Blockchain-based Service Network

Technical White Paper

BSN Development Association
April 25, 2020

CONTEXT

White Paper Contributors

	Name of Entity
1	State Information Center Informationization and Industry Research Department
2	China Mobile Group Design Institute Co., Ltd.
3	Research Institute of Electronic Payment , China Unionpay Co.,Ltd.
4	Beijing Red Date Technology Company Limited

Note: This white paper was most recently updated on 25 April 2020, as revision 1.0.0.

Chapter I
Objectives

This white paper primarily serves to explain the core technical features of the Blockchain-based Service Network (hereinafter "BSN") and does not further replicate the content covered in the *Blockchain-based Service Network Introductory White Paper*.

From its design to its construction, the main goal of the BSN has always been to create a public infrastructure similar to that of the internet and to provide a "one-stop shop" style blockchain-based service that integrates cloud resources, underlying frameworks, operating environments, key management, development SDK and gateway API. Just like building a simple website on the internet, developers can deploy and operate blockchain and distributed ledger applications (hereinafter "distributed application" or "DApp") conveniently and at extremely low cost. Moreover, just as websites deployed on the internet can mutually interact and communicate, all DApps on the BSN can also interchange data regardless of differences in their underlying frameworks.

This white paper will be continuously updated according to the latest BSN technical iterations. The current version introduces the three aspects of BSN, including public city nodes, data security and the BSN empowerment platform.

Chapter II
Public City Nodes

A public city node (hereinafter “PCN”) is the basic organizational element of the BSN. While the “node” part of its name is easily confused with a blockchain node, PCNs are not blockchain nodes; furthermore, the BSN itself is not a chain. In fact, each PCN is a resource pool, used to allocate a portion of the computing power, storage and bandwidth resources from the cloud service or data center on which it was deployed to the BSN. An entire blockchain operating environment has been built within this resource pool, including multiple blockchain frameworks, shared peer nodes, CA management, authority chain, PCN gateway and PCN manager systems. Developers can use any BSN portal to deploy their own DApps, through the following specific process: select a framework and upload the corresponding smart contract; select one or more city nodes on which the DApp will be deployed; select the number of peers to be deployed on each PCN; click to submit. After the DApp smart contract passes a security check, it will be automatically deployed through the BSN operating and maintenance center (hereinafter “NOC”) to the shared peer nodes of the developer’s designated PCNs and become operational. Then the developer’s off-BSN system can access its DApp through the gateway of any PCN on which the DApp is deployed. PCNs mainly comprise the following function modules:

1.Multiple frameworks

One of the core concepts of the BSN is to support as many blockchain frameworks as possible. Currently, blockchain technology is still in the early phases. We hope that the BSN will create an ecosystem to help framework providers to drive the development of blockchain technology. Within each PCN, all frameworks already adapted to the BSN will be installed as basic on the system. Moreover, different frameworks are not simply stacked together; rather, they are made uniform through their adaptation of cryptographic algorithms, CA management, transaction SDK and DApp management SDK in accordance with *Blockchain-based Service Network Framework Adaptation Standards*. This enables developers to use a single private key to deploy and manage DApps on multiple frameworks and to realize interconnectivity and mutual communication between DApps. Within this process, each framework retains the unique features of its own smart contract and consensus mechanism.

2.Shared peer nodes

In regard to each adapted framework, a set of corresponding shared peer nodes will be deployed on each city node by means of the channel, cluster or sub-chain defined by each framework, thereby allowing each peer node to serve multiple DApps. This ensures that while there is absolute isolation of process handling, smart contracts and ledger data of each DApp from other DApps, all DApps are able to share system resources. This means that developers can purchase resources on the BSN at a rate as low as 10 transactions per second (TPS) and, as such, bring the lowest cost of DApps deployed on the BSN to just several tenths of the cost of traditional blockchain cloud services.

3.Authority chain

The authority chain is used as one of the system-level chains and is deployed in all PCNs. The authority chain stores the application access key (public key) of DApp users and DApps' authority settings. Once a user's off-BSN system accesses a PCN gateway, the gateway will verify the user's identity and only allows the user to access DApps for which the user is authorized. Furthermore, in accordance with the DApp's authority settings, the user is only allowed to invoke the corresponding smart contract methods.

4.CA management

Each PCN deploys a uniform CA management system, used for the full life cycle management of all DApp user transaction keys within said city nodes, including generation, distribution, renewal, revocation, etc. User transaction keys are used to encrypt and sign data when a user accesses a DApp. Please refer to *Chapter III Data Security* for further details concerning the generation and management of user transaction keys and application access keys.

5.PCN gateway

PCN gateways are the only entry point for data interaction generated between business systems outside of the BSN and DApps deployed on the BSN. Each PCN has one gateway. Users can use any of the PCNs deployed by a DApp to gain access; however, selection based on the principle of proximity is recommended. In addition to verifying user identities, PCN gateways also possess the following functions: transaction validation, transaction routing, flow limit control, load balancing, gateway API, SDK, etc.

6.PCN manager

The PCN manager system is a function module responsible for the connectivity between PCNs and the BSN NOC platform. After the NOC platform receives a command or request from each BSN portal, it uses the PCN manager system to carry out operations on each PCN such as managing DApps, deploying smart contracts, configuring peer nodes, managing key certificates, configuring application authorities and obtaining operational information.

Given that the BSN itself is not a chain, it will not incur the operating efficiency issues faced by public blockchains. Transaction performance of each DApp on the BSN is entirely dependent on the number of peer nodes deployed, the type of framework being used, the number of PCNs selected for use and the physical distance between data centers on which these PCNs are installed. For example, if a 3-peer-node DApp is deployed on the same PCN, its operating efficiency will clearly be higher than that of a 30-peer-node DApp being deployed on 20 PCNs. The BSN is a blockchain public network system. The internet transmission speed between PCNs is an important factor in determining the operating efficiency of the DApp. Furthermore, we recommend that no more than 40 peer nodes are deployed for any single DApp on the BSN.

Currently, developers can independently deploy 500 TPS DApps through any BSN portal. For higher TPS requirements, developers should contact BSN's NOC personnel to implement a customized deployment. For most of the distributed ledger DApps, 500 TPS is sufficient to satisfy all business requirements.

When the resource usage volume of a PCN reaches saturation point, the BSN NOC platform stops any new DApps from being deployed on that node. Cloud service providers can increase the configuration at any time to add new resources to the city node. In principle, there is no limit to the extent to which the resource pool of a PCN can be expanded.

Chapter III
Data Security

Blockchain and distributed ledgers use technology based on public-key cryptography. The security of said technology is inherently higher. Within the design of the BSN, utmost priority is given to data security and user privacy protection. During the process of using the BSN, developers can incorporate data security mechanisms within each step. The BSN provides a series of rather complex key management and authorization setting functions; in accordance with their own specific DApp requirements, developers can combine these at their own will to form their own appropriate system for data security. The following describes actual mechanism content provided by BSN:

1.In the BSN Developer's User Guide, developers are repeatedly reminded that prior to uploading off-BSN system data to DApps, it is best to encrypt that data. If developers use the BSN SDK, we provide a certain number of different types of encryption mechanisms and recommendations within SDK for developers to choose from.

2.When distributing a DApp on any BSN portal, developers can choose the mode with which the DApp provides users with an access key: key trust mode or public key upload mode. In key trust mode, the user entrusts the BSN to generate a pair of keys (private and public keys) to be used by the user after downloading it via the BSN portal. In public key upload mode, the DApp user self-generates a pair of keys locally, uploads the public key via the BSN portal and then uses the private key to carry out a transaction signature to connect to the PCN gateway, completing the application access authority validation. Key trust mode is rather more convenient; however, public key upload mode is more autonomous. The choice of which method to use and designate is entirely up to the developer.

3.In terms of DApps that have already been distributed, when configuring the user transaction key, developers can configure a uniform key for the whole DApp, provided for the use of all accessing users. Alternatively, they can configure an individual user transaction key for each user. The key configuration mode also comprises either a key trust mode or a public key upload mode. The difference is that the PCN gateway provides several user transaction key management APIs, and therefore, developers and users are not required to carry out any setup within the BSN portal.

4.When developers distribute a DApp smart contract, they can combine the methods within the smart contract itself to form all sorts of roles. Each role invokes the authority to one or more methods. For example, some roles can write data to the DApp and some roles can only read data. When a user participates in a DApp, they can be allocated with one or more roles. The information concerning these roles and the corresponding authorities are stored in the authority chain. When a user's off-BSN system uses the gateway to access the DApp, only the functions and data authorities of the allocated roles will be available to use.

5.When compiling smart contracts, developers can further control transaction and data handling so that if two users possess the same role authorities, then at the smart contract code level, they can also define that these two users can query and implement different data transaction operations.

The aforementioned five mechanisms form the whole BSN series in terms of DApp data security and, therefore, guarantee absolute data security. Moreover, they allow developers ample space to design their own DApp security mechanisms according to need. In particular, when using the public key upload mode, the security level can reach that of Bitcoin Wallet, where no one else can come into contact with the DApp data except for the developer and the authorized users.

Chapter IV
BSN Empowerment Platform

The operations and maintenance center platform (hereinafter "NOC platform") is responsible for the uniform management of the BSN's actual operations and maintenance. If a DApp needs to be deployed or managed on the BSN, all BSN portals and other front-end services need to install a BSN empowerment platform on their own systems. The empowerment platform consists of a set of APIs that communicate with the NOC platform, while the NOC platform implements the related orders sent from each BSN portal. Empowerment platforms mainly include all core APIs provided by the BSN. The following is a brief categorization and explanation of all APIs:

API Type	API Quantity	Description
PCN management	4	Used to obtain blockchain PCN information, information regarding the price of resources on PCNs, etc.
Framework management	2	Used to obtain underlying framework information, including sellable resources of affiliated frameworks, etc.
DApp management	8	Used to realize DApp operations such as distribution, upgrades, start and stop, uninstall and resource configuration upgrades
DApp participation management	10	Used to realize the management of DApp participation, user authority and key management
PCN information management	3	Used to obtain PCN operational status information, including the operations of related DApps and blockchain information
Data usage information	1	Used to obtain data usage information of related DApps

The BSN’s official portal (www.bsnbase.com) is also entirely built on the basis of the BSN empowerment platform. In addition to being able to create BSN portals, the empowerment platform is also able to provide embedded blockchain application and data services to many websites, APPs and SaaS services. We can use a file collaboration management website as an example: by using the empowerment platform, this website is able to provide users, within its own site, a one-click generated DApp on the BSN and, therefore, can provide a service to choose which of the shared, collaborative file data to automatically upload to the DApp and store.

The BSN places extreme focus on the personal privacy of developers and DApp users. For this reason, absolutely no private user data is stored on the BSN or within the NOC platform. There is no API to personal private data on the empowerment platform used within portals, and personal information of all developers and DApp users is managed independently by each BSN portal. Within the BSN NOC platform, it is only possible to track which portals have distributed any given DApp and how many users are using this DApp. However, there is absolutely no detailed information about the DApp’s developer and no detailed information about the DApp users.

Chapter V
Contact Us

The BSN relies upon continuous research, development and optimization, which is a vast and hugely diverse undertaking. We welcome technology companies with experience and resources to join the BSN so that together, we can build the BSN into a blockchain internet of genuine significance.

Interested parties can contact info@bsnbase.com.