White paper

CRON Group

Contents

Abstract

Existing investors have held financial assets by investing in stocks of publicly traded listed companies or investing in bonds, but investing in start-ups, SMEs and venture businesses has been extremely limited to private individuals. There was difficulty in the recovery of investment or the sale. To solve this problem, the CRON is designed to allow an unspecified number of ordinary individuals to invest in or facilitate the sale of financial products such as stocks, debentures and convertible bonds issued by startups, SMEs and venture companies. With CRON, Everyone can invest in financial products such as stocks, bonds and convertible bonds issued by start-ups and small venture companies and also sell or transfer them to others. CRON is an ERC20 token using DAPP(Decentralized application) function of Ethereum network which is one of the most representative blockchain platform of today focusing on transparency, security and independence in intrinsic transactions. Unlike other virtual currencies, it approach from a business perspective. We hope that it could be alternative currency to the non-transaparent business transactions that have been problematic since it focuses on the integrated monetary viewpoints for individual to individual, business to individual, business to business business.

1. What is cryptocurrency?

Cryptocurrency is a form of virtual money whose origins can be found in virtual money. Virtual Money refers to digital money or electronic money that is used electronically in a virtual space that is connected to the network without any bills or coins. This virtual money is issued or managed by the developer, as the issuing institution is an enterprise or an individual. Because of this feature, virtual money is a payment method that is used only in a specific virtual community. The first virtual currency was first raised in 1983 by David Chaum. In 1990, he founded DigiCash and moved his research into practice but in 1998, the company went bankrupt and left the company.

Even after that, there was an attempt to create a virtual currency called eGold that transcends the border but it was difficult to recognize the power of money from the government or the financial industry as long as the developer had control, issuance and operation rights. eGold was operated by real gold or silver operators and tried to give real value but it quickly collapsed due to government and financial regulations.

All of the initial failed virtual currencies have the limitation that the issuing or operating entity is dependent on a specific company. Therefore, when the operator loses trust or terminates the service, the value is lost. Even if the service is not terminated, the possibility of the end of service is also lowered in reliability and value of virtual money. So the possibility of virtual money seemed to have lost its light unless it was under the control of powerful institutions like real money.

But beyond this kind of dependency, using strong cryptographic technology that can prevent hacking in advance combined with blockchains which can not be controlled by any individual is the key concept of Bitcoin which is proposed by Satoshi Nakamoto. With the emergence of bitcoin, a cryptocurrency market has been formed. Unlike previous virtual money, network is not maintained by developers but distributed. So after initial deployment, developers are not able to modify them nor do developers or individuals have the authority to operate them. And because of the unique irreversible nature of encryption technology and the blockchain, all transactions are transparent and seamless. Especially, the characteristic of being able to deal with the global market beyond the control of the central organization became noticeable and the cryptocurrency market became a big opportunity gradually.

2. Structure of Blockchain

Basically, a block chain is a chain of digital blocks which can be seen as an encrypted digital electronic book. Each block contains the transaction details of the participants trading currency and the hash value, difficulty and nonce value of the previous block. The effective algorithm for building the first block coinciding with the bitcoin is as follows.

a. Make sure that the timestamp value is greater than the timestamp value of the previous block and is within 2 hours.

b. Verify that the proof of work is valid.

c. Set S[0] to be the last state of the previous block.

d. Let TX be the transaction list of the block with n transactions. Returns false if any of S[i + 1] = APPLY (S[i], TX[i]) sets returns an error for all i in the closed interval 0 ... n-1 And terminates.

e. Returns true and registers S[n] as the last state of this block.

Here the conditions for the two proofs of work are as follows. The double SHA-256 hash value of each block represented by a 256-bit number must be smaller than the dynamically adjusted target value. The purpose of the proof-of-work is to make it difficult to create blocks, preventing attackers from arbitrarily manipulating the block chain. Since SHA256 is designed as an unpredictable pseudo-random function, the only way to create a valid block is to check the process of verifying that the new hash value generated while increasing the nonce value of the block header satisfies the condition. The bitcoin is readjusted by the network every 2016 blocks allowing nodes to generate new blocks on average every 10 minutes. From a structural point of view, we use the merkle Tree protocol. A merkle tree is a kind of binary tree which consist of numerous leaf nodes containing base data which is located at the bottom of the tree, an intermediate node consisting of a hash of two child nodes immediately below itself and a hash of two child intermediate nodes. It is a set of one root node located at the top of the constructed tree. The structural specificity of this merkle tree guarantees the integrity of the data while allowing the data of any block to be transmitted separately. If a node of the bitcoin downloads only the block header from one source and downloads the remaining transaction information from the other node, it is guaranteed that the data is still accurate. In addition, since the hash value of the lower nodes affects the upper nodes, even if the data is changed to a fake, the root value of the final merkle tree is changed as a result of changing to the hash value of the upper parents. As a result, Proof of work can be easily done. This merkle tree protocol is a bitm coin based protocol and Ethereum uses a similar method. The biggest difference, however, is that the Etheric block has the most recent copy of the state and two other values (block number, difficulty) are also stored in the block.

The validation algorithm of Ethereum is as follows.

a. Make sure that the previous block you are referring to exists and is valid.

b. It is confirmed that the time stamp of the current block is larger than that of the previous block referenced and smaller than 15 minutes after the current time point.

c. Make sure block number, difficulty, transaction root, uncle root, gas limit, etc. (various other low level concepts) are valid.

d. Verify that the proof of work contained in the block is valid.

e. Let S[0] be the last state of the previous block.

f. Let TX be the n transaction list of the current block. Set S[i + 1] = APPLY (S[i], TX[i]) for 0 to n-1. If the application returns an error or the total gas consumed in the block up to this point exceeds GASLIMIT, an error is returned.

g. Let S[n] be the reward block paid to the digger and call it S_FINAL.

h. Verify that the merkle tree root of state S_FINAL is equal to the final state root of the block header. If these values are the same, the block is a valid block, otherwise it is judged to be invalid.

The biggest difference between the tree structure of ethereum and bitcoin is that the state is stored in a tree structure and the difference between blocks and blocks is very small. In other words, most of the contents of the tree are the same between two adjacent blocks, so once data is stored, pointers (hash of the subtree) can be used for reference. By modifying these existing merkle tree concepts, the tree used for ethereum, known as the actual Patricia tree, not only modifies the node but also effectively inserts and deletes the node to increase the efficiency of the operation. So this saves much more storage space than bitcoin.

3. Ethereum platform

Bitcoin, unveiled in 2009 by Satoshi Nakamoto, was not much of a spotlight then, but gradually came into focus the innovation. Bitcoin based on blockchain is the root and the beginning of the current cryptocurrency market, as Bitcoin solves the following problems: the large amount of fees that inevitably arise from the centralization of currency exchange through financial institutions and the security of the blockchain of distributed network-based arrangements.

Alternative applications using blockchain technology often include the following: Colored coins that represent custom currencies and financial products on a block chain, smart assets that represent ownership of physical objects, Namecoins that record non-dynamic assets such as domain names, a more complex form of smart contracts that manage digital assets by code that implements arbitrary contracting rules and a decentralized autonomous organization("decentralized autonomous organizations", DAOs).

The Ethereum platform, in particular, supports smart contracts. Smart contracts are digital contracts and are one of the computer protocols. Automatically perform reliable transactions without involvement of other third parties. These transactions are traceable and irreversible. Smart Contract was first proposed by Nick Szabo in 1994. Smart contracts enforce contractual provisions partially or completely automatically and this objective is to provide more economically superior functionality in terms of being more secure than traditional paper contracts and reducing commissions. These smart contracts are implemented in many cryptocurrency. At present, smart contracts are mainly used for general purpose calculations in blockchains or distributed ledgers. It is mainly used by the ethereum foundation or IBM and is a kind of computer program rather than a classic contract. Basically, a smart contract is not a new concept at all but rather a program that coded existing contracts.
On the other hand, what Ethereum is offering is a blockchain framework in which a complete turing-complete programming language is built. Conventional bitcoin internally handles transfer through the inner script language. It is difficult to apply various levels of application because it intentionally supports only about 30 limited commands. To overcome this limitation, Ethereum has chosen the Turing complete

language as the language for smart contract creation from the beginning and this programming language allows users to create "contracts" includes arbitrary state transition functions that convert 'any state' according to coded rules. This not only makes it possible to implement the systems described above, but it will also make it very easy to create many other applications we have not even imagined yet.

Ethereum was proposed as a functional upgrade of Master Coin by Vitalik Buterin, a participant in the first Master Coin project. In 2013, Ethereum was proposed as an independent project and used 'ether' as a medium to use computing resources and to use blockchain network. Unlike bitcoin, Ethereum serves as a platform for performing various types of smart contracts on a blockchain network through Turing's complete language. The currency to perform work on the platform has a unit called ETH, which performs the intermediary role(basic trading unit) in all transactions and smart contracts.

4. ERC20 for smart contracts

ERC20 is the technical standard for smart contracts that is the basis for implementing tokens in Ethernet blockchains. It was originally proposed by Fabian Vogelsteller on November 19, 2015 and defined some of the general features that ethereum-based tokens should implement, helping developers to program what new tokens must adhere to in the ethereum-based ecosystem. ERC20 is now attracting the attention of many ICO-based crowdfunding companies with its potential based on the ease of deployment and the integration of Ethereum token standards. ERC stands for Ethereum Request for Comment and 20 is the number assigned to this request. The majority of tokens published in the Ethereum blockchain are compatible with the ERC20. ERC20 has more than 83,400 tokens as of May 2018 and the most successful ERC20 tokens.

The ERC20 token has the following functions.

a. totalSupply
Total token volume

b. balanceof(address _owner) constant returns (uint256 balance)
Account lookup of owner's account

c. transfer(address _to, uint256 _value) returns (bool success)
send '_value' to '_to' address

d. transferFrom(address _from, address _to, uint256 _value) returns (bool success)
send from '_from' to '_to' about '_value' amount

e. approve(address _spender, uint256, _value) returns (bool success)
Allow _spender to withdraw up to _value amount in account.

f. allowance(address _owner, address _spender) constant returns (unit256 remaining)
The amount that _owner has the _spender fetch

The ERC20 tokens implemented in keeping with this set of technical standards are transparent to transactions, easy to use and compatible by everyone and many cryptocurrencies now form a variety of new kind of crpytocurrency using these standards.

5. CRON token

CRON is a cryptocurrency which has the following three purposes for the following start-up and venture company investments:

The first is a free transaction for personal-to-individual online business.
Second, horizontal transactions between individuals and companies.
Finally, the goal is transparent transactions between companies.

CRON's free trading and transparent transaction history can be used as a clear indicator of trading business. It also provides transparency and anonymity of transactions, ease of account creation and smart contracts, all available 24 hours a day worldwide. Existing investors have held financial assets by investing in stocks of publicly traded listed companies or investing in bonds but investing in start-ups, SMEs, and venture businesses has been extremely limited to private individuals. There was difficulty in the recovery of investment or the sale. To solve this problem, the CRON is designed to allow an unspecified number of ordinary individuals to invest in or facilitate the sale of financial products such as stocks, debentures and convertible bonds issued by startups, SMEs and venture companies. With CRON, everyone can invest in financial products such as stocks, bonds, and convertible bonds issued by start-ups and small venture companies and also sell or transfer them to others.

References

1. https://github.com/ethereum/go-ethereum
2. Vitalik Buterin(2014), "So where did the name Ethereum come from?" https://forum.ethereum.org/discussion/comment/3389/#Comment_3389
3. White Paper: ethereum/wiki Wiki, Github, https://github.com/ethereum/wiki/wiki/White-Paper
4. White Paper: bitcoin, https://bitcoin.org/bitcoin.pdf
5. Accredited Standards Committee X9, *American National Standard X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)*, November 16, 2005.
6. Certicom Research, *Standards for efficient cryptography, SEC 1: Elliptic Curve Cryptography*, Version 2.0, May 21, 2009.
7. López, J. and Dahab, R. *An Overview of Elliptic Curve Cryptography*, Technical Report IC-00-10, State University of Campinas, 2000.
8. Daniel J. Bernstein, Pippenger's exponentiation algorithm, 2002.
9. Daniel R. L. Brown, *Generic Groups, Collision Resistance, and ECDSA*, Designs, Codes and Cryptography, **35**, 119–152, 2005. ePrint version
10. Ian F. Blake, Gadiel Seroussi, and Nigel Smart, editors, *Advances in Elliptic Curve Cryptography*, London Mathematical Society Lecture Note Series 317, Cambridge University Press, 2005.
11. Hankerson, D.; Vanstone, S.; Menezes, A. (2004). *Guide to Elliptic Curve Cryptography*. Springer Professional Computing. New York: Springer. doi:10.1007/b97644. ISBN 0-387-95273-X.