HOTBITSTAKE

STAKING AND REWARDS

Proof of Stake (PoS)

WORLD'S LEADING CRYPTOCURRENCY STAKING PLATFORM

HotbitStake: A Peer-to-Peer Interchain Economy

April 2020

Abstract

HotbitStake is a decentralized platform providing a trust interchain economy, World's Leading Cryptocurrency Staking Platform. It is powered by a Proof of Stake blockchain with Lightning Network, Masternodes, and dApps. Its use case is to provide a highly secure cross-chain platform for cryptocurrencies, where individuals can easily operate with any blockchain simply by using HotbitStake and its native currency BTS.

1. Introduction:

In the last few years, the cryptocurrency community has steadily grown. There are now hundreds of cryptocurrencies to choose from - with more appearing each passing day. It is important to understand which technologies, communities, and decentralized ledger technologies will separate themselves from the rest, pushing through the noise of constant ventures entering the crypto-sphere. Instead of a one chain rule, we believe the future will instead be in the formation of a global backend - a blockchain mesh consisting of every chain, technology, and service created thus far. A united network of different chains all communicating with each other through different interfaces. This conversation will be completely unbeknownst to end users as swaps between different chains will be done case by case on the backend - never seen, realized, or even chosen by the user.

1.1 Purpose of HotbitStake:

While most associate the word stake with staking, stake has its roots in the economics of business administration and stands for far more than just passive income. HotbitStake is more than staking; it is a network for stakeholders. To create a common understanding, we need to define the term network and connect it to the appropriate definition of a stake and a stakeholder.

− A network is defined as a system consisting of many similar parts that are connected.
− A stake is defined as a vital interest in a business or its activities.
− A stakeholder is any person or society at large that has an internal or external stake in the vision and mission of a business.

Thus, anyone who is actively or passively influenced by the activities of cryptocurrencies becomes a stakeholder of the blockchain economy. This includes ownership and holding of coins, property and legal interests, economic and social dependencies, developer and community activity, and any other crypto related work or interest. That way, cryptocurrency stakeholders:

− Affect the blockchain economy.
− Are affected by the blockchain economy.
− Be both affected the blockchain economy and affect the blockchain economy.

Putting all this together, we can start to see the vision HotbitStake is pursuing. A technical architecture to connect all the stakeholders of the blockchain economy into one giant network - the HotbitStake.

1.2 Plan of action:

To create a successful interchain solution for the blockchain economy, we need to identify the majority of its stakeholders, find a way to connect them, and ensure that our approach does not harm their integrity. Therefore, the following three sub-items are particularly important for our plan of action.

1.2.1 Identify the majority:

The most common stakeholder in the blockchain economy is Bitcoin itself, which is a peer-to-peer version of electronic cash growing stronger day by day. Most notably gaining major traction and a wide audience these past few years. Nowadays, countless people are affected by Bitcoin, and in return, also affect Bitcoin due to their work and activities. This includes the mining industry, financial products, different wallet solutions, and many other Bitcoin-related work. In addition to Bitcoin, blockchains with smart contract capacities are particularly well-known too. The beauty of their blockchain architecture is that they enable both side and subchain creation. This allows for the development of decentralized applications, or dApps. The best-known smart contract blockchain is Ethereum which hosts the largest number of tokens for different blockchain related businesses. Another famous blockchain with a similar use case is EOS which is currently the most used blockchain in the space of cryptocurrencies. Both blockchains are individually affected by internal and external interests, too. There is not a single blockchain where the stakeholder approach is not used.

1.2.2 Connect the majority:

After finding out who our stakeholders are, we need to find a way to connect them. Bridging the gap between blockchains will be possible if both chains are using a compatible interface, like second layer protocols, or are supporting the same cryptographic hash function.
That given, it is possible to execute trustless transactions between different blockchains. In Bitcoin's case, we can utilize the Lightning Network as the default interface for peering two different chains, as we have already done with Bitcoin, Litecoin, and HotbitStake. Other blockchains such as Ethereum or EOS can be integrated into our stakeholder network via their own smart-contract language. The usage of hashlocks and timelocks provides us a solution to lock BTS on our native chain while unlocking the corresponding BTS tokens on the smart contract chain and swap these tokens in the opposing side and subchain mesh with other cryptographic currencies. Besides the exchange of coins and tokens, connecting the stakeholders of blockchains also means that you need to integrate the periphery industries of these blockchains as well. Therefore, we drafted a solution for decentralized mining pools, cross-chain staking, and the hosting of dApps with interfaces to other chains' applications, too.

1.2.3 Protect integrity:

All these ideas would be empty words if we just developed another centralized solution. We protect everyone's integrity by combining the advantages of different blockchains into one interchain management architecture. The key pillars are our very own Trustless Proof of Stake consensus, an upgraded Masternode layer with watchtower functionality, and an upgraded Lightning Network layer with specialized swap resolvers. As well as several products, one of which is our hardware device BTS Viper - used for storing, exchanging, and utilizing different chains native assets and tools. In short, HotbitStake connects the largest distributed network developments into one decentralized place where individuals can operate with any blockchain simply by using HotbitStake as the default interface.

2. Blockchain architecture:

HotbitStake is a Proof of Stake blockchain, which provides a truly decentralized, highly secure, and profit-driven interchain network for the blockchain economy. It is powered by its native coin BTS, while being managed by its own network of Masternodes and Lightning Network nodes. HotbitStake has a one second confirmation time, and up to 240 on-chain transactions per second. It is based on a block size of 1-4 megabyte and a block generation time of 60 seconds. Additionally, the HotbitStake blockchain can infinitely scale off-chain with practically zero fee transactions by using Lightning Network.

2.1 Consensus

The consensus in a decentralized digital currency is used for the validation of the newly generated blocks of a blockchain. Simply expressed, it is a software component that the validator uses to vote on whether a story about the past is true or not. For this proof, HotbitStake uses a minting Proof of Stake consensus which is expanded with an offline staking solution, called Trustless Proof of Stake.

2.1.1 Minting Proof of Stake

Unlike Proof of Work, where the workers use the hashing power of their hardware to solve cryptographic puzzles, the stakers in Minting Proof of Stake use their coinage (up to 24 hours) and wealth to suggest new blocks. Here, the coinage is defined as the time since the staker's coins were not moved while the coin wealth is simply the number of coins a staker owns. The proof of newly generated blocks
is done with a special transaction, called coinstake. Within this transaction, the first input is named kernel. To ensure that the creator of a new block is selected by a stochastic process, the kernel input must satisfy a specific hash target protocol. This hash target is defined as a target per unit coinage that needs to be reached before it is subsequently consumed in the kernel. The technical consequences are that the chosen staker has to pay himself a set number of coins, thereby consuming the coins coinage to gain the privilege of generating a new block for the network. Thanks to the coinage consumption, the chance for one staker to validate several blocks in a row decreases quite substantially because their voting power is reset after each successful vote.

2.2.1 Supply:

With a total supply of 500 million tokens, BTS is distributed in the following proportions:

* 40% Stake for participating in PoS consensus.
* 30% is issued for free to eligible Staking members.
* 20% for developing the HotbitStake ecosystem.
* 10% is held by the development team with a disbursement period of 4 years (equivalent to 12,5 million BTS each year).

2.2.2 Coin distribution

We believe that network security and network services are equally as important as to have a robust and powerful infrastructure. Since the HotbitStake blockchain is powered by two types of nodes: Staking nodes and Masternodes, we do not discriminate between their works. That’s why the staking nodes and Masternodes are equally rewarded, each with 45% of the block rewards. Finally, 10% of the block rewards are sent to the treasury. The treasury is a cryptographically sealed public address that holds funds allocated to it by the network. It is used to fund HotbitStake further coin developments and new projects. There is also a long-term development fund for larger projects, partnerships, and key developments.

2.3 Second layers

The HotbitStake blockchain uses several second layer solutions for on-chain, offchain, and cross-chain features. The most important ones are its own Masternode and Lightning Network layer, as well as the Tokenization Layer of other blockchains.

2.3.1 Masternodes

A Masternode is a dedicated fullnode of a blockchain that resides on servers around the world to ensure decentralization and redundancy. While a staking node is responsible for the validation of the blockchain, a Masternode provides several services for the network. To operate a Masternode a valid collateral output of 15 000 coins for each Masternode is required. This was made to counter a wild growth of the nodes and to avoid rogue nodes. In addition to Masternode default features like instant send and decentralized democracy, our
Masternodes are aimed to be one of the most powerful stations within the crypto industry and will earn a passive income based on the services they provide. They will:

- Host and run BTS Dex.
- Host all needed blockchain explorers to ensure true decentralization.
- Host all blockchains needed to keep BTS Dex decentralized and light.
- Handle Lightning Swaps and Tokenized Swaps between different blockchains.
- Be used as watchtowers to host and monitor Lightning Channels.
- Use their collateral to provide Lightning Network liquidity.

- Authorize and secure the transfer of tokenized coins between different blockchains.
- Facilitate instant and private on-chain transactions.
- Provide onion routing and ensure secure exit points for the network.
- Host dApps for HotbitStake and other blockchains.
- Be used for the decentralized democracy of the network.
- Offload CPU and database capacities for everyone within the HotbitStake mesh.

Thanks to the Masternodes, the HotbitStake blockchain becomes an ecosystem in which no single entity can govern and serve the entire network.

2.4 Lightning Network

The Lightning Network is a second layer solution to enable peer to peer off-chain transactions within a blockchain, or between different blockchains. It requires providers to lockup their coins in channels to ensure liquidity and to route payments between different nodes. To understand how the Lightning Network works, the knowledge of unidirectional and bidirectional payment channels is needed.

Unidirectional payment channels: Without Lightning, the classic payment channel only exists between two parties or peers. This technology uses the Multi-Signature (MultiSig) feature and a so-called locktime. With the MultiSig mechanism, you can generate a transaction that requires more than one private key to sign this transaction. This means that the coins associated with the transaction require both parties' approval to be sent. The locktime ensures that the coins within the MultiSig are non-transferable for a certai n period. Bidirectional payment channels: The mechanism described above was called unidirectional channel since only one party could send coins to another party. If both parties want to exchange payments with each other, they need a bidirectional channel. This leads to a dilemma: Why should one party wait for the
entire locktime instead of claiming the whole stake right away? To prevent this, Lightning uses a mechanism of mutual protection. Here, each party think of an individual secure-number before setting up the channel and send each other a hash of this number. As in the case of a unidirectional payment channel, the payment partners generate a MultiSig address. Before broadcasting their MultiSig address to the network, each party generate a transaction called commitment transaction.

In this commitment transaction, the funds are split up: one part goes to the creator of the commitment transaction, and the second part goes to a time-locked address to which the counterparty has access after a set time. Thus, both have created contracts that prevent fraud. As we now understand how bidirectional payment channels work we need to find a way to connect them into a network. Before the Lightning Network, all parties would have to create a new channel for each new payment activity. So, if party A wants to do business with party C, both business partners would have to set up a payment channel - regardless of whether A and C are already exchanging with party B or not. So why should A and C use a new channel, when they can use B to bridge between both. The only question is, can B be trusted? What if B is fraudulent, claims the money, and just does not pass it on? So with this in mind, how do we ensure that B does not shut down his Lightning node or has technical issues that force him to set his node offline? As a solution for these problems, the Lightning Network uses hashed timelock contracts
(HTLCs) to guarantee that these issues cannot happen. An example: C thinks up a secret, which is a specific random number with the usage of cryptographic proof. C gives the hash of this secret to A. This hash now becomes a pledge. B only receives a payment if he knows this secret. This can be checked by party A by using the hash. B passes the hash through again with the promise to pay, if the recipient knows the secret hash, too. In principle, the path between A and C may include other participants, all of whom use the hash as a pledge. Using HTLCs, payment channels can be linked between different parties.

As you can see, participants in the network who build a bridge between A and C as nodes, form the backbone of the Lightning Network.
Their importance can be compared to that of miners or minters on the regular blockchains.
Hotbitstake upgrades the current Lightning solution by funding its Lightning channels by default with the Masternode's collateral and using the Masternodes as bridge nodes between all parties.

You can imagine this like a pool where different masternodes allocate their funds in a specialized multisignature address, while additionally providing the possibility for random wallets to join these channels.
Now within this master channel all parties can open many 2-of-2 channels concurrently and thanks to Lightning Swaps even between different blockchains.
This solution does not only benefit Stakenet, but it is also an upgrade for every blockchain with a Lightning Network, because HotbitStake's currency, BTS, can be used as a carrier coin for both Bitcoin and Litecoin transactions, too.
Consequently, HotbitStake wipes out the risk of low funded channels and offers a solution to merge different Lightning Networks into one interchain solution.

2.4.1 Tokenization

Tokenization is known as a process to convert rights to an asset into a digital token. Thus, each token represents the underlying asset. Using a blockchain for this purpose guarantees that the ownership information is immutable. Currently, we are developing BTS tokens on the Ethereum and EOS blockchains, which represent the native BTS coin and can be converted between Ho tbitStake, Ethereum, and EOS with the help of a bridging protocol. With specialized multisignature addresses, hashlocks and timelocks we can lock BTS on our native chain addresses while unlocking the BTSETH and BTSEOS tokens on the opposing smart contract chain. HotbitStake users do not need to manually transform their coins to the tokens, because all is executed by smart contracts on the network and governed by our Masternodes layer. It is important to note the number of native BTS coins does not increase. The existing amount of all moveable coins and tokens is equal to the total BTS supply and is cryptographical auditable. Once the bridge protocol is used to send BTS coin to the Ethereum or EOS network, they are locked up and stored in a special smart contract address. Thus, the sender has no access to the native coins, while getting permissions for the opposing tokens. By connecting the HotbitStake blockchain to the Ethereum and EOS blockchain through tokenization, we can integrate every known token of these blockchains into our interchain network. This way we will be able to provide an interoperable technology for swapping assets across different networks to allow everyone to freely operate with any coin and token within the blockchain mesh. An additional advantage
is that this workflow is compatible with any other blockchain which supports tokenization. This means that the HotbitStake interchain network can easily grow day by day and new achievements of other developers benefit our network as well.

3. BTS Products

To ensure a user-friendly and secure place for people to deal with different blockchains, BTS Products provide software and hardware solutions for daily interactions with HotbitStake.

3.1 HotbitStake Wallet

The HotbitStake Wallet is a non-custodial multi-cryptocurrency light wallet and the main interface to interact with, for the cryptocurrency world. Essentially, it is a one-stop place for everything - in both mobile and desktop versions. It is the main product of HotbitStake and thus the naming. A wallet itself is an important and integral component of the cryptocurrency universe. It is a secure digital purse which helps in storing and transacting digital currencies like Bitcoin and Ethereum. Most of the coins and tokens have their official core and light wallets,
but here comes the problem: for every cryptocurrency that a user holds, he also requires a wallet to store it, thus making it cumbersome for the holder to have so many wallets.
HotbitStake provides a solution to this problem as its Masternode network will hold databases and also run full nodes of multiple blockchains, allowing for HotbitStake to create a wallet that can securely send, receive, and confirm a transaction on separate blockchains. Holding these blockchains in the second layer provides us the possibility to develop the HotbitStake Wallet truly light without any limitations. In contrast to other light wallets, the HotbitStake Wallet will not be limited to basic blockchain interactions like storing, sending, and receiving. In combination with other BTS Products, like the BTS Viper, all users within the HotbitStake interchain economy can use it as the interface to access additional features like offline staking from a hardware device, setting up Masternodes, or running hubs for the Lightning Network.

Additionally, the HotbitStake Wallet will have an in-house over the counter trading engine, which will be connected to the BTS Dex, where users can swap their assets between different blockchains without revealing their private keys. To ensure secure access to our interchain mesh, the HotbitStake Wallet provides native TOR support. This will be managed by our Masternode layer. TOR itself is an IP obfuscation service to enable anonymous communication across a layered circuit-based network. Each HotbitStake Masternode will direct the blockchain traffic of our network among thousands of relays to conceal the user's location. In simple words, when users connect their wallets to the TOR network, their traffic is then routed through a number of global masternode servers, each of which removes information of the previous server, thus, the last exit node server gets no information where the network originated from.

3.2 BitStake Coin

BTS is a state of the art cryptocurrency that allows a peer to peer method of payment. It is money with unique properties not achievable by any central bank issued currency, as BTS is open, permissionless, decentralized, trustless, censorship-resistant, immutable, smart, interoperable, fungible, secure, and has a fixed emission rate. So, it is a medium of exchange used for real-world transactions on a global scale, including the transactional activities happening within the HotbitStake ecosystem. Each service that generates fees needs to be paid in BTS one way or another - in some cases users won't even realize they have paid in BTS as it will all be handled by Lightning Swaps in the background. All in all BTS is the currency, the gas, and the foundation of HotbitStake, as everything runs on top of it. It is required for the ecosystem to operate.

3.3 BTS Core

BTS Core is the open source software component to run a fullnode within the HotbitStake blockchain to receive, store, and send BTS. It acts as the core interface for using all the functions of the HotbitStake network and is required in order to operate a staking node, merchant node, lightning node, and Masternode. These nodes are the core pillars for our blockchain, as they allow to connect computers in a peer to peer network to reach agreements over shared data. BTS Core is compatible with the most popular operating systems, such as Linux, macOS, Windows, and can be accessed through the command line interface or graphical user interface.

3.4 BTS Cloud

BTS Cloud is a centralized application that offers blockchain services, designed to grant a better and easier experience for BTS users, thus helping with adoption. Please note that BTS Cloud is not based on the HotbitStake blockchain, and has nothing to do with its decentralized ecosystem and dApps. Simply put, https://hotbitstake.com is an informational website hosting the BTS Cloud app, while HotbitStake is the decentralized network built upon the blockchain. BTS Cloud features the following:

− Staking-as-a-Service (Online staking wallet): Wallets that automatically stake. Deposited users' coins are sent to one main address (called pool) that regularly receives many stakes, and are then distributed in real time.

− Masternodes-as-a-Service (Masternodes hosting): Our very own trustless Masternode hosting solution. It is risk-free, as you remain in control of your coins at all times in your local wallet.
− Monitoring services: A real-time monitoring service for Masternodes
and trustless Proof of Stake contracts. Customers will immediately receive e-mail alerts if anything goes wrong.
− ROI calculator: The relation between staking nodes and Masternodes changes daily, so the profitability of each changes, too.
The ROI calculator is a tool to find the best choice with more interest for you.
BTS Cloud collects fees from the users for using some of these services. Fees are then sent to the BTS Cloud treasury to cover costs and further development.
Note, you lose ownership of the coins you deposit to BTS Clouds wallets, as you do not control the private keys.
Please do not deposit large amounts of coins, but instead, stake on your own with Trustless Proof of Stake or common staking solutions.
BTS Cloud wallets are only suitable for newcomers with no experience and a small coin balance that otherwise would not earn any staking rewards for months.
The rest of the BTS Cloud services are trustless solutions safe to use by everybody as you do not lose ownership of your coins.

4. Summary

HotbitStake is a distributed network for incentivized stakeholders; providing a trustless interchain economy. It is based on an enhanced Proof of Stake blockchain with several second layer solutions, like the Lightning Network, Masternodes, and dApps. It has one second confirmation time and up to 240 on-chain transactions per second. Over the Lightning Network

Hotbitstake (https://hotbitstake.com/)
HOTBITSTAKE Safe CryptoAsset Staking Platform, where the majority of the transactions will take place, the HotbitStake blockchain can infinitely scale with instant and practically free transactions. Its use case is to provide a cross-chain architecture for cryptocurrencies, where individuals can easily operate with any blockchain simply by using HotbitStake native coin BTS, as the blockchains are connected to each other through the Lightning Network and other cross-chain technologies. HotbitStake supports the building of code-agnostic dApps on top of it, such as the BTS Dex. All dApps will be powered by BTS Masternodes, which charge fees for the services they provide.
Unlike the vast majority of cryptocurrencies, HotbitStake does not impose a brand new standard, but rather adhere to the existing BTC/LN protocol and existing smart contract solutions, which are both the present and future of the blockchain economy.

HOTBITSTAKE

STAKING AND REWARDS

HotbitStake provides one of the highest levels of security among any Proof of Stake blockchain. It allows easy and secure staking of its currency BTS by using its invention Trustless Proof of Stake - effectively achieving decentralized cold staking. TPoS allows the minters to cold stake their coins through a special agreement on the HotbitStake blockchain, which means validators can stake their BTS even from a hardware wallet, thereby removing any unnecessary security risk. Furthermore, HotbitStake Masternodes create a massive decentralized network of computers that generate incredible amounts of computational power.

They provide high-end network services and run the dApps that are built upon the blockchain. For example, the BTS Masternode network powers the BTS Dex by performing Lightning Swaps and Tokenized Swaps between different coins, hosts Lightning Channels, and provides liquidity to the Lightning Network with Masternodes' collaterals.

HotbitStake is the first Proof of Stake blockchain with Masternodes to successfully execute Lightning Network compatibility and is among the first, besides Bitcoin and Litecoin, to ever perform atomic swaps over the Lightning Network (Lightning Swaps). Therefore, the HotbitStake blockchain can interact with any Lightning Network compatible merchant, application, wallet, or upcoming crypto device. Thanks to HotbitStake cross-chain capabilities users will be able to pay anyone that accepts Bitcoin, or any other Lightning Network compatible coin, seamlessly with their BTS, improving adoption on a massive scale as thousands of merchants already accept Bitcoin payments over Lightning Network.

HotbitStake is building the safest, fastest, and cheapest interchain architecture for the blockchain economy by combining Lightning Network, different smart contract solutions, and cold storage to trustlessly stake, exchange, and pay.