross-border payment solution based on Block chain。



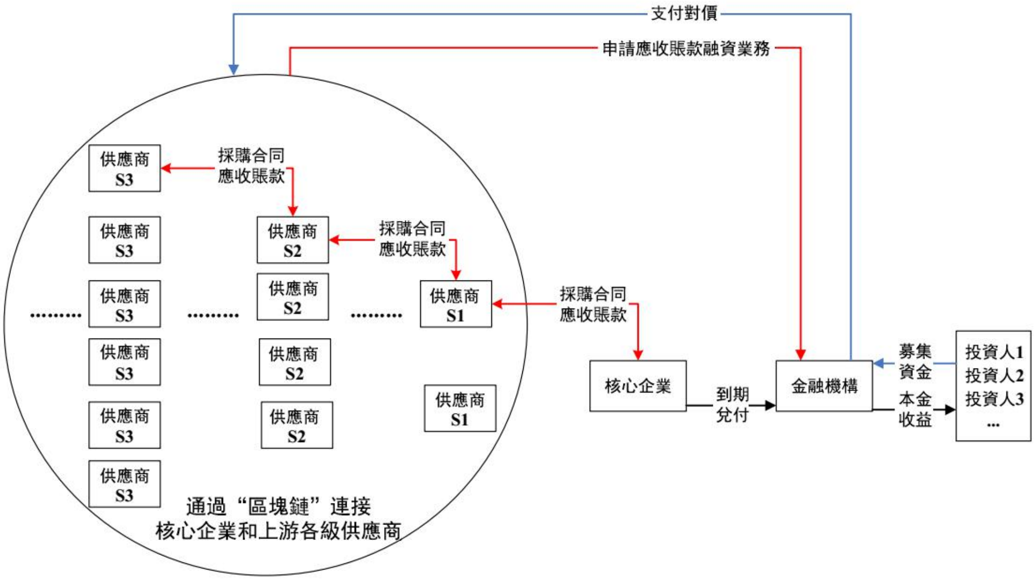
6.2.4. screen culture

The application of film and television culture is mainly to integrate the various links in the cultural industry chain by using block chain technology, accelerate circulation and effectively shorten the value creation cycle. Through block chain technology, the works are authenticated to prove the existence of text, video, audio and other works, to ensure the authenticity and uniqueness of ownership. The works are confirmed in the block chain and the subsequent transactions will be recorded instantly to realize the whole life cycle management of the entertainment industry. It can also be used as the technical guarantee in the judicial evidence collection. Block chain digital proof can protect the integrity, consistency and intellectual property rights of the data.。

6.2.5. supply chain

Supply chain finance business is very suitable for block chain and distributed accounting technology. First, the business involves many main bodies, including the core enterprises, suppliers, financial institutions, investors, etc., the transaction information is transmitted through the block chain between the multi-agents. Secondly, the transaction information in the supply chain is usually commercially sensitive information. The block chain technology can realize data encryption, and finally, through the block chain technology, the data can not be tampered with and traceability, can effectively eliminate the common false trade phenomenon in supply chain financing.

In general, the platform is aimed at the core enterprises with high credit rating and low financing cost, using block chain technology to link the supply chain transaction information and transfer credit from the central enterprise to the end supplier. To improve the allocation efficiency of financial resources among enterprises in supply chain。



6.2.6. Commercial real estate

In the traditional real estate market, there are some problems, such as lack of transparency, complicated formalities, fraud risk, error of public record and so on. The payment chain uses block chain technology to record and track land ownership, lease, lien, and other information, and to ensure the accuracy and verifiability of the relevant documents. GCH, a digital currency that can link up with the global currency, enables paperless and instant trading of commercial real estate. In concrete operation, the application of payment chain block chain technology in the protection of house property right can reduce the time of property right searching, realize the sharing of property right information, and avoid the deception in the course of real estate transaction. Fraudulent behavior to improve the efficiency of Real Estate Industry。

7. reference documentation

1. Nakmoto,S.(2008).Bitcoin:A Peer-to-peer electronic cash System.

2. Mazieres,D.(2015). The stellar consensus protocol: A federated model for internet- level consersus. Steller Developent Foundation.

3. Brown,R.G.(2016). Introducing R3 Corda: A Distributed Ledger for Financial Services.R3 April,5.

4. UK Government Chief Scientific Adviser:Distributed Ledger Technology: beyond block chain.
5. Sachs, G.(2016). Blockchain-Putting Theory into Practice,this-blockchain.com,25-32.

6. Buterin,V.(2014).A next-generation smart contract and decentralized applicationplatform.white paper.

7. Zindros,D.,(2016).Trust in decentralized anonymous markerplaces.

8. Swan,M.(2015). Blockchain:Blueprint for a new econimy.”O’Reilly Media,Inc.”.

9. Kosba,A.,Miller,A.,Shi,E.,Wen,Z.,&Papamanthou,C.(2016,May).Hawk:The blockchain model of crytography and privacy-preserving smart contracts. In Security and Privacy(SP),2016 IEEE Sym[posium on (PP.839-858).IEEE.