2021-12-15

SAFE(AnWang)：

A blockchain platform focusing on secure payment and digital-assets privacy protection v1.3

By the SAFE Foundation, Singapore

catalogue

SAFE network is the best application development and practice platform for enterprises and institutions to implement the "blockchain +" strategy. This white paper mainly introduces the development history, research and development team, commercial value, system architecture and technical solutions of SAFE network. The technical solutions are constantly updated and iteration, please go to the official website of SAFE network (anwang.com), the latest version.

1 Preface

SAFE network (SAFE) is a decentralized blockchain digital asset issuance and application development platform focusing on blockchain application security and privacy protection, launched by the SAFE Foundation of Singapore. Anyone can issue digital assets and develop blockchain applications based on the SAFE network without review. SAFE network provides more secure blockchain application development solutions through Sapp application development protocol, but also provides high security, compatible with EOS and ETH smart contract, side chain smart contract system-security code.

1.1 History of blockchain development

Bitcoin, born in 2009, is the first and most successful blockchain application. The core technology of blockchain, —— cryptography and distributed systems, have long since emerged.

- In 1976, the BaileyW.Diffie、MartinE. Hellman The paper "The New Direction of Cryptography" published by two cryptography masters marks the development of cryptography into a new era.
- In 1979, RalfMerkle proposed Merkle-Tree. Merkle-Tree was mainly used to quickly verify the data integrity of a distributed network, and Bitcoin used Merkle-Tree for data integrity verification.
- In 1985, Koblitz and Miller proposed the famous elliptic curve encryption (ECC) algorithm. Compared with RSA, ECC is more secure, faster computing and lower bandwidth requirements, which makes asymmetric encryption enter the practical stage. Bitcoin uses ECC as a signature technology.
- The NSA released SHA-1, SHA-1 and later continued releases SHA-224, SHA-256, SHA-384, SHA-512, forming the large family of SHA algorithms. Bitcoin uses SHA-256 as a hash algorithm.
- In 1997, AdamBack proposed the HashCash algorithm in a paper to prevent spam email, a technology used by Bitcoin as a Proof-of-work (POW, proof of work) algorithm.
- Turing Award winner LeslieLamport is a pioneer in distributed computing. He started distributed computing research as early as 1978. In 1982, he published the paper "General Byzantine

Problem", marking the entry of distributed computing from research to practical research.

- P2P protocol began to appear, especially the BT appeared in 2003, let the development of P2P technology into the fast track.

At this point, the cryptography, distribution, POW algorithms, and other technologies needed for Bitcoin are all ready. In November 2008, Satoshi Nakamoto's famous paper "Bitcoin: Point-to-Point Electronic Cash System" was officially released. In January 2009, Satoshi Nakamoto dug out the founding block, containing the classic words: " The Times 03 / Jan / 2009 Chancellor on brink of second bail out for banks.", marking the official birth of bitcoin, the first application of blockchain.

1.2 Project Background and Significance

The background and significance of the SAFE network security project are mainly explained from three aspects: application and asset security, convenience of asset issuance, and privacy protection.

.11.2 Application and asset security

Open source, the mainstream of the community block chain application development platform is Ethereum, EOS, enterprises, unit level, the mainstream of no token block chain application development platform is Fabric, their common feature is the use of smart contracts to issue tokens and development block chain application, with compilation tools the source code compiled into executable code embedded into the transaction, then use virtual machine to load executable code verification execution results.

Smart contract system is a very new direction and topic, but at present, the security is worrying. Fabric Smart contracts are rarely used in the free community, without too many problems, but Ethereum and EOS, the smart contract security problem has been very prominent.

In 2016, DAO smart contract was stolen by hackers from ETH. In order to protect the interests of investors, the Ethereum official team canceled all DAO transactions, which clashed with the concept of blockchain, and led to the fork of ETH and ETC;

In July of that year, Parity, also based on Ethereum, stole more than $30 million, and about $150 million of user money was frozen in Parity in November.

On 24 February 2018, University College London computer scientist Sergey and his colleagues analyzed nearly a million samples of Ethereum smart contracts. About 34,000 copies were all had safety concerns, involving millions of dollars, 2,365 of which were prominent projects.

At present, more than 20 serious smart contract vulnerabilities have been found on Ethereum, seriously threatening the financial security of smart contracts.

On the one hand, on-chain smart contract is a pioneering technology that deserves further exploration and optimization, and its security should continue to improve; On the other hand, non-smart secure application development models can be explored before smart contract matures. The application development protocol of the SAFE network is the exploration of the more secure application development mode.

SAFE network uses the blockchain protocol "security capital" protocol to issue digital assets, which has higher security compared with Ethereum issuing digital assets with smart contracts. Smart contract is a typical program, the status changes very much, the security control of the virtual machine is not mature, the test is difficult to complete, the possibility of error is more. Since the currency, from the currency protocol vulnerabilities currency events has not happened, investigate its reason, because the status of the protocol change is very limited, easier to test and security control, net use protocol to issue digital assets, more secure, and smart contracts in the net only for the implementation of business logic.

.21.2 Convenience of issuing assets

Asset issuance is an important part of application development. Almost every application involves digital asset issuance, such as tokens, points, game equipment, documents and so on. Ethereum Smart contract, the asset issuance process is more complicated, so it needs to write smart contract according to ERC 20 standard. Although some open source code, it needs technical personnel research and development, and there is a certain threshold.

Whether digital assets can be issued in a simpler way, so that people who do not have the ability to develop blockchain applications and smart contracts can have a few mouse clicks and input some information. The SAFE network fully achieves this, allowing non-technical personnel to issue digital assets with one click on the mobile APP.

1.2 Privacy protection.3

Privacy protection on the blockchain is focused about money and past transactions. Given a Bitcoin address, anyone can see the balance of the address and the details of past transactions, which cannot meet users' privacy needs.

DNC (DarkNetSpace, project name dark Net Space, later renamed SAFE network), was released by the founder of SAFE Foundation in October 2014, and the second version was released in July 2017, and was renamed SAFE network 2. DNC uses the technology of ring signature and stealth address, which hides the sender and receiver, separates the correlation between input and output, and makes the blockchain cannot be analyzed and achieve the purpose of privacy protection.

CrytpoNote The series of currencies of technology, due to its unanalyzed blockchain, leads to the difficulty of the introduction of blockchain application and smart contract to increase dramatically, so the SAFE network v3 regards the characteristics of privacy protection as an option.

1.3 History of the SAFE network

As mentioned above, the token DNC of SAFE network Space (referred to as SAFE network) was released as early as October 2014, which is the earliest digital currency focusing on personal privacy protection in China.

In July 2017, the SAFE network team upgraded the SAFE network 1 to the SAFE network 2 (Anwang 2), and upgraded DNC to DNC 2. DNC 2 requires less memory and is more secure and efficient than DNC. Main features: currency deposit and financial management, private communication (including individuals and groups), direct wallet mining, remote transaction release and so on.

- Strong privacy protection: such as support for TOR network, ring signature, stealth address, transaction remote release, etc., to achieve the real privacy protection:
- Deposit interest: DNC 2 can be locked on the blockchain, can not be used until unlocking time, and can generate an annual interest rate of up to 5% to prevent underselling and get more DNC 2.
- Secret chat: secret chat refers to the encrypted chat, DNC 2 with the public key system, with the public key of the chat object encryption, the chat object must use their own private key decryption to get the

chat content, the security is extremely high. Secret chat includes single secret chat and group secret chat. Single secret chat refers to chat with an object address, while group secret chat refers to chat with multiple addresses, and other personnel can easily join in the chat.

- Block browsing: Built-in, block browser, you can view all blocks and transaction data.
- Built-in mining: simplifies the mining function, directly in the wallet without installing other mining software.
- Network monitoring: it includes network monitoring functions, such as transaction memory pool, node list, etc. Easy to view the network.

In January 2018, SAFE Foundation decided to split DASH, merge voting chain and SAFE network 2, upgrade to SAFE network 3, and change the name to SAFE, to create a more open project with a larger ecosystem.

On January 20,2018, SAFE successfully crossed from DASH's block height 807085, and SAFE Network v3 was officially launched. As of March 25, the project has progressed as follows:

- The SAFE network already has 1,900 main nodes;
- SAFE network SAFE is already in zb.com ,coinegg.com, dragonex.io , hb.top, kex.com, oex.com, chaoex.com , btctrade,im, coolc oin .com online trading;
- SAFE network SAFE has been online mining pool vvpool.com, currently has stable computing power;
- SAFE network SAFE has been online coin see wallet bitkan.com and bitpie.com ;

By 3 January 2019, the project has progressed as follows:

- In August 2018, the v1.2 version of the digital currency payment platform has been launched;
- In September 2018, the main network 2.0 supporting the security capital agreement and SAPP protocol was successfully upgraded, and PC wallet, Android APP, IOSAPP and block browser were launched;
- In September 2018, the new project safety test (digital currency reward + blockchain public test + BUG management) has been launched;

- In October 2018, the new project Anyou (digital currency game platform) has been launched;
- In October 2018, the SAFE proposal management system was launched;
- In November 2018, the new project Anbao (hardware wallet) has been launched;
- On January 3,2019, there were 3,000 main nodes;

As of 15 December 2021, the project progress is as follows:

- The SAFE network already has 8,107 main nodes;
- New project SafeWallet, support for other currencies, is under development;
- New project SafeSwap, the DEFI application supporting SAFE ecology, is under development;
- SAFE network 4 is in the planning, is under technical investigation and verification;

1.4 Security and network application

SAFE network is a blockchain application development platform, developers can develop a variety of applications based on the SAFE network, to reduce the threshold of "blockchain +". Application development protocol is to realize the blockchain application development, standards and requirements, such as application registration, permission setting, data writing, entry, data query and other interfaces. The following are the official SAFE network applications that will be developed based on the SAFE network application development protocol:

- Security Capital (Asset Management and issuance):
  To realize the functions of digital assets issuance, additional issuance, transfer, destruction, candy distribution, candy and other functions, other applications to issue tokens on SAFE network 3, and build to build a larger ecosystem.
- Safe payment (instant support, secure payment):
  Real-time payments and privacy payments. To more efficient real-time payments and privacy payments that protect users' transactions.
- Antou (safety vote):
  A decentralized, fair, open and fair blockchain voting system, using blockchain technology to solve the problem of openness and transparency in the voting process.

More official apps may be developed in the future, while also allowing third-party development teams to freely develop third-party apps on them.

.51 The SAFE assignment

The initial number of SAFE coins was around 40 million at the fork on January 20,2018, after three large reductions:

(1) About 3 million candies, originally scheduled for Monroe coins, ZCash and other currencies, have been destroyed on May 11,2018. Transaction view: http: / / chain.anwang.com/tx/1490e0008eda2c499070d30a6f257932312a40e5a0038043961f598051469744

The idea is to send 3 million SAFEs to a special address, the XagqqFetxiDb9wbartKDrXgnqLah6SqX2S. The special address does not have a corresponding private key, so no one can use the 3 million SAFE. This address is called a black hole address.

(2) Nearly 8 million SAFE were scheduled for the holders of the coin, but because more than 7.2 million SAFE were not received in September, SAFE Foundation decided to seal the part of SAFE around September 26, and issued a notice of storage one week before the storage, so that users who did not receive them as soon as possible. The total number of 800,000 SAFEs, 7.2 million fewer than before.

(3) When DNC 1 upgraded DNC 2 in July 2017, a part of DNC 2 was not redeemed, so a part of SAFE was left. When the voting chain ELT issued in November 2017 was exchanged for SAFE, some SAFE were also not exchanged, and the total number of SAFE not exchanged was

366,593.6716. After the lockup interest activity to December 31,2018, there were 199,12 3 SAFE remaining, which were destroyed on January 3,2019. The destruction transactions are as follows:

https://chain.anwang.com/tx/90be0d790cefa414b78b35349f7ec4bc0563f6bd3ce9eb893516857fd0b59423

(4) SAFE mining rules are 45% to the main node, 45% to the mining revenue, and 10% to the proposal revenue. After nearly three and a half years of operation, 2.08 million will be dug out in June 2021. In these three years, if the monthly 10% of the proposal revenue can be dug out, it should be 222,000 (208 / 9), but in fact, it is only four months, about 23,000.200,000 SAFE have disappeared forever, so the maximum supply of SAFE should be reduced by 200,000.

After the above four significant reductions, the SAFE is allocated as follows:

(1) Number of tokens: 29.4 million, the actual number of SAFE will be even less, for example, no super block was produced from May to September 2021;

(2) 2.72% to the original holder of the world coin, about 800,000 pieces. This part is the candy, self-received;

[illegible]

(4) 13.60% to the team, about 4 million; this part was locked in September 2018, mostly unlocked after 3-4, but the SAFE team re-locked

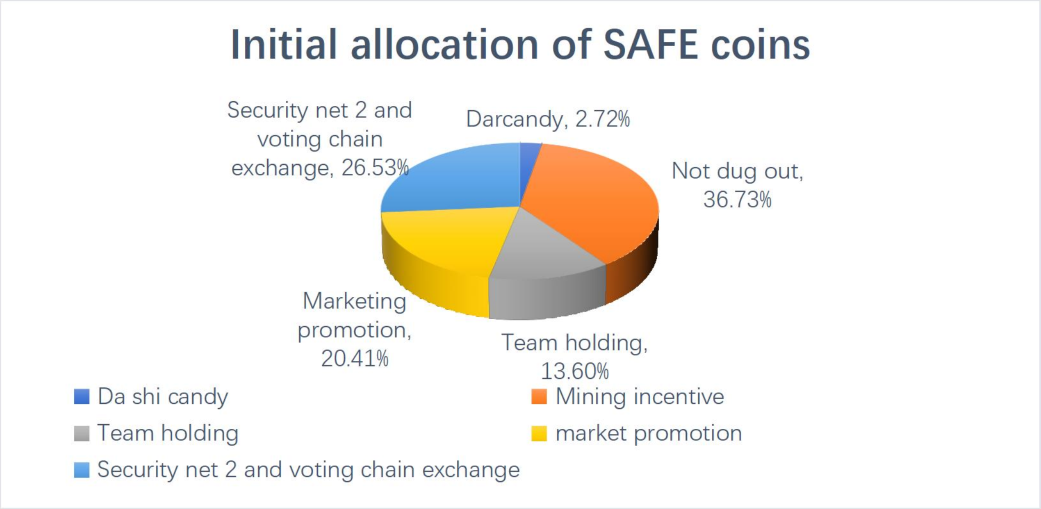
in July 2021, release rules: 500,000 released after 12 months, then 500,000 released every six months for 5 years.

SAFE official lock currency address:

XmVvAye4ph9s3M5AjrWDRFAzTKrkpwcHHR

(5) 20.41% is used for marketing, about 6 million pieces, this part has been used up;

(6) 26.53% for network 2 and voting chain ELT users into SAFE, about 7.8 million, this part was exchanged in January 2019; SAFE team in network 2 and ELT for nearly 2 million SAFE, after 3-4 years of team expenses, the remaining 500,000, locked together with the coins of part 4.



By December 2021, the status of the SAFE coins is as follows:

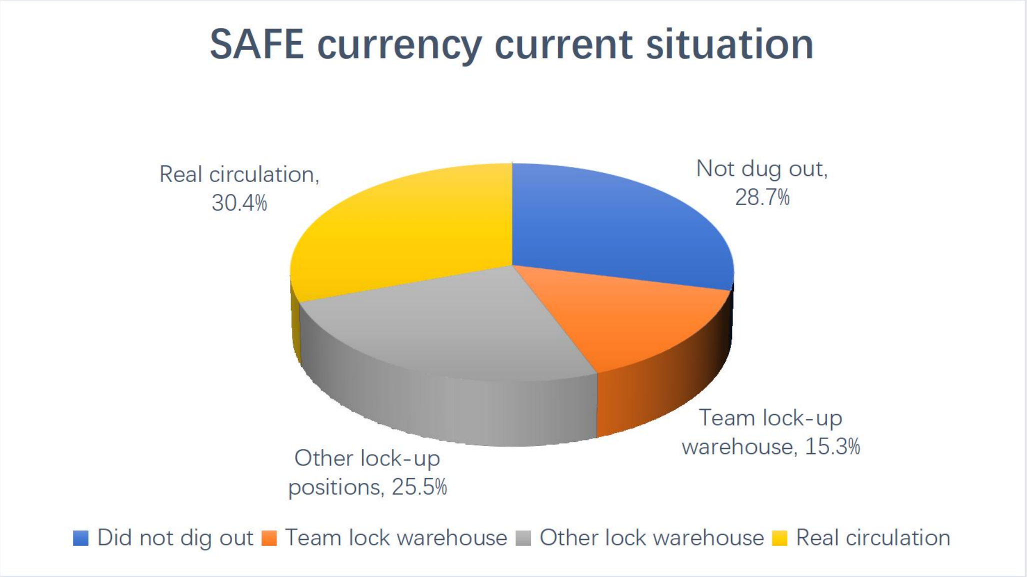
(1) SAFE coins totaled 29.4 million;

(2) Not dug out, 8.55 million pieces;

(3) Team lock 4.5 million; XmVvAye4ph9s3M5AjrWDRFAzTKrkpwcHHR

（4）Other locks, 7.5 million; available at https: / / chain.anwang. For com / rankings view, there have been 12 million lock positions, minus the team lock positions of 4.5 million;

（5）Real circulation, 8.85 million; 29.4 million minus the above three parts can get 8.85 million;



1.6 Mining gain

1.6.1 Master node and miner revenue

(1) With 1000 SAFE, revenue accounts for 45% of the total coin production of a block (currently 1.67 SAFE), and revenue decreases by 7.14% per 210240 mining. According to this rule, the main node revenue will also decrease; the same.

(2) For example, the total number of main nodes is 2000, and 576 blocks are generated in one day. One main node takes about 3.47 days to get a return, and the daily revenue is about 0.48 SAFE (calculated according to the current revenue of 1.67 SAFE);

1.6.2 Activity Gain

(1) Starting from the first block dug out after SAFE was successfully split on January 20,2018 Beijing time (block 807026, hereinafter counted as the first block), the subsequent block 103680 (nearly 6 months) has mining gain and main node gain, measured by SAFE (hereinafter referred to as gain);

(2) According to the first transaction of each block, that is, the receiving address and amount of the coinbase transaction, the SAFE official will send the corresponding gain to the corresponding receiving address, and the gain amount is as follows:

(3) SAFE officially sends the gain only to two coinbase receiving addresses. For the mine pool address, it is not officially known which mine pool or miner the address belongs to, so the gains of the

miners in the mine pool are distributed by the mine pool. The master node address that appears in coinbase transactions will receive a direct gain without being assigned by others;

1.6.3 Implementation of Gain activities

By July 28,2021, the main node and the mining gain have all been fully distributed. According to statistics, a total of 24 gains were issued, and a total of 142361.70199473 SAFE were issued.

2 SAFE network team brief introduction

The SAFE network team is composed of senior bitcoin and blockchain experts, technology research and development team and blockchain operation talents, and invited well-known technical experts and operation experts in the industry to serve as project consultants, aiming to create an influential project focusing on the landing of blockchain application.

The SAFE network team has deep business knowledge, solid technical knowledge and rich development practice experience in blockchain application:

- The founder began to study blockchain and Bitcoin in June 2013, wrote nearly 20 articles on blockchain technology, and in 2017 compiled the book "Blockchain Development Guide", which was published by China Machine Press;

- In October 2014, it launched the dark web space project focusing on blockchain privacy protection, which has been nearly three and a half years since then;
- The Alliance Chain (BLChain, Consortium Blockchain) was released in September 2016;
- Commercial bank collateral blockchain was released in September 2016;
- Digital integral blockchain was released in November 2016;
- In March 2017, the warehouse receipt pledge financing blockchain was released;
- In April 2017, the world's first blockchain middleware product —— blockchain middleware (Blockchain Middleware, BMWare) was released;
- In July 2017, dark Net space officially changed its name to SAFE network, and released SAFE network 2 wallet;
- In December 2017, the blockchain voting product —— was released (ElectionChain, ELT);
- On January 20,2018, the fork to the world, SAFE network 3 came out;
- In September 2018, the main network was successfully upgraded; the development agreement of Anzi and SAPP was launched;
- In October 2018, Anfu, Antest, Anbao, Anyou were launched;

It can be seen that the SAFE network team is a senior team that has been working in the blockchain industry for more than 6 years, has developed more than a dozen blockchain projects, and has rich experience in blockchain development and application. And the SAFE network will be the SAFE network team in the following 5 years of the most heavyweight blockchain products.

3 relationship with DASH

In this chapter, we want to explain the following questions: (1) why do we upgrade the network 2 (2) why do we merge the network 2 and the voting chain?(3) Why fork away without reopening the blockchain?(4) Why is the fork DASH instead of Bitcoin?(4) Why is SAFE no longer a forked coin after September 2018?

3.1 Why do I want to upgrade the SAFE network 2

Security space 2 inherits the privacy protection technology of security space 1, and has made more in-depth exploration in privacy protection.

With privacy protection comes the difficulty of developing applications on the SAFE network 2 blockchain. Because of the unanalytical nature of the SAFE network blockchain, it is much more difficult to introduce smart contracts and develop applications. This is in conflict with our idea of aiming to further implement blockchain applications, so we must shift from the underlying CryptoNote blockchain to the similar open blockchain of Bitcoin, using CryptoNote technology as an option, so that we can consider the application of privacy protection technology, the implementation of smart contracts and other blockchain applications.

3.2 Why to merge the SAFE network 2 and the voting chain

VotingChain (ElectionChain) is an ICO project launched by the SAFE network team in July 2017, with the token name ELC.

The voting chain aims to study and develop an application dedicated to voting and voting, voting donation, voting guessing, campaign speech and live broadcast, campaign games and other scenarios. In the voting chain, each voter votes in a real or virtual identity, which can verify whether the final result contains his own vote. The voting chain uses technical means to solve the disadvantages of paper ballot, electronic voting and online voting, making the election, decision-making and public opinion survey more open and transparent, avoiding the voting results being disturbed by external forces, and making the voting more credible.

On July 1, the network team successfully raised BTC, ETH and DNC worth 2700 BTC. On September 4, after the People's Bank of China stopped the ICO project, the team returned all the ICO funds at the ETH price at the ICO, and recovered nearly 99.99% of the ELC tokens. They also promised to give new ELT tokens to ELC users for free. In November 2017, the voting chain ELT network was released. ELT did not conduct any private equity and ICO, and all gave them away to the original ELC users for free.

One team operates two projects and tokens in different directions, which brings a lot of trouble to the SAFE network team. There are some problems in product planning, technology research and development, market operation and user relationship maintenance. After soliciting the opinions of many users, the team decided to merge the two projects.

The merger strategy is obvious, the SAFE network is the concept of the underlying technology application platform, and the voting chain is an application, voting can be published on the SAFE network, so it is a good idea to focus on the SAFE network, and voting becomes a specific application of the SAFE network, renamed Ancast.

3.3 Why fork away without reopening the blockchain?

Now we want to upgrade SAFE network 2 and integrate the voting chain to SAFE network 3. One technical route is to reopen the blockchain based on the code of existing excellent projects, and the other technical route is to be compatible with the data of current excellent projects to fork.

Why is the fork necessary? Mainly based on the perspective of project operation, (1) advantages: fork to be compatible with the data of the target chain, equivalent to send candy to the target chain, can obtain higher user visibility and participation, and help to improve market value; and reopen the users of the previous two projects, little impact on the market value (2) disadvantage: split candy is the target, block chain users free, may form a large selling pressure, while reopening the block chain without this problem. Under the balance of pros and cons, the SAFE network team still decided to split, not concerned about the rise and fall of the currency price in a short time, more concerned about higher visibility and long-term market value.

3.4 Why the fork DASH instead of Bitcoin?

There are two main reasons why DASH is the first choice of the SAFE network team:

(1) DASH and SAFE network have the same project theme: namely, privacy protection on the blockchain.

(2) DASH is based on bitcoin, and there are many technological innovations that attract the SAFE network team. For example, the two-layer network, namely the main node mechanism, is added, and the distributed community governance mechanism is established on this basis, which effectively solves the problem of decentralized monetary community governance. DASH has improved bitcoin payments,

providing instant payments, making DASH the possibility to challenge the Lightning network.

Here is a brief introduction of DASH's innovations:

3.4.1 Primary node (masternodes) network

In addition to the traditional proof of Work (PoW) rewards for DASH mining, users can also run and maintain special servers known as the master node. DASH can provide innovative functionality in this decentralized way.

The primary node provides the following services:

- InstantSend Allow near-instant transactions, and InstantSend transactions are confirmed within four seconds.
- PrivateSend Provide financial-level privacy protection by confusing the funding sources on the blockchain.
- The governance and budget mechanisms allow Dash stakeholders to direction the project and invest 10% of the mining to reward the project and ecosystem development.

The master node owner must have 1000 DASH that they prove by signing the message and broadcasting to the network. These coins can be transferred at any time, but the transfer will cause the master node to be removed from the master node queue and stop receiving rewards.

With 4700 master nodes, the master node network is very valuable; that is, 60% of DASH coins are mortgaged on the master node, which is one of the reasons for the increased value of DASH.

Master node users can also receive voting rights on the proposal. Each master node has a voting right, which can be exercised on budget proposals or important decisions affecting the DASH.

3.4.2 Privacy Payment (PrivateSend)

PrivateSend Provide users with real financial privacy by confusing funding sources. All the global coins in the user's wallet are made up of different "inputs", which we can see as separate, separate coins. PrivateSend Use innovative processes to mix user input with that of two others, without leaving the sender's token away from the sender's wallet. Senders always maintain control of their own funds.

3.4.3 Immediate Payments (InstantTX)

The DASH realizes the instant payment through the transaction locking mechanism. So-called trading locking mechanism, first through trading lock client request trading assets, through the election algorithm in the main node sort the top 10% of the selected 10 main node deal confirmation, select the main node consensus to the entire network broadcast, then all the client will follow the consensus of the main node, lock money, avoid the double flower attack. However, after the recipient receives the funds, it needs six confirmations before it can use the asset.

3.4.4 Other advantages

DASH also includes some features, including (1) the use of dark gravity wave as the difficulty adjustment algorithm; (2) the soft fork mechanism, the new version to the network but not in a hurry to activate, only 80% of the network participants reached the consensus, the new function is activated; (3) the distributed governance mechanism based on blockchain, that is, the main node allocates 10% of the mining revenue and the right to the development of DASH and budget.

3.5 Why is SAFE no longer a fork coin after September 2018?

There are two reasons. First, nearly 8 million SAFE were scheduled for the holders of the world currency. However, more than 7.2 million SAFE had not been received in September 2018, which did not reach the original intention of increasing the number of SAFE users and expanding the popularity of SAFE. Therefore, when the SAFE network was upgraded in September, this part of the unreceived SAFE was sealed, that is, after 10:00 on September 26, this part of SAFE could not be received or used again.

Second, SAFE has been upgraded to a digital asset issuance and application development platform in September 2018, which can issue assets and develop applications with one click.

Third, SAFE is introducing smart contract amcodes, a technology that DASH does not own.

Therefore, the development direction of privacy payment with DASH, SAFE is no longer a fork coin, but SAFE uses the source code of DASH and some technologies, thanks to the contribution of DASH development team.

4. The commercial value of the SAFE network

The SAFE network team will build a good application development platform, and focus on the three major application directions, combined with third-party applications, to build a huge SAFE network ecosystem.

4.1 Application development

The blockchain application landing cycle is long, the cost of talents is high, and the blockchain is difficult to use. These problems restrict the rapid landing of the blockchain application development.

SAFE network plans to simplify the application development process of blockchain and provide a series of application development services. The target users are small and medium-sized enterprises that do not understand the blockchain industry, have difficulties in the development of blockchain technology, but also want to carry out application development and digital assets issuance on the blockchain to gain the trust of users. All they need to determine is blockchain application scenarios, issue digital assets, and focus on the connection and application of digital assets and existing businesses.

SAFE network can provide a complete set of blockchain application consulting, technical support, assistance or outsourcing development, token real application landing services, which will bring profits to the team.

4.2 Security pay

When the number of SAFE network users is increasing, SAFE has become a general certificate in the SAFE network business circle. SAFE network users are willing to use SAFE to buy the goods and services provided by the SAFE network partners, and the SAFE network merchants are willing to accept the SAFE payment from customers, so the payment function of SAFE is reflected.

Security pay is the infrastructure of the SAFE network, and the security capital, security investment and other applications will use the security pay interface. The company is to open the channel for all the goods and services provided by the partners to pay using SAFE and other assets issued on the SAFE network; secondly, to open the channel for purchasing goods and services from other tokens issued based on the SAFE network.

The biggest characteristics of the security payment are instant payment and private payment. The instant payment speed is comparable to the existing third-party payment, which solves the problem of slow confirmation of bitcoin. The private payment is characterized by hiding the real address of the sender or receiver, which protects personal privacy. On the basis of DASH, Anpay has added several private payment modes, such as: transfer note, ring signature sending, stealth collection, amount, hiding, etc., so that users can have more choices for privacy protection.

4.3 Security

Valuable, transferable electronic data that we call digital assets. Security capital, that is, the digital asset management system based on SAFE network, can provide perfect digital asset issuance, additional issuance, transfer and destruction functions, and users can combine many application scenarios by themselves. There are original digital assets such as cryptocurrency, points, points cards, prepaid cards, game equipment, stocks and equity; Physical assets can also be digitized and issued and transferred in security assets, such as fiat currency, property and land, furniture, various documents, provided there is an acceptance agency.

The Commercial value of Anzi:

(1) Greatly simplify the issuance of digital assets. With a few clicks on the APP or PC wallet to consume a certain amount of SAFE, assets can be issued, safe and reliable, without the trouble and lot of risks of writing smart contracts;

(2) The digital assets issued on the security assets have a unified graphics, SAFE wallet support, block browser support, payment interface docking, exchange interface docking, and even the docking of other application scenarios, such as guessing, games, rewards, red envelopes, etc.;

(3) Cooperate with the exchange to establish the SAFE trading area, simplify the process of the digital assets on the exchange, and reduce the costs.

Many users brought by each digital asset issuer will become the SAFE network users and SAFE holders, which is conducive to the establishment of a huge SAFE network ecosystem.

The security capital agreement has been started at 10 am on September 26,2018, Beijing time.

4.4 Safety investment

Ann cast is the voting chain, voting chain translation to the security net 3 after the name. AnU aims to research and develop a blockchain application dedicated to voting, election and lottery, and support entertainment applications such as voting donation, voting guessing, campaign speeches and live broadcasting, and campaign games. In Ontario, each voter votes with real name or privacy in a real or virtual identity, which can verify whether the final result contains his or her own vote. It uses technical means to solve the disadvantages of paper voting, electronic voting and online voting, making elections, decision-making and public opinion polls more open and transparent, avoid the voting results being disturbed by external forces, and make the voting more credible.

4.4.1 Application Scenario

The application scenarios supported by Antou include election, decision-making, public opinion survey, voting, lottery, donation, etc. In the later stage, it may involve entertainment applications such as live broadcast and campaign games.

Voting and election: All elections and voting in the world can be conducted on Ann vote, such as the US governor and presidential election, China's NPC deputies vote, village committee election, voting of shareholders of listed companies, and various online voting;

Decision: Member referendum on a decision or matter, such as Brexit, force, commencement of infrastructure projects, etc.; this decision is relatively simple, yes, no or no.

Opinion survey: to solicit opinions from citizens on a certain topic, generally in the form of blockchain questionnaire survey, such as the presidential approval rating survey, views on a certain thing, and so on;

Voting: the subject should be popular and important voting results, such as presidential voting, brexit, etc. People can guess which candidate or decision will win;

Voting donations: People can donate to candidates at Ann, and blockchain can record donations from voters or non-voters to candidates, making payments more transparent.

Entertainment voting: introduce star selection, campaign speeches, live and tipping, campaign games and other recreational applications to make the voting chain more interesting rather than political items.

Lottery: Lottery distribution in China can only be conducted by licensed lottery agencies. In order to avoid conflicts with national laws, Antou will not issue lottery tickets by itself. The lottery scene will be conducted in cooperation with domestic and foreign lottery agencies.

4.4.2 Commercial value analysis

There are many application scenarios of Antou. If Antou is used for grassroots election, a vote of the neighborhood committee or village committee can bring tens of thousands of users to Antou, and a live broadcast can bring hundreds of thousands of potential users, while the entertainment voting for stars may bring millions of potential users.

It can be seen that Anantou's user base is huge, and user expansion is more based on the partners of SAFE network 3 to attract users. First is to attract participants to the voting sponsors to actively expand users for the SAFE network. The second is to vote in the users, give tokens to attract the other side to become SAFE network users. Third, through the introduction of more partners, so that users can participate in various activities on the investment, so as to become loyal users of the network.

4.4.3 Application cases

Antou is a blockchain voting system launched in November 2017, so there have been many application cases.

From January 1 to January 9,2018, A college in Huizhou, Guangdong province pioneered the application in the field of education, different from online voting methods such as wechat voting, Relying on the decentralized, fair, open and fair blockchain voting system —— An Investment, during the event, Of the college's total number of 15,000 students, A total of 8,672 students participated in the vote, "Give the best teacher in my mind", Participating in the selection are 44 teachers and 10 class directors from the School of Finance and Economics, And finally selected 3 class directors and 3 teachers as "the best teacher in my mind" candidates, Not only did they receive the corresponding year-end awards, It also received token incentives provided by AnU.

5 System architecture of SAFE network

SAFE network is positioned as a payment platform and application development platform that focuses on application security and privacy protection. Its system architecture diagram is as follows:

The underlying platform of SAFE network includes the underlying protocol and application interface layer. The underlying protocol includes the consensus algorithm, cryptography, P2P protocol, master node network, budget system, etc. used from DASH; in addition, it also includes the unique application development protocol, security capital protocol, candy protocol, smart contract and security payment extension function of SAFE network.

5.1 Consensus algorithm Safe POS

1. The mining algorithm of the following version of V 2.1 is inherited from DASH without modification.

(1) POW workload proof mining, X11 hash algorithm, using 11 specific Hash functions (blue, mw, groestl, jh, keccak, skein, lufa, cubehash, shavite, simd, echo);

(2) Mining can be CPU / GPU / ASIC, the current mining machine is mainly ASIC mining machine;

(3) Miners get 45% revenue, master node network gets 45%

revenue, 10% to the bill sponsor;

2. Version 2.5 of SAFE network will modify the consensus algorithm from POW to SafePOS, with the idea as follows:

Select bookkeepers from the main node of the whole network. The benefits are:

(1) Greatly shorten the production block time, and greatly improve the transaction performance. POW production time is 2.5 minutes, Safe POS production time is expected to be within 3-10 seconds, to prepare for the subsequent application;

(2) Greatly enhance security. At present, SAFE computing power is very low, and in the face of 51% attack risk of DASH computing power. Do not need to worry about 51% attack after converting into SafePOS. Compared with DPOS, reduce the risk of DDOS attack;

(3) Lower the mining threshold and reduce energy consumption. Users mortgage 1000 SAFE to establish the main node can mine, without expensive ASIC mining machine input;

(4) Bookkeeping is more decentralized. Random booklers from all main nodes is more in line with the spirit of decentralization.

The technical principle is as follows:

1) Select 9 bookkeepers from all the main nodes, and each main node is selected from the list of the main nodes of the whole network to enter the candidate list;

3) The candidate list is sorted according to the score from high to low. Score calculation rules: a HASH value is generated with the time of the main node mortgage address and the latest block of the current chain, and an integer is calculated for HASH;

4) Select 9 bookkeepers randomly from the arranged list. The random algorithm can ensure that 9 bookkeepers for each node is exactly the same. For the specific principle, please refer to: http://xorshift.di.unimi.it/；

5) Nine bookkeepers take turns generating blocks, 1,2,3,4,5,.....， 9；

6) After the completion of a round of blocks, 9 bookkeepers are randomly selected;

5.2 Cryptography algorithm

Cryptography algorithms will be inherited from DASH and Bitcoin, and will also inherit some cryptography algorithms of SAFE network 2, and will also introduce some new encryption algorithms, mainly involving:

- Merkle-Tree, the SAFE network uses Merkle-Tree to generate the root of all the transaction ID in the block for data integrity verification;
- Elliptic curve encryption (ECC) algorithm, the SAFE network using secp256k1 curve ECC algorithm as, the signature algorithm to sign the transaction;

- Hash algorithm: using blue, mw, groestl, jh, keccak, keccak, luciin, lufa, cubehash, shavite, simd, echo and other hash algorithms for mining;
- Ring signature payment: security payment, planned to use the ring signature algorithm for payment, in order to hide the sender;
- Stealth collection: Anpay plans to use stealth address technology for stealth collection, in order to hide the receiver;
- Homomorphic technology: Anfu plans to use homomorphic encryption technology to encrypt and hide the amount;

5.3 Main, node network

The master node network is the most important infrastructure of DASH, and it is also inherited by the SAFE network. The establishment of a master node requires the mortgage of 1,000 SAFE, obtaining 45% of the mining revenue of the whole network. DASH has been online for 4 years, the number of master nodes is 4,700, and the security cable for two months. By March 25, there were 1,900 master nodes, and 3,000 master nodes on January 4,2019.

The main node undertakes the functions of instant payment, privacy payment, voting and other projects of the SAFE network, and will also undertake more functions. We hope that the more master nodes in the SAFE network, the more extensive the distribution, and the more stable.

Therefore, the master node establishment is improved from the following aspects:

(1) One-key deployment of master node tool, set the VPS server IP address and password in the tool, and then make one-key deployment, making the deployment more convenient and fast. Currently support Aliyun, subsequent will support more VPS, provider, the tool can be downloaded on the official website;

(2) Upgrade the master node tool, upgrade the master node requires convenient and fast, to meet the fast application research and development and upgrade, the script can be downloaded on the official website;

(3) Change the master node mechanism, 1000 SAFE locked for more than 6 months to establish the master node; this function has been implemented in V2.0 version;

(4) In the future, the master node hardware box and configuration tools will be provided according to the situation. The hardware box will be connected to the Internet line. After the configuration is completed with the tools, it can become the main node without having to buy VPS server to save costs;

In the future, the SAFE network is expected to reach more than 10,000 main nodes, which may surpass Bitcoin to become the world's largest master node network.

5.4 Budget system

The budget system is a very distinctive community governance structure inherited from the DASH. Ten percent of the mining revenue in each block (7,000 SAFEs per month) is not generated, but is generated through "super blocks" by the end of the month.

The month, any per person can apply to the net budget, decided by the main node user vote, any proposal as long as at least 10% of the network consent, to the end of the month will create a series of "super block", to the approved proposal pay SAFE, for those who help the net community development promotion projects or research and development projects.

The proposal system corresponding to the function is already available on the official website.

5.5 Application development protocol

SAFE network provides a set of standard protocols based on the

SAFE network development blockchain application, which is the first step to become an application development platform. The design purpose of the application development protocol is to make the enterprises and institutions that want to develop the blockchain application to implement the "blockchain +" strategy. The extension function of security payment, security capital and security investment are the application examples in the SAFE network application development protocol. Based on the application developed by the SAFE network, we call it Safeapp, or Sapp for short.

Application development agreement includes application registration, application permission setting, application data writing and update, application data retrieval and query interfaces. Therefore, the process of S app application development is: application registration-> permission setting-> Application development-> Application deployment-> application operation.

The network application must first be registered on the S app application, can be accepted and identified by the whole network. The registration process does not need anyone to review. As long as a certain amount of SAFE is burned and the application name is not conflicting, the registration transaction can be accepted by the whole network and the registration is passed.

Application permission setting, define which users can access which application commands, these application commands are customized by the developer, but the SAFE network can help the developer to define the user's access control rights to the application commands. When a user wants to write an application command to the blockchain and broadcast the transaction to the whole network, all nodes and clients will check their access permission according to the access control permission table, and the operation transaction without the permission will be rejected.

Application deployment method, except Anfu and Anzi, other applications are connected with the SAFE network by RPC interface. Developers can only deploy S app at the nodes they need, without having to deploy in the whole network.

Data retrieval is a convenient method for local application of data query. All the data of Sapp will be stored in the network nodes. The nodes not deployed can identify which ID Sapp data, but the specific Sapp data cannot be correctly analyzed.

The SAFE network application development protocol makes the development of Sapp more standardized and convenient, and without the need to develop any smart contract, it is easy to combine with the blockchain middleware, provide the SAFE network middleware API and SDK, and further simplify the development of applications.

This feature has already been implemented in version V2.0.

5.6 Security capital agreement

Valuable, transferable data are called assets, such as points, digital currency, documents, credit investigation, insurance, loans, digital RMB, and so on. Security capital agreement, namely SAFE network asset management agreement, provides digital asset issuance, additional issuance, transfer, destruction, candy, candy, inquiry, etc. Developers can combine many application scenarios, such as digital currency issuance and transfer; bill of lading issuance, transfer and destruction; and even issue points and digital RMB points simultaneously, and exchange them at a certain exchange rate.

SAFE network only provides a platform for asset issuance, and does not endorse and review the issued assets. Asset issuers can issue digital assets as long as they burn 500 SAFE (decreasing by time, at least 50 SAFE), the asset name is not the same name, and a few clicks. SAFE network wallet, blockchain browser, exchange interface, and payment interface will be automatically supported, greatly reducing the cost and time of digital assets issued for developers.

The assets of the SAFE network are uniformly received and sent by the SAFE network address, which requires the transaction fee priced by SAFE. The SAFE network team will also open the SAFE trading area in several exchanges, and the tokens on the SAFE network will form trading pairs with SAFE to facilitate the establishment of the SAFE network ecology.

This feature has already been implemented in version V2.0.

5.7 Candy Agreement

The candy agreement is a very distinctive agreement in the security capital agreement. The main idea is: when issuing tokens through the security capital agreement, the token issuer needs to distribute 0.1%~10% of the newly issued tokens to the holders of SAFE, and the specific proportion is specified by the token issuer.

Main technical idea: When issuing the token, send 0.1% to 10% to 10% new token to a candy address at the same time, and each token can send up to 5 times. The SAFE holders manually click the candy in the wallet, issue a transaction to receive candy, and then get the part of the candy in the address. The candy will expire within 1-3 months (as defined by the issuer) and will not be collected again; if the SAFE holder does not receive it, the candy will sink forever and no one else will receive it.

Collection rule (1) The number of candy is calculated from the block at the time of the asset issue as the snapshot. (2) There must be a SAFE number greater than or equal to 1 in the SAFE address, Otherwise, you can not get (3) according to the proportion of the candy, Calculation method: the number of your candy = the number of candy issued in the whole network * (number of SAFE in this wallet / number of SAFE produced in the whole network), If the number of sweets available is less than 0, Also can not get (4) each, the kind of candy is only allowed to get a one-time finish, Do not claim it multiple times. (5) If the candy has expired, Cannot collect it..01

This feature has already been implemented in version V2.0.

5.8 amcode / smart contract

Smart contract faces greater security risk, and Ann net not smart contract as the first application, but with various protocols to safely meet the demand of application development, some more complex applications may use smart contracts, thus Ann net will also be introduced in the late code, namely Ann online intelligent contract system.

The technical route of Ancode is to transplant EOS account system, compatible with EOS, ETH and F ABRIC smart contract, to form a unique smart contract virtual machine SVM, as well as a unique super compatible SAFE network smart contract platform, so as to make it easier to build a SAFE network ecology from EOS and ETH.

5.9 Safety payment extension

At present, the underlying DASH has provided the functions of real-time payment and privacy sending, and it will be further expanded, mainly including the following functions:

.15.9 Add the transfer remarks

Each transfer transaction can be written in a note for subsequent review. This note will be written on the blockchain, which can be plain text or encrypted text, which is also convenient for users to make personal records on the blockchain. This feature has already been implemented in version V2.0.

5.9.2 Ring signature is sent

Ring signature transmission is one of the privacy payment functions in network 2. Its characteristics: (1) the signatory selects the user's public key to participate in the signature; and does not have to notify the selected user; (2) the private key of any member and cannot forge the legal signature; (3) unconditional privacy: even if the attacker obtains all the possible private key, the probability of the signer shall not exceed 1 / n, where n is the number of possible signatories. Using the ring signature technology, hidden the sender, equivalent to achieving a mixed currency.

SAFE network 3 will inherit the technology and realize the ring signature transmission.

5.9.3 Stealth collection

The stealth address is also the first privacy technology used by CryptoNote, derived from the elliptic-curve key exchange protocol (ECDH). The receiver discloses a special address called the stealth address, and the sender sends a SAFE to the address and comes with a disposable public key. The enemy cannot find any transaction from the public address, but the receiver calculates the correct receiving address and private key based on the attached public key, thus receiving the currency.

Ring signature sending and stealth collection can form a more private transaction.

5.9.3 Amount is hidden

Homomorphism encryption is a cryptographic technique based on the computational complexity theory of mathematical problems. Processing the homomorphism encrypted data gives an output, which is decrypted with the same result as the output obtained by processing the unencrypted raw data with the same method.

This feature applies to amount hiding, where A sends amount X to B, no one else can see the specific amount, but (1) can verify that the amount of X does not exceed the amount that A has. (2) B can decrypt the amount and can be spent later.

5.10 P2P protocol

The P2P protocol of the SAFE network extends the P2P protocol framework of bitcoin, and on this basis, some extensions are made to meet the subsequent needs of instant messaging and decentralized storage, and the technical scheme will be announced separately.

6 Technical scheme of SAFE network

The technical scheme of SAFE network includes bifurcation scheme, technical scheme of application development system, technical scheme of each application, etc. Some of these technical solutions have been successfully implemented, some are under development and some are still in the planning stage and may change, citing the latest white paper.

The implementation implementation implementation implementation technology implementation plan will be announced separately.

6.1 Fork technical scheme

.1.61 Fork principle

At the height of block 807085 (i. e., around 10:30 a. m. Beijing time on January 20,2018), the block 807085 is generated by the program, and the block is called the SAFE creation block. In this block, there is only one coinbase transaction, exporting 21 million SAFEs to the official wallet address, with no miner rewards. The difficulty of the block is reset to DASH creation block difficulty with Nce of 0. Miners then started digging from the block height 807086, and the coinbase output was restored to the original DASH reward rules.

.1.62 Related parameters

	primary network	Test network
P2P port	5555	15555
RPC port	5554	15554
ZMQ port	5553	15553
The P2P protocol identification	62696ecc	52595ebb

.1.63 Profile

- Data storage path

  Linux：/root/.safe

  Windows: C: \ Users \ User name \ AppData \ Roaming \ Safe

- Profile name

  Linux:/root/.safe/safe.conf

  Windows: C: \ Users \ User name \ AppData \ Roaming \ Safe \ safe.conf

.1.64 Trading structure

Starting from block height 807085, two fields are added to the output of the transaction structure:

(1) Starting from the block height of 807085, the transaction version number (nVersion) is 101, and the previous DASH transaction version number is 1;

(2) nUnlockHeight Field, reserved to add SAFE lock function, the default value is 0;

(3) vReserve Field, said, for the application data area, the maximum length of the application data area is 3000 bytes, the minimum is 4 bytes small case "safe", in order to facilitate the development of applications, such as: security, investment, security, intelligence, contract, etc.;

.1.65 Block difficulty and reward

(1) Starting from the height of block 807085, the difficulty of this

block is the difficulty of DASH creation block, the difficulty rules of the following rules are: the first 100 blocks adopt BTC calculation rules, the last 100 blocks adopt KGW calculation rules, and 200 blocks switch to DGW calculation rules; so the output of the first 200 blocks will be relatively fast, after the subsequent use of DGW difficulty adjustment algorithm, it will be quickly maintained at about 2 minutes;.5

(2) Because of the reduced difficulty, in order to ensure that the mining output of SAFE is consistent with that of DASH, the block yield algorithm has changed from the block height of 807086. DASH, block yield: 2222222 / ((Difficulty + 2600) / 9) ^ 2), minimum of 5 DASH and maximum of 25 DASH. SAFE is changed to: the maximum and minimum is five SAFE, to ensure that the block production is basically the same as the number of coins officially announced by SAFE. However, it also leads to some different subsequent behavior, DASH in the difficulty, sudden drop, may increase the block production, but SAFE does not;

.1.66 Mine pool

The ore pool needs to be modified as follows:

(1) Starting from block height 807085, transaction version number 101; add vReserve and nUnlockHeight fields in coinbase output structure when generating block; vReserver size is 4 bytes, content is lower case "safe"; nUnlockHeight value is 0;

(2) If you use the DASH directory for block data, delete the DASH files;

6.2 Application development protocol

We expanded the output structure of the transaction (see 6.1.4), where the application data area is used to store application data, such as data from A, and data written by other third-party applications.

The application development interface includes several common interfaces, such as application registration, application permission setting, which defines the problem of who has the permission to write data and what data to write.

At present, anyone can write any data to the public chain such as Bitcoin and Ethereum at a low cost, resulting in the flood of junk data on the blockchain. SAFE network does not want the application development interface to be abused, let alone the junk data.

All of the following application development interfaces consume SAFE, so when calling through an RPC, make sure that the SAFE node that provides the RPC service has the wallet function enabled and has a sufficient SAFE amount.

In the application data area, the application head structure is as follows:

Application data area	explain
safe	SAFE network application logo, lowercase
version number	Application header version number
apply ID	The unique application ID of the entire network is generated according to the registered application information
utility command	Application commands in the application data, as defined by the user

Among them, the application command should be the content of the application data area, but the SAFE network will advance it to the application head structure. Its purpose is to make the bottom layer of the

SAFE network identify the application command, control the application authority, and ensure the security of the application interface.

.16.2 Application registration

Application registration is the premise of application development. Only the registered application can be identified by the SAFE network. The SAFE network node and wallet can classify the application data to the correct application ID to facilitate subsequent retrieval and query; the unregistered application writing data to the application data area will be rejected by the whole network.

Application registration fee: registered applications need to burn 500 FE, the amount every 17280 blocks (about 1 month time) by 5%, until the lowest 50, the purpose is to make the net application developers more carefully consider whether to develop the net application, ensure the net application data are valuable, avoid junk data aggravating Ann net storage burden. However, on the network, there is no application registration fee to facilitate users to test applications.

The application registration to the SAFE network broadcast an application registration transaction, declare the application name, developer, website, application LOGO URL, application cover map URL, web address, brief introduction, etc., the application name should be unique to the whole network. With sufficient app registration fees paid to a specific black hole address to burn the SAFE, no one can recover the burned SAFE.

Application registration does not require any institutional review, only burn enough SAFE, and ensure that the application name is unique, you can obtain the application ID, transaction ID, and administrator address. The application registration transaction is packaged into a block and accepted by the whole network, and the application data can be written into the transaction.

The application ID is used in subsequent application data writing; the transaction ID is used to check the transaction details; the administrator address is an address in the SAFE wallet; the default is the address that pays the SAFE. If there are multiple such addresses, the first address is automatically selected.

.26.2 Apply the command design

To register a good application, we must first carry out the application command design, which is equivalent to the system analysis and demand extraction of the application scenarios of the SAFE network application. In technical principle, an application command is like a function of a smart contract. The function of a smart contract can be called by anyone, so the smart contract needs to do permission control at the beginning of each function, not allowing irrelevant users to call.

The application development system of the network stipulates that the application authority can be refined to the application commands, that is, the bottom of the network can control which people can call which application commands, while others can not. The permission to read all the application data is a natural permission for all addresses, no, and something else.

For example, please apply the command design process. There is an online movie ticket ordering system, the merchant publishes the movie ticket information, the buyer places orders and pays, the merchant sends the movie ticket ID, the buyer receives the movie ticket ID, the buyer goes to the cinema to show the ID to see the movie. The application command design involved for this application is as follows:

Founder-member utility command	holder	seller	developer
Registered business	√		
Business audit results			√
Publish movie ticket information		√	
Payment to place an order	√		
Send out the movie ticket ID		√	

In the table above, only in the tick box is the correct application command. For example, everyone can register the merchant, the developer can review the merchant to register and send the audit results, and the merchant can release the movie ticket information, etc. Only by explicitly drawing the above application design table, can the next step proceed.

.36.2 Application permission setting

The application permission system of SAFE network refers to the write and update permission of some public keys or addresses to the application data, and also involves the more detailed permission to write and update the specific application commands in some application data. After the above application command design, it is easy to rule the application permission.

The application permission setting interface must be invoked by the administrator address, which is also the only default address with permission to write the application data without ignoring the application permission rules. But the administrator of one application cannot define the permissions for another application.

Through this interface, the administrator can increase, delete, and update some public keys or addresses, if 0 means all public keys or addresses, if 0 means all application commands. Here are some examples of this example:

The above online movie ticket order system, assuming that its application ID is

cf4362534be51d429585ccf8cab7d2a07e190588c69bde9f56e4dfec09a0a666

There are 5 application commands: 1. Registered merchant 2, merchant, audit results 3, release movie ticket information 4, pay for order 5, send, send movie ticket ID; according to the application command design table above, the permission table of application command is as follows:

Initiate the address Command number	All addresses	Merchant address	Developers' address
Registered merchant 1	√		
Merchant audit result 2			√
Publish movie ticket information No.3		√	
Payment is made under the order 4	√		
Send a movie ticket to the ID 5		√	

Three authority rules:

(1) Public key 0 + 1,4, that is, all addresses can be registered for

merchants and paid to place an order;

(2) The merchant address + 3,5, that is, the merchant address can release the movie ticket information and send the movie ticket ID;

(3) The developer address + 2, that is, the address of the developer can announce the audit results of the merchant, and need to set the merchant + 3,5 authority according to the address of the merchant;

The above three authority rules can be set at one time or in different times. Some permissions can also be deleted later, such as two new rules: merchant address-3,5; that is, cancel the merchant address to release movie ticket information and send movie ticket ID permission, become the ordinary user address.

After setting the application permission through the administrator address, a permission set transaction will be sent to the whole network. After the transaction is confirmed, all nodes and clients will limit the writing permission of the public key or address to the application command, and reject the transaction of unauthorized application commands.

This decentralized application permission setting system is an original technology in the SAFE network application development system.

.46.2 Apply data writing

After registering the application, you can write the application data to the SAFE network transaction. If there is no additional application permission setting, only the administrator address has the write permission by default.

Application commands are already included in the application development interface, and do not appear in the following data structure, the application data is designed as follows:

order number	Apply data items	explain
1	version number	For version upgrades
2	Custom data corresponding to the application command	self-defining data

If there is an encryption requirement, add two more items between the above two data items:

2	encryption algorithm	None, AES, or ECC
3	A key encrypted with the receiver's public key	If it is an AES encryption

Some application data needs to be confirmed as soon as possible, and you can optional call the instant payment function in the SAFE network, which can be confirmed in 3-4 seconds.

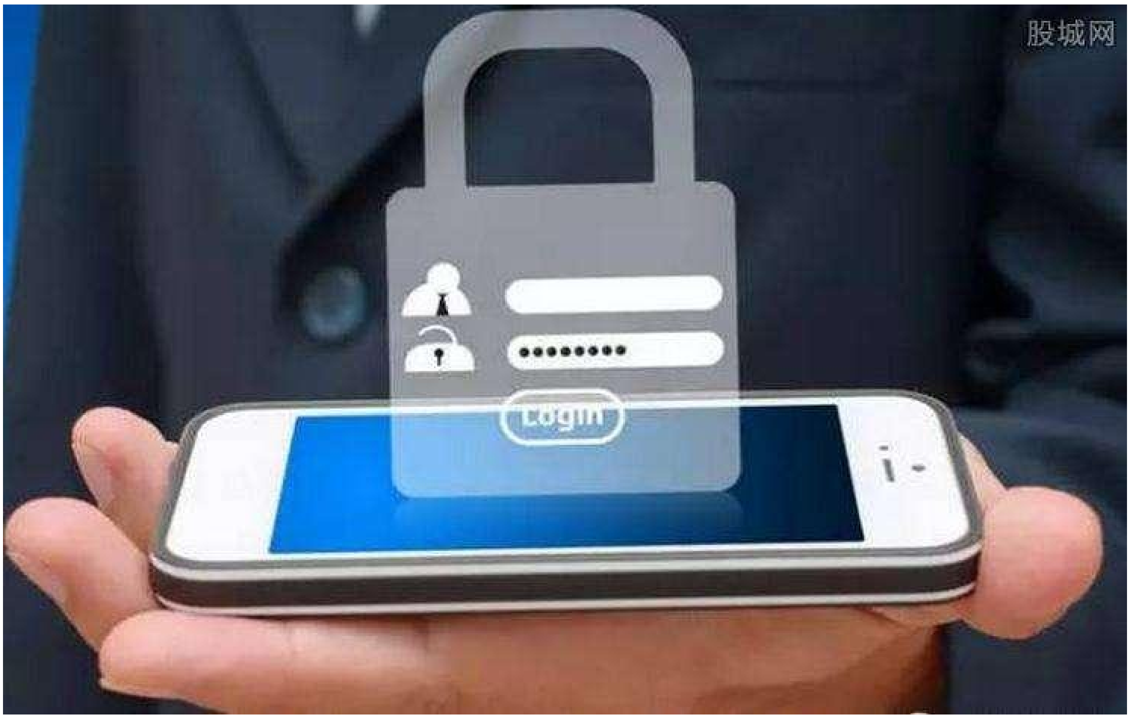
The current limit of the entire application data area is 3000 bytes, excluding part of the data possession of the application header and application data items, the amount of data that can be written is very limited.

6.2.5 Extra transaction fees

When there are more and more applications of SAFE network, the transaction of an application is too frequent, and there is a lot of junk data, which is bound to increase the burden of SAFE network. Therefore, SAFE network limits the number of transactions and worthless application data by increasing the additional transaction fee of application data. The rules are as follows:

- The application data area has only 4 bytes (SAFE) data, with no additional transaction fee;
- Application data area adds 0.0001 SAFE for every 300 more bytes, less than 300 bytes by 300 bytes;
- The application data area is up to 3,000 bytes, so the additional transaction fee is up to 0.001 SAFE;
- The additional transaction fee is reflected, like the normal transaction fee, and is obtained by the miners mining;

6.3 Security pay



Security payment refers to the transfer function based on the SAFE network platform, including instant support, mixed currency, added transfer remarks, ring signature payment, stealth collection, amount hiding and other technologies and payment methods.

6.3.1 Instant payment

The instant payment in the SAFE network 3 can be confirmed by the whole network in only about 3 seconds, without waiting for 6 blocks for confirmation, so as to improve the payment speed. The specific principle is as follows:

(1) After an instant payment transaction is sent to the network, all the clients of the SAFE network 3 are reached;

(2) The main node network randomly selected 10 main nodes,

by their vote to confirm that the transaction is valid, if 10 transactions are confirmed to be valid, the transaction is locked by the whole network;

(3) During the subsequent wait to produce the next block, all transactions that conflict with the locked transaction will be rejected;

(4) The mine pool packages the lock transaction into the block and broadcasts it to the whole network;

6.3.2 Mixed currency

Mixed currency is the prerequisite of private payment. Before private payment, the coins in your wallet must be mixed with others. This process is run in the background without any intervention.details are as follows:

(1) First, decompose the coins in the wallet into standard denominations, which are 0.01SAFE,0.1SAFE, 1 SAFE and 10 SAFE;

(2) Then, when you want to mix a certain denomination, the wallet sends the request to the main node on the network, the information will not be traced to you, because some unidentifiable information will be sent to the master node;

(3) When two other people send similar messages indicating that they wish to mix the same denomination, a mixed-currency session begins. The master node miinputs and instructs all three users' wallets to pay the same denomination to their own different

addresses.

(4) In order to fully mix funds, the wallet must repeat the process many times, each round of mixed money makes it more difficult to find out the source of funds;

(5) The mixed-currency process is conducted in the background without requiring any human intervention. When you want to make a transfer, your money has been confused and there is no extra wait;

.3.63 Add the transfer remarks

This function and the following security payment extension function, need to first in the security, network registration security payment application, application commands including adding transfer notes, ring signature sending, stealth collection, amount hiding, ring signature sending + stealth collection, etc.

Transfer notes can be encrypted but not encrypted. The encryption algorithm supports AES and ECC. The data structure is as follows:

1	version number	For version upgrades
2	encryption algorithm	None, AES, or ECC
3	A key encrypted with the receiver's public key	If it is an AES encryption
4	Transfer notes	Encrypted or unencrypted data

.3. The 64-ring signature is sent

The ring signature mainly consists of the following algorithms, assuming a user.n

- ❑ Key generation KeyGen: input security parameters to generate the public key and the corresponding private key for each user;k u_i P_i d_i
- ❑ m n $L=(P_1,P_2,...P_n)$ d_s m R R Signature Sign: enter a message, a user public key and a member's private key, to generate a signature, one of which a parameter is circular according to certain rules;
- ❑ Verify Verify: input and output.(m,R)

Ring signature is widely used because of its unconditional anonymity, spontaneity and group characteristics. According to different application fields, ring signature also developed other special attributes such as correlation, threshold features, deniability, revocable anonymity and so on.

The additional information of the ring signature will be written to the application data area in the form of the network application data. All nodes receive the transaction and can verify whether it is the transaction sent by the user, and the receiver can receive the amount without additional processing.

Ring signature transmission separates the association between the receiver and the sender, which may make blockchain applications subject to some restrictions, so further research is needed on the impact of blockchain applications.

.3.65 Stealth collection

Inalth address is an important privacy protection technology, which can separate the actual transaction from the public address, unable cannot find any corresponding transaction from the public address, but the payee can receive the currency from this address. There are double key and single key two cases:

(1) The stealth address of the double-secret key

The double key stealth address contains two public keys, one is called the browsing public key, the other is called the consumption public key, and there are two private keys, one is called the browsing private key, the other is called the consumption private key. The private key is used to view transactions and calculate balance, and the private key is used for transaction signature, namely consumer currency. The address of Annet 2 is the double-key address.

The usage scenarios are provided as follows:

❑ $SA=(Q,R)$ User A publishes an invisible address, which includes two elliptic curve public keys Q and R,, where the browsing public key and the consumption public key respectively, are the corresponding browsing private key and the consumption private key, and G is the base point of the elliptic curve.$Q = dG$ $R = fG$ Q, R d, f Q, R

- ❑ User B pays coins to A to generate A one-time public key pair, which is the public key of the destination address and the consumption public key of A. Publish the public key P in the transaction.(P, e) $T = R + sG$ T R $s = SHA256(eQ)$
- ❑ User A scans each transaction, discovering P, computing the possible destination address public key, where because.$T' = R + sG$ $s = SHA256(dP)$ $SHA256(dP) == SHA256(eQ)$
  - ❖ If user A does not have the correct browse private key, the error and are calculated d s T' $T \neq T'$, No correct destination address can be calculated.
  - ❖ If user A has the correct browsing key d, there is no private key, and A balance can be calculated.f $T' = R + sG$ $T = T'$
  - ❖ f $T' = (f + s)G$ $T = T'$ If user A has the browsing private key d and the consumer private key, then calculate, and. Can also consume coins, the private key.T $l = (f + s)$

(2) The usage scenarios of the single key are as follows:

- ❑ User A announces the stealth address,$Q = dG$ d Is the private key, and G is the base point of the elliptic curve.
- ❑ User B pays coins to A to generate A one-time public key pair,

which is the public key of the destination address. Publish the public key P in the transaction. (P,e) $T = sG$ T $s = SHA256(eQ)$

- ❑ User A scans each transaction, discovering P, computing the possible destination address public key, where because. $T' = sG$ $s = SHA256(dP)$ $SHA256(dP) == SHA256(eQ)$
  - ❖ If user A does not have the correct private key, calculate the error and, thus d s T' $T \neq T'$, No correct destination address can be calculated.
  - ❖ If user A has the correct private key d, calculate, and, calculate the A balance. $T' = sG$ $T = T'$

Similarly, stealth addresses split the association between receivers and sender, potentially influencing smart contracts and blockchain applications, thus limiting their applications to a certain range.

.3.66 The amount is hidden

Bitcoin side chain technology has a technology called a private transaction that only allows the participant (or the person they specify) to know the amount of the transaction. The principle is by using the Pederson commitment technology to hide the amount.

The commitment scenario allows you to save a piece of data as private, but promise it so that you can't change that data later. A simple commitment scenario is constructed with a hash function as follows:

Commitment = SHA256 (blind factor || data)

If you just tell someone what you promised, they can't determine what data you promised (give certain assumptions about the properties of the hash table). But you later expose the blind factor and the data that someone else can run the hash function to verify that it matches your previous promise. The blind factor must exist, or someone else can try to guess the data. If your data is relatively small and simple, the guess is more likely to succeed.

Pederson commitment is similar to the promise in the above scenario, but with a new feature: the promises can be added up, and the sum of multiple promises is equal to the sum of the data (the set of blinded factors is the sum of blind factors):

C(BF1, data1) + C(BF2, data2) == C(BF1 + BF2, data1 + data2)

C(BF1, data1) - C(BF1, data1) == 0

In other words, add law and exchange apply to commitment.

Using this tool, we replace the 8-byte integer amount in the Bitcoin transaction with 32 bytes. Pederson promises that if the sponsors of a transaction carefully choose their blindness factor to add it correctly, then the network can verify the transaction by adding the promise to zero.

(In1 + In2 + In3 + plaintext_input_amount*H...) -

(Out1 + Out2 + Out3 + ...fees*H) == 0

The above formula requires transaction costs, and in actual transactions, this is no problem. The principle of hidden amount is basically shown above, but in practical application also need to consider many safety, add some safety inspection measures.

6.4 Security

Security capital is a typical application developed based on the application development protocol of the SAFE network and integrated at the bottom of the SAFE network. It also needs to register the SAFE network application first, set the authority, and can develop various tokens or digital assets based on it. The technical solutions of Ancapital include issuance, additional issuance, transfer, destruction, candy, candy and receiving, etc.

.4.16 Asset issuance

Digital assets can be issued, and issuing tokens must consume 500 SAFE, down 5% per month (17,280 blocks) until no less than 50 SAFE, aiming to prevent spam of tokens on the site. The digital assets of publishing games and equipment can first issue a class of assets, and then issue additional classes of assets, then additional issuance does not need to consume SAFE;

Digital asset information includes: asset name (i. e., abbreviation, must be unique), asset profile, total assets, total amount of initial issuance, minimum unit, whether it can be divided, whether it can be additional issued, whether it can be destroyed;

At launch, it can also set whether to give candy to SAFE holders, and specify a candy ratio and expiration date, called the candy agreement.

The offering transactions are as follows:

- Output one:

Output amount: the SAFE to be consumed

Output script: normal transfer transaction script, the receiving address is the black hole address

vReserve Field: safe

- Output 2:

Output amount: the actual amount of assets issued

Output script: normal transfer transaction script, the receiving address is an address in the input (the address consuming SAFE);

vReserve Field: Application header + application data (asset issue)

Asset issuance field data	explain
version number	2 Bytes
Asset referred to as	Up to 20 bytes, 1 Chinese character may account for 3 bytes
Asset name	Up to 20 bytes, 1 Chinese character may account for 3 bytes
Asset description	Up to 300 bytes, 1 Chinese character may account for 3 bytes
Asset unit	Up to 10 bytes, 1 Chinese character may

	account for 3 bytes
Total assets	If it is 0, the total amount of representatives is not limited, can be issued
Total initial issuance	The number of first issues
The actual total amount of the initial issuance	
The decimal point	Minimum 4 digits, maximum 10 digits, for example: 100000000, representing the negative 8 power of 10;
Whether it can be destroyed	Some assets can be destroyed, some cannot, set up by the user
Whether to distribute candy	Whether to distribute candy to SAFE holders
Distribution of candy proportions	Send out 0.1% -10% of the total to the SAFE owners
Candy expiration date	In terms of the number of blocks, 1-3, between months, if the user sets 3 months, then 3, after the months, if you have not received the candy, it will be invalid.
remarks	Up to 500 bytes, 1 Chinese character may account for 3 bytes

A digital asset ID is returned upon issuance, and the digital asset ID generates the HASH from the above asset information.

- Output 3:

Output amount: number of candy

Output script: normal transfer transaction script, the receiving address is the candy address

vReserve Field: application header + application data (money transfer)

Transfer money application data	explain
version number	2 Bytes
Digital assets ID	Is 0, or the current digital asset
quantity	0.1% -10% in quantity
Candy expired time	Storage is the number of months, ranging from 1-3 months
remarks	Up to 500 bytes, 1 Chinese character may account for 3 bytes

.4.26 Additional issuance

For additional issuance, the digital assets must be specified at the time of issuance; the initial issue transaction ID and asset ID, and the additional issue number shall not exceed: Total assets, amount-total initial issue-number of candy.

The output address must be one of the input addresses at issue, the transaction format:

Output amount: the number of additional assets

Output script: normal transfer transaction script with the receiving address in the input (the address that consumes SAFE)

vReserve Field: application header + application data (money transfer)

Transfer money application data	explain
version number	2 Bytes
Digital assets ID	Asset ID to be issued
additional quantity	The number of additional issues made
remarks	Up to 500 bytes, 1 Chinese character may account for 3 bytes

.4.36 Transfer

Transfer tokens or digital assets, through the network address to transfer, transfer is also a lock option, can be locked for a period of time before spending. The transaction format is as follows:

Output amount: Number of assets

Output script: the normal transfer transaction script

vReserve Field: application header + application data (money transfer)

Transfer money application data	explain

version number	2 Bytes
Digital assets ID	Asset ID to be sent
quantity	Number of items sent
locking time	Lock time by block, 0 means no lock
remarks	Up to 500 bytes, 1 Chinese character may account for 3 bytes

.4.46 Destroy

Destroyed, some digital assets may need to be destroyed, such as after the points are redeemed or expired, if they must be designated when issuing token or digital assets, otherwise they cannot be destroyed; and only owners can destroy their own assets, this function is dangerous and used with caution.

At present, it can only be destroyed through command line and RPC interface, without any operation interface, and can only destroy the assets in your wallet. The transaction format is as follows:

Output amount: the quantity of the assets destroyed

Output script: the normal transfer transaction script, the output address is the black hole address

vReserve Field: application header + application data (money transfer)

Transfer money application data	explain

version number	2 Bytes
Digital assets ID	Asset ID to be sent
quantity	Number of items sent
remarks	Up to 500 bytes, 1 Chinese character may account for 3 bytes

.4.56 Give out candy

If the candy is not issued when the asset is issued, the interface can also be used to issue the candy. Even if the candy has been issued but wants to be issued again, the interface can also be called, but the candy can only be issued up to 5 times for each asset. The interface must be invoked by the asset issue address in the following transaction format:

Output amount: the number of candy distributed

Output script: the normal transfer transaction script, the output address is the candy address

vReserve Field: application header + application data (distribute candy)

Transfer money application data	explain
version number	2 Bytes
Digital assets ID	Asset ID to send candy
Distribution of assets	Send 0.1% to 10% of the total to SAFE owners, if the total amount does not reach the above proportion.

Candy expiration date	In terms of the number of blocks, 1-3, between months, if the user sets 3 months, then 3, after the months, if you have not received the candy, it will be invalid.
remarks	Up to 500 bytes, 1 Chinese character may account for 3 bytes

.4.66 Get candy

.5After the distribution of the candy in 6.4.1 and 6.4, the user needs to operate and collect it by himself. The trading format for receiving the candy is as follows:

Input: candy corresponds to transaction ID, output item index; one SAFE input for transaction fee;

Output: the normal transfer transaction script, holding the SAFE address; the output may be multiple, because there are multiple addresses with the SAFE;

Amount: the number of candy received;

Get rules:

(1) Scope of receipt: receive candy only if the address with at least 1 number of SAFE before the block;

(2) The claim proportion is: the number of SAFE in the wallet / the total amount of current SAFE issuance * the total amount of candy assets. If the calculated asset balance is less than 0.0001, it is not allowed;

(3) If the collection time is expired, it is not allowed to receive;

(4) In the local to maintain a whole network candy collection record, according to the block of the transaction record to generate the total collection record of each asset, used to judge whether the current candy can still be received, and quickly find the collection record;

(5) To maintain a local wallet address to receive the candy record form, each wallet address has received which assets, and SAFE, the number of assets;

6.5 Security code

Ancode will focus on strengthening the security, ease of use and compatibility of smart contracts.

.56.1 Safety

(1) The smart contract code must be open source, and the code base address, version number and hash of the source code must be provided to prevent the source code from inconsistent with the compiled code.

(2) Access control of smart contract interface, many smart contracts are attacked, because anyone can access any interface of the smart contract, so in some interface check operation permission is not strict, illegal visitors will be given higher permission; access control can set only the permitted address to access the specified smart contract interface, enhance security.

(3) Smart contract freezing and thawing mechanism, in the event of an emergency, developers can freeze the smart contract, but also freeze the funds, waiting for the appropriate treatment measures before thawing.

(4) Smart contract execution validation mechanism, SVM provide developers with friendly programmability, at the same time to larger performance overhead, for the maximum to avoid the net UTXO trading performance and stability, will be in the entire network vote 21 hardware performance standard super node, responsible for the execution of smart contract validation, ordinary master node is responsible for the execution of the UTXO transaction validation, for smart contract is directly from a super node for the execution of the validation results.

.56.2 Easy to use

(1) For the readability name of the smart contract, refer to FABRIC and EOS, and specify the name similar to the Internet domain name for artificial reading and memory during the creation of the contract, so as to facilitate the promotion of the contract.

(2) The scalable mechanism of smart contract, referring to FABRIC and EOS, separates the storage contract code and the contract status database. The Own er and its authorized users of the contract can be upgraded by redeploying the contract code to

avoid the tortuous upgrade of EVM by redeploying the contract and migrate the contract status database. The contract user references the desired version of the contract through the contract name and the contract version number, avoiding unknowingly citing the latest untrusted version of the contract. Unless the contract user fully trusts the contract developer, he can specify a virtual contract version number to reference the current latest version of the contract at any time. A contract developer cannot specify a contract user that references a version of the contract, but has the right to stop the external services of a version of the contract according to the needs of the smart contract upgrade.

(3) Smart contract status of the database upgrade, reference FABRIC and EOS, provide the corresponding smart contract API, support in smart contract running period rather than compilation period can dynamically modify the state database structure, avoid to modify the state database structure by migration to upgrade, can simplify the operation steps of developers, at the same time save SVM storage and performance overhead.

(4) Status database storage of smart contracts. In S a pp project practice, it is often necessary to store Sapp in block application data and transfer it to relational database for structured data query. SVM selects several relational database engines that meet the

performance as the storage backend of the contract status database. The contract developer specifies the engine type, reads and writes the contract status database through the contract code, and reads only the contract status database through the database engine client. The access control of the contract status database, data desensitization and privacy protection, and the data characteristics and associations in the desensitization process shall be handled by the contract developer themselves.

.56.3 Compatibility

(1) For the api of smart contract, the SAFE network has realized four functional sections of application development, payment, capital and investment through the protocol. SVM will open the programmable ability of each functional section to developers through the api of smart contract.

(2) The fuel and reward mechanism of smart contract calculates GAS usage according to Ethereum EVM and SVM, which is converted to SAFE dosage by GAS price. SAFE officials send specific transactions regulating GAS prices to specific addresses. The GAS is undertaken by the contract caller and is awarded to the miners. In order to encourage developers to contribute to high-quality smart contract services, SAFE officials will discuss with the community to award some GAS to developers being called by the current contract.

(3) At the same time, it is compatible with various smart contract source codes, such as Ethereum and EOS, to make it easier for developers to import and export technical results. Under the premise of unifying all kinds of referenced blockchain product function models, we can seek common ground while reserving differences, and realize the mutual call of different types of smart contracts in the SAFE network system..

The specific technical scheme of code is still continuing to improve, and another document will describe the technical details of code.

7 Joint products of SAFE network

The joint products of the SAFE network include a blockchain middleware and a digital currency payment platform. They do not belong to the SAFE network, but with the combination of the SAFE network, it can further strengthen the convenience of the application development and the convenience of payment.

7. Blockchain middleware

Blockchain middleware products of blockchain applications provide professional blockchain infrastructure services for financial institutions and enterprises and institutions that want to implement the "blockchain

+" strategy, and help customers quickly build the components needed for blockchain applications and quickly develop applications.

7.1.1 Middleware meaning

Blockchain technology must be combined with application scenarios to truly reflect its potential. A large number of domestic and foreign financial institutions, enterprises and institutions are studying blockchain technology in order to combine with business and promote the implementation of application. But they face many problems that hinder the process of application landing:

(1) Application landing cycle is long. To do the application of blockchain, we must first master the blockchain technology and concept, then select the application scenario, choose the blockchain, be familiar with the development technology of the blockchain, and finally carry out the application development and business transformation of the blockchain. The whole landing cycle is long.

(2) Working, high talent cost. Blockchain technology and application have put forward high requirements for the level of talents, technology accumulation and concept change. It is difficult to cultivate cross talents of finance and blockchain in a short period of time, and the talent cost and growth cost are very high.

(3) Blockchain selection is difficult. At present, the underlying technology platforms of blockchain, such as B itcoin, E thereum, Fa bric,

Corda, Chain, etc., are uncertain, and enterprises and institutions must consider a series of problems such as whether the blockchain can exist for a long time, compliance, copyright, operation and maintenance when implementing the application of blockchain.

At present, the underlying technology platform of blockchain (1) cannot fully meet the application needs (2) difficult to choose (3) high learning cost (4) may be replaced (5) unpredictable development. These uncertainties restrict the development and practice of blockchain applications.

Therefore, solving the above three difficulties has become the key to the application of blockchain, and the blockchain middleware arises at the historic moment.

7.1.2 Blockchain middleware

Combined with the concept of middleware, for a variety of block chain underlying technology platform, block chain middleware package a variety of, heterogeneous, block chain, to provide unified API interface, makes the customer switch block chain underlying technology platform at any time, no need to consider their programming language, design style, applicable scenarios, subsequent development, risks and technical uncertainty.

Block chain middleware to block chain cloud service mode run in public network, customers only front-end and JAVA developers, using

SDK development package, call API function, within 1-2 weeks block chain application prototype development, need not understand the underlying technology, greatly reduce the small and medium-sized enterprises to implement the "block chain +" time cost, labor cost and personnel requirements, to implement the strategy of "block chain +" faster.

Blockchain middleware builds a bridge between the blockchain application and the underlying technology platform of the blockchain, which can be considered as the entrance of the blockchain application, which is of great significance.

7.1.3 The combination of SAFE network and blockchain middleware

SAFE network is a typical underlying technology platform of blockchain, which is very convenient to develop blockchain applications and issue various digital assets. The combination of SAFE network and blockchain middleware will play a very interesting effect.

one side, Blockchain middleware can use the SAFE network public chain, With the help of the application development protocol of the SAFE network to achieve asset management, user management, blockchain management and other interface functions; on the other hand, It can also introduce some special functions and application API interfaces from the SAFE network, Such as instant payment, privacy payment, information records, And blockchain applications developed by third parties, And it is integrated into the SDK, Further reduce the difficulty of SAFE network application development, No need to establish the nodes, Just use the SDK to dock the API.

The factors that consume SAFE interfaces and services, are processed by middleware, and users do not need to pay attention to the currency. This is more appropriate for some units that don't like coins and just want to do pure blockchain applications.

7.2 AnPay: a digital currency payment platform

The SAFE network team has successfully developed a centralized, aggregated digital currency payment and application landing system (like Alipay), which mainly solves and provides:

(1) Look for consumption scenarios outside the secondary market for digital currency, and reapply digital currency to its essential monetary attributes. To provide a variety of digital currency with a real landing scene, to avoid the "air currency" said.

(2) Online services: The platform provides online types of merchants to move in and connect with consumers. Provide merchants with the most convenient payment channels for SAFE and other digital currencies. Merchants can choose to settle the digital currency or fiat currency. Choose the settlement of the digital currency to bear the rise and fall of the digital currency itself. When choosing settlement fiat, the platform will solve the digital currency exchange and pay the merchants with fiat

currency. The platform provides a sound settlement / clearing system, and the settlement method is T + X.

(3) Offline services: The platform provides software / hardware / QR code / APP and other equipment and applications for payment from offline portal / shopping mall, and provides a perfect settlement / settlement system to merchants in T + X mode. Merchants access the same way as online services, choose digital currency or fiat currency.

(4) Application services: Provide the public digital currency aggregation payment SDK interface, and provide the digital currency payment docking for the three-party applications. Such as payment, red envelopes, rewards, games and other applications.

(5) Solution services: Provide complete TOB digital currency payment / clearing / settlement solution services for enterprises in need.

(6) Shanghai currency side service: due to the perfect payment / application scenarios of the platform. The platform connects with various issuers of digital currency, and begins to expand to various digital currencies with SAFE as the center. And provide a perfect issuer display system. Improve the circulation rate of digital currency of issuers / network fee consumption / overall valuation of digital currency, etc.

In the implementation process, the construction of the whole digital currency payment platform and application landing platform will be completed according to the steps of "payment platform- -> personal mobile APP- -> digital currency application landing platform". First of all, the payment system of the SAFE network is supported, and the SAFE can be used to pay the handling fees, service fees or subsidies of the platform.

Digital currency payment platform is an excellent way to accumulate the number of users.

7.3 Anbao: digital currency hardware wallet

Anbao (SAFEGEM) is a one-stop digital asset security management hardware wallet produced by the SAFE network team. Anbao (SAFEGEM) adopts the national secret financial security chip to ensure the security of the seed password and private key. The private key never touches the network, the cold end constructs the transaction and signature offline, the hot end APP publishes the transaction online, and the hot and cold end transmits the data through the QR code scanning. At the same time, Anbao (SAFEGEM) adopts the unique security Bluetooth technology, binding one to one between the cold and hot end, stealth to other devices, so as to realize the security update of the cold end of the software, considering the security and application scalability from the design. Currently supports BTC, BCH, BTG, LTC, ETH, ETC, DASH, SAFE, FTO, QUTM, EOS, USDT, BCH fork, ERC 20 tokens, and tokens issued based on SAFE.

Function introduction: Five protection mechanisms to fully guarantee the security of digital assets:

1. Financial level encryption chips to ensure the security of the key

Anbao hardware wallet adopts financial grade hardware encryption chip, encryption chip integrates a variety of national and business secret algorithms, key and seed password are stored in the hardware encryption chip, but not stored in ROM / RAM, which can prevent cracking, prevent disassembly and reading, and physically ensure the security of key and seed password.

2. Cold end trading never touch the net completely cold isolation

Anbao (SAFEGEM) hardware wallet adopts the mode of the cold end structure transaction and the networked App broadcast transaction. The private key will never touch the network in the process of generation, storage and transaction, ensuring that the private key is "cold isolated". Anbao hardware wallet transaction transmission through the encrypted two-dimensional code, anti-interception, prevent hacker attacks, to ensure the security of the isolation of cold and hot end.

3. Multi-layer password protection

The Ambo (SAFEGEM) hardware wallet provides multiple layers of protection, and all the password data is stored in the encryption chip, not in the ROM / RAM.

Level 1: fingerprint / gesture password control wallet use;

The second layer: user password control transaction operation;

The third layer: the key control transaction signature;

Layer 4: HD layered deterministic wallet design to ensure that the seed password has the right to restore the wallet;

4. Multi-currency support

The Amber (SAFEGEM) hardware wallet already supports multiple currencies, It includes convenient management of more than 100 digital assets issued by Bitcoin (BTC), BitCash (B CHABC), BCH fork (B CHSV), Bgold (BTG), Ethereum (ETH), pomelo (EOS), Litecoin (LTC), Ether Classic (ETC), Dashcoin (D ASH), Security 3 (S AFE), USDT, FTO and all Ethereum ERC 20-TOKEN, EOS, and S AFE..0 Anbao (SAFEGEM) supports the timely import and update of high-quality new currencies to meet the basic asset management requirements.

5. Software security upgrade

In order to adapt to the changing rhythm of the currency circle, Anbao (SAFEGEM) original security upgrade mechanism, can ensure the private key on the absolute basis of the latest version at any time, so that users can timely import a variety of high-quality new currencies, enjoy the latest research and development results and functions of Anbao (SAFEGEM), a treasure in hand, permanent use!

7.4 Safety measurement: blockchain application public testing platform

SAFE network team security laboratory released an independent third-party public testing platform- "chain test treasure", Leveraging the value nature of digital currencies, Pionand promote the "Blockchain Quality Margin Plan" to the whole industry-that is, after the completion of the internal test, With the launch of smart contracts and software applications, Take the initiative to lock the corresponding amount of digital currency in the independent third-party public testing platform pledge as the quality margin of the product, Deposit as a bonus public reward loophole, And according to the intelligent vulnerability arbitration mechanism, Effectively protect the interests of the vulnerability submitters, Prevent the project party from showing denial, delay, etc., If no vulnerability is found, After the term of the pledge reaches, Deposit to unlock the original way to return, The project party's attention to software quality with practical actions, At the same time, it can improve the software quality in a high cost-effective way.

一、 Platform membership status: test expert, VIP expert, manufacturer

- Test expert: person who perform quality and safety testing for the application system.

- VIP experts: have involved in special test task (such as high bonuses, private, etc.), platform real-time according to the test experts submitted BUG quantity and level, when accumulated to a certain extent can be promoted to VIP experts, at the same time platform can also recommend industry recognized individual or team for VIP experts (no more than 10).
- Vendor: the owner and operator of the application system, which is the initiator of the public beta task.

2. How to create and publish a project on the platform and complete the review:

1. Register a manufacturer account on the platform, the manufacturer logs in the platform to authenticate the manufacturer, bind the mobile phone, and the administrator real-name authentication, and create the project.

2. Need to have a certain number of digital assets (currently support SAFE, the future can include BTC, ETH, SAFE and major exchange platform currencies), and then create the project for digital asset payment, the system will automatically release your project to the vulnerability reward platform.

3. Complete bug patching by submitting bugs and solution vendor testing and confirming bug level bonus.

7.5 Anyou: Blockchain game platform

Ann swim platform is the world's first docking block chain digital assets (based on SAFE Ann agreement) chess class game platform, Ann play method simple diversity, interesting, guide concise, quickly, use the value of digital assets and cross-platform flow characteristics, improve the value of the game system, can maximize the security of the game.

SGT is a digital asset issued by Anyou (Safe Game Token) based on SAFE. SGT can be exchanged for various digital assets (such as SAFE, ETH, etc.) on Anyou platform for physical prizes. In the future, SGT can also be used across platforms to participate in the points exchange and profit sharing of various game platforms.

8 Technology innovation point of SAFE network

There are many technological innovation points that other blockchain does not have, which are shown as follows:

8.1SafeDPOS consensus algorithm

The unique consensus mechanism of the 2.5 version of the SAFE network, SafePOS, randomly selects 9 long and stable master nodes from more than 3000 main nodes of the whole network to generate a block every 5-10 seconds. After this round of production is finished, another 9 main nodes are selected and carried out in turn.

SafePOS Faster than POW and less vulnerable to 51% attacks; more secure than 101 nodes in BTS and 21 nodes in DPOS, EOS.

8.2 Security and Capital Agreement

The security agreement issues digital assets in the form of agreement. Compared with the issuance of assets, it is safer, because the agreement is a limited state machine, which is more controllable, while the behavior of smart contract is more uncontrollable.

The capital not only realizes the functions of asset issuance, addition, issuance, asset transfer and destruction of assets, but also realizes the confectionery agreement on the blockchain, so that the issuer can distribute and receive candy on the network.

8.3 SAPP APP development protocol

SAPP application development protocol is a series of RPC interfaces, including application registration, application permission setting, application data writing and so on, which is convenient for blockchain application developers to easily write data to the SAFE network blockchain.

SAAPP applications need to be registered, and the RPC interface needs to consume SAFE, so that like ETH and BITCOIN, everyone can write data at will and junk data.

8.4 Ancode smart contract system

The biggest characteristics of safety code are strong security, high compatibility and high ease of use. Ancode will port the EOS account system, compatible with EOS, ETH and FABRIC smart contract, forming a unique smart contract virtual machine SVM, as well as a unique super compatible SAFE network smart contract platform, so that it is easier to build a SAFE network ecology from EOS and ETH.

So far, there is no such a compatible smart contract system.

9 SAFE network vision

Security net space (SAFE) fusion network space 2 (DNC 2) and voting chain (ELT), the introduction of Sa pp application development agreement, launched the original compatibility side chain smart contract system-Ann code, compatible with EOS and ETH smart contract, extend Ann pay (instant payment, security payment), security (asset issuance and management, based on the net issue tokens), Ann (safe vote, the original chain), Ann bao, and other application direction, aims to become the world's largest and most secure digital currency issuance, payment and application development platform. At the same time, together with blockchain middleware, Anfu, Anbao, Antest, Anyou and other products, it greatly simplifies the implementation of the "block chain +" strategy for enterprises and institutions, and builds a strong ecology of tens of millions of users and public chain community from multiple dimensions such as asset issuance and payment landing, application development, asset application, privacy protection, and block chain voting.

There is a long way to go, we, all the way forward.

SAFE network team

On December 15,2021