Phantom Technology

Yellow Book

Version 1.0.0

February 2019

I.Introduction

Blockchain is an important concept of Bitcoin. It is essentially a decentralized database. At the same time, as the underlying technology of Bitcoin, it is a string of data blocks generated by cryptography. The data block contains information about a network transaction, which is used to verify the validity of its information (anti-counterfeiting) and generate the next block.

The PHANTOM blockchain is the next-generation commercial-grade basic public blockchain, which aims to establish a ubiquitous trust network of value circulation, and is committed to creating a distributed business ecosystem with extensive digital trust, free value circulation, and mass shared applications. Through the core technologies such as innovative consensus algorithms, multi-chain structure of main chain-subchain, cross chain structure of main chain-main chain and developer-friendly smart contracts, the Internet infrastructure of ubiquitous value circulation is constructed. On the basis of the value representation and value transfer function of the blockchain, all types of user groups and partners are motivated to build a shared, win-win and autonomous industrial ecosystem by taking advantage of the pass for incentives and governance.

II.Intelligent Contract Engine

For mature blockchain technology systems, intelligent contract is a necessary feature and one of the main reasons why blockchain can be called disruptive technology. PHANTOM's intelligent contract is a piece of executable code stored on the blockchain book. It not only has complete Turing, rapid deployment, flexible call, reliable execution, but also provides a powerful eco-friendly execution environment engine PhVM (PHANTOM Virtual Machine). And it provides better support in performance, security, multi-language support, development friendly, application extensions and so on.

It is the improved implementation based on the technology of Google V8 and WebAssembly. And it can better meet the PHANTOM eco-friendliness needs. Google V8 is an open source JavaScript engine developed by Google. It can translate JavaScript code directly into binary machine code and be executed on a physical machine efficiently. WebAssembly (WASM) is a portable, load-efficient, platform-independent bytecode. The format can be executed on the platform at a speed close to the original speed. This is a totally new WEB standard, which is supported and formulated by several major companies such as Google, Apple,

Microsoft, and Mozilla. These two technologies can provide good functional support for PhVM, but they cannot be directly applied to the PHANTOM scenario, and cannot meet the requirements of PHANTOM in terms of contract execution security, interface permissions, contract interaction, exception handling and grammar checking. PhVM performs necessary and targeted function optimization, increases security check of contract execution, clarifies interface permissions, increases inter-contract interaction, and enhances exception handling mechanism and grammar security check. In addition, PhVM provides multi-language support such as JavaScript, C, C++, Python, Go, etc. It can run across platforms. The underlying interface is rich and extensible. And it has an independent sandbox environment to ensure PHANTOM smart contracts are safely executed in an isolated environment.

III.Book Structure

The book structure is an important form of blockchain data storage. As the blockchain application scenario becomes more and more complex, the requirements for the structure design of the book are getting higher and higher. PHANTOM's book structure mainly includes multi-asset account structure, global block structure, atomic transaction structure, efficient book data storage and multi-signature joint account.

Multiple operations that are interrelated form a transaction as a whole, either fully executed or not executed at all, which is a common real-world asset trading requirement. PHANTOM adds a sub-operation array attribute to the transaction structure, which can put one or more asset sub-operations into the same transaction execution. Failure of any sub-operation will result in the failure of the overall transaction and trigger a rollback of the transaction that has been performed, so that to avoid affecting the relevant account.

PHANTOM uses MPT (Merkle Patricia Tree) tree to store the book data. The MPT tree is the product of the integration of the Trie tree and the Merkle tree, which can effectively reduce the depth of the book tree, increase the balance of the tree, improve the security of the tree and Verifiability. Based on the book data structure of MTP tree, PHANTOM can achieve high efficiency and low consumption in data comparison and data insertion and modification operations. For example, the bitcon-level difference of the book of entire blockchain can be found through the root hash, and accurate data retrieval can be achieved by short path branch traversal.

In the account design, multi-weight operation threshold control attributes have been taken into account, different operation weights can be set for different member accounts, and thresholds can be set for operation execution. Account weight refers to

the operational weight that the owner and signer have for the account. The operation threshold refers to the weight threshold required for account operation. Only when the account reaches the weight threshold, the operation authority is available. In the above manner, the joint control on account by multi-party users can be achieved and the precise operation can be performed according to the operation threshold, to meet the needs of diversified user cooperation, refined operation mode and rich business model.

IV.Multi-layer multi-chain consensus algorithm

With the emergence of new blockchain applications, the proliferation of blockchain users and the continuous enrichment of operation types, users are increasingly demanding the reliability, security and performance requirements of consensus algorithms. Existing typical single-chain consensus algorithms are no longer sufficient.

PHANTOM proposes an innovative two-layer multi-chain consensus algorithm, which generates a set of main chain verification nodes through DPoS protocol voting, and then the selected verification nodes generate blocks through the improved BFT algorithm, so that to achieve higher transaction throughput, scalability and security.

PHANTOM Firework satisfies the needs of multi-chain interoperability scenarios, but instead of simply creating multiple similar single chains, it innovatively uses a main chain-subchain two-layer structure. The first layer is the main chain consensus: the user generates the main chain verification node set by voting in the DPoS protocol and then generates the block through the improved BFT algorithm, thereby achieving higher transaction throughput, scalability and security. The main chain verification node is a full node and has the ability to participate in any sub-chain consensus verification. The second layer is the sub-chain consensus: the sub-chain block is generated periodically by the proposer, and the block header is submitted to the main chain for verification consensus. The sub-chain verification node is a subset of the main chain verification node, is randomly generated based on the VRF (Verifiable Random Function) algorithm and dynamically changed, and is highly resistant to attack.

V. Incentive mechanism and cost model

PHANTOM combines the incentives of DPoS and BFT to verify that nodes are gaining more revenue, and need to continuously improve performance to gain more supporters. Ordinary nodes can also gain revenue by supporting verification nodes. At the same time, PHANTOM introduced a full-node incentive scheme, so that any ordinary node can be used as a full-node to obtain block rewards, so that to improve the enthusiasm of nodes to participate in blockchain common governance and service improvement.

The cost model and the incentive mechanism complement each other. In addition to the increase in revenue for block nodes, the transaction fee can also prevent users from spamming transactions and wasting blockchain resources. For traditional blockchain systems such as Bitcoin, transaction fees are charged according to the amount of the transaction. Since the blockchain size, transaction load, and digital currency prices are constantly changing, the cost model cannot be adjusted according to actual conditions and lacks flexibility. PHANTOM's cost model introduces a fee-based election mechanism that allows the cost to vary depending on the actual situation. Any verification node can propose a new cost proposal, which can be validated into a new fee standard after passing the verification vote. In addition, PHANTOM sets different fee standards according to the transaction content, which makes the transaction charges more refined.

VI.Two-layer polymorphic main chain-subchain multi-chain system

PHANTOM proposes a two-layer polymorphic multi-chain system of main chain-subchain: allowing each business to run more efficiently on its own "track" without causing operational errors or even system crashes due to "track forks." This system does not simply split a chain into multiple pieces, but takes into account factors such as storage efficiency, throughput and business differences, to create differentiated sub-chains for different services, and carries out higher levels consensus verification relying on the main chain, improves the blockchain processing performance and meets the diversity requirements of the business without reducing security.