BTCU
ULTIMATUM

White Paper of Bitcoin Ultimatum

Introduction

BTCU ULTIMATUM

Introduction

The cryptocurrency market is inextricably tied to the blockchain – its fundamental and underlying technology. The modern market is brimming with an abundance of blockchain protocols, algorithms, and concepts, all of which have fostered the development of a wide variety of services and applications.

The modern blockchain market offers users an alternative to both established financial systems and ecosystems/infrastructures of applications and services. The decentralized nature of blockchain allows it to better protect user data and offers other advantages, such as comparatively higher transaction speeds and lower commissions for international monetary transfers.

The abundance of decentralized applications, Dapps, grants users alternatives in a variety of industries, such as gaming, gambling, marketplace buildup, marketing campaign launches, advertising placement, and much more.

The total market of cryptocurrencies is projected to reach $1.40 trillion by 2024, with a CAGR of 6.18% over the forecasted period. Cryptocurrencies are considered to be a disruptive concept and a viable alternative to the fiat currencies used in the modern monetary systems of the world economy. Entrepreneurs, startups, as well as large, as well as small and medium-sized enterprises are interested in using cryptocurrencies and blockchain technologies and are considering them as a revolutionary concept for countering transactional compliance and fraud and avoiding high transaction fees.

Blockchain technologies are being considered as a highly valued and cost-optimizing alternative to modern enterprise management systems as well. The inherent characteristics of blockchain technologies allow them to be used for massive data storage in immutable fashions and allow all parties to a transaction to have fully transparent access to the information stored within the block of chains. In addition, non-sanctioned access to any information is impossible, making tampering with corporate and personal data an impossible undertaking.

Bitcoin still holds the largest share of the cryptocurrency market, with its share being 38.76% in 2017 and almost 64% in early 2020. The Bitcoin market is likely to reach $558.2 billion by 2024, increasing by an average of 4.23% during 2019–2024.

Introduction

However, the problem of scalability of the Bitcoin network is associated with the initial limitation set by the developers of one megabyte in size for the block – the basic structure for storing data in the blockchain. This restriction is dictated by the peculiarity of building a blockchain as a fully replicated distributed database, which requires constant transfers between all the participants of each new element. Reducing the block size significantly limits the effectiveness of a potential DDoS attack.

With the popularity of Bitcoin, the number of transactions increased, but due to the limitations of the maximum block size, not all transactions were placed immediately, and a queue periodically occurred.

In the Bitcoin network, a user can voluntarily set a commission to speed up processing. The regular occurrence of a queue led to an increase in transaction fees, but did not eliminate the delay in processing transactions. This makes the use of Bitcoins quite expensive and time consuming, especially for small payments.

Thanks to the growth of decentralized applications, the cryptocurrency market is likely to grow on the wave of popularity of alternative payment systems. This popularity is forecasted to allow the market to grow at its highest rate during the forecast period

According to forecasts, by 2024 the market for trading applications will be estimated at 837.2 billion US dollars, increasing by an average of 4.70% during 2019-2024. The payment market is expected to grow with the highest CAGR of 12.47% from 2019 to 2024. Payments through the use of cryptocurrencies have a number of advantages, such as increased transaction security, fraud protection, decentralized system governance, low fees, and protection against chargebacks from consumers, and fast international transfer speeds, thereby increasing the adoption of cryptocurrencies as alternatives to traditional fiat currencies.

According to forecasts, by 2024 the highest growth rates will be in the Asia-Pacific market, which will be valued at 705.4 billion US dollars, and its growth will be 3.52% on average from 2019 to 2024. This is due to the low cost of electricity in China and the early introduction of cryptocurrencies in Japan on the level of local payments.

BTCU
ULTIMATUM

Problematic of the Blockchain industry

btcu.io

BTCU ULTIMATUM

Problematic of the Blockchain industry

Blockchain technologies are advanced and gaining popularity as a solution in large structures, however, considering each of the types in particular, you can notice several problems that can be critical when using them. Let's take a look at the main ones.

Transactions Anonymity

Recently, control over cryptocurrencies has been strengthened. On January 10, 2020, the Fifth Money Laundering Directive (5AMLD), which was adopted by the EU in May 2018, came into force. The directive contains requirements for mandatory verification of all clients of cryptocurrency platforms in accordance with the KYC and AML standards, according to which all users making transactions with cryptocurrencies must pass verification.

With the development of modern technologies and the heightened interest of society to blockchain technologies in particular, anonymity on a blockchain network becomes dubious. The Blockchain Info resource allows to fully decode the transaction chain from the moment the coin was generated to the account on which it is currently located. The reason is the very structure of the blockchain, which is open. Therefore, the point of no return can be called the moment when the users explicitly indicate their personal data and associate them with a specific wallet.

The lack of “anonymous transfers” calls into question the main principle of blockchain as a technology, which the creator of the first blockchain network, Satoshi Nakomoto, bequeathed upon us – anonymity.

Lack of anonymity when making payments can hurt your business. When using fiat money, only the tax office can access the company's financial statements. On the blockchain, data will be available to all users, including competitors and attackers.

Bitcoin users can be de-anonymized after re-using the address or passing verification on the exchange. In the case of anonymous cryptocurrencies, such a situation is impossible. They use cryptographic protocols that make it difficult to audit network data. The address of an anonymous cryptocurrency wallet can only be disclosed by its owner.

Insufficient Development of Key Aspects of the Technology

The main reason for scaling the application of blockchain technology is the inability of individual blockchains to interact with each other, for example, to carry out transactions between the Bitcoin and Ethereum networks, is extremely limited - mainly because different blockchains use different protocols, algorithms and security procedures. Various companies use the same blockchain protocol to solve their problems, and cannot apply the same solutions to other problems, which is the reason for refusing to use blockchain technology in separate processes. The development of the possibility of interaction of various blockchain protocols will provide an opportunity for the mass implementation of this technology in business and social processes.

The smart contracts are the basic constituents of the blockchain, which allow users to create decentralized applications. Atomic swaps can be implemented natively in blockchain protocols to speed up transactions, and it is necessary to develop smart contract technologies to give people more solutions. The effective development of customizable smart contract templates and the expansion of their functionality is the key to the implementation of the blockchain in business processes, without which the technology itself cannot develop.

Centralization

It's nice to think that nobody controls the blockchain, i.e. network participants (miners) act as a decentralized community that serves the blockchain and chooses the direction of its further development. In fact, things are much worse.

In the case of popular cryptocurrencies using classic mining protocols, the hardware requirements are high even for simple blockchain verification. However, even if you have modern equipment that can quickly process blocks, your network channel may not be wide enough to quickly synchronize with the network. This leads to a situation where only companies with a large number of high-performance miners can effectively create new blocks (as is the case with the PoW algorithm), which leads to the centralization of mining. Cryptocurrencies were conceived as open systems that continue to function correctly as long as the majority of their users are honest, but at the moment most of the computing power is concentrated in a small number of miners who can easily agree on a 51 percent attack. Mining pools make the situation worse - for example, in the case of Bitcoin, only five pools control more than 50% of the hash rate.

Centralization

Proof-of-Stake is generally seen as less demanding on hardware, however, processing a really popular blockchain will still require a wide network bandwidth to synchronize with the network. In addition, the profit for holders of full nodes in PoS is usually small and only a small percentage of coins are mined, making the network vulnerable. This is often eliminated by delegating mining authority to someone else, but this also leads to a decrease in the number of full nodes in the network and, as a consequence, to its centralization.

New consensus algorithms are needed to solve this problem and return decentralization as the founding principle of blockchains.

Mining pools and commission manipulation

The consensus algorithm is one of the main parameters of a blockchain system along with hash functions, block size, and network bandwidth. In computer science, a consensus algorithm refers to a method by which distributed nodes in a network agree on an item of data. PoW and PoS algorithms leave room for monopolies. Participants with more computing power in PoW and participants with a larger supply of PoS tokens receive more profit and power over systems. Mining is reduced to a series of calculations with an enumeration of parameters to find a hash with given properties. Miners provide their computing power, and the network pays them to create each block.

The mechanism of commissions in Bitcoin is necessary to pay for distributed network services, where the network service, in fact, is reliable data storage. Bitcoin users actually pay for every byte of data added to the shared database. Due to the limited bandwidth of this database, users compete for write priority. When forming transactions, users set a commission in the form of a certain amount of satoshi per one byte of data. In this case, each validator node queues all unconfirmed transactions in such a way that first it confirms transactions that pay a large commission per unit of their weight. It is obvious that those transactions that end up at the end of the queue can remain unconfirmed for a long time. The consequences of a sharp increase in the flow of new transactions is the emergence of a large queue of transactions waiting to be written to the blockchain.

Mining pools and commission manipulation

Usually, the miner follows the standard scheme and sorts transactions based on the cost of writing 1 byte of data to the blockchain. It seems like everyone is doing it now. However, it is possible that the miner may have better motivation. He can independently from the policy of monetizing his activity. In other words, he can act in a non-standard way with respect to the transactions that he will write to his block. If there are more favorable terms than just taking a commission on your transaction, he will most likely change his policy. This approach assumes that users will pay the miner to confirm their transactions not through a predetermined commission, but directly (according to their own scheme). In practice, any sufficiently large mining pool can conduct its own campaign in order to increase profitability and use simple mechanisms for this. One of the main barriers to the broad implementation and application of blockchain technologies is the use of established and highly inefficient mining protocols relying on cumbersome and power-intensive equipment.

Avoiding the use of large quantities of electric power is one of the main prerequisites for popularizing the use of blockchain and making them accessible to a large base of users both on the private and corporate levels. Apart from the environmental factors resulting from the intensive operation of large mining farms, there are hardware issues involved as well. The mining equipment is used for validating transactions and mining blocks quickly becomes obsolete due to the constant updates being introduced in the various networks of blockchains. The use of ASICS cards makes them useless after their year-long lifetime expires, thus creating vast amounts of waste, both material and monetary for the world and their operators.

Decrease in Transaction Speeds

The speed of transactions that blockchain is hailed for is actually a point of doubt, considering that the number of network transactions grows daily, while the supporting infrastructure is lagging behind. This leads to the problem of scalability, which results in delays in transaction speeds that can last for as much as days in some cases, when the network is overloaded with traffic.

The bottlenecks that arise on the network in peak load times, such as during high market volatility, result in higher transaction fees and decrease the reputation of the blockchain as a viable alternative to Visa and MasterCard. Low transaction speeds and excessive delays plague networks with blockchains around the world, hindering the broad practical implementation of the technology by companies and for consumers.

Blockchain technology is largely associated with the trustful exchange of assets in everyday life, which means that it must be widely accepted in order to truly reach its full potential. However, in order to do this, the technology must be better than the available options in every way.

While blockchains have offered the market new ways of sharing value without intermediaries, they have not been able to surpass traditional scalability. In fact, most blockchain solutions available today have low transaction rates and high transaction fees.

Delays refer to the time that users need to wait until their transaction is processed. When using publicly distributed decentralized ledgers, there are a large number of nodes that need to reach consensus to confirm the transaction. In order to process the transaction so as to reach consensus, each node needs access to the entire chain of blocks. This creates a huge database over time. Giving access to the entire blockchain to hundreds of nodes also increases the security risks involved.

BTCU
ULTIMATUM

BTCU main solutions and concepts

btcu.io

BTCU ULTIMATUM

BTCU main solutions and concepts

The possible solutions to the main problems facing the modern blockchain and cryptocurrencies market can be solved through a complex approach that can be offered by the proper infrastructure for catering to the needs of market participants and anticipating any future trends.
The solution offered by the BTCU team involves the creation of a new mining algorithm, the UPoS (Ultimatum PoS), that would usher in the development of a new blockchain matrix capable of resolving the long-standing issues of the market.

Consensus algorithm basis

BTCU will be based on LPoS mining algorithm combined with PoA, where LPoS will work for users to mine, and PoA to validate transactions. PoA-algorithm of transaction confirmation will allow realizing the throughput of the blockchain at the level of 200 transactions per second, with the ability to scale up to 10,000 tps.

Leasing and Staking

The BTCU project team advocates avoiding classical mining for unloading the network, and also opposes the use of electricity on a massive scale for mining the cryptocurrency. The given approach is based on the fact that the crypto community has become more mature and is developing, changing its point of view in favor of preserving the environment and using more humane mining protocols.

The LPoS algorithm creates a voting system that directly depends on the reputation of the validators. If the selected node does not work correctly or works inefficiently, it will be quickly deleted and replaced by another. Therefore, the validators are motivated to act honestly and effectively, so that they are further voted for with their own steak.

The main advantages of LPoS are a democratic form of control, scalability and relatively low energy costs for network maintenance. LPoS validators use their processing power directly to process transactions. LPoS allows consensus on new blocks faster than PoW and PoS, as LPoS consensus implies the simplest mechanisms for creating blocks on relatively inexpensive equipment and with a high degree of honesty. In practice, in a LPoS system, a relatively small number of network nodes must agree with the validity of the block so that all transactions in it can be considered to be included in the main chain.

Projects tokenization and DeFi

The integration of EVM (Ethereum virtual machine) technology into the BTCU network, which will allow the implementation of smart contracts on the well-known Solidity provides huge opportunities for tokenization projects or the implementation of DeFi. Given the flexibility and scale, the Ethereum platform is the leader for the DeFi application, but that doesn't mean it's the only blockchain platform. High fees, problems with technical support of nodes, the oversupply of contracts, and network centralization, which is one of the most terrible threats to modern projects make them look for new solutions, one of which is BTCU.

DeFi is short for Decentralized Finance. Decentralized Finance includes digital assets, protocols, smart contracts, and dApps built on a blockchain.
Think of DeFi as an open financial ecosystem where you can build various small financial tools and services in a decentralized manner. Since these are applications built on a particular blockchain, they can be combined, modified, and integrated according to your needs.

Decentralized network, private transactions, leasing, transaction speed and low fees open up new possibilities for implementing smart contracts to tokenize your projects or make a DeFi, which are based on the same technology as Ethereum. This will not only allow you to easily continue to implement your projects on BTCU, but also easily transfer the already implemented ones.

Transactions Privacy

The Bitcoin payment network offers a highly decentralized mechanism for creating and transferring electronic cash around the world. Unfortunately, Bitcoin suffers from a major limitation: since transactions are stored in a public ledger it may be possible to trace the history of any given payment — even years after the fact. The Bitcoin ledger is public, any party can recover this information and data mine to identify users and patterns in the transactions. In other words: Bitcoin transactions are conducted in public.

The most common solution to this problem is to use Bitcoin laundries – services that mix together many users' bitcoins in order to obfuscate the transaction history. Laundries suffer from a number of potential drawbacks, however, as they must be trusted to return coins. Moreover, a compromised or malicious laundry offers no anonymity.

Transactions Privacy

So, how can we solve the problem? Answer BTCU is simple - Zerocoin protocol. Technology allows direct anonymous payments between parties. Private transactions exist alongside the non-anonymous. Each user can convert non-anonymous BTCU into anonymous coins, which we call zBtcu. Users can then send it to other users, and split or merge zerocoins they own in any way that preserves the total value. Users can also convert private coins back into BTCU, though in principle this is not necessary: all transactions can be made in terms of privacy.

Based on Zerocash protocol, this is a privacy-protecting, digital currency built on strong science. Transact efficiently and safely with low fees while ensuring digital transactions remain private. Selectively share address and transaction information for auditing or regulatory compliance.

Atomic Swaps

In the future, the development team plans to implement the possibility of integrating atomic swaps into the BTC Ultimate blockchain to enable the implementation of smart contracts not only on the BTCU blockchain network, but also with other popular blockchains.

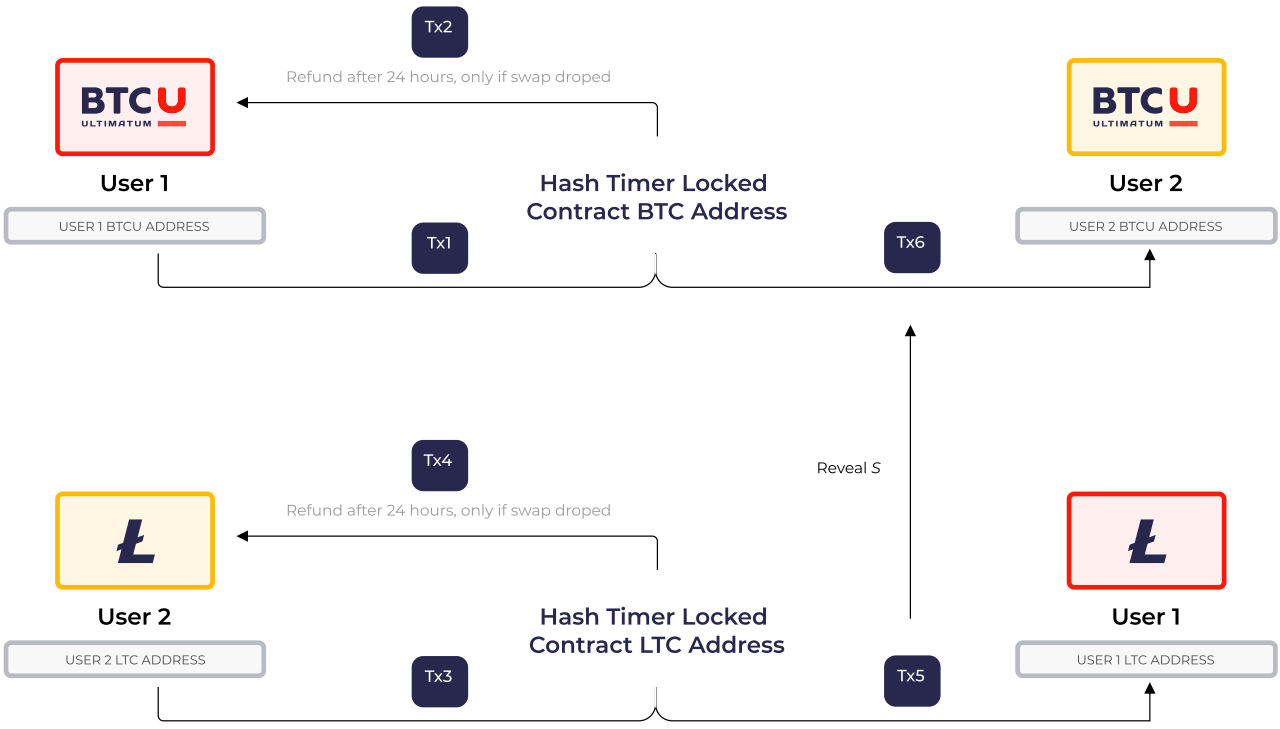
Atomic swaps are a method that provides the ability to quickly exchange cryptocurrencies working on different blockchains. This process, also known as atomic cross-chain trading, is based on smart contracts and allows users to trade coins directly from their wallets.

Atomic swaps can occur in two different ways: on-chain and off-chain. On-chain swaps occur in any of the available networks with support for HTLC and the same hashing algorithm. Off-chain swaps take place on the secondary layer. This type of swap is usually based on bidirectional payment channels similar to those used by the Lightning Network.

Our technology already accepted the next hash algorithm which converted by the on-chain way: **CRC-16, CRC-32, MD2, MD4, MD5 ,SHA1, SHA224 ,SHA256, SHA384, SHA512, SHA512/224, SHA512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512, Keccak-224 Keccak-256, Keccak-384, Keccak-512, Shake-128, Shake-256.**

One of the best features of cross swaps is the lack of need for intermediary tokens. Meaning that if a user has LTC and wants to buy BTCU, under current exchange options, the user will have to sell their LTC for BTC and then buy BTCU. When using atomic swaps, users can conduct such trade directly without any intermediary services. Pic 1 shows the principle of the atomic swap transaction.

Atomic Swap Transaction Roadway



Pic 1. Atomic Swap transaction roadway from User 1 to User 2

Atomic swaps have the potential of completely revolutionizing the money transfers system and shifting it into the crypto arena. Atomic swaps will enable people to directly trade with one another on a wallet-to-wallet basis. As we have stated earlier, can either be conducted on-chain or off-chain.

The most basic advantages of atomic swaps are related to the decentralized nature of the function, which is the elimination of the need for a centralized exchange or any other form of intermediary. Cross-chain cryptocurrency exchanges can be carried out between two or more parties without the need to trust each other. The security level of swaps is also much higher, since users do not need to transfer their funds to a centralized exchange or a third party. Instead, transactions can occur directly between two user wallets. The main advantages offered by BTCU Atomic Swaps are the following:

- Interoperability between different assets is a major problem with cryptocurrencies. Atomic swaps will allow users from different networks to interact freely on a peer-to-peer basis.
- Atomic swaps will enable trustless and fee-free decentralized exchanges.
- Centralized exchanges are also suspected of internal maintenance issues and corruption. Wallet maintenance or disabled withdrawals are big problems. Atomic swaps give users full control of their funds
- Since atomic swaps directly connect two wallets, they cancel all the steps and confirmations required by centralized exchanges.
- Atomic swaps make the crypto ecosystem more “currency agnostic”, because people with different crypto assets will be able to interact with each other on equal grounds as in the fiat world.
- Centralized exchanges are open to a host of attacks. Atomic swaps remove the need for having a third party and make trading direct.
- Direct wallet-to-wallet trading epitomizes decentralization in its purest form. Exchanges are constantly targeted for regulation purposes, which makes the trading process increasingly centralized.

BTCU
ULTIMATUM

Executive Summary

btcu.io

BTCU ULTIMATUM

Executive Summary

Our team is setting the task of not only developing an innovative solution that would meet all the requirements of the crypto community, but also setting up and constantly improving its product in order to expand its capabilities, and maintain its relevance depending on the needs of the market. The team is also determined to attract developers from around the world to develop the network and expand the underlying infrastructure to include international crypto organizations and companies.

The BTCU blockchain will be based on the LPoS mining protocol improved by network decentralization. At the start, the network will be based on 10 validators, and will scale up later depending on the network load and the number of masternodes. At the same time, in order to avoid the centralization of the network, the first 10 validators will be determined by the team itself. The first validators will be authoritative blockchain organizations and leading crypto exchanges that will support the fork and its distribution. The entities will also be acting as advisers on issues related to the technology that will regulate its distribution and development. The rest validators will be determined by the community on the basis of the PoS principle, as they will be determined by the largest coin holders who will receive coins for voting for the validators or will be able to act as validators and administrators of master nodes.

The development of the proprietary UPoS (Ultimatum PoS) mining algorithm will be able to resolve many of the issues associated with modern blockchains and offer the market higher transaction speeds, low and invariable commissions, and full decentralization with anonymity as a right of users.

BTCU
ULTIMATUM

Bitcoin Ultimatum Architecture

btcu.io

Bitcoin Ultimatum Architecture

The architecture of Bitcoin Ultimatum is based on combining the best directions of blockchain technologies and achieving their optimal symbiosis. Leasing, smart contracts, private transactions and other leading blockchain solutions integrated together into a decentralized consensus UPoS algorithm form a stable and wide network for the entire blockchain community.

Network working principle

Node is a computing device as a connection point with the BTCU network, which can perform various functions, the main one of which is the transfer of transactions to the BTCU network. The main types of transactions are: “Send BTCU” “Staking deposit BTCU” “Staking withdrawal BTCU” “Leasing deposit BTCU” “Leasing withdrawal BTCU”.

Main Transaction Types

Transaction is a signed data section (transaction signature) that is transmitted to the BTCU network and collected in a block performing an operation with an address balance.

A transaction is a section of data confirmed by a special signature (hash), which is transmitted to the BTCU network. The transaction enters the block after the corresponding changes on the balance of the recipient's address. The Validators are responsible for adding a transaction to the block.

- Transactions on the BTCU network can be “private” and “public”.
- Private transactions are associated only with the transfer of coins between addresses.
- Public transactions involve coin transfers, voting, staking, or leasing.

Public transactions

Each user of the BTCU network can perform operations related to the transfer of coins, voting, staking, or leasing.

- The user needs to sign the transaction with their private key.
- The Validator receives a list of such transactions generated on the network for a certain period of time, checks their validity and adds them to the block.

Private transactions

Each user of the BTCU network can transfer or receive a private transfer of BTCU coins by transferring them from one public address of the network to another.

- The user who sends the coins must indicate the recipient's public address and sign the transactions with their private key.
- Such transactions are not displayed in the public network and are stored and processed by the Masternodes and are confirmed by the Validators.

Master-node is a complete node that supports the operation of the network by performing computing operations and storing network data in order to provide the current blockchain and network information in real time.

Validator - the backbone of the network that generates blocks, validates and adds them to the blockchain of the public BTCU blockchain.

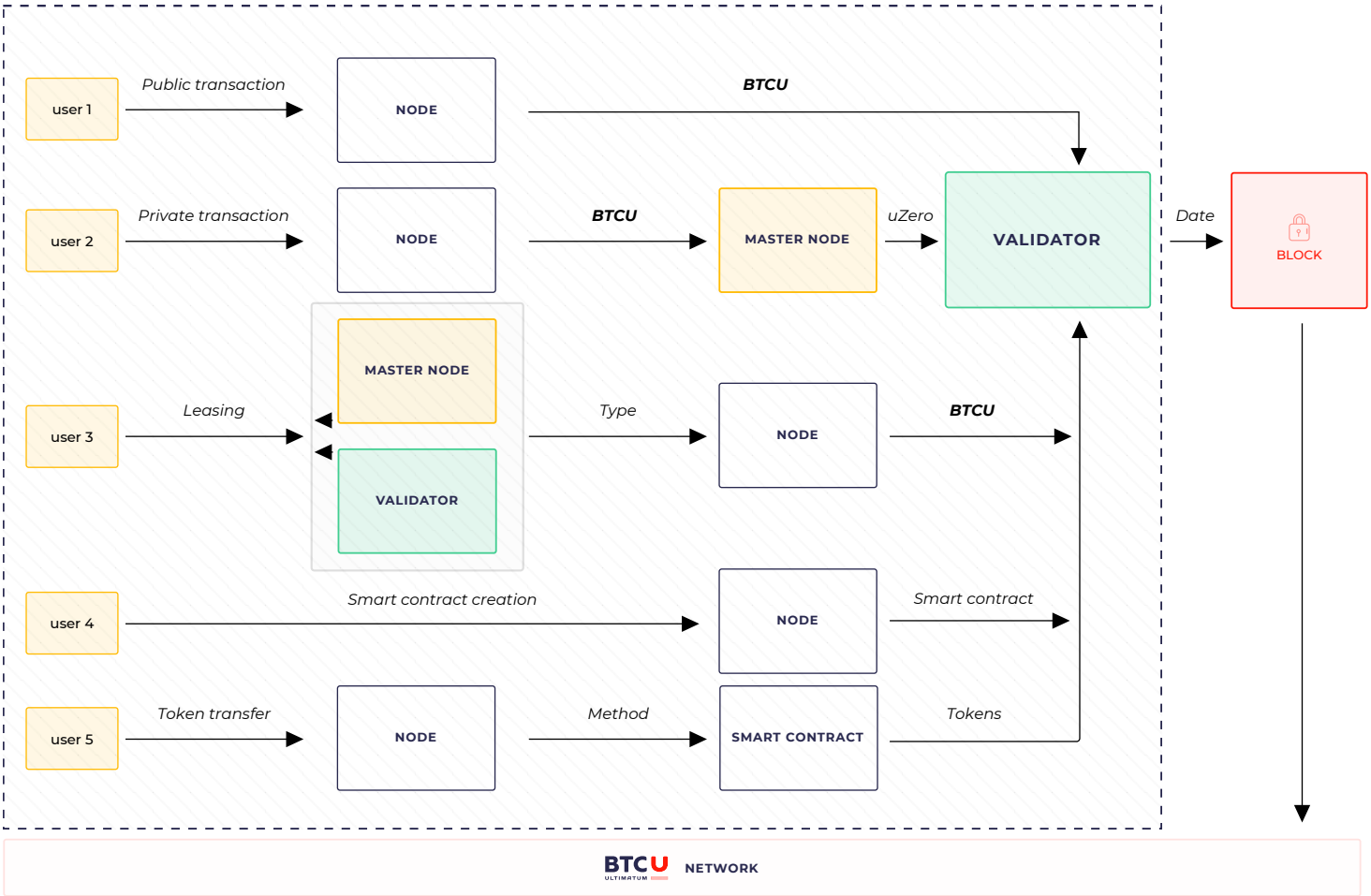
The Masternode status gives the node the ability to lease coins from users, which increases the speed and security of the network. For this, the node needs to perform Staking in the amount of 100 BTCU coins and keep at least 1000 BTCU coins in lease.

To obtain the “Validator” status, the node must perform Staking in the amount of 1,000 BTCU coins and keep at least 10000 BTCU coins in lease.

Masternode Network

The BTCU network is two-tiered. The network is composed of the first staking tier, which all BTCU holders can participate in through staking their coins. The second is the more exclusive masternode tier. Masternodes are a set of incentivized nodes on a network within the BTCU network responsible for the handling of particular specialized tasks. The functions carried out by BTCU masternodes are fundamentally similar, however, to those of other PoS coins. As such, these nodes are an integral part of the BTCU digital ecosystem, and necessary to network functionality.

The Masternode network fulfills a range of functions independent of staking nodes. These distinct functions are limited to Masternodes, and cannot be completed by a standard staking node. These responsibilities are distributed across the Masternode network, and no Masternode has power or authority in excess of others in the network.



Pic 2 - The scheme of interaction between the network and its participants

How to become a validator or masternode in BTCU

The validator and masternode perform one of the key functions in the network and the behavior of each of them affects the stability of the network. The highest rank and responsibility rests with Validators - the nodes that are responsible for generating blocks and validating it on the network. Masternodes' purpose is slightly smaller, but still important. The main purpose is to maintain the stability of the network to give users the opportunity to earn leasing profit. Each masternode with a lot of community support and completed minimum requirements has the ability to become a validator. Let's take a closer look at what is needed to become a validator or masternode.

Masternode

To become a Masternode, you must fulfill the following conditions:

- make staking in the amount of 100 BTCU or more.

After that, upon reaching 30 confirmation from the moment of staking, the node goes into the Masternode status.

Validator

The procedure for becoming a Validator is a little more complicated and contains the following conditions:

- raise your personal node (in the status of a Masternode);
- have 10,000 BTCU or more in a lease for Masternode;
- make staking in the amount of 1000 BTCU or more;
- receive confirmation from all validators in the network upon request to become a validator.

A vote is a set of transactions, each of which contains a response to a Masternode request to vote (True / False). The first 10 network validators will be selected among the major projects of the blockchain industry, which will mark the beginning of the Bitcoin Ultimatum decentralized network.

If the required number of positive votes is not collected (equal to the number of validators at the time of voting), then the request will be rejected, but the Masternode can make a repeated request. The number of Validators is limited in the network and depends on the network load or the height of its block.

BTCU ULTIMATUM

Network Scaling Principle

Network scaling is one of the main directions of the coin, since this factor directly affects the network load. The logic of increasing the number of network validators directly depends on the following criteria:

- Network load (users and transactions quantity)
- Number of masternodes and nodes

The table shows the predicted increase of validators number in the network depending on the block height or on the number of masternodes in the network.

Stage	Block height / Number of Masternodes	Number of Validators
Launch	Launch	10
1	From 250 000 block or 10 Masternodes	12
2	From 500 000 block or 50 Masternodes	14
3	From 750 000 block or 75 Masternodes	16
4	From 1 000 000 block or 100 Masternodes	18
5	From 1 250 000 block or 125 Masternodes	20
6	From 1 500 000 block or 150 Masternodes	22
7	From 1 750 000 block or 175 Masternodes	24
8	From 2 000 000 block or 200 Masternodes	26
9	From 2 250 000 block or 225 Masternodes	28
10	From 2 500 000 block or 250 Masternodes	30
11	From 2 750 000 block or 275 Masternodes	32
12	From 3 000 000 block or 300 Masternodes	34
13	From 3 250 000 block or 325 Masternodes	36
14	From 3 500 000 block or 350 Masternodes	38
15	From 3 750 000 block or 375 Masternode	40
16	From 4 000 000 block or 400 Masternodes	42
17	From 4 250 000 block or 425 Masternodes	44
18	From 4 500 000 block or 450 Masternodes	46
19	From 4 750 000 block or 475 Masternodes	48
20	From 5 000 000 block or 500 Masternodes	50

Masternodes and Validators Ranking System

The rating formula determines the level of confidence users to node in the network. The indicator is based on the volume of leasing, the number of users in leasing and the stability indicator of the masternode in the network. Each of the factors shows not only the current state of the main nodes, but also their past state, which demonstrates growth and trust over the entire time of nodes in the network.

Rank of main nodes leasing value:

$$V_m = K_1 \times \left(\frac{Current\ volume\ of\ leasing}{Total\ volume\ of\ leasing}\right)^2 \times \sqrt[4]{Current\ volume\ of\ leasing} \quad (4.1)$$

$K_1 = 0,25$ - rank of main nodes leasing value coefficient.

Rank of leasing users quantity:

$$U_m = K_2 \times \left(\frac{Current\ quantity\ of\ users\ in\ leasing}{Total\ quantity\ of\ users\ in\ leasing}\right)^2 \times \sqrt[4]{Current\ quantity\ of\ users\ in\ leasing} \quad (4.2)$$

$K_2 = 0,65$ - Rank of leasing users quantity coefficient.

Rank of successful blocks in the network value:

$$B_m = K_3 \times \left(\frac{Successful\ blocks\ of\ main\ node}{Total\ \ blocks\ of\ node\ in\ the\ network}\right)^2 \times \sqrt[4]{Successful\ blocks\ of\ main\ node} \quad (4.3)$$

$K_3 = 0,1$ - Rank of successful blocks in the network value coefficient.

Total rank of main nodes:

$$R_m = V_m \times U_m \times B_m \quad (4.4)$$

R_m - is a final indicator of main nodes rank in the network.

Smart Contracts

Each network user can create a smart contract by implementing it according to EVM (Ethereum Virtual Machine) standards. A special programming language called Solidity is used for this purpose to create smart contracts in the BTCU network.

To create a smart contract, users must specify the conditions for its functioning and methods of interaction with the network.

To add a smart contract to the network, the user needs to complete the transaction of adding the contract to the network and pay a commission not lower than the minimum. To conduct transactions within a smart contract (transfer of tokens), the user needs to specify the recipient's public address and sign the transactions with his private key.

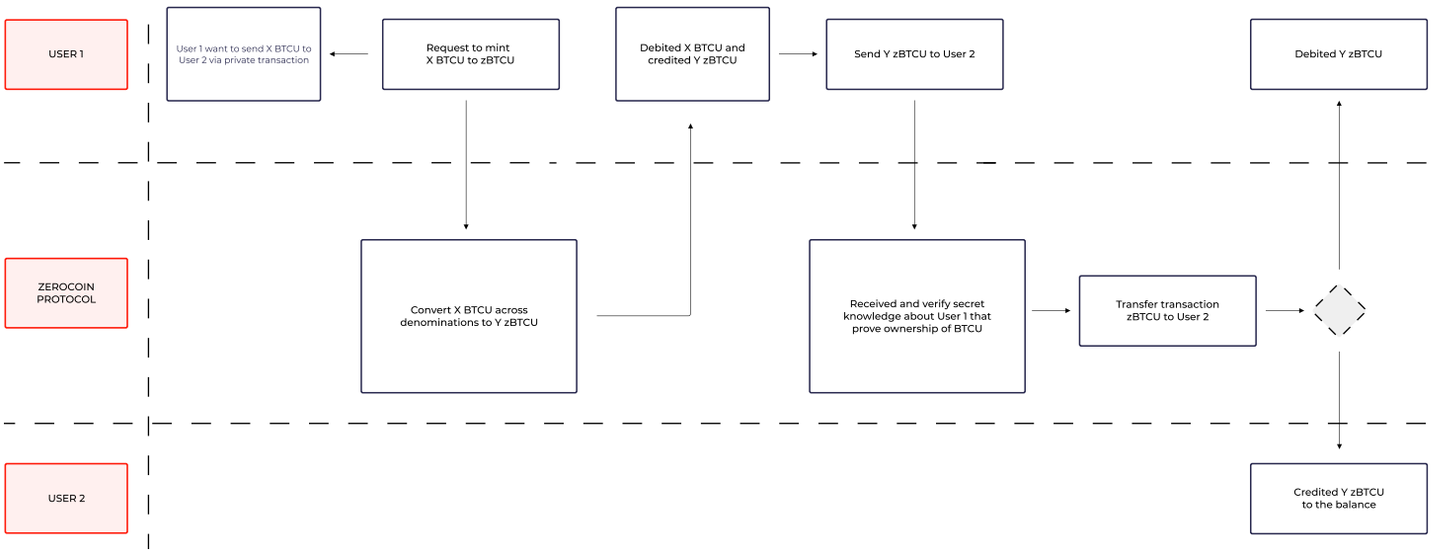
The user pays a commission for conducting transactions within a smart contract.

Anonymization principle

Anonymization of transactions is implemented through the integration of the Zerocoin protocol, which provides huge benefits for users such as:

- Zerocoin working without relying on a central coin issuer or bank (as used in previous e-cash schemes). Moreover, since no single trusted party operates the Zerocoin system, attacks on it must take on a substantial fraction of the whole network.
- Other anonymous cash systems rely on distributing the work of anonymizing users amongst a set of parties. This approach works well if all parties are fully available but can be subject to “denial of service” attacks where a small number of nodes are taken offline. Because Zerocoin is built on top of Bitcoin, it is widely distributed among all the Bitcoin peers, ensuring that the system can remain available even when many nodes are compromised.
- This protocol uses provably secure cryptographic techniques to ensure that Bitcoins cannot be traced. These techniques allow users to conduct transactions on the BTCU network while receiving strong mathematical guarantees that the transactions cannot be traced. These guarantees remain in place even if a portion of the network is compromised by an attacker.
- With this protocol users can make direct payments to each other with a vastly more efficient cryptographic protocol that also hides the amount of the payment, not just its origin.

The scheme shows the way of coins which were transferred from user 1 to user 2 via therocoin protocol.



Pic 3. Coins transfer via private transactions

To use private transactions, you need to convert BTCU to zBtcu and then you can make any transfers for an unlimited amount of time. The reverse conversion is free of charge. A private transaction requires 21 confirmations to successfully complete, allowing for anonymous transactions with virtually no time loss.

Staking and Leasing

The logic of staking coins for profit has gained popularity in the blockchain community. UPoS not only implements standard staking capabilities but also enables delegated staking (Leasing). This not only allows users to make a profit by freezing coins and removes a large volume of coins from the trading turnover, which has a positive effect on the exchange rate, but also makes it possible to improve the network decentralization by determining the level of user confidence in masternodes and validators due to the ability to choose whom to transfer coins to leasing. This is very well visualized with the main nodes rating in the network (see 4.4)

Staking

Coins can be stacked either by Masternode or by Validator (see 4.2). This is one of main actions in the network to prove the intentions of the network. As a two-tiered network, BTCU incentivises participants of both the staking tier to maintain the health of the network. Via staking, Masternodes contributing towards the network are rewarded either for staking in-wallet, or for storing their BTCU as collateral for a masternode to support the network. While both of these are a means of acquiring rewards over time, the amount and means differ. More on masternodes in the section of Economy (see 5.2 and 5.3).

Leasing

The leasing mechanism in the BTCU network is used to issue new BTCU coins and to increase the circulating supply of coins. Each network user can lease their coins to Masternodes and Validators by choosing the “Leasing” transaction type.

Interest on leasing is accrued to the user 30 blocks after the transfer of coins to the lease has been carried out. The accrual takes place on the main balance with the ability to immediately use the interest and without the need to close the lease. In addition, the bonus continues to be credited for each subsequent generated block (see 5.2). Rewards accrued on the main wallet which means that the users can use their coins including multistaking.

Multileasing

Each network user can lease coins an unlimited number of times, regardless of the number of previous charges.

If the user already has an active lease, he can add a new lease at any time by buying coins or transferring those that were already on their balance.

In the case of multi-leasing, the user will be charged a commission equal to the commission for the transfer between addresses on the current block. At the same time, these terms of the commission apply only to multi-leasing operations. In other cases of leasing, no commission is charged.

BTCU Technical Specifications

Consensus

Hybrid of PoA, LPoS, PoS. With the name of UPoS (Ultimatum PoS)

UPoS Phase Period

Active since the start of the project

Blockchain type

Linear - on launch period, but the next step to make a nonlinear blockchain.

Block size

2 MB

BTCU
ULTIMATUM

BTCU Technical Specifications

Block Time

60 Seconds

Coin Emission Logic

Supply will be equivalent 1:1 to BTC. All bonuses for staking and ownership will be used transaction commission by BTCU economic policy.

Coin Supply Control

Coin supply will be determined when BTCU is launched.
It means that the supply of BTCU is the same as the supply of BTC on a block of forking.

Staking Eligibility

Minimum Input Age: 60 minutes
Maturity Confirms: 21 confirms
Wallet Status: Requires master-node to be kept running & online.

Transaction Send Eligibility

Minimum number of confirmations: 3 which was calculated and based on UPoS BTCU logic.

Hash algorithm

SHA-256

Accumulator Encryption

RSA-2048

Private address algorithm

ECDSA - secp256k1 (Elliptic Curve Digital Signature Algorithm) - export in standard format WIF

BTCU
ULTIMATUM

BTCU Technical Specifications

Smart contract

based on Ethereum virtual machine (EVM) - popular virtual machine for building smart contracts. The next step - integrate the environment of the next generation - WebAssembly and make more opportunities for smart contract building.

Smart Contract language support

Solidity

SwiftTX Eligibility

1 confirm for locking and 3 confirms to spend.
Collateral held for 15 minutes.

Privacy Technology

Custom Zerocash Protocol based on ZK-Snarks (we call this zBtcu) - is a new protocol that provides privacy-preserving, the new generation of Zerocoin protocol.

Key Features

Custom accumulator check-pointing system, launching own smart contracts, increasing TPS parameter by using the limited amount of validators and SwiftTX technology.

The main Features is a fully decentralized system where 10 main validators are the largest crypto platforms in the world!

Mint time	Spend time	Fees (mint)
>= 0.5 seconds	>= 2.5 seconds	0.00000100 BTCU per minted zBtcu denomination.

Fees (spend)

No fee to spend
zBtcu back to BTCU.

BTCU Technical Specifications

Minimum BTCU confirmation count required to mint zBtcu

6 confirmations

Minimum zBtcu confirmation count required before spend

21 confirmations

Initial Coins Supply:

[block# 000001] Initial coin supply: airdrop of Bitcoin utxo set 1:1 BTCU for creating 10 Masternodes for the network functioning.

BTCU ULTIMATUM

Project Stack

Dependency	Version used	Minimum required
Berkeley DB	4.8.30	4.8.x
Boost	1.64.0	1.47.0
Clang		3.3+ (C++11 support)
D-Bus	1.10.18	
Expat	2.2.2006	
fontconfig	2.12.2001	
FreeType	2.7.2001	
GCC		4.8+ (C++11 support)
HarfBuzz-NG		
libevent	2.1.8-stable	2.0.22
libjpeg		
libpng		
librsvg		
MiniUPnPc	2.0.20180203	
OpenSSL	1.0.1k	
GMP	6.1.2002	4.8.x
PCRE		
protobuf	2.6.2001	
Python (tests)		3.5
qrencode	3.4.2004	
Qt	5.9.2007	5.5.2001
XCB		
xkbcommon		
ZeroMQ	4.3.2001	4.0.0
zlib	1.2.11	

BTCU ULTIMATUM

Private key generation algorithm

BTCU uses the ECDSA, or Elliptic Curve Digital Signature Algorithm. More specifically, it uses one particular curve called secp256k1.

This curve has an order of 256 bits, takes 256 bits as input, and outputs 256-bit integers. And 256 bits is exactly 32 bytes. To put it another way, we need 32 bytes of data to feed to this curve algorithm.

There is an additional requirement for the private key. Because we use ECDSA, the key should be positive and should be less than the order of the curve. The order of secp256k1 is in format F..FEBAAEDCE6AF48A03BBFD25E8CD0364141, which is pretty big: almost any 32-byte number will be smaller than it.

BTCU
ULTIMATUM

Bitcoin
Ultimatum Economy

btcu.io

Bitcoin Ultimatum Economy

The economy of BTCU has many factors as the combination of many technologies increases the number of them. The main factors affecting the economy are the specifics of the work of consensus, leasing, a large number of types of commissions and dependence on the Bitcoin supply. Let's take a closer look at each of these factors below.

Initial Supply and Airdrop

Airdrop will make Initial Supply the same as in Bitcoin on the launch block. The important thing to focus on for a Bitcoin airdrop is not a blockchain like a fork, but rather Bitcoin's UTXO (Unspent Transaction Output) set, which is a log containing the current ownership of Bitcoin and associated addresses. As new blocks are mined with a new set of transactions on the Bitcoin network, the UTXO set is modified to incorporate the change of ownership reflected by those transactions.

When the fork is launched, an airdrop will be conducted to all users of the Bitcoin network to wallets identical in the BTCU network in the ratio of 1:1 to the BTC balance on the branch block used by the BTC UXTO.

Leasing Economy

The following network factors are taken into account in calculating the amount of the bonus accrued to the user for leasing:

Table 1.

Block height (depending on the range in which the accrual block is located, the amount of payment is determined)

Phase	Block ranking	Reward
Phase 1	up to 500,000	15%
Phase 2	from 500,000 up to 1,000,000	14%
Phase 3	from 1,000,000 up to 1,500,000	13%
Phase 4	from 1,500,000 up to 2,000,000	12%
Phase 5	from 2,000,000 up to 2,500,000	11%
Phase 6	from 2 500,000 up to 3,000,000	10%
Phase 7	from 3,000,000 up to 3,500,000	9%
Phase 8	from 3,500,000 up to 4,000,000	8%
Phase 9	from 4,000,000 up to 4,500,000	7%
Phase 10	from 4,500,000 up to 5,000,000	6%
Phase 11	from 5,000,000 up to 5,500,000	5%
Phase 12	from 5,500,000 up to 6,000,000	4%
Phase 13	from 6,000,000 up to 6,500,000	3%
Phase 14	from 6,500,000 up to 7,000,000	2%
Phase 15	from 7,000,000 up to the end of supply	1%

Table 2

The volume of coins in lease at the time the bonus is credited:

Volume of coins leased	Ratio
up to 500,000	1
from 500,000 up to 1,000,000	0.95
from 1,000,000 up to 2,000,000	0.9
from 2,000,000 up to 3,000,000	0.85
from 3,000,000 up to 4,000,000	0.8
from 4,000,000 up to 5,000,000	0.75
from 5,000,000 up to 6,000,000	0.7
from 6,000,000 up to 7,000,000	0.65
from 7,000,000 up to 8,000,000	0.6
from 8,000,000 up to 9,000,000	0.55
from 9,000,000 up to 10,000,000	0.5

Individual factors also affect the accrual of bonuses for leasing:

Table 3

The volume of BTCU coins in lease from the selected Validator or Masternode

The volume of BTCU coins leased by the user	Ratio
up to 5,000	1
from 5,000 up to 10,000	0.95
from 10,000 up to 20,000	0.9
from 20,000 up to 50,000	0.85
from 50,000 up to 100,000	0.8
from 100,000 up to 200,000	0.75
from 200,000 up to 300,000	0.7
from 300,000 up to 400,000	0.65
from 400,000 up to 500,000	0.6
from 500,000 up to 1,000,000	0.55
from 1,000,000	0.5

Table 4

Duration of leasing for the user online:

Lease duration (blocks)	Ratio
up to 30,000	1
from 30,000 up to 90,000	1.1
from 90,000 up to 180,000	1.2
from 180,000 up to 270,000	1.3
from 270,000 up to 360,000	1.4
from 360,000 up to 540,000	1.5
from 540,000 up to 720,000	1.6
from 720,000 up to 1 080,000	1.7
from 1 080,000 up to 1,440,000	1.8
from 1,440,000 up to 1,800,000	1.9
from 1,800,000	2

Masternodes and Validators Commission

Table 5

The Masternode receives a percentage of the lease volume of the users on the accrual block, depending on the block height:

Lease duration (blocks)	Percent (%)
up to 30,000	0.1
from 30,000 up to 90,000	0.09
from 90,000 up to 180,000	0.08
from 180,000 up to 270,000	0.07
from 270,000 up to 360,000	0.06
from 360,000 up to 540,000	0.05
from 540,000 up to 720,000	0.04
from 720,000 up to 1 080,000	0.03
from 1 080,000 up to 1,440,000	0.02
from 1,440,000 up to 1,800,000	0.001
from 1,800,000	0

Table 6

The Validator receives a percentage of the volume of leasing of the users sent to it on the accrual block.

Lease duration (blocks)	Percent (%)
up to 30,000	0.2
from 30,000 up to 90,000	0.18
from 90,000 up to 180,000	0.16
from 180,000 up to 270,000	0.14
from 270,000 up to 360,000	0.12
from 360,000 up to 540,000	0.1
from 540,000 up to 720,000	0.08
from 720,000 up to 1 080,000	0.06
from 1 080,000 up to 1,440,000	0.04
from 1,440,000 up to 1,800,000	0.002
from 1,800,000	0

The general formula for calculating a reward for a network user for leasing *(R_U):*

$$R_U = V_L \times K_{block\ height} \times K_{net.\ vol.} \times K_{node\ vol.} \times K_d , \qquad (5.1)$$

Where:

V_L - is user leasing volume ;

$K_{block\ height}$ - is coefficient of current block height (Table 1) ;

$K_{net.\ vol.}$ - is coefficient of total leasing volume in the network (Table 2) ;

$K_{node\ vol.}$ - is coefficient of Masternode or Validator leasing volume (Table 3) ;

K_d - is a coefficient of leasing duration for the user counted in blocks (Table 4).

The general formula for charging a Masternode reward for a lease is *(R_m):*

$$R_M = K_M \times V_{L.M.}, \qquad (5.2)$$

Where:

K_M - is the coefficient of the Masternode leasing volume of the users on the accrual block, depending on the block height (Table 5) ;

$V_{L.M.}$ - the amount of total leasing volume on Masternode on the current block.

The general formula for calculating the Validator's reward for leasing *(R_v):*

$$R_V = K_V \times V_{L.V.}, \qquad (5.3)$$

Where:

K_M - is the coefficient of the Validator leasing volume of the users on the accrual block, depending on the block height (Table 6) ;

$V_{L.V.}$ - the amount of total leasing volume on Validator on the current block.

Transactions Fee

Fee – this is a payment for conducting public and private transactions in the BTCU network, integrating smart contracts into the network, as well as for using smart contract methods.

The commission for conducting public transactions on the network is 0.00000010 BTCU (10 sat). The commission can be increased by the Validators by voting if the network load grows and the cost of maintaining the network grows. Regardless of which of the Validators generated the block, the commission is distributed as follows:

- 10% of the commission is distributed among the Validators;
- 90% of the commission is distributed between the Masternodes.

The commission for conducting public transactions on the network is 0.00000100 BTCU (100 sat). The commission can be increased by the Validators via voting if the network load grows and the cost of maintaining the network increases. The commission for conducting private transactions is distributed according to the following principle:

- 10% of the commission is distributed among the Validators;
- 90% of the commission is distributed between the Masternodes.

The formula for calculating the commission of smart contracts transactions $(F_{S.C.})$:

$$F_{S.C.} = 0.00032\ [BTCU] \times 200 \times S_{bytes} \qquad \textbf{(5.4)}$$

Where:

S_{bytes} - is the size in bytes of the smart contract.

The minimum commission is 100 BTCU Satoshi or 0.00000100 BTCU

However, fees can be increased for faster deployment in the event of network congestion. For example, in the case of network spam or the need to spend computing resources to execute useless transactions, network Validators can only allow contract transactions with a commission exceeding the initial one. The commission is distributed according to the following principle:

- 10% of the commission is distributed among the Validators;
- 90% of the commission is distributed between Masternodes.

BTCU
ULTIMATUM

Project Roadmap

btcu.io

BTCU ULTIMATUM

Project Roadmap

January 21st, 2021
the launch of the fork, branching from the BTC network and distributing airdrop to users who own BTC. Reviewed and certified by **HackCtrl.**

February 2021
expansion of the network of complete nodes for stable network performance.

March 2021
start working on the transition to a non-linear principle of block generation and network operation.

April 2021
start working on the integration of atomic swap technology into the core of the protocol.

May 2021
start working on mobile wallets with the ability to send coins by phone number inside the application.

June 2021
forming a pool of master nodes of validators from the community.

July 2021
testing the network for switching to a non-linear protocol.

August 2021
transition and implementation of non-linear technologies into the protocol - soft fork of the network.

September 2021
development of a platform for asset tokenization based on the protocol.

October 2021
launch of mobile wallets.

November 2021
organising a hackathon among developers to improve and innovate the protocol.

December 2021
launching a protocol-based asset tokenization platform.

January 2022
updates and the beginning of work on product solutions based on the protocol following the results of the hackathon.
.

February 2022
launching a protocol-based asset tokenization platform.

March 2022
carrying out load testing of atomic swap technology.

April 2022
carrying out tests on vulnerability of atomic swap technology.

May - June 2022
launch of native atomic swaps in the protocol, conducting a soft fork.

BTCU ULTIMATUM

Legal

btcu.io

Legal

CAUTIONARY NOTE ON FORWARD-LOOKING STATEMENTS

All statements contained in this White Paper, statements made in press releases or in any place accessible by the public and oral statements that may be made by BTCU or their respective directors, executive officers or employees acting on behalf of BTCU (as the case may be), that are not statements of historical fact, constitute “forward- looking statements”. Some of these statements can be identified by forward-looking terms such as “aim”, “target”, “anticipate”, “believe”, “could”, “estimate”, “expect”, “if”, “intend”, “may”, “plan”, “possible”, “probable”, “project”, “should”, “would”, “will” or other similar terms. However, these terms are not the exclusive means of identifying forward-looking statements. All statements regarding BTCU’s financial position, business strategies, plans and prospects and the future prospects of the industry which BTCU is in are forward-looking statements. These forward-looking statements, including but not limited to statements as to BTCU’s revenue and profitability, prospects, future plans, other expected industry trends and other matters discussed in this White Paper regarding BTCU are matters that are not historic facts, but only predictions.

These forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results, performance or achievements of BTCU to be materially different from any future results, performance or achievements expected, expressed or implied by such forward-looking statements. These factors include, amongst others:

(a) changes in political, social, economic and stock or cryptocurrency market conditions, and the regulatory environment in the countries in which BTCU conducts its respective businesses and operations;

(b) the risk that BTCU may be unable or execute or implement their respective business strategies and future plans;
(c) changes in interest rates and exchange rates of fiat currencies and cryptocurrencies;
(d) changes in the anticipated growth strategies and expected internal growth of BTCU;
(e) changes in the availability and fees payable to BTCU in connection with their respective businesses and operations;
(f) changes in the availability and salaries of employees who are required by BTCU to operate their respective businesses and operations;
(g) changes in preferences of customers of BTCU;

Legal

CAUTIONARY NOTE ON FORWARD-LOOKING STATEMENTS

(h) changes in competitive conditions under which BTCU operate, and the ability of BTCU to compete under such conditions;
(i) changes in the future capital needs of BTCU and the availability of financing and capital to fund such needs;
(j) war or acts of international or domestic terrorism;
(k) occurrences of catastrophic events, natural disasters and acts of God that affect the businesses and/or operations of BTCU;
(l) other factors beyond the control of BTCU;
(m) any risk and uncertainties associated with BTCU and their businesses and operations, the XXX Tokens, the BTCU Initial Token Sale and the BTCU Wallet (each as referred to in the White Paper).
All forward-looking statements made by or attributable to BTCU or persons acting on behalf of BTCU are expressly qualified in their entirety by such factors. Given that risks and uncertainties that may cause the actual future results, performance or achievements of BTCU to be materially different from that expected, expressed or implied by the forward-looking statements in this White Paper, undue reliance must not be placed on these statements. These forward-looking statements are applicable only as of the date of this White Paper.
Neither BTCU nor any other person represents, warrants and/or undertakes that the actual future results, performance or achievements of BTCU will be as discussed in those forward-looking statements. The actual results, performance or achievements of BTCU may differ materially from those anticipated in these forward- looking statements.