2020

Enterprise Blockchain Security Whitepaper

NSFOCUS

About NSFOCUS

NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks. The company's Intelligent Hybrid Security strategy utilizes both cloud and on-premises security platforms, built on a foundation of real-time global threat intelligence, to provide multi-layered, unified and dynamic protection against advanced cyber attacks.

NSFOCUS works with Fortune Global 500 companies, including four of the world's five largest financial institutions, organizations in insurance, retail, healthcare, critical infrastructure industries as well as government agencies. NSFOCUS has technology and channel partners in more than 60 countries, is a member of both the Microsoft Active Protections Program (MAPP), and the Cloud Security Alliance (CSA).

A wholly owned subsidiary of NSFOCUS Technologies Group Co., Ltd., the company has operations in the Americas, Europe, the Middle East and Asia Pacific.

Special Statement

All data used for analysis has been anonymized and no customer information appears in this report to avoid information disclosure per GDPR.

CONTENTS

CONTENTS

Executive Summary

It has been 12 years since the blockchain technology was invented in 2008. From the initial application to the cryptocurrency Bitcoin (Blockchain 1.0) to the smart contract-based decentralized application (Blockchain 2.0) that is in full swing and then to the much-talked-about general application in verticals of different industries (Blockchain 3.0), the blockchain technology, restricted by regulatory controls, has developed slowly but steadily amid ups and downs.

Predictably, the blockchain technology, being tamper-resistant, decentralized, and traceable, will definitely go beyond its initial application in the financial and economic fields and find its way into e-government, transportation, culture, health care, digital finance, smart manufacturing, supply chain management, and digital identity fields. This technology can be used to develop a decentralized business model for trusted data exchanges, thereby reducing the social, financial, and time costs incurred by the lack of trust and enhancing the efficiency of systematic operations that involve multiple parties.

While more and more enterprises are employing the blockchain technology in their operations, enterprise blockchains are faced with increasingly severe security issues. In this context, NSFOCUS and its partners jointly release the *Enterprise Blockchain Security Whitepaper*, in an attempt to anatomize enterprise blockchains around the concept, architecture, and security and provide readers with an insight into associated issues.

This whitepaper has the following findings:

- Smart contracts are not "perfect contracts" and people should be wary of their security issues.

The application of enterprise blockchains is still at an early stage. With the wider adoption in future, there will be more vulnerabilities and related security events reported. Our prediction is that most of these vulnerabilities, especially such common security issues as insecure functions and out-of-bounds access, will be linked to smart contracts.

- Two major threats facing the blockchain technology are ransomware and cryptojackers.

Executive Summary

Of all business security events associated with blockchains, ransomware and malicious cryptomining are the dominant types of threat. Owing to the anonymity of cryptocurrency and the convenience of turning cryptocurrency into cash, these types of malicious attacks will not go away anytime soon. Then, understandably, the rise and fall of cryptocurrency prices can somewhat lead to the rise and fall of such attacks.

- The watchdog turns its eye to blockchain applications.

As data on blockchains cannot be deleted, which is convenient for post-event forensics, compliance requirements for blockchain applications will be different from those for other information services.

- Compliance is the only way out for blockchain applications.

With promulgation of a series of regulations on protection of personal data, such as the *General Data Protection Regulation* (GDPR), the collection, management, and exchange of personal data are required to be compliant with related regulations. No matter how the blockchain technology is applied, it should be done within the scope permitted by law. For the sound development of the blockchain technology, legal and regulatory compliance is a prerequisite. We should make it our top priority to make blockchain applications more secure and completely compliant with related regulations.

- Another concern about blockchain applications is privacy protection.

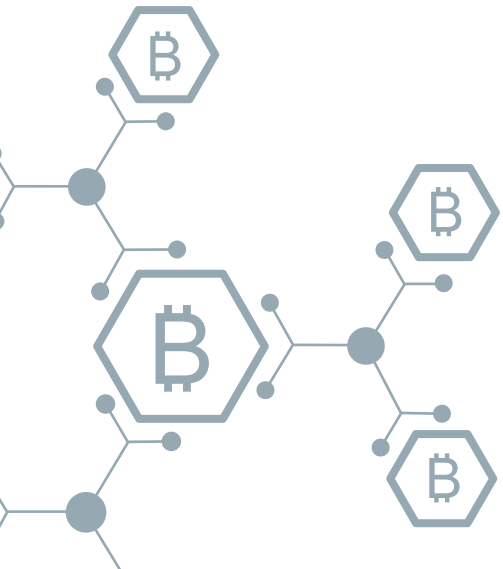
In the past few years, new techniques and mechanisms have emerged on end to tackle privacy protection problems on blockchains. Typical examples include the channel mechanism, private transaction, and encrypted authorized access. Besides, innovations have been made based on cutting-edge cryptography, including the zero-knowledge proof, ring signature, and secure multi-party computation.

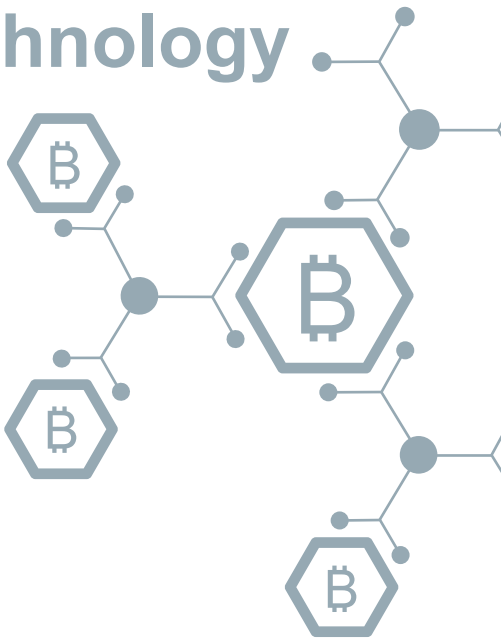
- The blockchain technology can be in full bloom only when secured.

Security vendors, universities, blockchain service providers (SPs), and users should work closely to step up the creation of a secure ecosystem for enterprise blockchains. The adoption of the blockchain technology makes security a marked issue for organizations. The traditional model of "promoting the fast growth of business in advance of security efforts" is no longer feasible. In fact, security should be considered through the blockchain system lifecycle.

1

Development of the Blockchain Technology





Development of the Blockchain Technology

Blockchains[1] are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules. Since its launch, the blockchain technology has gone through ups and downs, but predictably, will gain momentum for rapid growth in the years to come.

Generally, blockchains are divided into public, consortium, and private blockchains, each applied in particular scenarios.

A public blockchain, with no official body of management or centralized server, allows nodes to freely join and exit the network. These nodes, when in operation, interoperate with each other in a flat topology and work based on the consensus mechanism. The public blockchain usually finds its application in cryptocurrency like Bitcoin, Ethereum, and EOS, which is also an area the blockchain technology was first adopted.

In a private blockchain network, the write access to each node is internally controlled, while the read access is selectively granted as required. Built on a universal architecture with support for multi-node running, a private blockchain is suitable for internal data management and audits within organizations. Specific to an organization, the private blockchain system has rules defined that best suit the organization's needs. We can look at the private blockchain as a robust, forensicable internal distributed system, which is an evolved edition of the organization's internal system that has been decentralized.

A consortium blockchain sits on the fence between public and private blockchains. Each node corresponds to an entity, which can join and exit the network upon authorization. Different entities organize into a consortium of shared interests to jointly maintain the sound operation of the blockchain. Typical examples of the consortium blockchain are Hyperledger, Quorum, and R3 Corda. Inheriting the feature of decentralization inherent in the blockchain, the consortium blockchain introduces centralized management of a limited degree to make the entire system more operable and widely applicable to financial, logistics, and energy sectors and other enterprise-grade scenarios.

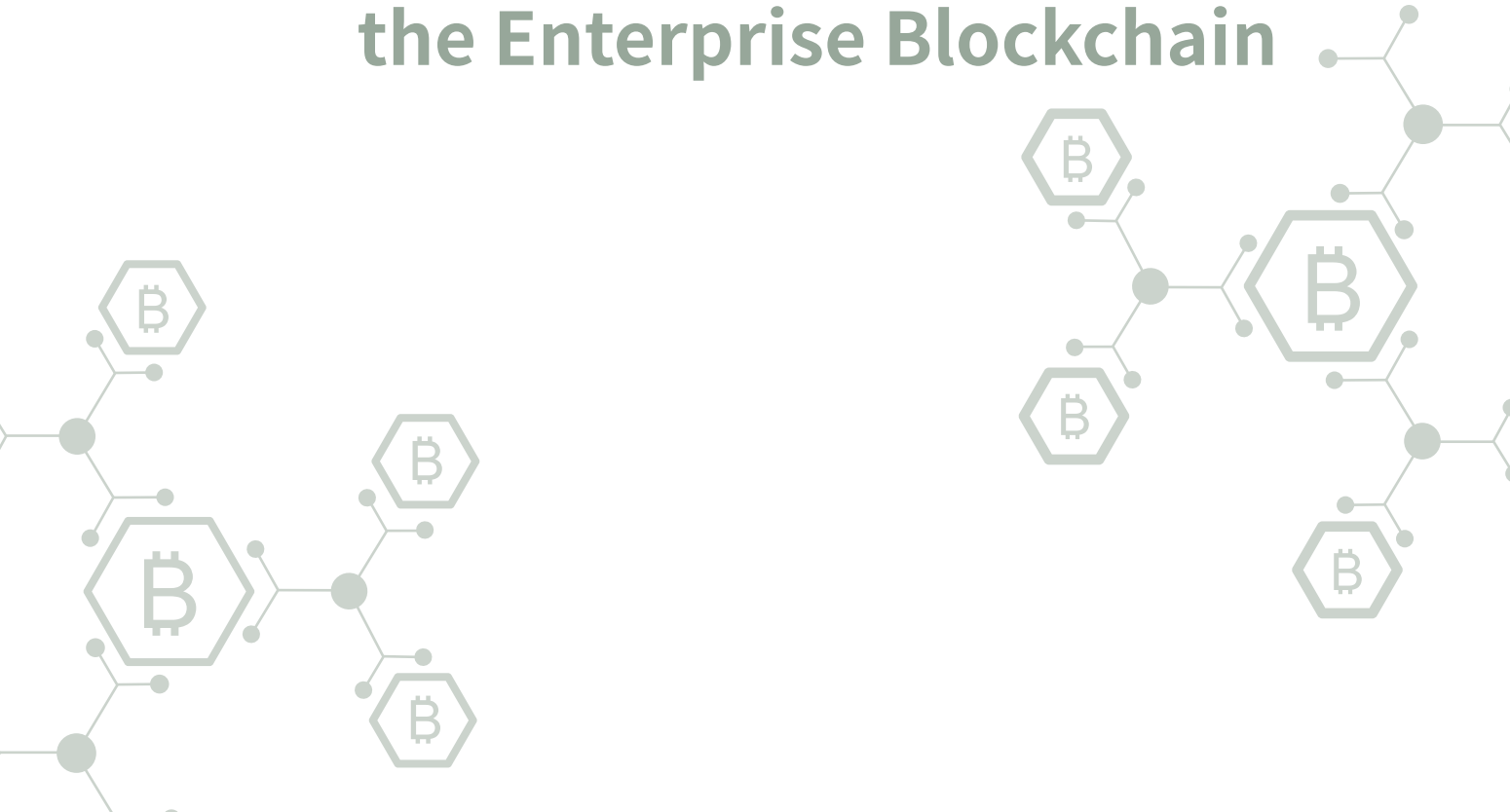
According to multiple research institutes, 2020 will mark a turning point in the history of enterprise blockchain applications. In its prediction about top 10 technological trends, Alibaba DAMO Academy mentions that the technical threshold for enterprise blockchain applications in 2020 will be further lowered, various hardware chips built with core algorithms around the node, cloud, and chain for blockchains will emerge as the times demand, and blockchain applications with over 10 million daily active users (DAUs) will become a reality. In its Industrial Internet: *A Look Back at 2019 and a Look into 2020*, Tencent Research Institute mentions 11 trends in the industrial transformation, for example, "2020: Blockchain applications, upon integration with industrial scenarios, are expected to be rolled out in large scale." Aside from these reports, cloud service providers (CSPs), such as Alibaba, Tencent, Amazon, and Microsoft, have also launched the Blockchain as a Service (BaaS), in a bid to help customers deploy blockchain applications cost-effectively and push the development of the entire blockchain industry. According to the forecast made by the International Data Corporation (IDC), as for the IT spending, Chinese companies will invest $2.7 billion in blockchain services (consulting, implementation, maintenance, support, and so on) by 2023, accounting for 29% of enterprise management service expenditures.

Gartner predicts that[1], by 2022, more than a billion people will have some data about them referenced on a blockchain though they may not be aware of it, and by 2024, enterprises will use the blockchain licenses to secure 30% of their sensitive data. In the *IDC FutureScape: Worldwide Blockchain 2020 Predictions – China Implications*[2], the research institute predicts that, by 2023, 40% of China's first-tier financial institutions will use blockchain networks for node-to-node processing of cross-border payments, bypassing SWIFT and central bank infrastructure, and by 2024, over 85% of China's container shipments will be tracked using blockchains, half of which will employ blockchain-supported cross-border payments.

As blockchain applications and infrastructure for finance, logistics, identity authentication, and other sectors are mostly based on the consortium blockchain, the remaining part of this report will dwell upon the application of this type of blockchains in enterprise operations.

2

Introduction to the Enterprise Blockchain



This chapter describes the characteristics, usage scenarios, and architecture of enterprise blockchains, and illustrates three major enterprise blockchain systems in three separate sections.

2.1 Relationship Between the Enterprise Blockchain and Consortium Blockchain

An enterprise blockchain is a type of blockchain applications adopted by multiple organizations for a particular purpose by following a unified authentication system, consensus mechanism, and smart contract specification for standards-based interoperability of their respective homogeneous or heterogeneous blockchain data, systems, and services.

The enterprise blockchain is a conceptual term that limits blockchain applications to enterprises. It must work on a certain blockchain platform. According to our observation, most enterprises choose the consortium blockchain technology when deciding to implement the blockchain technology. Therefore, the consortium blockchain is the main concern in this chapter. Hereinafter, the consortium blockchain and the enterprise blockchain are interchangeable.

2.2 Characteristics of Consortium Blockchains

A consortium blockchain is generally used to share data between organizations or run programs that they consent. Unlike a public blockchain that has a large number of unregistered nodes, a consortium blockchain has a limited number of participants that have been authenticated. It is also different from a private blockchain in that control over it is not granted to a single manager with the highest privilege, but rather a group of peer nodes.

In addition, a consortium blockchain is oriented towards particular scenarios, with a lot of variances from a public blockchain. In summary, it has the following characteristics:

- **Identity authentication.** All participants of a consortium blockchain have a unique identity. Only with such a unique identity, can a participant be granted permissions.
- **Access permission.** Consortium blockchains are permissioned. That is to say, a node can gain

access to a consortium blockchain only when meeting certain access control conditions. In this sense, a consortium blockchain is thought of as a permissioned blockchain.

- **High throughput.** In some usage scenarios (such as finance) that feature high-frequency transactions, a consortium blockchain should deliver high throughputs to support massive applications.
- **Low latency.** In a public blockchain, such as Bitcoin, the delay caused by generation of six blocks to confirm a transaction is too long for many consortium blockchain applications, which are supposed to support fast transactions. A consortium blockchain assumes a certain degree of trust in peer nodes by performing identity authentication and access controls. It shortens the time to reach consensus by simplifying the consensus algorithm, leading to a low latency.
- **Confidentiality and privacy.** A consortium blockchain should ensure the confidentiality and privacy of business transactions. For example, in a supply chain network, prices may be different for different customers. If contract and transaction contents were visible to all participants, it would be very difficult to differentiate prices. Out of this consideration, some consortium blockchains add the design of channels, providing confidentiality and privacy protection for different transaction participants.

Consortium blockchains have a limited number of authenticated peer nodes, particularly suitable for decentralized multi-party enterprise applications and applicable to a wide range of scenarios, including decentralized finance, Internet of things (IoT), jurisdictional forensics, food source tracking, and identity authentication. There are loads of research papers on this topic and no further details are provided here.

2.3 Reference Architecture of Consortium Blockchains

The blockchain technology is implemented in a hierarchical architecture based on multiple supporting techniques. Some emerging blockchain technologies initially developed for public blockchains, over time, have gradually been integrated into consortium and private blockchain systems. Therefore, public, private, and consortium blockchains are basically the same in the technical stack, but the latter two

have more control and management components, such as authentication and identity management, supervision, and audits.

The China Blockchain Technology and Industrial Development Forum (CBD-Forum) introduced a blockchain reference architecture (Figure 2.1) in 2017, which can also serve as the reference architecture of consortium blockchains.

In the reference architecture:

- The underlying layer provides components necessary for proper running of the blockchain system, including the storage and computation components and peer-to-peer (P2P) network.
- The core layer, as the core of the blockchain system, consists of the consensus mechanism, smart contract, cryptography-related functions, ledger records, and so on.
- The service layer, by calling functional components from the core layer, provides the access service for the user layer, including access management, node management, and ledger applications.
- The user layer provides the user function, service function, and management function.

This reference architecture is a universal one. For the purpose of manageable consortium blockchains, the architecture should have more components for development management, operations, security, and supervision and audits, which are distributed across layers of the technical stack of the reference architecture. For example,

The development function provides components necessary for blockchain development, including the integrated development environment (IDE), test management, and build management.

The operations function provides components for blockchain system management, including policy management and exception and issue management.

The security function is used to authenticate users and nodes, encrypt communications, encrypt transactions, and control access to data, consisting of authentication and identity management, authorization and security policy management, and privacy protection components.

Real-time supervision and post-event audits are also indispensable to consortium blockchains. In

practice, organizations, when implementing consortium blockchains, should keep in mind regulatory requirements for the specific industry that they are in.

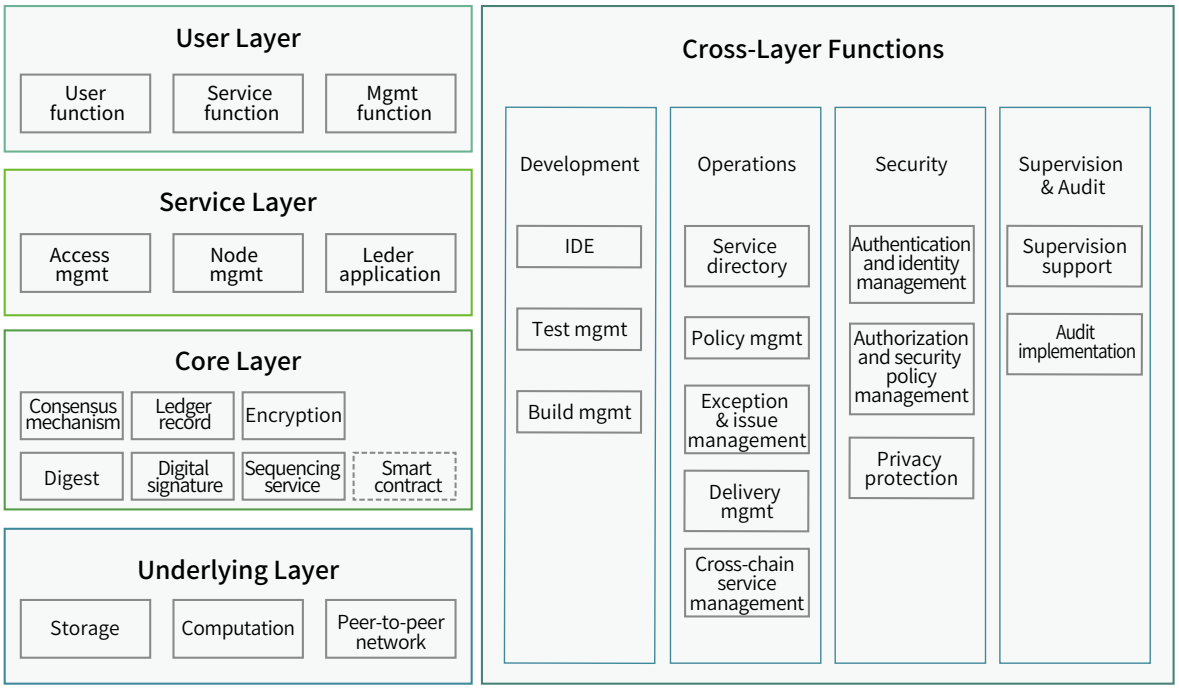


Figure 2-1 Reference architecture of consortium blockchains

2.4 Mainstream Consortium Blockchain Platforms

Current mainstream consortium blockchain platforms include Hyperledger, Quorum, and R3 Corda, which are described in detail in the following sections.

2.4.1 Hyperledger

The Hyperledger projectt[3] was started in December 2015 by the Linux Foundation. It is intended to support the collaborative development and maintenance of a cross-industry, open, and distributed ledger technology platform and standard that enable any digital exchange with value, such as real

estate contracts, energy trades, and marriage licenses, to be conducted and tracked securely and cost-effectively. Hyperledger's projects include Blockchain Explorer, Fabric, and Sawtooth Lake, among which Fabric, as a basis for development of blockchain application or solutions, is the most fundamental one.

Hyperledger Fabric is an open-source, enterprise-grade technology platform for permissioned distributed ledger solutions specially designed for use in enterprise environments. Underpinned by a highly modular and configurable architecture, it supports pluggable consensus and pluggable identity management protocols (such as Lightweight Directory Access Protocol (LDAP) or OpenID Connect), key management protocols, and cryptographic libraries. Besides, it supports smart contracts authored in general-purpose programming languages (such as Java, Go, or Node.js) and leverages consensus protocols that do not require native cryptocurrency to incent costly mining or to fuel smart contract execution. The Fabric platform is also permissioned. This means that a blockchain network can be operated under a governance model that is built off of the trust between participants who are known to one another, have been identified, and are often permissioned. The platform follows an execute – order – validate architecture.

These differentiated design features add up to make Hyperledger Fabric a good platform that performs well in transaction processing and transaction confirmation delays. Besides, it protects the privacy and confidentiality of transactions and implements smart contracts (called "chaincode" in Fabric).

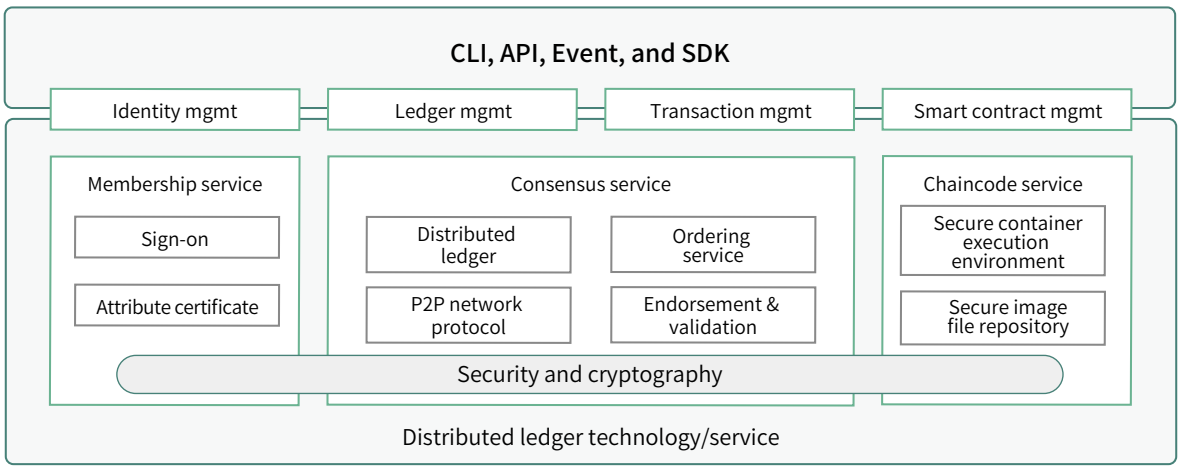


Figure 2-2 Hyperledger Fabric architecture

2.4.2 Quorum

Quorum[4] is an enterprise-grade, distributed ledger and smart contract platform built by J.P. Morgan, mainly designed to address special challenges of applying the blockchain technology in finance and other sectors. It is suitable for high-speed, high-throughput private transactions between organizations in a consortium. Quorum is an Ethereum-based distributed ledger protocol and so regarded as an enterprise edition of Ethereum. It provides private functions for transactions and contracts, supports various consensus mechanisms, provides permission management for networks and nodes, and delivers better performance. For these reasons, Quorum is considered a consortium blockchain platform.

The Quorum architecture has two layers: blockchain layer (lower) and business logic layer (upper), as shown in Figure 2.3.

- The blockchain layer consists of three components:
  - Quorum Node: Ethereum-based nodes for storage of transactions
  - Constellation – Transaction Manager: used for management of transactions
  - Constellation – Enclave: used for encryption and decryption of transactions
- The business logic layer uses functions provided by the blockchain layer to port traditional applications to the blockchain system. It consists of the following components:
  - Smart Contracts
  - DApps: decentralized application component
  - Legacy app integration: component for integration with legacy non-blockchain applications

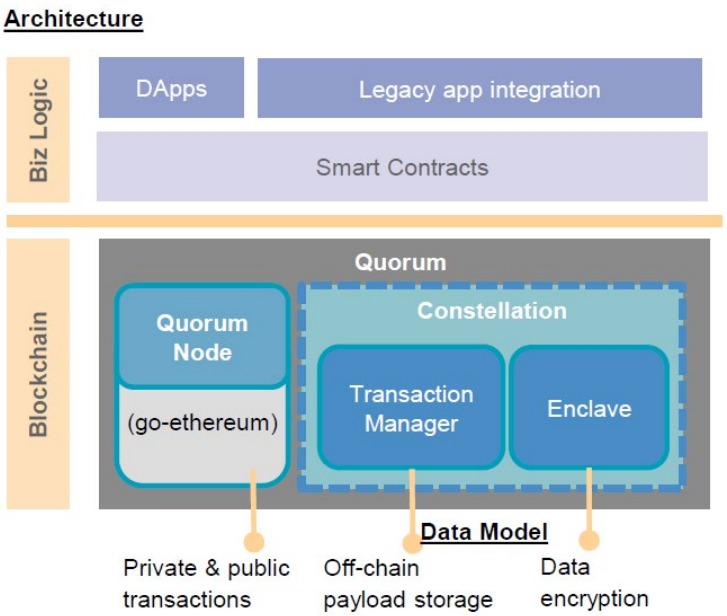


Figure 2-3 Quorum architecture

2.4.3 R3 Corda

Corda[5] is a distributed ledger platform launched by the R3 consortium. Founded in 2014, R3 leads a consortium of over 300 members. Initially, the consortium was made up of banks, with a view to exploring the possibility of using the blockchain technology for real-time financial transactions in global private networks. Today, R3 is expanding its focus from just financial scenarios to all areas where the blockchain technology can be potentially applied, including energy, health care, and supply chain management.

The Corda platform[6] is especially suitable for regulated financial institutions. Inspired by the blockchain system, Corda has gradually abandoned many traditional blockchain design options unsuitable for the financial sector. For example, unlike traditional blockchain platforms like Bitcoin and Ethereum, Corda does not use the global broadcast model that requires all nodes to be authenticated and all transactions to be recorded, but only requires participants of a transaction to have that transaction authenticated and recorded, thus greatly improving the throughput of transactions. Moreover, it resolves the dispute over

whether the shared ledger can ensure the privacy of transaction data and accelerates the commercial application of the distributed ledger technology.

Corda provides a smart contract framework that supports the following key behaviors and has the following characteristics:

- Based on the existing legal framework and being compatible with existing and emerging regulations, Corda records and manages financial agreements between two or more identifiable participants and changes in other shared data.
- Has an inter-firm workflow design that features decentralized controls.
- Supports consensus between enterprises at the level of personal transactions rather than at the global system level.
- Supports incorporation of regulatory nodes and observer nodes of the supervisory nature.
- Verifies the validity of transactions only between transaction participants.
- Supports a number of consensus mechanisms.
- Records explicit links between legal documents of the natural language and smart contract code.
- Uses tools that comply with industry standards.
- Strictly restricts data access only to users with explicit authorization or logical access permissions.

3

Security Threats to Enterprise Blockchains

This chapter analyzes security threats facing enterprise blockchains[7].

3.1 Threats to the Underlying Layer

- Storage and computation facilities, as carriers of blockchain systems and applications, are vulnerable to unauthorized access.

  Physical devices, if with vulnerabilities unpatched, have themselves and their physical environments (equipment rooms) exposed to potential risks, such as unauthorized device access and compromise. The virtualization technology, which is the basis of cloud-based blockchain services, is vulnerable to resource abuse and broken access control. As the carrier of cloud-based blockchain service systems and applications, the virtualization technology (container, virtual machine (VM), and virtual network) dynamically creates and deletes virtual applications depending on the platform's management function. As resources are used on a shared basis, security risks arise, including race condition for resources, resource abuse, and broken access control (VM escape, container escape, and virtual local area network (VLAN) hopping).

- P2P networks are crucial to blockchain operations and faced with various network and communication risks.

  The blockchain technology adopts the P2P network architecture, allowing only permissioned nodes to join a consortium blockchain. The risk in this aspect is compromise by malicious nodes that bypass the permission or identity check mechanism. Besides, nodes and networks may suffer such attacks as network communication interception, network routing attacks, and network denial-of-service (DoS) attacks. Typically, consortium blockchains are prone to Sybil attacks, where an adversary generates fake faulty nodes to make consensus impossible.

3.2 Threats to the Core Layer

- The consensus mechanism/algorithm design is flawed, which may result in the crash of the trust system.

  A consensus mechanism is an algorithm used to achieve the necessary agreement between

nodes on a blockchain. It is the core capability of blockchains. A design or implementation flaw in a consensus mechanism may allow attackers to launch consensus attacks, weakening decentralization and lowering the degree of trust in data on the blockchain. Current consensus attacks include 51% attacks, timestamp tampering attacks, bribery attacks, selfish mining, and double-spend attacks.

- Cryptographic algorithms, faced with challenges of enhanced computing power and new computation models, are at risk of being cracked in future.

  The blockchain technology employs a large number of cryptographic algorithms, including hash (digest) algorithms and asymmetric algorithms. Hash algorithms may suffer hash collision attacks, leading to identity impersonation, false transactions, and consensus mechanism failure. Asymmetric cryptography algorithms, when attacked, may affect the encryption and digital signature process, hence message disclosure, private key exposure, or identity spoofing. With the development of cryptography technologies and adoption of new technologies such as quantum computers, cryptographic algorithms now in wide use are faced with an increasing risk of being cracked.

- A vulnerable operating environment of smart contracts may prevent contracts from being executed securely and fairly. VMs where smart contracts are executed and authentication and control mechanisms may contain vulnerabilities that allow attackers to consume network, storage, and computing resources by deploying malicious smart contract code and disrupting the normal business order, which may give rise to other threats. Smart contracts, after being deployed, are seldom updated, making the impact of malicious smart contracts last longer.

  If the implementation of smart contract code is prone to any vulnerabilities, risks such as business fraud may arise. The language and code implementation of smart contracts may contain security vulnerabilities and backdoors, such as transaction order dependency, timestamp dependency, misoperation errors, and reentrancy attacks that once threatened the security of Ethereum. These vulnerabilities, when exploited during contract calls and execution, will affect the correctness and integrity of the contract processing logic, resulting in untrusted contract behavior and financial losses.

- Ledger records

  Ledger records are publicly accessible. If the ledger contains sensitive information or associates accounts with true user identities, or links between blockchain transactions are leveraged to guess sensitive information, blockchains are at risk of user privacy disclosure.

3.3 Threats to the Service Layer and User Layer

- An insecure access and node management mechanism may allow unauthorized users or malicious nodes to gain access to a consortium blockchain, giving rise to the risk of exposing internal data of the consortium blockchain. Some consortium blockchains use a weak consensus mechanism for the purpose of better performance and at the same time use trusted nodes as a complement to the trust mechanism. In this case, unauthorized node access would probably lead to 51% attacks or ledger tampering, affecting the consensus result.
- Any vulnerabilities in ledger applications or in the logic design and implementation of service functions may disrupt the secure operation of services.

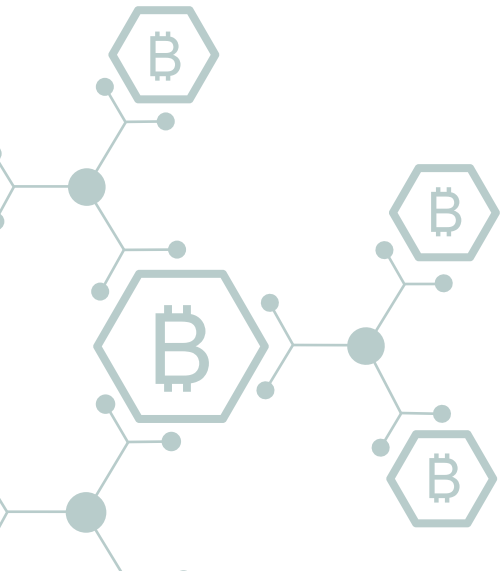
  Application security relies on the service logic, service code, and how thoroughly tests are conducted. Related risks include the logic error, trojans, and backdoors.
- User and management functions are responsible for management of blockchain users, platform users, and platform functions, with the potential risk of identity spoofing, improper permissions, privilege escalation, and misoperation.

3.4 Threats to Cross-Layer Functions

Cross-layer functions include development, operations, security, and supervision and audits, which are paramount to the proper running of the blockchain platform, services, and business. They are exposed to the risk of insufficient management of resources and business lifecycle management. Traditional monitoring, operation and maintenance (O&M), and disaster recovery functions are prone to the risk of improper administrative privileges and loss of control over the management process. Besides, cross-chain service management should take cross-chain data disclosure into consideration.

4

Enterprise-related Blockchain Security Landscape



The enterprise-related blockchain security landscape has two layers of meanings: enterprise blockchain security situation and blockchain-related enterprise security situation. The former refers to the security posture of enterprises that have deployed blockchain applications. In the latter case, although an enterprise does not deploy any blockchain applications, security threats facing it point to blockchains.

In terms of the enterprise blockchain security situation, historically, blockchains were mainly public ones at the initial stage. Therefore, most vulnerabilities disclosed and security events detected are related to public blockchains. Consortium blockchains are still infants, so research on their security is conducted tentatively, explaining why there are so few vulnerabilities and security events related to them. Technically, private, consortium, and public blockchains are basically the same in their architecture and technologies used. In this sense, for secure implementation of consortium blockchains, it is advisable to analyze known vulnerabilities in common blockchains, which will inform security controls for consortium blockchains. In addition, even if an enterprise does not deploy any blockchain applications, it should pay due attention to blockchain-related cybersecurity events.

This chapter first provides statistics about blockchain-related vulnerabilities, then discusses known enterprise security events, and ends with an analysis of the enterprise blockchain security situation.

4.1 Blockchain-related Vulnerabilities

As described previously, vulnerabilities in enterprise blockchain applications are not very many. To be specific, the number of blockchain-related vulnerabilities with a Common Vulnerabilities and Exposures (CVE) ID in the National Vulnerability Database (NVD) is 408, most of which (401) were discovered by a security laboratory in 2018. Among these 401 vulnerabilities, the vast majority are high-severity integer overflow vulnerabilities concerning smart contracts. In the NVD, there is one vulnerability related to Hyperledger, namely transaction and block signature verification bypass (CVE-2018-3756) in Hyperledger Iroha. The NVD has no vulnerability associated with Quorum and R3 Corda.

Obviously, there are only a small number of vulnerabilities related to enterprise blockchain platforms. However, when it comes to common blockchain applications, cryptocurrency-related vulnerabilities have been reported from time to time. The following analysis is conducted around vulnerabilities in Bitcoin

and Ethereum.

en.bitcoin.it/wiki/ lists all Bitcoin-related vulnerabilities[8], which had amounted to 43 by February 2020 and mainly fall within the categories listed in Table 4.1.

Table 4-1 Categories of Bitcoin-related vulnerabilities

Category	Quantity
DoS	14
Fake Conf	8
Netsplit	5
Theft	4
Exposure	4
Inflation	2
Deception	1

In the NVD, up to 532 vulnerabilities are related to Ethereum, the majority of which are found in smart contracts (including the aforementioned 401).

The CVE Details website and en.bitcoin.it/wiki classify vulnerabilities in different ways, but they both have the categories of data theft and DoS. On both websites, the largest number of vulnerabilities fall within the category of DoS, in which a node is paralyzed, preventing consensus from being reached. Following DoS are Fake Conf and Netsplit, which are mostly exploited to launch double-spend attacks on consensus mechanisms.

Although the consensus layer in a blockchain system is the hardest to break into, it does not mean that this layer is impregnable. Once a flaw is detected, attackers will make strenuous efforts to attack the consensus layer because of the potentiality of earning huge profits after compromise. This should sound the alarm for blockchain application developers. Although what is exposed is traditional vulnerabilities in the code layer, attackers exploit them to attack consensus mechanisms.

In the *Vulnerabilities on Hyperledger Fabric*[9], the authors point out two security limitations: First, the identity of an endorser is known to all members within a channel, which opens a gateway for DoS attacks on endorsers in order to either block transactions pertaining to a client, or to degrade network efficiency. Second, the technology is prone to wormhole attacks, that is, within a channel, compromising

a member leads to leakage of ledger information of all members to everyone outside the channel.

It should be noted that, although no vulnerability has been found in Hyperledger Fabric, Quorum, or R3 Corda, their runtime environments are never immune to vulnerabilities. For example, Hyperledger Fabric uses Go and Java as runtime environments of smart contracts. Vulnerabilities related to the two languages, such as CVE-2016-3958 and CVE-2017-10388[10], may be exploited by attackers. Besides, Hyperledger Fabric uses Docker as the engine for isolated execution of smart contracts. Vulnerabilities in the Linux kernel and Docker, such as Dirty COW (CVE-2016-5195), could allow attackers to escape Docker containers.

4.2 Security Events and Research Related to Enterprise Blockchains

In 2018, Gartner predicted that, by 2020, at least one disastrous vulnerability discovered would take down a major blockchain platform, incurring huge financial losses[11]. At present, blockchain-related security events are mainly attacks on cryptocurrency exchanges for theft of cryptocurrency. Up to now, no security event has been reported to target enterprise blockchains. However, with more and more enterprises choosing to apply consortium blockchains or other blockchain technologies in various scenarios, we believe that more security events pointing to enterprise blockchains will appear in years to come.

For in-house security teams, such security events as attackers maliciously targeting blockchains to compromise the integrity and availability of information systems (or more specifically, making money directly from cryptocurrency) deserve more attention.

An organization, once attacked, usually needs to pay a great amount of ransom via cryptocurrency or anonymous currency.

In ransomware events, attackers usually demand victims to pay a certain amount of cryptocurrency as ransom. In the past few years, some factories and carriers, such as Honda, LG, and TMSC, have suffered great losses from disrupted production or services caused by ransomware events. Cybersecurity Ventures predicted in 2017 that ransomware damages would reach USD 11.5 billion annually by 2019[12] . It is a paramount task for in-house security teams to create a defense-in-depth protection system that

enables organizations to take precautions before events, conduct prompt detection and response during events, and achieve better resilience after events.

In a cryptojacking event, a hacker, by planting malicious code in a website, makes website viewers unknowingly contribute their computing power to cryptomining activities, thus indirectly earning profits for the attacker. This will not only compromise the integrity of web services but also consume excessive amounts of electric power and computing resources, resulting in users' computers working improperly. According to *The Cyber Threat to UK Business* for 2018, nearly half of enterprises around the world had suffered cryptojacking attacks and nearly 50,000 websites had been infected with cryptojacking scripts. Compared with ransomware and other types of malware, cryptojacking is easier to conduct and has a higher return on investment (ROI) as it does not require compromise of the target system to establish command and control (C&C), but only consumes victims' CPU cycles and electric power for computation of hash functions to mine cryptocurrency. Thanks to its covertness and convenient profitability, cryptojacking has become the most popular cyberattack method these years.

In NSFOCUS's *2019 Annual IoT Security Report*, we disclosed a botnet that exploited IoT devices to mine Monero. According to rough statistics, this botnet controlled over 10,000 zombies, with the maximum number of active zombies approaching 600 in a single day. This botnet was the most active in July 2019 and is still there in the cyberspace.

4.3 Enterprise Blockchain Security Situation

The application of the enterprise blockchain is still at an early stage. With the wider adoption in future, there will be more vulnerabilities and related security events reported. It can be expected that most vulnerabilities, especially such common security issues as insecure functions and out-of-bounds access, will be linked to smart contracts. There will also be vulnerabilities that may disrupt services or enable attackers to earn profits.

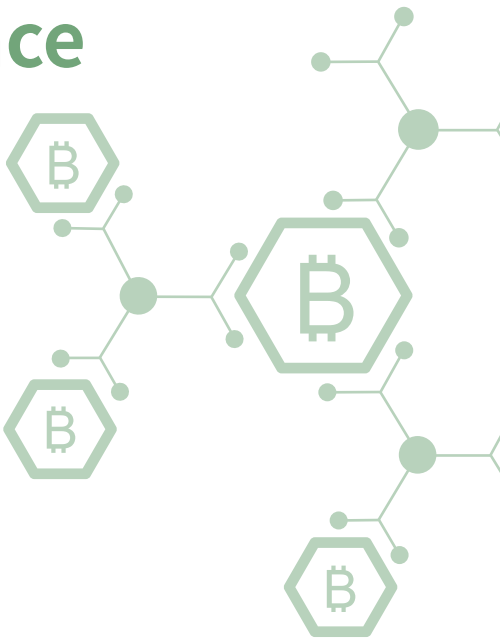
In blockchain-related security events targeting enterprises, ransomware and cryptojacking are major threats that have long harassed enterprises. The anonymity of cryptocurrency and the convenience of cashing in on cryptocurrency mean that these types of attacks will exist for a long time. Then,

understandably, the rise and fall of cryptocurrency prices can somewhat lead to the rise and fall of such attacks.

In a medium-to-long-term prediction, Gartner says that the poor scalability and interoperability of blockchains will be overcome by 2023 and envisages that the technology will unlock value in 2023[13]. With a predictable increase in enterprises' adoption of blockchain applications, security events targeting enterprise blockchains will probably become a new normal after 2023. For enterprises ready to deploy or having deployed blockchain applications, how to build up the situation awareness capability towards blockchain systems is an imperative problem that they should address.

5

Enterprise Blockchain Security Governance



5.1 Regulatory Policies

With years of development, the blockchain industry has taken shape, but enterprise blockchain applications are still at an exploratory stage. The blockchain ecosystem contains SPs, application vendors, and users. SPs in this context provide blockchain information services, whose compliance requirements are surely different from those for other information services (such as cloud services) due to the blockchain technology's unique characteristics of non-deletability and support for post-event forensics.

5.2 Data Governance

With the promulgation of laws and regulations, such as GDPR, data security is becoming increasingly important. Collection, management, and exchange of personal data are all subject to compliance requirements.

Some statutes stipulate that blockchain information providers, as a type of network SPs, should provide the data deletion capability. However, one of the most distinctive features that differentiate the blockchain technology from other technologies is non-deletability of data, which poses the greatest risk to compliance.

Malicious actors leverage this feature of blockchains to upload illegitimate information, creating an adverse impact, or upload malicious code or C&C addresses to achieve persistence. In this context, data governance is an important indicator to measure whether data in the blockchain system is operable. In traditional public blockchains, it is almost an impossible mission to delete incorrect or malicious information. The only exception is the DAO event, in which Ethereum prevents malicious on-chain transactions by means of hard forks. Despite of this, there are still political data and suspicious business data stored in Ethereum. In contrast, data governance for consortium blockchains is possible. This is because a consortium blockchain has a limited number of nodes that have been validated by each other. Besides the online consensus mechanism, it is possible to negotiate offline. When consensus is reached about deletion of a block, all nodes (nodes storing this block and orderer nodes) will be rolled back to the previous height. For example, in Hyperledger Fabric, we can run the rollback

command to roll back the current peer to the previous block height.

USU, a digital asset transaction platform built on the EOS ecosystem, has a mirroring mechanism to implement fast synchronization of node data and regular creation of images of local ledgers. With a convenient rollback mechanism, the platform allows users to specify an image label for rollback when consensus is reached.

The nature of blockchains makes it possible to manipulate data. The problem is that the cost of doing so increases with the number of nodes on a blockchain system. This explains why there are not so many attacks against blockchains. When it comes to data governance, it is necessary to find a balance between technologies and compliance by acquiring the capability of controlling data at some cost (communication cost of all involved organizations, potential system downtime cost, and so on).

5.3 Smart Contract Governance

A smart contract is executable code that all endorsers acknowledge. Consistent code and identical input enable all endorsers within the global scope to reach consensus on the transaction result, thus saving the costs of labor and time otherwise incurred by manual checks and execution for traditional contracts.

However, on the other hand, smart contracts need to be deployed on all endorsers of a decentralized blockchain system. Even if it is a consortium blockchain, it is impossible to simultaneously update contracts on all nodes, thus exposing blockchain applications to a great security risk: When a vulnerability is found in a smart contract mechanism, it may be rather costly to fix the code and update contracts.

The security of smart contracts is extremely important. When a vulnerability or error is found, it is impossible to shut down the system and fix it by means of centralized upgrade as we usually do for a centralized system. Smart contracts have a direct control of money or critical transaction data. A vulnerability in the mechanism could cause direct financial losses. In this sense, it is very important to enhance their security measures.

The current research in this area is focused on how to use formal verification methods, which are usually applied in chip design or military control systems, on smart contracts to minimize human errors by means of mathematical proofs. For example, Beosin's [1] (also known as Chengdu LianAn Technology Co., Ltd.) automatic formal verification tool can effectively detect common vulnerabilities in the chaincode of Hyperledger Fabric and provide users with repair suggestions.

1 https://www.lianantech.com/

6

Enterprise Blockchain Security Solution

To cope with security risks facing enterprise blockchains, we propose an enterprise blockchain security solution (Figure 6.1). Based on the technical stack of blockchains, the solution vertically consists of underlying layer security, core layer security, and user and service layer security. From the perspective of the security lifecycle, the solution covers development delivery, security protection, exception detection, response and recovery, and security services throughout the lifecycle.

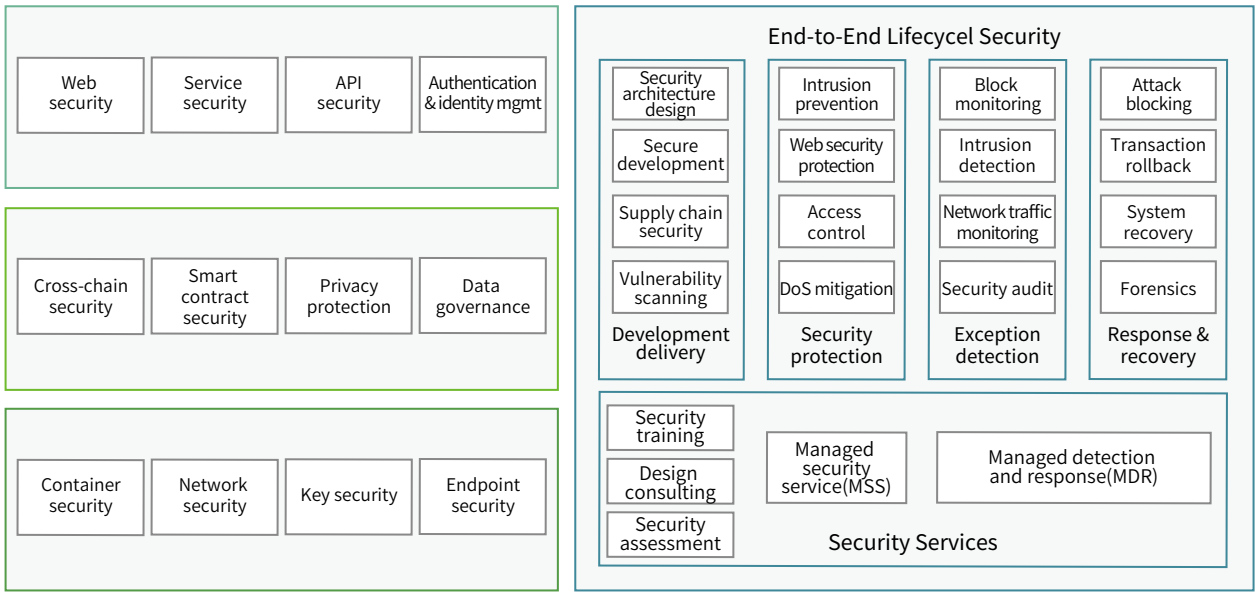


Figure 6-1 Enterprise blockchain security solution

6.1 Underlying Layer Security

Underlying layer security includes container security, network security, key security, and endpoint security.

6.1.1 Container Security

The container technology provides lightweight virtualization and isolation of resources by sharing the kernel of the host operating system. These years, it has been widely used in blockchains, DevOps, and microservices. Hyperledger Fabric is implemented based on the container technology, with smart contracts running in containers. Therefore, the security of containers has a direct bearing on the runtime

security of smart contracts or even the security of blockchain nodes.

Container security involves security assessment of container images and repositories, detection of container runtime exceptions (especially container escape), microsegmentation, and access control. For details about container security, refer to *2018 NSFOCUS Technical Report on Container Security* [14].

6.1.2 Network Security

Enterprise blockchain applications are typically deployed in a distributed manner and are interconnected over a computer network. Therefore, they cannot evade from traditional cybersecurity risks and need to be protected with traditional cybersecurity measures, including security zoning, access control, traffic scrubbing, intrusion detection, malicious code protection, and VPN access.

In addition, blockchain nodes are interconnected over a P2P network, so the deployed network security solution should include overlay network support.

6.1.3 Key Security

Key assignment and management play a very important role in enterprise blockchains. The leakage of keys can lead to disclosure of privacy and encrypted data, and worse still, may allow attackers to forge transactions, thus disrupting the normal operation of the blockchain system. Therefore, to ensure the security of keys, a common practice is to store keys in a hardware security module (HSM).

6.1.4 Endpoint Security

Endpoint security is intended for protection of blockchain nodes, which should be implemented around the following aspects:

- Routine cleanup operations: operating system (OS) security configuration and hardening, trusted computing stacks, installation of antivirus software or EDR software, …
- Runtime monitoring: abnormal behavior detection, memory monitoring, escape detection, …
- Response to ongoing malicious attacks

6.2 Core Layer Security

Core layer security involves cross-chain security, smart contract security, privacy protection, and data governance.

6.2.1 Cross-Chain Security

The interaction of enterprise blockchain applications inevitably involves the use of the cross-chain technology. To break the bottlenecks of a single-chain framework in performance, capacity, and segmentation and meet requirements for coordinated multi-organization applications, consortium blockchain projects represented by Hyperledger Fabric adopt the cross-chain technology to improve system availability. The cross-chain technology is designed for data exchange between blockchains, but vulnerable to such security issues as notary collusion, sidechain verification for parent chain transactions, transaction channel DoS, long-range attacks, eclipse attacks, block bloat, and cross-chain replay attacks.

Therefore, at the time of designing sidechains, the preceding possible threats should be considered and multiple security mechanisms should be deployed against them. For example, Interledger initially adopted the notary mechanism to facilitate cross-chain operations. Then considering the possibility of notary collusion, Interledger later incorporates the hashlock concept. Polkadot introduces a new shared security model that provides the same security assurance for chains by enabling them to share "pool security" while interacting with each other. The Cosmo system manages its security model by introducing the sovereign zone concept. To prevent a malicious zone from entering the Cosmos Hub to attack the Cosmos network for obtaining atoms, each zone allowed access to the Cosmos Hub should have its own secure, decentralized network. Such a mechanism allows Cosmos to have a higher degree of decentralization, effectively isolating malicious attackers and avoiding security risks caused by centralized privileges.

A key management mechanism, including but not limited to key generation, distribution, storage, and recovery, can be employed to implement strong authentication. Hyperledger Fabric manages and authenticates all system participants with a participant identity management mechanism, which

includes the access control function that authorizes specific participants to perform specific operations and grants different permissions to different chains, thereby enhancing the security of cross-chain data and avoiding unauthorized access and leakage of critical data. For example, as described previously, Hyperledger Fabric allows specific user IDs to call chaincode applications, but does not allow deployment of new chaincodes.

Setting up definitive checkpoints is a good method against long-range attacks.

Another thing to note about cross-chain operations is compliance. It is advisable to define security levels for different blockchains to prevent higher-security chain data from flowing into lower-security chains.

6.2.2 Smart Contract Security

As we mentioned previously, most blockchain-related vulnerabilities point to smart contracts. Insecure code or logic flaws can pose severe security risks to enterprise blockchain business.

Therefore, it is important to design smart contracts in strict accordance with secure design specifications and conduct security audits on smart contracts before they go live to avoid potential security risks. Security audits of smart contracts should be conducted around logic flaws, data security, race conditions, and incorrect handling of external calls.

Moreover, formal verification can be adopted at the security audit stage to verify the validity of smart contracts. For example, Christian Reitwiessner introduced Why3, a formal verification engine, into Ethereum, allowing computers to create and check a mathematical proof of assertions about the behavior of the contract[15].

6.2.3 Privacy Protection

In blockchain applications, transaction participants' true identities, IDs, and IP addresses should be under privacy protection, which can be implemented by using an obfuscation mechanism. This mechanism obfuscates addresses included in transaction input and output, thus disassociating

transaction contents from identities while verifying transactions. Another option is to use a cryptographic scheme based on ring signatures to achieve identity anonymity and privacy protection in transactions. For a higher level of privacy protection, our recommendation is to use the cutting-edge zero-knowledge proof method to ensure the legitimate execution and verification of transactions without revealing transaction participants' privacy. Generally, the higher level of privacy protection a technique delivers, the larger time overhead it requires to work properly in a blockchain network. In practice, users should select an appropriate technique depending on particular scenarios.

For privacy protection of transaction contents and ledger data, an encrypted and authorized access mechanism facilitates finer-granularity access controls for identity data of transaction participants; a private transaction mechanism and channel mechanism isolate ledger data of one organization from another in a consortium blockchain, and isolate transaction broadcasts from verification. When a smart contract performs computations for two or more parties, decentralized secure multi-party computations can be used as a complementary means to prevent original data and privacy of transaction participants from being exposed and disclosed in the computation process while ensuring reliable computation results.

6.2.4 Data Governance

For the purpose of data governance, blockchain information SPs should provide the data deletion capability. For example, a convenient rollback mechanism can be employed to regularly create images of local ledgers. With consensus reached, users can specify an image label for rollback.

6.3 User and Service Layer Security

User and service layer security covers web security, service security, API security, and authentication and identity management.

6.3.1 Web Security

Enterprise blockchain applications involve websites accessible to users. Therefore, in blockchain

implementation, web security should be considered and related controls should be deployed against common web attacks, including SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).

Current web security controls include web application firewalls (WAFs) and Runtime Application Self-Protection (RASP) deployed on the server side, and the content security policy (CSP) deployed in client browsers.

6.3.2 Service Security

Security risks are specific to industries. Enterprise blockchain SPs should develop appropriate business risk control systems for different business scenarios to ensure business security.

There is no one-size-fits-all solution for all enterprises deploying blockchain applications that vary from industry to industry. When developing solutions, blockchain SPs usually have two paths to follow: (1) profiling normal services, such as the normal service scope and common service call sequence, to detect service requests that deviate a lot from baselines and therefore require particular attention; (2) analyzing malicious service patterns before developing rules or training generative model parameters.

6.3.3 API Security

The wide adoption of application programming interfaces (APIs) lays the foundation for digital transformation of enterprises. APIs are also widely used in programmatic driven blockchain applications, as demonstrated in Hyperledger Fabric, which deploys blockchain nodes through APIs of Docker and loads or executes chaincodes through APIs of Fabric peers.

In blockchain applications, if an attacker launches a DoS attack on APIs, the availability of the entire system will be affected; if the attacker steals the login credential of a legitimate user, he or she can perform operations and further conduct frauds, steal information, or expose privacy.

For this reason, the API design should be put under security assessment and API calls should be

managed and monitored to prevent the abuse or unauthorized call of APIs.

6.3.4 Authentication and Identity Management

In enterprise blockchain applications, each endorser node, committer, and management node are authenticated by the Certificate Authority (CA). This authentication mechanism simplifies the consensus mechanism of blockchains and provides underlying support for high-throughput, lower-latency applications.

In the past few years, data breach has become an increasingly severe issue, giving rise to more protection regulations, which are continuously supplemented and improved. A large number of data breach events result from identity theft. For this reason, the zero-trust concept has found its way deep into people's heart. The principle behind it is that each operation should be authorized and each access request, before being authenticated, is untrusted. To ensure the security of enterprise blockchain applications, the CA should properly manage identities of all participants and verify their permissions for operations on resources. In addition, a unified resource access policy should be designed and applied globally, ensuring that, for each attempt to access the blockchain system and each attempt to access and perform operations on data on chains, the initiator should be authenticated and authorized to do so.

6.4 End-to-End Lifecycle Security

Laterally, security should be considered throughout the lifecycle of an enterprise blockchain. From the perspective of security teams, end-to-end lifecycle security is conducted in four phases, namely, delivery, protection, detection, and response, plus third-party security services throughout the lifecycle.

6.4.1 Development Delivery

From the perspective of security teams, the delivery phase involves the architect team, R&D team, and test team, aimed at delivering a secure blockchain system. Specifically, the architect team should study characteristics of and analyze risks to blockchains before designing a secure full-stack blockchain

platform and applications. The R&D team should write secure and robust code by following secure coding principles to minimize bugs in code. The test team should try their best to identify all bugs in code according to security test principles.

A thing to note in code development is that third-party libraries and open-source software referenced in code should be free from vulnerabilities to ensure the supply chain security.

After a blockchain system is deployed, ongoing vulnerability assessment should be conducted by scanning the blockchain platform, smart contracts, and container images from time to time for vulnerabilities, which, once detected, must be fixed as soon as possible.

6.4.2 Security Protection

After a blockchain system is deployed, necessary security protection mechanisms should be deployed promptly, such as the intrusion prevention system (IPS), WAF, network firewall with the access control functionality, and anti-DDoS system (ADS). For details about these products, refer to the related user guides.

6.4.3 Exception Detection

For a blockchain system in operation, defense-in-depth is a good idea, which always assumes that attackers may break the aforementioned protection mechanism. Based on this assumption, an exception detection mechanism should be in place to promptly detect exceptions. Typical examples of such detection mechanisms include block monitoring, intrusion detection, network traffic analysis, and security audit.

- Block monitoring: For an enterprise blockchain in operation, a block monitoring system must be deployed to create various indicators according to the characteristics of the blockchain and business to detect abnormal transaction values, forks, or other abnormal behavior.
- Intrusion detection: continuously monitors network communications and generates alerts on suspicious attacks.

- Network traffic analysis: analyzes behavior related to network traffic (including but not limited to flows, payloads, and files), helping enterprises identify suspicious traffic or network access.
- Security audit: records and checks participants' access to resources and audits network behavior to identify unauthorized access or other abnormal behavior.

6.4.4 Response and Recovery

When some abnormal behavior is detected, the security team should check whether it is an attack and, if so, make immediate efforts to respond to the event. The response and recovery phase involves attack blocking, transaction rollback, system recovery, and forensics.

- Attack blocking: blocks a malicious attack when it happens and isolates the affected hosts as required to protect the system from further damage.
- Transaction rollback: When a malicious transaction is detected, the transaction rollback function, upon consent of all transaction participants, rolls back ledgers of all committers to the normal state before this transaction happens to meet compliance or business requirements.
- System recovery: recovers a system that becomes faulty because of an attack, including but not limited to the preceding transaction rollback operation.
- Forensics: provides evidence to help identify attackers behind security events.

6.4.5 Security Services

The enterprise blockchain system uses a variety of technologies, hence a complex architecture. Given the complexity of this system, it is impossible for an in-house security team to independently fulfill the security assurance task. In this context, using third-party security services throughout the system lifecycle is undoubtedly a good idea. That is why so many public cloud platforms begin to provide Blockchain-as-a-Service (BaaS).

In the development delivery phase, security services include security consulting at the time of system design, security training during system development, and security assessment prior to system go-live.

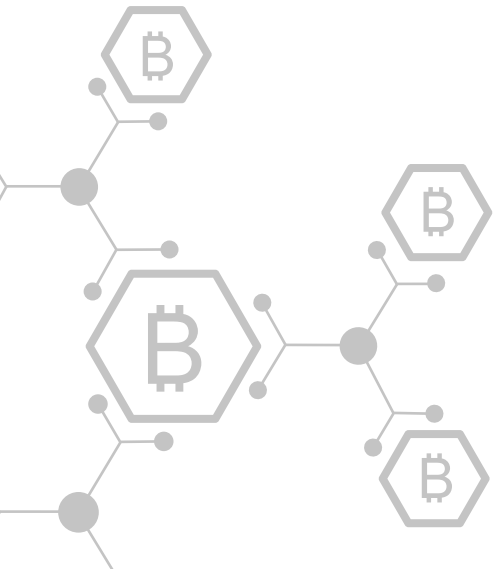
- Security consulting: includes, without limitation, consensus mechanism-specific and cryptographic algorithm-specific security recommendations and recommendations about privacy protection.
- Security training: provides systematic training services that fit in with enterprises' needs by familiarizing enterprises with the blockchain technology, blockchain security techniques, and blockchain application security solutions. With an anatomy of blockchain-related security events, the SP helps in-house security professionals understand and grasp security knowledge about blockchain applications and put such knowledge into practice. In the long run, blockchain-related security events caused by the lack of blockchain security knowledge in the secure development lifecycle will, hopefully, be minimized.
- Security assessment: includes source code audits and penetration tests to promptly discover bugs in the code and system, thus nipping security hazards in the bud.

In the security protection phase, security vendors can provide the managed security service (MSS), helping in-house security teams with the go-live of security products, policy configuration, and event management.

In the exception detection and response phases, third-party SPs can also step in, providing managed detection and response (MDR). With regular or on-demand security detection, an SP, when detecting a malicious attack, helps the in-house security team through the event response process before finally resolving the issue.

7

Conclusions



The adoption of the blockchain technology makes security a marked issue for organizations. The traditional model of "promoting the fast growth of business in advance of security efforts" is no longer feasible. In fact, security should be considered throughout the blockchain system lifecycle. Blockchains are less tolerant of security risks. In public blockchains, the lack of security controls could result in the cryptocurrency value dropping to zero, chain forking, financial losses to transaction participants, or even bankruptcy of cryptocurrency exchanges. Such events are nothing new in the blockchain industry. Although there are few media reports on security events concerning consortium blockchains, the lack of security controls in such a blockchain will potentially lead to data written by all participants onto chains being untrusted, hence the failure to perform smart contracts as expected. As a result, this blockchain will probably "collapse". Even if discovering security vulnerabilities in a blockchain, in most cases, legitimate users will not exploit them considering the risk of being tracked and the importance of keeping the blockchain integrated to avoid business disruption. But this does not mean that there is no risk at all. A legitimate user's misoperation or an act of sabotage by a "mole" within an enterprise will expose the system to threats. Worse still, an insecure system may be compromised by attackers, who, by obtaining private keys of legitimate users, may engage in some disruptive activities. These issues, if not properly handled, may cause devastating image to blockchain systems.

For the preceding reasons, we develop this whitepaper, in a bid to promote close collaboration between security vendors, universities, blockchain SPs, and users. Security is not an issue that can be addressed by one player. Only through multi-party cooperation, can a secure ecosystem be established for enterprise blockchains, enterprise blockchain users be better served, and the value of enterprise blockchains be effectively tapped.

References

1 Predicts 2020: Blockchain Business

2 http://www.chinabankingnews.com/2020/02/18/idc-makes-10-predictions-for-chinas-blockchain-sector-10-of-chinese-cities-using-digital-currency-by-2023/

3 Hyperledger project, https://www.hyperledger.org/

4 Quorum, https://www.goquorum.com/

5 Corda, https://www.corda.net/

6 https://docs.corda.net/_static/corda-introductory-whitepaper-zhs.pdf

7 ITU-T X.1401. Security threats to Distributed Ledger Technology

8 https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures

9 Nitish A, Raghav G, Manas G. Vulnerabilities on Hyperledger Fabric[J]//Pervasive and Mobile Computing, 2019

10 Overview of hyperledger (blockchain technology) security design, http://www.antihackingonline.com/blockchain/overview-of-hyperledger-blockchain-technology-security-design/

11 David Anthony Mahdi, Blockchain, Is This Stuff Secure? How CISOs Can Evaluate the Security Risks of Blockchain, Gartner Summit 2018

12 Global Ransomware Damage Costs Predicted To Hit $11.5 Billion By 2019, https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/

13 Gartner sees blockchain as top tech trend for 2020, https://www.ledgerinsights.com/gartner-sees-blockchain-as-top-tech-trend-for-2020/

14 2018 NSFOCUS Technical Report on Container Security, https://nsfocusglobal.com/2018-nsfocus-technical-report-container-security/

15 Formal Verification for Solidity Contracts, https://forum.ethereum.org/discussion/3779/formal-verification-for-solidity-contracts

SECURITY MADE SMART & SIMPLE

www.nsfocusglobal.com