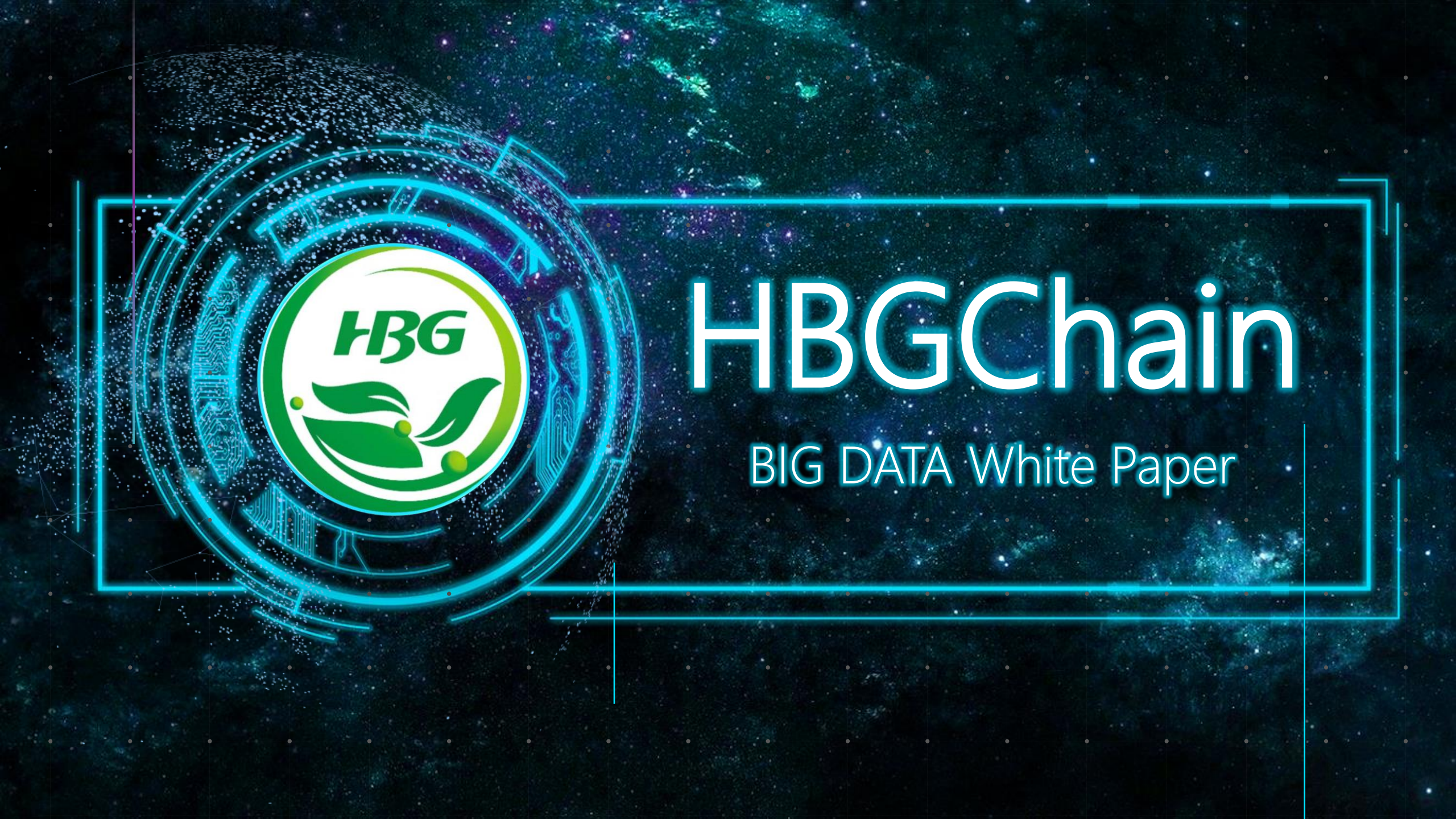

HBG
HBGChain
BIG DATA White Paper

What is Blockchain

Blockchain is a new application mode of computer technology such as distributed data storage, point-to-point transmission, consensus mechanism and encryption algorithm. The so-called consensus mechanism is a mathematical algorithm to establish trust and obtain rights and interests between different nodes in the blockchain system.

Blockchain is the underlying technology of HbG, like a database ledger, recording all transaction records. Because of its security and convenience, this technology has gradually attracted the attention of the banking and financial industry

HBG Block Chain

HBGChain is jointly issued and established by the Malaysian environmental protection foundation. It is the first integrated system in the world using blockchain technology to promote the development of environmental protection, waste classification, environmental pollution reduction, energy management and emission monitoring (hereinafter referred to as HbG ecosystem) 。

Catalog

CONTENTS

HBG introduce

Block network

data structure

ecosystem

Prospects

HBGChain

Definition of blockchain

Blockchain is a distributed ledger, a technical solution to collectively maintain a reliable database by decentralizing and trusting.

From a data point of view

Blockchain is a distributed database that is almost impossible to change. The "distributed" is not only reflected in the distributed storage of data, but also in the distributed records of data (i.e. jointly maintained by system participants).

From a technical point of view

Blockchain is not a single technology, but the result of the integration of multiple technologies. These technologies are combined with new structures to form a new way of data recording, storage and expression.

「 Dynamics of blockchain 」

International authoritative magazines such as the economist, Harvard Business Week and Forbes magazine have successively reported that blockchain technology will affect the world.

R3, a start-up company, has established a blockchain alliance with 42 top banks in the world, including JPMorgan Chase, Bank of America, HSBC, Citibank, Wells Fargo, Mitsubishi UFJ Financial Group, Barclays Bank, Goldman Sachs, Deutsche Bank, etc.

HBGChain

HbG ecosystem is a habit cultivation application dedicated to environmental protection. It uses the distributed technology of blockchain to realize the new mode of domestic waste classification and treatment. Through online tasks, it can effectively distribute the living garbage to the masses and members, promote the development of renewable resources industry, organically combine garbage treatment and protect the environment The reasonable utilization of waste classification and renewable resources can promote the harmonious development of human and environment.

Block Nekwork

Blockchain

B
L
O
C
K

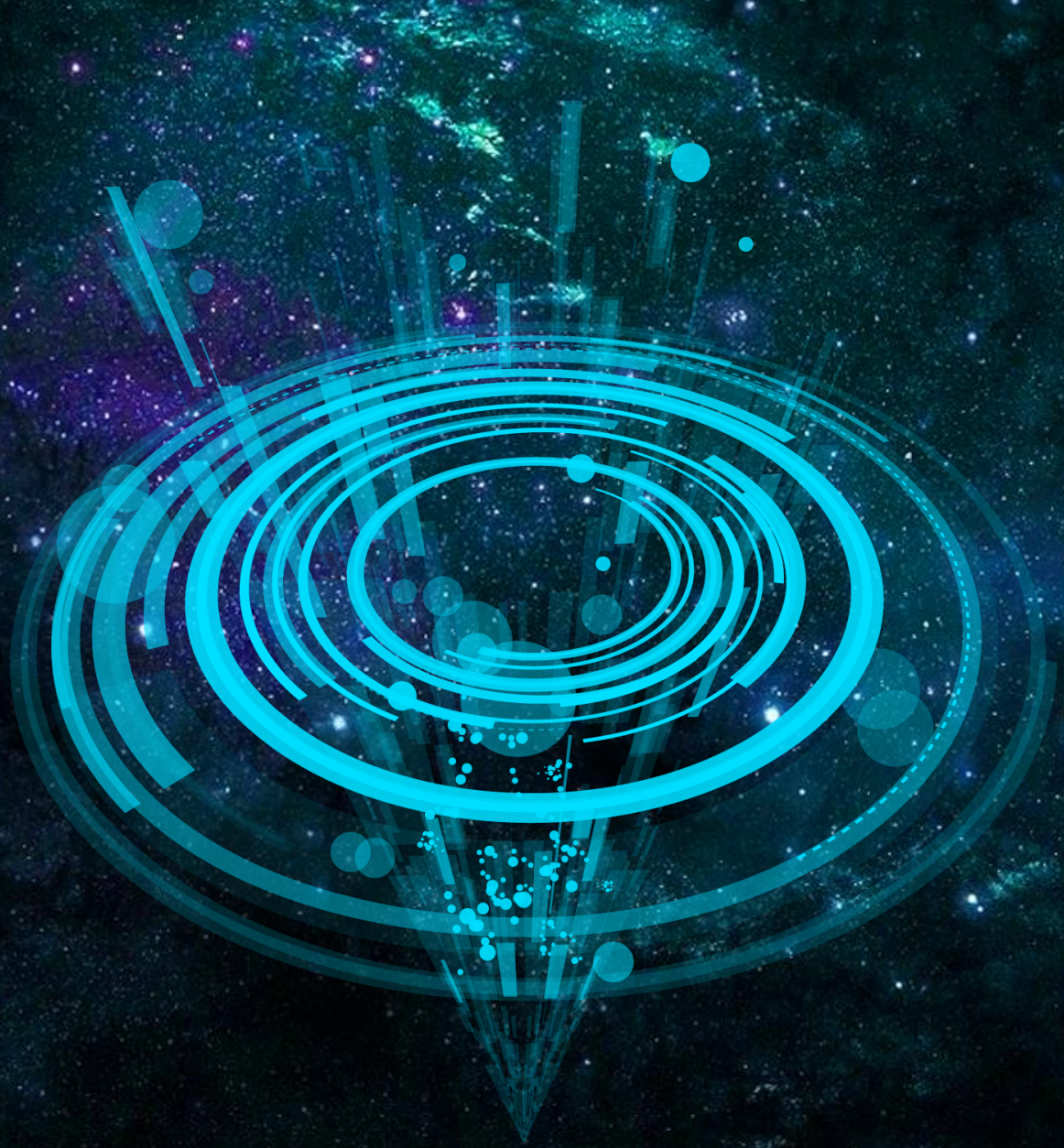
working principle

When sending a message, the sender uses a hash function to generate the message digest from the message text, and then encrypts the digest with its own private key. The encrypted digest will be sent to the receiver as the digital signature of the message and the message. The receiver first uses the same hash function as the sender to calculate the message digest from the received original message

digital signature

Digital signature involves a hash function, the sender's public key and the sender's private key. Digital signature has two functions: one is to confirm that the message is indeed signed and concurrent by the sender. Second, digital signature can determine the integrity of the message.

Blockchain



SHA256

An encryption algorithm for hash value.

working principle

Entering any string of data into sha256 yields a 256 bit hash value (hash value). Its characteristics: the same data input will get the same results. If the input data changes slightly (for example, a 1 becomes 0)

Merkle Tree

A hash binary tree that can be used to quickly verify the integrity of large-scale data. In HbG network, Merkle tree is used to sum up all the transaction information in a block, and finally generate a unified hash value of all the transaction information in the block. Any change of the transaction information in the block will make the Merkle tree change.

working principle

The calculation method of non leaf node value is to combine all the child nodes of the node, and then hash the combination results to get the hash value.

Blockchain

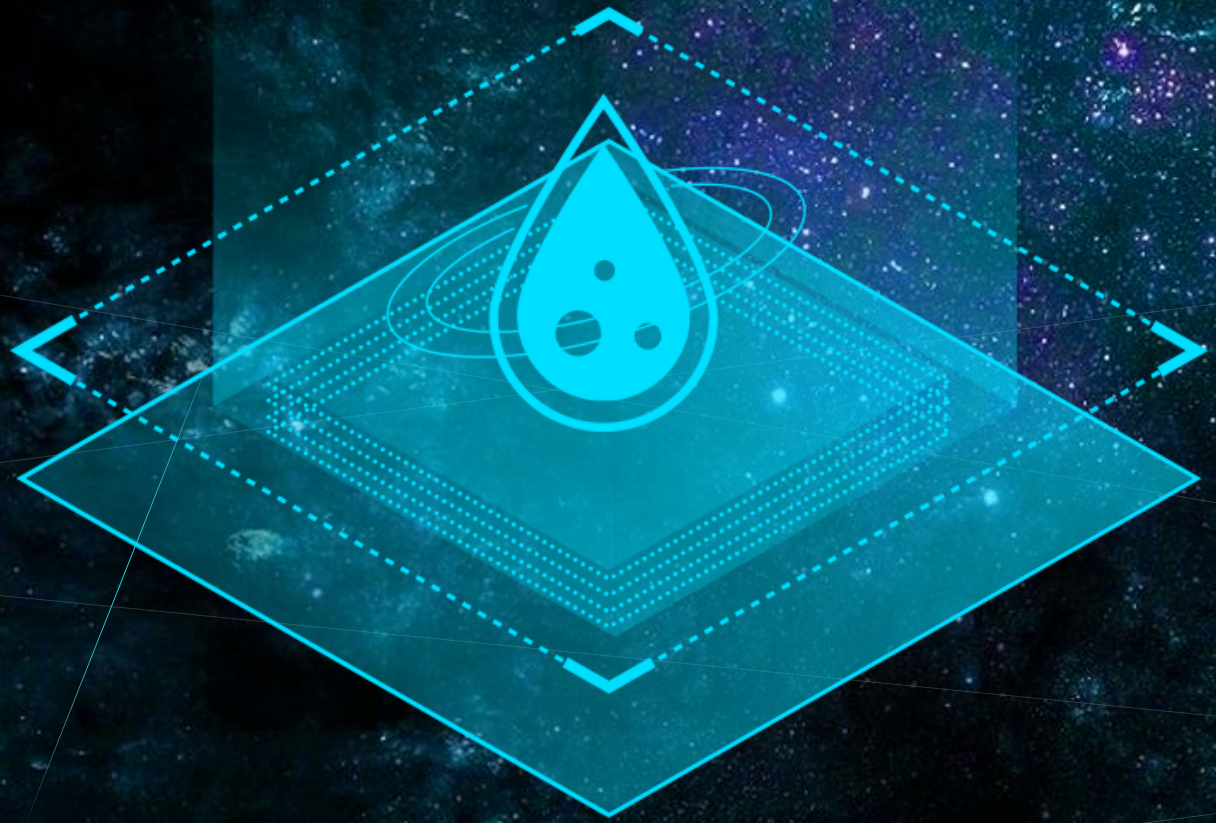
「 Node network 」

Any machine can run a complete HBG node. A complete HBG node includes the following functions: wallet, allowing users to trade on the blockchain network. The complete blockchain records all transaction history, ensures the security of historical transactions through special structure, and is used to verify the legitimacy of new transactions. It is generated by recording transactions and decrypting mathematical problems If the new block is successful, it can earn reward routing function, and then transmit transaction data and other information from other nodes to more nodes. Besides routing function, other functions are not necessary.

「 timestamp server 」

Most of them are used for comparison and verification. Timestamp server is an authoritative timestamp system based on PKI (public key cryptography infrastructure) technology, which provides accurate and reliable timestamp services to the outside world. It uses accurate time source, high strength and high standard security mechanism to confirm the existence of system processing data at a certain time and the relative time sequence of related operations, and provides basic services for time non repudiation in information system.

Blockchain



Node network step 1

Owner a uses his private key to sign a digital signature for the previous transaction (bitgoods source) and the next owner B, and appends the signature to the end of the currency to make a transaction receipt. Main points: B uses the public key as the receiver's address

Node network step 2

A will broadcast the transaction order to the whole network, and HBG will be sent to B, each node will receive the transaction information into a block. Key points: for B, the HBG will be displayed in the HBG wallet immediately, but it will not be available until the block is confirmed to be successful. At present, a HBG payment is successfully confirmed from payment to final confirmation, and it can only be confirmed after six blocks are confirmed

Transaction step 3

Each node obtains the right to create a new block by solving a mathematical problem, and strives for the reward of HBG (the new HBG will be generated in this process). Key points: the node repeatedly tries to find a value, so that after the value, the hash value of the last block in the blockchain and the transaction order are sent into the sha256 algorithm, the hash value x (256 bits) can be calculated to meet certain requirements For example, the first 20 bits are all 0, that is to find the solution to the mathematical problem. Thus, the answer is not unique

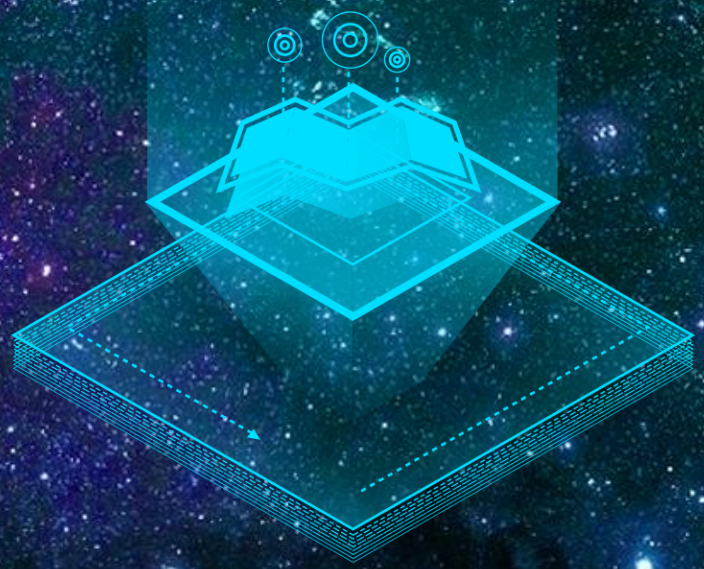
Transaction step 4

When a node finds the solution, it will broadcast all the time stamp transactions recorded in the block to the whole network, and check them by other nodes in the whole network
Important: timestamps are used to confirm that a particular block must exist at a certain time. In HBG network, the time is obtained from more than five nodes, and then the intermediate value is taken as the time stamp.

Blockchain

Step 5 of the transaction process

Other nodes in the whole network check the correctness of the block bookkeeping. If there is no error, they will compete for the next block after the legal block, thus forming a block chain with legal bookkeeping. Important: each block takes about 10 minutes to create. With the continuous change of the computing power of the whole network, the generation time of each block will be shortened with the increase of computing power, and extended with the decrease of computing power. The principle is to automatically adjust the generation difficulty of each block (such as reducing or increasing the number of 0 in the target value) according to the time difference (about two weeks) of the most recently generated blocks in 2016, so that the generation time of each block is 10 minutes.



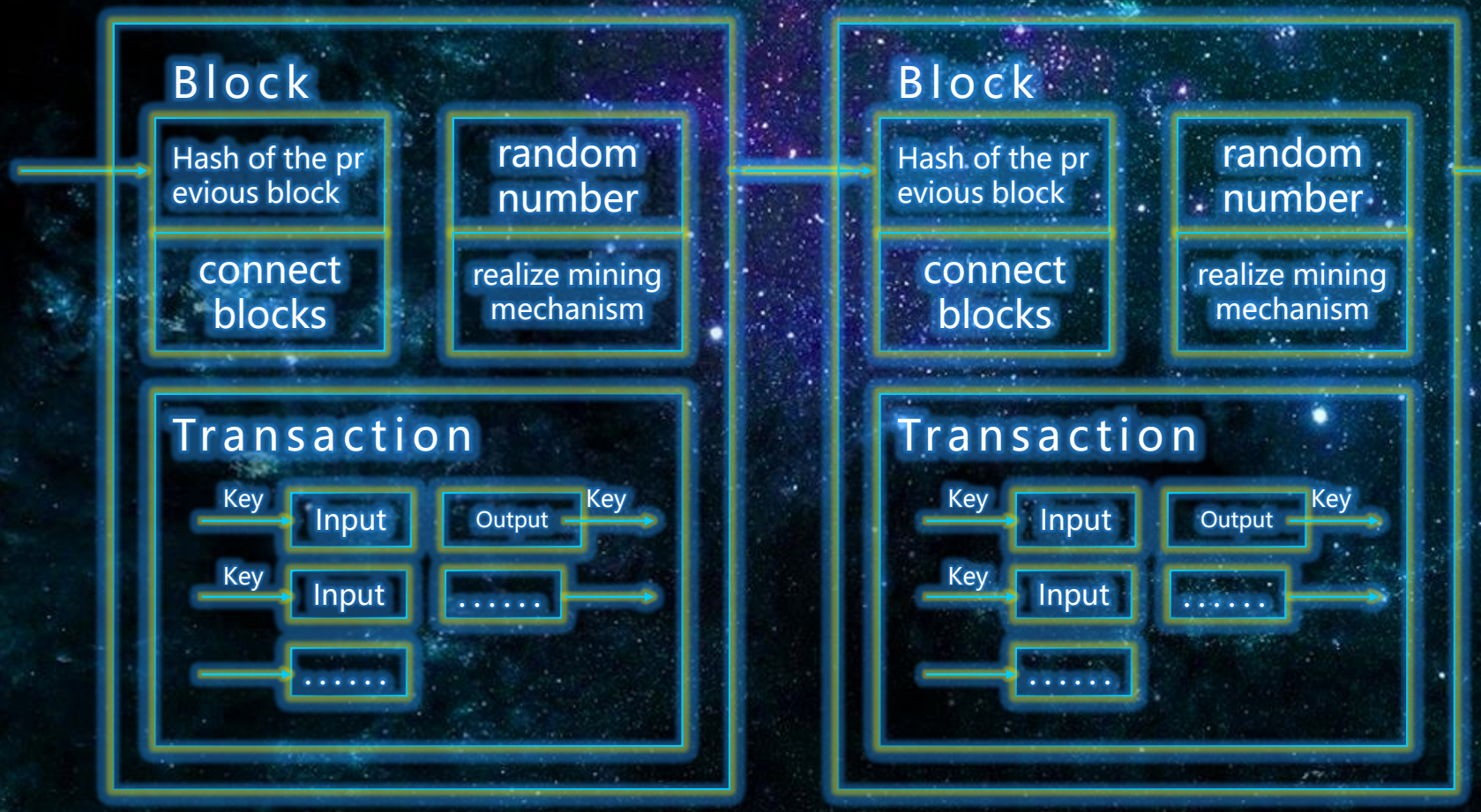
Data Structure

Data structure

HBGChain

HBG Blockchain organizes data in blocks. All transaction records of the whole network are stored in the unique blockchain of the whole network in the form of transaction sheet.

Data structure



Block

A block is a data structure that records transactions. Each block is composed of block head and block body. The block body is only responsible for recording all the transaction information in the previous period of time. Most of the functions of the blockchain are realized by block head.

Data structure

Block Header

- Version number, indicating the relevant version information of software and protocol
- The parent block hash value refers to the hash value of the parent block header in the referenced blockchain. Through this value, each block is connected end to end to form a blockchain, and this value plays an important role in the security of the blockchain
- Merkle root. This value is a value calculated from the hash value of all transactions in the block body and then hashed two or two levels. It is mainly used to check whether a transaction exists in the block
- Time stamp, recording the time of the block generation, accurate to seconds
- Difficulty value, the difficulty target of related mathematical problems in the block
- A random number (nonce), which records and decrypts the value of the answer to the relevant mathematical problem in the block

Data structure

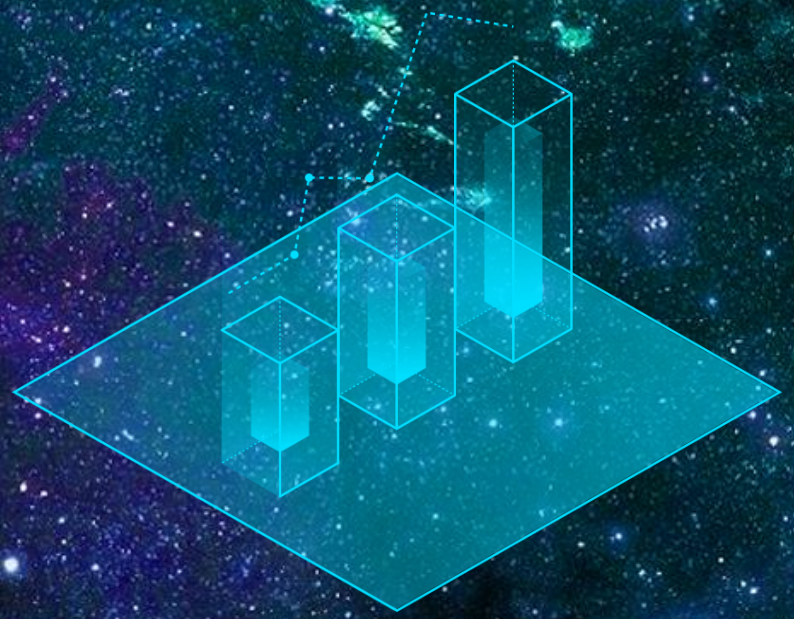
block formation process

1. After the current block is added to the blockchain, all miners immediately start to generate the next block

2. The transaction information in the local memory is recorded in the block body, and all the transaction information in the block is generated in the block body

3. A chunk of data just generated by sha256's header algorithm

4. The difficulty value field will be adjusted according to the average generation time of blocks in the previous period to cope with the changing total calculation amount of the whole network



Core Issues

Core issues

proof of work

- The block header contains a random number, making the random hash value of the block appear the required number of 0. The node tries to find the random number repeatedly, so it constructs a workload proof mechanism.
- The essence of workload proof mechanism is one CPU one v ote, and the "majority" decision is expressed as the longest c hain, because the longest chain contains the largest workloa d. If most CPUs are controlled by honest nodes, the honest c hain will extend at the fastest speed and surpass other comp etitive chains. If an existing block is to be modified, the attac ker must redo the workload of the block plus the workload o f all blocks after the block, and finally catch up with and surp ass the workload of honest nodes.

Core issues

In the same period of time, more than one node in the whole network can calculate the random number, that is, multiple nodes will broadcast their respective packaged temporary blocks in the network (all are legal).

Bifurcation

If a node receives multiple subsequent temporary blocks for the same preceding block, it will establish branches on the local blockchain, and multiple temporary blocks correspond to multiple branches. The deadlock will be broken until the next workload is proved to be found, and one of the chains is proved to be a longer one, then the nodes working on the other branch chain will switch camp and start to work on the longer chain. Other branches will be completely abandoned by the network.

Solution

- On the basis of blockchain and Internet, HBGChain can put forward better solutions to various major environmental protection problems, help the general public improve their environmental habits, establish energy-saving awareness, reduce the "three wastes" emissions of enterprises, improve the recycling efficiency of wastes, and comprehensively monitor and analyze all known and valuable energy use in the world Resource recycling, waste recycling, and important data of global ecological change.
- HBGchain's mission is to connect and transform all renewable energy. As a part of nature, with the help of HbG system, people will re integrate natural ecology and humanistic ecology. The world of heaven and earth coexists with me, and the world of everything and I will be realized. Mankind will have a better tomorrow!

Prospects

Prospects

Demand

- Financial, medical, notarization, communication, supply chain, domain name, voting and other fields are beginning to realize the importance of blockchain and try to connect technology with the real society.

Investment

- The supply of investment funds for blockchain is gradually rising, the investment enthusiasm of venture capital is also rising, and the investment density is increasing. The supply of funds on the supply side is expected to promote the further development of technology.

Market

- Blockchain can become a market tool to help the society reduce the platform cost and make the intermediary organization become the past; the blockchain will promote the shift of the focus of the company's existing business model, and is expected to accelerate the development of the company.

Prospects

Technology

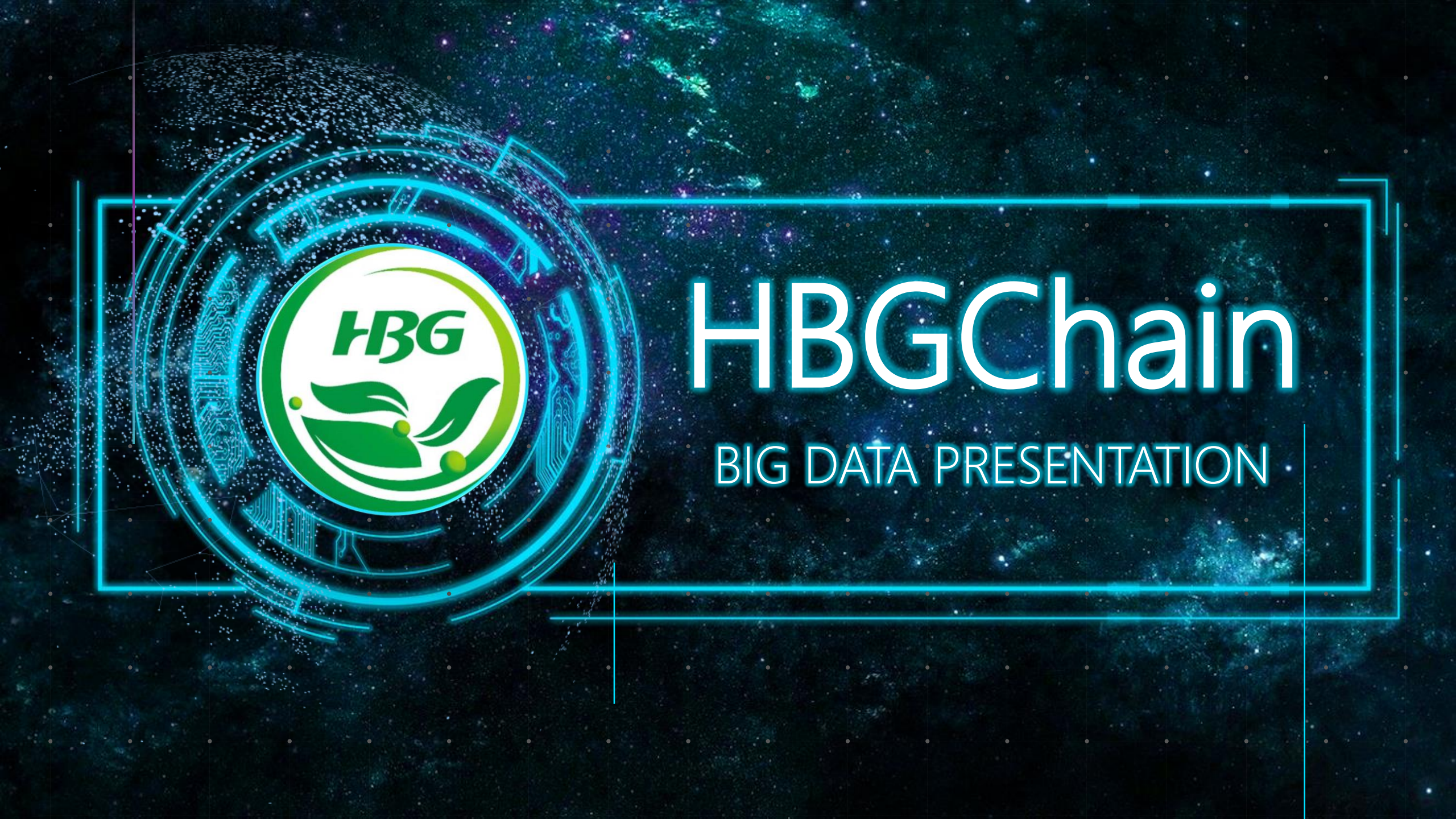
HBGchain is expected to promote the transformation of data recording, data dissemination and data storage management; blockchain itself is more like an open source protocol at the bottom of the Internet, which will touch or even completely replace the underlying basic protocols of the Internet in the near future.

Social Structure

HBGchain technology is expected to integrate law and economy, completely subvert the original social regulatory model; organizational form will change because of it, and blockchain may eventually lead people to a distributed and autonomous society

Mission

HBG means innumerable oases, containing the deterioration of the earth's environmental resources, and creating a harmonious future between human beings and nature. To this end, we are committed to environmental protection, sustainable use of renewable resources, promote waste reduction, build beautiful oases in every community that is troubled by environmental problems such as pollution and emissions, and bring distributed energy management technology into our common people's side, making contributions to the construction of green ecological communities.


HBG
HBGChain
BIG DATA PRESENTATION