BSG

Whitepaper

TABLE OF CONTENTS

Blockchain

ORIGIN

The blockchain originated from Bitcoin. On November 1, 2008, a self-proclaimed Satoshi Nakamoto published the article "Bitcoin: A Peer-to-Peer Electronic Cash System", which elaborated on P2P network technology, The architectural concept of electronic cash system such as encryption technology, time stamp technology, blockchain technology, etc., which marks the birth of Bitcoin. Two months later, the theory entered into practice, and the first genesis block with serial number 0 was born on January 3, 2009. A few days later, on January 9, 2009, a block with serial number 1 appeared and was connected with the genesis block with serial number 0 to form a chain, marking the birth of the blockchain.

In recent years, the world's attitude towards Bitcoin has been ups and downs, but blockchain technology, one of the underlying technologies of Bitcoin, has been paid more and more attention. In the formation process of Bitcoin, the block is a storage unit that records all the communication information of each block node within a certain period of time. Each block is linked through random hashing (also called hash algorithm), and the next block contains the hash value of the previous block. The result is called a blockchain.

DEFINITION

What is blockchain? From a technological point of view, blockchain involves many scientific and technological issues such as mathematics, cryptography, Internet and computer programming. From the application point of view, in simple terms, blockchain is a distributed shared ledger and database, which has the characteristics of decentralization, non-tampering, full trace, traceability, collective maintenance, openness and transparency. These features ensure "honesty" and "transparency" of the blockchain, laying the foundation for creating trust. The rich application scenarios of the blockchain are basically based on the fact that the blockchain can solve the problem of information asymmetry and realize the cooperative trust and action among multiple subjects.

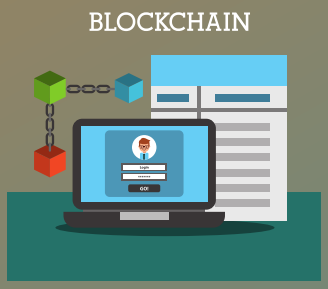
What is blockchain? From a technological point of view, blockchain involves many scientific and technological issues such as mathematics, cryptography, Internet and computer programming. From the application point of view, in simple terms, blockchain is a distributed shared ledger and database, which has the characteristics of decentralization, non-tampering, full trace, traceability, collective maintenance, openness and transparency. These features ensure "honesty" and "transparency" of the blockchain, laying the foundation for creating trust. The rich application scenarios of the blockchain are basically based on the fact that the blockchain can solve the problem of information asymmetry and realize the cooperative trust and action among multiple subjects.

The original English version of the Bitcoin white paper does not actually use the word blockchain, but instead uses chain of blocks. In the earliest Chinese translation of the Bitcoin white paper, the chain of blocks was translated into a blockchain. This is the earliest appearance of the Chinese word "blockchain"

Features

Decentralization

Blockchain technology does not rely on additional third-party management agencies or hardware facilities, and there is no central control. Except for the self-contained blockchain itself, through distributed accounting and storage, each node realizes information self-verification, transmission and management. Decentralization is the most prominent and essential feature of blockchain.



Openness

The foundation of blockchain technology is open source. In addition to the encrypted private information of transaction parties, blockchain data is open to everyone. Anyone can query blockchain data and develop related applications through public interfaces. System information is highly transparent.

Independence

Based on consensus specifications and protocols (similar to various mathematical algorithms such as the hash algorithm adopted by Bitcoin), the entire blockchain system does not rely on other third parties, and all nodes can automatically and securely verify and exchange data within the system without the need for any human intervention.

Security

As long as 51% of all data nodes cannot be controlled, network data cannot be manipulated and modified arbitrarily, which makes the blockchain itself relatively safe and avoids subjective and artificial data changes.

Features

Anonymity

Unless required by legal regulations, technically speaking, the identity information of each block node does not need to be disclosed or verified, and information transmission can be carried out anonymously.

Core technologies

Distributed ledger

Distributed ledger means that transaction accounting is completed by multiple nodes distributed in different places, and each node records a complete account, so they can all participate in monitoring the legality of the transaction, and at the same time, they can jointly testify for it.

Different from traditional distributed storage, the uniqueness of blockchain distributed storage is mainly reflected in two aspects: First, each node of the blockchain stores complete data according to the block chain structure, and traditional distributed storage Generally, the data is divided into multiple copies according to certain rules for storage. Second, the storage of each node in the blockchain is independent and has the same status, and relies on the consensus mechanism to ensure the consistency of storage, while traditional distributed storage generally synchronizes data to other backup nodes through the central node. No node can record the ledger data alone, thus avoiding the possibility of a single bookkeeper being controlled or bribed to keep false accounts. There are also enough accounting nodes. In theory, unless all nodes are destroyed, the account will not be lost, thus ensuring the security of the account data.

Features

Asymmetric encryption

The transaction information stored on the blockchain is public, but the account identity information is highly encrypted and can only be accessed with the authorization of the data owner, thus ensuring data security and personal privacy.

Consensus mechanism

The consensus mechanism is how to reach all the accounting nodes to determine the validity of a record. This is a means of identification and preventing tampering. The blockchain proposes four different consensus mechanisms, which are suitable for different application scenarios and strike a balance between efficiency and security.

The consensus mechanism of the blockchain has the characteristics of "minority obeys the majority" and "everyone is equal", in which "minority obeys the majority" does not completely refer to the number of nodes, but also the computing power, the number of shares or other computers that can be compared. Feature amount. "Everyone is equal" means that when a node meets the conditions, all nodes have the right to give priority to the consensus result, which may become the final consensus result after being directly recognized by other nodes. Taking Bitcoin as an example, the proof of work is used. Only when more than 51% of the accounting nodes in the entire network are controlled, it is possible to forge a non-existing record. When enough nodes join the blockchain, this is basically impossible, thus eliminating the possibility of fraud.

Smart contracts

Smart contracts are based on these trusted and immutable data, and can automatically execute some pre-defined rules and terms. Taking insurance as an example, if everyone's information (including medical information and risk occurrence information) is true and credible, then it is easy to automate claims settlement in some standardized insurance products. In the day-to-day business of insurance companies, although transactions are not as frequent as in the banking and securities industries, the reliance on trusted data continues unabated. Therefore, the author believes that the use of blockchain technology, from the perspective of data management, can effectively help insurance companies improve their risk management capabilities. Specifically, it is mainly divided into the risk management of policyholders and the risk supervision of insurance companies.

SMART CONTRACT

SMART CONTRACT CONCEPT

Smart contract are a very popular concept at the moment, so what are smart contracts? What problems can smart contracts solve?

In 1997, Nick Szabo wanted to use a distributed ledger to store contracts, thus using the concept of smart contracts for the first time, long before the birth of Bitcoin.

Nick Szabo is a computer scientist, jurist and cryptographer known for his research on digital contracts and digital currencies. In 1989, he graduated from the School of Computer Science and Engineering at the University of Washington with a BS in Computer Science, and at the George Washington University School of Law with a LL.B. He was also awarded an honorary professorship by the Universidad Francisco Marroquín. Szabo coined the term and concept of "smart contracts," initially to design what he called "highly evolved" contract law and customary algorithms into e-commerce agreements between strangers on the Internet. "Smart contracts" are the main feature and programming language of cryptocurrencies. Szabo insightfully proposes that the minimum guarantee of micropayments is determined by people's psychological (expected) transaction costs.

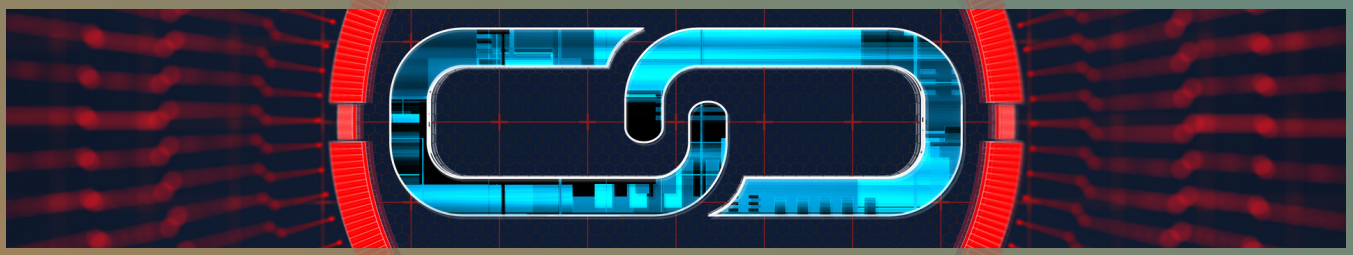
Smart contracts are very similar to today's contracts, the only difference is that smart contracts are completely digital. In essence, a smart contract is a small piece of computer program stored in a blockchain network. We use a crowdfunding platform as an example to illustrate how smart contracts work: product teams can create their own projects on it, set a crowdfunding goal, and To raise funds from those who support their ideas, a crowdfunding platform is a third-party platform between the product team and the backers, which means that both parties trust the platform to handle their funds properly. If the crowdfunding is successful, The product team trusts the platform to transfer crowdfunding funds to them, and similarly, the backers trust the platform to send their funds to the product projects they support. If the crowdfunding goal is not met, investors trust the platform to return the money. In this process, both the product team and its supporters must trust the crowdfunding platform. We can use smart contracts to build a similar system, but it does not require the existence of a third-party platform.

SMART CONTRACT

How to create such a platform?

We can write a smart contract to hold the received funds until the crowdfunding goal is reached, and with this program, the backer transfers the funds to the smart contract. If the crowdfunding is successful, only the contract will automatically transfer the funds raised to the product team. If the crowdfunding goal is not achieved, the money will be automatically returned to the supporters, isn't it great?

Since smart contracts are stored in the blockchain, all this information is distributed, this technology guarantees that no one can control the money, why? Since smart contracts are stored in the blockchain, it has some interesting features, they cannot be tampered with and are distributed. Immutable means that once a smart contract is created, it cannot be modified, so no one can tamper with your contract behind your back.



Distributed means that your contract needs to be verified by everyone in the network, so it is impossible for one person to force the contract to release funds, because others will find your attempt and mark it as invalid, so it is basically impossible to tamper with the contract .

Smart contracts can have many applications, not just in crowdfunding. For example, banks can use it to issue loans or provide automatic payments, insurance companies can use it to process specific claims, postal companies can use it to deliver settlements, and so on.

There are already some blockchain platforms that support smart contracts. The largest platform is Ethereum, which was created to support smart contracts. Smart contracts can be written in a programming language called Solidity, which is specially Invented for Ethereum, its syntax is similar to JavaScript. It is worth mentioning that Bitcoin also supports smart contracts. Compared with Ethereum, Bitcoin has more limitations.

Smart Contract Definition

The definition is short: a smart contract is a set of promises defined in digital form, including agreements on which contract participants can execute those promises.

The digital form means the contract has to be written in computer-readable code. This is necessary because as long as the parties reach an agreement, the rights and obligations established by the smart contract are executed by a computer or computer network.

To explain further:

reach an agreement

When will the participants of the smart contract reach an agreement? The answer depends on the specific smart contract implementation. Generally speaking, a contract is discovered when a party commits to its execution by installing the contract on the contract hosting platform.

Contract execution

What "execute" really means also depends on the implementation. Generally speaking, implementation means active implementation through technical means.

Smart Contract Definition

Computer readable code

In addition, the specific "digital form" required for a contract is very dependent on the protocol the parties agree to use.

A protocol is a technical implementation on which a contract promise is fulfilled, or the contract promise fulfillment is recorded. The choice of which protocol to use depends on many factors, the most important being the nature of the asset being traded during the execution of the contract.

Take the example of a sales contract again. Suppose, the parties agree to pay for the goods in Bitcoin. The chosen protocol will obviously be the Bitcoin protocol, on which smart contracts are implemented. Therefore, the "digital form" that the contract must use is the Bitcoin scripting language. The Bitcoin Scripting Language is a non-Turing-complete, imperative, stack-based programming language similar to Forth.

A smart contract is a "computer transaction agreement that enforces the terms of the contract". Blockchain-based smart contracts are visible to all users on the blockchain. However, this leaves all vulnerabilities, including security holes, visible and may not be fixed quickly.

Such attacks are difficult to resolve quickly, for example, the June 2016 vulnerability in The DAOEther cost $50 million while developers tried to reach a consensus solution. The DAO's procedures had a period of delay before the hackers removed the funds. A hard fork of the ethereum software completed the recovery of attacker funds before the time limit expired.

Issues in ethereum smart contracts include contract programming Solidity, compiler bugs, ethereum virtual machine bugs, attacks on the blockchain network, invariance of program bugs, and other undocumented attacks.

Smart Contract Security Audit

Smart contract auditing is actually the process of carefully studying the code, that is, deploying the contract to the main network of Ethereum (assuming this project is running on Ethereum), reviewing it for errors, vulnerabilities and risks, and then discussing How to improve. Because once published, the code can no longer be modified.

An important part of the "smart contract" blockchain project, if the loopholes in the contract are exploited by the perpetrators, the token will be stolen and often cannot be recovered, and the development history of the wrong code.

Why you need a security audit?

Hackers use loopholes to invade the system, causing huge losses to smart contract users. All smart contracts contain critical vulnerabilities.
The Dao project was stolen due to a technical flaw in the smart contract code Smart contract code lost due to human error.
External audits of smart contracts will help identify bugs and vulnerabilities in the code and check program logic.

Test Methods

In order to check the security of the contract, various attacks are generally tested to ensure the security of the contract. Such as Reentrancy attack, Over and under flows, Replay attack, Reordering attack, Short address attack. Review evaluation and optimization opinions

There are the following ways to evaluate projects through smart contract audits

STEP 01

Critical issue (critical, critical): 0

Vulnerabilities and exploits that result in theft of funds, lock access to funds (which cannot be recovered), or cause any other loss of funds to be transferred to any party; high-priority unacceptable bugs deployed on mainnet; critical to owners, customers, or investors warn.

STEP 02

Errors, errors and warnings (medium, low severity): 0

Errors that could trigger contract failures, which can only be further recovered by manually modifying the contract state or replacing the contract entirely; lack of necessary security precautions; other warnings to owners and users.

STEP 03

Likelihood of optimization (low severity): 0

Possibility to reduce transaction and data storage costs for smart contracts.

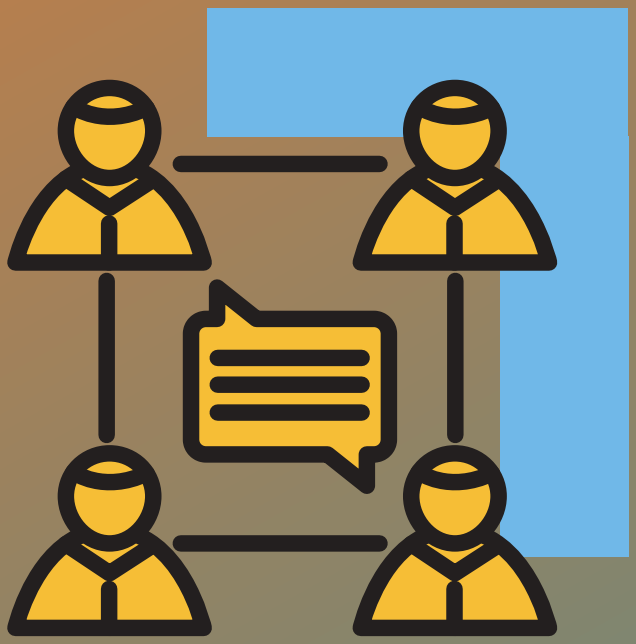
STEP 04

Comments and suggestions (very low severity): 0

Tips and tricks, all other questions and suggestions, and bugs that do not affect smart contract functionality.

According to the audit conclusion, make optimization suggestions for recording statistical parameters in the blockchain.

Smart Contract Classification



Smart contracts are written in the form of code on the public chain, and are executed in strict accordance with the established logical terms. Only when the execution conditions are met can the terms be triggered, and the code is the law. Therefore, the current smart contract types are mainly Ethereum public chain, TRON public chain, Binance public chain, EOS public chain, etc. Our BSG blockchain split game is a smart contract system built on the TRON public chain.

TRON public chain

Official statement of TRON: TRON is committed to promoting the decentralization of the Internet and is committed to building infrastructure for the decentralized Internet. Its TRON protocol is one of the world's largest blockchain-based decentralized application operating system protocols, providing highthroughput, high-expansion, and high-reliability underlying public chain support for the operation of decentralized applications on the protocol. TRON also provides better compatibility for Ethereum smart contracts through an innovative pluggable smart contract platform.

Since July 24, 2018, TRON has acquired BitTorrent Inc., an internet technology company based in San Francisco. BitTorrent Inc. is designed with distributed technology that scales efficiently, remains intelligent, and enables creators and consumers to control their content and data. More than 170 million people use products developed by BitTorrent Inc. every month. BitTorrent Inc.'s protocol can transport 40% of the world's internet traffic every day.

Features

01 HIGH THROUGHPUT

High throughput is achieved by improving the TPS in TRON, and its practicality in daily use has surpassed that of Bitcoin and Ethereum.

02 SCALABILITY

Based on good scalability and efficient smart contracts, applications can be deployed in more ways in TRON, and TRON can support a large number of users.

03 HIGH RELIABILITY

TRON has a more reliable network structure, user assets, intrinsic value, and a higher degree of decentralization consensus brings an improved reward distribution mechanism.

TRON Smart Contract

A TRON smart contract is a computable transaction agreement that executes the contract terms, that is, a smart contract is an algorithmic contract and an executable code contract that reflects the contract. The parties agree to determine the content of the contract, conclude the contract, and perform the contract (execute the code) according to a certain computer algorithm. Behavior is a special kind of software. The basis and guarantee of the contract spirit is the law, and the contract code must contain legal relationships and interest transactions. Therefore, smart contracts are a fusion of information technology and law. Only when the two are well combined can the second-generation contract described above be realized. smart contracts and third-generation "code is law" smart contracts.

TRON smart contracts are deployed on the blockchain, and their contract content is naturally open and transparent. Similarly, because it is deployed on the blockchain, the content of the smart contract cannot be modified. The smart contract running on the blockchain is also jointly maintained by the network nodes on the blockchain. As long as the blockchain exists, the smart contract will be can run forever.

Wavefield Energy and Bandwidth

In fact, when each of us creates a TRON wallet, there will be a certain amount of free bandwidth. What we actually lack is the CPU resources that are consumed by the creation and operation of smart contracts, that is, "energy". Because smart contracts take time to run in a virtual machine (VM), the time consumed in the system is calculated in microseconds, while CPU resources are consumed in the form of energy, which means 1 Energy == 1 microsecond. If the contract takes 100 microseconds to execute in the VM, it needs to consume 100 Energy, but the total amount of CPU resources provided by the TRON network in 24 hours is 50,000,000,000 Energy.

TRON also has the concept of RAM and CPU, namely "Broadband" and "Energy". TRON-based DApps can choose to consume the player's energy or choose to consume the developer's energy when deploying the contract. If it consumes the player's energy and you happen to have not mortgaged TRX, then when you play the DApp, the smart contract will automatically deduct it. The corresponding TRX is dropped as a handling fee, which is why many players find that the TRX they actually get does not match the TRX they should get when they play DApps.

If you still want to continue playing, you should immediately mortgage broadband and energy. You don't need to mortgage too much, just mortgage according to your own needs.

Rules for obtaining bandwidth and energy by freezing TRX in wallets.

Obtain bandwidth by freezing TRX, and the quota is the total amount of TRX frozen for obtaining bandwidth / the total amount of TRX frozen for obtaining bandwidth * 43,200,000,000. That is, all users equally share the fixed amount of bandwidth according to the frozen TRX.

Energy can only be obtained by freezing TRX. The amount of energy obtained = TRX frozen for obtaining energy / total amount of TRX frozen for obtaining energy in the entire network * 50,000,000,000. That is, all users equally share the fixed amount of energy according to the frozen TRX.

Wavefield Energy and Bandwidth

Energy can only be obtained by freezing TRX, the energy obtained = TRX frozen for energy / the total number of TRX frozen for energy in the entire network * 100,000,000,000, which is based on the total number of frozen TRX fixed energy equally divided by all users.

For example, suppose the total amount of TRX frozen for energy in the current network is 1000_000_000 TRX, and an account freezes 1000 TRX, which is one millionth of the total and equals 32400 microseconds. If it takes 324 microseconds to execute the contract, then the user can trigger the contract 100 times.

Remark

- Since the total amount of frozen funds in the network and the frozen account funds may change at any time, the CPU resources owned by the account are not fixed.
- When freezing funds, bandwidth points and energy cannot be obtained at the same time. If you freeze TRX for bandwidth, your energy won't change.

Therefore, BSG chooses the TRON smart contract, as long as it pledges an appropriate amount of TRX, it can obtain enough energy, so that the smart contract operation will not incur any additional costs. Of course you can use our front page lease energy button to lease enough energy to operate the BSG system for a small amount of TRX. The experience is very good, and we look forward to realizing the freedom of wealth together here!

BSG Mathematical Model

BSG blockchain split game is a completely decentralized, open and transparent data, fair and just system for global players. After the most rigorous mathematical model deduction, it has the most rigorous control model + market operation mechanism + blockchain technology, and is committed to building the world's first blockchain decentralized split game platform.

This is a subversive and innovative system that can bring huge benefits to players around the world. This is an excellent opportunity to achieve financial freedom together. BSG stands for "trust, sincerity, and future". The future has arrived, and I look forward to walking with you!

Introduction to BSG Games

Level and Standard

Deposit 50 to 450 USDT

One Star Player

Deposit 500 to 950 USDT

Two Star Players

Deposit 1000 to 2000 USDT

Three Star Players

Personal deposits of 1,000 USDT (inclusive) or more, with a team of 50 players, the effective performance of one line in the team is at least 10,000 USDT, and the sum of the effective performance of all lines is more than 10,000 USDT (Note: Effective performance refers to team members Unblocked deposits in the account)

Four Star Players

personal deposit of 2,000 USDT, with a team of 200 players, the effective performance of one line in the team is at least 50,000 USDT, and the sum of the effective performance of all other lines is more than 50,000 USDT (Note: Effective performance refers to the unfrozen accounts of team members deposit)

Five Star Players

BSG Game Earnings

Income per cycle: the initial 15-day cycle, the fixed income per cycle is 22.5%, and then a 1-day freeze period is added for every 2 deposits after that, and the income will not increase until it increases to 45 days and no longer increases.

A total of 20 layers of benefits

Tier 1 5%

Tier 2 1%

Tier 3 2%

Tier 4 3%

Tier 5 1%

Tier 6 2%

1% for layers 7 to 10

0.5% for layers 11 to 20

One-star~Three-star player income

enjoy 1 layer of income, the following members complete the deposit release bonus

Four-star player income

enjoy 1-5 layers of income, of which 2-5 layers of income need to be released after the player completes the next cycle of deposits; enjoy the four-star bonus dividend (distributed once in 24 hours)

Five-star player income

Enjoy 1-20 layers of income, of which 2-20 layers of income need to be released after the player completes the next cycle of deposits, and the amount of income released from 6-20 layers needs a 1:1 new deposit before they can be withdrawn

TOP Award

Daily top inviter in the first tier shall be rewarded. If the top three have the same performance, they will be ranked according to the completion time. 1000USDT, 20% for the third place, up to 500USDT

Lucky Prize

Daily last 10 deposits shall also be rewarded and the prize pool will be allocated according to the proportion of the deposit amount of each account. If there are less than 10 depositor the prize pool will be allocated according to the proportion of the current number of places. If there is no entry on the day, the prize pool will be accumulated until the next day

Four-star award

4 star player shall evenly spread the pool money.

BSG game rules

Minimum 50 USDT, maximum 2000 USDT, in multiples of 50, the amount of each deposit must be greater than or equal to the previous deposit amount

Bonus is calculated based on the small amount of the deposit

After the deposit of the previous cycle expires, the deposit must be continued for the next cycle, and the amount of the deposit is greater than or equal to the deposit amount of the previous cycle, and then the unfrozen deposit can be withdrawn

add 1 day of freezing period for every 2 deposits, no increase in income, maximum increase of 45 days, no more increase.

30% of all income goes into split account (this amount is only used as a new account deposit), this account is set up with transfer and deposit functions, the transfer amount must be a multiple of 50, and there are no other restrictions; the deposit function is only The newly registered account can only be activated once, and this function cannot be used for the activated account. 70% of all earnings are used for withdrawals, no additional withdrawal fees

Fund allocation mechanism

Summary

To sum up, the BSG blockchain split game is a future that cannot be let down, and it is the expectation of all our players. We will all get rich benefits here. It is the most sincere and trustworthy. The mathematical model of this system and the precise simulation actuarial can run stably in the future, so take it seriously now and obtain stable and long-term benefits here. Our system is completely open, open, completely decentralized, and completely handed over to all players in the world. Players are autonomous, and players are the system.