VON CHAIN

WHITEPAPER

THE FLOEER OF LIFE
THE ORIGIN OF THE UNIVERSE

Content

ABSTRACT

THE FLOEER OF LIFE
THE ORIGIN OF THE UNIVERSE

Abstract

Blockchain may be the most promising and divergent technological and economic trend at the moment. It brings two brand-new basic functions of "value expression" and "value transfer" to the digital world. Its potential is showing up, but it is now in a stage of hazy and barbaric growth.

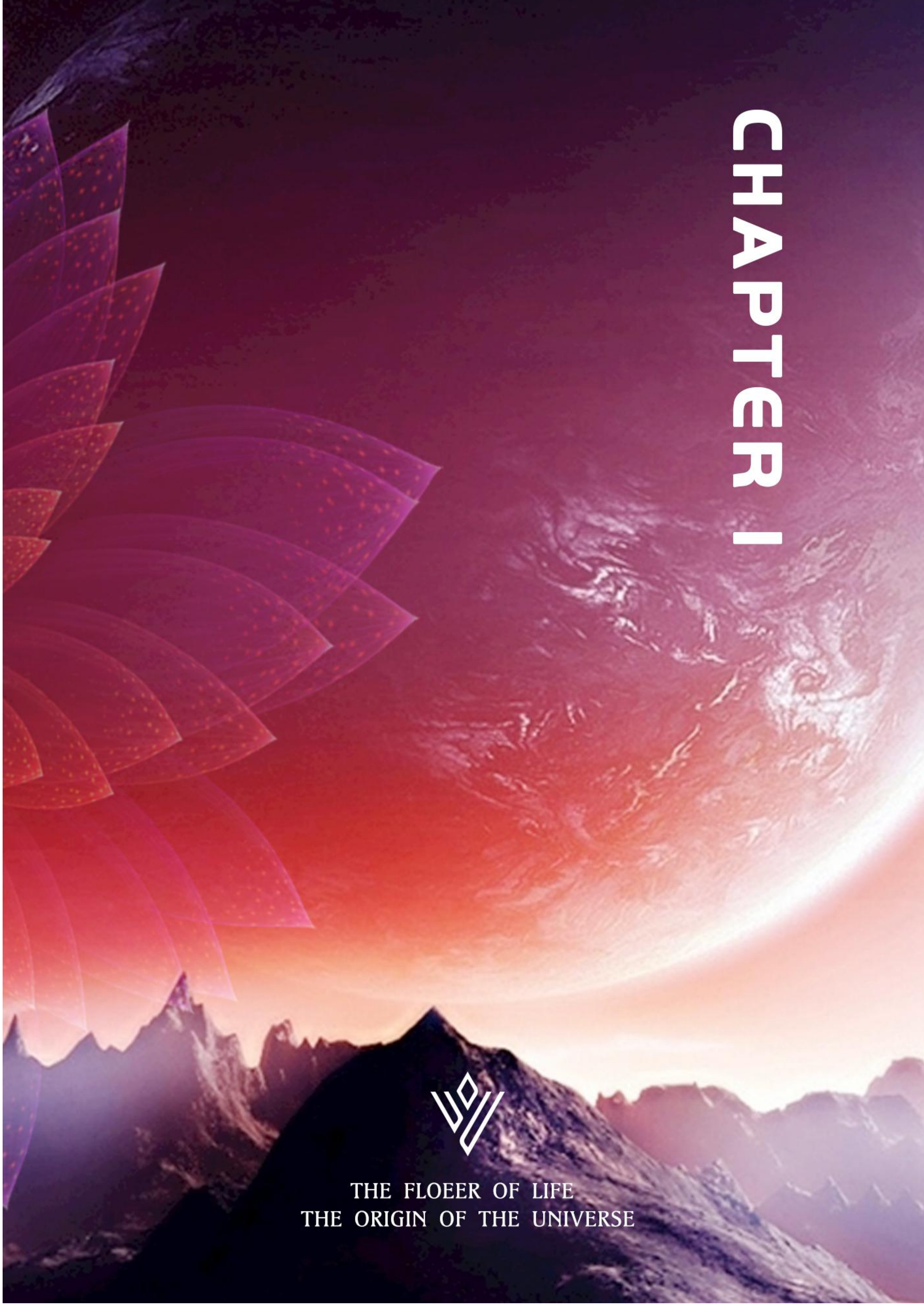
Comparing the development history of the Internet, the current blockchain may be equivalent to the Internet in 1994, that is, the period when the Internet has just entered the public eye, and that is also the period when the first wave of the Internet revolution was budding. Google, Amazon, Facebook, and even Apple, which now has a market value of over trillions, benefited from that moment.

After the advent of the blockchain, in comparison, we found that a key feature of information transmission makes the Internet very powerful, but there is a limitation that we have not paid special attention to before: the method of information transmission is replication. This feature allows us to rely on the assistance of a trusted third party when transferring value in the digital space. Those trusted third parties, that is, various centralized institutions, such as Amazon and PayPal.

Satoshi Nakamoto developed the underlying technology of blockchain in the Bitcoin system. When he tried to create new technologies to remove these credit intermediaries and let the network itself play the role of credit intermediaries, we began to discover that the current Internet This kind of credit intermediary does not necessarily exist.

After ten years of development, the Bitcoin system has demonstrated that value expression in the digital world can be decentralized, and value transfer can also be decentralized. As one of the underlying technologies of the Bitcoin system, blockchain technology has received increasing attention. Based on blockchain technology, we may establish a new transaction infrastructure that expresses and transfers value through the network itself.

Change is about to happen, and the future has come.



CHAPTER I

THE FLOEER OF LIFE
THE ORIGIN OF THE UNIVERSE

Chapter 1 - Decentralization is becoming the key to driving financial development technology

In the digital world on the Internet, people have designed various electronic cash or digital cash solutions. When writing the foreword for the book "Blockchain: Technology Driven Finance", Jeremy Clark collected about 100 Kind of payment system. He wrote: “The road to Bitcoin is full of countless failed attempts.” Among the various systems listed, he believes that only PayPal is known to the public. In all of these systems, there are intermediaries such as banks, payment institutions, and witnesses. How to create electronic cash that can be used in the digital world, it can be peer-to-peer, that is, person-to-person transactions, without any intermediary participation in the transaction? Decentralization has gradually become the key to driving financial development.

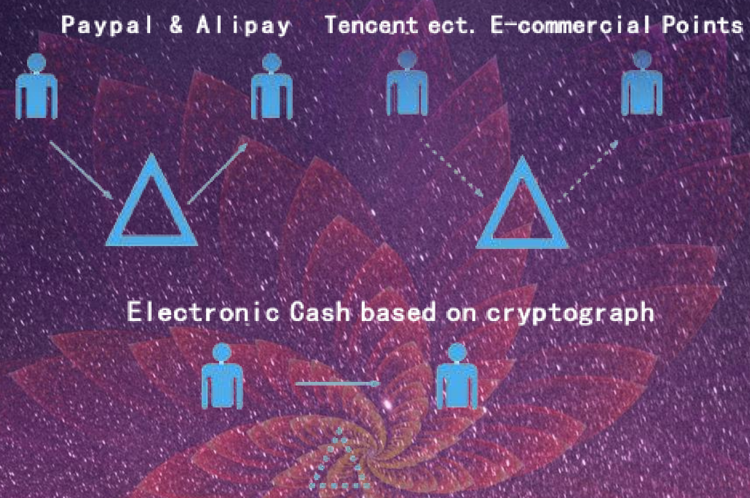
1.1 Looking at decentralization from the "currency" form of the digital world

We found that there have always been three forms of "currency" in the digital world:

1) Centralized online payment;

2) Centralized computer points or Internet points;

3) Decentralized electronic cash.


Paypal & Alipay
Tencent ect. E-commercial Points
Electronic Cash based on cryptograph

Picture 1: 3 types of CURRENCY in digital world

1.1.1 The first form: centralized online payment

Now, the mainstream payment systems widely used by Internet users are PayPal, Square, etc. These third-party online payment systems rely on the currency system and financial system in the physical world, and they provide users with payment and transfer services in the digital world. When using them, the money we use is legal currency in the physical world, such as U.S. dollars, Euros, Japanese yen, etc. The money is mapped from bank accounts to online payment accounts.

In the past, plastic cards such as credit cards and savings cards realized the digitization of paper currency cash, turning paper currency cash into digital cash in card accounts. Now, online payment systems transfer the functions of credit and debit cards to the digital world of the Internet.

In these systems, the electronic cash that corresponds to the legal currency is one-to-one, and only the "account" is changed, not the "currency". The role of these systems is to connect the physical world and the digital world on accounts and currencies.

These systems are centralized. The traditional financial system they rely on is centralized, and fiat currencies are issued by central banks of various countries. They themselves are completely centralized, with a single institution operating the online payment system. They play a centralized intermediary role in transactions, conduct account bookkeeping, and are the center of digital cash circulation among users. When two users transfer money, the online payment system acts as an intermediary role for a trusted third party, which is why it is called "centralized electronic cash."

1.1.2 The second form: centralized computer points or Internet points

Centralized Internet points/computer points refer to game points, game currency, airline miles, etc. They also had a more well-known name-virtual currency.

For example, users can purchase game currency from game companies with fiat currency, which can be used in game company products such as instant messaging tools, online games, music and literature, etc., to exchange for various online services.

For another example, in a game, users can pay to buy props, or they can win game currency through battle. The form and value of these props and game coins are different. It is difficult to determine the price and exchange in one game, and it is almost impossible to interchange between multiple games. Of course, game players can still find a way to exchange, and under certain conditions, they can even be converted back to legal currency.

Usually, they do not correspond to the legal currency of the physical world, but are issued centrally by commercial companies, and can only be used in a company's system. They are centralized, and their issuance and transactions are centralized.

1.1.3 The third form: decentralized electronic cash

In addition to these two mainstreams, there has always been another exploration: Can you create a completely decentralized peer-to-peer electronic cash? The ultimate assumption is that in the digital world, currency issuance and transactions do not require the intervention of a centralized institution, and are executed automatically by computers: when issuance, there is no need for centralized institutions like central banks of various countries; two people are transferring to each other In the case of electronic cash, there is no need for the participation of centralized institutions.

Decentralized electronic cash has been explored by computer cryptographers for many years. Following the path of predecessors, Satoshi Nakamoto finally turned this path into reality. Satoshi Nakamoto designed and developed the Bitcoin system, and gave birth to numerous encrypted digital currency and blockchain technology projects.

1.2 Bitcoin is decentralized

Combining the above three forms of currency and comparing cash in the physical world, we have made the following comparison chart:

	Cash in the real world	Centralized Electronic cash	Centralized computer points/points	Decentralized Electronic cash
Issue	Centralized	Centralized	Centralized	Decentralized
Trade	Decentralized	Centralized	Centralized	Decentralized
Whether to map currency	/	Yes	No	No
Is it self-issued	/	No	Yes	Yes

Compared with the above chart, Bitcoin is the opposite of the existing centralized electronic cash system (online payment system):

The currency issuance of the online payment system is centralized, and the issuance of Bitcoin is decentralized;

The currency flow of the online payment system is centralized, and Bitcoin transactions are decentralized;

The online payment system maps currencies in the physical world, and Bitcoin does not map any existing currencies;

The online payment system does not issue currency by itself. Bitcoin is issued out of thin air in the digital world.

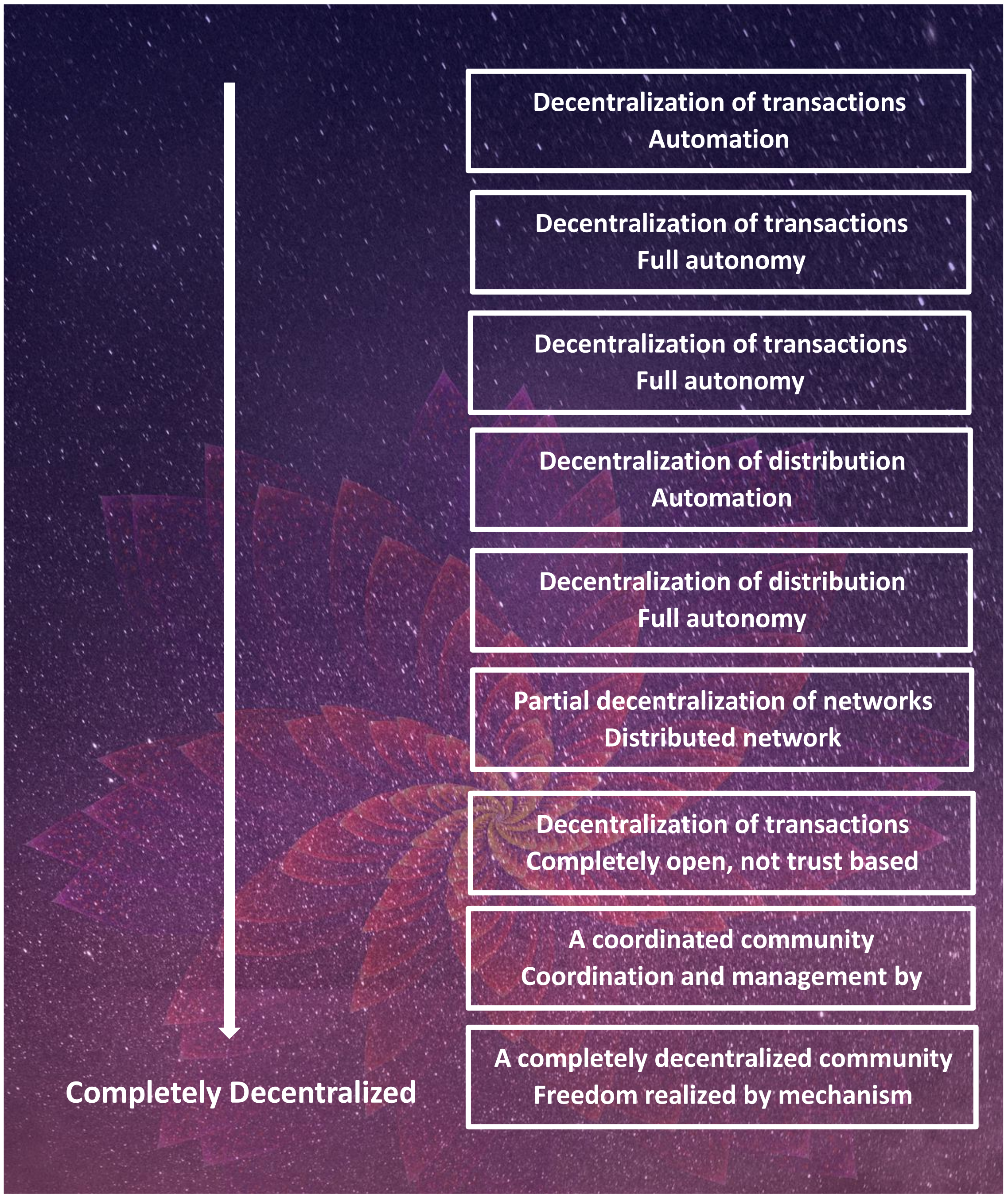
1.3 Stage development of decentralization

The initial stage of decentralization is automatic, that is, it runs automatically according to rules set by people, while the advanced stage of decentralization is autonomous, that is, completely autonomous and spontaneous. The electronic cash system represented by the Bitcoin system embodies the decentralized development path of the electronic cash (ie digital currency) system:

As a currency application, not only is its transaction autonomous, its issuance is also autonomous.

As a computer network, it is completely decentralized, not just a distributed network.

As an organization, it is completely community autonomous and does not require a leader to coordinate.



Decentralization of transactions
Automation

Decentralization of transactions
Full autonomy

Decentralization of transactions
Full autonomy

Decentralization of distribution
Automation

Decentralization of distribution
Full autonomy

Partial decentralization of networks
Distributed network

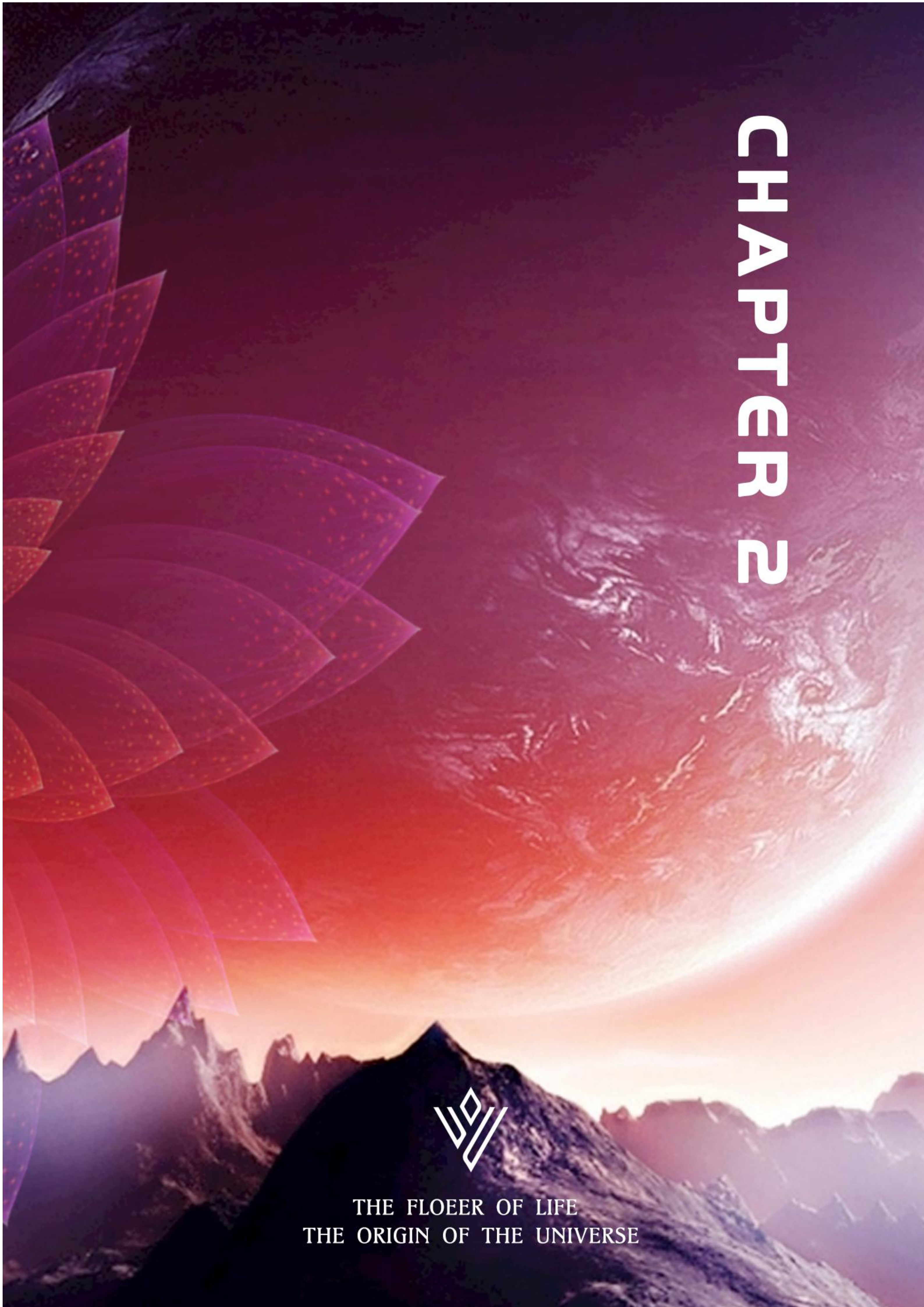
Decentralization of transactions
Completely open, not trust based

A coordinated community
Coordination and management by

A completely decentralized community
Freedom realized by mechanism

Completely Decentralized

CHAPTER 2



THE FLOEER OF LIFE
THE ORIGIN OF THE UNIVERSE

Chapter 2 - The road to blockchain integration: VON

The Bitcoin network does not have a central server. It is composed of many full nodes and light nodes, which form a decentralized network. among them:

The full node contains all the block data of the Bitcoin blockchain;

Light nodes only include data related to themselves.

The Bitcoin network is completely open, and any server can access and download all block data to become a full node. All bitcoin information held by users is stored in a distributed ledger. Based on the distributed ledger and decentralized network, the Bitcoin system realizes decentralized value expression and value transfer, which is very different from centralized online payment systems.

2.1 The transaction process of the Bitcoin system

2.1.1 Description of transaction process

In contrast, the Bitcoin system uses a distributed ledger in which users open an "account", strictly speaking, an address. Everyone can create an "account" on the Bitcoin blockchain and obtain a pair of public and private keys. The address is the hash value of the public key. We interact with the address through the private key.

Each of us has a wallet, which stores private keys. When two people transfer bitcoins to each other, they can directly use their wallet software. Here, the decentralization of Bitcoin is reflected in: there is no longer a centralized institution to centrally manage the ledger. The ledger is stored in a decentralized network composed of many nodes; there is no longer a centralized organization to help us manage accounts and process transactions, everyone manages their own wallets, and transactions are recorded by distributed ledger.

Someone will ask further down that the bitcoins in our address are recorded in the ledger, and it seems that there is still a "center" to store our assets. In fact, this ledger is stored in a distributed manner in a decentralized network, so from this perspective, it can be regarded as decentralized.

In contrast, for a centralized online payment system, it is usually a centralized server to manage a centralized ledger. For the Bitcoin system, the system behind it is a decentralized network, and network nodes jointly maintain a distributed ledger.

2.1.2 Transaction method: On Chain VS Off Chain

1) On-chain

On-chain is the conventional Bitcoin transaction method: Take A and B as an example, A gives B a Bitcoin address (public key), B uses the client to create a transaction and send Bitcoin to A, and this transaction is broadcast on the entire network , Is confirmed and packed into the block. Obviously, transactions happen directly on the chain.

2)Off-chain

That is, transactions on the exchange. A and B open an account in an exchange respectively, and the exchange will generate a pair of public key and private key for A and B respectively, but A and B do not know the private key generated by the platform for them, only their own public key. Then, A and B use their wallets to recharge bitcoins in the public key address that the platform opened for them. Note that this operation is still on chain.

Then, A transfers 0.5 BTC to B through the exchange, but because A does not have a private key, the exchange needs to take A's private key to sign and broadcast the transaction, but does the exchange really need to broadcast the transaction? No, the exchange only needs to set A's account balance -0.5BTC and B's account balance +0.5BTC in its own database. In this step, only the information maintained by the exchange itself is being updated and not on the chain, so this operation is off chain.

Finally, when A and B withdraw cash from the exchange, and the exchange transfers the bitcoins of their online accounts to their own bitcoin addresses (addresses where A and B have their own private keys), this operation will be re-on chain .

2.2 The road to blockchain integration: Bitcoin or other blockchains

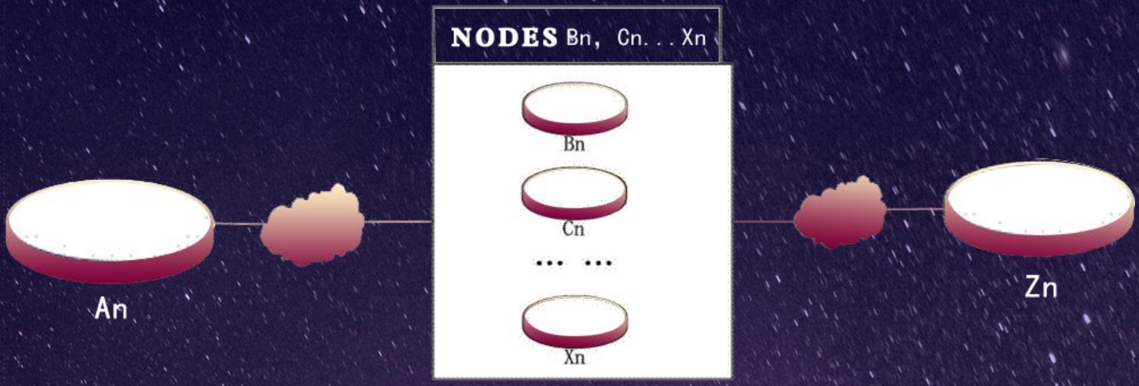
Because Bitcoin's blockchain is dedicated to currency, it is very challenging to transform it to represent other applications. The natural starting point for blockchain integration is Bitcoin. The advantage is that it is easy to implement-the code is easy to run, the Bitcoin network has strong mining power, and the consensus process is flawless. However, we have to make some changes to Bitcoin before it can be used in the application areas we want to develop.

Take decentralized crowdfunding services as an example:

In 2015, the most widely used crowdfunding website was Kickstarter, which connected entrepreneurs and funding providers through a centralized website. We appreciate the idea of Kickstarter, but hope to build a completely decentralized alternative system. This system needs to allow entrepreneurs to request donations from investors, but the entrepreneur cannot spend any money before receiving a certain pre-set amount. All of these are unmediated.

To implement such a crowdfunding service with Bitcoin technology, entrepreneurs need to create a transaction with a specific input (the number of inputs can change with the process) and an output paid to themselves, such as paying 1,000 Bitcoins (BTC). This transaction will circulate among potential funders.

Any funder can add the funding amount to the input of the transaction, and digitally sign their input and total output. Only when all the inputs are equal to or greater than the output, the entrepreneur can obtain all the inputs of the transaction. Because the signature form is limited, we need to use some of the little-known features of Bitcoin to spend the final transaction amount. Although this can be done in today's Bitcoin system, we must delve into the corners of Bitcoin that few people know about. This is not a standard Bitcoin transaction that we see every day.



Therefore, we came up with a solution: just use Bitcoin as a time stamp service, not as a data storage, but to provide another blockchain or data storage service, that is: choose an alternative blockchain that already exists, this area Blockchain can support new applications, adapt to actual challenges, and create an ideal platform for decentralized complex contracts. Therefore, an anonymous public chain based on the DASH master node network: the VON·origin, came into being.

2.3 Introduction to VON CHAIN

The VON is a very ancient totem with infinite energy. The perfect proportion symbolizes the original shape and vibration (frequency) of the universe. It is also a kind of sacred geometry. It is the blueprint of creation and the symbol of life and the universe. This all-encompassing geometric symbol, the origin of all things, is a pure flame of spiritual consciousness, the source of the universe, and it condenses the human consensus on the origin of life.

Out of admiration for the VON, hope for the development of the digital economy era, and recognition of the BITCOIN (Bitcoin) and DASH (Dash) technology, we decided to create a symbol based on the technology of BTC and DASH An anonymous public chain that is free, inclusive of all things, records the origin, and builds consensus: VON Chain.

We hope that through the United Mining Exchange and many well-known mining farms around the world, with decentralization, good anonymity, smart contracts and other technical characteristics as the core, we can create a consensus and respect for life through blockchain technology. A new blockchain underlying basic system that "does not take the individual's consensus will as a transfer, but connects the individual with the consensus" as the consensus network. At VON Chain, we encourage users to consolidate consensus through sustainable mining, and provide blockchain technology support for users’ consensus network. We give VON this consensus network greater scalability and stability to help blockchain technology in The combination and exploration of the commercial side will make the blockchain ecology prosper, truly enter people's daily life, and make imagination possible.

CHAPTER 3

THE FLOEER OF LIFE
THE ORIGIN OF THE UNIVERSE

Chapter 3 - VON CHAIN Technical Architecture

3.1 Sustainable mining mechanism of " One System Mine Double Coins"

When we create consensus, we need an algorithm, a mechanism for sustainable growth, to maintain this consensus and build a more stable and expandable consensus network. Through the sustainable mining mechanism, VON truly realizes " One System Mine Double Coins" for the first time. In the VON blockchain system, the consensus network will be updated and maintained every moment, creating value for consensus builders.

3.1.1 Bitcoin dividend

In the VON network, 30% of the VON will be automatically converted into a 2-year Bitcoin mining machine hashrate, and mining will be carried out according to the Bitcoin's entire network hashrate. You will receive daily Bitcoin mining dividends and be synchronized with Bitcoin. Development to ensure the long-term stability of VON CHAIN.

3.1.2 VON liquidity mining

In the VON network, 30% of VON participates in Bitcoin mining, and the remaining 70% is used for VON liquidity mining. The VON CHAIN liquidity mining mechanism promotes the circulation of VON in the entire network and provides security for the rapid growth of VON.

3.1.3 The most powerful consensus network in history

How is the VON consensus network formed? In fact, we don't even need to deliberately build this consensus network, because there is usually a hidden consensus network in any communication system. VON CHAIN, through the sustainable mining mechanism of " One System Mine Double Coins ", naturally realizes economic self-circulation, thus establishing a "long-term, stable and safe" consensus network.

Why do we use the consensus network of VON? We firmly believe that there is very important information in the consensus network. Who has established the network and who has contributed the most to the value of the network. For example, consensus. This will help our algorithm to determine who should get more or less consensus. force. Second, let us analyze the core goal of this algorithm. Please pay attention to the three keywords, "stable", "enhanced" and "growth". " One System Mine Double Coins " turns the originally simple single-level consensus network into a tighter multi-level link. In other words, what is related to you, what you can influence, and what can influence you is not only your own circle of friends, but also your friends' circle of friends and friends' circle of friends, etc. Such a network is not only stable, but also influences and even promotes each other. The establishment, enhancement and growth of such network structure links, coupled with elimination, makes us have to think of the process of biological evolution and the emergence of intelligence in neural networks, and look at the world, the universe, life and what humans have experienced. History, this is an inevitable barbaric expansion, an infinitely growing group evolution system.

3.2 Anonymous payment

We believe that in order to increase the strength and protect user privacy on the client side, it is important to implement a standard non-trust system. For example, clients such as electrum, Android and iPhone will also directly embed the same anonymity layer and make good use of protocol extensibility. This allows users to have the same experience when sending funds anonymously using a solid and stable system.

PrivateSend is an improved and extended version of CoinJoin (software that provides anonymous technology). In addition to the core concept of CoinJoin, we have also made a series of improvements, such as decentralization, the use of links to achieve strong anonymity, the same face value, and passive advanced coin mixing technology.

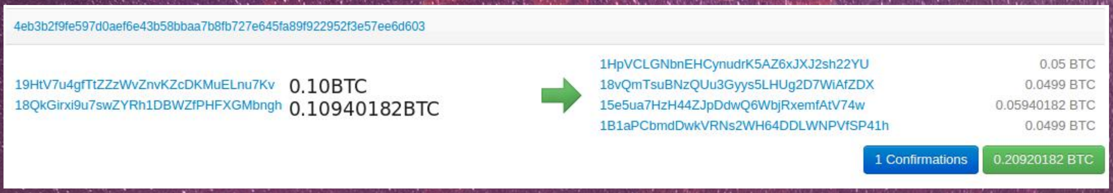
When improving privacy and the interchangeability of encrypted digital currencies, the biggest challenge is that the entire blockchain cannot be encrypted. In the Bitcoin-based encrypted digital currency system, you can see which outputs are not sent and which are sent, usually called UTXO, the full name is unused transaction output. This allows each user to act as a guarantor of honest transactions in the public ledger. The Bitcoin protocol is designed without relying on the participation of a third party. Without the participation of a third party, it is vital that user information can be read at any time through the public blockchain for auditing. Our goal is to improve confidentiality and interchangeability without losing these elements. We firmly believe that this is the key to creating a successful digital currency.

Using decentralized currency mixing services within the scope of digital currency, we can make the currency itself fully interchangeable. Fungibility is an attribute of money, and all units of currency must be equal. When you receive funds in the form of currency, the funds should not retain the previous user's use history, or the user can easily separate from the previous use history, so that all currencies are equal. At the same time, any user guarantees that every transaction in the public ledger is honest without affecting the privacy of others.

In order to improve the interchangeability and maintain the honesty of the public blockchain, we propose to use advanced non-trusted decentralized currency mixing technology. In order to maintain currency interchangeability, this service is directly integrated into the currency system , It is easy and safe to use for every user.

3.2.1 Coinjoin

A simple strategy is to integrate Coinjoin on the basis of existing Bitcoin, which is simply to merge transactions together. By tracking the flow of user funds in a joint transaction, the user's identity will be exposed.



4eb3b2f9fe597d0aef6e43b58bbaa7b8fb727e645fa89f922952f3e57ee6d603

19HtV7u4gfTtZZzWvZnvKZcDKMuELnu7Kv 0.10BTC
18QkGirxi9u7swZYRh1DBWZfPHFXGMbngh 0.10940182BTC

1HpVCLGNbnEHCynudrK5AZ6xJXJ2sh22YU 0.05 BTC
18vQmTsuBNzQUu3Gyys5LHUg2D7WiAfZDX 0.0499 BTC
15e5ua7HzH44ZJpDdwQ6WbjRxemfAtV74w 0.05940182 BTC
1B1aPCbmdDwkVRNs2WH64DDLWNPVfSP41h 0.0499 BTC

1 Confirmations 0.20920182 BTC

In this transaction, 0.05 bitcoins are sent out using the currency mixing technology. In order to track the source of the funds, you only need to add up the amount on the right and match the amount on the left.

Regrouping transactions:

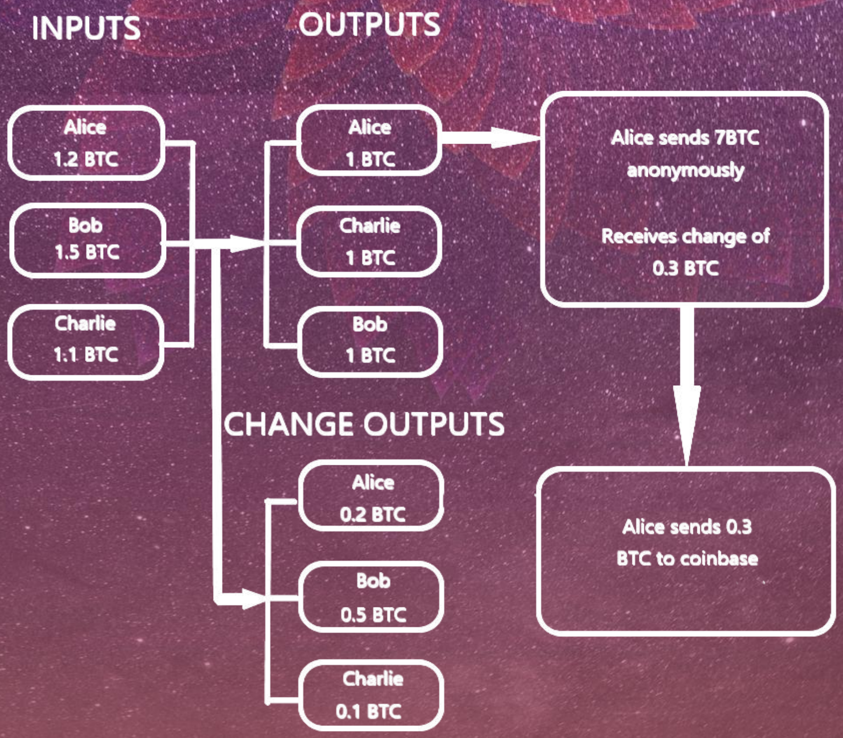
0.05+0.0499+0.0001(fee)=0.10BTC.

0.0499+0.05940182+0.0001(fee)=0.10940182BTC.

As more users join the process of mixing coins, the difficulty of obtaining results will increase exponentially. However, the results can still be tracked at a later point in time, and anonymity is invalidated.

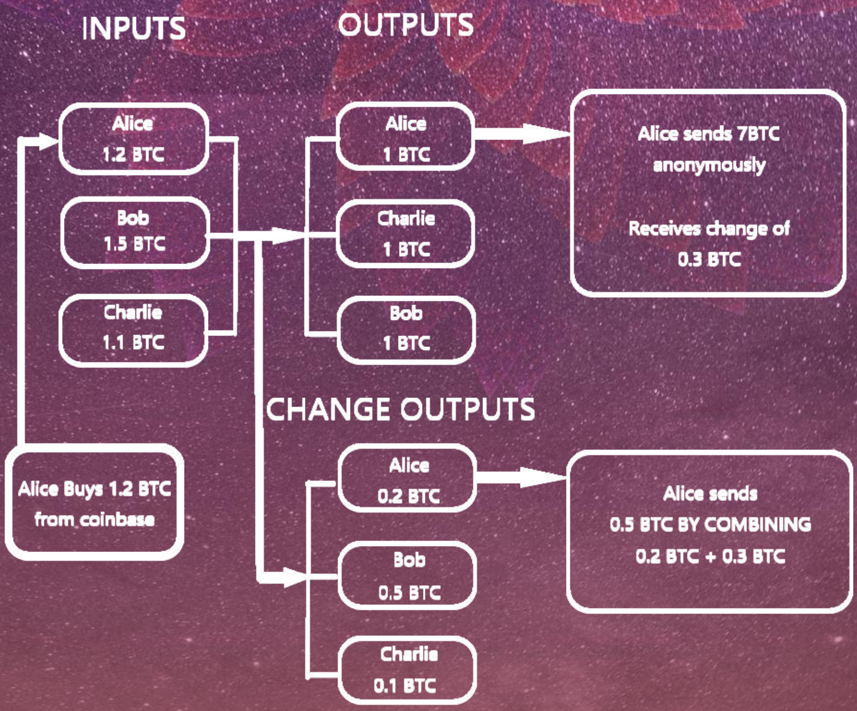
3.2.2 Direct link and relay link

In other applications implemented by Coinjoin, users first anonymize funds, and finally send transactions to platforms or individuals that know the identity of the sender. This is possible.But this breaks the anonymity and allows others to track the user's transactions forward. We call this type of attack a"relaylink."



In this example, Alice sends 1.2 BTC anonymously, outputs 1 BTC and 0.2 BTC to the outside, and then outputs 0.7 BTC from the output of 1 BTC, leaving 0.3 BTC. This 0.3 BTC output is sent to an identifiable object, but in essence Alice has successfully sent 0.7BTC out anonymously.

In order to determine the identity of the sender of an anonymous transaction, it is necessary to start with the "exchange transaction" link and go back through the blockchain until "Alice sends 0.7 BTC anonymously". Once you find it, you will find that your user has recently purchased something anonymously, so you can see through this anonymous transaction. We call this type of attack "intermediary conversionlink".



In the second example, Alice spent 1.2 BTC on coinbase, then anonymized this amount and output it as 1 BTC. Then, she spends another 1BTC, and the remaining 0.3BTC is combined with the previous 0.2BTC to form 0.5BTC for external output.

Combining anonymous transactions and CoinJoin transactions, sort out the entire transaction history before and after, so that this anonymous function can be thoroughly seen.

3.2.3 Enhanced privacy and DOS protection

Multi-party transactions can be combined into one transaction. PrivateSend makes good use of this. It merges funds from multiple parties and sends them together, so that once they are integrated, they cannot be split again. Taking into account that the PrivateSend transaction is set up specifically for user payment, this system is highly secure and anti-theft, and the user's currency is very safe. Currently, the use of PrivateSend's currency mixing technology requires at least three parties to participate.

In order to enhance the privacy of the system as a whole, we propose to use the same face value of 0.1Token, 1Token, 10Token and 100Token. In each round of currency mixing, all users should input and output funds in the same face value form. In addition to using the same face value, transaction fees will be removed, and all transactions will be broken down into scattered, independent, and unrelated small transactions.

The next step is to deal with possible DOS attacks. We propose that all users submit their transactions to the mining pool in the form of deposits when they join, and the transactions are finally output to the users, while at the same time paying a high reward to the miners. In other words, when a user requests an increase from the mixed currency pool, a deposit must be provided at the beginning of the transaction. If the user fails to cooperate at some point, such as refusing to sign, the deposit transaction will be automatically broadcast on the entire network. If a continuous attack is to be carried out on an anonymous network, the price paid is extremely high.

3.2.4 Passive funds and blockchain anonymity

PrivateSend's currency mixing is limited to a certain amount of Tokens, and multiple rounds of currency mixing can anonymously mix a considerable amount of funds. In order to make the user experience convenient and attacks difficult, PrivateSend runs in a passive mode. At the same time, the time interval is set, and the user's client must connect to other clients through the master node. Once entering the master node, the amount of denomination required by the user to be anonymous will be queued up and broadcast across the entire network, but no information will reveal the user's identity.

Each round of the PrivateSend process can be regarded as an independent event that enhances the anonymity of user funds. However, each round is limited to only 3 participants. Therefore, observers have one-third of the opportunity to track transactions. In order to improve the quality of anonymity, links will be used Method, the funds are sent out sequentially through multiple master nodes.

The depth of the blockchain	Number of possible users
2	9
4	81
8	6561

3.2.5 Security considerations

Because the transactions are merged together, the master node may "snoop" when user funds flow through. Since each master node is required to hold a certain number of tokens and users choose random master nodes to deploy their funds, the impact of "snooping" is not great. The probability calculation of tracking transactions through the blockchain is shown below. Expanding the system by covering up transactions that occur on the master node will also greatly improve the security of the system.

The number of master nodes/total master nodes controlled by the attacker	Need to be selected consecutively	Probability of success
10/1010	2	9.80e-05
10/1010	4	9.60e-09
10/1010	8	9.51e-11
100/1100	2	8.26e-03
100/1100	4	6.83e-05
100/1100	8	4.66e-09
1000/2000	2	25%
1000/2000	4	6.25%
1000/2000	8	0.39%
2000/3000	2	44.4%
2000/3000	4	19.75%
2000/3000	8	3.90%

3.2.6 Use a relay system to cover the master node

In Section 3.24, we described the probability of tracking a single transaction using PrivateSend multiple rounds of currency mixing technology. This can be further enhanced by masking the master nodes so that they cannot see the user input/output direction. To do this, we propose a simple relay system that allows users to protect their identities.

We do not allow users to directly submit input and output transactions to the mining pool, but instead let them randomly select the master node from the entire network and ask it to relay the input/output/signature to the target master node. This means that the master node will receive N input/output and N sets of signatures. Each round of coin mixing only serves one of the users, but the master node cannot know which user it is.

3.3 Smart contract

Smart contracts have been successfully implemented on many blockchain systems. The more well-known systems are Ethereum and Hyperledger. Since Bitcoin and other scripting languages do not have Turing completeness, the smart contract transaction mode written is very limited and can only be used for virtual currency applications. Therefore, we have launched a smart contract platform that supports Turing complete language, which is endowed by the smart contract mechanism. The automation of the decentralization of data on the chain：

Use the data on the chain to determine the contract conditions, and automatically execute them when they are met, and no institution can intervene in this process.

The execution process satisfies all or nothing, that is, atomicity. All operations in a transaction are executed either successfully or all failed.

The smart contract is deployed on the blockchain in the form of bytecode. The developer wraps the smart contract method and parameters that he wants to call in the form of transaction and sends it to the virtual machine; the virtual machine obtains the corresponding contract bytecode and uses the dispatcher to complete the contract Method call. Asynchronous response, that is, only when the transaction is packaged into the block and confirmed on the chain, the call will have a real response.

In theory, scripts that conform to the above principles can be regarded as the realization of a smart contract. However, this is not enough, we also need to provide the necessary features for smart contracts:

Certainty

Downtime

Resource model

Read and write blockchain data

Cross-contract call

Resource isolation

3.3.1 Certainty

As the execution script of blockchain state transition, smart contracts must satisfy certainty, so that all nodes can run on different computer devices and at different times, and the same input can always output the same result. There are many factors that make the contract non-deterministic, and they can be summarized as follows:

For floating-point numbers, the accuracy of floating-point numbers in different operating systems and different hardware devices may be different, resulting in different results when floating-point operations are involved. Therefore, mainstream contract solutions such as solidity prohibit the use of floating point numbers.

Calling non-deterministic system functions, that is, non-deterministic functions such as generating random numbers, obtaining system time, and obtaining the current block header are called, which makes the result non-deterministic. The current contract scheme will link these non-deterministic functions to the state of the blockchain. For example, obtaining the system time is changed to obtaining the time when the current block is packaged; the random number is generated by the blockchain data as a seed, at the same height The same random number can be obtained under the block.

Using non-deterministic data sources, a typical example is the use of oracles to obtain external data in contract execution, which will also make the same input produce non-deterministic results. Currently, there is no mature solution to obtain data from non-deterministic data sources (such as the Internet).

Dynamic calling refers to a contract calling another contract method, and the calling target can only be determined when the contract is running. Dynamic call is almost non-existent in existing contract schemes.

3.3.2 Downtime

The halting problem is a problem of the calculable theory in logic mathematics. In layman's terms, the shutdown problem is to determine whether any program can end its operation within a limited time. In 1936, the halting problem was proved by Alan Turing to be an undecidable problem on the Turing machine, that is, there is no general algorithm to solve the halting problem.

Why do we need to consider downtime when designing smart contracts? We need to prevent developers from writing infinite loops in smart contracts, so that the virtual machine is stuck in a certain contract call when it is running, causing the entire blockchain to work abnormally. Therefore, we need to design a mechanism that can stop the execution of the smart contract under certain conditions.

Since there is no general algorithm, different solutions can only be designed according to different blockchain protocols. We will use gas pricing to solve the downtime problem. Each transaction contains the gas Limit and gas Price fields. The execution of the contract bytecode requires gas (different bytecode operations correspond to different gas), and the contract execution stops when the cumulative gas consumption exceeds gas Limit.

3.3.3 Resource model

In the public chain environment, due to the limited hardware resources of the blockchain, how to reasonably allocate resources for contract execution and data storage to optimize the allocation of computing resources and prevent malicious abuse is a very critical issue. Here we use the Gas-based resource model, the gas consumption for contract execution is multiplied by the block field gasPrice to get the final number of tokens consumed. For data storage, there is no additional charging mechanism except for bytecode charges when reading and writing.

3.3.4 Read and write blockchain data

Reading and writing blockchain data is the core function of a smart contract, and it is also where it is called "smart".

Read: The data of the blockchain can be read when the contract is called, the contract conditions are determined and executed automatically. This process is atomic and does not require any human intervention.

Write: treat the blockchain state as a database, write contract state data to implement more complex business logic

We will adopt the form of (RAM) trading. Users need to buy storage space before they can store data; after data is deleted, the space can be sold back to the system.

3.3.5 Cross-contract call

Cross-contract calls greatly enhance the interoperability of smart contracts and simplify development costs. At the same time, the contract status data can be opened in a reasonable form, which also prevents the contract from becoming a data island, greatly expanding the imagination of the business.

The cross-contract call must be a deterministic static call-the address of the called contract is known before it runs, and the call result is deterministic.

In the design of cross-contract calls, we paid attention to two aspects：

1)Context switching

Context switching often occurs in cross-contract calls: when contract A calls contract B, whether the context should be contract A or change to contract B. A typical example, in Solidity, msg.sender and storage are context-sensitive. The language provides call, callCode, and delegateCall to meet the needs of different context switching (see the article for specific differences between the three).

2)Access control

Permission control is an inevitable problem in cross-contract calls, and it is related to user data security. Let's look at the following example:

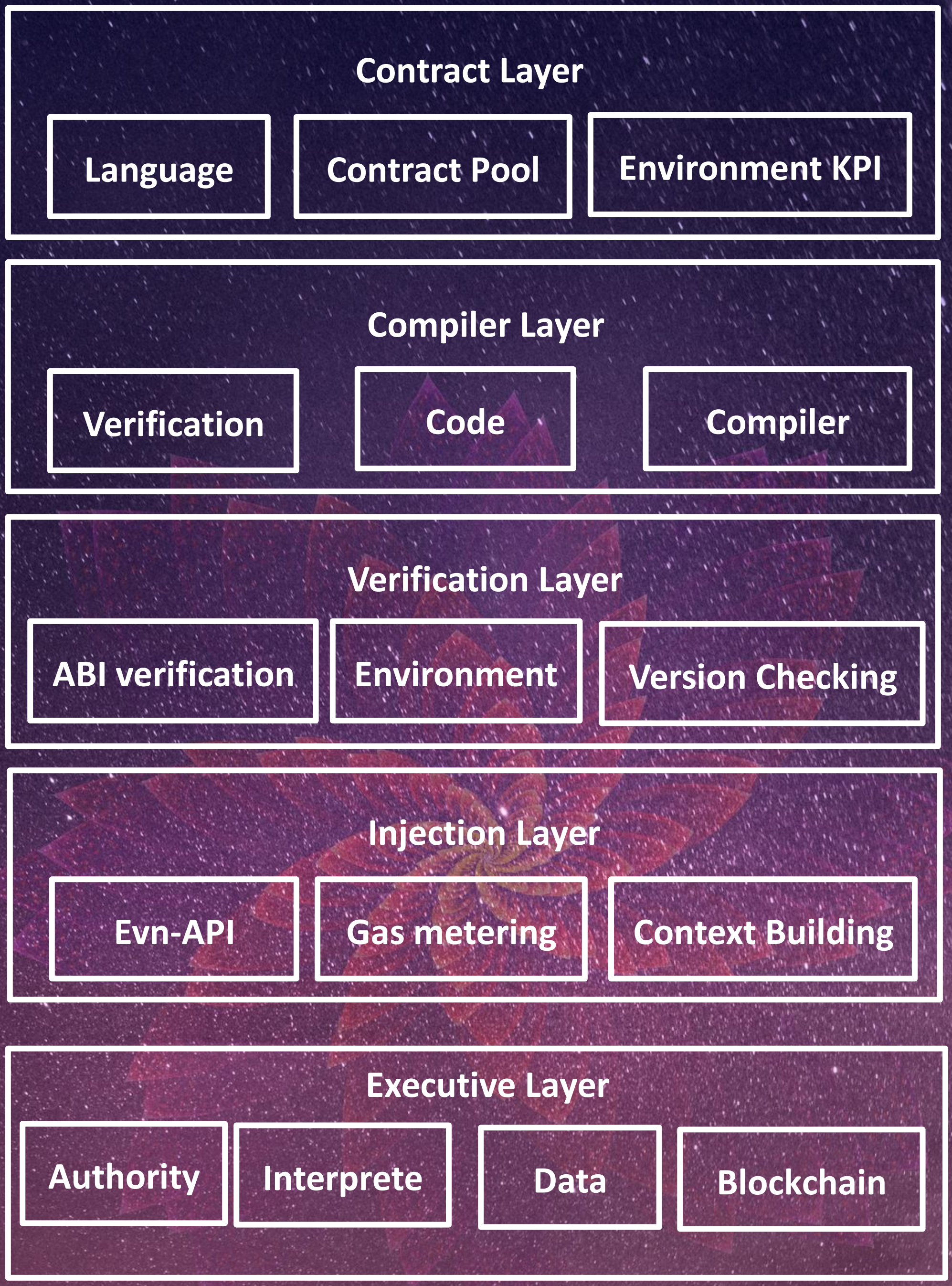
Bob calls the hi method of contract A, and hi contains a cross-contract call, like B.hello(), which calls the hello method of contract B.

So the question is: Bob just wants to call the method of contract A, and does contract A have the right to call contract B with Bob's account?

Taking into account that no one can modify or upgrade the contract after deployment, as long as the user confirms that the code meets the requirements, the user shall be responsible for the consequences of the call. This involves concerns about asset security. Therefore, we provide an authorized interface, that is, only authorized contracts can transfer the user's corresponding assets to achieve permission control.

3.3.6 Resource isolation

The following figure is a basic structure diagram of a smart contract, from top to bottom are the contract layer, compilation layer, injection layer, and execution layer. The contract layer provides the language and code library for smart contract development, as well as the necessary API for interacting with the blockchain; the compilation layer is responsible for compiling the contract code into bytecode that can be executed by the virtual machine; the injection layer generally gives the contract word before the contract is executed The section code injects some components, including the specific implementation of Env API, the measurement function of Gas, and the context of the construction of contract execution; the execution layer checks the execution authority of the contract, creates a sandbox environment and allocates resources, and uses the interpreter to run the contract bytes code. During the execution process, the state database and blockchain ledger are provided as the data backend.



Contract Layer

Language

Contract Pool

Environment KPI

Compiler Layer

Verification

Code

Compiler

Verification Layer

ABI verification

Environment

Version Checking

Injection Layer

Evn-API

Gas metering

Context Building

Executive Layer

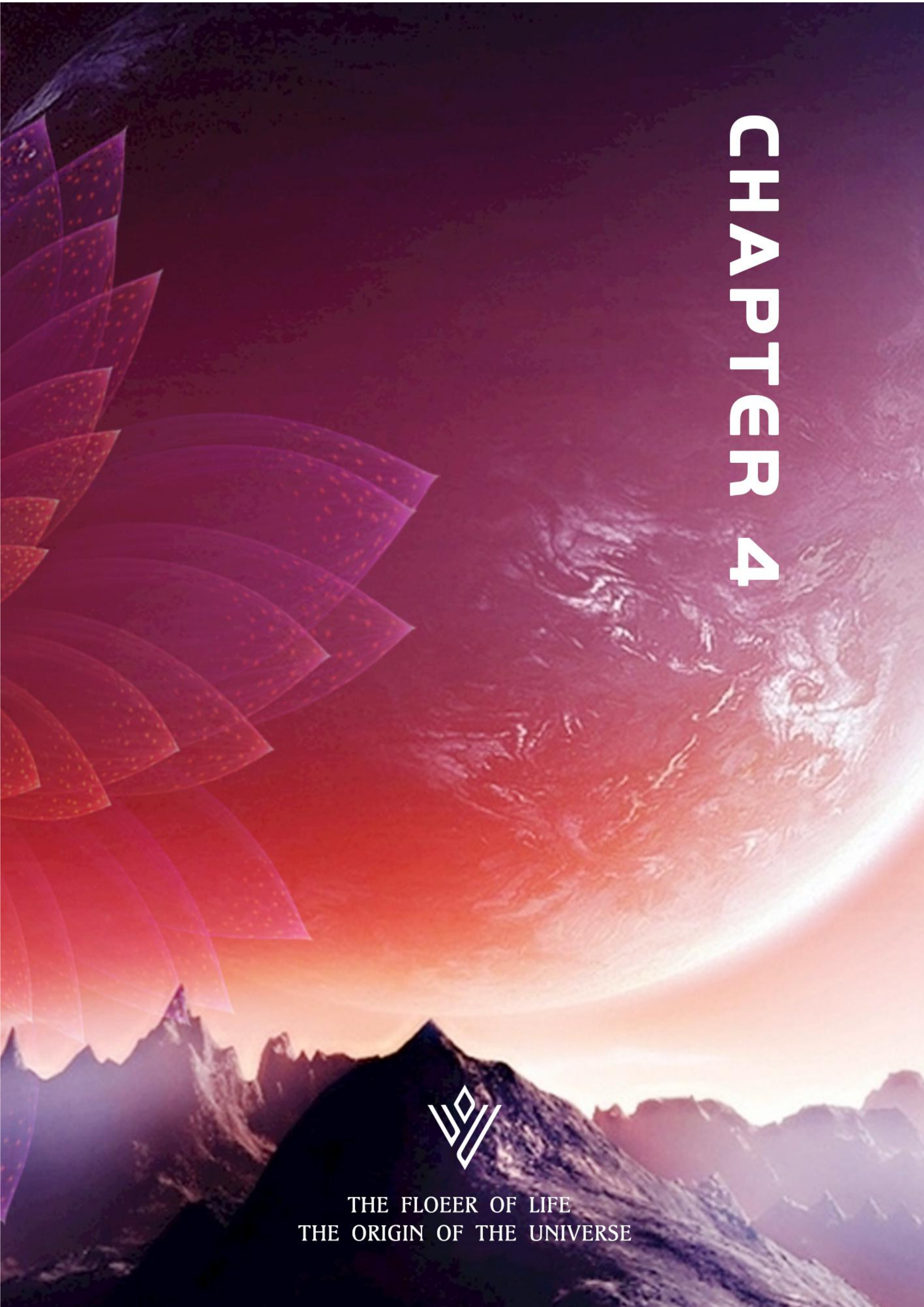
Authority

Interprete

Data

Blockchain

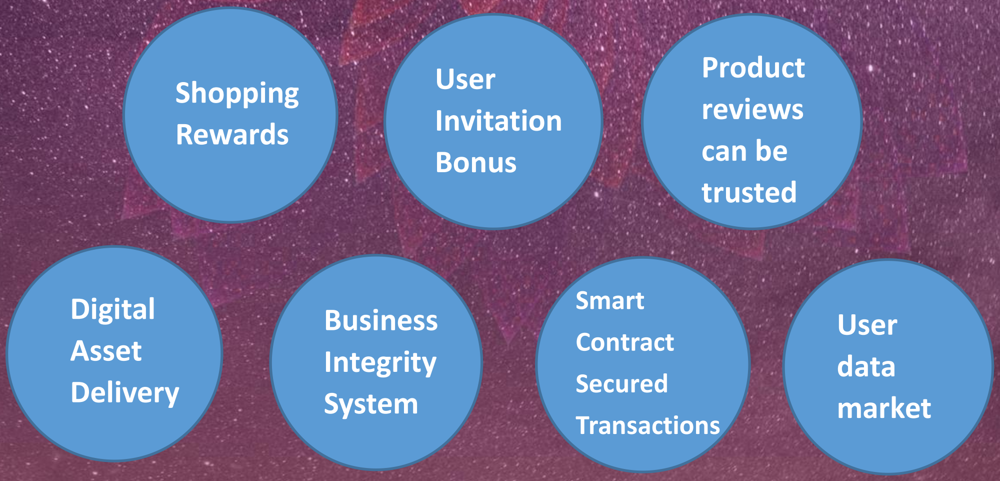
CHAPTER 4



THE FLOEER OF LIFE
THE ORIGIN OF THE UNIVERSE

Chapter 4 - VON CHAIN application and layout

VON Chain will be a completely open anonymous public chain, providing underlying technical support and cooperation in the development of various industries, starting from community autonomy, linking more digital economy participants, including individuals, entrepreneurial projects/enterprises, digital banks, and insurance , Venture capital institutions, etc., integrate cutting-edge technologies such as AI, big data, cloud computing, 5G, and the Internet of Things to digitally transform industrial resources and realize the digital upgrade of the physical industry.



Shopping Rewards

User Invitation Bonus

Product reviews can be trusted

Digital Asset Delivery

Business Integrity System

Smart Contract Secured Transactions

User data market

4.1 All purchases are returned to the shopping mall

We will create the first platform for the perfect integration of consumer shopping and blockchain technology-let the advantages of blockchain technology serve the actual transaction scenarios of consumer shopping and help consumers realize their dream of value-added shopping. VON Chain, as a consensus blockchain system condensing the consensus network, will use its strong linking capabilities to conduct network diversion for the smart contract shopping mall. Countless consensus connections form a community of interests that are truly connected and bundled through VON Chain, which will form the world's most stable value consensus system, help the mall to quickly increase product sales, and also allow individuals in the consensus connection to get the most out of shopping The benefits, thus subverting the traditional mall. The consensus value points that will be realized in the smart contract mall in the future include:

Rebate for shopping consumption: Users can rebate digital assets when they consume a certain amount in the mall to stimulate users to spend more.

Digital asset delivery: Users can use digital assets to deduct all or part of the amount of consumption in the mall, thereby realizing the extension of digital asset offline consumption scenarios.

User invitation rewards: Users can receive digital asset rewards after inviting others to register, which can encourage users to develop other users independently.

User data marketing: Record the user's consumption browsing data on the blockchain, and cooperate with data marketing agencies. Users who use the data can also get rewards of digital assets.

Trustworthy product reviews: record the user's product review data on the blockchain, so that the product review data cannot be tampered with and is authentic.

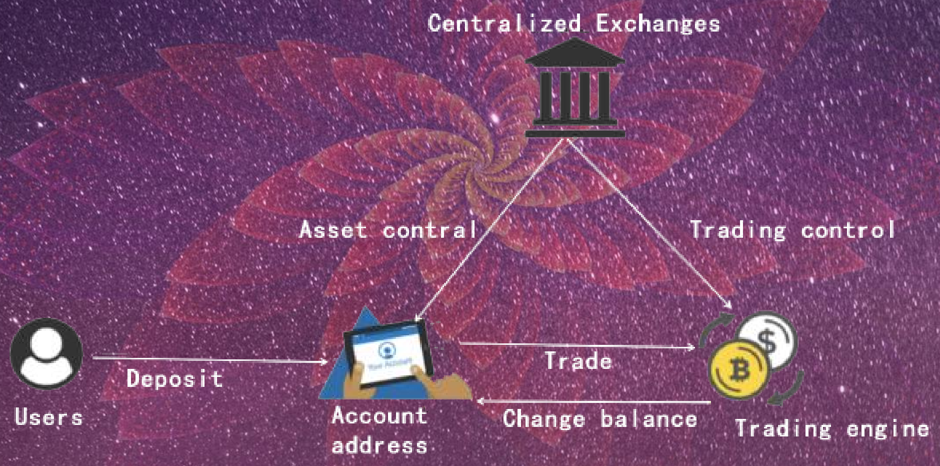
Smart contract secured transactions: Secured transactions are carried out through the trust of smart contracts.

Merchant integrity system: All transaction information, reviews, and after-sales information of the merchant are recorded on the blockchain, and the information is authentic and credible, which improves the integrity of the merchant.

In addition, the smart contract mechanism of VON Chain can avoid complicated systems and create a more direct payment process between the payer and the payee. Whether it is domestic transfer or cross-border transfer, this method has low price and speed. Features, and no intermediate fees. And the consensus network formed by users in the mall will also support cancellation (that is, after-sales for mall consumption). Once the after-sales is reached, the tokens paid in the VON Chain smart contract shopping mall will be transferred back to the user’ s account/wallet through smart contract transfers to form a complete The shopping mall industry chain can better protect the rights of users.

4.2 Smart contract decentralized exchange

The mechanism of a centralized exchange is relatively simple: users register for an account on the platform and obtain the account address given by the platform, and the user can recharge digital assets in the account address and then trade on the platform. The platform provides users with asset transaction matching and clearing services. After the transaction is successful, the asset balance in the user's account changes.



We also found that the operation mechanism of centralized exchanges has the following main problems:

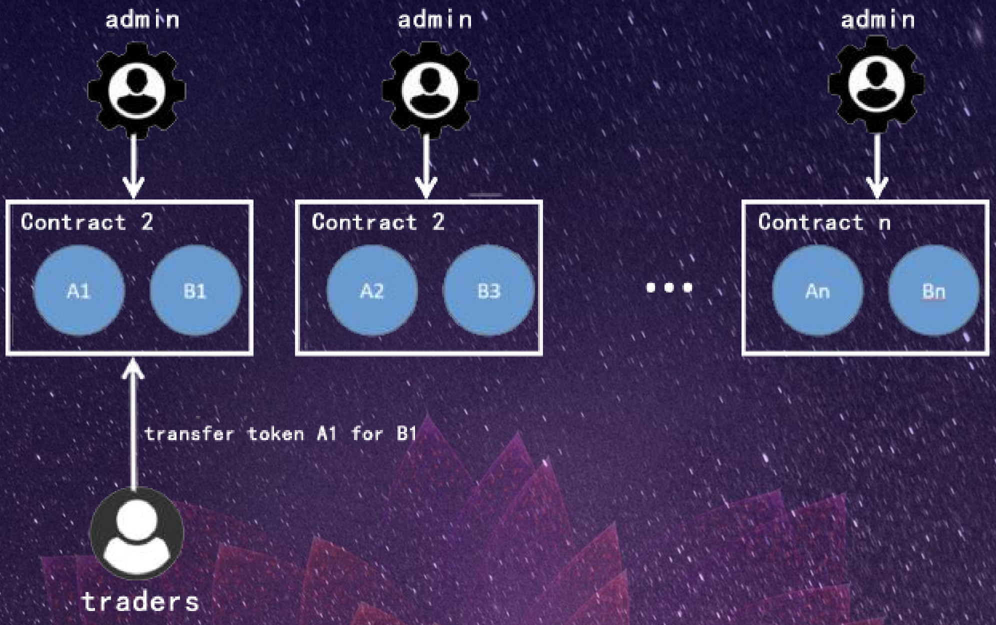
Asset security risks: the entire process is managed by the platform.

Asset control restrictions: users cannot freely control their own assets.

Transaction clearing is not transparent: The transaction clearing process is completed by the platform and cannot be traced back in the blockchain.

In order to solve the shortcomings of the centralized exchange mechanism, we have begun to explore the establishment of a trading system on the blockchain to ensure that users' assets are not controlled by the platform, and transaction settlements can be open and transparent. Therefore, we have proposed a solution for transactions on the chain-smart contract exchange, namely: "orderbook on the chain, settlement on the chain" full chain transaction. The internal transaction records of the exchange are uploaded to the chain in real time through smart contracts, which perfectly combines the efficient experience of a centralized exchange and the transparency and security of a decentralized exchange.

Each trading pair has a smart contract called relay. The contract calculates a conversion ratio (price) based on the number of assets in the trading pair, and automatically adjusts it dynamically according to the increase or decrease in the number of assets. Taker selects a trading pair and transfers the relevant token to its contract to obtain the assets it wants.


admin
admin
admin
Contract 2
A1
B1
Contract 2
A2
B3
...
Contract n
An
Bn
transfer token A1 for B1
traders

Transaction matching and settlement are executed on the chain through smart contracts, introducing the role of token reserve and related reserve administrators and reserve token contributors. Each reserve library provides transaction pair exchange prices and competes with each other.

Smart contracts differ from centralized exchanges in the following points:

1. All transaction operations are carried out on the blockchain, that is: through smart contracts;

2. In the entire transaction process, users always hold the ownership of digital assets , Therefore, there is no KYC process and certification records, and the root cause is to achieve anonymity and protect user privacy.

When trading on the smart contract exchange established based on the VON·Essence, the transaction data will be packaged every 10 seconds and uploaded to the chain through smart contracts to achieve safety and efficiency:

The transaction data is uploaded to the chain in real time to ensure that the transaction data cannot be tampered with, cannot be deleted, and is irreversible;

By querying the address, the internal transaction data of the exchange is open, transparent and traceable;

Unified matching reduces transaction waiting time, fast asset matching and matching, and improves asset liquidity;

To reduce transaction costs, the on-chain transaction of "orderbook on the chain, settlement on the chain" only consumes polar gas fees.

4.3 Privacy Defi Platform

Defi is a broad concept that can be understood as decentralized pan-finance, which covers mortgage lending, decentralized trading platforms, oracles, stable coins, synthetic assets, option derivatives, and so on.

Privacy pain points have always existed in various industries, but they have not been taken seriously. The original intention of the blockchain is to achieve decentralization, openness and transparency, but as the industry grows, users gradually find that privacy protection is still necessary in the blockchain, and then many anonymous projects began to be created by technical geeks, such as Monroe, Dash, etc., the subsequent performance of these privacy projects also proved the necessity of the existence of a privacy blockchain. Therefore, we hope to launch a privacy and anonymous Defi platform that can maintain high performance and high scalability while effectively protecting user privacy.

The VON·Essence In the future, we will focus on aggregating the open source APIs of all decentralized financial DeFi products, and divide the platform design into product layer, aggregation layer, protocol layer, and base layer. Agreements or projects that will achieve integration in the future include:

DeFi projects: Compound, dydx, BZX, Aave, Curve.fi

Currency: DAI, USDC+Altcoins

Insurance: Nexus Mutual, Opyn

Privacy category: Aztec, Tornado.cash, Camoflag.eth, Open VPN, ToR

Wallets: Metamask, Fortmatic, Ledger, Trezor, Portis, WalletConnect and Authenticreum

The privacy and anonymous Defi platform focuses on seamless aggregation. The aggregation layer mainly uses an interactive page and a series of smart contracts to provide protocols. The protocol layer will include multiple protocols such as DeFi payment, insurance, DEX, derivatives, and lending. On the privacy and anonymity Defi platform, developers can quickly develop distributed applications that focus on privacy protection. At the same time, the privacy and anonymity Defi platform will provide the issuance function of anonymous assets. Anyone can issue their own anonymous assets for subsequent asset transactions. Except for the participants, no one else can snoop on the amount of assets.

The privacy and anonymity Defi platform will adopt an account model and use homomorphic encryption and zero-knowledge proof technology to provide underlying cryptographic support for its anonymity. These cryptographic technologies can be used at the smart contract layer, and DAPP will also easily obtain anonymity.

4.4 Privacy storage platform

The Interplanetary File System (IPFS) is becoming one of the preferred storage platforms for dApps. IPFS is an open source distributed file storage system that uses blockchain to facilitate the storage and management of Internet data by distributing it to connected nodes or Internet users, so that it can resist attacks and censorship. This system attempts to replace the storage of Internet data on a centralized server or the classic server-client architecture of the traditional Internet. The function of the IPFS system is similar to that of a P2P network (such as BitTorrent), and the requester of the file becomes an additional host. The system uses the IPNS naming structure to replace the DNS system in the old system. The stored data is represented as a cryptographic hash on the blockchain and linked to the IPNS naming structure.

As an anonymous public chain that also pays attention to privacy and security, VON·Essence will join the IPFS protocol to develop the application of a new generation of privacy storage platform and build a P2P storage market in the future ecological layout.

With the help of a distributed hash table that stores information as keys/values, and the data is scattered in the computer network, the connected nodes do not need central coordination, even if the node fails or leaves the network, DHT can be expanded to accommodate millions Nodes can also operate reliably.

Build a distributed network, where nodes use encrypted currency to pay for their storage and bandwidth, and the files in the nodes are always open to everyone.

The global storage node must continue to save the stored files within the specified time, and the submitted proof can be verified to obtain the token rewards and realize the permanent storage of file data.

All nodes of each shard store the same files. When a node goes offline, it will immediately trigger another node to automatically and seamlessly repair the file, synchronize the file, and ensure the integrity of the file data read by the user.

4.5 Privacy social platform

The current social network is a centralized structure, users create content, social networking sites set rules, store content, and distribute content. The interaction between users is realized through a centralized social network, which uses social networks to communicate and maintain interpersonal relationships, obtain information such as friend dynamics, hot content, etc., while the social network as the service provider masters the data generated by users, and By analyzing these data, accurate advertising recommendations can be used to benefit.

We found that these centralized social network platforms generally have the following problems:

The rules are formulated by the platform, and users can only comply with them and cannot participate in autonomy

The authentication privacy information of users on social networking platforms cannot be effectively protected, and there is a danger of abuse and misappropriation

There is a danger of chatting information leakage, and the platform has low trustworthiness

The value creation brought about by user-produced content belongs to the platform, and users cannot earn value income.

Therefore, we decided to introduce the anonymity technology and smart contracts of the VON origin into the current centralized social network platform and carry out transformation: the blockchain is technically a distributed ledger solution, and records cannot be tampered with. Authenticity. For ordinary users, it is essentially a trusted intermediary network platform. When applied to social networks, it is a trusted peer-to-peer social platform.

VON Chain will carry out the strategic layout development of a new generation of privacy social platforms, namely: social (including communities, media) projects, using blockchain distributed technology to build a platform, allowing users to control their data.

What are the advantages of this anonymous and private social platform? On the one hand, it benchmarks the unfair revenue distribution mechanism of traditional social platforms, and advocates returning the commercial value brought by users ' content to users, that is, by introducing blockchain financial mechanisms, the revenue will be replaced by the platform based on user activity and other criteria. It is returned in the form of coins; on the other hand, it addresses the potential privacy protection issues of standard centralized social platforms, and advocates the use of blockchain technology to escort encrypted transmissions, and further promote the privacy and security of social networking.

Specifically embodied in:

Communication is completely anonymous: it is no longer necessary to register personal information such as mobile phone numbers and email addresses, and return control of user data and information to individuals

Free control of the account, permanent storage of the address book: One-click export of the private key to other apps can continue to use, communication friends follow the account flow, no longer restricted by the APP account system

Peer-to-peer social interaction:

Allow users to run nodes on their own devices to access the network, and real-time interconnection between nodes, user information is stored in encrypted form on network nodes, forming a distributed cloud

Cross-app real-time social networking:

just like sending emails, even if you choose different applications, you can still communicate with each other without barriers

Value return to users:

The network will provide compensation to users who have made storage and computing power contributions to encourage users to make more contributions.

In addition, the privacy social platform will also link all blockchain companies to build an industrial communication platform, provide technology, share, information, applications, communities, and exchange for blockchain users, including consumers, investors, and project service providers. , Payment, e-commerce, games, entertainment and other one-stop services, based on blockchain encryption technology and consensus mechanism, to achieve the entire blockchain industry ecology.

CHAPTER 5

THE FLOEER OF LIFE
THE ORIGIN OF THE UNIVERSE

Chapter 5 - VON Issuance Plan

5.1 Total issuance and usage

We will issue the first token applied to this anonymous public chain based on VON Chain, namely: VON, and will gradually be applied to the development and application of VON Chain. The issuance plan is as follows:

Token name: VON

Total issuance: 168 million

Circulation of Origin Coin: 6 million

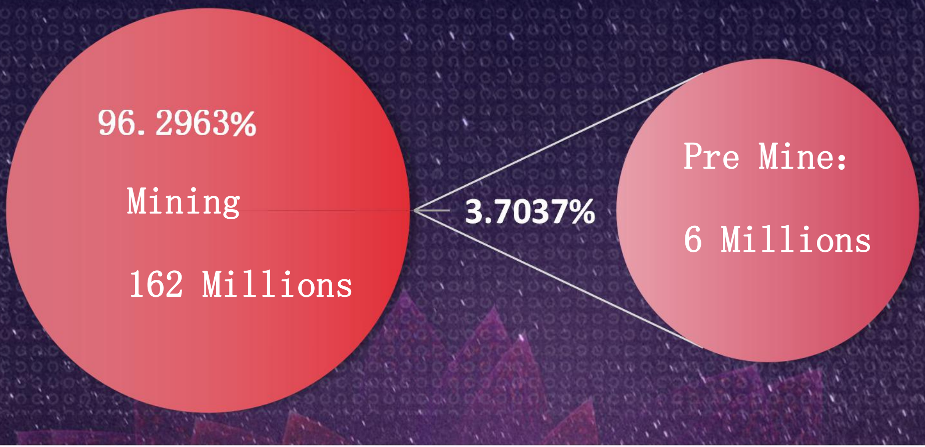
Distribution of Origin Coins:

1 million VON CHAIN ecosystem holdings (used for future technical maintenance, market support and ecological construction, etc.), 1.5 million are reserved for super nodes (rewards issued in stages, for a period of three years), 3.5 million pieces are used for early liquidity mining.

VON CHAIN coin production rules: A block is calculated every 10 seconds, each block contains 5, and the daily output is 43200, which will decrease by 7% every two years until the end of 162 million.

Distribution

Total Amount 168 Millions



96.2963%

Mining

162 Millions

3.7037%

Pre Mine:

6 Millions

5.2 " One System Mine Double Coins" - Sustainable mining mechanism

VON CHAIN pioneered the “One System Mine Double Coins” sustainable mining mechanism. In the VON network, 30% of all VON participating in mining will be automatically triggered by smart contracts to convert into the corresponding Bitcoin mining machine computing power, according to the full Bitcoin mining Net computing power conducts mining and dividends, and another 70% participates in VON liquidity mining.

“One System Mine Double Coins” Final income = Bitcoin + VON

5.3 Origin Coin Limited Sale

3.5 million VON circulates freely in the market for early liquidity mining:

After 7 days of warm-up, 500,000 VONs flow to the free trading market every day. The initial price is 0.3USDT. 30% of the successfully purchased Origin Coins will be converted into Bitcoin mining power based on the market price, and the remaining 70% can participate in VON liquidity Mining or free circulation.

5.4 Super node

In order to ensure the stable operation of the VON public chain, the Ecological Foundation reserves 1 million Origin VON for future technical maintenance and ecological construction, and also uses smart contracts to lock 1.5 million Origin VON for 3 years and continue to issue monthly. 1.5 million VON will be used to reward the top 50 super nodes in the future, aiming to motivate them to make continuous contributions to maintaining the VON ecological network. Super node rewards will announce the results of the election ranking once a month, and rewards will be issued in stages.

CHAPTER 6

THE FLOEER OF LIFE
THE ORIGIN OF THE UNIVERSE

Chapter 6 - Development Plan

The fourth quarter of 2019:

The China Mining Exchange takes the lead in conducting market research, team building, project approval, and technology development.

The first and second quarters of 2020:

In-depth strategic cooperative development with global mines.

The third quarter of 2020:

The project white paper is released.

The fourth quarter of 2020:

Core technology research and development, VON CHAIN construction is completed; the first application running on VON CHAIN is launched, and the main network test is started; the VON public issuance plan is gradually completed.

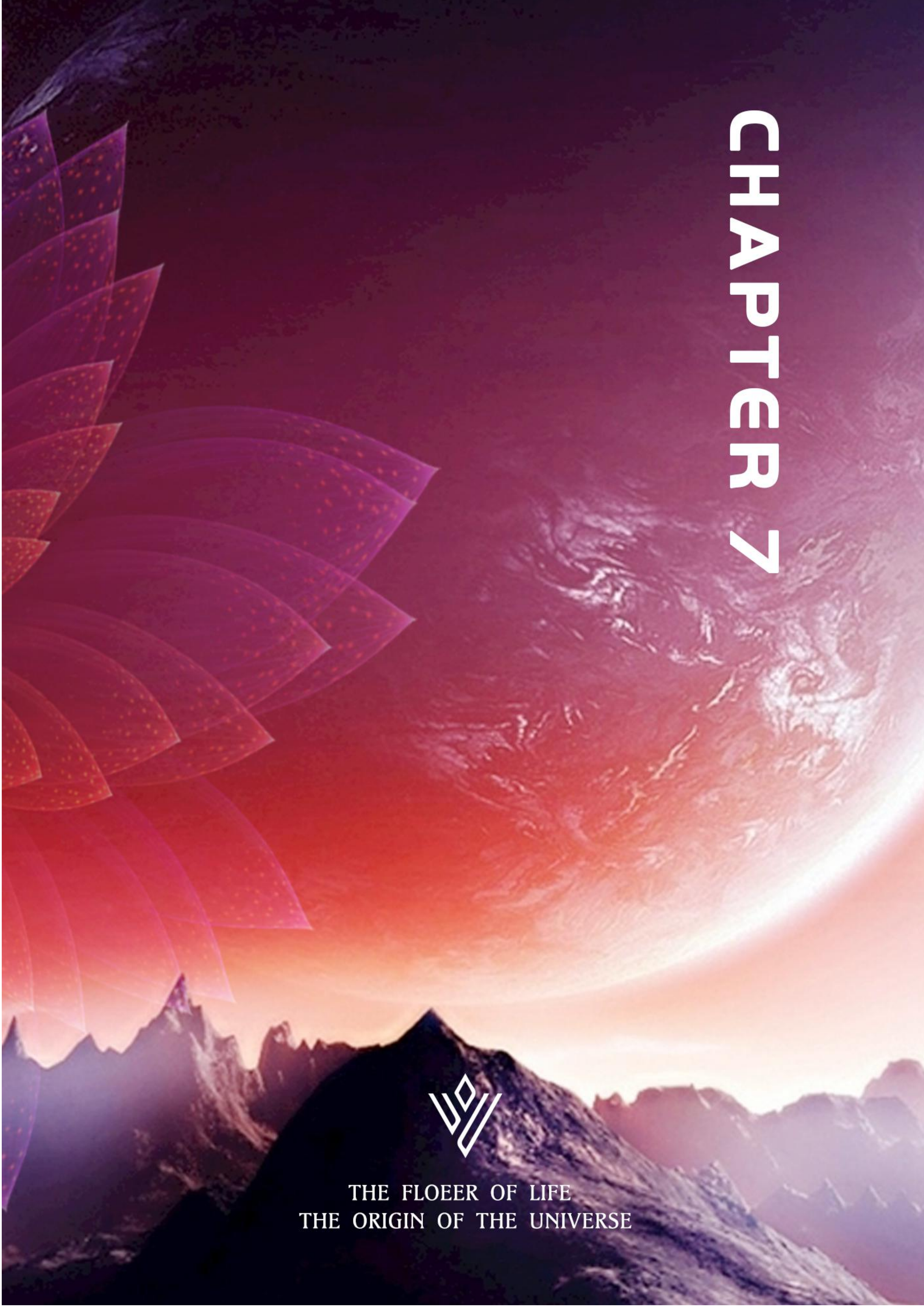
2021:

Enrich the application scenarios of VON CHAIN's first pass VON, such as returning all consumption to the mall.

2022:

Ecological expansion; introduction of on-chain projects, including but not limited to privacy anonymous Defi platform, privacy storage platform, and privacy social platform.

CHAPTER 7



THE FLOEER OF LIFE
THE ORIGIN OF THE UNIVERSE

Chapter 7 - Risk Warning and Disclaimer

7.1 Risk Warning

There are various risks in the development, maintenance and operation of VON CHAIN, many of which are beyond the control of VON CHAIN developers. In addition to the other content described in this white paper, participants are requested to fully understand and agree to accept the following risks:

Regulatory risk

Digital asset transactions, including VON, have extremely high uncertainties. Since the field of digital asset transactions currently lacks strong supervision, there will be risks of skyrocketing and falling, manipulation by dealers, etc., if individual participants lack experience after entering the market , It may be difficult to withstand the asset shock and psychological pressure caused by market instability. Although academic experts and official media have all given suggestions for cautious participation, there are no written supervision methods and provisions, so it is difficult to effectively avoid such risks at present.

Market risk

The issuance of Token by VON CHAIN is inseparable from the situation of the entire digital currency market. For example, the overall downturn in the market or the influence of other uncontrollable factors may cause VON CHAIN itself to have a good prospect, but the price is still undervalued for a long time.

Competitive risk

At present, there are many teams and projects in the field of blockchain technology, and the competition is fierce. There is strong market competition and project operation pressure. Whether VON CHAIN can break through many excellent projects and be widely recognized is not only linked to its own team ability, strategic planning, etc., but also affected by many competitors in the market, and it may face vicious competition.

Team risk

VON CHAIN has gathered a team of talents with both vitality and strength, attracting senior practitioners of blockchain and technical developers with rich management. In the future development, it is not ruled out that the departure of core personnel and internal conflicts within the team will cause the flower of life and the origin of the whole to be negatively affected. Project technology risk The accelerated development of cryptography or the development of technology such as the development of quantum computers may bring the risk of cracking to the flower of life. This may lead to the loss of VON CHAIN data. During the project update process, vulnerabilities may appear, and the vulnerabilities will be fixed in time after they are discovered, but there is no guarantee that they will not cause any impact.

Other unknown risks

With the continuous development of blockchain technology and the overall situation of the industry, VON CHAIN may face some unexpected risks. Participants are asked to fully understand the team background, understand the overall framework and ideas of the project, adjust their vision reasonably, and participate rationally before making participation decisions.

7.2 Disclaimer

This document is only for the purpose of conveying information. The content of the document is for reference only, and does not constitute any suggestion, abetting or solicitation to sell stocks or securities in Flower of Life. This document is neither constituted nor understood to provide any trading behavior, nor is it any form of contract or promise. In view of unpredictable circumstances, the goals listed in this white paper may change. Although the team will do its best to achieve all the goals of this white paper, all individuals and groups involved in the Flower of Life Origin will take their own risks. The content of the document may be adjusted accordingly in the new version of the white paper as the project progresses. The team will publish the updated content to the public by publishing announcements or the new version of the white paper on the website. This document is only used to convey information to specific objects actively requesting to understand the project information, and does not constitute any future investment guidance, nor is it any form of contract or commitment.