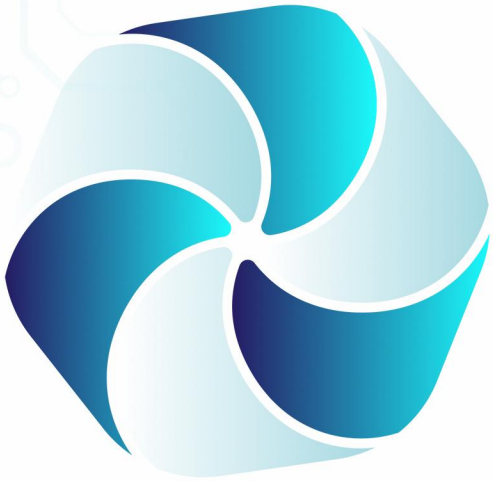


HPB

HPB Non-Technical White Paper

V1.5

www.gxn.io

Abstract

High Performance Blockchain (HPB) is a new approach to solving one of the most critical problems facing all blockchains today: scaling.

Low transaction speeds and excessive latency plague blockchain networks around the world, preventing widespread practical adoption by businesses and consumers.

HPB will solve this problem and meet true business needs by creating a platform designed to handle millions of transactions per second. It will consist of both hardware and software architecture, placing it ahead of current platforms which seek to solve the same problem through software-only solutions.

With a target of 1 million TPS and a 3-second confirmation time, HPB aims to become the standard for all major business applications in industries that require handling of billions of data points with extremely low latency.

1. Industrial Background

1.1 Industrial Background

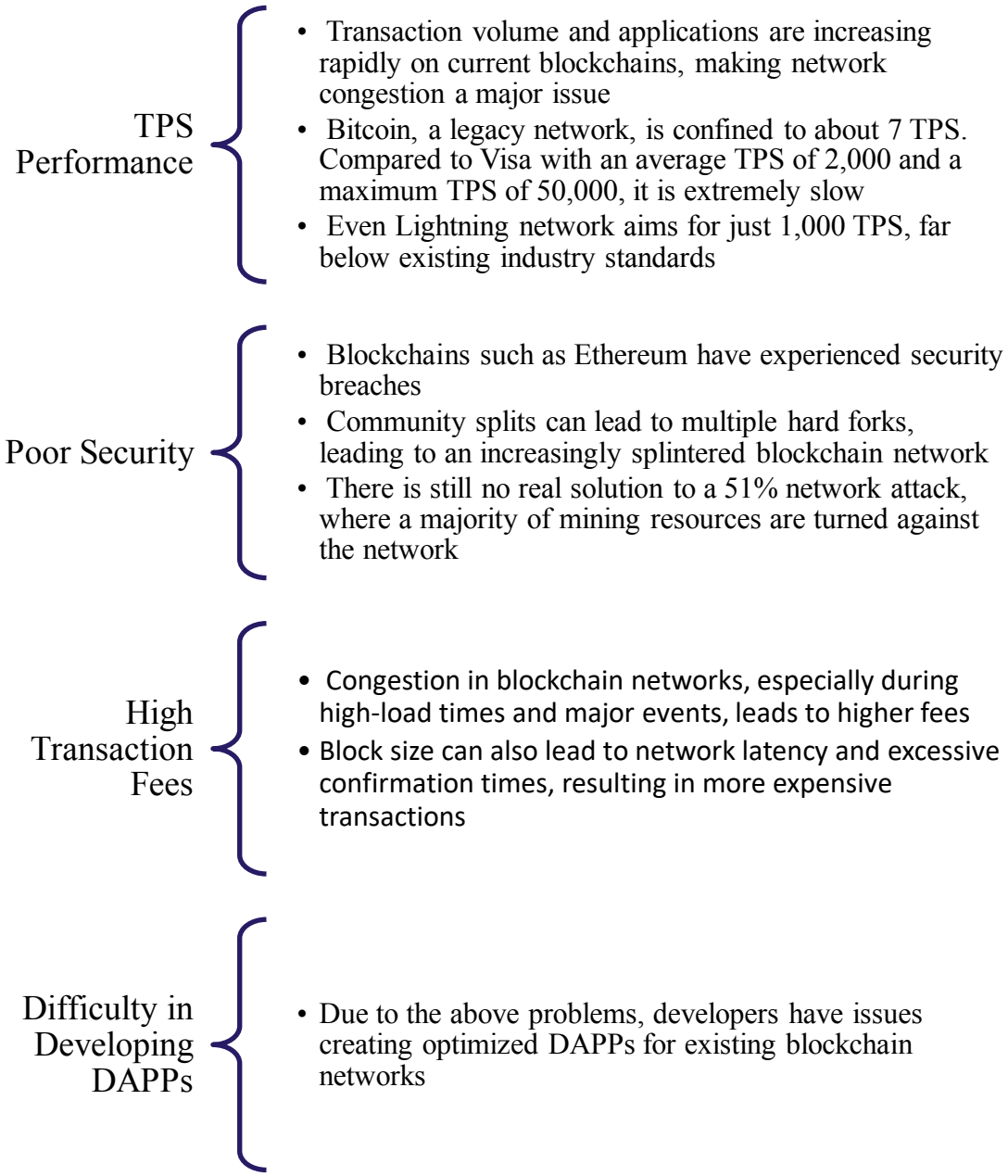
Blockchain is the foundational technology behind Bitcoin. It is also a potentially groundbreaking innovation in how data is created, shared, and edited. Through an immutable ledger and consensus algorithms that ensure the integrity of the blockchain, it is possible to create a “trustless” type of information; a type that is truly decentralized and transparent.

Many current uses of blockchain are restricted to its original purpose: as a peer-to-peer cryptocurrency. However, it has numerous potential applications in several industries: financial instruments, energy and resource management, social networking, big data and IoT applications, governance protocols, advertising and marketing, and perhaps completely new, unforeseen industries which may only be possible through blockchain’s successful maturation.

Blockchain technology is still quite limited by a critical problem: transactions per second (TPS).

1.2 Current Status of Blockchain Technology

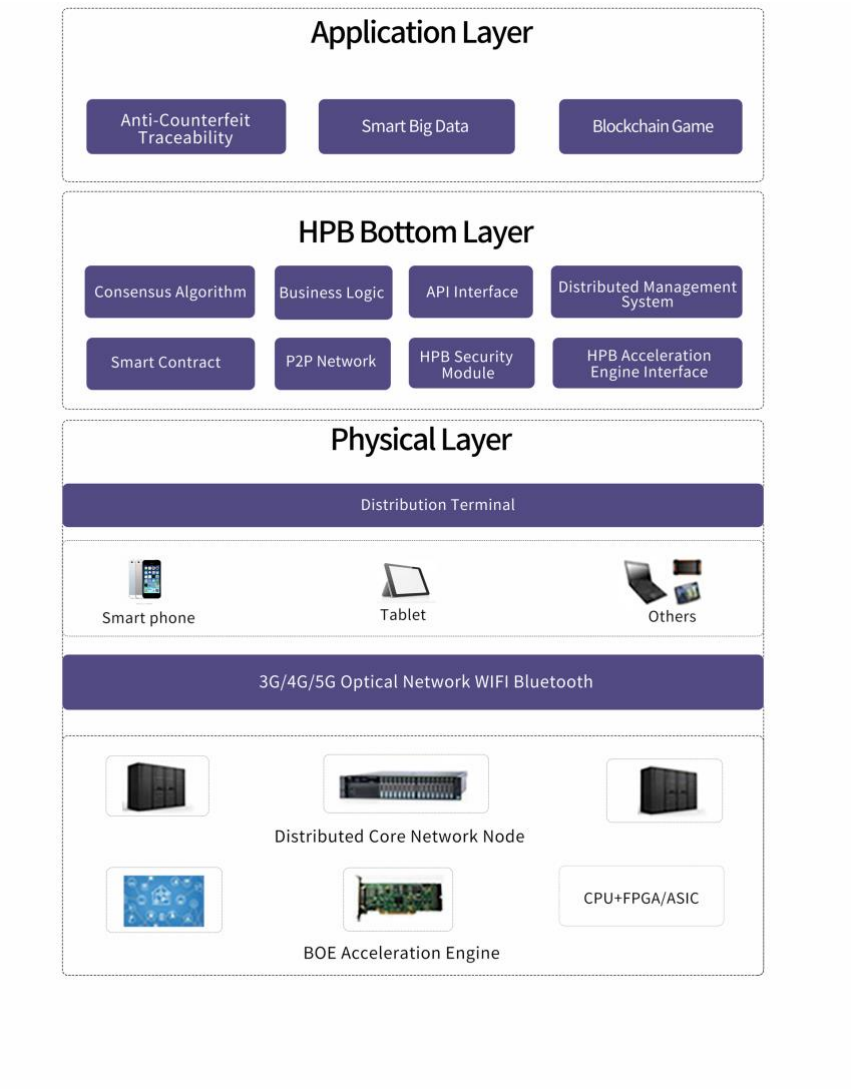
Current major iterations of blockchain possess several problems:



2. Design Concept

HPB is a new blockchain architecture, positioned as an easy-to-use, high-performance blockchain platform. It aims to extend the performance of distributed applications to meet real-world business needs.

The software architecture provides accounts, identity and authorization management, policy management, databases, and asynchronous communication on thousands of CPUs, FPGAs or clustered program schedules. This is a new architecture that can support millions of transactions per second and support authorizations within seconds.



As shown above, the architecture consists of two parts: hardware architecture and software architecture. It is a fusion of the HPC (High Performance Computing) blockchain concept, cloud computing, hardware systems with distributed core nodes, a HPC-powered universal communication network, and a HPC-powered cloud platform.

In addition to network management, the architecture supports core node blockchain standards, and consensus algorithm and blockchain task processing functions. The core node includes a hardware acceleration engine embedded with software.

Through BOE technology, consensus algorithm acceleration, data compression, data encryption and other technologies, the architecture can support millions of concurrent users. The cloud terminal under this architecture can be a traditional PC, intelligent terminal, or any other related machine.

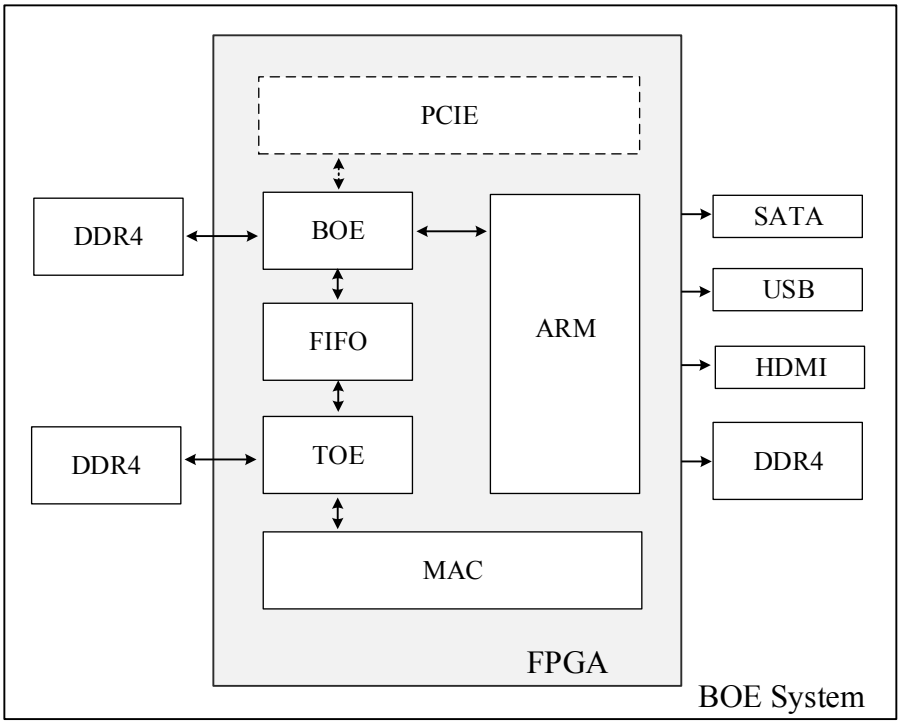
3. Technology Overview

3.1 BOE

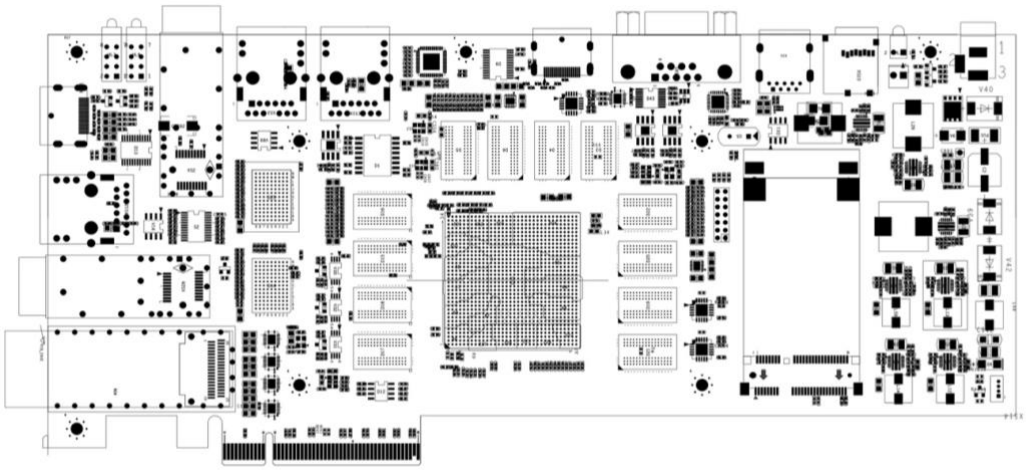
For traditional blockchain nodes, functions such as transaction broadcasting, transaction verification, block broadcasting, and block packaging are all implemented on the software level. The data connection between each node is a serial process, resulting in problems such as complex network topology, long delay time and low serial processing performance.

In response to the above problems, HPB created a new technological innovation: Blockchain Offload Engine (BOE). The BOE is a heterogeneous processing system, including hardware, firmware, and corresponding matching software.

To achieve high performance and high concurrency computing acceleration, this heterogeneous processing system combines CPU serial capabilities and parallel processing capabilities of FPGA/ASIC chips.



BOE Flow Chart



BOE Board Chart

The BOE is connected to other devices in the P2P network through Gigabit/10 Gigabit Ethernet interfaces. The MAC module processes Ethernet data packets and interacts with the TOE module. The BOE module implements the resolution of TCP and UDP packets. To save CPU resources, the CPU is not required to participate in the process.

The BOE module is responsible for establishing encrypted communication channels with other nodes through the TOE module.

It performs integrity checks, signature verifications, and account balance checks on incoming transactions, blocks, and other messages. It also performs fragment processing on the excessive block data to be sent, and encapsulates each fragment to ensure the integrity of the received data. It collects statistics according to the received traffic of each TCP connection. The BOE is designed to be able to provide corresponding incentives for the contribution of the system, so as to attract more users to participate in maintaining the network's operation.

3.1.1 ECDSA Acceleration

For security considerations, every transaction and block broadcast in the network requires a signing and verification process. ECDSA, the Elliptic Curve Digital Signature Algorithm, is currently the most mature and widely used digital signature algorithm in the industry. However, pure software implementation methods are limited to thousands of verifications per second on general computing platforms, which is far from high-performance requirements.

The BOE acceleration engine with the embedded ECDSA module will significantly improve this signature verification speed, aimed towards verifying millions of signatures per second.

3.1.2 Hardware Random Number Generator

When data transmission is performed between nodes, an encrypted channel needs to be established through a key exchange. To make the key exchange random number completely unpredictable, a hardware random number generator is employed to protect the reliability of the encrypted channel.

3.1.3 Data Fragmentation

In the case of high TPS, the amount of data transmitted between the nodes is far beyond the endurance of current network infrastructure, which leads to slow data

synchronization. BOE acceleration engine adopts block data fragmentation broadcast processing technology. Each block fragmentation contains a complete block header, in order to easily broadcast newly generated blocks to all nodes and realize the fast convergence of blockchain.

3.1.4 Network Performance

In the HPB network, one of the conditions to become a high contribution node is to provide network bandwidth to the system. BOE technology is based on the hardware level to achieve node connection traffic statistics. Through BOE technology, the consensus algorithm can calculate the network bandwidth data provided by a certain node.

3.1.5 Concurrency

The BOE acceleration engine can achieve considerable concurrency connections while maintaining support for more than 10,000 simultaneous TCP sessions and processing 10,000 sessions in parallel. This will greatly reduce the number of distributed network layers. Dedicated parallel processing hardware will take over traditional software serial processing functions, such as transaction data broadcasts, unverified block broadcasts across the network, transaction confirmation broadcasts, and so on. The session response speed and the session maintenance numbers are more than 100 times that of the general computing platform node.

3.2 Consensus Algorithm

To meet BOE technology's requirements and simultaneously improve the secure TPS[1], the HPB consensus algorithm adopts an efficient two-tier election mechanism, namely outer elections and inner elections.

- Outer elections: Adoption of node contribution evaluation indicators and select

[1] Secure TPS refers to the TPS confirmed by several trusted nodes under efficient network coverage.

high contribution node members from a multitude of candidate nodes.

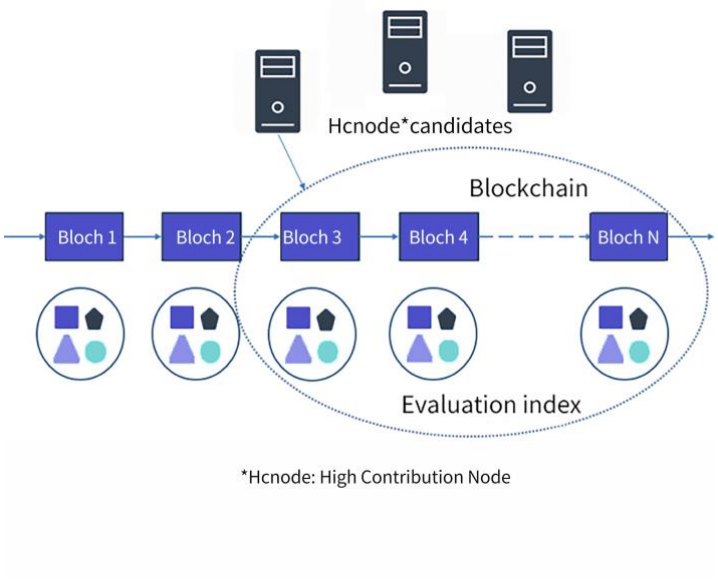
- Inner elections: Based on the anonymous voting mechanism of Hash queues, the priority of high contribution node -generated blocks is calculated at each block generation, and high contribution nodes with high priority have the right to generate blocks first.

Thanks to the Lightweight Message Exchange Mechanism, the consensus efficiency of the HPB consensus algorithm is far higher than others. At the same time, it also greatly improves security and privacy.

3.2.1 Outer Election

The outer election phase is used to select high contribution nodes from a large number of candidate nodes. To minimize network synchronization and make full use of the data of each node on the chain, an innovative adaptive consistent election plan is adopted: the “account” consistency guarantees the consistency of the outer election.

As shown in the figure on the next page, each evaluation indicator is built into the block. Under the precondition of past account consistency, each high contribution node can adaptively calculate the ranking of all currently participating candidate nodes. The higher ranked candidate node will formally become a high contribution node in the next round.



Adaptive Performance Index Evaluation System

The evaluation index of candidate node contribution includes the following factors:

➢ BOE hardware engine: Whether BOE acceleration engine is configured .

➢ Network bandwidth contribution: Data throughput in a fixed history period.

➢ Reputation assessment: Node reputation assessment based on packed block and transaction forwarding behavior and data analysis.

➢ Total holding time of node: Real-time statistics based on account information.

3.2.2 Inner Election

According to the design of the HPB consensus algorithm, the inner election is based on the high contribution nodes. The goal is to efficiently find out the corresponding high contribution node for each block, which includes three stages: nomination stage, statistical stage and computing stage.

Nomination stage: At the beginning of each voting period, the BOE acceleration engine generates random Commits. Each high contribution node submits the Commit, that is, the blocks generated by the Commit along with the high contribution nodes are eventually synchronized into the chain.

Statistical stage: At the end of each voting period, the high contribution nodes count the Commits in the blockchain and create a voting Pool: ($Commit_1$, $Commit_2$, $Commit_3$, $Commit_4$, … $Commit_n$)

Computation stage: When a block is generated, each high contribution node quickly calculates the generation priority of the node in the block by using the fixed weight algorithm of the Commits in the voting pool. The high contribution node with the highest priority will obtain the block package right. Following the principle of Verifiable Random Functions (VRF), other nodes verify the signature of the random number and the address when the block gets into the chain. This not only ensures the reliability, but also guarantees the unpredictability and the address privacy of high contribution nodes.

The HPB consensus algorithm plan provides strict privacy - before the block is packaged, the current node cannot predict the node that generates the next block - and takes into account the security verification of high contribution nodes.

3.3 Application Services

3.3.1 Blockchain APIs

At the base layer of the blockchain, the system provides a series of blockchain data access & interaction interfaces and uses JSON-RPC & RESTful API to support various data applications and development languages. It supports multi-blockchain, data query, transaction submission and other blockchain operations. In different business scenarios, the interactive access interface can be further integrated with the privilege control system.

3.3.2 Application SDKs

Application SDKs are comprehensive services for development in different programming languages of comprehensive service function interface. It allows for the execution of blockchain operations and functions, packet-based encryption, data signatures, transaction generation, etc. It can be extended to integration of specific business logic functions, and seamlessly support expansion and integration into various

business system languages. It will support Java, JavaScript, .NET, Ruby, Python and other SDK languages.

3.4 Smart Contract

3.4.1 General Virtual Machine (GVM) Mechanism

The goal of HPB is to support a variety of virtual machines, and, over time, add new virtual machines as needed.

HPB adopts a modular design. It supports multiple virtual machines, and adjusts the list of supported virtual machines at any time according to market requirements. The underlying virtual machine is combined with upper-level programming language parsing and transformation to flexibly support the basic applications of the virtual machine. Through customized API operation, the external interface of the virtual machine can be realized, and can flexibly interact with ledger data and external data. This mechanism achieves high performance of native code execution when running smart contracts. A GVM supporting different blockchains is also implemented.

3.4.1.1 Ethereum Virtual Machine (EVM)

EVM has been the most popular solution for existing smart contracts, and can also be used on HPB. It is feasible that the HPB operating system's blockchain and EVM smart contracts can run in an internal sandbox, and can interact with other HPB applications with only minor adaptations.

3.4.1.2 Neo Virtual Machine (NeoVM)

NeoVM is actively being used for enterprise-level finance solutions and other industries, and can be used with HPB. When future NeoVM users run into scenarios requiring high-performance, they can interact with HPB with only small adaptations.

3.4.2 Smart Contract Lifecycle Management

The system handles full lifecycle management of each smart contract as digital assets, including the complete controlled management of submission, deployment, usage, and cancellation. Furthermore, with integration into the right management mechanism, comprehensive smart contract management is successfully implemented.

3.4.3 Smart Contract Auditing

Smart contract auditing is achieved through secure auditing, a combination of automated auditing tools and professional auditors. It goes a step further with automated code review and formal verification, as well as integrated unit coverage testing tools.

3.4.4 Smart Contract Template

Through active adoption by several business models and processes within different business domains, a general smart contract template is gradually formed, which can support flexible configurations for a multitude of scenarios.

3.5 System Management

3.5.1 System Configuration

HPB's technology adopts a combination of software and hardware.

The system architecture can be divided into four levels: hardware layer, hardware abstraction layers, middle layers, and implementation layers.

The software and hardware versions of each layer need to be compatible with each other. With regard to the complexity of the system, HPB provides system upgrade services. Through simple command operations, various levels of compatibility checks, automatic downloads, automatic upgrades, and automatic deployments can be implemented.

3.5.2 System Monitoring

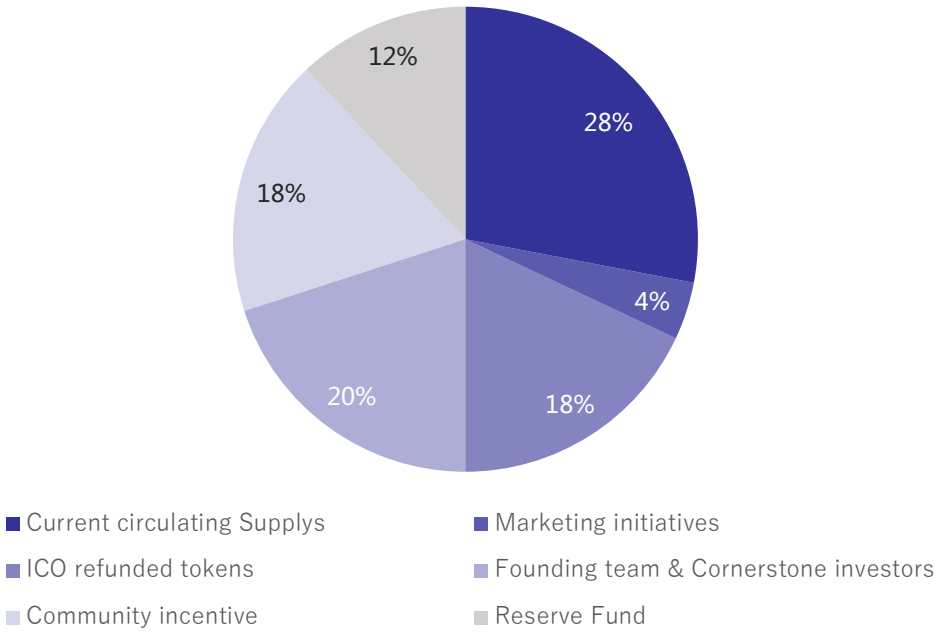
HPB provides the blockchain system, network and nodes with comprehensive monitoring, logging visualization applications, and real-time activity alerts and notifications. HPB supports the specific situations of remote fault recovery and network system restart services. It also supports integrated monitoring and expansion according to the requirements of different business areas.

4. HPB Economic Model

4.1 HPB Token Introduction

- HPB token initialization total supply is 100 million.
- Based on the HPB consensus algorithm, a high contribution node (hcnode) has the right to generate a block. Three necessary conditions for becoming a high contribution node (hcnode) are:
    - Adopt BOE hardware acceleration engine.
    - Hold a certain number of HPB tokens.
    - Contribute to the necessary network bandwidth for the entire system.
- After HPB launches its Mainnet, the high contribution node (hcnode) that generates the block will receive HPB Coin rewards automatically issued by the system.
- The additional number of coin reward issued annually by the system is proportional to the total number of high contribution nodes and candidate nodes. The number of additional issuances does not exceed 6% per year.

4.2 HPB Token Allocation



a. Current circulating Supply：28%

Private Placement includes crowdfunding participants, early investors;

b. Marketing Initiatives：4%

Marketing fees to increase brand influence, including white list awards, exchange listings, etc;

c. ICO Refunded Tokens：18%

ICO Refunded Tokens (remained locked) after People's Bank of China issued the Announcement on Prevention of Financing Risks of Token Issuance on September 4th, 2017.

d. Founding team & Cornerstone investors：20%

Used to motivate the founding team, new members and cornerstone investors of the HPB Foundation;

Founding team & Cornerstone investors will be locked for one year and its unlock is limited to one-third per year;

e. Community Incentive：18%

Used to promote community ecological development, such as application development, community operation incentives, etc.;

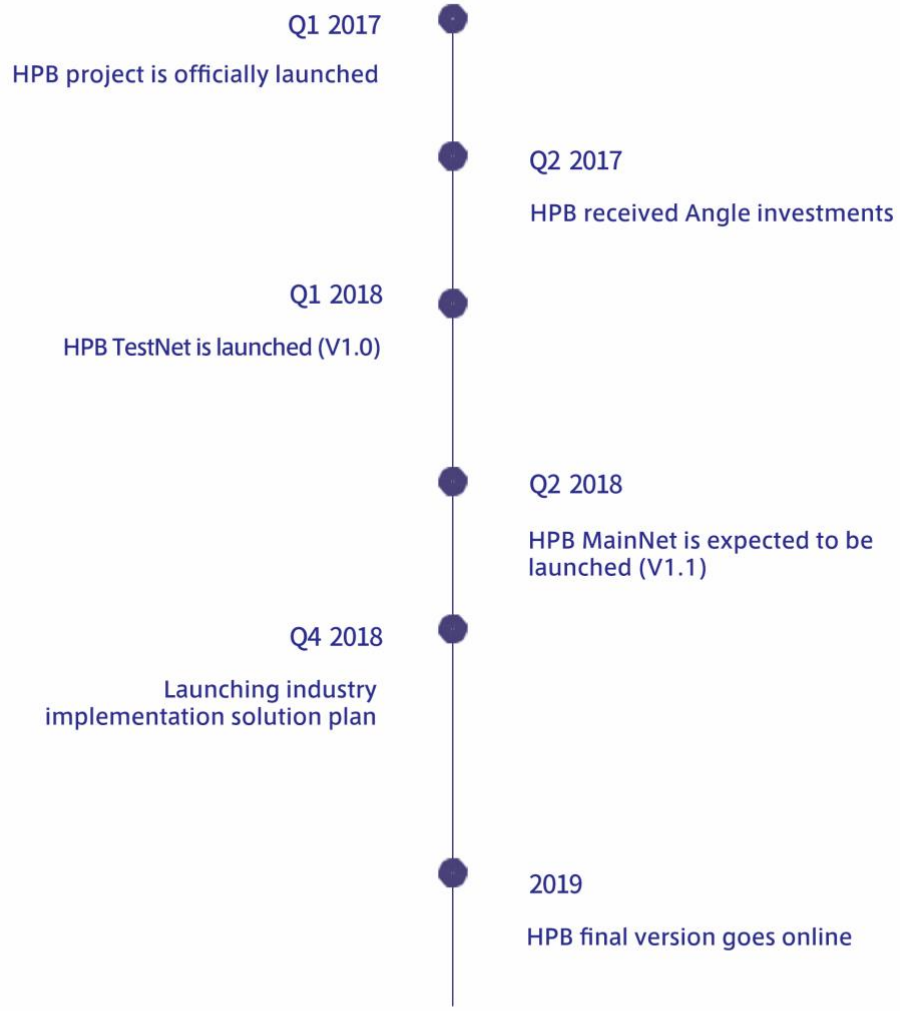
Community Incentive unlock is limited to one-third per year;

f. Reserve Fund：12%

Used for strategic investment, token exchange, government cooperation, response to industry changes, etc;

Reserve Fund will be locked for one year and the unlocking process is limited to one-third per year.

5. Development Roadmap



6. Application Scenarios

6.1 Smart Big Data

Security and privacy remain as the key issues of development of big data. Practical evidence shows that even harmless data, once collected in large quantities, poses the risk of exposing personal data. In addition, big data may also encounter potential security risks during storage, processing, and transmission. It is extremely difficult to implement large data security and privacy protection, simply through technical means to restrict service providers from collecting user information.

To find out the potential value of data sharing, we need to move toward a better solution in managing data security.

Centralized IT systems provide advantages in terms of efficiency. However, frequent data leakage, lack of transparency, and data incompleteness require a distributed consensus mechanism to compensate for defects. HPB collects, uses, and authorizes data through smart contracts to ensure data purity. Building smart big data solutions on the HPB ecosystem will greatly enhance data security, privacy and availability. Concurrently, the use of authorized transmission of data on the public chain and the inquiry of transaction fees can be charged by HPB Coins.

After listening to the design concept of HPB, China's largest financial data company UnionPay Smart has established a partnership with HPB. As a part of UnionPay, UnionPay Smart is specialized in big data innovation business and currently handles 80% of China's banking transaction data, with an annual turnover of 80 trillion Yuan.

With the common goal of technological practice and exploration of big financial data and high-performance blockchains, HPB is currently collaborating with UnionPay on the authorization, certification, and traceability of big data. The tentative launch time for this project is Q3 2018.

6.2 Gaming: Virtual Currencies and Items

The global gaming market reached US$109 billion in 2017. In addition to "F2P (Free-to-play) games", the online gaming business generally consists of two types: users pay to get in-gaming experience time or users pay to buy virtual in-game products.

Virtual game products are provided by a centralized service provider.

For commercial purposes, centralized service providers usually limit the transfer of in-game products so that players can only use them on service providers' proprietary platform, but not in circulation across different platforms.

It is possible for some players to launch transactions on virtual in-game products outside the gaming environment. However, information asymmetry can lead to tedious transaction process and fraudulent issues. Players' virtual in-game products may be lost, confiscated or altered, while players do not have the right of recourse. In addition, online games may also have a closed economic system, including production, distribution, exchange and consumption. Thus, inflation and deflation are unavoidable.

If virtual in-game commodities and assets are stored on the blockchain, encrypted digital currency such as HPB replaces virtual in-game currencies. Virtual in-game products can then be conveniently transacted between players without the need of a centralized game publisher, or a centralized organization such as Google Play or Apple Store.

At the same time, decentralized virtual game currencies, and the sharing of the ledger transaction flow, can introduce real-world scarcity to virtual-world assets, thus introduce real-world value.

Through the hardware and software architecture design, HPB supports a stable million-level concurrency and can be widely used in the online gaming industry.

6.3 Anti-Counterfeit Traceability

Information asymmetry results in difficulty in the traceability of products. Even with anti-counterfeiting traceability technology such as bar codes and QR codes, single-way traceability is gradually distorted in the communication process and counterfeiting

technology has constantly evolved and improved. Blockchain technology with distributed ledgers, ledger traceability and its untraceable characteristics are naturally suited for anti-counterfeiting traceability use.

HPB is currently exploring this field and is reaching initial cooperative intentions with partners and related companies.

7. Summary & Outlook

Throughout the HPB design process, we thank not only the work of the HPB team, but also the contributions and funding of partners, developer communities, and industry organizations. We are very honored to receive the recognition and support of partners. At present, various industrial companies have shown active cooperative intentions in anti-counterfeit traceability, smart big data, and gaming industries.

We would like to express gratitude towards future participants in the development of the HPB architecture, the technology community, business partners and blockchain industry experts. We also sincerely invite technical and business partners to take part in the common cause of development of an open source, high-performance blockchain platform.

HPB Foundation

April 2018