Wabei Blockchain White Paper

Index

1. Introduction

Satoshi Nakamoto created Bitcoin and implemented a purely peer-to-peer electronic cash system. Bitcoin is not backed by any assets nor does it have intrinsic value. It is not issued by any central government or financial institution. Transactions in the bitcoin network can be sent directly from one party to another without going through a financial institution. Bitcoin has the following features:

1. It has no centralized issuer or controller.

2. Transactions can be sent between parties without going through a trusted third party.

3. A transaction's originating and receiving parties are anonymous.

4. No transaction can be reversed.

Since bitcoin's birth it has become the most popular electronic cash system worldwide. Although it presents a beautiful solution to the double-spending problem using a P2P network and creates a mechanism to transfer value between trustless parties over the internet it encounters three significant issues: centralization of hash power, security concerns with accounts, lost coins can never be retrieved.

The Wabei blockchain is a project that attempts to fix the aforementioned issues.

Among existing permissionless blockchains the biggest issue is centralization of hash power. Bitcoin's mining algorithm is based on SHA-256. A block's eighty-byte header is hashed twice with SHA-256 to a 256-bit (32-byte) value. It verifies this block's validity by comparing this 256-bit value to a nonce. This is known as proof of work. Although it works well and plays a crucial role it is prone to be attacked by centralized hash power which means that either large number of nodes can possibly cooperate to attack the network or a node with an extremely powerful hash rate can outperform other nodes. For the latter case it already comes true. Nowadays bitcoin's mining rigs are nearly all ASIC machines whose efficiency is thousands of times higher than that of a common desktop computer. Common computers which were used to mine bitcoins in the early years have been phased out by ASIC machines. This turns a mining activity into one that needs huge investment.

We think blockchain has huge potentials and is not just an electronic cash system. Bitcoin's lack of a Turing-Complete mechanism severely limits its adoption in wider areas. The Wabei project will be a permissionless blockchain with a Turing-Complete mechanism on which all transaction-based state machines can be built.

We will analyze several issues the current bitcoin network has in the following section.

2. Potential Risks with Bitcoin

The concept of decentralized crypto currency was created by Friedrich August von Hayek in one of his great works <<Denationalization of Money>> decades ago. But it is not until Satoshi Nakamoto who introduced bitcoin this decentralized coin became the first widely adopted global crypto currency.

Bitcoin's network is composed of nodes all of which work under a proof-of-work consensus. Transactions are digitally signed into a block which is generated every ten minutes. Blocks are chained with hash values to form a blockchain. A node with a higher hash rate has greater probabilities to mine a block.

Bitcoin is one of the most popular crypto currencies and one of the most robust blockchain systems.

2.1 Bitcoin Mining

In the bitcoin network a block is generated every ten minutes. Every block has a timestamp, a nonce, a reference (hash value) to its parent block and a list of all transactions which were completed after the last block in the blockchain. As ongoing transactions are hashed into the blockchain it will become increasingly longer. When a block is generated it needs to be verified by all the nodes. It needs to pass the tests of intrinsic validity. These tests include:

1. Validate its parent block. This examines whether the parent block it is linked to is valid.

2. Validate its timestamp. A valid timestamp should be greater than its parent block's timestamp and less than its parent block's timestamp plus two hours.

3. Validate its proof-of-work. This examines whether its proof-of-work is valid.

4. Set S[0] to its parent block's state.

5. Let TX denote a list of transactions and S[i] denote transaction i's state. We suppose there are n transactions. For each transaction i in 0……n-1, S[i+1] = APPLY(S[i], TX[i]). If a transaction fails the system will exit with an error. S[n] is the final state of the block.

An interesting part of the bitcoin validation mechanism is its proof-of-work. Bitcoin's proof-of-work prevents Sybil attacks. Each block is hashed with SHA-256 to a 256-bit hash value. If this hash value is less than the difficulty value which is dynamically adjusted by the bitcoin network this block will be a valid block and the bitcoin system will proceed otherwise the system will keep doing such calculations.

In general the bitcoin network resets the difficulty value every 2016 blocks to ensure a block is generated every ten minutes. When a block is generated and chained to its parent block in the blockchain the miner who mined this block will be rewarded with 12.5 bitcoins. In addition the block's total transactions' fee will be rewarded the miner too.

Although this system works it might still face the potential risk of double-spending. Here is how an attacker might initiate a double-spending attack.

1. Sender sends 100 BTC to receiver A to buy goods or services.

2. Sender waits for delivery of the goods or services.

3. Sender sends 100 BTC to himself right after he gets the goods or services.

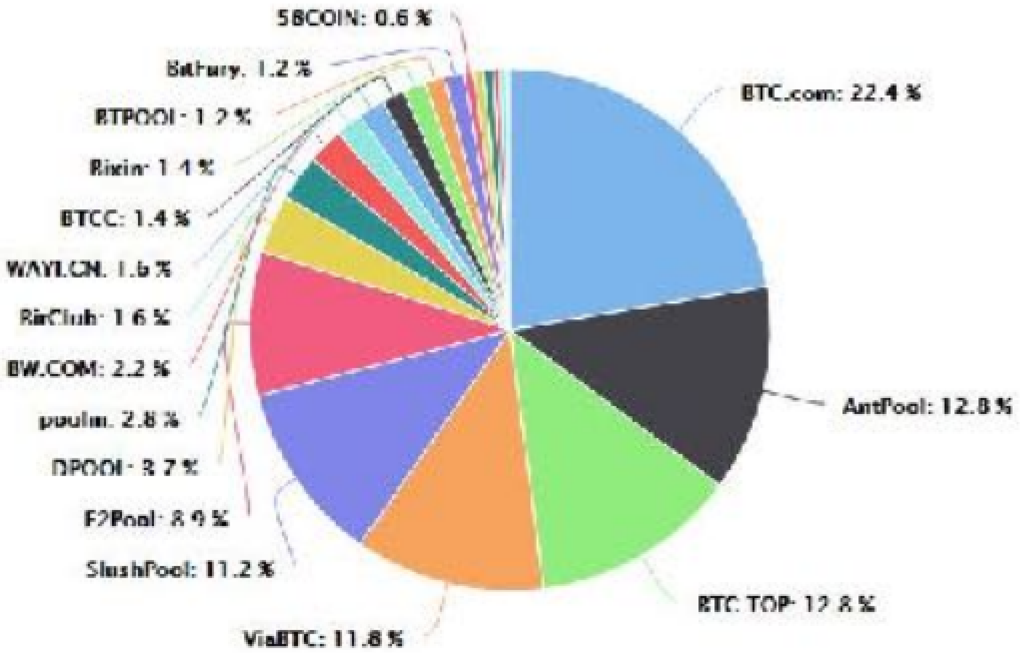
4. Sends tries to convince the bitcoin network that the transaction of 100 BTC to himself happened before the transaction of 100 BTC to receiver A.

We suppose the transaction of 100 BTC to receiver A is hashed to a block and the block's height is 270000. One hour later there will be five new blocks (270001 ~ 270005) generated after this block. Each of these five blocks will be either directly or indirectly linked to this block. When receiver A gets 100 BTC he will send the goods or services to the sender. We suppose what the sender pays for is a digital item which can be sent immediately from receiver A then right after receiver A gets 100 BTC he will send the digital item and the sender can get it right away. Then right after the sender receives the digital item he initiates a new transaction to send 100 BTC to his own address. If the sender merely broadcasts the latter transaction to the bitcoin network in no way can this transaction be hashed into a block because all miners will eventually find this is an invalid transaction. In order for the sender to hash this transaction in a block he needs to fork the original blockchain at height 269999 and generate a new block after the 269999th block and this new block will be the 270000th block in the forked chain. We suppose all honest miners will generate new blocks either directly or indirectly pointing to the 270005th block in the original blockchain and only the sender (attacker) will generate a new block pointing to the 269999th block in the forked blockchain. Up to this point the length of the forked chain is shorter than the original chain. In the bitcoin network the longest chain is considered the only valid blockchain. Therefore if the sender wants to make his forked chain the valid chain he has to make his forked chain surpass the original chain on which all honest miners work. Hence the sender has to have at least 51% of the bitcoin network's hash power.

2.2 Centralization of Hash Power

Bitcoin's price has risen tremendously since its birth. This has made bitcoin mining a huge business with rich profit. The mining business directly drives rapid development of ASIC rigs which gradually phase out general computers and GPU machines in this area. On the other hand in order to gain higher probabilities to mine bitcoins massive individual nodes began to cooperate and have formed big mining pools therefore individual mining can hardly compete with pool mining nowadays. It is estimated that the top three mining pools in the world altogether control 48% of the whole bitcoin network's hash power.

It is observed that in November 2013 the mining pool GHash.io launched multiple attacks on BetCoin Dice. A report released by Cornel University reveals that since June 3 2014 GHash controlled 51% of the whole bitcoin network's hash power for at least five times during one of which it had this hash power for at least 12 hours.



2.3 Loss of Private Key

A bitcoin address is a string that consists of 34 characters. Every address has a private key that consists of 64 characters. A bitcoin holder possesses a private key to his bitcoin address. The private key needs to be carefully stored. If the private key is lost all the bitcoins stored in the address will be permanently lost. When a bitcoin holder sends his bitcoins to another address he will need the private key to authenticate the transaction.

A hacker usually uses keylogger programs, malware or Trojan programs to steal a bitcoin holder’s private key. It becomes harder to prevent a system from being infected by these programs in a globally interconnected network.

Statistics reveal that there are nearly two million bitcoins stolen so far, which accounts for 9.5% of the total number of bitcoins. And this number keeps going up. The latest incident happened in April 13 2018 when hackers stolen 438 bitcoins ($3.3 million) from an Indian exchange, Coinsecure.

3. Wabei Blockchain

We propose a more secure and decentralized electronic cash system, known as Wabei. A significant improvement of this project is that it circumvents centralization of hash power which increasingly becomes a common trend for nearly all PoW based permissionless blockchains.

3.1 Pain Points in IT Infrastructure in Financial Industry

In the Wabei system an account consists of 20 bytes and it comprises the following fields:

1. nonce: a counter used to make sure each transaction can only be processed once.

2. balance: an account's current balance of Wabei coins.

3. contract code: the account's contract code, if present.

4. storage: the account's storage. It is empty by default.

The Wabei coin is the internal crypto-fuel of the Wabei system. There are two types of accounts: external accounts (controlled by private keys) and contract accounts (controlled by contract code). An external account doesn't have code. One can send messages from an external account by creating and signing a transaction. When a contract account receives a message call the code it contains will get activated and the code is allowed to read and write to internal storage and send other messages or create contracts in turn.

3.2 Mining

The Wabei system inherits a lot of features from the bitcoin system but it has significant differences. A Wabei block has a field known as "block number" and a field known as "difficulty". The process of finalizing a block in the Wabei network involves four stages:

1. Validate its parent block to which this block is linked.

2. Validate the timestamp. It should be greater than its parent block's timestamp but less than its parent block's timestamp plus fifteen minutes.

3. Validate the block number, difficulty, transactions root, uncles root and gas limit.

4. Validate proof-of-work.

5. Set S[0] to its parent block's STATE_ROOT.

6. Set TX to the block's transaction list. Suppose there are n transactions, for each transaction i in 0 … n-1 set S[i + 1] = APPLY(S[i], TX[i]). If any transaction's state change fails or the consumed gas exceeds the GASLIMIT the system will return with an error.

7. Set S[n] to S_FINAL and apply rewards to a beneficiary.

8. Verify if S_FINAL is equal to STATE_ROOT. If the two are equal the block is valid otherwise the block is invalid.

This validation process keeps and examines a block's all states and doesn't seem efficient. But actually the Wabei's finalization process is as efficient as bitcoin's because all states are saved in a tree structure and when a new block is generated only minor changes will be applied to the tree structure. Therefore most of a block's data is the same as its parent block and it is unnecessary to save a copy of every block's complete data. A "Patricia Tree" structure is introduced to the Wabei system to store all the blocks' data and this greatly saves storage.

3.3 Restriction of Pool Mining

Bitcoin mining is prone to be attacked by ASIC rigs and pool mining. Nowadays nearly all mining machines are ASIC rigs. Common desktops or machines with GPU in no way can compete with ASIC rigs. It is nearly impossible for individual miners to mine any bitcoins either. Most of individual miners have to join a pool which collects individual miners' hash power and tremendously increases the probability of successful mining. It is estimated that the top three bitcoin mining pools altogether control 48% of the bitcoin network's hash power. All these facts show a de facto trend: the bitcoin network's hash power is being centralized. And this trend can hardly be reversed.

In the Wabei system a hash value is generated based on one thousand random numbers. This algorithm restricts an ASIC rig's advantages. In short a Wabei node needs to utilize large amounts of RAM to mine coins while a bitcoin node doesn't need this much RAM thus making an ASIC rig much more efficient in mining. With this design a common desktop or laptop can run as a full Wabei node and be able to mine coins. Even when there exists a Wabei node with an extremely large hash rate a common computer still has good chances to mine coins successfully as long as the system's reward is less than (E + H)/E. In addition the mining algorithm requires a Wabei node to traverse the whole Wabei blockchain therefore a miner needs to store the whole blockchain. This restricts the advantages of a node with large hash power too. Furthur more the Wabei system specifically targets and limits an area with more than 48% of the total hash power of the Wabei network. When an area's hash power exceeds 48% of the total network's hash power the Wabei system will block entry of new nodes in that area to limit the growth of its hash power.

3.4 Wabei's Security Engine

1. The system picks a seed block and the distance between the latest block in the blockchain and this seed block will be used to generate a hash value for later calculations.

2. The seed block will be used to generate a 16MB pseudo-random cache.

3. This pseudo-random cache will be used to generate a 2GB dataset. A Wabei node needs to store this dataset. And this dataset grows linearly as the blockchain grows. The mining algorithm takes a specific part of the dataset and hash it to a hash value. This specific part of the dataset can be generated from the pseudo-random cache. This gives chances to a machine with low RAM to verify and mine a block.

The dataset is regenerated every thirty thousand blocks. A miner's work is to read through this dataset instead of performing heavy calculations which an ASIC rig can do with much higher efficiency. Thus with this algorithm a common computer can compete with an ASIC rig and has fair chances to mine a block successfully.

4. The mining algorithm in the Wabei system limits an ASIC chip to share RAM thus restricting its mining advantages.

4. Wabei Wallet

The Wabei system has a decentralized wallet, Token-S. When a wallet is created its private key and seed phrase are stored locally. If a user sends a transaction he will sign the transaction off-line. The whole process is decentralized. It minimizes chances of being attacked. Besides these the Token-S has the following features:

TOKEN-S

4.1 Smart Security Check

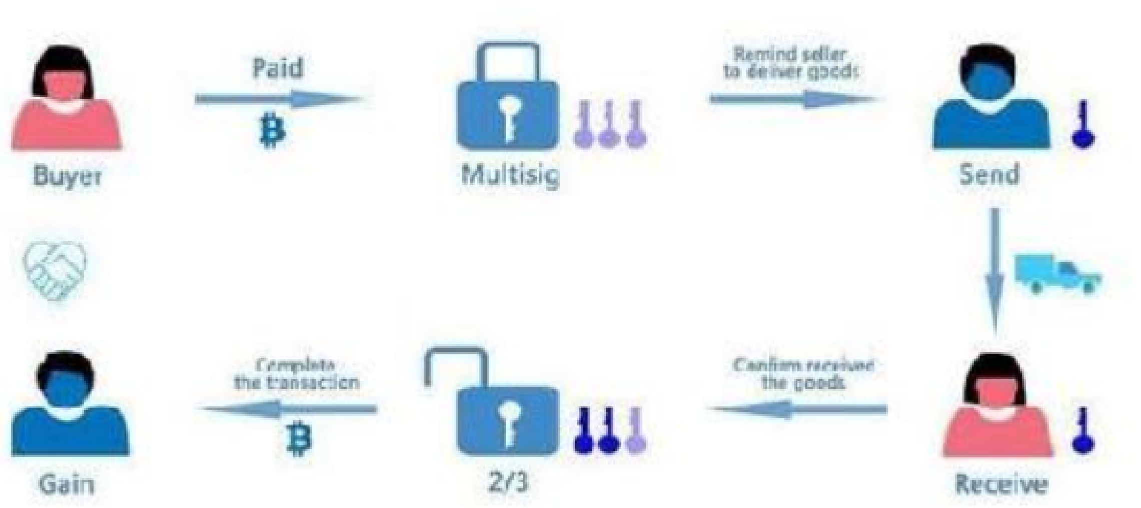
When a user logs into his Token-S wallet for the first time its smart security check mechanism will be launched to check if this login device has potential risks and alarm if it has. The login password is required to have at least six digits being numbers and letters. This password is used to restore the wallet's seed phrase and sign a transaction. This password is stored locally in the user's login device insteadhttps://www.baidu.com/ of any other device. Token-S doesn't provide a mechanism to restore a password therefore a user must keep his password safe and secure.

4.2 Multisig

A better way to protect a wallet is to use multisig. As for a typical bitcoin wallet each address has only one private key/digital signature. As for a multisig wallet at least multiple signatures/private keys are required to control an address. For instance an address is secured by three private keys thus in order to control this address at least two keys are needed for authentication.

For an online multisig wallet each private key should be stored in a different place and the wallet's UTC files are not allowed to be stored in the same place. With this design even if any one of these multiple keys is compromised the wallet is still safe.

There are two types of wallets: online hot wallets and cold wallets. Token-S combines both of their features.



4.3 Cold Wallet

With a cold wallet a user signs a transaction with his private key offline and sends the signed transaction online. The whole process keeps the private key isolated from any network. With Token-S when a user wants to send a transaction what he needs to do is to log in with his password, sign a transaction with "sendrawTransaction", move away the wallet file and send the transaction online. The whole process completely isolates the private key from the internet.

4.4 Verification with AI

When Token-S receives a transaction request it will use machine learning algorithms based on the request's transaction amount, frequency, history and sender ID to assess its potential risks. If the risks are low the request will be allowed to proceed otherwise it will send the request to professionals for further verification.

4.5 Secure and Trustworthy Trading Platform Compliant with KYC and AML

Token-S uses cutting-edge fraud-prevention technologies. It is a highly secure and trustworthy trading platform. All crypto assets on this platform are traceable and trading parties should be compliant with KYC (Know Your Client) and AML (Anti Money Laundry) policies. More advanced technologies such as fingerprint recognition and voice recognition will be incorporated into the system and make it more secure, safer and easy to use.

4.6 Privacy Protection

To protect a user's privacy Token-S limits the use of "getBalance". When a miner generates a block and needs to examine an account's balance the system only allows the miner to check whether the account's balance is enough to pay for gas instead of allowing the miner to get the exact balance of that account.

Existing Ethereum browsers e.g. etherscan.io expose an account's information to the public such that anyone could check the account's balance. No account has any privacy. This gives hackers chances to target and attack accounts which have large amounts of tokens.

Token-S blocks public access to an account therefore minimizes this risk and greatly protects an account's privacy. To accomplish this goal the Wabei team has a lot of work to do and is striving to make this happen.

4.7 Multi-Token Wallet and One-Station Solution

Token-S allows a user to import a wallet with a private key or a seed phrase. For now the wallet only supports the Wabei token and its smart contract tokens. ETH, BTC and other tokens are scheduled to be supported soon. That will give a user great convenience to manage all his crypto assets in just one wallet.

5. Miscellaneous

5.1 Applications

The Wabei system is not only a decentralized electronic cash system but a system with a Turing-Complete language that users can use to write smart contracts and decentralized applications.

There are three categories of applications that can be deployed on the Wabei system. The first one is financial applications. Users can deploy smart contracts to handle financial transactions such as crypto trading, derivatives trading, hedge fund trading and etc. The second is applications that rely on financial transactions. The third is non-financial applications such as online voting, decentralized governance and etc.

The Wabei team is now working closely with food industries. One ongoing project that the Wabei team is working on is to make a platform for an alcohol producer and later on this producer's alcohol products can be purchased with Wabei coins.

5.2 Token Sale and Distribution

The Wabei blockchain has an intrinsic currency, the Wabei token. It is mainly used as the internal crypto fuel.

The Wabei mainnet has been online for four months and 1.7 million WAB coins have been mined. The annually mined coins will be 5.2 million. After the Wabei coin gets listed on an exchange we will propose an annual issuance of 0.1875 million Wabei coins. This proposal will be voted by Wabei's miner community. On the other hand it is estimated that there will be 0.85% of existing Wabei coins lost or frozen due to various incidents annually. And the amount of lost and frozen coins will be nearly equal to the amount or newly mined coins annually thus making the total number of existing Wabei coins to be constant at 22 million.

The Wabei token will be sold at 1 BTC for 500 Wabei coins. Early birds will get discounts. The fund will used to support the project's development and community building.

One third of the total number of Wabei coins will be rewarded early developers and contributors with. Two thirds of the total number of Wabei coins will be used to fund the project's long term research and development.

5.3 Conclusion: A More Secure and Safer Electronic Cash System

The Wabei blockchain will have huge advantages over existing permissionless blockchains in trading security and circumventing centralization of hash power.

5.4 About Us

The Wabei project is funded and managed by Singapore Wabei Fund. For more details you can refer to:

Source Code: https://github.com/wabei

Home Site: www.bitwa.org

Email: service@bitwa.org