Bit Finance：Forked Network based on Bitcoin

BTF Foundation
www.btf.finance

Abstract. Bit Finance is a forked network based on Bitcoin. It is based on Bitcoin but operates independently from Bitcoin. Bit Finance is currently managed by the DAO community of the BTF Foundation.
Satoshi Nakamoto proposed Bitcoin, which does not require any central organization to issue and manage. It only requires a network of countless computers to maintain and operate.This network is like a huge DNA molecule. It is connected by many small data blocks. Each data block contains some transaction information and a digital fingerprint. These data blocks are like DNA nucleotides. They are arranged according to the Certain rules are arranged together to form an ever-growing chain. This chain is the Bitcoin ledger, which records all transaction history. It is public and can be viewed and verified by anyone.

1. Introduction

Bit Finance is a forked network based on Bitcoin. It is based on Bitcoin but operates independently from Bitcoin. Bit Finance is currently managed by the DAO community of the BTF Foundation.Satoshi Nakamoto built a peer-to-peer network technology to realize a true online direct payment method that is free from the shackles of third-party financial service institutions, and is used to deal with the "double payment" problem in the electronic payment system of Internet commerce. Existing electronic payment systems are built on a trust-based model, and the inherent flaws of this model are obvious.With financial institutions having to step in to resolve disputes, fully irrevocable transactions become a luxury. Mediation costs raise transaction costs, compress the minimum size of feasible transactions, and kill the possibility of providing services for daily micro-transactions. Costs in a broad sense make the system lose the ability to provide irrevocable payments for irrevocable types of services. Since users have the possibility of reversing payments, trust needs to be sustained over a period of time, which leads merchants to have to be wary of their customers and harass them for more information they no longer need. Inevitably, a certain percentage of fraudulent transactions will be

tolerated. Although using cash can avoid these costs and payment uncertainties, no merchant will pay without going through a trusted third-party communication channel.
This is why an electronic payment system based on cryptographic proof is needed to replace the original trust-based model, allowing any two parties intending to transact to pay directly without going through a trust-based third party.Calculated invalid transactions will be automatically rejected to protect sellers from fraud, and regular conditional contracts will be automatically executed to make it simple to protect buyers. In this paper, Satoshi Nakamoto proposes a peer-to-peer distributed timestamp server to generate a cryptographic proof scheme for time series-based transaction ordering to solve the double-spending problem. As long as the sum of the CPU computing power controlled by honest nodes is greater than the sum of the computing power set of colluding attack nodes, the system is safe.

2. Transactions

We first think of an electronic currency as a chain containing a series of digital signatures. Each currency trader encrypts both the previous transaction information and the public key of the subsequent owner using hash technology, then digitally signs it, and finally connects this information to the tail of the electronic currency. The latter payee performs signature verification through the private key and the public key in the chain to confirm that he is the owner of the chain, that is, the electronic currency.The problem with this process, however, is that the payee still cannot verify whether an owner of the coin has double-spent the currency. The usual solution is to introduce a trusted central authority or mint to check every transaction. of has been double spent.
After each transaction, the currency must be recycled by the mint to issue a new currency. Only currency issued directly from the mint can be trusted to not be double-spent. The disastrous thing about this solution is that the entire money system relies on some company to run the mint, just like a bank, and every transaction has to go through them.We need a way to let the payee know that the previous owner of the currency did not sign and authorize any earlier transaction to cause a double spend.Our purpose is to calculate the previous transaction, and we don't need to care whether the subsequent transaction double-spends it.The only way to confirm that the transaction does not exist is to know all the previous transactions. Based on the Mint model, the Mint is aware of all transactions and determines which transaction request arrives first.To accomplish this without a trusted third party, transactions must be published publicly, and we need a system where each participant agrees on a unique order history that they

have received.The payee needs to prove each transaction by having the primary node agree that they have received the transaction first.

3. BTF Network

Bit Finance is a cryptocurrency based on a peer-to-peer network, and its transaction records are saved in a distributed ledger called a blockchain.The blockchain is composed of many interconnected data blocks. Each data block contains a certain amount of transaction information and a hash value.A hash is a digital fingerprint that uniquely identifies a block of data and is linked to the hash of the previous block to form an ever-growing chain.

We can compare the blockchain to a molecular structure similar to DNA. It is also composed of many interconnected units. Each unit contains certain information and a pointer to the previous unit.The unit of DNA is nucleotides composed of four bases (A, T, C, G). They are arranged in a certain order in a double-stranded helical structure. Each nucleotide is connected to another strand. The complementary bases pair up to form a base pair.The base pairs of DNA can be used to store genetic information and are linked to the previous base pair to form an ever-extending chain.

Blockchain and DNA are also similar in that they both have the function of replication and verification.Blockchain replication means that each node can have a complete copy of the blockchain, which can increase the security and reliability of the blockchain.The verification of the blockchain means that each data block needs to go through an algorithm called proof of work to verify its validity, which can prevent the blockchain from being tampered with or forged.Similarly, DNA replication means that each cell can have a complete copy of DNA, which can ensure the transmission and expression of genetic information.DNA verification means that the addition of each nucleotide needs to be catalyzed and tested by an enzyme called DNA polymerase, which can ensure the accuracy and stability of DNA.

4. Proof of work

Satoshi Nakamoto will need to use a proof-of-work system to build a distributed timestamp server on a peer-to-peer basis, rather than the previous newsgroup and forum mechanisms. After the data is hashed, the proof-of-work checks the hash value of a data using the secure hashing algorithm SHA-256.Hashing starts with a certain number of 0 bytes, and

the average workload of checking increases exponentially with the number of 0 bytes, while verification only requires one hash operation.

To make an on-chain timestamping network feasible, Satoshi Nakamoto adds a non-repeatable random number into the data block and performs a certain amount of work to find it. The hash of the data block already contains the required number of zeros. byte.Once the CPU processing power has been proven to be sufficient for the required workload, this block of data cannot be modified without redoing all the work. Subsequent data blocks are linked at the end, and modifying the information in the data block requires redoing the workload of all subsequent data blocks.

This workload system also solves the problem of collective decision--making about who represents the majority.If the majority is based on a one IP address one vote mechanism, it will be destroyed by someone who can allocate a large number of IP addresses. The workload proof is based on one CPU one vote.Most decisions are represented by the longest chain, which also represents the input of the greatest effort effort.If the majority of CPUs are controlled by honest nodes, the honest chain will grow the fastest, outpacing any competing chains.To modify a past block, an attacker would have to redo all the work in that block and all subsequent blocks to catch up with the work of more honest nodes.Satoshi Nakamoto In order to compensate for the gains from the pace of hardware increases and changes in node runtime, the proof of work will be determined by a moving average, which is the average number of data blocks generated per hour.If they are generated too quickly, the difficulty increases.

New transaction broadcasts do not need to reach all nodes, they only need to reach as many nodes as possible and they will be integrated into data blocks.Block broadcasts also tolerate discarded information. If a node does not receive a data block, it will keep requesting it until it receives the next data block, believing it to be the missing one.

5. Motivation

Bit Finance was forked directly from the original Bitcoin source code so there are many similarities between the two. Both networks use a proof-of-work consensus mechanism, and anyone can participate and contribute.It does not require any central organization to issue and manage, it only requires a network of countless computers to maintain and operate.This network is like a huge DNA molecule. It is connected by many small data blocks. Each data block contains some transaction information and a digital fingerprint. These data blocks are like DNA nucleotides. They

are arranged according to the Certain rules are arranged together to form an ever-growing chain.This chain is the ledger of Bit Finance, which records all transaction history. It is public and can be viewed and verified by anyone.

However, this ledger cannot be modified casually. It requires a special algorithm to ensure its correctness and security. This algorithm is proof of work. It is like the replication of DNA. It requires a lot of energy and time to complete.In the Bitcoin network, there are some special computers called miners. Their task is to generate new data blocks through proof of work and add them to the ledger, so as to ensure the update and consistency of the ledger.Miners are like DNA cells, they increase their number and functionality through DNA replication.

However, miners are not selfless. They need to be motivated enough to perform these complex calculations. This is the incentive mechanism of Bitcoin miners. It is like the incentive mechanism for DNA replication. It is a way to pay a price to obtain rewards. process.The reward for Bit Finance miners is Bit Finance, which is a digital currency that has a certain value and scarcity. Miners can obtain Bitcoin income through mining, which is their advantage for survival and prosperity.The price of Bitcoin financial miners is electricity and hardware, which are the resources and tools for mining. Miners need to consume a lot of electricity and hardware to mine, and this is the price of their energy and materials.

This is the incentive mechanism of Bitcoin financial miners. It is a key factor in ensuring the sustainability and security of the operation of the Bitcoin financial network. It is an artificially created digital structure that is surprisingly similar to naturally existing biological structures. The analogy between them can help us better understand their principles and characteristics.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.
[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal
trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.
[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no
2, pages 99-111, 1991.
[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping,"
In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.
[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference
on Computer and Communications Security, pages 28-35, April 1997.
[6] A. Back, "Hashcash - a denial of service counter-measure,"
http://www.hashcash.org/papers/hashcash.pdf, 2002.
[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and
Privacy, IEEE Computer Society, pages 122-133, April 1980.
[8] Satoshi Nakamoto, "https://bitcoin.org/bitcoin.pdf" .