Descartes Chain

The First Digital Financial Universal **Super FinGate** in the World

DESCARTES CHAIN

WHITEPAPER

CONTENT

BACKGROUND OF DESCARTES CHAIN

INTRODUCTION OF DESCARTES CHAIN

Background of Descartes Chain

1.1 Finance — Core of Global Economic Development

From 2000 B.C. in Babylon, finance developed along with global economy. Till 2018, the size of global financial derivative market has reached over 60 billion dollars (USD). Finance, in the key position of modern economy, operates normally with efficiency, which indicates the fully efficient raising, financing and using of monetary capitals. Finance also plays an obviously important role in the virtuous cycle of global economy. Monetary capitals, as the important economic resources and wealth, have become the life line and the bridge to communicate with the whole social and economic activities. Nowadays, all kinds of economic activities can never go without monetary capital movements.

1.2 Four Great Stages of Financial Digitalization Development

1.2.1 Entity Finance

Entity finance features the special businesses that operate financial products under the traditional economic environment, including banking, insurance, trust, securities and leasing. Financial industry is originated from the monetary keeping and loan business with interests in

Babylonian temples in 2000 B.C. and in Greek temples in 6 B.C. Modern financial business, through a long-term historical development, has developed from a comparatively single form in the ancient society into a financial institution system with various categories. All kinds of banks play a leading role in modern financial business. Commercial bank is the earliest and most typical form of modern banks. Modern commercial banks basically comprehensively operate various financial businesses. Except for banks, modern financial business also includes all kinds of mutually cooperative financial organizations, finance companies, discount companies, insurance companies, securities companies, financial consultation companies, specialized saving and exchange organizations, pawnbroking, gold and silver industry, financial exchanges as well as credit assessment companies, etc.

1.2.2 Electronized Finance

Electronized finance features the application of modern technical methods, including modern communications technology, computer technology and network techniques; it improves the working efficiency of traditional financial service industry, and lowers operation cost, and realizes the automation of financial business processing, the informatization of business management as well as the scientification of decision-making. That will provide fast and convenient services for customers and reach the goal of strengthening the market competitiveness. From the latter half of 20th Century, electronized finance has thrived with the development of electronic technology and its wide spread in financial business. The birth of it has vastly changed the look of financial businesses, and it has enriched service types; it is still influencing people' s way of economic and social life. Today, all social organizations, groups and individuals, whether willingly or not, are experiencing electronized finance indirectly or directly and enjoying the services of it.

The birth of electronized finance has made a huge difference in financial rules and efficiency, but there are still obstacles between financial products, between financial products and users, between finance and managers, which will lead to tough communication and cooperation. Therefore, internet finance was born in the right time.

1.2.3 Internet Finance

Internet finance is the combination the internet technology and the internet spirit with the core functions of finance, to largely lower the costs and reduce the imbalance of information, which will bring customers, including common individuals and enterprises, enjoyment of better inclusive financial services.

Internet technology contains emerging techniques, such as the big date that will drive the internet to fully dig out the "connective bonus", as well as the cloud computing, etc.

The core of internet spirit includes equality, openness, transparency and sharing, conforming to the concept of decentralization. According to the theory of Nobel Economics Prize winner Robert Merton, the key functions of finance include resource allocation, payment and settlement, risk management, price discovery, division of resources and ownership as well as incentive mechanism construction.

In addition, whether service providers are internet enterprises or traditional financial institutions, or other organizations, they can be included in internet finance, as long as they conform to the description about internet finance mentioned above.

Internet finance, as a product of cross-industry fusion, shows different features in its business form, compared to traditional finance.

First, metamorphosis of species, which means breaking through the forms and boundaries of old inherent products. Suppose that finance is an ecosystem, implanting the genes of internet finance will result in increasingly vague boundaries between different financial businesses. The "cross-boundary fusion of species" between "finance and non-finance" and between "finance and finance" will become a normal condition. Many new business activities and "new species" will spring up, which never happened in traditional financial service mode.

Second, diversity of species, which means the business modes show abundant differences. Take crowdfunding as example. As for the mode of return, there is sponsored crowdfunding that takes products of invested projects as return, equity-based crowdfunding that takes the stock rights of invested projects as return as well as charitable crowdfunding that takes nothing as return.

Third, evolution of species, which means the increasing speed of product iteration. Even the content of some classified internet finance businesses will be refreshed. Take payment as example. New ways of payment, such as QR code, payment by sound-wave, NFC, Beacon and payment by biological characteristics, appear in our life, successively. The boundary between online and offline has been broken through.

In general, the ecosystem of finance is stepping rapidly from a comparatively segmented, static and modularized industrial stage into a dynamic, "molecular" (compared to modularized, it means a distribution at a more detailed level) stage. Financial business forms cannot be easily classified. Even they are classified, they can change very fast.

Internet finance essentially follows the rules and regulations adopted from traditional finance, and only improves the absolute efficiency of information. However, centralized finance operation is not an optimal solution, because the participation of numerous third parties will cost more while it improves the operation efficiency. Blockchain is a new option for improving the operation mode of finance in basic logics.

1.2.4 Digital(Blockchain)Finance

The internet was invented for highly efficient transmission of information. On the internet, peer-to-peer information transmission in the world has become extremely high-efficient and cheap. Nevertheless, this kind of information transmission network does not have an internal mechanism to protect valuable information. Copying, transmitting or even tampering a strip of information costs nothing, so information with ownership cannot be transmitted from peer to peer. Some traditional industries (such as record industry and publishing industry) were deeply impacted by internet, which is an inevitable result. Although governments of different countries are enhancing the protection for copyrights of online contents, it is still hard to technically avoid problems like right infringement.

From the view of electronic currency' s birth and development, we have tried to circulate digitalized currencies efficiently, but the level of their digitalization is still primitive. We have to rely on lots of third-party institutions to guarantee currency circulation, which lifts up transmission costs, such as transaction fee, with risks of centralization.

Blockchains were born under the background. Due to the close relationship between information and value, if we enjoy a worldwide efficient and reliable information transmission system, an efficient and reliable value transmission system will be necessarily needed to match. In other words, the birth of blockchains is not an accident but a certain event with logic. The name "blockchain" might be an accident, but the birth of the system to operate blockchains is a certain thing.

Credit is a real raw material for the production of currency. Blockchains, by creating an economic system that can quantize credit, realize the peer-to-peer electronic cash system – Bitcoin. In other words, blockchains have

created a digitalized credit system that can realize peer-to-peer value transmission.

1.3 Rise of Digital Currency – Primitive Germination of Digital Finance

Bitcoin is no longer the only digital currency based on blockchain technology. According to statistics, until March in 2018, the number of digital currencies published and displayed on larger platforms has been over 1700.

In fact, from the birthday of Bitcoin, many imitators and competitors have been coming out endlessly. Among those coins, most are simple imitations and copies of Bitcoin, without any innovation. We call them simple Altcoins (Altcoin is Bitcoin alternative; these simple Altcoins are not innovated but simply copied coins). Some are not just simple imitations, and they have their own innovations and focused areas. This kind of coins are competitive Altcoins (these Altcoins are innovated and more competitive, compared to the Altcoins mentioned above). As for the market value of digital currencies, the value of Bitcoin is far ahead of others, but the value of later-born coins from Ethereum and Ripple, is already over 10 billion dollars (USD), separately.

Digital currency is the most widely used and most highly admitted application of blockchains now. Digital currencies once were symbolized by Bitcoin. What can be anticipated is that digital currencies will still be the most important application of blockchains, even in the future when blockchains are widely used.

Digital assets and blockchains are of natural affinity. Generally speaking, digital assets contain all kind of assets in binary format, with ownership. Narrowly, digital assets are non-monetary assets in form of electronic

data, sold in daily life. Typical examples are financial products, such as stocks and bonds.

Besides, due to its features – openness, transparency and tamper proof, blockchain technology can make trustable proofs for any digital asset or any valuable information; it can also realize the registration or transformation of various real assets. In this way, the application includes property right, copyright, notarization, etc.

1.4 Present Difficulties for Digital Assets

1.4.1 Increasingly High Transaction Cost

Due to the existence of centralized operation subjects, centralized exchanges cause high costs, and reduplicate costs will be charged from users. Transaction costs of centralized exchanges basically depend on the market environment and supervisory policies. Adjustment rules for transaction fee can be made according to operation strategies. To encourage frequent transactions by users, transaction fees can be canceled, but a service fee will be generally charged for withdrawing assets. Most centralized exchanges adopt IOU to keep accounts. All internal orders and transactions in an exchange are recorded by IOU on its platform. Therefore, transaction costs seem very low technically. (IOU is the abbreviation of "I OWE YOU", similar to bank note.)

1.4.2 Extremely Low Application Efficiency

The designing of Bitcoin and most blockchains only concerns about transactions, and it cannot support the definition of other assets or complicated transaction logic. If new functions need to be added in, the system have to be upgraded. However, difficulties lie in the completely decentralized system (like Bitcoin), because any change in the system

needs the consensus from the community, which slows down the changing speed.

Most of changes are not necessary or unattainable, because more flexibility means more complexity and less stability. In consideration of diversified even conflicted demands in real life, blockchains cannot meet all demands at the same time.

1.4.3 Anti-Regulation Control on Centralization

Recently, the field of blockchains is increasingly popular. The early generation of investors for that already made their first fortune. Under the influence of wealth effect, large quantities of new investors burst into the market. Most of them are lack of investment experience and good judgement. Moreover, all countries are lack of relative supervision and management, which leads to bankers' malicious control on coin prices. The coin price can increase or decrease several times in a day. More surprisingly, the price even can drop off 1500 times in a day. Secondary markets keep finishing the harvest of that. All countries have paid more attention to the risks and problems about the speculation behind the market, the high instability, money laundering and corruption.

1.4.4 Isolation from Real Finance

The resistance to the emerging of digital finance is derived from traditional system's fear for "financial disintermediation". The "chief culprit" of "financial disintermediation" is not internet or blockchains but the low efficiency of the original financial system; new technology is only a helper for "financial disintermediation". Efficiency problems are very common in economic entities. Only in a highly marketized environment, will the market entity seek for improvements automatically,

due to sufficient competitions. If under an environment full of "financial repression", the distribution of financial resources will not fully follow the market mechanism – resulting in a fact that people who needs the resources most and can create new value from them can obtain the resources earlier, but will follow the mechanism of power – leading to a condition that distribution will be made according to the control of the distributor on the resources as well as the closeness between distributor and distribution objects. That will naturally go against the improvement of efficiency problems. The heavier "financial repression" becomes, the bigger desire for "financial disintermediation" exists and the larger obstacle for innovation. Meanwhile, it means once "financial disintermediation" is realized, both its scale and influence are unprecedented. Although internet finance and blockchain finance are both substitutes for traditional finance, internet finance is a gradual replacement, which brings "financial semi-disintermediation"; blockchain finance is the replacement of reconstruction or the terminator of "finance with intermediary". The age of harvest earnings without efforts by monopoly positions will come to an end. For big players who distribute financial resources in the old financial system, it is their instinct to resist the change, and the isolation they made has become the biggest difficulty in today's digital financial development.

1.5 Trends and Opportunities of Digital Finance

1.5.1 Computability of Credit

Blockchains were born as the base technology and fundamental structure of Bitcoin. Bitcoin is an electronic cash system that can realize peer-to-peer payment, without the dependence on any third party. In virtue of cryptographic technology, the inventor of Bitcoin Satoshis Nakamoto structured an ingenious economic system, which solved the problem

about how to create a reliable value transmission system under a decentralized structure.

Shannon (Claude Elwood Shannon), as the inventor of information theory, solved the significant problem about "how to definite information by mathematical methods", which gave information a quantized unit "bit" and made it possible to accurately calculate information. That laid the theoretical foundation of digital communication, and also solved a big problem for the birth of blockchains -- how to definite information by mathematical methods.

In the context of economics, credit, as an element of risks, is defined as a subjective probability level to take some special actions when a subject assesses another subject. Different scholars have different views on the establishment premise of fiduciary relationship. The difference mainly lies in whether credit is of computability.

Only when different decisions are made, will the problems of credit come out. The situation when a subject shows itself under the opportunistic risks made by the other party is called the presentation of credit. In this aspect, credit is a behavioral strategy, and the choice of the strategy seems computable, from the view of mathematics and game theory. It is easy to think of that credit is an advantageous behavioral strategy when the product of potential income and credit behavior probability is larger than the product of potential loss and credit-losing behavior probability (potential income× credit behavior probability> potential loss× credit-losing behavior probability). In 1990, Coleman proposed this computing method in algebra.

Many scholars hold the opinion that credit is computable, with various computable concepts and methods. However, there is an unavoidable problem of bad operability. One of the scholars wrote in his article and admitted that humans were ultimately bounded rational social animals, and different social environments could change the behavioral choices made by economic subjects confronting with transactions. if take into consideration the facts, such as the diversification of environments and

the inexistence of absolutely rational individuals, it will be founded that credit is not just a simple concept of calculation, so the credit behaviors in the society cannot be always simply reduced to the interactive influence based on calculated subjects.

In other words, the problem is not that credit is incomputable, but that the system or the environment to accurately calculate it hasn't been created. Blockchain technology will be the hope to solve the problem.

1.5.2 Credit Expression of Blockchains

The definition of credit here is not to calculate the credit of participants or involved subjects, but to calculate the credibility of credit behaviors (such as transactions), or to calculate the possibility of defaulting (fraud or cheating) a credit behavior in the future. The lower the defaulting possibility becomes, the higher the credibility of the behavior will be; conversely, higher defaulting possibility, lower credibility.

From the view of economics, the obstacle to solve this problem is rooted in the difficulty of accurately calculating defaulting cost and benefit before the happening of defaulting behaviors. The economic system of blockchains, structured by the mathematic method, is an open and transparent system to everyone. More importantly, the cost caused by the defaulting (cheating or fraud) behaviors and the predictable earnings can be accurately calculated in the system of blockchains.

The credibility of credit behaviors can be defined by the ratio of default costs and default earnings (credibility of credit behavior = default cost/ default earning). Any transaction in the blockchains can have an accurately calculated result confirmed by the equation.

Bitcoin has gone through seven years of dispute since its birth. In this kind of decentralized economic system without any reliable third party to guarantee, no serious cheating behavior or fraud happened. The reason

for that is the costs of fraudulent behaviors are much more than expected earnings, which is conformed with the computation and the prediction Satoshis Nakamoto did when he created blockchains. Obviously, when the costs of fraudulent behaviors are much more than expected earnings and when the costs and earnings can be accurately calculated in advance, any rational participant will not have the motivation of fraudulent behaviors.

1.5.3 Internet of Value

Information asymmetry indicates that all parties participating in a transaction hold different information that can influence the transaction. Generally, sellers have more information about transactional goods than buyers. On account of the birth of internet, people can more easily receive the information they want by a new generation of communication channels and a nearly instantaneous transmission speed. The reason why the internet can make a deep influence on the commercial community today is that it has broken the information asymmetry.

However, there is still a long way for the internet to make a breakthrough in information asymmetry. On the internet, there is united information transmission layers but no united value transmission layer, so a great number of intermediary organizations are still needed to make sure the reliable saving and transfer of value, during transactions (value transmissions). Those intermediary organizations result in the reduce of value transmission efficiency and the increase of value circulation costs.

The united value transmission layer structured by internet, which means the birth of value internet, will be an inevitable consequence of blockchains development and evolution. The birth of value internet will further break down the wall of information asymmetry, to realize the independence of digitalized value (represented by currencies and digital assets) from a large quantity of intermediary organizations. Therefore,

the free circulation of the value can be achieved. It will be a qualitative leap of the market efficiency, which will thoroughly change the present structure of finance and economy.

1.5.4 Basic Protocol and Layered Structure

The internet, the same as blockchains in nature, is a decentralized network, without any "internet center". The difference is the internet is a highly efficient information transmission network without any concern about the ownership of information, and it doesn't have a protection mechanism for valuable information; blockchain, as a protocol that can transmit ownership, will establish a new basic protocol layer based on the existing internet protocol structure. From the point of view, blockchain (protocol) will develop as one of the basic protocols for the future internet, just like TCP or IP.

It should be known that blockchain is a complicated multi-layered system. Like the layered structures of TCP or IP stacks, different layers have different functions. Varieties of application layers have been made on the foundation of the united physical layer, which has eventually constructed a colorful and diversified internet.

In the future, different kinds of blockchains in different layers will play different roles. It is believed that blockchains will develop various application layers from the united physical layer in the future, to cultivate a diversified ecological internet of value.

1.5.5 Development Curve of Revolutionary Technology

Changes stimulate people to give up prejudice and pick up new thoughts.

The rise of blockchains will overturn the inherent cognition of most people. People, lacking in exponential thinking, always misjudge the development of new things, for they overestimate their short-term influences and underestimate their long-term influences. Just like the breakdown caused by the Internet Bubble in 2000, the internet is regarded as a powerful thing that can change everything, chased by many people with assets. All of a sudden, it was found that the internet was not as magical as people thought. People left it behind successively and the internet fell down from the worship alter into troubles. Unexpectedly, the internet started easily changing human' s business structures, financial conditions and the way of living after several years.

Introduction of Descartes Chain

2.1 Why Descartes Chain was Designed

1. Innovation of Project Technology

Although cross-chain is widely known by the public, no cross-chain project is commonly recognized and used by the community. Therefore, cross-chain is regarded as an unmatured technology. Speaking of stability and security, it still cannot compete with traditional public blockchains. Some projects proposed to use cross-chains or side chains as solutions, but few made progress on the landing.

2. Possibility to Implement the Technology

The key to analyze the project is to see the feasibility of implementing the technology. The realization of Cross-chain requires complicated mechanism design and programming ability of cross-chain smart contracts. The key to know if a project is investable is to see whether the project can be operated stably with Cross-chain.

3. Outstanding Advantage compared to Similar Projects

In spite that few projects realized their landing, it is observed that the projects using cross-chain are usually under similar mechanisms. The key to make a project stand out is the stability of its technology and the project progress.

4. Design of Economic Incentive Model

To see if a project can have a long-term development, its economic incentive model should be thoroughly investigated, from which we can know if the model can support initial cold boot of the community, and if it can constantly motivate miners to participate in the development, and if it can continuously develop and promote the entire value of the project to cultivate a positive feedback ecosystem in the later stage.

5. Operation Ability of Community

In the long term, the development speed of a project mostly depends on if its team has the ability to operate its community, which is the ability to raise the user volume of the project and to cultivate a network effect by the community.

6. Business-Level Service Quality

Storage reliability and service availability ultimately needs the proof of actual market demands. At present, most cross-chain projects and application programs are out of business availability. How to design appropriate smart contracts? The projects that can propose excellent solutions to the problem will certainly become the leading ones in the field.

2.2 Why it has to be Descartes Chain

Descartes Chain aims at establishing the super public blockchain in the age of digital finance, in hope of breaking through the isolated closed island situation of value, to solve the problems of the incompatible relationship between traditional finance and digital finance. Descartes Chain thoroughly provides improved financial functions in support of metadata recording, and fully releases the liquidity of various assets, and digs out the potential value of assets as well. On promoting the development of the global digital financial ecosystem, Descartes Chain is now becoming the key infrastructure to connect the entire digital currency world with traditional financial world.

2.3 Logic and Methods

The huge potential of blockchain technology has been proved in many fields, such as finance, information management, distributed network and storage, assets management and administrative management, etc. Up to now, the commercial system in the real world has not adopted the new technology immediately. There are many reasons for that. In our opinions, there are three main problems:

1. Lack of Expandability: Nowadays, even the biggest internet company is bothered by the rapid increasing of daily data and transaction information. Oversized volume of data and transactions will cause network congestion, which will lead to more expensive and lower network services. According to the generation speed of blocks, there is a long way to go to realize business-level applications.

2. Lack of Connectivity: Every public blockchain has to design a complete economic system, including miner ecosystem, original coins and DApps. Every existing public blockchain is an isolated island of digital assets, and they cannot connect with each other. Even it can work theoretically, it is extremely difficult to actually transfer and pay digital assets between all public blockchains. Lack of interoperability between

public blockchains is the big problem that stops blockchain technology from being widely adopted.

3. Low Availability: Existing internet services already can satisfy most information processing demands of humans at several main aspects, including computation, storage and network bandwidth. However, blockchain internet is limited by abilities of computation and storage, and it is very primary at the aspects of standardized protocol, programming language system, development framework and application ecosystem. Therefore, it is tough for blockchain internet to take over all businesses of traditional internet.

Among the three problems mentioned above, the most urgent one is lack of connectivity; it is necessary to solve the bottleneck of cross-chain communication to realize the free transfer, exchange and payment of digital assets. The second urgent one is lack of expandability, and the third one is low availability. The improvement of availability is a long-term infrastructure, for traditional internet reached today' s technical level for a long time too. The technical elites in the field as well as the research development team of Descartes Chain have already joined in the work of solving those three problems.

2.3.1 Development Path of Cross-Chain

If a person doesn' t know about the history, he cannot understand the present and seize the future. In September 2016, Vitalik Buterin published a research report *Chain Interoperability*, which concluded three types of cross-chain:

The early cross-chain was represented by Ripple, BTS and Cybex who concerned about asset transformation; they adopted notary technology.

The second type of cross-chain has two directions: one is sidechain, represented by RSK, Bytom and Lisk, which anchor coins on the main chain to solve the expendability of the main chain. The other is relay,

represented by BTC Relay, Polkadot and Cosmos, which concern about cross-chain infrastructures.

The third type is hashlock, represented by lightening network, with a purpose to improve the processing capacity of off-chain transactions in Bitcoin network. It is the most widely used technology for now.

Types of Cross-Chain Connectivity

- Centralization or Multiple Notary Mechanism: when a group of trusted participants make some event happen on chain A, the corresponding operations will be conducted on chain B.
- Sidechain/Relay: a blockchain built-in can verify and read the events and/or status systems on other blockchains.
- Hashlock: set up interoperating triggers between chains, which are usually to-be-exposed nonce hash values in cleartext.

Notary Mechanism

The easiest technological way to promote cross-chain operation is to use notary mechanism; according to the definition by Vitalik, notary mechanism indicates:

> In a notary mechanism, a trusted entity or set of entities that is trusted as a group is used in order to claim to chain X that a given event on chain Y took place, or that a particular claim about chain Y is true.

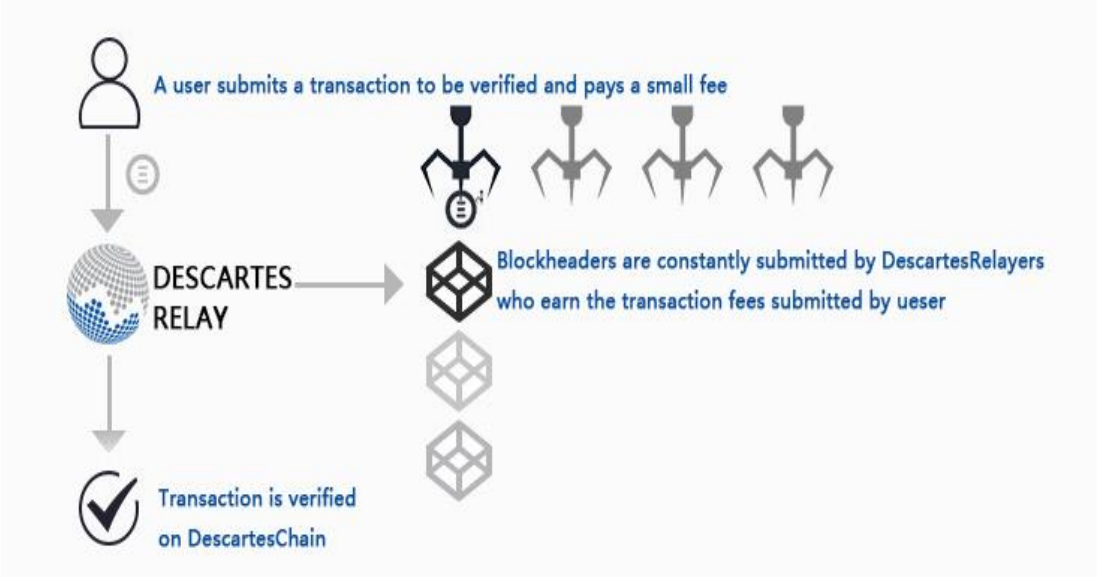
Those trusted entities can initiatively monitor and automatically trigger relative operations according to some events on some chains; moreover,

they can be called passively or publish signatures and information. Simply speaking, it means mutually free currency transformation through third-party "connecters" or "verifiers" to realize asset transformation on different chains. A typical representative is Ripple Interledger Protocol. Its executive process is showed as follows:

1. notary election: notaries are elected by participants;
2. proposal initiation: initiators come up with proposals and all participants verify the ledgers;
3. preparation: implement the ledger transfer through escrow mechanism; the initiators first need to authorize and the connectors take over in orders;
4. execution phase: participants sign transaction receipts, and submit them to notaries, who verify the transactions through Federated Byzantine Agreement.

Relays

Compared to relying on the chain-to-chain information transmission of reliable intermediaries, the most direct way to realize cross-chain connectivity is to use relay chains. The detailed implement processes are as follows:



sidechain/relay, on the basis of new chains, is to peg tokens on the main chain, to realize functions, including asset transformation, transaction verification and information exchange. Typical representatives are BTC Relay, Polkadot and COSMOS, etc.

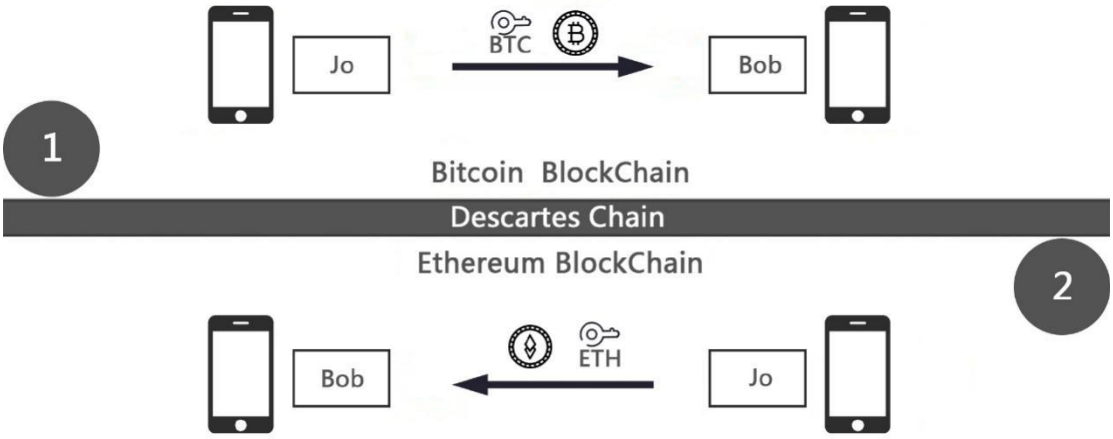
1. the main-chain transaction: the main chain initiates cross-chain transactions, and indicates target chains, money amount and recipient address.
2. Monitoring and verification of sidechains: when a sidechain receives an event, it will do a main-chain verification on the transaction. Through the light client protocol, it will read block headers and operate cryptographic verifications by Merkle Tree.
3. Produce relative assets on the sidechain for circulation.
4. Destroy the assets in a negative direction to realize the return of assets to the main chain.

Hashlock

Except the technologies mentioned above, there is a technology that can realize the atomic operation of cross-chain connectivity, without much knowledge of other chains. To establish the interoperating triggers between chains are usually the to-be-exposed nonce hash values in cleartext. Exchange and redemption mechanism is to lock the original hash values for a while. Hashlock is originated from Bitcoin lightening network. The mechanism can be explained by the following case of cross-chain digital asset swap:

1. A generates nonce S and send hash (S) to B.
2. A locks its assets and makes a time setting: if A can receive S in 2X of time, the assets will be transferred to B; if not, the assets will be returned back to A.
3. After B verifies the lock and the time setting on A, B locks its assets and gives a time setting: if B receives S in X of time, the assets will be transferred to A; if not, the assets will be returned back to B.

4. A exposes S in X seconds, to ask for its assets from the contract of B.
5. B receives S, which allows B asks for its assets from the contract of A.



The atomicity of the mechanism can be verified. Suppose that A exposes S in X seconds, a window of X seconds at least can be provided for B to state its assets. A may have errors that delay the exposure of S, which causes a result that A cannot get the assets back. That is usually the fault of A, and it can be avoided easily. If A exposes S in X to 2X seconds, A cannot get its assets but B can, which is also A' s fault; if A exposes S after 2X seconds or even gives up the exposure, A and B will get their own assets back. If A does not lock its assets, B will not lock its assets as well. If B does not lock its assets (or fails to lock in appointed time), A can choose not to expose S. In that way, A can get its own assets back.

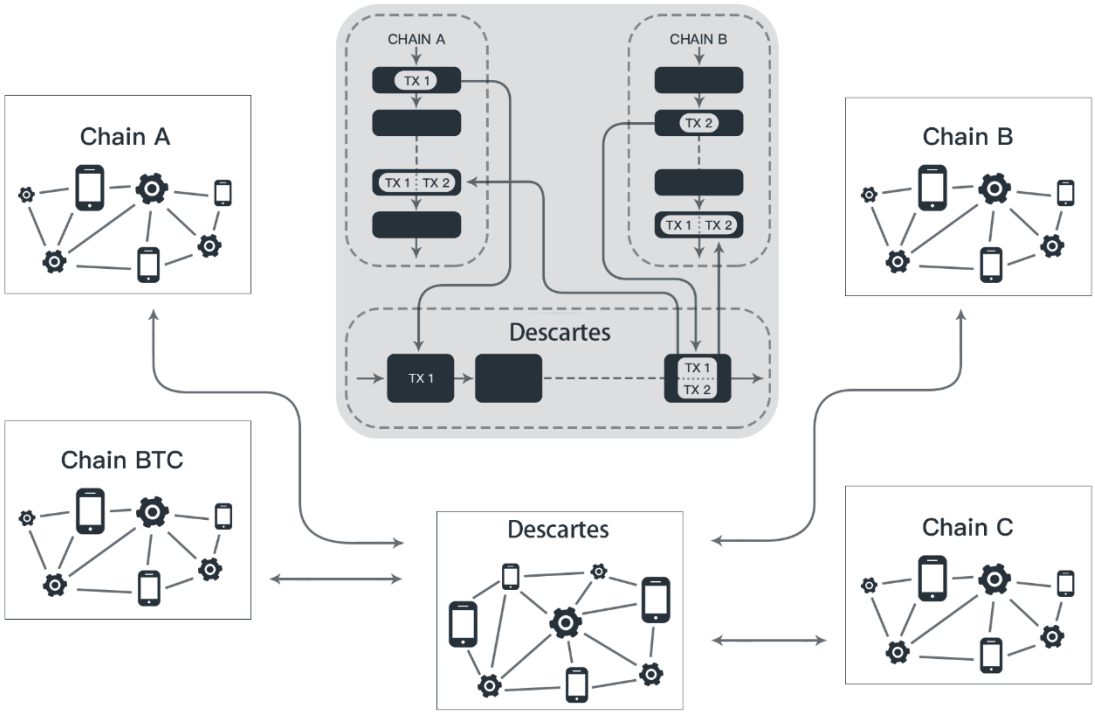
2.3.2 Descartes Cross-Chain Solutions

To transfer the assets of traditional financial world to chains, cross-chain connectivity is of great importance, but it is not easy to realize, because every chain has its own network protocol, communication standard and consensus, which are still in the process of improvement. In hope of transferring assets between chains, we have tried relay system, notary technology, atomic swap, hashlock and other technologies, with a purpose of finding a centralized solution to realize the Pareto optimality of developers, users, miners and other parties. All researches point to one direction — how to safely authorize multiple trustless nodes to jointly operate one digital asset account. That is the core of Descartes Chain technology.

- guaranteeing digital asset security
- supporting cross-chain smart contract programming
- high robustness
- immediate processing and response of large-scale financial applications
- no increase in the computation pressure of miners, with the satisfaction of the system scale expansion
- cross-chain asset transformation
- cross-chain transactions
- separation of ownership and right of use

According to the requirements mentioned above, Descartes research and development team has gathered most advanced theories of the academic world, and it has developed the distributed private key generation and control technology, which we call DKSC (Distributed Key Secure Cluster). The locked accounts on original chains generated by DKSC don’ t need two-way peg, and they don’ t need script extender to recognize and verify SPV proof on original chains. Transaction data are sent back to the original blockchain network, in a legal format of the communication standard and network protocols, to realize the combining completion of cross-chain transaction core process and computation in Descartes Chain. It is not necessary to make any change in the mechanism of original chains. Therefore, all public blockchains,

private blockchains and consortium blockchains can connect with Descartes Chain with less limits, which will reduce cross-chain transaction costs and flexibly map the assets on every chain.



Distributed Key Secure Cluster (DKSC) can safely transfer the control right of the digital assets held by individuals and organizations to a completely decentralized blockchain network. The generation and the storage of secret key is distributed, so no node can obtain a complete secret key, which is guarantee for the security of digital asset right of control and digital assets. The operation of releasing the right of control is called Release. All digital assets controlled by secret keys can realize distributed control and mapping through Release. The operation of recycling the right of control is called Recycle, a reverse operation of Release. Recycle can help users take the right of control back and terminate the asset mapping.

2.3.3 Key Technologies

Highly Connective Network Cluster Algorithm

The physical layer of blockchains is a P2P distributed network. Its communication feature is aperiodicity, and any single node is permitted to broadcast on the whole network, which brings out two problems: one is efficiency problem – time consuming, energy dissipation and low efficiency; the other one is security problem – how to know a node is honest or malicious.

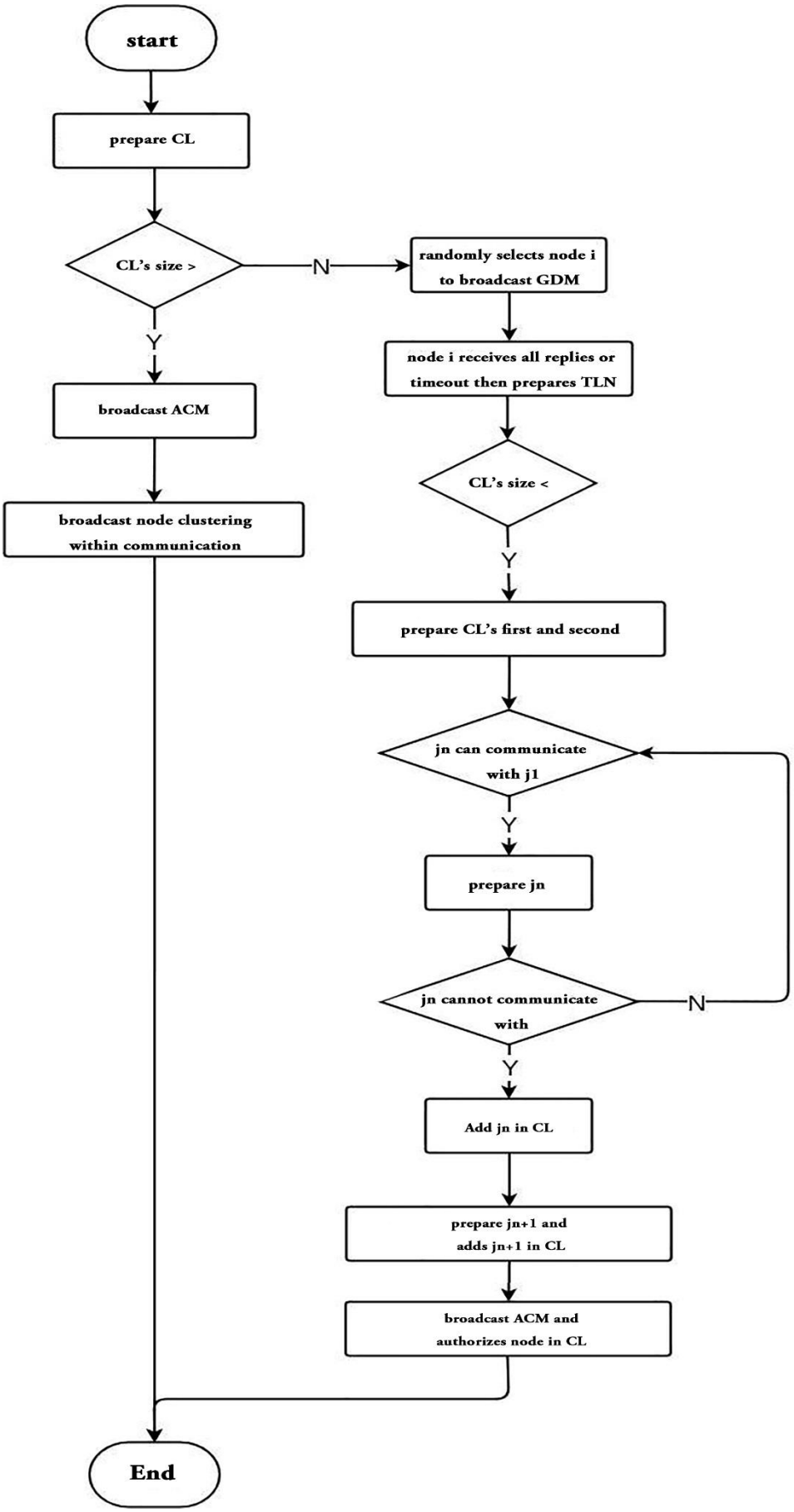
Descartes Chain, distinguished from traditional network communication methods, uses the inherent characteristics of triangle to ensure the connectivity of cluster algorithm. By the algorithm, a highly connective backbone network will be formed, which will reduce the routing list cost and the communication cost of the whole network.

In the implement process, nodes will be assigned by the system before being deployed. Network messages trigger the initialization process by broadcast, and the whole network is initialized, which will trigger the cluster algorithm. When a node exists over a period of time and the number of neighbor cluster headers hasn’ t reached to three, the node will supplement nodes and request to cluster, to ensure any non-cluster-header node in the whole network will be in the communication range of those three cluster headers. Therefore, the highly connective backbone network will be built up. As the time changes, cluster header node will not consume much energy. The technology can realize no increase in the computation pressure of miner nodes, with the satisfaction of the system scale expansion.

The core algorithm is shown as follows and some symbols used in the algorithm are shown in table 1 (i represents the node broadcasting GCM messages):

Symbol	Definition
LN(i)	neighbor node list of i
LN(I,j)	Public neighbor node of i and j
OM(I,j)=LN(I,j)	Redundancy of i and j
GCM	Clustering message
ACM	Broadcast clustering message
CL	Clustered sequence
TLN	Temporary list of neighbors

```
Cluster Algorithm:
1) prepares CL and if CL' s size > 5 broadcast ACM  then exit
2) Node i broadcast the GCM
3) receives all replies or timeout then pre-
pares TLN
4) if CL' s size < 2 then prepares CL' s first and second node
5)     While(jn can communicate with j1)
6)          Prepares jn
7)          If jn cannot communicate with
8)               add jn into CL
9)          end if
10)    end while
11)    prepares jn+1 and add jn+1 into CL
12)    broadcasts ACM  and authorities permission to node in CL
13) end if
```

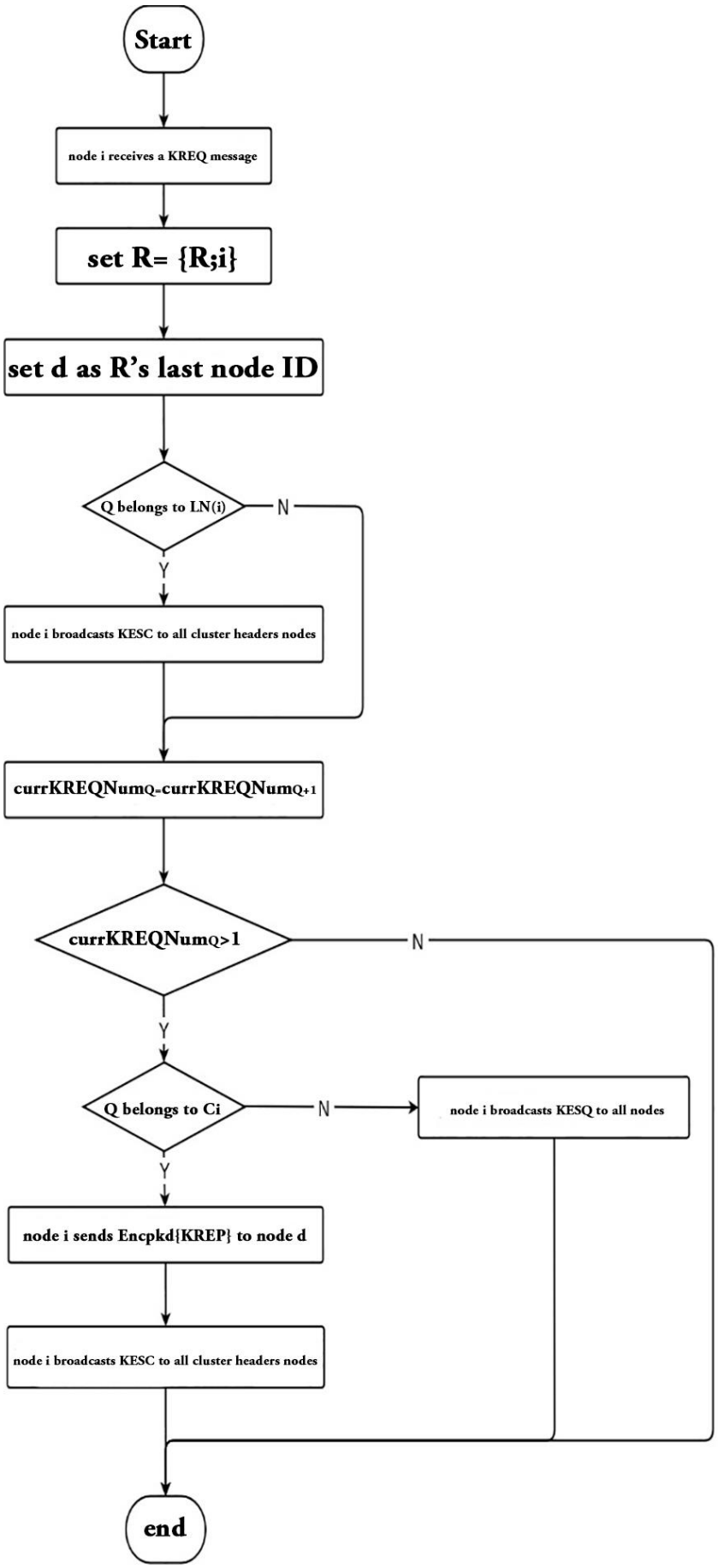

start
prepare CL
CL's size >
N
randomly selects node i to broadcast GDM
Y
broadcast ACM
node i receives all replies or timeout then prepares TLN
broadcast node clustering within communication
CL's size <
Y
prepare CL's first and second
jn can communicate with j1
Y
prepare jn
jn cannot communicate with
N
Y
Add jn in CL
prepare jn+1 and adds jn+1 in CL
broadcast ACM and authorizes node in CL
End

DKSCA (Distributed Key Secure Cluster Algorithm)

For public blockchains are open to others, the possibility cannot be excluded that some malicious nodes may join in the network. Descartes Chain adopts a secure cluster algorithm, to realize the generation and the management of distributed secret keys. The nodes joining in the network need to pass the system verification. The realization process is as follows: after the formation of all cluster headers, the broadcast cluster messages contain their own public keys. The nodes that receive the messages will store the public keys, to ensure nodes in the whole network can have corresponding public keys of cluster header nodes near to them. Before deploy the system, randomly pick some public keys from the key pool for storage.

The verification of nodes is divided into four phases; only when two broadcast messages are received, will nodes process and transmit them. Protocols initiate the broadcast of verification messages by cluster header nodes. The three nearby intercommunicating cluster header nodes initiate the protocols, which leads to the phase of secret key search. Secret keys are found in the network, and the keys return by the paths they come, which leads to the phase of response. When the protocols initiate the signature verification by cluster header nodes and satisfy the number of the initially set threshold value, the verification messages of secret keys will be broadcast. The protocols get into the phase of verification. Through the entire verification of the protocols, if anything exceptional happens, the protocols will go to the phase of termination, to avoid the attacks of malicious nodes.

The core algorithm is shown as follows and some symbols used in the algorithm are shown in table 2:


Start
node i receives a KREQ message
set R= {R;i}
set d as R's last node ID
Q belongs to LN(i)
N
Y
node i broadcasts KESC to all cluster headers nodes
currKREQNumQ-currKREQNumQ+1
currKREQNumQ>1
N
Y
Q belongs to Ci
N
node i broadcasts KESQ to all nodes
Y
node i sends Encpkd{KREP} to node d
node i broadcasts KESC to all cluster headers nodes
end

Symbol	Definition
Ski	private key of node i
Pki	Public key of node i
Ci	public key list stored in nodes
R	route of message transmission
(m)SK	use SK signature on message m
EncPK(m)	use public key encryption on message m
cunKREQNumQ	the message number of KREQ about Q
SSN	protocol initiates cluster header node
S	request for node
Q	request for public key ID

DKSCA (Distributed Key Secure Cluster Algorithm):

```
1)  Node i receives a KREQ message
2)  d ← lastnodeIDinRandR←{R;i}
3)  if Q ∈ LN(i) then
4)        Node i radios KESC to all Cluster
Heads Nodes
5)        exit
6)  end if
7)  currKREQNumQ ← currKREQNumQ +1
8)  if currKREQNumQ > 1 then
9)        if Q ∈ Ci then
10)             Node i sends EncPKd{KREP} to node d
11)             Node i radios KREQ to all Cluster Heads Nodes
12)       else
13)          Node i radios KREQ to all nodes
14)       end if
15)  end if
```

Network Security

The main threat for Network Security is the attacks from malicious nodes. No matter attackers know the information of secret key pool or not, they have to know the IDs of normal nodes and the corresponding private key information of the IDs, if they want to pass the verification of cluster header nodes. Because private keys are not directly related to IDs and all the attackers know is no more than the public key information in the attacks, there is no way to calculate public keys to generate private keys. Therefore, it is guaranteed that attackers cannot obtain private keys though public keys, which can avoid attackers from fabricating nodes with specific IDs for communications.

Application Security

The management of digital assets is actually the management of private keys. Taking Bitcoin as example, a private key is essentially a nonce. The private key algorithm of Bitcoin is to operate SHA256 algorithm on a nonce and generates a 256-bit nonce. Add version number in front of the nonce; add compression mark and additional check code after the nonce; then, code it into Base58 and a private key in WIF (Wallet import Format) is obtained. Public keys are generated by private keys through elliptic curve algorithm, and the address of Bitcoin is generated by hash function (RPIEMD+SHA).

Whether the privet key keepers are individuals or exchanges, privet keys are always completely stored in a place, where might be users' computer hard disk, a third-party server that provides wallet applications

or an exchange server. Once hackers attack, the privet keys will be exposed, lost and defalcated by third parties, all of which will cause losses for users.

DKSC not only solves the big problem of cross-chain communication, but also improves the security of digital assets, which is shown in two aspects:

- Sharding of Secret Key
  An entire key is divided into several parts, and each part is a shard. After sharding, a secret key doesn’ t need any reassembly from its generation to its storage and usage. Therefore, no complete private key will appear in any place at any time.
- Distributed Data Store (DDS)
  After sharding, storing private keys on different nodes in a decentralized network is called distributed data store. In distributed data store, every node only contacts with a shard in a secret key; any single node or some nodes cannot reassemble a secret key by several shards, which reduce the risk of secret key leakage. Distributed data store can completely avoid any malicious misappropriation by third parties.

2.3.4 Mixing Consensus

PoW Consensus represented by Bitcoin is simple and efficient, but there are two big problems:

- Long Delay
  The average confirmation time of every transaction lasts for ten minutes, and the maximum speed for supporting concurrent transactions is two bits per second.
- Waste of Resources
  Any consensus based on permissionless models needs extra hash rates to insure the security. Before the deadline of dispatch, the

confirmation of every Bitcoin transaction consumes six dollars (USD) of electricity in average.

Hybrid Consensus adopted by Descartes Chain is a mixing consensus, which can solve the two problems mentioned above:

- High-Speed Processing
  The transaction speed on blockchains depends on network transmission speed, without any visible limit.
- Economical Quality
- Transaction confirmation is completed by a group of nodes, with low energy consumption.

The mixing consensus of Descartes Chain is a fusion of PoW and PoS, operating in layers. The physical layer (the bottom layer) of PoS miners is in charge of the transaction information confirmation and the generation of blocks. The top layer of PoS miners is responsible for packing transaction records and submitting them to PoS miners for processing.
Every node will verify itself belonging to PoW miners or PoS miners, by operating a random algorithm. The process is automatically operated once per 24 hours, without any interference of the system, to make sure the election mechanism is unprejudiced and trustable. All PoS miners can realize the transaction information processing of the whole network by cluster technology; the transaction information processed by each cluster header is not intersecting, which largely improves the processing capacity of Descartes Chain and provides fundamental supports for the deployment of large-scale financial applications.

2.3.5 Anti-ASIC Algorithm

The operation of blockchain systems relies on miners. Miners verify transaction records; they generate and store all blocks; they also reach a consensus on the written-in blocks. The essence of mining is to operate “incomplete hash function of preimage puzzles” by chip technology.

The result of the algorithm is not a value but a block. The result of chip operation lands in the block, which is regarded as a success of mining. When numerous chips participate in the operation, success of mining will become probabilistic. Generally, in a unit time, the probability of getting the results matching the condition is directly proportional to the hash rates contributed by chips.

The first generation of miners finished mining operations on average computers, which means CPUs were used for operations. CPU processes problems in a linear model, so miners can only simply try all nonce numbers in the linear model. Mining by CPUs on average computers has been unprofitable now.

The second-generation miners realized the unprofitability of mining by CPU, and they started mining by graphics cards or GPUs. GPU is of high throughput and highly concurrent processing capacity, which is very beneficial to mining. There is a great amount of concurrent processing in hash decryption operation, because different nonce numbers are needed to be calculated to have many hash rates at the same time. However, mining by GPU has many disadvantages, such as lack of cooling treatment equipment and high energy consumption of GPU, which will lead to purchasing specific main boards carrying many graphics cards at a high price.

The third-generation miners appeared in 2011, which are called Field-Programmable Gate Arrays (FPGA). The operation theory of FPGA is to enable users to do on-site debugging or modify hardware arguments while pursuing the optimum performances of custom hardware. By contrast, common hardware is already designed before delivery. After leaving the factory, the customized hardware cannot be changed and will run the same operations forever. FPGA has more good performances than GPU and it is easier to cool down, but FPGA was not widely used for a long time in the history of miners, for its high operation standard and difficult accesses to purchasing.

Nowadays, the mining market is mainly led by Application-Specific Integrated Circuit (ASIC). Those IC chips are designed, produced and optimized for only one purpose – mining. The appearance of ASIC transferred mining from individuals to big professional mining centers. To maintain their competition advantages, those big mining companies purchased a great number of latest ASIC miners with high performances, not miners directly sold to individuals.

The existing cryptocurrencies based on PoW Consensus are already away from common users. Only people who buy specialized ASIC miners can participating in the mining and get rewards, which results in the situation that "late comers go to the top" or the "capital-dominated" situation. From a long run, that is harmful to the spread and development of digital currencies. In hope of changing the situation, Descartes Chain has designed a set of anti-ASIC algorithms. To attract common users to participate in mining, a big investment on hardware is not necessary, which means satisfying rewards and avoidance of hardware arms race are needed. It is meaningless for both project parties and participants to put in a big number of money into the competition of hash rate upgrading.

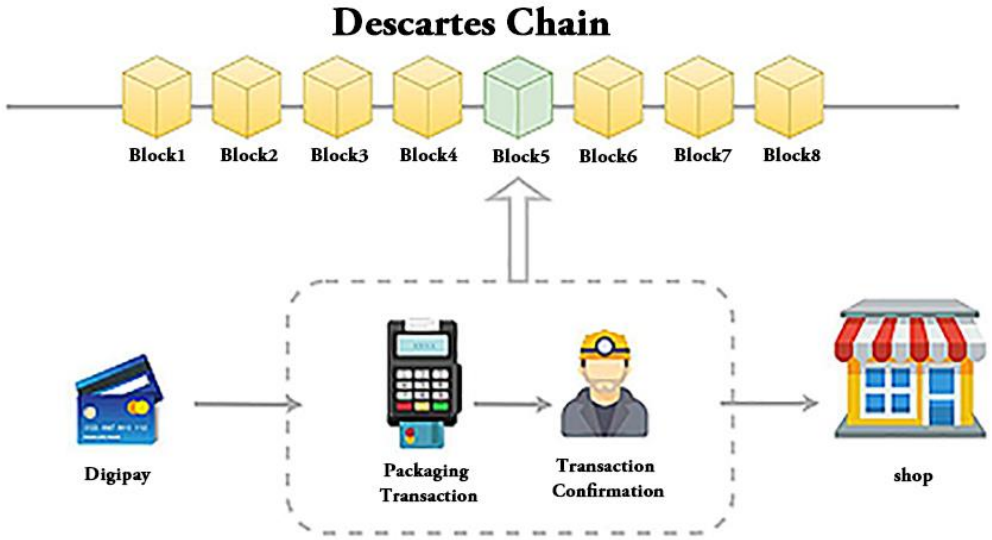
The existing puzzles algorithms (such as SHA-256), only occupying 256 bits, can be easily put into the register of CPU, which builds up the base for designing specialized mining equipment. On the contrary, if the computation modules are expanded and become too big to install in CPU, a great amount of memory is necessary to help with the computation. This method is called Memory-Hard Puzzles. This kind of puzzles algorithms only need comparatively simple hash rates but a large amount of memory, which indicates the increasing speed of puzzle costs will maintain at a comparatively low level, same as the increase of memory speed. There is no worry that some individual will suddenly have over 51% hash rate and attack the whole network.

2.4 Applications

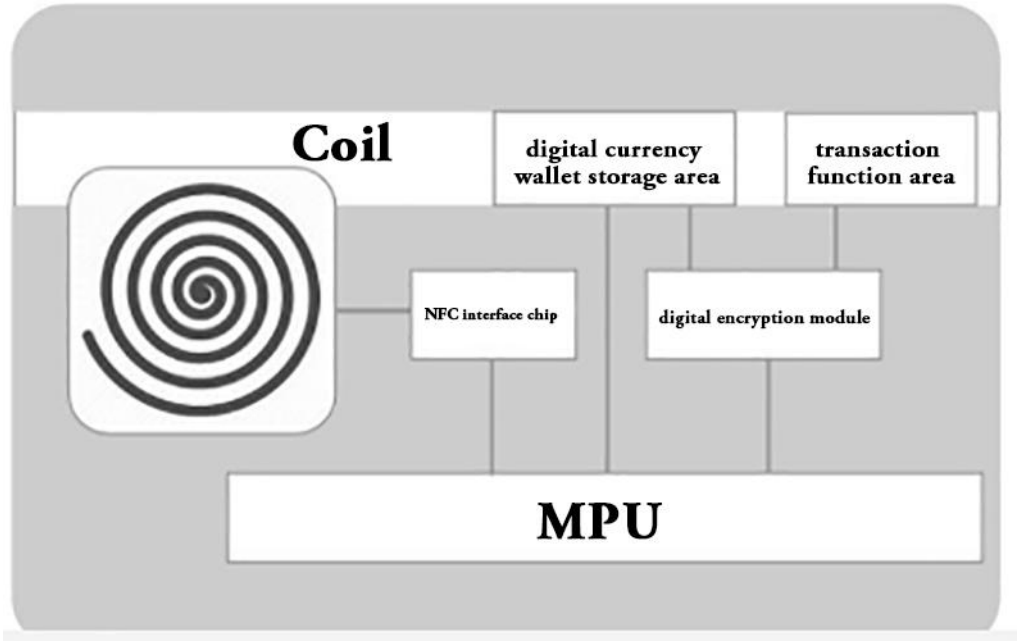
2.4.1 Convenient Payment

Representative Application —— Digipay Card

An increasing number of merchants are accepting using digital assets (such as Bitcoin) as a way of payment. For users, they are gradually getting used to or even rely on electronic currencies. Bank card is a tool for user identification and transaction participation. Digital currencies are alternatives of electronic currencies, so Descartes Chain brings out Digital Currency Payment Card (Digipay Card), which is a blockchain financial service with a perfect combination of digital assets and bank cards.



User of Descartes Chain, only with Digipay Card, can enjoy pay-by-card consumption in any place around the world. The card reader of a merchant, a cluster node (a PoS miner), can process the transaction immediately. It can pack all transaction information and submit to the closest PoW miner. The miner will add the transaction information into the latest generated block information and complete verification of it, all of which will be done in one second.



The image above is the internal structure of Descartes Digipay Card, including coils, NFC interface chip, digital encrypted chip, MPU microprocessor and memory module of digital currency.

Users' private keys of digital asset are stored in Digipay Card, so the security of Digipay Card is of great significance. Common magnetic bank cards are of extremely low security. A bank clerk can make a copy card by copying the information of a bank card. In recent years, banks have installed EMV chips in debit cards and credit cards, in hope of providing extra security protection for pay-by-card transactions. In recent Black Hat Conferences, NCR security researchers have proved that EWV chip cards can be forged as easily as magnetic cards.

Digipay Card adopts MPU encryption+ ASIC encryption, where data are stored in specialized storage modules in ciphertext. Even when attackers download data from data bus, they will not find any private key or any other sensitive information. The protection can efficiently prevent hacking and semi-hacking attacks. The bus of every cards has different encryption keys, so even when hackers can completely decrypt the keys, they cannot generate chips with the same key. The chip of every Digipay Card has its own exclusive ID number, so it is no possible to buy a Digipay

Card with the same ID number. On the aspect of circuit design, Digipay Card will adopt the logic of ASIC to design its standard module structures, such as decoders and register files. The designing method is mixed logic design. Mixed logic makes it impossible for dishonest users to manually find signals or nodes to obtain the information of payment cards and conduct physical attacks, which has largely improved the performance and the security of MPU core. The card reader of Digipay Card uses DKSCA algorithm to realize end-to-end encryption; any transaction information from any forged reader or maliciously tampered reader will not be confirmed. The details of the theory have been thoroughly explained in *2.3.2 Key Technologies*.

Digipay Card adopts NFC identification technology. Users can conveniently recharge the card on phones that support NFC technology; set up double verifications (fingerprint verification and face identification) and add mainstream digital assets in the card. No need for more digital currency wallets. It can realize the dream of traveling all over the world with only one card in hand. Payment and account transfer can be confirmed in just a few seconds. Cash return in every consumption, and discount in every payment.

2.4.2 Credit and Loan & Debit and Credit

Representative Application —— Credit-Chain Loan

As digital currencies are becoming as more widely used transaction media and more important carriers of value storage, it is an avoidable trend to create new value and obtain relative earnings by digital currencies, such as investments of Bitcoin in "mining" and other blockchain projects (like ICO). With the extension of digital currency applications, there are more fields and opportunities of direct (no need for exchange of fiat currencies and the earnings of investments can be

evaluated by digital currencies.) investments by digital currencies. More digital currencies are needed by individuals who create value by digital currencies; possessors of digital currencies need to preserve and increase the value of their currencies. Therefore, there will be increasing demands for loan services of digital currencies. Descartes Chain supports organizations or individuals with credit and financial capacity as supplying intermediaries of digital currencies, to finish deposits and loans businesses. Take Ether as example. Intermediaries use the smart contract on Descartes Chain to build up deposit applications and set interests; the deposit party of Ether, through cross-chain mechanism, transfers the Ether coins on Ethereum to the corresponding address of the smart contract on Descartes Chain. The smart deposit contract will release the corresponding token of the deposit (token on Descartes Chain, similar to bank deposit receipt) into the user account on Descartes Chain. The smart contract will automatically calculate the interest rate. When the user (the deposit party) needs to withdraw the deposit from Ethereum, the deposit can be returned back to the intermediary address through the token. The smart contract will conduct a cross-chain transaction and return the corresponding Ether coins to the original user account, by unlocking them from the original chains. Compared to traditional mode, the outstanding advantage of the whole operation is that the deposit reserve (the locked original-chain assets corresponding to the intermediary address) of the deposits and loans intermediary is transparent, which means the deposit party can know the condition of the reserve at any time.

2.4.3 Universal Circulation or Exchange During Transactions

Representative Application —— Descartes Coin

The circulation and exchange of digital currencies now mainly rely on

centralized exchanges and the intermediaries of curb exchanges. All transactions are based on the trust for exchanges and intermediaries. After various currencies put into Descartes Chain, exchanges or intermediaries can realize multi-currency competitive price transactions and peer-to-peer curb exchanges by smart contracts. A transaction mechanism of privacy protection will be provided by Descartes Chain, to give an overall support for transactions in need of privacy protection. The digital currencies without privacy protection are led into Descartes Chain, and then private transactions are initiated on Descartes Chain. The digital currencies will be returned back to the original chains. To some extent, the original chains are under privacy protection by cutting off the money tracking routes. This kind of situation is similar to the mixing mode happened before.

2.4.4 Artificial Intelligence

Representative Application —— Smart Computation Nest

Artificial intelligence is like a monster that needs to be fed by a mass of data, so the source, the quality and the privacy of data are problems to be solved. The smart contracts on blockchains can realize privacy protection by the physical isolation between data owners and data users. For hash rate demands, artificial intelligence (AI) high performance servers (HPS) are very costly; the update of servers is a huge cost for all AI enterprises, because the updating speed of servers is very fast. Therefore, through blockchain technology, the hash rate cost in the industry can be reduced and the computation efficiency can be improved, to reach the goal of reducing the business venturing limits for AI enterprises.

For artificial intelligence, Descartes Chain is aiming at the establishment of a virtuous ecosystem by blockchains and special technical methods, to promote the sharing of resources and to motivate more people to participate in the development and landing of intelligent applications; it accelerates the development of AI in a trustable and reliable environment;

based on private data, it provides more specific and customized services for every individual.

Smart Computation Nest is an AI computation platform driven by blockchain technology, with a main purpose to help global AI enterprises with the tough problems in the industry: reduce in hash rate cost and data protection. It is designed to provide a shared blockchain platform for more complicated AI applications, which enables date resource parties, application parties, operation platform parties and users to freely publish and use their own resources and applications on the blockchain.

2.4.5 Assets Management

Representative Application —— Digi-Up Digital Assets Platform

The trend is seen that traditional assets, in form of consortium blockchain, will be mapped on blockchains, such as commercial papers, commercial points, future right of earnings and receivables. More financial assets will be recorded in form of a distributed ledger based on consortium blockchains. After those consortium blockchains are connected with Descartes Chain, they will become suppliers of financial assets, which can be purchased by digital currencies from digital currency possessors. Compared to traditional bank businesses, that is similar to purchasing financial products in banks. The difference from banks is more participation of intermediary organizations or the direct asset financing of asset possessors.

ICO (Initial Coin Offering) now has become an important method of crowdfunding in the field of blockchain, and the trend is spreading to non-blockchain fields. An increasing number of projects, especially projects based on Ethereum, directly operate ICO by smart contracts. The whole process is more transparent and fairer, but the crowdfunding can only be operated through Ether, which brings inconvenience to investors who possess other digital currencies. On the basis of the ICO platform

developed by Descartes Chain or individual ICO projects, publishers can support multi-currency investments while following smart contracts. Investors can invest more conveniently by tokens of Bitcoin, Ethereum and any other blockchain connected with Descartes Chain. Initiators can further manage their own raised assets in an easier way; when projects landing online, new blockchains can easily complete the exchange between their crowdfunding amount and original coins by cross-chain mechanism, as long as they are connected with Descartes Chain. The application of Descartes Chain can lead us into an age of launching digital rights and interests fully based on blockchains.

Digi-up is a ground-breaking financial ecosystem of blockchains, which defines the protocols of financial products based on cryptocurrencies. There are smart contracts, borderless leverage, financial products (such as constant returns, market indexes, binary options, futures and leverage ETF) on the platform. Digi-up ecosystem provides an overall financial market for investors and is full of financial products, services and applications that can satisfy their demands.

2.4.6 Insurance Contract

Representative Application —— Collective Security Protection

There are many problems in the leading companies of traditional insurance industry. Over 70% of the insurance premium paid by users has not been used for compensation but for a series of unnecessary costs, such as the profits of the companies and the service commission. If those centralized business entities can be eliminated, the users can spend less money or obtain more services and compensation while avoiding the imparity clauses of insurance companies.

The decentralized mutual guarantee and insurance contract platform, based on blockchain technology, has established a smart insurance contract market, replacing the traditional centralized insurance mode by

a disintermediated mutual insurance mode. On the platform, anyone in the world can have a smart contract support at a very low cost. It can realize mutual guarantee, mutual offset of risks, efficient reduce in the operation costs of insurance and guarantee products as well as higher security of assets. It can support applicants for mutual aids with money to treat serious diseases, and the users will share the expenses. The users on the platform are both helpers and beneficiaries.

2.4.7 Decentralized Exchanges

Representative Application —— Coin Fusion Exchange

The fungible digital assets are created by the general ledger of decentralized transactions, which is protected by DPoS. It has a verification speed in seconds. During transactions, the fluctuation in currency prices changes constantly; currency-to-currency transaction is like swimming in the sea, non-stop. The assets can marketize and anchor the value of any item, such as US dollar, gold and gas, etc. Like all DACs, Coin Fusion enjoys the stock rights transferred between users (similar to Bitcoin); it has implemented a business mode similar to banks or brokerage companies; it is distinguished from traditional centralized exchanges, avoiding a series of problems, such as high cost, bad security and malicious behaviors of exchanges, etc.

Processes and Plans

June, 2017

The project and development teams of Descartes Chain were set up and the projects of Descartes Chain stepped into the stage of planning and preparation.

March 21st, 2018

Tests for modules of smart contracts; the Asian-Pacific project operation and development team was built up to focus on the Asian-Pacific market

May 3rd, 2018

The only agency of Descartes Chain in Asian-Pacific area was settled in Changsha, influencing the whole area; the test for Descartes Chain V1.0 was started.

June 26th, 2018

The international website of Descartes Chain was launched online; the intelligent ecosystem of the project /white paper was published; the worldwide advance sale for some open source of Descartes Chain and mining rigs was started.

Late September, 2018

Token of Descartes Chain will be issued in international digital currency exchanges (such as Huobi, A.T.Xchange, Bter, etc.).

March, 2019

Descartes Blockchain Browser, Descartes Blockchain Wallet and Digital Currency Online Store will be launched; Descartes online application matrix will be initially completed.

October, 2019

The first offline application of Descartes Chain "Digipay Card" will be developed; the applications for global vendors will be launched and global stateless digital currency circulation and exchange will be realized.

December, 2019

The connection of 100 sidechains will be finished; the entire intelligent ecosystem structure will be completed.

October 2nd, 2017

Tests for base modules of Descartes Chain and tests for anti-fusion of ASIC technology were finished.

May 3rd, 2018

The financial service license in Ukraine was examined and approved; Ukraine Gold Exchange Ltd. was established officially.

May 30th, 2018

Descartes software and hardware products were officially in the stage of research, development and production; the closed tests for the official website of Descartes Chain was operated.

September, 2018

The development of Descartes Chain mining rigs will be finished and the mining rigs will be launched for sales; Descartes Chain Wallet will be launched simultaneously.

January, 2019

The establishment of 100 Descartes genesis blocks will be completed; The open source code of main Descartes Chain will be published on its official website.

May, 2019

Descartes digital platform will be in the stage of development; Descartes Decentralized Exchange will be officially launched online.

November, 2019

Descartes digital platform will be tested online; the transaction pair BTC/ETH will be open; Descartes digital currency credit and loan service will be started.

Qualifications


ВИПИСКА
з Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "ДЖІНБІ ДЕЙТЕ АССЕТС ТЕХНОЛОДЖІ ЛІМІТЕД"

Ідентифікаційний код юридичної особи:
42173455

Місцезнаходження юридичної особи:
03065, М.КИЇВ, БУЛЬВАР ВАЦЛАВА ГАВЕЛА/АКАДЕМІКА КАБЛУКОВА, БУДИНОК 51/16

Дата та номер запису в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань:
01.06.2018, 1 073 102 0000 037233

Прізвище, ім'я та по батькові осіб, які мають право вчиняти юридичні дії від імені юридичної особи без довіреності, у тому числі підписувати договори, та наявність обмежень щодо представництва від імені юридичної особи або фізичної особи-підприємця:
КУЗНЕЦОВ ІГОР МИКОЛАЙОВИЧ - керівник

Код: 314464085065

ОПИС
документів, що надаються юридичною особою державному реєстратору для проведення реєстраційної дії "Державна реєстрація новоутвореної шляхом заснування юридичної особи"

Для проведення реєстраційної дії "Державна реєстрація новоутвореної шляхом заснування юридичної особи" юридична особа **ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "ДЖІНБІ ДЕЙТЕ АССЕТС ТЕХНОЛОДЖІ ЛІМІТЕД"** надала наступні документи:

1. Реєстраційна картка на проведення державної реєстрації юридичної особи, утвореної шляхом заснування нової юридичної особи.
2. Рішення засновників або уповноваженого ним органу про створення юридичної особи (Примірник оригіналу).
3. Статут.
4. Документ, що засвідчує повноваження уповноваженої особи.

МЕЛЬНИК І.В.

Заявник: (прізвище, ініціали заявника) (дата) (підпис)

Фактична дата формування опису: 31.05.2018

Стор. 1 з 1

Ukraine

Approved by Ministry of Finance and on Records of Ministry of Justice

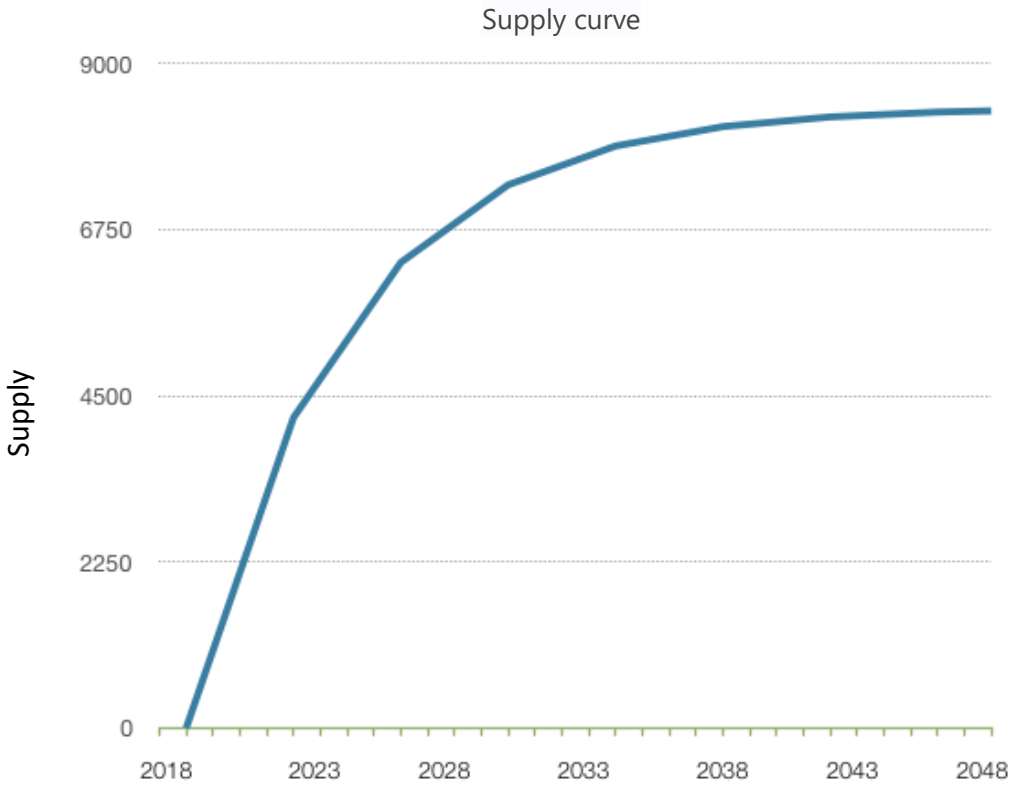
First Blockchain Company with Ukrainian Blockchain Financial License in the World

In 2018, Ukraine put forward an act to define cryptocurrencies (including Bitcoin) as legal assets, which can be used in exchanging goods and services. The first part of the act gives definitions of cryptocurrency, exchange, transaction, blockchain, cryptocurrency owner and miner. It is proposed in the act that the owners of encrypted currencies have the choice to decide how to deal with their cryptocurrencies, including exchanging other cryptocurrencies, fiat currencies or goods and services.

In January 2018, National Bank of Ukraine mentioned that the digital version of its national currency would be taken into “consideration”. In May 2018, (SSMCS) declared that cryptocurrencies would be used as financial tools. Soon afterwards, relative laws were carried out to admit the legal position of digital assets in payment. Timur Khromaev, President of SSNCS, said that blockchains, Bitcoin, tokens and other technical solutions had become a part of Ukrainian financial market.

Till now, the entire Ukraine has only issued eight digital currency licenses. Only five projects have the honor to obtain those licenses, and Descartes Chain is one of them. The license is not only the admission from Ukrainian government for the efforts Descartes Chain made in the past few years but also the encouragement and expectation for the future development of Descartes Chain.

Token Publishing Plan



Publishing **126 million** of coins, **all produced by mining: 70% for reward to miners, 10% for Descartes Foundation, 15% for operation cost, 5% for research & development cost.**

Risks

Policy Risk: At present, the supervisory policies for blockchain projects and swap financing are not specific and clear, and there is a possibility that certain policies might cause losses of participants. Among the market risks, if the whole value of digital asset market is overestimated, the investment risk will grow bigger. The participants will have high expectations for the increase of swaps, and those expectations might be too high to be realized.

Risk inside Team: Descartes Chain has gathered a talented team full of vitality and strength, attracting senior practitioners of blockchains and well experienced technical developers, etc. In its future development, it is possible that Descartes Chain may be negatively influenced by the absence of core team members and the conflicts inside the team.

Risk Between Teams: Nowadays, there are many technical teams and projects related to blockchain. In this field, there are many fierce competitions and a lot of operation pressure. Whether Descartes Chain can become an outstanding and widely recognized project among all those excellent ones, it depends on not only the ability of its team and plans but also the influence of many competitors and even some magnates in the market, where there is a possibility that Descartes Chain may need to confront with vicious competitions.

Technical Risk of the Project: Firstly, the construction of the project is based on cryptology algorithm, so the development of cryptology will bring potential risks of code cracking. Secondly, technologies, such as blockchains, distributed ledger, decentralization and tamper proof, support the development of core businesses, but Descartes Chain team cannot completely guarantee the landing of all technologies. Thirdly, during the update and adjustment process, there may be bugs, which can be mended by patches. However, the level of influence cannot be assured.

Security Risk: Talking of security, the capital of a single supporter is a small number; as supporters increase, the project requires a higher level of security guarantee for a bigger amount. Electronic tokens, anonymous and difficult to trace, can be easily used by criminals, or attacked by hackers, or involved with criminal acts, such as illegal asset transformation.

Disclaimer

The paper shall be regarded as information transmission for reference only. It shall not be regarded as any investment and transaction suggestion, instigation or invitation of the stocks or securities sold on Descartes Chain or in relative companies. This kind of invitations shall be made in form of confidential memorandum, and they shall accord with relative securities laws and other laws. Any content of the paper shall not be explained as any compulsive force of participating in swaps. Any behavior related to the white paper shall not be regarded as behaviors of participation in swaps, including the requests for copies of the paper or the sharing of the paper with others. Participation in swaps indicates the participants have already reached the legal age standard, with integrated civil capacity of conduct. All contracts between the participants and Descartes Chain shall be valid. All participants should sign the contracts voluntarily, and it is necessary for the participants to have a clear understanding of Descartes Chain before signing anything.

Descartes Chain team will continuously take rational attempts to make sure the information in the paper is authentic and accurate. During the research and development, Descartes Chain platform will be updated, including but not limited to platform mechanism, tokens and token mechanism as well as distribution of tokens. The content of the paper can be adjusted in a new version, in response to the progress made in the project. The team will release an updated content by publishing

announcements or a new-version white paper, etc. Participants must obtain the latest version of white paper to adjust their policies according to the updated content.

References

[1] S. Nakamoto, " Bitcoin: A peer-to-peer electronic cash system, [Online]. Available: https://bitcoin.org/bitcoin.pdf, 2008, accessed: 2018-01-22.

[2] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger, " [Online]. Available: http://gavwood.com/paper.pdf, 2014, accessed: 2017-01-22.

[3] Jonathan Katz and Chiu-Yuen Koo. On expected constant-round protocols for byzantine agreement. J. Comput. Syst. Sci., 75(2):91{112, February 2009.

[4] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[5] Alysson Neves Bessani, Jo~ ao Sousa, and Eduardo Ad lio Pelinson Alchieri. State machine replication for the masses with BFT-SMART. In 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2014, Atlanta, GA, USA, June 23-26, 2014, pages 355{362, 2014.

[6] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The Bitcoin Backbone Protocol: Analysis and Applications. Cryptology ePrint Archive, Report 2014/765, 2014.

[7] Ran Canetti and Jonathan Herzog. Universally composable symbolic security analysis. J. Cryptology, 24(1):83{147, 2011.

[8] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[10] Ronald L Rivest, Adi Shamir, and David A. Wagner. Time-lock puzzles and timed-release crypto. Technical Report MIT/LCS/TR-684, 1996. Also available as http://theory.lcs.mit.edu/ ~rivest/ publications.html.

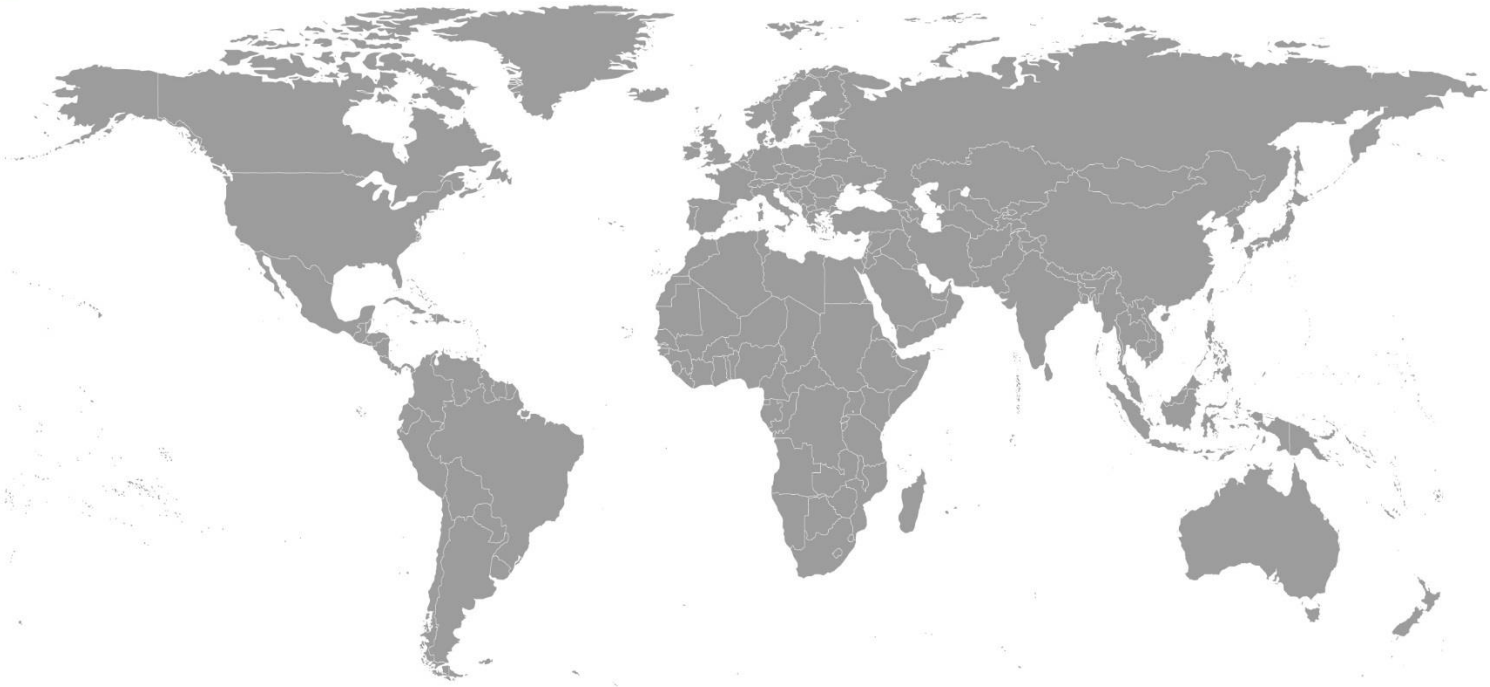
[11] Herman te Riele. Security of e-commerce threatened by 512-bit number factorization. Published at http: //www.cwi.nl/ ~kik/persb-UK.html, Aug 1999.

[12] Dennis Fisher. Experts debate risks to crypto, Mar 2002. Also available
as http://www.eweek.com/ article/0,3658,s=720&a=24663,00.asp.

[13] Drew Dean and Adam Stubblefield. Using cleint puzzles to protect tls. In Proceedings of the 10th USENIX Security Symposium, Aug 2001. Also available as http://www.cs.rice.edu/ ~astubble/papers.

[14] Hal Finney. Personal communication, Mar 2002.

[15] Thomas Boschloo. Personal communication, Mar 2002.



DESCARTES CHAIN

Opening a Brand-New Era of Digital Finance