HASHBIT BLOCKCHAIN

Fast, Secure and Encrypted

A White Paper
v.1.10.00
16/December/2021

HASHBIT BLOCKCHAIN [HBIT]

Contents

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.
- Voting System.
- Decentralized Marketplace.
- Alias.
- 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://hashbit.org** the mining section allows you to mine HBIT in Cloud, without using any resource from your side.

You can Mine HBIT just Buy the Mining Activator (one per wallet) to allow most possible users to Receive HBIT.

Mining HBIT is the way how the total supply can be distributed to Community.
Is also possible to buy vCPU and receive Daily payout.

Mining Activator and vCPU will be active until all HBIT can be Distributed.

The distribution is divided as follows:
0 to 5B HBIT Distributed: Around 1152 HBIT.
5B to 10B HBIT Mined: 500 HBIT / vCPU Decrease 50%
10B to 20B HBIT Mined: 200 HBIT / vCPU Decrease 50%
20B to 40B HBIT Mined: 100 HBIT / vCPU Decrease 50%
40B to 49.5B HBIT Mined: 50 HBIT / vCPU Decrease 50%

500M HBIT reserved for developers.
49.5B HBIT for Mining.

Mining can be Restarted every Monday for Manual Start Mining.
VCPU not need to be restarted.

17. *HBIT Messenger*

HBIT Messenger, available directly in the HBIT wallet, allows each user to send and receive encrypted messages to other users, where only the sender and recipient can read the content in clear text.
Everything always decentralized and the data on the Blockchain.
All transactions are in real time, and we can interact with our friends in complete security and privacy without the use of external applications.

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://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. *HBIT Voting System*

The voting system allows each user to launch a survey on the Blockchain, and allow each user to vote.
Using the HBIT Blockchain, votes cannot in any way be tampered with, real-time voting after the vote has been confirmed in the blockchain.
This system can be used by any type of local or national voting agency by entering specific parameters that can be found and implemented using the http API.

25. *HBIT Alias System*

Alias system feature of HBIT essentially allows one piece of text to be substituted for another, so that keywords or keyphrases can be used to represent other things – names, telephone numbers, physical addresses, web sites, account numbers, email addresses, product SKU codes... almost anything you can think of.

For example, you could ask HBIT to associate "search" with "www.google.com". Once this is done, all you have to do to get to Google is type "hbit:search" into a HBIT-capable browser, and it will translate your request in one for "www.google.com".

Immediate applications are simple: you can create an easy-to-remember alias for your HBIT account number, for example. But since the Alias System is open-ended, it can be used to implement a decentralized DNS system, shopping cart applications, and more.

Creating aliases is

A user sends a transaction that states "ThisText = ThatText"

If the alias is to be changed, just send another transaction with a new definition. Only the account that created an alias can change it.

Details

The alias can be any string of latin-character numbers and letters. The address can be anything like:

"173.194.112.174" (an IPv4 address)

"2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d" (an IPv6 address)

"mydomain.com/secretpage.php?parameter=value" (a URI)

"johnsmith@matrix.com"

"tel:+44-20-8123-4567"

...or even "bitcoin:1BTCorgHwCg6u2YSAWKgS17qUad6kHmtQW".

There are 2 main ways to use HBIT aliases without having to rely on third-party plugins for your browser:

Server-side. A web server analyses the HBIT blockchain and replaces "hbit-links" with corresponding addresses before sending HTML documents to users.

Client-side. A web browser runs javascript code that connects to HBIT bootstrapping nodes and replaces "hbit-links" with their addresses. This requires to embedding a small script which is executed in an "onload" event. The script will do all the work via CORS, JSON, or other techniques.

Alias Transfer/Sale

Aliases can be transferred for a 0.00001 HBIT fee.

Alias can be sold to either specific HBIT Accounts or to the general public. To sell an alias, you can set the price to sell for every alias.

Sell Alias Functions

It is possible to sell the Aliases by setting a sale price in HBIT, once the order has been started, each user can buy the alias by paying the requested amount.

It is possible to update the sales price by sending the sales form again with the updated price.

Each sale or update request costs only 0.00001 HBIT as a transaction cost in the Blockchain.

26. *HBIT Cloud Data*

The HBIT Data Cloud is a decentralised data storage system.

In addition to keeping a record of HBIT transactions, the blockchain can also be used to store user-defined data. All forms of data can be uploaded to the HBIT blockchain, providing a secure (and, if desired, permanent) method of storing, retrieving and publishing information. HBIT

Messaging makes use of this ability to embed data in the blockchain, and the Data Cloud can be seen as an extension of the Messaging system.

One of the most important features of data storage on the blockchain is that the HBIT blockchain is a permanent and immutable record that provides a tamper-proof time stamp. This allows for legal records (such as contracts) to be embedded in the blockchain, with absolute certainty about the time at which they were created.

A single data item is currently limited to 40K on the public blockchain. Only the The sha256 hash of the data is stored on the blockchain as proof of existence. The data itself is pruned after several days.

EXTEND CLOUD DATA

The files sent on the Blockchain remain available for about 7 days, then they are deleted to keep the Blockchain clean and light.

It is possible to extend the duration simply by clicking on Extend, you pay a commission for sending it to the Blockchain, equal to that required to upload the file again.

Anyone can extend the duration of a file's stay in the Blockchain, but whoever uploaded it will always remain the same user.

27. *HBIT Non-fungible Tokens*

What are NFTs?

Non-fungible tokens, or NFTs, are pieces of digital content linked to the blockchain, the digital database underpinning cryptocurrencies such as bitcoin and ethereum. Unlike NFTs, those assets are fungible, meaning they can be replaced or exchanged with another identical one of the same value, much like a dollar bill.

NFTs, on the other hand, are unique and not mutually interchangeable, which means no two NFTs are the same.

Think of Pokémon cards, rare coins or a limited-edition pair of Jordans: NFTs create scarcity among otherwise infinitely available assets — and there's even a certificate of authenticity to prove it. NFTs are typically used to buy and sell digital artwork and can take the form of GIFs, tweets, virtual trading cards, images of physical objects, video game skins, virtual real estate and more.

How to make an NFT?

Anyone can create an NFT. All that's needed is a HBIT wallet, a small purchase of HBIT and a data uploaded to HBIT Cloud Data and link the content into an NFT or crypto art. Simple, right?

28. *HBIT Decentralized Marketplace*

Description

The HBIT Marketplace is an open decentralized store for all goods. You may sell or purchase software, music, video or any other kind of good here.

In a way, it's like purchasing an electronic product from Amazon or eBay, you browse the available products, you place an order and the seller will send you information of how to download the good (usually a link), or give you a tracking code to check inside HBIT system.

Buying/Selling on the Marketplace:

To buy or sell the products in the Marketplace, simply fill out the "BUY" or "LIST YOUR PRODUCT" form and follow the instructions indicated to buy or sell the product.

All transactions are managed by the HBIT Blockchain in a totally decentralized way.

- If you sell, specify the details indicated, when a user purchases your product, you will find the order in the "My Store Orders" menu and you will have to proceed with the shipment indicating all the details, whether they are a tracking code for physical products, or a link to digital products.

The buyer will receive this information to track their order.

- If you buy, press "BUY NOW" on the product you want to buy, insert the request fields carefully and send the order. The seller receives your order and will ship it. Once the order is marked as shipped, you will be able to see the details of the tracking or how to receive your product.

When the order is completed (Shipped) you can leave a feedback that will be displayed by everyone on the product page, this will allow other users to shop safely.

Product Image:

- To add an image to the product, you must first upload it to Cloud Data, and make a note of the UID of the image.
- This UID must be entered in the form where indicated, so the image will be uploaded together with the product.

What will come?

The upcoming Products are still many, and we could even say infinite given the nature of the Blockchain.

The next scheduled are:

***HBIT Auth** - Login System through the HBIT Blockchain, for websites, apps and all those services that require maximum security during user login.*

***IDWVS** (Institutional Decentralized World Voting System) - is an online voting service on the Blockchain, Institutions, agencies or surveys can be managed safely through this service without additional management costs.*
What does it solve?
It solves the problem of electoral fraud, counting of ballots and security. It will be possible to create your own voting asset and distribute it to the voters, each voter will then be able to vote where that particular voting asset is required. Institutions will have results in real time, no possibility of fraud or wrong counting, since everything will be managed by the Blockchain and therefore it is impossible to modify or change a certain result.

If developers deem it necessary, it is possible that other products will be released sooner than others.

Conclusions

The functionalities present in the wallet on **https://hashbit.org** are just examples of how it is possible to use the HBIT Blockchain for each type of application.
It is possible to create much more complete and complex services using all the parameters available in the http API.

We also remind you that by connecting to **https://hashbit.org** you interact directly with the HBIT Blockchain, your Passphrase is never saved and you can carry out transactions in complete safety.
The Wallet is just a bridge between the user and the blockchain, trying to make its use as simple and intuitive as possible.

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.