Bitcoin Krypton

BTC Eternity - Bitcoin Krypton

Sustainable in the future without updating P2P (Peer to peer) Electronic Currency System

Satoshi.K satoshi.k@bitcoinkrypton.org

https://bitcoinkrypton.org

Abstract.

"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone".

The content mentioned above is a quote from the abstract of Satoshi Nakamoto's Bitcoin whitepaper.

The original Bitcoin stated in its abstract that its goal was to build a trusted third-party electronic cash system through proof-of-work.

As of 2024, 15 years after the original Bitcoin was announced, it has been confirmed that compatibility between the newly updated Bitcoin program and the original program is not working properly, and the Bitcoin derived due to that problem has been confirmed. It raises the issue of future sustainability, and as an alternative to solve the problem, it is a new electronic money program that can be operated continuously without updates at any point in the future without a trusted third party that meets the goals of Bitcoin Original. We would like to announce in Bitcoin Krypton.

0. Satoshi Nakamoto’s Bitcoin and current Bitcoin are different.

Bitcoin is a program that started with the distribution of the source code in January 2009, and is a P2P electronic cash system. Despite initial doubts, Bitcoin has grown into an important asset in global finance, with its users and transaction volume steadily increasing. The inherent limit of 1 megabyte per block allowed approximately 2,100 transactions per block, and within this limited size of the distributed ledger, a competition system was introduced to ensure that transactions that offered higher fees were transmitted first, and those that did not Transactions were stored in the Mempool memory space, and as network usage increased, the fees were designed to increase accordingly. Among the numerous proposals that can dramatically improve Bitcoin's transmission limit, the SegWit update using the Lightning Network separates the signature part and data part when recording a block transaction, and sends the signature part to the Lightning Network. It proposed a dual method of recording data blocks and recording data blocks on the Bitcoin network, but although there was initially resistance to the introduction of SegWit from the Bitcoin miner network and user and supporter groups, over time, efficiency and data blocks were recorded on the Bitcoin network. In 2017, as the profit perspective emerged and the argument was accepted that the SegWit upgrade is nothing more than soft forking, that

the original Bitcoin source and the future source are compatible with each other, and that blockchain data is synchronized between nodes, Finally, the SegWit upgrade was applied to Bitcoin's original code. Because of this, Bitcoin transactions have improved by about 2 times. However, despite the incompatibility between the originally promised original program and the current version, no one is interested in the problem.

Currently, the Bitcoin network is in crisis. Satoshi Nakamoto is gone, and his original Bitcoin program no longer works.

If you think about it carefully, this represents the most serious contradiction and threat to Bitcoin's blockchain (its incompatibility).

The Bitcoin developer group proposed two methods, the SegWit method and SegWit2X, as a way to improve Bitcoin's transmission speed and resolve the transaction backlog in the Mempool. Of course, even after the application of SegWit was completed in 2017, the problem of waiting transactions accumulated in the memory pool was not resolved.

The former, SegWit method, does not physically increase the block capacity of 1MB by using a soft forking method, but divides the signature part and the data part, so in reality, an increase in block capacity of 4MB can be expected, but in the past version It was a proposal that it could be perfectly compatible with (Satoshi' s Bitcoin program), while the SegWit 2X method raised the block capacity to 2MB, improved many parts, and branched into a completely different new blockchain, called Hard Forking. It was inside. Naturally, most users preferred soft-forking, as it preserved the identity of Satoshi Nakamoto's blockchain while enhancing speed and security, fixing various bugs and especially improving TPS by 4 times and reducing transmission costs. Users had anticipated a perfect upgrade that would remain fully compatible with the original blockchain. However, in reality, not many people are aware of these technical nuances."

The number 21 is the same as the Easter Egg planted by Satoshi Nakamoto. The total amount is 21 million coins, and halving is reached every 210,000 blocks. One block allows for 2,100 transactions. When an additional 21 halvings are reached after 2021, the blockchain reward will

converge to 0. It was designed. When the halving reward reaches the satoshi unit reward, Bitcoin will no longer be split by the halving.

80 years from now, Bitcoin halving rewards will no longer be implemented. However, since Bitcoin is designed to additionally compensate participants in the proof-of-work for the total transfer fee per block, an early version of the Bitcoin program was designed so that Bitcoin can be maintained even after the halving period ends.

Therefore, setting an appropriate fee that is appropriate for the times is very important for the continued maintenance of the Bitcoin network, and if the fee is lowered due to the application of SegWit, it should not be overlooked that it may make the continued maintenance of the original Bitcoin network impossible. According to data from Mempool.space, fee rewards are highly variable, ranging from 0 to 0.3 BTC. In some cases, a situation of zero rewards (no fee compensation) can occur.

Bitcoin's value and credibility are sustained because of the belief in its immutability. The belief that the total mining volume of 21 million is maintained, the belief that falsification through a distributed ledger is impossible using blockchain technology, and the confidence that the Bitcoin network is decentralized and there is no risk of it disappearing due to someone outside makes Bitcoin the most valuable asset on Earth.

If, in the future, any Bitcoin developer were to betray these fundamental principles—by issuing more than the total supply of 21 million BTC or altering Bitcoin’s existing rules under the guise of efficiency or innovation—Bitcoin's value could collapse in unforeseen ways.

Meanwhile, Bitcoin is already using a dual distributed ledger system that divides the existing unified distributed ledger into data and signature parts through the SegWit update.

It must be acknowledged that this represents a significant event, undermining the public’s belief that Bitcoin has successfully implemented the attributes of gold or diamonds in the digital form.

1. Sustainable without updates

Bitcoin Krypton is a project presented with the purpose of completely inheriting the electronic money system between individuals without the intervention of a trusted third party, which was the design purpose of Satoshi Nakamoto's Bitcoin.

Bitcoin Krypton was developed as a P2P electronic cash program that can continue to operate in the future without updates. However, the original version of Bitcoin Krypton was created by referencing, imitating, or modifying open source programs, and should not be completely trusted even though sufficient testing was conducted after completion of the program. This means that unknown bugs or errors may occur. Although performance can be improved, errors corrected, and upgraded through efficiency processes by arbitrary developers, the original version of Bitcoin Krypton' s program and the higher version program must be compatible.

2. Bitcoin halving and block cycle

Bitcoin has a total supply of 21 million coins and is designed to produce one block approximately every 10 minutes. A halving event occurs every 210,000 blocks, which equates to a period of about 4 years. Initially, the mining reward was set at 50 bitcoins per block. After 840,000 blocks and four halving events, the current mining reward is 3.125 bitcoins per block.

If the block period is set to the minimum necessary time between networks for broadcasting to prevent errors in node records for proof-of-work, several variables must be taken into consideration. Considering the allowable waiting time of the Internet, etc., the longer the time, the fewer errors. However, the minimum time for proof-of-work should not be shorter than 3 seconds. Bitcoin sets the verification time per block to 10 minutes, which reduces the possibility of errors, but the time to deliver assets is set so that it does not fit human life patterns. It is believed that the most comfortable time for humans is less than 1 minute per block rather than 10 minutes per block. Based on experience, it is clear that it will be

very convenient if Bitcoin's block cycle is less than 10 seconds. However, the block period does not need to be set to 1 second or less. One second is the minimum unit of time physically felt by humans and has been embodied in the human body for a long time. Blockchain with units smaller than a second is not a blockchain for humans, and operating it requires enormous operational costs. This occurs, making it impossible to achieve anonymity and decentralization of blockchain. Therefore, it is revealed that Bitcoin Krypton was designed to maintain blocks of 3 seconds and allow anyone to use the distributed ledger through an environment in which a full node can be sufficiently operated on a home computer. If the block cycle is about 3 seconds, I am confident that it will not feel slow or uncomfortable by human standards.

The four-year halving of block rewards is an obvious factor that provides motivation to maintain the Bitcoin blockchain, but it is also an adventure for those participating in proof-of-work. In order to participate in proof-of-work, one must first consider the profitability of the activity, so participants in the activity will not willingly participate in proof-of-work unless the profitability of participation is at least guaranteed. That would raise doubts about Bitcoin's future sustainability. Bitcoin's high fees are essential to ensure Bitcoin's future sustainability. It is the most important element of the system, which compensates participants in the proof-of-work by burning the total amount of Bitcoin transfer fees per block as presented in Satoshi Nakamoto's Bitcoin original source code, and rewarding participants in the proof-of-work by the amount burned.

Therefore, SegWit's goal of more transactions per block and lower transfer fees may first destroy the reliability of Bitcoin's single blockchain, and the low fees they propose may affect whether the Bitcoin blockchain can be maintained in the future. It raises doubts.

In order to resolve these doubts, ensure that Bitcoin Krypton is sustainable in the future, and motivate continued proof-of-work participation, various factors such as block cycle, half-life, and total reward were considered and applied to the program.

To this end, it was designed to be able to express up to 11 decimals (11 decimal places), and the transmission fee was lowered compared to the range of compensation, so that the fee was reduced by one-tenth every three half-lives.

This can be calculated up to 1000 times smaller than Bitcoin's 8 decimal places, but the efficiency of data per block has been increased by using Bitcoin's data type unit64.

(For reference, 1 Satoshi generates one additional unit of 1,000 Krypton.)

Bitcoin Krypton is tested quickly with a block cycle of 3 seconds from block 1 to 1,100,000 blocks. After block 1,100,001, the source code and program will be released, and the block cycle will be 63 seconds, lasting up to 2.1 million blocks. From the 1st block to the 2.1 million block, a reward of 5 coins will be given per block. Afterwards, the block cycle will be reduced by 3 seconds for every 2.1 million blocks, and in the 21st halving, the block cycle will be reduced to 3 seconds.

The total currency of Bitcoin Krypton is the same as 21 million individual Bitcoins, but Ethereum address rules

It was designed to be compatible with Ethereum's Dapps.

Bitcoin Krypton uses the existing Bitcoin method, Mempool, and does not introduce a competition method based on high fees, and plans to use the fee as much as the weight of data according to the actual usage used by each transaction, and 2.1 million blocks. It was designed to reduce the fee rate by 1/10 for every 6.3 million blocks, which is 3 multiples of It is limited to use, but is designed to increase by 100kb per block every 21 million blocks.

3. Data growth rate and decentralization of blockchain nodes

Bitcoin nodes use approximately 100GB of full node storage space every three years, and require 577GB of node storage space as of June 5, 2024.

On the other hand, the Ethereum mainnet has a full node storage space of 18.195TB as of June 5, 2024, and more than 5TB must be added to the node every year

The update of Ethereum 2 is named The Merge update in September 2022, meaning a transition from the existing proof-of-work (POW) method to the proof-of-stake method (POS), which will lead to a rapid change in the Ethereum network. Usage has increased

With the application of Ethereum's Denkun upgrade (EIP-4844, March 13, 2024), the Ethereum commission rate was reduced by up to 1/60, and on average by more than 75%. This will reduce the financial burden for more users due to the development and use of smart contracts and DAPPs through the Ethereum network. Accordingly, Ethereum's biggest problem is the increase in the node's physical hard disk due to usage, and the Verkle Tree upgrade, which is implemented to alleviate this to some extent, efficiently manages the disk space that stores staking data despite efforts to reduce its capacity, the absolute disk space used for data is expected to continue to increase.

It is anticipated that, over time, it will become increasingly challenging for Ethereum-related developers to operate full nodes directly, leading to an inevitable decrease in the number of nodes compared to the present. This highlights a structural issue within blockchain technology, wherein the system gradually shifts from a decentralized ledger to a more centralized one, contrary to its foundational principles as a distributed ledger.

Bitcoin Krypton's size per block starts at 100kb, and the storage space used by a full node gradually increases. The disk capacity expected to be used for one year is expected to be 30GB to 50GB, and it is designed so that there will be no problem even if block data increases by about 5% per year on average. This is compared to the price of storage devices being reduced by more than 10% per GB based on current technology, and maintenance costs were considered to ensure sustainability in the future.

4. Purpose of Bitcoin Krypton

The purpose of Bitcoin Krypton is to maintain an effective compensation system for future proof-of-work participants as a peer-to-peer financial program that pursues complete anonymity

without third party intervention, and to ensure that future improved versions are compatible with the original program that has already been released. It is done.

Even though 2024 Bitcoin Krypton was developed by a specific group and developer, after a certain period of time after the announcement, the duties of the initial developer and the initially designated Satoshikei will be terminated, and all rights will be transferred to a new Satoshikei, an anonymous replacement. Domain management, open source management, email management, and initial mining asset management are delegated, and the initial developer group is disbanded before December 31, 2024.

Not only is Bitcoin Krypton not guaranteed by the value of any asset, but there are also no plans for its future survival, listing, vision, or operation of a planned community.

The Bitcoin Krypton Network does not officially exist or belong to any individual or group. If anyone wants, it is possible to list Bitcoin Krypton, and anyone can use the name as they wish. However, you must not claim any rights when using it, and you must not use any official title or name. In order to satisfy the listing conditions, contents should not be arbitrarily written about official subjects, members, institutions, and communities that are required in the basic documents required by general exchanges.

The original developers of Bitcoin Krypton and those who played a role in its development do not bear any legal or economic responsibility for any consequences arising from Bitcoin Krypton in the future.

However, you can discuss new ideas, proposals, discussions on new developments, verification and certification of new source code, etc. through by emailing at satoshi.k@bitcoinkrypton.org. We cannot guarantee a reply, but as long as the message is friendly and polite and not abusive, spam, or fraudulent, any suggestions will be listened to and considered. In some cases, Bitcoin Krypton's compensation for voluntary listing on each exchange, etc. It can be discussed sufficiently.

5. Satoshi Nakamoto’s experiment on Bitcoin source code.

Bitcoin's original source code Bitcoin-V0.1 is based on the Bitcoin white paper (bitcoin.pdf (md5sum d56d71ecadf2137be09d8b1d35c6c042)) written by Satoshi Nakamoto on Saturday, November 1, 2008, and published at 14:27 on January 8, 2009. The official public version was released at :40 (EST), and the private version was released before that on November 16, 2008.

This version is not at Bitcoin's current source code public address (https://github.com/bitcoin/bitcoin),

But at a different public address (https://www.metzdowd.com/pipermail/cryptography/2009-January/ 014994.html)

Regarding SegWit, we conducted a direct experiment to refute the false claims about soft forking made by current developer groups.

First, as a result of compiling and executing the source code obtained from metzdowd.com, the latest nodes for broadcasting could not be found and it was impossible to sync with the nodes, so the experiment was meaningless. After execution, only the “Not Connected” error was reported. What we found out through various tests is that the broadcasting address for connecting multiple nodes does not currently work, and the IRC address for this no longer exists.

For some reason, Bitcoin's official GitHub account had 24.x as the oldest version, and the latest version was 27.x.

Next, the source code tested was bitcoinv0.3.

At block 124,276, node sync is no longer possible, and the output message is as follows.

```
ERROR: ConnectInputs() : fb0a1d8d34 VerifySignature failed
InvalidChainFound: invalid block=0000000000004939267f
height=124276  work=66138705631989025O8
```

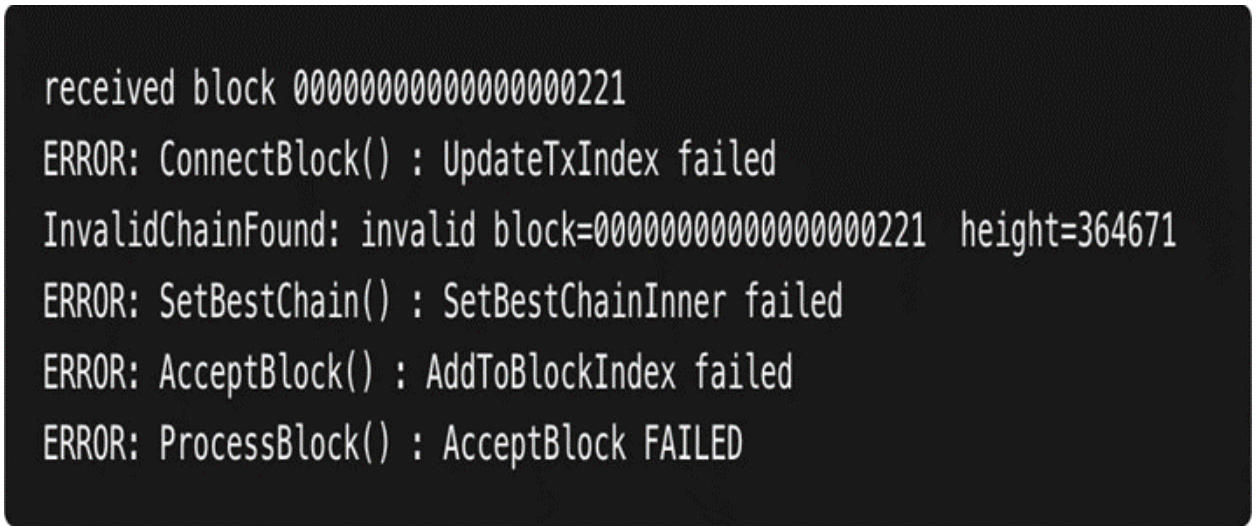
In V0.4 and v0.5, syncing is not possible at block 258,354, and the message below is displayed.

```
EXCEPTION: 11DbException
Db::put: Cannot allocate memory
bitcoin in ProcessMessage()

ProcessMessage(block, 901212 bytes) FAILED
received block 0000000000000023e872
REORGANIZE
```

The V0.6 version can no longer sync at block 364,670, and the message below is output.

```
EXCEPTION: 11DbException
Db::put: Cannot allocate memory
bitcoin in ProcessMessages()

ProcessMessage(block, 999787 bytes) FAILED
received block 00000000000000001d3
```

The V0.7 version can no longer sync from block 364,671, and the message below is output.



The cause of all errors is believed to be the same. By dividing the block into data and signature parts, it can be suspected that the latest nodes applying SegWit and past nodes are conflicting due to various unknown causes. In other words, it has become evident that soft forking had effectively broken the premise of compatibility between past and present programs.

6. Krypton

Krypton is a chemical element with symbol Kr and atomic number 36. It is a colorless, odorless, and tasteless inert gas that exists in trace amounts in the atmosphere and is obtained by fractional distillation of liquid air. It was first discovered by William Ramsay in England in 1898. Ramsey, who discovered helium and argon, began looking for noble gases with atomic weights between 4 and 40. 1898. They distilled a small amount of liquid air through red-hot copper and magnesium and discovered a new green element. Because this green element was more difficult to discover than other noble gases, it was given the name 'krypton', which means 'hidden thing' in Greek.

Unlike helium, which is an inert gas, it has a property that changes the molecules of high-energy substances to a slower moving speed. When krypton gas is inhaled, it produces a voice with a low-pitched sound wave, as opposed to inhaling helium gas.

When you watch the movie Superman, Kryptonite, an imaginary substance, is used as Superman's weakness. This is an imaginary substance named after Krypton.

Bitcoin Krypton advocates CPU-based mining in the sense of weakening abnormal approaches such as ASIC chips in mining (proof of work), and introduced a web-based one-click mining method so that anyone can easily participate in proof of work.

In addition, the Satoshi (8 decimal places) digits, the minimum unit of the original Bitcoin program, were further subdivided and expanded to Krypton (11 decimal places) digits. In other words, 1kr (Krypton) is 0.00000000001BTCK, and 1,000kr is 1 satoshi. In other words, 1BTCK can be expressed as 100 million satoshi or 100 billion Krypton.

Bitcoin Krypton went through 21 halvings and 7 fee cuts, requiring fees below Satoshi, and to run this smoothly, a unit called Krypton was introduced into the Bitcoin network.

If the data type of Bitcoin Krypton's executable program is set to unit64, calculations can be made up to a total currency volume of up to 21 million and up to 11 decimal places. Accordingly, the block size can be reduced more effectively than using the unit128 data type.

7. The Path to True Decentralization.

Bitcoin Krypton’s ultimate vision is achieving complete decentralization. This goal entails the eventual dissolution of any centralized entity managing the network, marking the final stage of true decentralization.

The subject is the fate of Bitcoin Krypton, and the process of proving that Bitcoin Krypton is different. Bitcoin Krypton's node starts from the connection and exploration of the Seed node in the source code. The connection of the Seed node is the process of connecting the Bitcoin

Krypton worldview like a spider web, and the Seed node must be continuously added and updated, which affects the vitality of Bitcoin Krypton.

In order to give it vitality, a special procedure was designed for Bitcoin Krypton as a procedure to spread it widely like a virus. Since any node can be a Seed Node, the initial Seed Node was designed to spread by providing a special reward to the information provider who provides information about the node.

The method of providing compensation is to quantify the status of the Seed Node provided as information, that is, the server's maintenance ability, and then provide compensation differentially every month based on the score.

Once a sufficient number of Seed Nodes is established, the Bitcoin Krypton network will achieve a stable decentralized architecture. At this point, the network is expected to self-sustain, maintaining its robustness and decentralized nature through the widespread distribution of Seed Nodes.

BITCOIN KRYPTON

https://bitcoinkrypton.org