自由共识
freeconsensus

Free Consensus

Foundation of the Crypto Economy

Free Consensus White Paper 1.0

July 2020

Table of Contents

Free Consensus is a Cryptographic Consensus system that evolved based on the Satoshi Nakamoto Consensus framework. It is an evolution of a peer-to-peer electronic cash system towards the infrastructure of the cryptographic economy (crypto economy). By extending from the decentralized FreeCash to the areas such as the decentralized identity, relationships, credibility, protocols, storage, and the others, it became the foundation of the crypto economy.

1. Cryptographic Consensus (Crypto Consensus)

The Cryptographic Consensus is a technological and economic system built using asymmetric cryptography and distributed consensus mechanisms to mainly solve the problems of information security and information monopoly found in the information economy.

Asymmetric cryptography was created for military use in the 1970s and promoted by the cypherpunk in the 1980s for civilian use to solve problems in network information security and to protect personal privacy. It is mainly applied in network communications and the construction of digital currency systems also known as cryptocurrency.

The essence of distributed consensus mechanism is a simple democratic mechanism, which means it acts in accordance with the rules and judgements agreed by most people. At the end of the 20th century, the emergence of peer-to-peer network technologies, such as Napster, BitTorrent, and others, have provided technological conditions for establishing a global-scale distributed consensus through the Internet.

From 2007 to 2009, Satoshi Nakamoto discovered that the fundamental cause of the failure of early cryptocurrencies was the "centralization" of the system. For this reason, he implemented a distributed consensus mechanism in cryptocurrency and established the first decentralized cryptocurrency: Bitcoin.

The Bitcoin system established by Satoshi Nakamoto using asymmetric cryptography and distributed consensus mechanism is not only a technological system but also an important economic system. It allows people who do not know each other to take the initiative to maintain a vital economic system of the world currency based on self-interests.

"Cryptographic Consensus" or “Crypto Consensus” was titled by combining both concepts of asymmetric cryptography and distributed consensus. It uses asymmetric cryptography to ensure information security while distributed consensus to eliminate central monopoly. Therefore, it can be applied in the construction of information economy infrastructure. Blockchain, however, is only one of the data structures used in the distributed consensus mechanism, so it cannot fully reflect the nature and significance of the Crypto Consensus.

2. FreeCash

Bitcoin is the first Crypto Consensus system, and the basic economic model had fulfilled the requirements of the early development. However, after entering the mainstream economy around 2013, the economic model began to face severe challenges and the contradictions had erupted in the 2015 - 2017 scaling debate.

The main problems exposed in the scaling debate include: 1) the lack of endogenous incentives for developers; 2) the lack of effective governance mechanism; 3) non-professional decision-making by developers and miners in the economic and political issues; 4) serious differences had led to high-cost forks.

The emergence of these problems has showed that Bitcoin is indeed a great experiment. With the in-depth development of social and economic practices related to the Crypto Consensus system, the system needs to evolve, grow, and improve continuously on the economic, political, and social levels.

Unfortunately, most people in the Bitcoin community have not seen the problems yet while Bitcoin has already become a huge economic system. However, it is difficult to evolve efficiently without a tested governance mechanism. This had led to the failure of scaling, the core function of Bitcoin then changed from peer-to-peer electronic cash to digital gold, a store of value asset.

On the other hand, Bitcoin Cash has recognized the block scaling, inherited the direction of peer-to-peer electronic cash, and has been evolved for survival since its inception. It also modified the difficulty adjustment algorithm and added reorganization protection. But it is still not easy to solve the problems of developer incentives, community governance, professional decision-making, and high-cost forks.

On the basis of inheriting the achievements of Bitcoin Cash evolution, FreeCash has improved the Nakamoto Consensus framework in order to solve these problems:

1) Increase the issuance of governance funds from each block, and use the governance funds to incentivize builders in various fields, including developers;
2) All builders participate in the post-event evaluation of contributions together to realize funds distribution based on contributions;
3) Builders in various fields obtain the decision-making rights according to their contributions in order to achieve professional decision-making in various fields;
4) Encourage consensus forks to be initiated if major differences occured, and make use of the delay of the contribution rewards released to achieve the interests compatibility of all fork parties.

FreeCash was initiated at 0:00 on Jan. 1, 2020 from block 0. It then experienced CPU mining, GPU mining, and ASIC mining within one day. It also achieved diversification of the ecosystem

facilities, such as mining pools, browsers, wallets, portals, etc., within two months and has been operating normally.

The governance mechanism of FreeCash has completed two phases of contribution evaluation (this article is wrriten in July, so far 4 phases has completed), where 269 contributions of 103 cryptographic identities have been rewarded. The contribution incentive mechanism has pushed forward a rapid growth of the scale of the ecosystem builders. The first stage of the improvement on the Nakamoto Consensus framework was successful.

3. Cryptographic Identity (Crypto Identity)

The decentralized governance mechanism of FreeCash requires builders to build, collaborate, evaluate, distribute, and engage with other activities with a decentralized identity. As a decentralized currency system, the Nakamoto Consensus framework has already provided a decentralized identity system, which consists of private key, public key, and address system.

In the community governance, although it addresses and public keys can represent identities, they are not user-friendly, lack social traces, and are difficult to remember. To this end, FreeCash has established “Cryptographic Identity” or “Crypto Identity” (CID) system. Anyone can declare on chain, a self-defined username with the last four suffixes of the address to create a Crypto Identity that is one-to-one correspondence between the address and the public key and it is unique over the entire network.

CID contains social meaning, easy to recognize and remember, and it corresponds to an address after adding the suffix of the address. It also improves security and prevents the behaviour of resources monopoly and rent-seeking caused by cybersquatting.

The application of CID in the contribution evaluation proves that individuals can use multiple CIDs to engage in different activities independently and each activity can form a single complete loop of life. For example, with two independent identities such as developer and promoter, one can

separately work, collaborate, evaluate, obtain distributions, purchase, or invest and so on to achieve identity freedom.

CID not only can be used for different identities of individuals, it can also represent a team consisting of many people as well as represent a product, website, app, or a device. It is actually a universal subject identity in the crypto economy. The FreeCash ecosystem has already started to use CID to register teams and release products.

The Crypto Identity system is developed from the FreeCash system, but it is actually the cornerstone of the crypto economy. This identity system has been established in the Nakamoto Consensus framework and then on top of it is the Bitcoin currency system. CID is the transformation of the identity system in Nakamoto Consensus framework based on the demands in applications. It not only can improve the currency system but also can encourage the evolution of a richer crypto economy.

4. Cryptographic Relationships (Crypto Relationships)

Once the builders began to use crypto identities to deal with various activities, the need for crypto identities to establish mutual relationships arose. These relationships are registered on the main chain through private key signatures, then an open and credible crypto relationships network could be established to build the social foundation of the crypto economy.

For example, if a person has at least two CIDs, one is to store private key offline to ensure the safety of the main rights and interests. The other one is to store private key online for frequent signings on daily basis. The offline CID can be defined as the master of the online CID. Once the online private key is disclosed, the offline CID can declare and transfer some transferable rights and interests.

Besides one-way authorization, multiple CIDs can sign simultaneously to declare mutual relationships on the chain. For example, three CIDs can declare an equaivalent relationship on the chain to share all the executable rights and interests therefore identity backup can be achieved.

More scenarios of Crypto Relationships can be found in the authorizations or contracts between multiple people. For instance, in the contribution evaluation, a builder CID can issue a statement on the chain in order to entrust a evaluator CID to represent all of its contribution evaluation matters.

The evaluation application platform will then allow the evaluator CID to act as a representative of the authorizer for the evaluation matters based on such on-chain statement.

Multiple CIDs can form a team or release a product (app or service) through an on-chain joint statement to establish a collaborative and contractual relationship or to share publishing rights. In this way, various complex business relationships which can be checked, proven. and cannot be tampered can be established on the chain.

5. Open Credibility

Based on CID and Crypto Relationships, economic activities are recorded on the chain, which later can be accumulated and used to form an open credibility system. This system provides a basis to the commercial activities of the crypto economy.

The amount of FreeCash (FCH) owned by a CID and its on-chain transaction records act as an important credit indicator which may show the solvency of the CID, reflecting its financial status and providing credit reference for further business purposes.

The unique Coin Days (CD) of the Nakamoto Consensus framework can be used to prevent “click farming” and “deal-hunter”. Once any amount of FCH is received, Coin Days will start to generate as time passes until they are spent. Coin Days will be destroyed once they are spent. With the condition of destroying Coin Days, the cost of counterfeiting can be greatly increased. FreeCash has successfully applied Coin Days in the activities such as winning prizes with CID registration and Coin Days rewards.

Contribution rewards are the rewards given to CIDs which contributed to the construction of the ecosystem. It is recorded on the chain and can be used as an important indicator in the CID credibility evaluation. The CID with greater historical contributions and received more rewards will gain higher reputation.

CIDs can also evaluate each other directly through on-chain declarations. They can also perform on-chain authentication on the declarations or behaviours (such as contribution declarations, products release, and others) made by other CIDs. These evaluations and authentications can combine with the subject's credibility to add more credibility information to the CIDs being evaluated.

Institutions that are good at credibility evaluation can make use of the rich on-chain data to build their own credibility evaluation system, rate the CID's credibility and use it for further business purposes. This kind of credibility evaluation can achieve a complete disclosure of the basic data and allow for healthy competition in the rating services, which will then eliminate information monopoly and improve social credibility.

6. Free Protocols

Since the Nakamoto Consensus framework, the decentralized Crypto Consensus system is an open protocols system. Anyone can follow the protocols to enter the consensus voluntarily. FreeCash, Crypto Identity, and Crypto Relationships are all realized through protocols. The decentralization of the protocols determines the decentralization of the Crypto Consensus.

Free Protocols are the prerequisites for the open infrastructure. The protocols system of Free Consensus is completely open, anyone can publish protocols in their own ways. Anyone can also adopt or implement any protocol in their own ways. No individual, organization, or protocol is obliged to implement any protocol.

Various protocols are free to compete in the market, the best ones will remain and evolve to become a relatively stable protocols system.

The newly emerged protocols need to attract adoption from more applications. The more adoptions a protocol can get, the bigger collaborative advantage it will have. But whether it can be adopted by more applications ultimately depends on whether these applications can get more users in the market.

The Free Consensus system does not have any enforcement institution and enforcement measure. Hence, various protocols can be duplicated and improved freely. According to the current consensus, a protocol should be published on the main chain and signed with the publisher’s CID.

Anyone can improve any published protocols and then publish the improved protocols with their signature, the person only needs to mark the referenced protocols. In this way, adopters can trace the source of the protocols and subscribe to the updated information of the publishers at all levels for easier understanding, trusting and adopting the protocols.

7. Hierarchical Consensus

In the process of expanding FreeCash to more decentralized facilities, the contradictions between decentralization, a higher performance and more functionality has emerged. This can be summed up to a trade-off between “security” and “convenience”. Decentralization is highly secure but it is difficult to achieve the conveniences provided by performance and functions. In other words, it is difficult to achieve good user experiences.

In fact, security and convenience have always been trade-off for human beings under given technological conditions. A rational solution is to cater trade-offs in the sense of multi-layers or hierarchically based on actual demands. The demand for high security requirements is met using the decentralized way, the demand for high convenience requirements can be realized with the centralized method, and the demand for moderate security and convenience can be realized with the multi-centered method.

The FreeCash system has adopted this hierarchical consensus strategy whereby the hash of the currency, identities, protocols, important relationships, and important data are published on the main chain to achieve high degree of security and to ensure basic freedom. Users’ important data is stored in multi-nodes distributed storage to prevent information monopoly while improving performance and experience. Large amount of daily data which are not important to users are stored in local or centralized cloud storage to provide the best user experience.

Currently, the data volume stored in the FreeCash main chain is rather small, as large amount of user data and public data have started to be stored in the Freedrive multi-nodes distributed storage system. With Free Protocols, these data do not depend entirely on Freedrive, they can be migrated to other distributed storage system (such as IPFS) or centralized storage system.

FreeCash will continue to adhere to the market economy direction of collaboration and free competition in order to absorb and adopt various achievements, applications, and facilities of both the internet economy and crypto economy to jointly build a free and open collaboration system which is hierarchical and cross-chain capable that will help to enhance human economic freedom.

8. Free Consensus

Crypto Consensus began with Satoshi Nakamoto's goal of achieving peer-to-peer electronic cash. FreeCash is also trying to achieve the same goal by improving the Nakamoto Consensus framework.

The practices of the currency improvement show that purely currency decentralization is difficult to change the fragmentation of global economy caused by information monopoly. Thus, Crypto Consensus can and must build the decentralized global economic infrastructure in more aspects.

Without prior planning, the practice of FreeCash has been extended to Crypto Identity, Crypto Relationships, open credibility, Free Protocols, distributed storage and some other fields and will continue to extend to more fields.

"FreeCash" could no longer represent the rich contents of this consensus. So, we are expanding it to become "Free Consensus" system and FreeCash acts as the main currency in this system.

Free Consensus is an example of the Crypto Consensus mechanism. The phrase "Crypto Consensus" fully embodies the decentralized logical framework constructed by asymmetric cryptography and distributed consensus, so it should not be used as the name of an example to avoid any confusion.

The purpose of Crypto Consensus, almost like all other great human inventions, is to realize greater human freedom. For this reason, we named this example of the Crypto Consensus as “Free Consensus”, that is a freely evolving Crypto Consensus system.