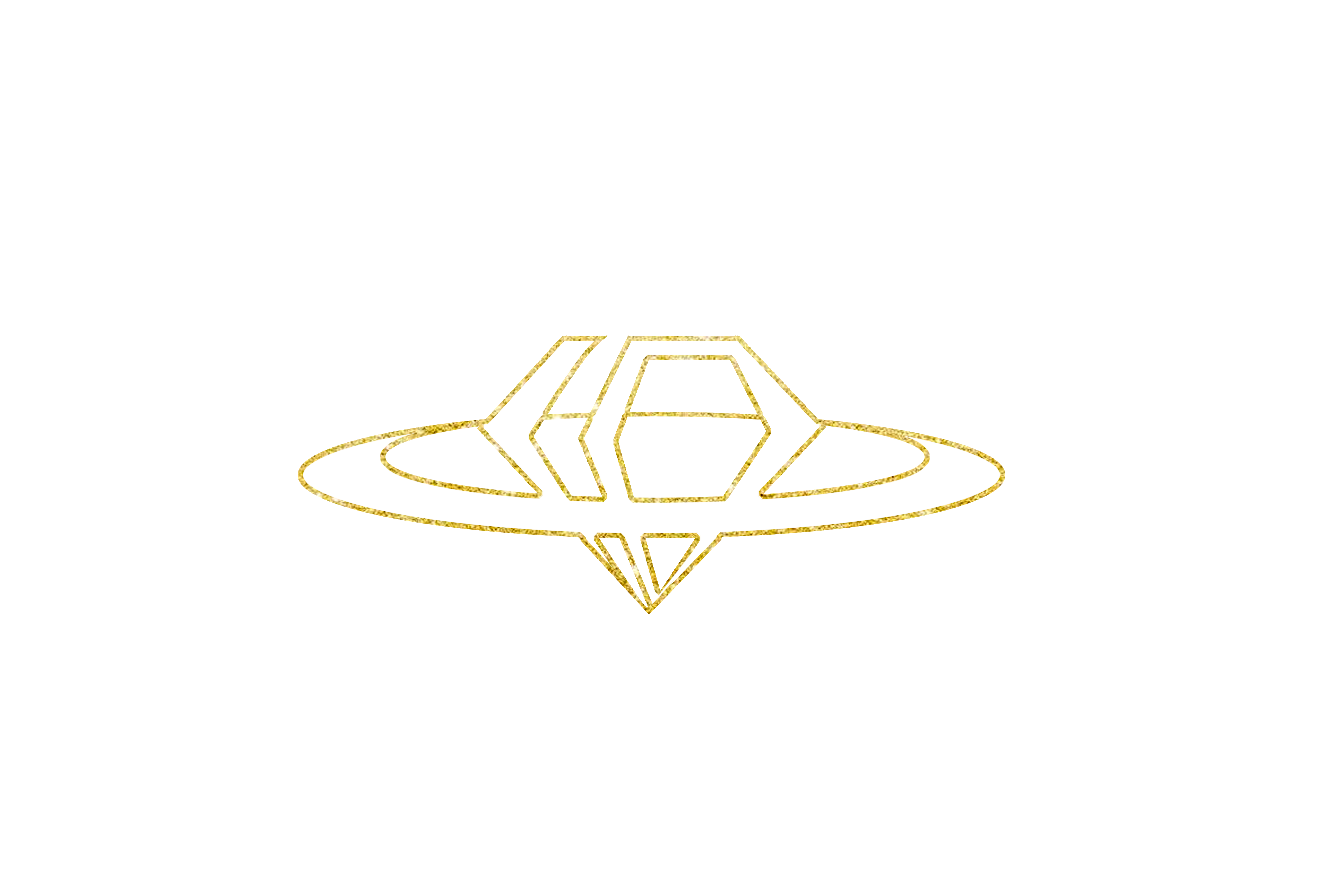
**South Africa Diamond Blockchain VAC White Paper**

****

**VAC: Build the cornerstone of the digital economy**

- The world's first blockchain innovation to cover the entire industry value chain

**table of Contents**

Foreword

1. Blockchain rise and future

1.1. What are the areas of diamond economic development that we want to cut into?

1.2. What is the diamond economy system?

1.3. What is the characteristic of the diamond economy?

2. Traditional trade can no longer meet the needs of global informationization

2.1. Lack of advanced source traceability system

2.2. Lack of service provider

2.3. There is a big problem with data transfer

3. blockchain application opportunities

3.1. Use digital cryptography to build trust

3.2. Policies favorable outlet

What do we do?

4.1. Create blockchain electronic resumes

4.2. Create a hybrid cross-chain service based on three types of blockchain

4.2.1. Personal application services based on the public chain

4.2.2. Multi-level traceability system and application based on coalition blockchain

4.2.3. Diamond blockchain-based informatization

5.VAC was born

5.1. Fundamentals

5.2. Blockchain design ideas

5.3. Blockchain core technology

5.4. Trends

5.5. Running into the economic era of blockchain

6, diamond block chain (Consortium Blockchain) and multi-level traceability system

6.1. Why use diamond blockchain

6.2. What is a multi-level retrospective system?

6.3. How to build multi-level traceability system with diamond block chain

7. Based on the diamond blockchain source form

7.1. How form data is stored and transmitted based on blockchain

7.2. Key Industries in Economic Development of Diamond Block Chains

8, application service layer (Trust Application)

8.1. Basic Services

8.2. User Management

8.3. Smart contracts

8.4. Operation Monitoring

8.5. Custom Assets and Identity Management

8.6. Decentralized transactions

8.7. Business Logic Processor

8.8. Designing Transactions for Static Verification

8.9. Object Data Schema

9. Platform product service layer

9.1. Digital assets

9.2. Assurance Services

9.3. Sharing Book

9.4. Sharing the economy

10. Technical Features and Benefits

10.1. Resolver Technology

10.2. Technical advantages

10.2.1. High Performance

10.2.2. High-speed access

10.2.3. Security

10.2.4. Without limitation

10.2.5. Low rates

10.2.6. Efficient operation

10.2.7. Privacy

10.2.8. Open source and fully transparent

10.2.9. Scalability

11. Diamond chain profit model

11.1. Business progress

11.2. Product Development Progress

12. Diamond Chain Market Forecast

13. Tokens, and chain-based services

13.1. Development and distribution of tokens

13.2. Chain-based services

13.3 Trading

13.4 Account System

14. Risk control audit

15. Why we can do it well

16. Problems and Solutions

17. Leading the future

**Foreword**

In 2018, in his State of the Union address, the new President, Ramaphosa, reiterated his central emphasis on the core policies of fighting corruption and boosting the economy. He will lower unemployment, stop corruption and strengthen infrastructure as the primary goal of the new government, with a focus on creating jobs. President Ramaphosa, who emerged as the "transformative" image, promised to carry out thorough economic reforms and crack down on corruption, will repeatedly break through multiple dilemmas such as economic stagnation, serious unemployment and financial market turmoil.

South Africa has developed its financial, legal, communications, energy and transportation industries. It has a complete hardware infrastructure and stock exchange market. Both gold and diamond production rank first in the world. Technologies such as deep-well mining occupy the leading position in the world. Diamonds deeply touched people's hearts with its bright luster. On the one hand, as a token of love, it represents the eternal love of romance. On the other hand, diamonds have great investment value and are one of the important forces boosting the economy.

However, the fickleness of the diamond market, true and false, and the physical transaction of online diamonds have long been controversial. How to ensure that consumers buy diamonds both genuine and clear path seems to be a problem.

With bitcoin's rapidly growing use in South Africa, blockchain technology is widely recognized as a turning point for this issue or a new turning point for the luxury goods industry such as gold and diamonds.

Blockchain technology in luxury transactions in the actual application project - VAC diamond wind control transactions to the center of the platform, combined with blockchain technology for the real industry to create a traceability system, through the establishment of a digital currency and the legal currency of the block Chain system to facilitate the trading of physical products easier, faster and more transparent.

Looking at the developed countries in the world, they have joined the "arms race" in the blockchain. South Africa has also integrated the blockchain into its national development strategy, actively participated in global competition and is committed to becoming a leader in a big era.

**1. Blockchain rise and future**

Prior to 2009, there were three ways of holding assets in the world: physical ownership, physical registration and digital registration.

After 2009, a "cryptocurrency" appeared. It is held in the same way as an "entity holds" the ownership of the ownership through the owner's private key; and, like the "entity registration", its value is recorded in the general ledger.

The best-known cognition is that the underlying system of cryptocurrencies is blockchain technology, which is a shared transaction database stored on the Internet computer network,

Further research found that blockchain is a distributed computing technology that produces an indelible, tamper-proof ledger at its core. It has the power to "reduce costs," streamlining processes and reducing unnecessary transaction costs and system costs, and many believe that this new approach to recording can change many social areas, such as shipping, insurance and finance , More practical for improving the current economic downturn.

With blockchain technology, digital currency breaks the "dark" box of traditional paper currency. The flow of banknotes as entities is invisible. No one knows where a banknote is coming from, and the blockchain allows every movement of the digital currency to be clearly identified with a "chain" It also protects the privacy of the participants.

All in all, the significance of blockchain lies in the ability to build a more reliable Internet system that fundamentally addresses fraud and rent-seeking that exist in the exchange and transfer of value. More and more people believe that with the popularization of blockchain technology, the digital economy will become more credible and the economy and society will become more just and transparent.

**1.1. What are the areas of diamond economic development that we want to cut into?**

"Diamonds last forever and forever, which is an extremely successful example of De Beers' propaganda, cleverly linking diamonds to love and loyalty." Diamonds bring a sense of visual enjoyment and mental pleasure.

In addition to being a jewelry, more manufacturers regard diamonds as an alternative investment asset. However, in the past, it has been very difficult to achieve this due to the lack of uniform standards. Like gold, the charm of diamonds is rare and long. But unlike gold and its public benchmarks, there is no price volatility for diamonds. This is because diamond trading is often done behind mysterious veils.

At present, we are treating digital currency as capital. If you buy digital currency at a particular point in time and then sell it, you may experience capital appreciation, which we then consider as capital gains.

**1.2. What is the diamond economy system?**

From offline to online, retailers are taking action to ensure the transparency of diamonds. They proactively track the route of supply of their products from mining sites to markets. In addition to the 4C features on the surface (color, carat, sharpness and cut), the 4Ts standard was created: traceable, transparent, real and thoughtful. Recorded every piece of diamond stone from procurement to production of the entire process. (That's what we call internal Intel chips. Vertically integrated retailers source from the most reputable diamond producers and have midstream processes such as polishing, cutting and distribution, as well as downstream sales platforms.)

**1.3. What is the characteristic of the diamond economy?**

Due to inadequate monitoring, many fictitious diamond sellers have made the reputation of online diamonds poor. This phenomenon has become even more serious in the liquidation of assets after the 2008 financial crisis.

The diamond industry has always had a certification body, a central database that uses spectral analysis to identify color-coded laboratories but does not have information. Lost diamonds rely on paper certification records. As information is stored on the blockchain, this creates an aggregated dataset, a shared visible record, and an audit trail to prevent incidents such as double financing or lab-grown gems being misidentified.

2. Traditional trade can no longer meet the needs of global informationization

2.1. Lack of advanced source traceability system

According to a survey released by the non-governmental organization Global Witness, blood diamond trading originating in the Central African Republic has entered the Facebook online market. A fictitious buyer uncovered this illegal digital activity on social media sites. The group found that the instant messaging platform was also used as a tool to smuggle conflict gems into international supply chains.

2.2. Lack of service provider

Unscrupulous dealers will find opportunistic buyers. Even legitimate diamonds are known for their cash behind the scenes. Problems caused by precious gems still exist. In the insurance industry, billions of fraudulent claims are often lost each year on the basis of false claims of the loss of jewelry.

Due to the industry's higher risk, banks typically avoid the diamond business. Standard Chartered Bank also stopped its diamond business last year due to earnings and compliance reasons. Exotic assets such as diamonds, to a large extent, are not commercial commodities and, given their nature, provide a tremendous advantage for money laundering and tax evasion.

2.3. There is a big problem with data transfer

In order to stop the influx of conflict diamonds, the United Nations made a landmark decision as early as 2000, the "Kimberley Process." At the same time, a three-step verification method was introduced, in which mining countries were required to provide declarations for each gemstone. A total of 75 diamond producing countries in the world have complied with the plan to establish an import and export control system. However, the resolution covers only rough diamonds used by rebel groups to finance wars initiated against legitimate governments, but does not deal with the broader trade-related human rights violations. Venezuela, for example, was unable to legislate to prove the legitimacy of its diamonds and was therefore removed from the Kimberley Process.

3. blockchain application opportunities

3.1. Use digital cryptography to build trust

Although it is argued that since diamonds are unique and require a separate assessment, they can not be considered as a commodity and the industry is beginning to change, and although the implementation of the blockchain is still in its infancy, we still see it as a potential investor Potential for greater transparency and security. Blockchain technology complements existing practices by not only tracking diamonds safely but also providing valid digital proofs. (Blockchain) is a record of any product from

The resulting public record book, and all records are not reversible, in addition, this technology is more secure than any single service system.

Ensuring ethical procurement of diamonds is the key to maintaining consumer confidence. The majority of diamonds produced in general are produced in countries such as South Africa and will be sold to authorized buyers for cutting or polishing and then for sale to retailers. In order to prevent the influx of synthetic materials into the natural diamond market, the blockchain technology is a good preventive measure to improve the transparency of the transaction and eliminate the transaction of the blood diamond.

3.2. Policies favorable outlet

In fact, South Africa is considered one of the key players in improving the digital currency environment.

As the South African Minister of Finance said, we welcome blockchain and digital currency because blockchain technology is a low-cost, efficient and extremely secure trading model that can also be used as a transfer of funds between individuals or institutions, generally favored The potential of digital money. We must not only encourage development but also control risks. Besides creating cryptocurrencies, it is imminent to explore the potential application of blockchain technology.

What do we do?

4.1. Create blockchain electronic resumes

Examines in detail the digital currency structure of the central bank and gives the blockchain system a brand new name, "Diamonds Blockchain." Because such a system becomes officially recognized as soon as it becomes effective, securities, stocks, derivatives, and even real estate and vehicle registration information from other financial institutions are transferred to the diamond blockchain system. In this way, the central bank can also supervise the assets created by commercial banks in real time.

4.2. Create a hybrid cross-chain service based on three types of blockchain

4.2.1. Personal application services based on the public chain

Private chain: Intra-agency application, which is the application chain of terminal information flow in all production circulation links within the organization;

Alliance chain: Institutional applications in the region, that is, each agency is a node, a block;

Chain: System benefits, that is, the application-oriented chain for the majority of users.

Just as the unrestricted flow of information alters the way humans interact with the digital age, unrestrained flow of value may also change human trade and industry. Blockchain has created cryptographic tools, a mixture of digital and digital registration tools, the least frictionless form of value so far.

4.2.2. Multi-level traceability system and application based on coalition blockchain

In addition to physical products such as diamonds, multi-asset books, bonds, stocks, derivatives, contracts and a host of other records will be allowed to be registered thereon,

4.2.3. Diamond blockchain-based informatization

We are taking a balanced approach to supporting innovation, competition and inclusive finance in the financial sector. Advancing bitcoin and cryptocurrency development. Through the judiciary, support for the goal of strengthening innovation, competition in the financial sector and financial inclusion, while reviewing cooperation with financial clients

Protect the related risks, combat money laundering, and maintain financial stability. The opposition in South Africa also echoed the enactment of laws to protect consumers.

For example: the application of the diamond block chain can completely reform the tax model. Such a system leverages taxes as transactions take place, shifting from the traditional post-trade tax to real-time tax.

5.VAC was born

As the development of hundreds of years of history of the diamond industry is how to apply blockchain this new technology to help the development of the industry?

First of all, let us first look at the diamond industry chain, diamonds from the rough mining and trading, diamond cutting, wholesale and retail diamonds, jewelry processing and circulation to consumers, which also need to issue a certificate through the diamond identification, cross-border transactions Customs declaration import and export, foreign exchange settlement and other links, can be described as uncomplicated, and because of the different national conditions in the world, so the rules and regulations in the transaction process is not the same, there are also many different issues, especially the diamond certificate card phenomenon, an endless stream Therefore, the application of blockchain tracing back to diamonds, self-evidence innocent become more and more important, consumers understand their purchase of diamonds and some later service operations can get better service through the blockchain technology;

Second, the system of documenting the movement of diamonds from mines to jewelry stores helps companies trace the origins of diamonds and various transactions of cut diamonds, using a variety of blockchain tools including Distributed books. The blockchain creates a record that can never be tampered with, is ideal for tracking the origin of diamonds and other goods, and the seller wants to know the source of the goods and the owner's information.

The project sponsors include De Beers and several multinational banks such as ABSA, Investec and Nedbank in South Africa. In support of the project, the South African Central Bank (South African Reserve Bank), South Africa's Financial Services Board and the Johannesburg Securities Trading settlement firm Strate and other relevant agencies will provide corresponding support. Among them, the central bank will be mainly responsible for the circulation of smart contracts within the test network. In the meantime, the project will use JPMorgan's blockchain technology for bank clearing services. Will work with Ethereum Technology Development Company to promote the technical verification of the project.

5.1. Fundamentals

As a science and technology innovation project targeting the diamond industry, the VAC team has long focused its efforts on the development of blockchain technology for the global diamond trading platform. It will be the first diamond trading platform in the world to use blockchain technology.

VAC is a platform that uses blockchain to build a global share of the digital ledger to track and protect valuable items. Using machine vision, you record 40 metadata points, creating a unique personality for each gem. Nearly 16 million diamonds will be found on the blockchain. Its technology helps validate the authenticity and origin of diamonds through a single source throughout the supply chain and keep it.

More importantly, each new account must be created by an existing account, and this requirement is required in order for the existing account to pay for the account registration fee. The person who paid the fee is the Registrar. In general, the registrar is likely to be a wallet user. At any time, they have the right to separate the recommended income and an optional referrer.

5.2. Blockchain design ideas

Reduce fraud, reduce costs and improve efficiency, which is the outstanding advantage of blockchain technology. Blockchain technology is widely used,

In order to speed up the "digital credit society," it is bound to trigger changes in the government's management style and social credibility. In our opinion, it is very necessary for the government to participate in the development and regulation of the blockchain, and further research on blockchain technology and continuous practice of blockchain should be encouraged.

5.2.1. Economic Design Ideas

From an economic and social point of view, blockchain economy has been sprouting. Many blockchain-based solutions can improve existing business rules, build new industry collaboration models and increase the efficiency of collaborative distribution. Both central banks and major commercial banks in various countries, as well as the UN, IMF and many government research institutes all pay great attention to the "blockchain +" investment. Blockchain can provide systematic support for economic and social transformation and upgrading. The significant advantages of blockchain + are optimizing business processes, reducing operating costs, and increasing synergy efficiency, which has been initially demonstrated in various sectors of society including financial services, supply chain management, intellectual property, smart manufacturing, social welfare and education and employment.

5.2.2. Technical Design Ideas

Reduce costs, blockchain technology is an important design idea. In the blockchain system, participants can trade "without trust" without having to know each other's basic information, and change the traditional third-party-centered trust model.

The basis of value interaction is the establishment of mutual trust. The revolution of blockchain technology lies in that it realizes a brand new way of trust. Through the design innovation at the technical level, the trust relationship between people in the process of value exchange can be transformed into the trust of people and technology, even by the process automation Some aspects of the implementation, business activities to achieve lower costs.

5.3. Blockchain core technology

The blockchain Blockchain technology principle is the underlying technology for Bitcoin digital currency, used to track the financial transactions of banks and exchanges. Companies such as NASDAQ, TSF, JPMorgan and Bank of America are experimenting with blockchains. Only a small number of companies, including Toyota Motor Corp., use blockchain technology to monitor their supply chains. A blockchain is a data structure that makes it possible to create and share trading digital books. Blockchain uses encryption to empower everyone to add to their books in a safe manner, without going through central agencies. Once the data block is recorded in the blockchain ledger, the data record can not be tampered with or removed.

5.4. Trends

VAC's diamond blockchain will be open to the entire physical sector, providing the tracking and monitoring of every single diamond, which is by far the first blockchain innovation to cover the industry's entire value chain. Blockchain can also help banks dispel funding concerns and improve the efficiency and transparency of the mining supply chain.

When the entire platform is completely completed, it will operate as an open source platform and as a basis for developing related cloud platforms.

5.5. Running into the economic era of blockchain

We have noticed that blockchain technology has shown an unfolding development in various parts of the world. From a business point of view, with the help of the security features and trust mechanisms of the blockchain, it will become an important technology engine for the development of the digital economy and play a role in many industries. The development potential in the field of industrial applications is huge.

However, from the system requirements point of view, to build applications on the blockchain, blockchain solutions need to have a strong three underlying capabilities: First, the perfect old and new system compatibility / switching capabilities, and second, the new system security capabilities Third, the user privacy protection for multi-scene.

6, diamond block chain (Consortium Blockchain) and multi-level traceability system

Diamond blockchain enables visual service delivery and visual service metrics. In service delivery, from the code compilation, testing, grayscale acceptance of the environment to the formal deployment of the environment, the entire service delivery process to achieve visual management. In terms of service metrics, the data is standardized and categorized into categories, collecting various indicators from infrastructure, upper layer components, application services, user side, and application-based topologies to a unified analysis platform.

The diamond blockchain provides common and efficient information collection components deployed in the business layer, consensus node layer and account storage layer. The information collection component integrates the system information (such as CPU, memory, hard disk and network) of the machine, the node usage status (Such as node traffic, access time consumption, health status of nodes, etc.) as well as business usage (traffic, success rate, time-consuming distribution, etc.) are displayed in real time to the monitoring interface for the management of the entire system.

6.1. Why use diamond blockchain

Block chain all commissioned account operations will be recorded independently in the blockchain, and commissioned the operation of the account there are strict frequency limits and independent risk control strategy, you can strictly control the operational risk entrusted to the account.

6.2. What is a multi-level retrospective system?

The user information in the blockchain and the blockchain address are isolated. From each node's record store, the associated user information can not be obtained. User information stored permissions control, access authentication, encrypted storage and other multi-layer protection. Users with higher degree of confidentiality of transactions can also choose to trade unrelated mechanism, every transaction of the same user is mapped to different addresses in the blockchain, so as to ensure that multiple users can not be obtained from the transaction account Transactional relevance

6.3. How to build multi-level traceability system with diamond block chain

At the public service level, blockchain technology is exploring applications in such areas as public administration, social security, intellectual property management and protection, and land ownership management. Relevant practices show that this technology helps to increase public participation, reduce social operating costs and improve the quality and efficiency of social management, which plays an important role in promoting social management and improvement of governance.

Diamond blockchain will be the cornerstone of building digital credit. If used for charity donations, each sum will be recorded on the blockchain, there is no room for malpractices. If it is used for anti-counterfeiting and counterfeiting, every product can be traced and related transactions are recorded, thus eliminating the space for fraud and safeguarding market justice. If a business or an organization, it will be used for salary distribution, then all walks of life or there will be no labor disputes.

7. Based on the diamond blockchain source form

7.1. How form data is stored and transmitted based on blockchain

Node self-checking: The diamond blockchain uses blockchain structure to store data records, some of which will destroy the integrity of the blockchain structure and can be quickly verified and restored from other nodes. In addition, each of the diamond blockchain has its own private key, each block header contains the private key of the node's signature, the data within the block can be modified by signature verification.

Multi-node real-time data verification: When the private key of a node is stolen and the malicious user has the possibility of modifying all the data in the account book chain, the diamond blockchain provides the quasi-real-time data comparison mechanism among multiple nodes and can Timely find a node accounting data has been tampered with.

7.2. Key Industries in Economic Development of Diamond Block Chains

Whether in the financial, IoT, or public service segments, the diamond blockchain is committed to delivering an organization-wide blockchain infrastructure, industry solutions, and secure, reliable, and flexible blockchain cloud services.

Through high-performance blockchain services, we can effectively reduce the overall operating costs and improve operational efficiency through the use of visual data management tools under the premise of secure and reliable transaction docking.

8, application service layer (Trust Application)

The application service layer provides diamond blockchain-based applications to end-users, and will use blockchain solutions to provide various scenarios for mass users. In the future, digital services such as bill of lading, precious metal trading, intellectual property protection, , Institutions clearing, public welfare and other scenes to provide users with reliable, safe and convenient blockchain services.

Diamond Blockchain will also work with various industry partners to explore more blockchain scenarios and open up the capabilities of Trust SQL and Trust Platform in the principle of open sharing. New application services, along with maintaining the ecology of the blockchain.

8.1. Basic Services

The underlying service is deployed on all nodes of the blockchain to verify the validity of the service request and record the valid request on the storage after consensus has been reached. For a new service request, the basic service first parses the interface adaptation. The authentication process then stores the transaction or contract with the signature and the encryption by a consensus algorithm, and stores the same in the shared account completely and consistently.

8.2. User Management

Responsible for the management of identity information of all blockchain participants, including the maintenance of public and private key generation, keystore management, and maintenance of user real identity and blockchain address correspondence, and in the case of authorization, supervising and auditing certain real identities The transaction situation. The application of financial transactions such as digital assets also provides the rules of risk control configuration to ensure the security of system transactions.

Generally speaking, the blockchain can be regarded as a set of multi-participatory and reliable distributed data storage system. Its uniqueness lies in the following aspects: First, multiple parties involved in the recording act, that is, all parties can participate in the recording; secondly, the data The multi-parties involved in the storage and common maintenance, that is, all parties involved in the storage and maintenance of data; Third, through the chain of data storage and contract, and can only read and write, can not be tampered with.

8.3. Smart contracts

Responsible for the registration of the contract and the triggering and execution of the contract. After the user defines the contract and logic in a programming language, the logic of the contract is released to the blockchain, and the logic of the contract clause triggers the execution of the contract by the user's signature or other events to complete the contract settlement transaction.

Many blockchain are integrating a common scripting language to define all the operations. These designs eventually define the business logic processor as a virtual machine, and all transactions are defined as scripts run by this virtual machine. The solution has a single-threaded performance limit on real processors, and the problem gets worse by forcing everything through a virtual processor to execute. A virtual processor will always be slower than a real processor, even if it's implemented (JIT), but computing speed is not the only issue with this "everything is a scripting" solution.

When the transaction is defined at such a low level, static inspection and encryption algorithm operations are still included in the business logic processing, which also allows the overall throughput will be reduced. A scripting engine should never require that a request be made for a cryptographic algorithm signature check, even if the request is made through a native mechanism.

8.4. Operation Monitoring

Responsible for product deployment process deployment, configuration changes, contract settings and real-time product running status, visual output, such as: alarm, transaction volume, network status, node health status.

The state data collected in the system is collected and visualized. Status data in the system includes the system traffic, time-consuming, health status of the node and the use of the underlying machine resources (CPU, memory, hard disk), etc. Through the visual monitoring can be real-time understanding of the status of the entire blockchain system.

8.5. Custom Assets and Identity Management

For example, the NYSE as a company whose primary function is to maintain a ledger that contains information about the company's issued shares or bondholders. Its main profitability is the transaction costs, as well as its own stock and so on. Similar to the New York Stock Exchange, diamond blockchains allow people to issue their own stocks or bonds in the system and can trade in a distributed ledger. Diamond blockchain can mark each account in the system to ensure correspondence. This trust network allows issuers to empower others to ensure compliance with the securities restrictions.

The VAC decentralized platform offers a feature called "user-assets (UIA)" designed to help drive the consolidation of profitable business models for some services into the platform. Is essentially a credential registered on the platform that can be traded on the platform while complying with certain requirements. The creator of the voucher can set the public name, description and other information, and issue it according to his own wishes. The publisher can customize certain UA features: for example, it may require that only users in the whitelist be allowed to hold the voucher, or that the user be required to pay a fee when transferring or trading the voucher.

Digital currency exchanges and remittance agencies can issue their own gateway assets (UA) so that capital can be accessed at VAC.

Businesses can issue their own company shares directly on VAC's blockchain, and these UAs can be set to fully comply with existing regulatory and related legal provisions.

UA can also be used as a voucher, coupon, third-party currency, credit, product receipt, crowdfunding, warranty certificate, and more.

8.6. Decentralized transactions

VAC offers a highly-performance, decentralized trading platform that provides everything you would expect from a trading platform. Not only will the execution of an order be completed at the moment you submit it, but it also provides secured bonds that allow you to leverage and provide interest, and the option contract will allow you to hedge your position.

Decentralization enables the original carrier to maintain its integrity after being subjected to various signal processing procedures or to be able to identify accurately without losing the secret information after handling the attack. When a centralized exchange is compromised for millions of dollars, it can affect thousands of users instantaneously, and a decentralized system compromised or compromised affects only a single user and his money. Users can control their own security, which can actually be far better than any centralized entity.

In fact, there is a fixed cost of diamond blockchain in trying to crack an exchange or a single user. The difference is in the size of the benefits that can be gained. If you spend millions of dollars on attacking a particular goal, then you're sure to expect so much energy on an exchange instead of your single personal account.

Many people have access to money in a given company. You may listen

As the saying goes, "Three people could not keep the secret, unless the other two are not alive." Most exchanges want to control the funds through multiple individuals responsible for protecting the private keys. And if any one of them has a problem, everyone's money can be dangerous. In this respect, in fact, it may be more secure for each individual to be solely responsible for guarding his or her own password.

8.7. Business Logic Processor

All transactions in the cryptocurrency network rely on signing with an encryption algorithm to verify permissions. In most cases, the requested permissions can be changed by the result of other transactions. This means that in the business logic processor, permissions need to be defined to be irrelevant to the computation of the encryption algorithm.

To achieve this goal, all public keys need to be assigned a unique and irreplaceable ID. When the ID is assigned, the input splitter can verify that the provided signature matches the specified ID. When the transaction arrives at the business logic processor, only need to check the ID on it.

This same technique can be used to remove precondition checking on objects that have irreplaceable static IDs.

8.8. Designing Transactions for Static Verification

For transactions, there are many features that can be checked statically without the need to refer to the current global state. These checks include checking the range of parameters, input de-redundancy and array sorting. In general, there are many checks that can be made if the transaction contains data that it "assumes" to be in a global state. After these checks have been performed, the business logic processor has to do only to make sure that the assumptions are correct, and the process is summed up by checking the modification timestamp of an object reference involving the transaction signature time.

8.9. Object Data Schema

One of the benefits of having everything stored in memory is that the software can be designed to mimic the relationships in the real world. This means that business logic processors can quickly find data from pointers in memory instead of being forced to do expensive database queries. This means that the data can be accessed without copying, and can be modified on the spot. This optimization provides an order of magnitude performance over any database-based solution.

9. Platform product service layer

Platform product service layer abstracts all kinds of typical blockchain applications and provides the basic capabilities and implementation framework of typical applications. Based on these basic capabilities, users can easily implement the business logic blockchain by stacking the unique features of their services. It helps users quickly relocate existing services to the blockchain in order to cope with the new scenarios or set up entirely new business scenarios. It uses previously unmanageable and non-repudiating blockchain features to solve previously difficult problems.

Consensus mechanisms can be adaptive, with high concurrency under normal network and node conditions, and with strong fault tolerance in the case of network anomalies or node spoofing.

9.1. Digital Assets: Based on the analysis of digital assets such as virtual currency, valuables and commercial paper, we found that asset chain is a key link. To this end, the concept of "asset gateway" is introduced to assist users in transferring assets from the chain to the chain. Once the assets on the chain,

Transfer, split, withdrawals and other operations will be strictly controlled by public and private key account system, and all operations will have a signature verification, both parties will leave traces, can not be erased. Such as commercial paper, card coupons such as the existence of the existence of the assets, but also provide the ability to automatically expire due, including asset issuance, transfer of assets, asset withdrawals, asset liquidation, asset inquiries.

9.2. Assurance Services: For the application scenarios of intellectual property, policy preservation (proof of entitlement), product and enterprise qualification certificates, the blockchain gives full play to the capabilities that can not be erased and publicized so that institutions and individuals can use a simple interface or client Copyright information, insurance information, qualification certificates, etc. can be posted to the blockchain so that all accounting nodes can jointly testify for themselves. In addition, based on VAC's own intellectual property platform, users' rights protection will be more convenient and the evidence will be more authoritative. Such as ownership registration, ownership cancellation, infringement evidence entry.

9.3. Shared books: The reconciliation between financial institutions is basically conducted in a day-to-day cycle. The reconciliation method is basically an interactive statement, comparing the transaction flow between the two parties. This will bring a certain delay to the final confirmation of transaction and transfer of funds. Some business scenarios that require real-time payment must even be funded by business operators. Blockchain natural shared book, so the reconciliation do not have to send the next day summary, but can be carried out at any time, as long as the reconciliation logic of the two sides docking on the blockchain, you can complete the funds check. The basic can be realized in real-time transaction confirmation and transfer of funds, and either can not be denied. Especially for the funding chain is relatively long, involving more aspects of the business is very competitive. At the same time regulators can also participate in the shared book records.

9.4. Sharing Economy: Through the BRICS meeting, we fully learn some advanced ideas in China, such as sharing economy. A key factor in sharing the long-term viability of the economy is the establishment of trust between supply and demand parties to ensure the smooth implementation of sharing activities, and the blockchain provides a way of achieving it from a technical perspective. Endorsed by technical assurance capabilities, allowing multiple stakeholders who are hard-won to reach one another to work together to build credibility and eliminate the need for an intermediary or service platform to build strong internal audit processes, rigorous accounting and backup systems, and regulatory compliance Additional facilities, you can achieve the same effect. Thus saving a lot of cost, make sharing more efficient and feasible.

10. Technical Features and Benefits

"This diamond traceability platform was developed on the basis of blockchain technology and utilizes a highly secure digital register that creates tamper-evident, permanent records of transactions - in which case the diamond can travel through the entire value chain "Said Bruce Cleaver, chief executive of De Beers.

A blockchain is a global book that issues a global transaction about determining to modify a share. The orders included in these deals can change the validity of other transactions. For example, you can not withdraw money from your bank account before your check deposit takes effect. You can not know whether a transaction is valid until all previous transactions that affect a particular account have been processed.

10.1. Resolver Technology

The resolver provides a learning example of what can be achieved on a single thread and is a trading platform for end-users that aims to be the fastest trading platform in the world.

The Business Logic Processor is where all sequential transactions and order matching happen. It's a single thread that can process millions of orders per second. This architecture can easily be used in the area of ​​crypto-currency and blockchain design.

The role of the input splitter is to gather orders from many users from different sources and then assign them to a certain order. When assigned to them in good order, they will be copied, recorded and then broadcast to many redundant business logic processors. The input splitter is highly parallel and easily subcontracted to a computer cluster system.

After the input is processed by the business logic processor, an output resolver is responsible for notifying those interested in the result. This is also a highly parallel task.

Ultimately, VAC can execute 6 million transactions per second by using single-threaded sample processors and Java virtual machines in the business logic processor. If this achievement is successfully achieved, then the cryptocurrency and smart contract platform do not need to consider the clustered networking solution without even having 10 transactions per second.

10.2. Technical advantages

10.2.1. High Performance

Designing a high-performance blockchain is not a rocket science and does not require complicated protocols or the need to process tasks across all nodes on the network. Instead, the most needed thing to do to build a high-performance blockchain should be to remove the computationally-critical computational tasks that are not related to criticality, order dependencies, and assessments in the core business logic and devise a protocol that helps to optimize those things. This is what the bit stock has done.

There are a few things that must be done to build a high-performance blockchain:

Put everything in memory, avoiding synchronization primitives (locking, atomic operations) and avoiding unnecessary calculations on the business logic processor.

As memory design is highly parallel, it is getting cheaper. The amount of data needed to track account balances and permissions for everyone on the Internet can be on less than 1TB of RAM memory and can be mounted on a commercial (high-end) server board. Before this system was adopted by 3 billion people, such hardware would be seen in ordinary desktop computers.

The real bottleneck is not the demand for memory capacity, but the bandwidth requirements. At 1 million transactions per second and 256 bytes per transaction, the network will require 256MB of data per second, or 1Gbit / s of bandwidth. This bandwidth is not common on average desktop computers. However, this bandwidth is only a little bit of the 100Gbit / s bandwidth of the second generation Internet.

In other words, blockchain technology makes it easy to keep everything in memory and, if properly designed, can scale to support millions of transfers per second.

10.2.2. High-speed access

South Africa's second-largest supermarket chain, Pick n Pay, founded in 1967, has branches throughout Africa. Known as the "largest retailer in the world to open this precedent" - consumers can shop in digital currency at Pick n Pay Retail in Cape Town, South Africa.

In a single-threaded system, processor cycles are scarce resources that need to be preserved. The traditional blockchain design uses the hash calculation based on the encryption algorithm to generate a globally unique ID system so as to ensure that there is no statistical collision. The problem with doing this hashes is that it consumes more and more memory and processor cycles. Compared to a direct array index, this approach significantly consumes more processor time to find an account's records. For example, 64-bit integer comparisons and operations are easier than IDs above 160. A larger hash ID mechanism means less CPU cache space and more memory. RAM, which is infrequently accessed in modern operating systems, is compressed, but the hash identifier is a random number that can not be compressed.

The diamond blockchain gives us a way to assign unique IDs globally that do not conflict with each other and thus completely avoid using an identifier based on a hashing algorithm like a Bitcoin address to reference an account , Balance or permission.

In order to provide the industry with a solution that may replace existing financial platforms, high-performance blockchain technology is necessary for cryptocurrencies and smart contract platforms. In order to be able to achieve higher levels of transactions per second than VISA and MasterCard together, VAC redesigns from the ground up. Through the proof of stock authorization, Diamond Chain Network can confirm the transaction in an average of one second, the only limit is the speed of light.

With the VAC's trading speed in a few seconds can be implemented, this has been and the centralized web interface almost. Unlike centralized exchanges, they can set priority orders or hide orders in high-frequency deals, placing all traders in a level playing field.

10.2.3. Security

The dollar, the euro, diamonds, and gold all have three times the asset support of the traditional centric exchange in the BitShares exchange. Those traditional banking systems should in fact be called the "fictitious reserve banking system" and often referred to as the "partial reserve banking system." In the digital currency ecosystem, we often demand that at least 100% of the reserves be provided. Even though these exchanges can do it, once a hacker, a mistake, or a theft can easily turn the 100% reserve system into a fictitious reserve system or, worse, sometimes become "unready system". In the absence of any reserves, it is impossible for these exchanges to give you your money back.

By always keeping at least 200% of your reserves, you can be assured that VAC will be solvent in any market. All reserves are safely stored on the blockchain so that they will never be stolen because no one can get the private key to steal these reserves.

10.2.4. Without limitation

You can trade any amount at any time, from anywhere, and there are no cash limits. All other legally compliant exchanges have daily withdrawal limits of the order of a few thousand dollars. If you want to go beyond these limits, you have to provide a lot of documentation to upgrade your level. Some exchanges even limit what your money can only be used for later. There are other exchanges that require you to provide documentation to prove how you got these digital currencies.

With the advent of VAC, your account will no longer require anyone's approval and you will have full financial freedom.

10.2.5. Low rates

With just a few cents per trade, VAC is certainly the lowest-cost exchange in the world. Other exchanges charge a percentage of your trading volume. VAC is cheaper than a more traditional exchange.

10.2.6. Efficient operation

It provides comprehensive, real-time and visual operation and maintenance management system to rapidly identify the system status and support various deployment methods such as cloud deployment and server deployment according to different user needs to meet various needs.

It should be noted that the performance achieved by the diamond chain is highly dependent on one of the compatible trading protocols. It would not be possible to achieve the same level of performance if you wanted to run your business logic on a virtual machine that performs cryptographic algorithms and calls all objects with recognizers. Blockchain is inherently single-threaded, and single-core CPU performance is the shortest of all kinds of resources, the most difficult aspect of expansion. VAC is designed to make this single-threaded execution extremely efficient.

Here you can trade diamonds, gold, silver, gas and oil, as well as your favorite national and digital currencies, with virtually no restrictions on VAC exchanges. Supporting assets include stocks, bonds, indices or Inflation. Companies can issue their own shares on the block network, not only for convenience and low cost, but also for the protection of transactions to prevent naked short selling.

10.2.7. Privacy

You can be able to protect your privacy by using VAC. Like Bitcoin, all transactions are completely public but do not need to be bound to your real identity. No IRS documentation, no one will require a copy of your passport, driver's license, utilities and credit reports.

10.2.8. Open source and fully transparent

The entire exchange is open source and supported by a very open community. Nothing else will give you the level of transparency you can find with VAC.

Another advantage of this diamond blockchain is the use of system transparency to drive tax compliance. That is, smart contracts can be used to collect taxes in real time.

10.2.9. Scalability

If two unrelated accounts do not share any common dependencies, the theory

The transactions on these two accounts can be processed at the same time. In fact, it can be tricky to identify which transactions are truly separate from one driven by a smart contract driven arbitration. The only way to ensure that the two deals are truly separate is by maintaining a completely separate ledger and then periodically transferring the value between them. If you want to use this performance trade-offs like the relationship between non-uniform memory access (NUMA) and uniform memory access architecture (UMA).

In fact, a consistent memory access architecture is easier for developers to design and consume less. Non-uniform memory access architectures are often used as a last resort when building supercomputers and mainframe clusters.

11. Diamond chain profit model

There are many innovations in this design pattern, two of which are worth noting:

First, trading trust is determined by machines and algorithms. Blockchain solves mutual trust issues in anonymous trading by building a trading system that relies on machine and algorithmic trust. All participants will establish their identity through the principles of cryptography in an environment without the establishment of trust relations and rely on consensus mechanisms to achieve mutual trust.

Second, the transaction process can be executed automatically by the program. The blockchain, through programmable smart contracts, automatically enforces the contracts reached by both parties and eliminates human interference and systematically prevents repudiation by either party. Thus pushing economic and social into an intelligent state and achieving a qualitative leap in the current economic exchange system.

Mode upgrade, given the security of the public chain and the increasing volume of transactions on the balance between the capacity of the current network, the future application of the block chain will be based on the coalition chain, private chain or hybrid. The Bitcoin model adds to the maintenance costs of blockchain networks and is not entirely suitable for low value, low risk transactions. Considering the efficiency and safety improvement, the future will consist of a diamond chain, a private chain or a hybrid chain of diamond chains and private chains.

11.1. Business progress

Diamonds are a valuable accessory for people. VAC hopes to use tracking platforms to re-establish consumers' trust in the diamond sales process and adopt blockchain technology while reducing fears of money laundering involving diamonds and clashes with diamond trafficking.

There are many start-ups in the diamond industry, and even many international agencies, including the United Nations, are trying to use blockchain technology. If the application of blockchain in diamond trading, whether it is data tracking, or the source of diamonds, is to give a full guarantee of consumer, there is a lot of convincing.

11.2. Product Development Progress

De Beers De Beers CEO Bruce Cleaver, speaking about the blockchain, said: "It's a huge, immutable public ledger, a system that's harder to crack than any single server."

In the actual business docking scene can be divided into three categories: The first category, after the original system transformation

Access to blockchain, the second category, the new demand on the original system using blockchain development, the third category, the use of blockchain in new systems and scenarios. A variety of user deployment environment.

The computer industry has come to realize that scaling performance through parallel computing is not as easy as it was in the early days, after all, the most needed thing to do at that time was simply to raise the processor's frequency. It is for this reason that processor designers are desperately trying to improve single-threaded performance until they try to go multi-threaded to improve performance. When multithreading is not enough, and if that is the case, the cluster computing solution will be considered.

12. Diamond Chain Market Forecast

Blockchain technology has already begun to deploy applications around the world. Developed countries such as the United States, Britain, Japan, Germany, Canada, and Australia have realized that there is a huge potential for application of blockchain technology in public service and social mechanism optimization. Block chain development path.

Use of blockchain to track diamond sources, including number of applicable institutions, current market coverage and growth rate, market capacity,

Issues like overuse of energy when utilizing Bitcoin's blockchain will not affect other applications as new technologies are more energy-efficient.

 13. Tokens, and chain-based services

13.1. Development and distribution of tokens

Diamond Chain issues the appropriate token for the better decentralization and commercial use of the diamond chain. Diamond chain of coins in English code: VAC, a total volume of 69 million constant, the first issue of 8.5 million, is based on the credit chain to the decentralized digital currency.

It is responsible for handling the configuration of network nodes, such as the selection of consensus algorithms, adaptive thresholds, storage of stored books, and routing of networks. The configuration itself can be delivered as a transaction in the blockchain and can be reached through the consensus algorithm Re-effective after the agreement.

13.2. Chain-based services

Under the principle of "independent innovation, safe and efficient, open sharing", the overall framework of the VAC Diamond Blockchain Solution is divided into three levels: the bottom of the diamond blockchain is the trust SQl platform independently developed by VAC, the Trust SQL is managed by SQL And API interface for the upper application of blockchain basic services. The core position is to build a leading infrastructure-level blockchain-based platform. In the middle is the platform product service layer for the Trust Platform, built on top of the Trust (SQL) based on high availability, scalability blockchain application platform products, including shared books, authentication services, shared economy, digital assets, etc. Direction, integration of related products in the field of basic functions to help organizations quickly set up the upper block chain application scenarios.

13.3 Trading

VAC system built a transactional abstraction layer, almost all of the core system functions are based on the transaction, such as transfer, voting, application store, recharge, withdrawals and so on. Sub-chain itself can also achieve their own different types of transactions. The main difference between transactions is the transaction type and asset. The basic transaction data structure is as follows, the expansion part will be based on the type of different exist in different asset table.

Transaction {

required VARCHAR (20) id;

required VARCHAR (20) blockId;

required TINYINT type;

required INT timestamp;

required VARCHAR (21) senderId;

optional VARCHAR (21) recpientId;

required BIGINT amount;

required BIGINT fee;

required BINARY (64) signature;

optional BINARY (64) signSignature;

optional TEXT signatures;

required BINARY (32) senderPublicKey;

13.4 Account System

Each VAC account consists of a password, a pair of public and private keys, and an address. Users can also set a second level password. Note that there is a bit different with Bitcoin, each

Each account corresponds to only one address, and each wallet in Bitcoin has multiple addresses and private keys.

Passphrase is a BIP39-compliant mnemonic used to generate deterministic wallets. This mnemonic is more friendly to human memory than binary or hexadecimal characters. The password is generated by converting the entropy of a multiple of 64 bits to a number of words. The entropy length selected by the VAC system is 128 bits and is converted into 12 words. Password as a password, the custody of the user, not open to the public, once lost, users will lose the corresponding account ownership. The password is as follows:

barely decline dust stamp protect color certain cup arena busy latin shell

The key pair, including the public key and the private key, is generated using the sha256 hash of the password and then ed25519 edwards curve signature algorithm. The form is as follows:

Public key:

9989388b220a13465e49f52df5ba28ba08eb1e7a973320347f9687a107dc2f 9a

Private key:

91e891f653e3ed0232d8c7de2e72b625d50d48593fc0fb570c0db25c5e4456 9a9989388b220a13465e49f52df5ba28ba08eb1e7a973320347f9687a107dc 2f9a

Account address is to take the first two sha256 hash of the public key, converted to bignumber in reverse order, the form is as follows:

5034187504202890358

The key pair, including the public key and the private key, is based on the sha256 hash of the password, and then ed25519 Edwards

Account address is to take the public key sha256 hash the first 8, after the reverse conversion bignumber,

14. Risk control audit

The risk control module is responsible for the risk control of the transaction of digital asset classes in the blockchain. The Tencent blockchain provides the risk control expert model system. By analyzing and capturing the deep relationship between the massive data, adaptive regulation of wind control can be found in time Risk management risk control and risk control, so take preventive measures. The audit module provides the auditing agency with auditing capability and ensures that auditing capability can only be used by the auditing agency through strict authority control.

The blockchain contract includes two types, standard contract and business custom contract. Standard contracts include a one-time check of assets, automatic transaction matching, multi-joint confirmation of the transfer, expiration, and other relatively simple logical contract liquidation, the blockchain built-in contract, you can hang directly on the blockchain. Custom smart contracts include modifying configuration and adding additional business logic through contract templates, as well as supporting more complex, user-programmed contracts that run in a standalone environment.

15. Why we can do it well

De Beers De Beers, the world's largest gemstone producer, has led the industry in verifying the authenticity of diamonds, while ensuring they do not come from areas of conflict that could be used to fund violent conflicts.

The blockchain, which is the underlying technology of digital currencies, provides a secure way to track the origin of diamonds and provide digital records that show that diamonds have no conflicts.

From an economic point of view, the creation of a new value interactive diamond blockchain is based on decentralized books, but this does not mean the complete disappearance of various "centers" in the traditional society, and the massive blockchain will appear in the future Of the "multi-center" system, dominated by the public chain, the private chain or the hybrid chain, the block chain will further improve the operational efficiency of "each center" and reduce a considerable part of its costs.

From a technical point of view, we believe that the diamond blockchain is a technology that is jointly maintained by many parties, stores data in a blockchain structure, uses cryptography to ensure transmission and access security, enables consistent data storage, and can not be tampered with and can not deny system. This technology has brought unlimited reverie space to the world. The global attention to the block chain continues to heat up. The major global economies begin to study the technology and development trend of the blockchain from the national strategic level.

16. Problems and Solutions

Just as any technological revolution will bring about some new problems, the challenge in the development of the blockchain is how to establish a regulatory environment that can promote the application of the technology. If we apply the traditional regulatory model, we will greatly curb innovation and will not be able to play Its potential. Therefore, there is an urgent need for the government's management philosophy to shift from "supervision" to "governance". The tone should be to encourage innovation while keeping the bottom line.

In order to effectively promote the technology and application development of blockchain in South Africa and nurture the formation of a globally competitive blockchain industry, the following suggestions are made: The immature blockchain technology faces the challenges of algorithm security, protocol Security, usage security, security and system security, it is necessary to strengthen the security research on encryption technology, key storage, privacy protection and technology implementation, and strive to improve the overall security and reliability of blockchain technology.

First, to encourage the key key technology research to form an independent innovation system

We will encourage key domestic enterprises, research institutes and universities to step up cooperation so as to speed up tackling key core technologies such as consensus mechanism, programmable contract, distributed storage and digital signature, and strive to form technological achievements with independent property rights so as to create a product more in line with national security requirements Fully autonomous control of the block chain platform for the development of many applications and landing escort.

Second, to promote the formation of a good environment for the development of blockchain applications

Faced with the disruptive technologies such as the blockchain, these challenges will eventually be tackled despite their challenges in terms of personal privacy and consumer protection, ethics and social impact, as the Internet is a good precedent. Therefore, the relevant departments are advised to strengthen communication and coordination and gather resources from industries, universities, research institutes and other sources to closely follow the trends in the international industrial development. Through various forms of work, they will jointly promote relevant research in the blockchain, technology research and development, application and popularization, optimize the blockchain Technology industry development environment, and strive to obtain a new round of industrial competition opportunities.

Third, the introduction of policies to support the development of blockchain technologies and applications

Draw lessons from the advanced practices of developed countries and regions and combine the development of blockchain technologies and applications in China with the timely introduction of related supportive policies, focusing on key key technological breakthroughs, industrial application solution research and development, major application demonstration projects, and public service platform construction. At the same time, relax restrictions on market access, strengthen supervision after events and optimize service levels.

Fourth, accelerate the construction of the standard system in the area of ​​blockchain

Focusing on the key aspects of industrial development, we accelerated the deployment and formulation of key and urgently needed standards and gradually improved the blockchain technology and application standard system. Actively participate in the development of international standards, docking international standards bodies and open source community organizations, strengthen international exchanges and cooperation in

While contributing actively, we should continuously improve the international voice in China's standard work.

Fifth, accelerate the application of blockchain technology

It is suggested that the application solution of blockchain industry should be researched and put forward based on the typical application needs of such industries as finance, culture, medical care, education, internet of things and supply chain. Facing the industries with good basic conditions and strong demonstration effect, the Bank explored the pilot demonstration of the application of block chains, and promoted the integration and development of blockchain technology and industry applications. Encourage and support domestic enterprises to actively participate in the open source community in the international blockchain chain and contribute to enhancing their influence and voice. Encourage learning from the construction and operation mode of international open source communities, strengthen the cooperation among domestic enterprises, and build an open source community in blockchains in China. Exchanges and cooperation should be carried out based on key key technology research and development, major application demonstration and standard formulation. .

17. Leading the future

Imagine if there is an exchange risk that exposes you to privacy when buying and selling digital assets without any exposure to the other. Imagine if an exchange can offer a very low transaction fee without any recharging and cash withdrawal limits. Imagine you can use any currency in the transaction, even gold and silver. Imagine being able to provide the best liquidity in the market. This is VAC, the best decentralized trading platform in the digital asset industry.

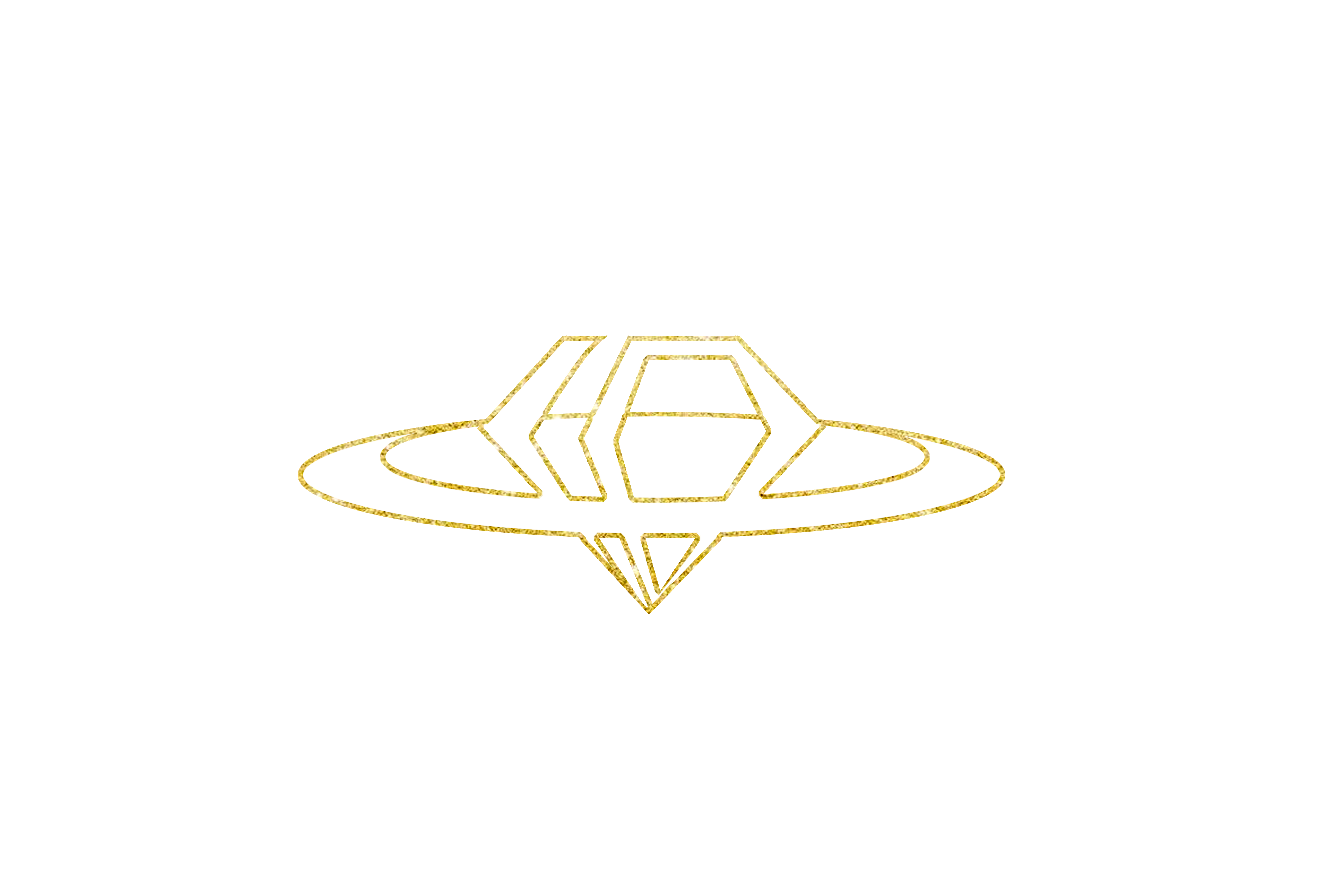
VAC aims to explore new ways in the financial technology sector such as cryptocurrencies in South Africa in order to better cope with the emerging financial technology issues in the financial sector. It will greatly enhance the viability of the economy, reduce systemic risk and promote the ability to more effectively deliver monetary policy throughout the economy.

According to the 2018 budget report released by the Ministry of Finance, the economy of South Africa is expected to grow by 1% in 2017, 1.5% in 2018 and 2.1% in 2020. can

Imagine, we are working with some of the world's top technology companies for exchanges and cooperation, but also to contribute to South Africa's economic development.

As the first diamond blockchain spanning the entire value chain, it is clear that with VAC's innovations and strengths, we have been able to meet the future of VAC.

**南非钻石区块链VAC方案白皮书**

****

**VAC：打造数字经济时代的流通基石**

——全球首个覆盖行业全价值链的区块链创新技术

**目录**

前言

1.区块链的兴起和未来之路

1.1.我们要切入的钻石经济发展领域是什么

1.2.钻石经济系统是什么样的

1.3.钻石经济的特点是怎样的

2.传统贸易已不能满足全球信息化的需求

2.1.缺乏先进的源头追溯记录体系

2.2.缺乏相应的服务提供商

2.3.数据传输存在较大问题

3.区块链的应用机会

3.1.用数字密码学来建立信任关系

3.2.政策利好的风口

4.我们要做什么

4.1.建立区块链电子简历

4.2.打造基于三种区块链形式的混合跨链服务

4.2.1.基于公有链的个人应用服务

4.2.2.基于联盟区块链的多级追溯体系和应用

4.2.3.钻石区块链为基础的信息化

5.VAC的诞生

5.1.基本原理

5.2.区块链的设计思想

5.3.区块链的核心技术

5.4.发展趋势

5.5.跑步进入区块链经济时代

6、钻石区块链（Consortium Blockchain）与多级追溯体系

6.1.为什么用钻石区块链

6.2.什么是多级追溯体系

6.3.如何用钻石区块链打造多级追溯体系

7.基于钻石区块链的源头表单

7.1.表单数据如何基于区块链保存和传输

7.2.钻石区块链经济发展的重点行业

8、应用服务层（Trust Application）

8.1.基础服务

8.2.用户管理

8.3.智能合约

8.4.运营监控

8.5.自定义资产和身份管理

8.6.去中心化交易

8.7.业务逻辑处理器

8.8.为静态校验设计交易

8.9.对象数据模式

9.平台产品服务层

9.1.数字资产

9.2.鉴证服务

9.3.共享账本

9.4.分享经济

10.技术特色和优势

10.1.分解器技术

10.2.技术优势

10.2.1.高性能

10.2.2.高速接入

10.2.3.安全性

10.2.4.无局限

10.2.5.费率低

10.2.6.高效运营

10.2.7.隐私

10.2.8.开放源代码和完全透明

10.2.9.可扩展性

11.钻石链的盈利模式

11.1.商务进展

11.2.产品开发进展

12.钻石链市场前景预测

13.代币（Token），以及基于公链的服务

13.1.代币开发及分配方式

13.2.基于公链的服务

13.3交易

13.4账户系统

14.风控审计

15.为什么我们能做好

16.面临的问题及解决方案

17.领导未来

**前言**

2018年，新总统拉马福萨在国情咨文中，重申了他再三强调的核心政策：打击腐败和提振经济。他将降低失业率、杜绝腐败和加强基础设施建设作为新任政府的首要目标，并重点着手于创造就业机会。以“变革者”的形象崛起的拉马福萨总统，承诺进行彻底的经济改革和打击腐败，将重拳突破经济发展停滞、失业严重、金融市场动荡等多重困境。

南非财经、法律、通讯、能源、交通业发达，拥有完备的硬件基础设施和股票交易市场，黄金、钻石生产量均占世界首位，深井采矿等技术居于世界领先地位。钻石以其璀璨夺目的光彩深深地打动着人们的心，一方面作为爱情信物，代表着浪漫的永恒之爱；另外一方面，钻石极具投资价值，是提振经济的重要力量之一。

然而，钻石市场中鱼目混珠，真假难辨，实物钻石的在线交易业务长期以来一直饱受争议。如何保证消费者所购买的钻石既是正品又来路清晰，似乎成了难题。

凭借比特币在南非的使用正在迅速增长的东风，区块链技术被公认为解决这个问题的契机，或将为黄金、钻石等奢侈品行业带来全新的转机。

区块链技术在奢侈品交易中的实际应用项目——VAC钻石风控交易去中心化平台，结合区块链技术为实体行业打造可追溯体系，通过建立一个连接数字货币和法定货币的区块链系统，促使实体产品交易变得更加简单、快速和透明。

纵观全球发达国家，已经加入区块链的“军备大赛”。南非也已将区块链纳入国家发展战略，积极参与全球竞争，致力于成为成为大时代的领导者。

**1.区块链的兴起和未来之路**

2009年之前，世界上存在的三种资产持有方式：实体持有、实体登记和数字化登记。

2009年之后，出现了“加密货币”。这一持有方式既和“实体持有”一样，通过持有人私有的秘钥显示其所有权；又和“实体登记”一样，其价值被记录在总账里。

最著名的认知是加密货币的底层系统就是区块链技术，是保存在互联网计算机网络中的共享交易数据库，

进一步的研究发现，区块链是一种分布式计算技术，在其核心产生一个不可磨灭的、防篡改的分类帐本。它具备一种“降低成本”的强大能力，能简化流程，降低一些不必要的交易成本及制度性成本，不少人认为，这种新型的记录方式可以改变航运、保险和金融等许多社会领域，对于改善当前低迷的经济环境更有现实意义。

在区块链技术的支持下,数字货币币打破了传统纸币的“暗黑”盒子。作为实体的纸币的流通是看不见的，没有人知道一张纸币从哪里来到哪里去，而区块链却可以让数字货币的每一笔动向都清清楚楚有“链”可查，同时还可以保护参与者的隐私。

总而言之，区块链的意义在于可以构建一个更加可靠的互联网系统，从根本上解决价值交换与转移中存在的欺诈和寻租现象。越来越多的人相信，随着区块链技术的普及，数字经济将会更加真实可信，经济社会由此变得更加公正和透明。

**1.1.我们要切入的钻石经济发展领域是什么**

“钻石恒久远，一颗永流传，这是戴比尔公司极其成功的宣传范例，巧妙地把钻石与爱情、忠贞联系起来。钻石给人带来一种视觉上的享受，精神上的愉悦。

除了作为首饰，更多的制造商将钻石视为一种另类投资资产。但由于缺乏统一的标准，过去一直很难实现这一点。像黄金一样，钻石的魅力稀有且长久。但与黄金和其公共基准不同，钻石没有出现价格波动。这是因为，钻石交易往往是在神秘的面纱后面进行的。

目前，我们正在把数字货币当作资本实现来对待。如果你在某个特定的时点买入数字货币，然后再卖出去，你可能会经历资本增值，然后我们会将其视为资本收益。

**1.2.钻石经济系统是什么样的**

从线下到线上，零售商们正在采取行动，以确保钻石的透明度。他们主动追踪其产品从采矿地点到投入市场之间的供应路径。在表面的4C特征（颜色、克拉、清晰度及切割）以外，开创了4Ts标准：可追溯、透明、真实与周到。记录了每一块钻石石从采购到生产的全部过程。（就是我们所说的内部英特尔芯片。垂直整合的零售商从最有信誉的钻石生产商处进行采购，并拥有抛光、切割和分销等中游流程，以及下游销售平台。）

**1.3.钻石经济的特点是怎样的**

由于监控不到位，许多虚构的钻石卖家使得在线钻石交易名声不佳。这一现象在 2008 年金融危机后的资产清算潮中变得尤为严重。

钻石行业一直以来都存在认证机构，即使用光谱分析来识别色彩等级的实验室，但却没有信息的中央数据库。丢失的钻石依赖于纸质认证记录。随着信息存储在区块链上，这就会创建一个聚合数据集、一个共享的可见记录以及一个审计追踪，用来防止双重资金融通或实验室培养的宝石被错误识别等事件的发生。

**2.传统贸易已不能满足全球信息化的需求**

**2.1.缺乏先进的源头追溯记录体系**

非政府组织Global Witness发布的一份调查报告显示，产自中非共和国的血钻交易已经进入了Facebook的线上市场。一名虚构买家在社交媒体网站揭露了这种非法数字活动。该组织发现，即时通讯平台也被当作了将冲突宝石走私到国际供应链的工具。

**2.2.缺乏相应的服务提供商**

无良的经销商会找到投机取巧的买家。即使是合法钻石，也因其幕后现金交易而闻名。因珍贵宝石的而起的问题仍然存在。在保险行业，每年谎称珠宝丢失而进行的欺诈性索赔通常会达到数十亿的资金损失。

由于该行业的风险较大，银行通常会避开钻石类业务。因盈利和合规原因，渣打银行（Standard Chartered Bank）去年也叫停了其钻石业务。诸如钻石之类的异国资产在很大程度上并非商业化的商品，鉴于其性质，反而为洗钱和逃税提供了巨大的优势。

**2.3.数据传输存在较大问题**

为了阻止冲突钻石的流入，联合国早在2000年就作出了一项具有里程碑意义的决定，即“金伯利进程（Kimberley Process）”。同时，还引入了一项三步验证法，其中要求采矿国家对每一颗宝石提供申报单。全球共有75个钻石生产国都遵守了设立进出口管制系统的方案。但是，这项决议只涵盖了反叛组织用来资助反对合法政府而发起的战争的未加工钻石，却并不涉及通常与贸易有关的更广泛的侵犯人权的行为。例如，委内瑞拉无法立法来证明其钻石的合法性，因而被从金伯利进程中除名。

**3.区块链的应用机会**

**3.1.用数字密码学来建立信任关系**

尽管有人认为由于钻石独一无二且需要单独的评估，所以不能被视为一种商品，该行业也正开始发生变化，尽管区块链的实施仍处于初期阶段，但我们仍然看到了它为潜在投资者带来更大的透明度和安全性的潜力。区块链技术是对现有做法的补充，不仅能安全的追踪钻石，还能提供有效的数字证明。（区块链）是一本记录了任何产品从产生到灭亡的公共记录簿，且所有记录都不可逆，此外，这项技术比任何单一服务商的系统都安全。

确保道德采购钻石是保持消费者信心的关键。一般开采的钻石多数产自南非等国家，会出售给授权买家进行切割或抛光，再出售给零售商。为防止能以假乱真的合成材料流入天然钻石市场，区块链技术对此有很好的预防作用，以提高交易透明度和消除血钻交易。

**3.2.政策利好的风口**

事实上，南非被认为是改善数字货币环境的主要实施者之一。

正如南非财政部长所说，我们欢迎区块链和数字货币，因为区块链技术是一种低成本、高效以及极其安全的交易模式，还能用作个人或机构之间的资金转移，普遍看好数字货币的潜力。我们既要鼓励发展又要控制风险，除了创造加密货币之外，探索区块链技术的潜在应用已然迫在眉睫。

**4.我们要做什么**

**4.1.建立区块链电子简历**

详细研究了央行的数字货币结构，并赋予区块链系统一个全新的名字——“钻石区块链”（Diamonds Blockchain）。因为这种系统一生效就成为官方认可的管理模式,其他金融机构的证券、股票、衍生品，甚至是房产和车辆登记信息都会转移到这个钻石区块链系统中。这样央行也就能对商业银行创造的资产进行实时监管。

**4.2.打造基于三种区块链形式的混合跨链服务**

**4.2.1.基于公有链的个人应用服务**

私链：机构内应用，即机构内各个生产流通环节的终端信息流转的应用链；

联盟链：区域内机构应用，即每家机构都是一个节点、一个区块；

公链：系统收益权益，即面向广大用户的应用基础链。

正如不受限的信息流动改变了人类与数字时代的互动方式，不受约束的价值流动也可能将改变人类的贸易和工业。区块链已经诞生了加密工具，一种数字不记名工具和数字注册工具的混合体，是迄今为止最无摩擦的价值形式。

**4.2.2.基于联盟区块链的多级追溯体系和应用**

除了钻石等实体产品外，将允许多资产账本、债券、股票、衍生工具，合约和大量其他记录可以在其上注册，

**4.2.3.钻石区块链为基础的信息化**

我们正在采取一种平衡的方式来支持金融领域创新、竞争和普惠金融。推进比特币和加密数字货币法规的发展。通过司法机构，支持加强创新的目标，金融领域的竞争和金融包容，同时审查与金融客户保护相关的风险，打击洗钱、维护金融稳定。南非反对党也呼应了制定法规用以保护消费者。

如：在钻石区块链中的应用可以彻底改革征税模式。这种系统可以在交易发生的同时进行征税，从传统的‘交易后征税’切换到‘实时征税’。

**5.VAC的诞生**

作为发展了几百年历史的钻石行业是如何应用区块链这一崭新的技术，来为行业发展助力呢？

首先，我们先从钻石的产业链来看，钻石从毛坯开采和交易、钻石切割、裸钻批发和零售、首饰加工后流通到消费者手中，这其中还需要通过钻石鉴定开具证书、跨境交易报关进出口、外汇结算等环节，不可谓不复杂，而且由于世界各国国情不同，因此在交易过程中的规则和监管也不相同，出现的问题也千差万别，特别是钻石证书套证等现象，层出不穷，因此区块链的应用对钻石追溯、自证清白就显得越来越重要，消费者对自己购买钻石的了解和后期一些服务操作等就可以通过区块链技术获得更好的服务；

其次，记录钻石从矿山到珠宝商店行动轨迹的系统，帮助公司追踪钻石的原产地、以及切割好的钻石裸石的各个交易环节，其过程中用了各种各样的区块链工具，包括分布式账本。区块链可以创建一个永远无法被篡改的记录，非常适于追踪钻石以及其他货品的来源，卖家也想知道货品的来源以及原物主的信息。

此次项目的发起机构包括戴·比尔斯（De Beers）公司以及南非联合银行集团（ABSA）、天达银行（Investec）、南非莱利银行（Nedbank）等数家跨国银行。为了支持该项目，南非央行（南非储备银行 South African Reserve Bank）、南非金融服务委员会（Financial Services Board）以及约翰内斯堡证券交易结算机构Strate等相关机构都将提供相应的支持。其中，央行将主要负责智能合约在测试网络内的流通。同时，该项目将把摩根大通的区块链技术用于银行间的清结算业务。将与以太坊技术开发公司合作，推进该项目的技术验证。

**5.1.基本原理**

作为一个针对钻石行业的科技创新型项目，VAC团队很早就着力研究区块链技术对全球钻石交易的发展促进作用，平台将是全球第一个使用区块链技术的钻石交易平台。

VAC是一个使用区块链来构建全球共享数字分类账本以追踪并保护贵重物品的平台。使用机器视觉的方式，记录了40个元数据点，为每个宝石创建一个独一无二的个性特征。近1600万颗钻石会存在于区块链上。它的技术有助于通过整个供应链中的单一来源来验证钻石的真实性、来源，并对其进行保管。

更重要的是，每一个新的帐户必须由现有的帐户创建，之所以需要这个要求是为了让现有账号能够支付账号注册手续费用。那个支付这个手续费用的人就是注册者（Registrar）。一般来说，这个注册者（Registrar）很可能就是钱包使用者。在任何时间，他们就有权划分推荐收入和一个可选的推荐者（Referrer）。

**5.2.区块链的设计思想**

减少欺诈，降低成本，提高效率，这是区块链技术的突出优势。区块链技术的广泛应用，

为加速“数字化信用社会”的到来，势必引发政府管理形态和社会公信力的变革。我们认为，政府参与区块链的发展和监管非常有必要，应该鼓励对区块链技术的深入研究和区块链应用的不断实践。

**5.2.1.经济层面的设计思想**

从经济社会来看，区块链经济已经萌芽。许多基于区块链的解决方案，可以改善现有的商业规则，构建新型的产业协作模式，提高协作流通的效率。无论是各国央行和各大商业银行，还是联合国、国际货币基金组织以及许多国家政府研究机构，都对“区块链+”投入极大关注。区块链可为经济社会转型升级提供系统化的支撑。区块链+的显著优势在于优化业务流程、降低运营成本、提升协同效率，这个优势已经在金融服务、供应链管理、知识产权、智能制造、社会公益以及教育就业等社会各领域初步体现出来。

**5.2.2.技术层面的设计思想**

降低成本，是区块链技术的一个重要的设计思想。在区块链体系中，参与者可以不需要了解对方基本信息的情况进行交易，实现了“无需信任的信任”，改变了传统模式中以第三方为中心的信任模式。

价值交互的基础是双方信任的建立。区块链技术的革命性在于它实现了一种全新的信任方式，通过在技术层面的设计创新，使得价值交互过程中人与人的信任关系能够转换为人与技术的信任，甚至于由程序自动化执行某些环节，商业活动得以更低成本的实现。

**5.3.区块链的核心技术**

区块链Blockchain技术原理是比特币数字货币的底层技术，用于追踪银行和交易所的金融交易记录。公司如纳斯达克公司、美国证券托管清算公司、摩根大通和美国银行都在用区块链进行实验，只有小部分的公司，包括丰田汽车公司，用区块链技术监控他们的供应链。一个区块链是一个数据结构，让创建和共享交易数字账本成为可能。区块链用加密技术让每个人都有权限添加到账本中，用一种安全的方式，而不用通过中央机构。一旦数据区块记录到区块链账本中，基本就无法篡改或移除数据记录。

**5.4.发展趋势**

VAC的钻石区块链将面向整个实体行业开放，为每颗钻石提供追踪监控的可能，这还是迄今首个覆盖行业全价值链的区块链创新技术。区块链还能帮助银行打消融资疑虑，提高开采供应链的效率和透明度。

当整个平台彻底完成时，会以开源平台形式运营，也可以此为基础开发相关云平台。

**5.5.跑步进入区块链经济时代**

我们注意到，区块链技术已在世界各地呈现方兴未艾的发展态势。从业务上看，借助区块链的安全特性与信任机制，将成为发展数字经济的重要技术引擎，可以在多行业领域发挥作用，行业应用领域发展潜力巨大。

但从系统需求的角度来看，要在区块链上构建应用，需要区块链解决方案具备强大的三个底层能力：一是完善的新旧系统兼容/切换能力，二是全新的系统安全能力，三是适用多场景的用户隐私保护能力。

**6、钻石区块链（Consortium Blockchain）与多级追溯体系**

钻石区块链实现了可视化的服务交付和可视化的服务度量。在服务交付方面，从代码编译、测试、灰度环境验收到正式环境部署，整个服务交付流程实现可视化管理。在服务度量方面，对数据进行了标准化的分层归类，从基础设施、上层组件、应用服务、到用户侧，基于应用的拓扑架构，收集各类指标，统一到一个分析平台中展现。

钻石区块链提供通用高效的信息采集组件，部署在业务层、共识节点层以及账本存储层，信息采集组件把机器的系统信息（如，CPU，内存、硬盘、网络等状态）、节点使用状态（如节点访问量、访问时耗、节点健康状态等）以及业务使用情况（业务访问量、成功率、耗时分布等）实时展示到监控界面上，便于整个系统的管理。

**6.1.为什么用钻石区块链**

区块链所有委托账户操作会独立记录在区块链上，并且对委托账户的操作有严格的频度限制和独立的风控策略，可以严格控制委托账户的操作风险。

**6.2.什么是多级追溯体系**

区块链中用户信息和区块链地址是隔离的。从各节点的记录存储中，无法获取到相关联的用户信息。用户信息存储有权限控制，访问认证，加密存储等多层保护。对交易保密程度较高的用户还可以选择交易不相关性机制，同一个用户的每次交易都映射到区块链上不同的地址上，从而保证了在交易账本上无法获取一个用户的多笔交易的关联性

**6.3.如何用钻石区块链打造多级追溯体系**

从公共服务层面来看，区块链技术正在探索在公共管理、社会保障、知识产权管理和保护，土地所有权管理等领域的应用。相关实践表明，这种技术有助于提升公众参与度，降低社会运营成本，提高社会管理的质量和效率，对社会管理和治理水平的提升具有重要的促进作用。

钻石区块链将成为构筑数字化信用的基石。如果将之用于公益捐赠，每一笔款项都会记录在区块链上，没有营私舞弊的空间。如果将之用于防伪打假，每一个产品都可以溯源而相关交易都有记录，进而消除了造假的空间维护了市场正义。如果企业或某一组织，将之用于薪酬发放，那么各行各业或将不存在劳资纠纷问题。

**7.基于钻石区块链的源头表单**

**7.1.表单数据如何基于区块链保存和传输**

节点的自校验性：钻石区块链采用块链结构存储数据记录，其中部分记录的修改会破坏块链结构的完整性，可以快速校验出来并从其他节点将数据恢复。另外钻石区块链每个记账节点都有自己的私钥，每个区块头中包含了本节点私钥的签名，区块内数据的修改都可以通过签名校验出来。

多节点准实时的数据校验：当节点的私钥被盗取，恶意用户是存在修改账本链上所有数据的可能性的，钻石区块链提供了多节点间准实时的数据对比机制，可以及时发现某个节点账本数据被篡改的情况。

**7.2.钻石区块链经济发展的重点行业**

不管是金融领域、物联网领域还是公共服务领域，钻石区块链致力于提供机构级区块链基础设施，行业解决方案，以及安全、可靠、灵活的区块链云服务。

通过高性能的区块链服务，在实现安全可靠的交易对接的前提下，通过可视化的数据管理手段，有效降低机构运营综合成本，提高运营效率。

**8、应用服务层（Trust Application）**

应用服务层提供基于钻石区块链的应用方案给最终用户，使用区块链解决方案中将尽力为海量用户提供各类场景的服务，未来将在数字票据、贵金属交易、知识产权保护、网络互助、机构清结算、公益等场景为用户提供可信、安全、便捷的区块链服务。

钻石区块链也会本着开放分享的原则，将携手各个行业伙伴发掘更多区块链的应用场景，开放区块链底层（Trust SQL）和平台应用层（Trust Platform）的能力，共同开发新的应用服务，一同维护区块链生态。

**8.1.基础服务**

基础服务部署在所有区块链的节点上，用来验证业务请求的有效性，并对有效请求完成共识后记录到存储上。对一个新的业务请求，基础服务先对接口适配解析，鉴权处理然后通过共识算法将交易或者合约加上签名和加密之后，完整一致的存储到共享账本上。

**8.2.用户管理**

负责所有区块链参与者的身份信息管理，包括维护公私钥生成、密钥存储管理以及用户真实身份和区块链地址对应关系维护等，并且在授权的情况下，监管和审计某些真实身份的交易情况。对数字资产等金融交易类的应用，还提供了风险控制的规则配置，以保证系统交易安全。

通俗的说，区块链可以看成是一套由多方参与的、可靠的分布式数据存储系统，其独特之处在于：一是记录行为的多方参与，即各方可参与记录；二是数据存储的多方参与、共同维护，即各方均参与数据的存储和维护；三是通过链式存储数据与合约，并且只能读取和写入，不可篡改。

**8.3.智能合约**

负责合约的注册发行以及合约的触发和执行。用户通过某种编程语言定义合约，逻辑，发布到区块链上之后，根据合约条款的逻辑，由用户签名或者其他的事件触发执行，完成交易结算等合约的逻辑。

很多区块链正在整合一种通用的脚本语言去定义所有的操作。这些设计最终将业务逻辑处理器定义为一个虚拟机，而所有的交易被定义为由这个虚拟机运行的脚本。这个方案有一个在真实处理器上的单线程性能极限，并且由于将所有东西强制通过一个虚拟处理器去执行，让问题更严重了。一个虚拟处理器即使用上了实施编译技术（JIT）也总会比一个真正的处理器要慢，不过计算速度并不是这种“任何东西都是一个脚本”方案的唯一问题。

当交易被定义在这么低的层次上，意味着静态检查和加密算法操作还是会被包含到业务逻辑处理的环节里，这也让会让整体的吞吐量降低。一个脚本引擎永远不应该要求执行一个加密算法签名检查的请求，即使这个请求是通过原生的机制实现的。

**8.4.运营监控**

负责产品发布过程中的部署、配置修改、合约设置以及产品运行中的实时状态，可视化的输出，如：告警、交易量、网络情况、节点健康状态等。

收集系统中运行的状态数据，并且可视化的呈现出来。系统中的状态数据包括系统的访问量、耗时、节点的健康状态以及比较底层的机器资源（CPU、内存、硬盘）使用状况等，通过可视化监控可以实时了解整个区块链系统的状态。

**8.5.自定义资产和身份管理**

比如：纽约证券交易所作为一个公司，它主要的职能是维护包含公司所发行股票或者债券所有者信息的账本。它主要的盈利方式是交易费用，以及它自己的股票等。类似于纽约证券交易所，钻石区块链允许人们在系统中发行自己的股票或者债券，并且能够在一个分布式账本中进行交易。钻石区块链能够在系统中标记每个账户来确保对应关系。这个信任网络能够让发行者在确保符合证券限制相关规定的情况下授权给其他人。

VAC去中心化平台能够提供一种称之为“用户资产（user- assets，UIA）”的特性，旨在帮助推动能够让一些针对某些服务的盈利性商业模式能够整合进入平台。本质上是一种注册在平台上得某种凭证，它能够在遵守某些特定要求的情况下在平台上进行交易。凭证的创造者可以设定公开名称、描述等信息，并且根据自己意愿来发行它。发行者业能自定义UA的某些特性：例如可以要求只能允许在白名单内的用户才可以持有凭证，或者要求用户在转移或者交易这些凭证时需要支付一定的手续费。

数字货币交易所和汇款机构可以发行自己的网关资产（UA），这样可以在VAC完成资金的进出。

企业可以直接在VAC的区块链上发行自己的公司股票，而且这些 UA能够设定为完全符合现有监管和相关法律条文。

UA还可以用来作为奖励券，优惠券，第三方货币，信贷，产品收据，众筹凭着，保修凭证等等。

**8.6.去中心化交易**

VAC会提供一个具有极高性能的去中心化交易平台，能够提供一切你所希望在一个交易平台上应该具有的功能。不仅订单的执行在你提交的瞬间就能够完成了，并且还能提供抵押债券让你能够使用杠杆和提供利息，期权合约能够让你对冲你的仓位。

去中心化让原始载体在经历各种信号处理过程后，隐藏信息仍能保持完整性或仍能被准确鉴别，不因处理攻击后而导致秘密信息丢失的能力。当一个中心化的交易所被泄露数百万美元将会瞬间影响数千个用户,而一个去中心化的系统被攻击或者出现故障只会影响单个用户和他的资金。用户能够控制他们自己的安全性，这其实可能远比任何中心化实体要好得多。

其实钻石区块链在试图破解一个交易所或者单个用户是存在一个固定成本的。这个区别就是在能够获得的收益大小。如果你花费数百万美元的成本来攻击一个特定的目标，那你肯定期望把这么多的精力放在一个交易所而不是你的单个个人账号。

在一个特定的公司里许多人都有机会可以接触到资金。你也许听到过俗话说“三个人守不住秘密，除非另两个不在人世”，大多数交易所都希望通过多个人来负责保护私钥的方式来控制资金。而如何其中的任何一个人出现问题，则每个人的资金都会是危险的。在这方面，事实上每个人独立负责守护自己的密码可能要比多签名要安全的多。

**8.7.业务逻辑处理器**

所有在加密货币网络的交易依赖于用加密算法签名去校验权限。大部分情况下，请求的权限可以由其他交易的结果改变。这意味着在业务逻辑处理器里面，权限需要被定义成与加密算法计算无关的情况。

要达到这个目的，所有的公钥需要分配一个独特的和不可代替的ID。当ID被分配后，输入分解器可以校验提供的签名与指定的ID是否匹配。当交易到达业务逻辑处理器后，只需要去检查ID就可以了。

这个同样的技术可以在拥有不可代替的静态ID的对象上实现去除前提条件检查。

**8.8.为静态校验设计交易**

对交易来说，有很多特性是可以进行静态检查的，而不需要引用当前的全局状态。这些检查包括参数的范围检查、输入的去冗余和数组排序等。通常来说，有很多检查是可以被进行的，如果交易包含它“假设”是全局状态的数据的话。在这些检查被执行后，业务逻辑处理器必须要做的事情就只有去确保这些假设还是正确的，这个过程总结下来就是检查一个涉及交易签名时间的对象引用的修改时间戳。

**8.9.对象数据模式**

在内存中保存所有东西的其中一个好处是，软件可以设计成模仿现实世界中数据的关系。这意味着业务逻辑处理器可以迅速根据内存内的指针去找到数据，而不是被迫去进行耗费高的数据库查询任务。这意味着数据不需要复制就能访问了，而且可以当场就被修改。这个优化提供了比任何数据库为基础的方案高一个数量级的性能表现。

**9.平台产品服务层**

平台产品服务层抽象了各类典型的区块链应用，提供典型应用的基本能力和实现框架，用户可以基于这些基本能力，叠加自己业务独有的特性，轻松完成业务逻辑的区块链实现。帮助用户快速搬迁已有业务到区块链上，以应对新的场景需求，或者搭建全新的业务场景，利用区块链的不可篡改、防抵赖等特性解决之前难以解决的问题。

共识机制可自适应，在网络和节点都正常情况下具有高并发性，网络异常或者节点欺骗的情况下具有强容错性。

**9.1.数字资产：**根据对虚拟货币、贵重物品、商业票据等数字资产的分析，我们发现资产上链是一个关键环节。为此引入“资产网关”的概念，协助用户进行链下资产到链上资产的转换。资产一旦上链，转移、拆分、提现等操作就会通过帐户公私钥体系严格控制起来，并且所有的操作都会有签名校验，交易双方都会留下痕迹，不可抹除。如商业票据、卡券等存在有效期的资产，还会提供到期自动清算的能力，包括资产发行、资产转让、资产提现、资产清算、资产查询等。

**9.2.鉴证服务：**针对知识产权、保单保全（权益证明）、产品和企业资质证明等应用场景，区块链充分发挥不可抹除和公示的能力，让机构和个人通过一个简单的接口或客户端就可以把版权资料、投保资料、资质证明等发布到区块链上，让所有记账节点共同为自己作证。另外基于VAC自建的知识产权平台，用户的维权将更加方便，证据确认更有权威性。如权属登记、权属注销、侵权证据录入等。

**9.3.共享账本：**金融机构间的对账清算目前基本都是以天为周期进行，对账方式基本也都是互发对账单，对比双方的交易流水。这给最终的交易确认和资金划拨都带来一定的延时，一些需要实时付款的业务场景甚至必须要业务运营方去垫资进行。区块链天然的共享账本，让对账不必第二天汇总发送，而是随时都可以进行，双方只要把对账逻辑对接到区块链上，就可以完成资金的核对。基本可以实现准实时的交易确认和资金划拨，并且任意一方都不可抵赖。特别对于资金链条比较长，牵涉环节比较多的业务非常有竞争优势。同时监管机构也可以参与到共享账本记录中。

**9.4.分享经济：**通过金砖会议，我们充分学习中国的一些先进思想，如分享经济。分享经济能否走的长远，一个关键因素就是供需方之间信任的建立，保证分享行为的顺利实施，而区块链从技术层面提供了一种实现途径。技术保证能力的背书，让彼此难以达成信任的多方参与者，共同建立起公信力，不再需要中间机构或者服务平台构建强大的内部审核流程，严谨繁复的记账备份体系，以及配合监管机构做的额外设施，就可以达到相同的效果。从而节约了大量的成本，让分享更加高效可行。

**10.技术特色和优势**

“这个钻石可追溯平台是基于区块链技术开发的，利用了一个高度安全的数字化寄存器，可以创建防篡改的、永久性的交易记录——在这种情况下，钻石可以在整条价值链中被追踪。”戴比尔斯公司首席执行官布鲁斯•克里佛（Bruce Cleaver）如是说。

区块链是一个下达关于确定去修改一个共享的全局状态交易的全球账本。这些交易中包含的命令可以改变其他交易的有效性。例如，你不能在你的支票存入生效前去从你的银行账户理解支取金钱。在能够影响一个特定的账户的所有先前交易都被处理之前，你不可能知道一个交易是否有效。

**10.1.分解器技术**

分解器提供了一个在单线程上可以实现什么表现的学习例子，是一个针对终端顾客的交易平台，目标是成为世界上最快的交易平台。

业务逻辑处理器是所有顺序交易和订单匹配发生的地方。它是一个可以每秒处理百万级别订单的单线程。这个架构可以很容易地用在加密货币和区块链设计的领域。

输入分解器扮演的角色是从很多来自不同源头的用户里面收集订单，然后分配给它们一个确定的顺序。当给它们分配好顺序后，它们会被复制、记录然后广播到很多冗余的业务逻辑处理器。输入分解器是高度并行的，而且容易分包到一个计算机集群系统中。

当业务逻辑处理器处理完输入后，一个输出分解器负责通知那些关心结果的人。这也是一个高度并行的任务。

最终，通过在业务逻辑处理器里使用单线程样品化处理器和Java虚拟机，VAC可以在每秒内执行600万次交易。如果顺利达到这个成绩，那么加密货币和智能合约平台平不需要在每秒连10个交易都不到的情况下去考虑集群网络方案。

**10.2.技术优势**

**10.2.1.高性能**

设计一个高性能的区块链并不是什么火箭科学，而且既不需要复杂难懂的协议，也不需要在网络上的所有节点里分处理任务。反而，要建造一个高性能的区块链最需要的事情应该是在核心业务逻辑上去除与关键性、订单依赖性和评估无关的计算任务，并且设计一个可以帮助优化这些事项的协议。这就是比特股做了的事情。

要建造一个高性能的区块链，这是几个必须实现的事项：

将所有东西放在内存上，避免同步原语（锁定，原子操作），避免在业务逻辑处理器上不必要的计算。

由于内存的设计是高度并行的，因此越来越便宜。追踪互联网上每个人的账户余额和权限所需要的数据量是可以放在小于1TB的RAM内存上，而且可以装在商品化（高端）的服务器主板上。在这个系统被30亿人采用之前，这类硬件会在普通的桌面计算机里面看到。

真正的瓶颈不是内存容量的需求，而是带宽的需求。在每秒100万次交易和每笔交易占256字节的情况下，网络会需要256MB每秒的数据量，即1Gbit/s的带宽。这样的带宽在普通的桌面计算机上并不是常见的。不过，这样的带宽只是二代互联网100Gbit/s带宽的一点而已。

另一句话说，区块链技术可以轻松将所有东西保存在内存里，而且如果设计的合理的话可以扩展到支持每秒百万级别的转账。

**10.2.2.高速接入**

南非第二大连锁超市，成立于1967年的Pick n Pay，其分店已经遍布整个非洲。被称为“世界首家开此先例的大型零售商”——消费者能在南非开普敦的Pick n Pay零售店用数字货币进行购物。

在单线程系统的系统里面，处理器周期是需要被保留的稀缺资源。传统的区块链设计使用加密算法基础上的哈希计算去生成一个全球独特的ID系统，以实现统计学上不会有碰撞的保证。进行这些哈希计算的问题是，它会耗用越来越多的内存和处理器周期。与一个直接的数组索引相比，这种方式会显著地占用更多处理器的时间去查找一个账户的记录。例如，64位的整数对比和操作起来都要比160位以上的ID更简单。更大的哈希ID机制意味着CPU缓存里面的空间更少了，而需要更多的内存。在现代的操作系统里不常访问的随机存储器是会被压缩的，不过哈希识别器是随机数，这是没法压缩的。

钻石区块链给了我们一个在全球内分配独特的ID的方法，这些ID互相之间不会起冲突，因此完全避免使用像比特币地址那样的哈希算法为基础的识别器去引用一个账号、余额或者许可。

为了给业界提供一个有可能代替现有的金融平台的方案，高性能的区块链技术对加密货币和智能合约平台来说是必须的。为了能够实现比VISA和MasterCard加起来每秒可以处理的交易数量更高的级别，VAC从底层开始重新设计。通过股份授权证明机制，钻石链网络可以在平均一秒的时间内确认交易，唯一的限制只是光速。

随着VAC的交易速度在几秒内就可以得到执行，这就已经和中心化的网站界面差不多了。这不像中心化的交易所，他们可以在高频交易中设置优先单或者隐藏单，而是把所有的交易者放在一个公平的竞争环境中。

**10.2.3.安全性**

美元，欧元，钻石和黄金，在BitShares交易所中都有着三倍于传统中心化交易所的资产支撑。那些传统的银行体系，其实应该被称为“虚构储备银行体系”，也常常称为“部分准备金银行体系”。在数字货币的生态系统中，我们常常要求能够至少提供100%准备金。即使这些交易所能够做到，但是一次被黑客攻击、错误或者被盗窃都很容易让这个100%准备金系统变成一个虚构准备金系统，或者，有时候更糟糕的成为了“没有准备金的系统”。在没有任何准备金的情况下，是不可能让这些交易所把你的钱还给你的。

通过始终保持至少200％以上的准备金的情况下，你可以放心，VAC在任何市场中都将具有偿付能力。所有准备金都会安全的存放在区块链上，这样它们永远不会被盗取，因为没有人能够获得偷窃这些准备金的私钥。

**10.2.4.无局限**

你可以在任何时间，从任何地方，交易任何金额，而且没有提现限制。所有其他合法合规的交易所，每天提现的限制大约都是数千美元的数量级。如果你想超越这些限制，你必须提供许多文件来提升你的等级。一些交易所，甚至限制了你的钱在提现后只能用于哪些方面。还有一些其他交易所要求你提供文件来证明你是如何获得这些数字货币的。

随着VAC的出现，你的帐户不再需要任何人的批准，你将会获得完整的财务自由。

**10.2.5.费率低**

因为每笔交易只需几美分，VAC肯定是全球成本最低的交易所。其他交易所会根据你的交易量来收取一定比例的费用。比较传统的交易所，VAC更加便宜。

**10.2.6.高效运营**

提供全面、实时、可视化的运维管理系统，快速识别系统状态，针对不同的用户需求，可以支持云部署、服务器部署等多种部署方式，适应各种各样的需求。

应该需要注意到，钻石链达到的性能表现是高度依赖其中的一个兼容交易协议。如果想用业务逻辑运行在一个进行加密算法操作和用识别器去调用所有对象的虚拟机上的话，是不可能去达到同样层级的性能表现的。区块链天生就是单线程的，而单核的CPU的性能是各种资源中最短缺的、最难扩展的一个方面。VAC设计成能够让这个单线程的执行达到极可能的高效。

在这里你可以交易钻石、金，银，天然气和石油，还包括你所喜爱的国家法币和数字货币，在VAC交易所上几乎没有任何限制。支持资产包括股票，债券，指数或通货膨胀(Inflation)。公司可以在区块网络上发行自己的股票，不仅方便，成本低，而且能够对保护交易来防止裸卖空。

**10.2.7.隐私**

通过使用VAC你可以能够对隐私进行保护。就像比特币一样，所有交易都是完全公开但无需绑定到你的真实身份。不需要国税局文件，没有人会要求你的护照的复印件，驾照，水电费以及信用报告。

**10.2.8.开放源代码和完全透明**

整个交流是开源的，由一个非常开放的社区支持。没有别的地方会让你有透明度，可与VAC发现的水平。

这种钻石区块链的另一个优势就是利用系统的透明性推动税务合规。也就是说，智能合约可以用来实时征收税款。

**10.2.9.可扩展性**

如果两个无关联的账号没有共享任何通用的依赖关系的话，理论上这两个账号的交易可以是在同一时间进行处理的。实际上，在一个由具备仲裁条件的智能合约驱动的账本上识别哪些交易是真正独立存在的耗费是很棘手的。唯一的保证两个交易是真正独立存在的方法，是通过维护完全分离的账本，然后定期在它们之间传输价值。如果要用这种性能表现的权衡关系去打比方的话，可以像是非一致内存访问架构（Non-Uniform Memory Access ，NUMA）和一致内存访问架构（Uniform Memory Access ，UMA）之间的关系。

实际上，一致内存访问架构对开发者来说是更容易去设计的，而且耗费更低。非一致内存访问架构通常是在建造超级计算机和大型计算机集群时作为不得已的方法去采用的。

**11.钻石链的盈利模式**

这种设计模式有许多创新性，其中两项值得关注：

第一，交易信任由机器和算法确定。区块链通过构建一个依赖于机器和算法信任的交易体系，解决在匿名交易过程中的相互信任问题。所有参与者将在无须建立信任关系的环境中，通过密码学原理确定身份，依靠共识机制实现相互间的信任。

第二，交易过程可以由程序自动执行。区块链通过可编程的智能合约，自动执行双方所达成的契约，排除了人为的干扰因素，从制度上防止任何一方的抵赖。从而推动经济社会进入一种智能的状态，实现当前经济交易系统的质的飞跃。

模式的升级，鉴于公有链的安全性及交易量与日俱增对现网容量之间的平衡问题，未来区块链的应用领域将以联盟链、私有链或混合链为主。比特币模式增加了区块链网络的维护成本，对于低价值、低风险的交易来说并非完全适用。考虑到效率及安全的提升，未来将是以钻石链、私有链、或由钻石链和私有链组成的混合链组成。

**11.1.商务进展**

钻石是人们的贵重装饰品，VAC希望利用追踪平台重建消费者对钻石销售过程的充分信任，采用区块链技术，同时降低人们对涉及钻石洗钱、以及因为钻石贩运而引发冲突的担忧。

在钻石行业里还有很多初创公司、甚至包括联合国在内的不少国际机构也在尝试使用区块链技术。如果区块链应用在钻石交易上，不管是数据追踪上，或者钻石的来源，都是给消费一个充分的保证，有一个很大的一个说服力。

**11.2.产品开发进展**

De Beers戴比尔斯首席执行官Bruce Cleaver在谈及区块链时表示：“这是一个庞大的不可变公共账本，是一种比任何单一服务器都更难以破解的系统。”

在实际的业务对接场景大致分为三类：第一类，原有系统改造后接入区块链，第二类，原有系统上新的需求使用区块链开发，第三类，在全新的系统和场景使用区块链。多种用户部署环境。

计算机产业逐渐意识到通过平行计算去实现性能的扩张并没有早期那么容易，毕竟那时候最需要做的事情只是提高处理器的频率而已。就是因为这个原因，处理器的设计者们在尝试去采用多线程设去提高性能之前都在拼命去提高单线程的性能。当多线程还不够的话，而且只有这样的话，集群计算这个方案才会被考虑。

**12.钻石链市场前景预测**

区块链技术已经在全球开始部署应用，美、英、日、德、加、澳等发达国家已经认识到区块链技术在公共服务和社会机制优化上存在着巨大的应用前景，开始设计区块链的发展道路。

利用区块链对钻石来源进行追踪，包括适用机构数量、当前市场覆盖率及增长率、市场容量，

在利用比特币的区块链时产生的过度能源利用等问题，不会影响其他应用，因为新技术更加节能。

**13.代币（Token），以及基于公链的服务**

**13.1.代币开发及分配方式**

为了钻石链应用更好的去中心化运行和商业应用的需要，钻石链发行相应的代币。钻石链的代币英文代号：VAC，恒定总量6900万枚，首期发行850万枚，是基于信用链的去中心化的数字货币。

负责处理网络节点的相关配置，如共识算法的选择、自适应阈值、存储账本的存储方式、网络路由方式等，配置的本身可以作为区块链中的一个交易的形式下发，通过共识算法达成一致之后再生效。

**13.2.基于公链的服务**

在“自主创新、安全高效、开放共享”设计原则的指导下，VAC钻石区块链方案的整体架构分成三个层次：钻石区块链的底层是VAC自主研发的 Trust SQl 平台，Trust SQL 通过 SQL和 API 的接口为上层应用场景提供区块链基础服务的功能。核心定位于打造领先的机构级区块链基础平台。中间是平台产品服务层为 Trust Platform，在底层（Trust SQL）之上构建高可用性、可扩展性的区块链应用基础平台产品，其中包括共享账本、鉴证服务、共享经济、数字资产等多个方向，集成相关领域的基础产品功能，帮助机构快速搭建上层区块链应用场景。

**13.3交易**

VAC系统内建了一个交易抽象层，核心系统的几乎所有功能都是建立在交易上的，比如转账、投票、应用商店、充值、提现等。子链本身也可以实现自己的不同类型的交易。交易之间的区别主要是交易类型和 asset。基础交易的数据结构如下，扩展部分会根据类型的不同分别存在不同的 asset表中。

Transaction{

required VARCHAR(20) id;

required VARCHAR(20) blockId;

required TINYINT type;

required INT timestamp;

required VARCHAR(21) senderId;

optional VARCHAR(21) recpientId;

required BIGINT amount;

required BIGINT fee;

required BINARY(64) signature;

optional BINARY(64) signSignature;

optional TEXT signatures;

required BINARY(32) senderPublicKey;

**13.4账户系统**

VAC的每个账户由一个口令、一对公私钥、一个地址组成。用户还可以额外设置一个二级密码。注意这里与比特币有所不同的是，每个账户仅对应一个地址，而比特币中每个钱包对用多个地址和私钥。

**口令**（ passphrase）是符合 BIP39标准的用于产生确定性钱包的助记符。 这种助记符与二进制或十六进制字符相比对人类记忆更友好。口令的生成方式是将一个64bit倍数长度的熵转换成若干个单词， VAC系统选择的熵长度为128bit，将转换成12个单词。口令作为一级密码，由用户保管，不对外公开，一旦丢失用户将失去对应账户的所有权。口令形式如下：

barely decline dust stamp protect color certain cup arena busy latin shell

密钥对包括公钥和私钥，是以口令的 sha256哈希做种子，再通过 ed25519爱德华兹曲线签名算法生成的。形式如下：

公钥：

9989388b220a13465e49f52df5ba28ba08eb1e7a973320347f9687a107dc2f 9a

私钥：

91e891f653e3ed0232d8c7de2e72b625d50d48593fc0fb570c0db25c5e4456 9a9989388b220a13465e49f52df5ba28ba08eb1e7a973320347f9687a107dc 2f9a

账户地址是取公钥的 sha256哈希的前8位，逆序后转换成 bignumber，其形式如下：

5034187504202890358

密钥对包括公钥和私钥，是以口令的 sha256哈希做种子，再通过 ed25519爱德华兹

账户地址是取公钥的 sha256哈希的前8位，逆序后转换成 bignumber，

**14.风控审计**

风控模块负责对区块链中数字资产类的交易行为进行风险控制，腾讯区块链提供风控专家模型系统，通过分析和捕捉海量数据间的深层关系，自适应调整风控规则，及时发现风险、管理风控和控制风险，做到防患于未然。审计模块为审计机构提供审计能力，通过严格的权限控制来保证审计能力只能被审计机构使用。

区块链合约部分包括标准合约以及业务定制的合约两种类型。标准合约包括资产一次性检查、自动成交撮合、多方共同确认的转账、到期自动清算等逻辑相对简单的合约，是区块链内置合约，可以直接挂在区块链上使用。用户定制的智能合约包括通过合约模板修改配置和添加其他业务逻辑的形式，也可以支持更加复杂的用户自编程的合约，在独立的环境里运行。

**15.为什么我们能做好**

全世界最大的宝石生产商De Beers戴比尔斯已经引领行业进行钻石真实性的验证，同时确保它们并非来自可能会被用于资助暴力冲突的冲突地区。

作为数字货币底层技术的区块链提供了一种可以追踪钻石来源的安全方法，并能提供表明钻石无冲突的数字记录。

从经济学意义来看，钻石区块链创造新的价值交互式是基于去中心化分布式账簿，但这并非意味着传统社会里各种“中心”的完全消失，未来区块链将出现大量的“多中心”体系，以公有链、私有链或混合链为主，区块链将会进一步提高“各个中心”的运行效率，并降低其相当一部分成本。

从技术角度来说，我们认为，钻石区块链是一种由多方共同维护，以块链结构存储数据，使用密码学保证传输和访问安全，能够实现数据一致存储、无法篡改、无法抵赖的技术体系。这种技术给世界带来了无限的遐想空间，全球对区块链的关注热度持续升温，全球主要经济体从国家战略层面开始对区块链技术及发展趋势进行研究。

**16.面临的问题及解决方案**

正如任何一次技术革命都会带来一些新的问题，区块链的发展遇到的挑战是如何建立能够促进该技术应用的监管环境，如果套用传统的监管模式，会极大的遏制创新，无法发挥其应有的潜力。因此，迫切需要政府的管理理念实现由“监管”到“治理”的转变，基调应当是鼓励创新，同时守住底线。

为有效推动南非区块链技术和应用发展，培育形成具有全球竞争力的区块链产业，提出以下建议：尚未成熟的区块链技术，从安全性分析的角度，面临着算法安全性、协议安全性、使用安全性、实现安全性和系统安全性的挑战，要加强对加密技术、密钥存储、隐私保护、技术实现等方面的安全研究，努力提高区块链技术的整体安全可靠水平。

第一、鼓励核心关键技术攻关，形成自主创新体系

鼓励国内重点企业、科研机构、高校等加强合作，加快对共识机制、可编程合约、分布式存储、数字签名等核心关键技术的攻关，争取形成具有自主产权的技术成果，打造更加符合国家安全要求的完全自主可控的区块链平台，为众多应用的发展与落地保驾护航。

第二、推动形成区块链应用发展的良好环境

面对区块链这类颠覆性技术，虽然在个人隐私和消费者保护、伦理和社会影响等方面面临挑战，但这些挑战最终都将会被解决，因为互联网就是一个很好的先例。因此，建议相关部门加强沟通协调，集聚产学研用等多方资源，密切跟踪国际产业发展前沿动向，通过多种形式共同推进区块链相关理论研究、技术研发、应用推广等工作，优化区块链技术产业的发展环境，力争在新一轮的产业竞争中取得先机。

第三、出台扶持区块链技术和应用发展的政策

借鉴发达国家和地区的先进做法，结合我国区块链技术和应用发展情况，及时出台相关扶持政策，重点支持核心关键技术攻关、行业应用解决方案研发、重大应用示范工程、公共服务平台建设等。同时，放宽市场准入限制，加强事中事后监管，优化服务水平。

第四、加快推动区块链领域的标准体系建设

围绕产业发展的重点环节，加快推进关键急需标准的部署和制定工作，逐步完善区块链技术和应用标准体系。积极参与国际标准研制工作，对接国际化标准机构和开源社区组织，加强国际交流合作，在积极做出贡献的同时，不断提升我国标准工作的国际话语权。

第五、加速推动区块链技术的应用落地

建议围绕金融、文化、医疗、教育、物联网、供应链等行业的典型应用需求，研究提出区块链行业应用解决方案。面向基础条件好、示范效应强的行业领域，探索组织开展区块链应用试点示范工作，推动区块链技术和行业应用的融合发展。鼓励和支持国内企业积极参与国际区块链开源社区，贡献力量，提升影响力和话语权。鼓励学习借鉴国际开源社区建设和运营模式，加强国内企业间的合作，建设我国区块链开源社区，围绕核心关键技术攻关、行业应用解决方案研发、重大应用示范、标准制定等，开展交流与合作。

**17.领导未来**

想象一下，如果有一种交易所能够让你在购买和出售数字资产时完全无需承受接触对方而带来暴露隐私的风险。想象一下，如果一个交易所能够提供非常低的交易手续费，并且没有任何充值和提现金额限制。想象一下你可以在交易中使用任何一种货币，甚至包括黄金和白银。想象一下如果能够提供市场中最好的流动性。这就是VAC，这是数字资产行业中最棒的去中心化交易平台。

VAC旨在为南非加密货币等金融科技领域探索新路子，以更好地应对金融领域不断出现的金融科技问题。它将大大提升经济活力，降低系统风险和促进货币政策在整个经济中更有效传递的能力。

据财政部发布的2018年度财政预算报告显示，2017年南非经济预计增长1%，2018年有望达到1.5%，2020年可能达到2.1%。可以想像，我们正在与全世界的一些顶级科技公司进行交流合作，更是在为南非经济发展贡献一份力。

作为首个跨越整个价值链的钻石区块链，随着VAC创新和优势的展现，我们显然已经能够遇见VAC的未来。