AntomPay

White paper

PAYPAL IN THE FIELD OF ANTOMPAY
BLOCKCHAIN PAYMENT

Foreword

In recent years, the cryptocurrency market has become gradually hot. Cryptocurrency has the advantages of high liquidity, high counterfeiting cost, low production cost, decentralization, fair and transparent accounts, and high cost of additional issuance, which is widely sought after by the market and its core

Supporting technology block(Blo AntomPay chain) attracts more and more attention, and is considered to be the core technology of building the next generation of value Internet. The development of blockchain has also led to the rise of distributed accounting technology (Distributed Ledger Technology). Generally speaking, the two concepts are generally considered to be interconnected, referring to the same kind of technology. But in a strict sense, it can be considered as blockchain as an implementation of distributed accounting technology.

Block chain decentralized concept is gradually subvert the traditional monetary concept, and a short time in the world, although the distributed account technology development is very fast, but the whole is still in the early stage, technology far less than the commercial requirements, part of the core technology bottleneck no breakthrough, hindered the large-scale application of the technology. Among them, in the performance bottleneck and communication across the chain pain points, block chain technology high independence and transaction speed greatly limit the circulation of digital assets use space, each block chain system is not connected, agreement, have extremely high independence, each other to message communication and collaborative operation, each block chain digital assets circulation and trading also suffered a great restrictions, and with the increase of block chain system, solve the information exchange between different block chain network and transaction speed problem has become a new trend of the development of block chain technology.

In the existing blockchain technology, the processing capacity of the blockchain is mainly limited by the performance of the consensus algorithm, while the performance of the consensus algorithm is limited by the size of the system node and the processing capacity of a single node. At the current technical level, the space for improvement of single blockchain performance optimization is very limited, and there are performance limits, which seriously restricts the application of distributed ledger technology in large-scale, high concurrency and low latency transactional business scenarios. In the case of Bitcoin, for example, high transfer fees and extremely slow speeds are great drawbacks. The slow transfer speed is unbearable, and the high fees also make small transactions not cost-effective and impossible. It can be predicted that, with the rapid development of the digital economy, the frequency of future transactions rate and scale will go far beyond current levels, and the performance bottleneck is one of the primary problems to be addressed by distributed accounting technology.

In the field of payment, with the increase of the digital currency heat and currency application, the demand for payment is higher and higher, lightning network and lightning network technology should be born, lightning network and lightning network design, however, technology landing difficult, development cycle is longer, the future landing actual application time and effect is unknown.

Therefore, we propose AntomPay network , a layered channel payment network based on flexible multiple signatures, using the existing mature technology, simple principle, simple design, based on AntomPay Network can easily and reliably realize the digital currency.

AntomPay Network is based on AntomPay technology for the underlying AntomPay Network, the integrated use of 2-of-2 multiple signatuare, lock time transactions, transaction structure delay technology such as broadcast, can be in no need to trust, implement block chain assets zero fee second speed transfer, in terms of speed, security and privacy, comparable to Lightning Network.

AntomPay The Advantages Of Networks Are:

- Mature Underlying Technology:

The underlying technology of AntomPay Network is a AntomPay channel established based on mature multiple signature technology, time stamp transaction technology and transaction cold signature technology and other technologies.

- Good Compatibility:

Support most mainstream currencies, even currencies like Dogecoin, which has not been updated with core maintenance for a long time. As long as it is digital currency, it can generally support the implementation of AntomPay Network, and can realize cross-chain cross-currency payment without any adjustment of the core wallet.

- Flexible Application:

AntomPay Network technology can be integrated into the core wallet of the target currency.

- Safe And Concise:

AntomPay Network compared with lightning network, the underlying technology used has been applied on a large scale, safe enough, and the design of AntomPay Network is simple, the application is high.

In the traditional fiat world, users only need one email as an PayPal account to complete high-speed transfer, collection and shopping of more than 20 countries around the world, thus PayPal has become a world-class enterprise. In the blockchain industry, there are no similar products born yet. The design concept of AntomPay is to build an PayPal in the blockchain payment field.

AntomPay We provide different services for business users and individual users, and is committed to creating the era of blockchain payment 3.0. Next, we will introduce the AntomPay design concept, technical architecture, DAPP application and commercial scenarios and other information for you in detail.

Catalogue

5. AntomPay Product

6. AntomPay Token

7. Risk And Statement

1. AntomPay Introduction

1.1 What Is AntomPay?

AntomPay Committed to building a PayPal in the field of blockchain payment, The AntomPay development team has independently developed many core technologies including AntomPay technology, which has significantly solved the low transmission of the existing blockchain system effect problem, Based on the self-developed AntomPay technology and Matching hedge Technology matching hedging technology, AntomPay Built a new blockchain asset payment network- -AntomPay Network, Using AntomPay network (AntomPay Network) to achieve zero cost fast payment of blockchain assets, At the same time, AntomPay integrates the blockchain payment channels of various digital assets into the SDK interface, Create a variety of open tools used in blockchain payment scenarios, For businesses and businesses, Finally, build an open ecosystem based on blockchain finance.

AntomPay The development team has a lot of technological innovations in the development. The key functions such as AntomPay technology and Matching hedge Technology matching and hedging technology independently developed by AntomPay are all innovative functions independently developed by AntomPay.

Based on AntomPay, the AntomPay Network is built by technology for the bottom, comprehensively using 2-of-2 multi-signature, time lock transaction, transaction structure delayed broadcast and other technologies, which can realize zero commission and second speed confirmation of blockchain assets without trust, which is comparable to Lightning Network in terms of speed, security and privacy.

At present, the AntomPay team owns color blockchain technology patents and several software works copyright. The core members of the AntomPay team are all from the blockchain industry, with profound industry resources and background.

2. AntomPay Overview

2.1 AntomPay Concept

AntomPay concept is committed to creating open, comprehensive block chain payment ecosystem AntomPay is committed to creating open, comprehensive block chain payment ecosystem, AntomPay in the face of business users and individual users provides different services and products, in the face of business users, AntomPay provides AntomPay Commercial platform, can achieve a key access AntomPay payment and cross-border payment solutions, etc. For individual users, AntomPay provides mobile DAPP wallet, encrypted communication module based on RSA algorithm, over-the-counter guaranteed transaction, high-speed transaction and other customized functions for cryptocurrency users.

2.2 AntomPay Technology

The AntomPay has independently developed the AntomPay technology, AntomPay independently developed "AntomPay technology", AntomPay Technology uses a variety of mature technologies, such as timestamp trading and 2-of-2 multiple signature technology, Real-time payments can be made using AntomPay technology, Real-time payment, And has zero handling fees, So using AntomPay to send bitcoin (or other cryptocurrencies) can be paid with zero fees, Bring users a brand new payment experience, And unlike the off-chain wallet implemented by centralized database technology, AntomPay Technology is decentralized, The user's assets are completely in the user's own hands, The query channel can be performed on the blockchain, Will not be used by the platform, absolute security.

Compared with the high transfer fee of ordinary digital wallet and the extremely slow transfer time, AntomPay can realize zero commission and second-level digital asset transfer between users through the self-developed AntomPay, bringing the 3.0 era of blockchain payment!

2.3 Universal Address For AntonPay

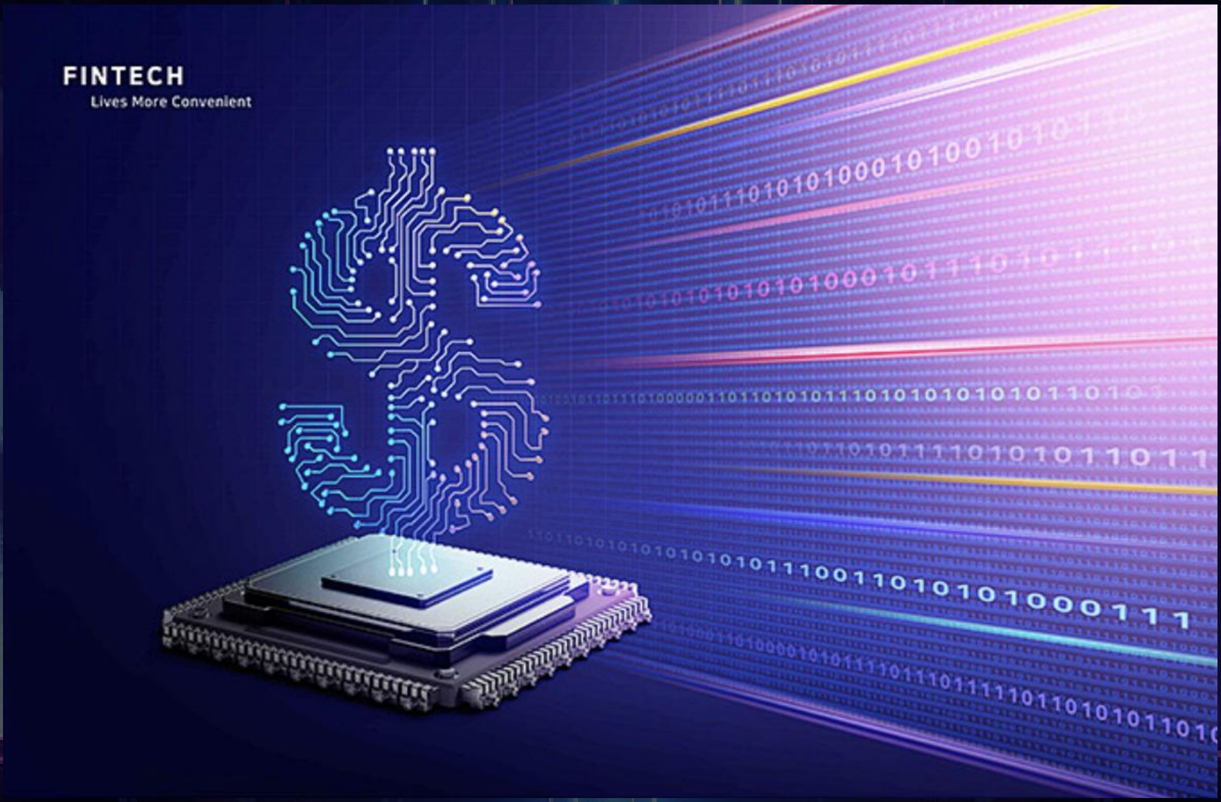
AntomPay uses a universal address, which can receive and send 95% of cryptocurrencies, The emergence of common addresses can help users avoid the trouble of managing multiple currency addresses, just as having an paypal account, can send and receive more than 20 legal currencies around the world. The general address is defined by the user, which can be the currency address of a mainstream digital asset, or an ID number, mailbox or mobile phone number. Using the common address, you can easily receive, send, maintain and manage your own blockchain assets.

2.4 Matching Hedge Technology

AntomPay has independently developed the Matching hedge Technology matching and hedging technology, which can realize cross-chain trading.

AntomPay Through the self-developed MatchinghedgeTechnology matching hedging technology, it can meet the free conversion and payment between different users in multiple currencies. Even with good matching hedging and established AntomPay channels, cross-chain transactions can be realized at second speed and zero fee.

The cross-chain implemented in this cross-chain protocol is an open source open protocol, as long as users abide by this protocol without even going through the AntomPay platform, so as to ensure that the cross-chain can be open, fair and enough decentralized.



3. AntomPay Core Technology

3.1 AntomPay Technology

Use multiple signature technology to establish transaction channels and realize the top speed transaction comparable to lightning network. The core of AntomPay technology is to realize the high speed transaction through multiple signature technology. Its security is higher than zero confirmation, and its simplicity and landing are better than lightning network.

3.1.1 Core Process Of AntomPay Technology Implementation

- Collect The Respective Public Keys Of A And B To Generate The Multiple Signature Addresses Of Two AntomPay:

Suppose A is the holder of the 1 Bit address and B is the holder of the 1Dog address. The public key can generate two multiple signature composite addresses of 2-of-2, namely 3 CSm address and 3 Njd address. The public key is the information that can be disclosed and can be disclosed voluntarily. Composite addresses can also be quickly generated online.

- A Constructs The Transaction TX 1 Sent To The Contract Address, And Sends Back The Transaction TX 2 From The Composite Address Lock Time To B:

A uses the private key of 1 Bit address to sign A transaction sent to the 3 CSm composite address. As long as the transaction ID and location n data are built enough, it can be released without broadcasting.

Then A or B, or preferably A, construct A transaction TX 2 from the 1 Bit address. Please change the n-AntomPay-time lock time to A reasonable time, such as after one year. The n-AntomPay-time, also known as Lo-AntomPay-Time or lo-AntomPay _time, is usually set to 0, indicating that transactions can be sent to the Bitcoin network at any time. If the value of nLo-AntomPay-time is between 100 and 500 million, it means that a block whose height should be greater than or equal to nLo AntomPay time can only be written to the blockchain. If the value of nLo-AntomPay-time exceeds 500 million, it starts from January 1,1970, plus a time point after nLo-AntomPay-time seconds, namely Unix timestamp, for example, January 1,2017 is 1403200,000, if earlier than that point, the transaction will not be sent to the Bitcoin network. Note note sequence field, not the maximum INT 32 (0xffffffff), otherwise nLo-AntomPay-time will be ignored.

- TX2 Transactions

A to B transaction TX 2 transaction, get the signature broadcast TX 1 to form the lightning payment channel to send the above transaction TX 2 to B, ask B to confirm that there is no problem, then sign with the private key. After receiving the signature from B, A then signs it again with its own private key to see if it is successful. If successful, the previous transaction TX 1 can be sent out, thus forming a lightning-like payment channel. The TX 2 transaction in hand is preserved, and may need to be broadcast after the lock time.

In fact, on the basis of certain trust in B, A can not manually construct transactions TX 1, but directly use the wallet software to the 3 CSm address. Then let B use the information of the transaction TX 1 to construct A signed 1 Bit address transaction with locked time, and then sign B and sends it to A, so that A can keep it properly. It can also form a lightning payment channel, and the technical requirements for A will be very low, but B should have enough credit, and the previous scheme does not need B to have any credit.

After the establishment of the lightning payment channel, when A needs to pay B coins, a pair of two transaction TX 3 from 3 CSm address to 1Dog address and 1 Bit address. Signed with its private key and send to B. When B gets the signature transaction TX 3, it is already equivalent to confirming to get the currency. This speed is only generated transaction and transmission strings can do the second speed, and even can do real-time payment under some tools.

3.1.2 Specific Application Of The AntomPay

If A transfers 0.1 BTC to the 3 CSm address, A needs to pay 0.02 BTC to B, then construct A 0.02 BTC to B and 0.0799 BTC to 1 Bit address to A, with 0.0001 BTC as the handling fee. A uses the private key signature, and B sends it to B. B uses the private key signature to confirm that there is no problem in determining A signature, that is, the payment of 0.02BTC is received, so it is not necessary to broadcast this transaction TX 3. Can continue to maintain the class of lightning type payment channel.

Then, A few days later, when A needs to pay B 0.03 BTC again this time, plus the last total is 0.05 BTC, then to construct A TX 4 again, this time to send B 1Dog address 0.05 BTC, change to 0.0499 BTC of 1 Bit address of A. After signing, it can be sent to B, second speed confirmation, and because it is under the chain, there is no handling fee.

Note that someone may have found that this kind of lightning payment channel is one-way, but A pays B, so what when reverse B needs to pay A? You can repeat the above steps to establish a lightning-type payment pass between AB.

Do, pay attention to the swap AB, and use another 2-of-2 multiple signature composite address 3 Njd address as the main address of the lightning payment channel, the main control of this address is B, B can be signed to the transaction to A, to achieve B to pay A. In fact, this way with two channels to achieve both directions will be more clear.

Essentially, because of the locked time transaction TX 2 existence, the coin on the 3 CSm address belongs to A.3 The coin on the Njd address belongs to the B. In need class lightning payment, A can sign transaction TX 3 redistribution 3 CSm address currency will need to pay B currency allocated to B, as long as get signature transaction TX 3, is released as long as before the lock time, there is no need to immediately announced and close the channel, and many frequent between send and receive transaction is just send the latest transaction, and the data even if the third party get no use, also can broadcast, because there is only A signature.

3.1.3 Two Closed Forms Of The Payment Channel

1.There is no lightning payment transaction between A and B. After the lock time is up, A can broadcast the transaction TX 2, so as to get back all the coins on the 3 CSm address, so as to close the channel. A loses only the locking time and A little commission fee, and no big loss. The next time, you can only open B, which is likely to pay at a higher frequency, and try to set the lock time for a long time, so as to avoid the opening of the lightning payment channel without use.

2.A has coins reassigned 3 CSm address through several signature transactions issued to B through the lightning payment channel. Before the lock time comes, B is the most beneficial for itself and generally the latest signature transaction, after signing and then broadcasting, so that the lightning payment channel chain settlement successfully closed the channel.

Then if there is a lightning payment demand, you can repeat the above steps to open again, and 2-of-2 multiple signature composite address 3 CSm address, is not replaced, can continue to use. Because the transaction ID in TX 1 and the transaction ID of TX 2 have changed, the previous signatures will become invalid, so there is no need to worry about the transaction signature of the last lightning payment channel, which will have an impact on the new lightning payment channel.

3.2 Core Design Of AntomPay Network

3.2.1 Multiple Signature And Composite Address Generation

Multiple signature composite address, starting with 3 Bitcoin address sending and receiving coins, and this Bitcoin address starting with 3 is the contract script, and then the contract script hash160 algorithm, and then with the 005 version of Base58Che-AntomPay code. The coins in these synthetic addresses, according to the requirements of the contract script set at the time of generation, generally requires multiple private keys for signature, so it is often called the composite address as multiple signature addresses. In fact, depending on the specific contract script set when generated, some scripts can be set to need only a signature, not necessarily multiple signatures. Because it is generally synthesized by multiple public keys, it is better to name it as a composite address.

Multiple signature technology createmultisig command generation composite address, the generation of "contract script" content is very critical, can be used with this createmultisig command to generate. This command is widely used and flexible, but it is simple, with only two parameters that must be input:

One parameter is the number M, which is a positive integer, and requires that M be greater than N in the following parameter. Another parameter is an array of length N, where the number of public keys placed in the array is N.

He specific meaning is that you need to provide any M signatures of the private keys corresponding to N public keys. If M=1, the private key corresponding to any public key in the following array can be used. If M=N, it means that all private keys must be signed to spend coins. The intermediate cases of these two extremes tend to be more often used.

The commonly used composite address generation method of multiple signatures of 2-of-3 is that the first parameter M is set to 2. In the second array parameter, three public keys are put in, so the generated composite address is that as long as any two of the private keys corresponding to the three public keys are signed, you can spend the transaction. There are also many applications in the field of e-commerce. Buyers, sellers and platforms can each take a private key, usually buyers and sellers can gather enough two signatures, but when there is a dispute, the platform can use its signature to decide the distribution of flat coins.

3.2.2 Signature Of The Distribution Fee To Redistribute The Payment

This allocation fund is the key to realizing the payment channel. Specifically, use the multiple signatures mentioned above. Specifically, 2-of-2 multiple signatures are generated, which simply refers to the transaction only when a consensus agreement is reached between the two addresses. The parameter M is set to 2, while the array of public keys are filled in two public keys. Both sides agreed to sign the allocation in the 2-of-2 multi-signature composite address.

The channel design idea of lightning network and lightning network is that both sides jointly send a certain amount of funds to form the allocation of gold, and then give the allocation scheme of how many coins. Then sign together to update the assignment scheme. The same mechanism is designed to abolish the previous historical distribution. The difference between the latest distribution scheme and the previous distribution scheme, which is the amount of currency paid by the channel. Because only the signature, the verification is correct, just need to send to the other party, do not need to broadcast on the main "Bitcoin" main network, so it can achieve second speed confirmation. Although the opening and closing of the channel requires a certain handling fee, but the establishment of the channel after the transaction on the channel is completely free, or very low cost.

AntomPay The network is also the distribution gold channel, the basic principle of signature to redistribution, but will be easier to understand and easy to implement.

3.2.3 The AntomPay Unidirectional Channel Was Established

Simply put, it is the sender and the receiver, the sender sends the currency to the public key generation address of both, and then realizes the payment by signing multiple times to allocate the increasing proportion to the recipient. In addition, there is a timestamp transaction that, after time, returns all the allocated coins to the sender.

This channel is one-way, only when A needs to pay B coins, and the amount allocated to B will be increasing. When B needs to pay A, you needs to build a reverse channel with 3 Njd address. Two channels can interact to make a two-way payment. And the channel closes when the amount is exceeded. Additional note the need to close the AntomPay channel before the time of nLo-AntomPay-time. Note that the modified nLo-AntomPay-time lock time to a reasonable time nLo-AntomPay-time, also called Lo-AntomPay-Time or loAntomPay_time, is usually set to 0, indicating that a transaction can be sent to the Bitcoin network at any time. If the value of nLoAntomPaytime is between 100 and 500 million, it means that a block whose height is greater than or equal to nLo-AntomPay-time can only be written to the blockchain. If the value of nLo-AntomPay-time exceeds 500 million, it starts from January 01,1970, plus a time point after nLo-AntomPay-time seconds, namely Unix timestamp, for example, 1514736000 on January 1,2018. If earlier than that time point, the transaction will not be sent to the Bitcoin network. Note note sequence field, not the maximum INT 32 value (0xffffffff), otherwise nLo-AntomPay-time will be ignored.
1.Collect A and B to generate the multiple signature address of two AntomPay assuming that A is the sender and B is the receiver, the public key can generate two 2-of-2 multi-signature composite addresses after exchanging the position of the public key, the public key, the public key is the information that can be disclosed, can be proactively disclosed, or the composite address can be quickly generated online.

2.A constructs the transaction TX 1 sent to the contract address, and from the composite address lock time sends the transaction TX 2 to B3) A sends to B transaction TX 2, broadcast the channel to send the transaction TX 2 to B. B will send the transaction back to A with the private key of 1Dog address. After receiving the signature from B, A then signs with the private key of its own 1 Bit address to check for success. If the TX 2 is successfully verified, the previous transaction TX 1 can be sent out to form a lightning-like payment channel. TX 2 trading in hand attention to save, such as the lock time may need to broadcast back.

3.2.4 AntomPay Channel Realizes Bidirectional And Cross The Chain

The 2-of-2 multiple signature AntomPay network channel is one way, which may be the biggest difference with the lightning network, only one direction from one direction to the other side. If you want the two sides to switch, it is necessary to establish two independent channels to achieve. The lightning network can be increased or reduced, completely can be arbitrarily redistributed, can be added can be reduced, as long as there are both sides can sign, with the latest time allocation scheme shall prevail, the previous any allocation scheme will be invalid. And the kind of lightning payment is no time order, are effective. But as the recipient, of course, will take the largest amount of money, is generally the latest allocation plan. The sender of the coin cannot issue any assigned version without the signature of the recipient. Wait for the time stamp, or wait for the recipient to close.

Because as long as multiple signatures are supported, AntomPay channels can be realized with time stamp transactions, A to B can be the Bitcoin AntomPay channel, while B to A is the Dogecoin AntomPay channel. This is equivalent to the realization of cross-chain and safe currency transactions.

3.2.5 A AntomPay Network With A Hierarchical Tree Topology

Network topology mode, the third-party payment will be (a) star shape, while the point-to-point of bitcoin is figure (c) network status. Lightning network estimates early may pepper (b) ring has travel chain six, and our AntomPay net naked will be similar to the tree shape.

The AntomPay operation principle is to initiate 2of2 multiple signature, and then initiate a delayed transaction of all coins regression. By sending the transaction signature, gradually increasing the distribution to achieve one-way rapid payment. Establish two channels because you only need to send the signed string, do not need to broadcast, which can achieve fast real-time and 0 fee transaction.

3.2.6 AntomPay Network Payment Path Design

The root node will be responsible for the transactions across the branches, so if only one layer is similar to a star line network, passing through one node. And the two layers of the network, up to three nodes in the middle. The three-layer network is, at most, with five nodes in the middle. The N layer network has up to 2N-1 nodes, all first from the previous level to the root node. To the goal. If it is in the same branch, it does not need to go up, similar to the domain name resolution service.

The root node can store all the latest data here, and settle with the lower node regularly.

3.2.7 Application In Special Cases

AntomPay Response to node problems:

Because 2of2 requires the signature of both parties to move the currency, even if a large number of nodes are gone, it will not cause a loss of funds.

1. There is no lightning payment transaction between A and B. After the lock time is up, A can broadcast the transaction TX 2, so as to get back all the coins on the 3 CSm address, so as to close the channel. A loses only the locking time and A little commission fee, and no big loss. The next time, you can only open B, which is likely to pay at a higher frequency, and try to set the lock time for a long time, so as to avoid the opening of the lightning payment channel without use.

2. A has coins reassigned 3 CSm address through several signature transactions issued to B through the lightning payment channel. Before the lock time comes, B is the most beneficial for itself and generally the latest signature transaction, after signing and then broadcasting, so that the lightning payment channel chain settlement successfully closed the channel.

Then if there is a lightning payment demand, you can repeat the above steps to open again, and 2-of-2 multiple signature composite address 3 CSm address, is not replaced, can continue to use. Because the transaction ID in TX 1 and the transaction ID of TX 2 have changed, the previous signatures will become invalid, so there is no need to worry about the transaction signature of the last lightning payment channel, which will have an impact on the new lightning payment channel.

3.2.8 Using The Matching Hedge Technology Matching Hedging Technology Can Realize The Cross-chain Trading

AntomPay wallet client to connect users with AntomPay Network, AntomPay Network as the middle layer to link each user.

Specific case:

Take the cross-chain transaction of Dogecocoin and Bitcoin as an example,the specific process is as follows:

I users through common address technology to obtain their common address in AntomPay Network, Dogecoin and Bitcoin address are one to one.

In the case of a single user II, A uses the btc and AntomPay to anchor the latest transaction data on AntomPay, build AntomPay channel and multiple signature technology, and broadcast the transaction to the corresponding blockchain system respectively.

3.3 Universal Address: A Common Address Can Receive And Send 95% Of The Cryptocurrency

3.3.1 Traditional Address Generation Principle

General blockchain address generation needs to go through the following process:

1.Randomly selects a number of 32 bytes as the private key, lying in between Between the 1-and 0-0 xFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141

2.Uses the elliptic curve encryption algorithm to calculate the private key.

3.Calculates the SHA-256 hash of the public key, assumed AIV RIPEMD-160 hash of A, BV plus address version number before B, the resulting value is assumed the SHA-256 hash of CVI C and D.

4.Calculated the SHA-256 hash of D and Jiading as E.

5.Takes the first four bits of E, loads the four bits after C, as a test, and the result value is F.

6.Transforms F with the Base58 representation, and the result is G, of which G is the most common Bitcoin address form.

3.3.2 Specific Cases: Mutual Conversion Between Addresses

Ethereum, Ethereum-based tokens, Bitcoins, and the public key of the mainstream currencies on the market, as well as the 40 hex number after SHA-256 and RIPEMD-160 are the same, the difference between the currency addresses, is in the pre-version area shown in the serial number in figure 2.1 above, such as the currency area is 0x00, dogcoin is 0x1E, Wright coin is 0x30.

After understanding this process, the mutual conversion between currency addresses can be realized. To dog currency, for example, in the process 11 any other currency address for Base58 reverse coding, remove the first two hexadecimal version number and after 4 elements to check code, according to the need to add into the corresponding currency front version 0x1E and calculation with additional inspection, then after Base58Encode can get the corresponding dog currency address.

4. Rrchitectural Design

4.1 Overall Architecture

AntomPay The overall architecture is divided into three layers: core layer, service layer and application layer.

4.1.1 Core Layer

The blockchain part composed of blockchain nodes and message network realizes the broadcast of transaction data and is input into the blockchain through miners. Among them, AntomPay channel technology is adopted to open the payment channel in advance to realize fast transactions. Provide data storage for IM services.

4.1.2 Service Layer

For business scenarios, this layer adopts MVC architecture to separate the client and B-segment merchant business: provides corresponding API interface for wallet client; provides integrated SDK for B-end merchant applications to facilitate third-party docking and calling. For the IM part, this layer provides the corresponding processing logic to carry the interaction between the read and write of the application layer IM and the core layer data cluster.

4.1.3 Application Layer

This layer provides application services based on distributed ledger to end users, such as currency digital asset wallet, transactions, third-party application docking SDK writing transactions, etc.

4.2 Overall Architecture Design

4.2.1 Each Level Is Described As Follows

- User Side

This layer focuses on the mobile terminal, supports the iOS / Android system, and connects to the customer service system.

- User-Side API

This layer provides TCP protocol and HTTP protocol according to different business types to provide iOS / Android development SDK for mobile terminals. H5 page, providing the WebSoAntomPayet interface.

- Access Layer

This layer mainly protects the massive user connection and attacks protection, and the rectified massive connection forms into a small number of TCP connections and communicates with the logic layer.

- Logic Layer

This layer is responsible for the core logic implementation of the IM system, such as: group chat, single chat, circle of friends, and so on.exist

- Such As

Group chat, Single chat, Circle of friends, and so on.exist

- Reservoir

This layer is responsible for caching or storing IM system related data, mainly including user status, message data, file data, etc.

4.2.2 Data Storage Format Adopts ProtocolBuffer, And Database Selects MoogoDB

ProtocolBuffer Is a lightweight and efficient structured data storage format, in the. The message format is programmed, and the protocalbuffer compilation program is used to directly generate the target file, so that it is convenient for multi-terminal synchronization. In addition, the target file can be run between major platforms to solve cross-platform problems.

ProtocolBuffer Is like XML, but smaller, faster, and simpler, with good performance and high efficiency in resolution speed and footprint. ProtocolBuffer No need to parse before mapping, direct serialization directly corresponds to the data class in the application.

MoogoDB Hot data can be loaded into the memory, in the large amount of data is, the query efficiency advantage is obvious Moo-goDB using the BSON way to store data, has a very good support for JSON format data, convenient between the platform docking MoogoDB database fragmentation cluster load has a very good scalability and very good automatic failover.

5. AntomPay Product

5.1 AntomPay Mobile Wallet

AntomPay mobile wallet, based on AntomPay technology and general address technology and other technologies disruptive blockchain wallet for individual users, AntomPay provides DAPP wallet, AntomPay mobile wallet exclusively for encrypted digital industry users, based on AntomPay technology and general address technology to build AntomPay mobile wallet, AntomPay mobile wallet can realize the following functions:

- 1.1 It takes only a private key and a common address to easily manage blockchain assets.
- 1.2 Sending and receiving Bitcoins (or other cryptocurrencies) is a quick arrival and zero fees.
- 1.3 Support for most mainstream cryptocurrencies.
- 1.4 Communication module based on RSA algorithm encryption, to achieve absolutely private information communication.

AntomPay Mobile wallet built-in encryption communication function, based on AES algorithm encryption, using the principle of public or private key to build efficient, trusted and secure encrypted communication services, all you send information through the AES algorithm encryption, ensure the user's data and privacy, AntomPay built-in encryption communication function will provide encrypted digital users with absolute privacy communication services.

Ordinary IM communications have a central system to manage user accounts, and security issues rely on reliable or qualified certificates. In this mode, if the certification authority has certain network hardware between the user server and the target server, it will be able to conduct targeted man-in-the-middle attacks on seemingly secure communication at will.

Solution: AntomPay On the basis of traditional server technology, AntomPay will generate a pair of public key and private key for users, in which the public key and private key are generated by RSA algorithm and are unique corresponding to ensure data security. During the communication process, the message is transmitted from A to B, and the message content of A is encrypted with the public key of B. After the message is sent, B decrypts the message content with its own unique private key. In this way, the whole message is invisible to all users except B in each link of the system.

- 1.5 Realize Over-The-Counter Guaranteed Transactions Based On Smart Contracts

AntomPay Mobile wallet can realize the over-the-counter guarantee transaction based on smart contract, that is, the two parties will hit the currency to the channel, and by the smart contract to guarantee and open the currency exchange channel, it will be 7 * 24 hours without rest, and realize the exchange of second speed, the handling fee is almost zero.

5.2 AntomPay Commercia Lplatform:

All-channel support, full-platform support, and full-scenario support.

For merchant users, AntomPay provides AntomPay Commercial platform, AntomPay Commercial platform provides traditional payment level SDK, and provides a sandbox environment for testing, and SDK supports access to traditional Web, app and offline stores.

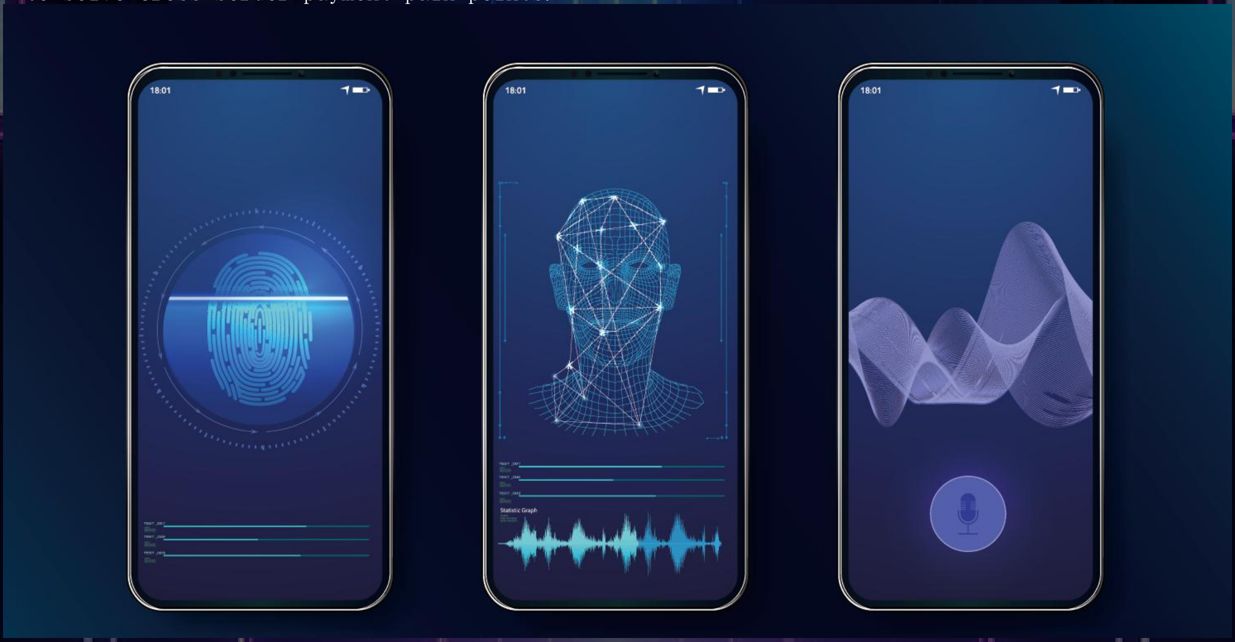
AntomPay Commercial platform Provide support for full payment scenarios on mobile and PC terminals, including IOS, Android and HTML 5, to meet the needs of merchants in multiple business scenarios and provide support for the diversification of user business scenarios. Merchants can use AntomPay Commercial platform to accept digital currency payment from users all over the world at zero cost.

5.2.1 Merchants Can Access AntomPay Payment With One Click

Businesses all over the world can easily access the SDK provided by AntomPay to their own websites and apps with one click, Can accept transnational payments from users around the world, The full-platform SDK allows merchants to minimize access time and manpower for payment, Users will only have to pay for the cryptocurrency, You can buy exotic goods quickly, AntomPay The service is real-time and low, And the use of blockchain as a capital channel can achieve real-time, security, Merchants can manage all orders in these payment pipelines through the merchant management background provided by the AntomPay commercial platform Commercial platform.

5.2.2 Cross-Border Payment Solutions

In the traditional cross-border payment, often face high transfer fees, settlement cycle, slow to the account, transfer amount limit, frozen risk, these risks often bring to enterprise users management unnecessary losses, cross-border payment under the traditional financial system is difficult to have a breakthrough point, and block chain provides friction-free, real-time and efficient decentralized payment network, is an effective tool to solve cross-border payment pain points.



6. AntomPay Token

6.1 AntomPay Mobile Wallet

- Entry Name：AntomPay
- Token Name：ATPT
- Total Issuance Amount：500 Million Pieces
- Specific Allocation:

IDO：10%，through the market IDO output，without lock warehouse，all released before the line.

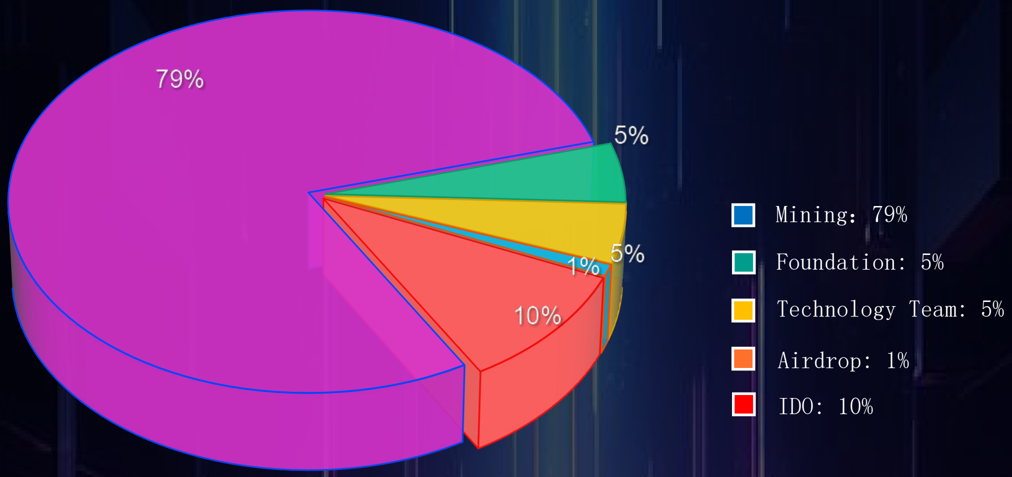
Community Foundation：5%，locked up for 6 months，after which the foundation representative disclosed the details of the use.

Technical Team：5%，locked up for 3 years，and then release 1% every year until the release.

Air Drop：1%，0.5% of the online money，0.5% after the online release.

Mining：79%，mined by global consensus users，is expected to be excavated within 10 years.

Allocation as shown in the figure 500 million pieces：



6.2 The Application Of Antom Tokens

- Antom Tokens Are Applied Tokens. The Main Uses Of Antom Tokens In AntomPay Network are:

1. As a trace transaction fee to prevent dust transaction attack charges.

2. Credit guarantee fee and settlement service fee when building the soft network joints.

3. Intermediate conversion of various digital currencies in cross-chain AntomPay.

4. Income certificate of idle bandwidth share.

5. AntomPay system circulation certificate.

6. In the AntomPay network, CDN accelerates the demand to buy the tokens necessary for traffic.

6.3 Core Team

The core team of AntomPay has created an innovative ecosystem that combines advanced blockchain and artificial intelligence technologies by bringing together world-class technology experts, business strategists, and regulatory experts, aiming to provide users worldwide with a more efficient, secure, and intelligent service experience.

Steve/CEO

Graduated from Nanyang Business School in Singapore with a degree in Banking and Finance. Steve once served as the General Manager of an import and export trading company, with a revenue of $50 million, before switching to cryptocurrency business. Steve is also an active member of the Reddit Bitcoin community.

Matt /COO

Matt has 12 years of operational experience in marketing, blockchain, and business development. At present, Matt focuses on the operation incubation of blockchain projects and the evaluation of the security of blockchain underlying architecture technology. Before joining the Gemini Spiral, Matt was the General Manager of Operations at the well-known financial institution Overseas Chinese Bank in Singapore.

TEO/CTO

TEO has over 10 years of experience in software engineering and blockchain technology. As a technical expert, he worked at a computer and software services company specializing in the Internet of Things. At the same time, TEO is also a member of the Singapore Blockchain Association and began operating in the blockchain and payment fields at the age of 25.

Janice/CFO

Graduated from a public university in Singapore and obtained an MBA degree. Before joining the Gemini Spiral, Janice worked as the Chief Accountant at the well-known financial institution in Singapore, Dahua Bank. Earlier, she also served as the Deputy Director of Finance for Globespan Group (Asia Pacific region) in the United States. Janice has over 10 years of work experience in the finance field, with locations throughout major regions around the world such as Singapore and the United States.

7. Risk And Statement

7.1 Risk Warning

The AntomPay team believes that there are many risks in the development, maintenance and operation of its ecosystem, many of which are beyond the control of the platform. Each AntomPay token participant should carefully read, understand and consider the following risks. If they participate in the AntomPay ecosystem, it will depend that the participants are fully aware of and agree to accept the following risks:

Blockchain technology is limited to the supervision and control of several different regulatory organizations around the world. AntomPay Or limited to their requests or actions, including but not limited to limiting the use of digital tokens, token buyers must conduct their own responsible investigations to ensure that they follow all their local relationships to cryptocurrencies, taxes, bonds, and other regulations.

7.1.1 Legal Policies And Regulatory Risks

AntomPay The ecology is still in the development stage, and due to the complexity of the development technologies, the team may occasionally face unpredictable and insurmountable technical difficulties. Therefore, the development of the AntomPay ecology may fail or terminate at any time for any reason.

7.1.2 Technical Risks

No one can guarantee that the source code of the AntomPay ecosystem is completely flawless. The code may have certain flaws, errors, defects, and vulnerabilities that may compromise the availability, stability, security of the ecology, and thus negatively affect the value of AntomPay.

7.1.3 Source Code Vulnerability Risk

AntomPay It is not a currency issued by any person, entity, central bank or national, supranational or quasi-state organization, nor is it supported by any hard assets or other credit. AntomPay Transactions in the market are based only on the consensus of the relevant market participants on their value. No one is obliged to purchase from the AntomPay holder, and no one can to any extent guarantee the liquidity or market price of the AntomPay at any time.

7.1.4 Liquidity Risk

When traded on the open market, crypto tokens are usually volatile in price. Price shocks can often occur in the short term. Such price fluctuations may be caused by market forces (including speculative trading), regulatory policy changes, technological innovation, availability of exchanges and other objective factors, which also reflect changes in the balance between supply and demand. AntomPay The risks involved in the transaction price shall be borne by the AntomPay trader himself.

7.1.5 Risk Of Price Fluctuation

As of the date of this white paper, AntomPay ecology is still in the development stage, its philosophy, consensus mechanism, algorithms, code and other technical specifications and parameters may be constantly updated and changed, insufficient information disclosure is inevitable and reasonable.

7.2 Disclaimer

AntomPay Ecological participants to volunteer, risk, responsibility, cost principle, participants should be at least 18 one full year of age, with the law of the natural person, and voluntarily accept and abide by AntomPay ecological rules and matters needing attention, all by participants directly or indirectly caused legal responsibility shall be borne by the participants.

Project participants have confirmed that they have sufficient physical, psychological and material preparation to attend, to all the risks and lead to all kinds of consequences can be borne, and promised in the project all about their personal, property and spiritual losses will not be to the project organizers, organizers or association shall be investigated for legal responsibility.