



Fast, Secure and Encrypted

**A White Paper
v.1.00.10
08/July/2021**



HASHBIT BLOCKCHAIN [HBIT]

Contents

1. Introduction.....	2
2. Business Case.....	2
3. Problem Statement v/s Proposed Solution.....	2
4. Product Overview.....	3
5. Conclusions.....	7

1. Introduction

HashBit Blockchain (HBIT) is a Java-based Blockchain, extremely light, fast and simple for any type of integration, be it applications, games, online stores but above all we are working to make it perfect for everyday use, allowing everyone to day to be able to use it quickly and easily, when buying in a store or a simple transfer of coins between two users via their smartphone.

HBIT is used through a normal browser, using all available tools, simplicity must be the basis for easy mass use, speed for practically instant transactions and the safety of each user is our priority.

2. Business Case

3. Daily use via POS, fast transfers, decentralized applications, such as discussion forums, instant messages, creation of own assets and much more.
4. Anyone can create any kind of program, application, game using HBIT technology effortlessly, in no time and safely.
The limit is your imagination!

5. Problem Statement v/s Proposed Solution

Problem	Solution
Consumption of Resources	HBIT is "Green" it is possible to run a node on a smartphone or a raspberry pi, with a resource consumption of less than 20%, no expensive hardware is needed to make it work.
Transaction Speed	30+ times faster than Bitcoin, block time of 30 seconds, which can decrease if the transaction load is high.
Easy to use	Integrating it into an app or website is easy, no specialized programmers are needed, the tools available make it easier to use than ever before.

6. Product Overview

HBIT is a 100% proof-of-stake cryptocurrency, constructed in open-source Java. HBIT unique proof-of-stake algorithm does not depend on any implementation of the coin age concept used by other proof-of-stake cryptocurrencies, and is resistant to so-called nothing at stake attacks. A total quantity of 50 billion available tokens were distributed in the genesis block. Curve25519 cryptography is used to provide a balance of security and required processing power, along with more commonly-used SHA256 hashing algorithms.

Blocks are generated every 30 seconds, on average, by accounts that are *unlocked* on network nodes. Since the full coin supply already exists, HBIT is redistributed through the inclusion of transaction fees which are awarded to an account when it successfully creates a block. This process is known as *forging*, and is akin to the mining concept employed by other cryptocurrencies. Transactions are deemed safe after 10 block confirmations, **and HBIT current architecture and block size cap allows for the processing of up to 1,101,600 transactions per day.**

HBIT transactions are based on a series of core *transaction types* that do not require any script processing or transaction input/output processing on the part of network nodes.

These transaction primitives allow core support for:

- Transfer Coin.
- Mining.
- Discussion Board.
- User to User Encrypted Messages.
- Merchants Tools.
- Issue Assets.
- Asset Exchange.
- Online and Offline Payment Gateway (HBIT Pay).
- Developers Tools.

By leveraging these primitive transaction types, HBIT core can be seen as an agile, base-layer protocol upon which a limitless range of services, applications, and other currencies can be built. This version of the whitepaper documents features and algorithms that are implemented in HBIT as of version 1.00.00.

Future revisions will be made to reflect additional planned features and algorithm changes.

7. Proof of Stake

In the traditional Proof of Work model used by most cryptocurrencies, network security is provided by peers doing work. They deploy their resources (computation/processing time) to reconcile double-spending transactions, and to impose an extraordinary cost on those who would attempt to reverse transactions. Coins are awarded to peers in exchange for work, with the frequency and amount varying with each cryptocurrency's operational parameters. This process is known as mining. The frequency of block generation, which determines each cryptocurrency's available mining reward, is generally intended to stay constant. As a result, the difficulty of the required work for earning a reward must increase as the work capacity of the network increases.

8. As a Proof of Work network becomes stronger, there is less incentive for an individual peer to support the network, because their potential reward is split among a greater number of peers. In search of profitability, miners keep adding resources in the form of specialized, proprietary hardware that requires significant capital investment and high ongoing energy demands. As time progresses, the network becomes more and more centralized as smaller peers (those who can do less work) drop out or combine their resources into pools.
9. In the Proof of Stake model used by HBIT, network security is governed by peers having a *stake* in the network. The incentives provided by this algorithm do not promote centralization in the same way that Proof of Work algorithms do, and data shows that the HBIT network has remained highly decentralized since its inception: a large number of unique accounts are contributing blocks to the network.

10. Coins

The total supply of HBIT is 50 billion coins, divisible to eight decimal places.

All tokens were issued with the creation of the *genesis block* (the first block in the HBIT blockchain), leaving the *genesis account* with an initial negative balance of 50 billion HBIT.

The existence of anti-tokens in the genesis account has a couple of interesting side effects:

- the genesis account cannot issue transactions of any kind, since its balance is negative and it cannot pay transaction fees. As a result, the private passphrase for the genesis account is free for anyone to use.
- any tokens sent to the genesis account are effectively destroyed, since that accounts negative balance will cancel them out.

The choice of the word *tokens* is intentional due to HBIT intention to be used as a base protocol that provides numerous other functions. HBIT most basic function is one of a traditional payment system, but it was designed to do far more.

11. Network Nodes

12. A *node* on the HBIT network at the moment it is only the Official one, monitored and guaranteed by the development team, this allows greater security, 99.9% uptime and guarantees access from all over the world without any problem.

13. Official node features a built-in DDOS (Distributed Denial of Services) defense mechanism which restricts the number of network requests from any other node to 30 per second.

14. **Blocks**

As in other crypto-currencies, the ledger of HBIT transactions is built and stored in a linked series of blocks, known as a blockchain. This ledger provides a permanent record of transactions that have taken place, and also establishes the order in which transactions have occurred. A copy of the blockchain is kept on every node in the HBIT network, and every account that is *unlocked* on a node (by supplying the account private key) has the ability to generate blocks, as long as at least one incoming transaction to the account has been confirmed 1440 times. Any account that meets these criteria is referred to as an *active account*.

In HBIT, each block contains up to 255 transactions, all prefaced by a block header that contains identifying parameters. Each transaction in a block is represented by common transaction data, specific transaction types also include transaction attachment, and certain transactions may include one or more additional appendices. The maximum block size is 42KB. All blocks contain the following parameters:

- A block version, block height value, and block identifier
- A block timestamp, expressed in seconds since the genesis block
- The ID of the account that generated the block, as well as that accounts public key
- The ID and hash of the previous block The number of transactions stored in the block
- The total amount of HBIT represented by transactions and fees in the block
- Transaction data for all transactions included in the block, including their transaction IDs
- The payload length of the block, and the hash value of the block payload
- The block's generation signature
- A signature for the entire block
- The base target value and cumulative difficulty for the block

15. **Staking**

Blocks in the HBIT Blockchain are created with Staking, you can generate blocks using any amount that has at least 1440 blockchain confirmations in your account.

The staking person receives the fees for each transaction included in the block that is created.

The greater the number of HBIT, the greater the number of blocks generated in the blockchain, and the greater the HBIT of Fees earned.

HBIT are always available even if they are in Staking, you can send them at any time without having to unlock them.

Staking is currently managed by the Development Team, to keep the Blockchain safe, soon staking will be available to everyone, initially directly on the main node, then on the nodes of users who use the HBIT software.

16. Mining HBIT

The HBIT distribution is done at 99.5% by Mining.

Directly in the frontend of the blockchain (currently <https://chain.hashbit.org>) the mining section allows you to mine HBIT with your computer, using the power of the CPU. It is also possible to undermine HBIT via smartphone.

The distribution is divided as follows:

0 to 1B HBIT Mined: 1 Accepted Share = 0.1 HBIT

1B to 10B HBIT Mined: 1 Accepted Share = 0.01 HBIT

10B to 20B HBIT Mined: 1 Accepted Share = 0.001 HBIT

20B to 40B HBIT Mined: 1 Accepted Share = 0.0001 HBIT

40B to 49.5B HBIT Mined: 1 Accepted Share = 0.00001 HBIT

500M HBIT are reserved for developers.

49.5B HBIT is for Mining.

17. Inbox

The Inbox section in the Frontend uses the power of the HBIT Blockchain for communication between users and the public.

It is possible to send messages in the public chat, each user in the blockchain can read and write their own message.

It is also possible to send encrypted messages to users of the Blockchain, where only the sender and the receiver can read the message thanks to a series of algorithms used to encrypt.

18. Assets

The Assets section in the Frontend allows each user to create their own Token with a simple click.

By entering the required data the token is created in seconds (usually it is created and confirmed in less than 30 seconds)

The supply is added to the wallet of the creator who can start distributing his own currency to the users.

Transactions use HBIT as fees, of approximately 0.00001 HBIT per transaction.

In addition, the creator can distribute Dividends to the holders of his currency, at the cost of one transaction.

Dividends are in HBIT, and are sent only to those who own the coin. Again, the transaction and transfer takes a few seconds for all users.

19. **Assets DEX**

The DEX allows you to buy and sell the assets present in the Blockchain with HBIT. The listing is automatic and once the asset has been created it is automatically entered in the DEX, where it is immediately possible to enter purchase and sale orders.

As with most transactions, placing orders costs just 0.00001 HBIT in fees.

20. **API**

The HBIT Blockchain uses API to interact and to be easily integrated into any website, exchange, small or large application.

The APIs are http and with simple POST and GET requests you can use all the features without problems.

The response from the blockchain comes in JSON format, easy to interpret with all programming languages.

The APIs are available in the Frontend <https://chain.hashbit.org>

21. **Group Chat**

The group chat, present in the frontend, is an example of how the blockchain can be used to create decentralized applications or services.

Our group chat allows each user to enter a message visible to all, in a few seconds, with commissions between 0.00001 and 0.00004 HBIT.

Confirm and chat visible in seconds.

22. **Merchants Point of Sales**

The POS is a tool for accepting HBIT payments in any location, simply by entering the amount and currency of your country.

The system will make the change and calculate how many HBITs are required, the customer using Scan to Pay, just scan the QR code and all the required fields are filled in automatically. Once the payment has been sent, the system detects the transaction and shows the confirmation on the screen.

This product, in addition to being totally free, there are no hidden fees, allows you to accept HBIT anywhere, in a few seconds.

We are ready for mass adoption!

Over 160 local currencies are supported for local payments.

23. HBIT Pay

Unlike the POS, HBIT Pay allows you to accept online payments, whether it is a website, a shop, a game or an application, with a few lines of code you can accept payments in HBIT, in seconds, and in complete safety.

As for the POS, over 160 local currencies are also supported here with real-time exchange.

Furthermore there is the possibility to set successful url, cancellation url and verify payments through ipn url.

This guarantees maximum security in the verification of transactions.

24. Conclusions

Many new features will be added over time and this Whitepaper will be updated accordingly. The team is working to make them available as quickly as possible.

Thank you for your support and welcome to the HBIT Blockchain.