Proceedings of the 3rd International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/6/20230463

Security analysis of blockchain-based service network

Xuzhuo Zhang[1,3], Pengju Lyu[2]

[1]Faculty of Engineering, Computer and Mathematical Sciences, University of Adelaide, Adelaide, SA 5000, Australia
[2]Faculty of Data Science, City University of Macau, Macau SAR, China

[3]Zhangxuzhuo9613@163.com

Abstract. Recently, the extensive applications of blockchain technology in fields like financial exchanges, insurance, Logistics and healthcare has proven to be pragmatic and revolutionary. In order to enable the blockchain to have a more complete development space, Blockchain-based Service Network (BSN) was proposed. It integrates the developers, portal, cloud resources and blockchain framework to provide the basic environment for blockchain applications. Researches on its security have kept place with the advent of blockchain technology, while potential issues on BSN security remain largely unexplored. In this paper, we are devoted to diving deep into BSN security-related problems, specifically the security of BSN is analysed, and corresponding real attacks are summarised and investigated by checking the blockchain system adopted by BSN, which will provide a good reference for the future research. Finally, we reach the conclusion that although security issues still exist, there are fewer security issues compared with traditional blockchain.

Keywords: blockchain-based service network, BSN, security, blockchain.

1. Introduction

The development and innovation of blockchain technology have made an enormous contribution to regional information sharing and exchanging. There are nonetheless substantial spaces for further improvement on existing blockchain ecosystem. Hence in 2020 emerged the most significant tool-Blockchain-based Service Network (BSN), a global universal blockchain infrastructure is essentially conducive to a wide range of setbacks evident in nowadays blockchain technology [1]. It provides a common worldwide infrastructure for the deployment, operation and maintenance of blockchain applications [1]. The prominent security issues concern as much with blockchain as it does with BSN, the former has been vastly investigated while the fact that BSN adopts various blockchain technology does not mean the security situation for BSN is the same as that for common blockchain.

In this paper, the function of BSN is delineated in the next section. The security problem of BSN and the potential attacks are closely examined dealing with respects to each BSN component in the subsequent following sections.

2. Background

The purpose of BSN is to create a complete and convenient development environment for blockchain. It integrates the developers, portal, cloud resources and blockchain framework together to provide the

DOI: 10.54254/2755-2721/6/20230463

basic environment for promoting the sustainable development of blockchain technology by letting framework operators use BSN to create better business models and build their own ecosystems.

In general, the BSN consists of 4 components: public city nodes, blockchain framework, BSN portals and BSN network operation platform, and the structure of BSN is displayed in figure 1, blockchain application can be deployed via BSN portal by selecting appropriate blockchain framework and purchasing related computing and other resources from public city nodes, and applications are governed by BSN administrator from BSN network operation platform.

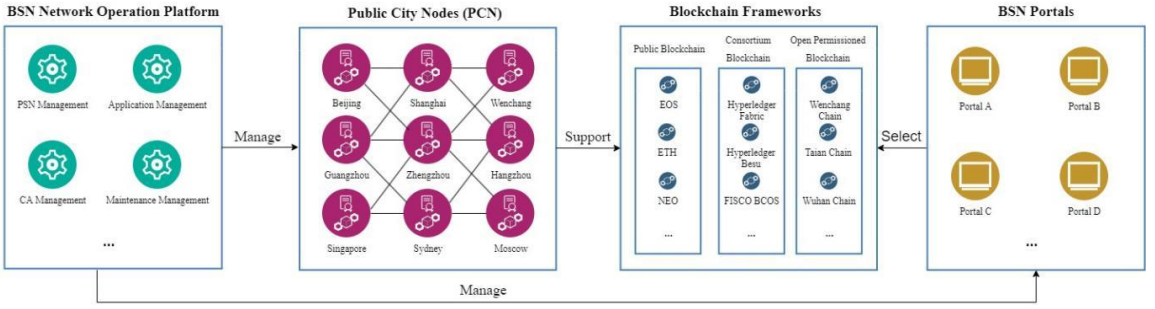

Figure 1. The structure of BSN.

2.1. Public city node

Public city nodes (PCNs) form the fundamental structure of BSN network, it provides cloud-like resource allocation including computing power, data storage, data transaction and access control for blockchain [1]. The BSN includes a consensus order cluster service and public city nodes [2]. Each city could develop one or multiple public city nodes linked through the internet for developing a national physical city node blockchain service network. Blockchain application publishers could now just deploy their application across multiple city nodes on the BSN.

2.2. Blockchain framework

Blockchain frameworks are to BSN what operating systems are to computers. Various mainstream public blockchain, consortium blockchain and open permissioned blockchain frameworks are supported by BSN. By selecting the suitable framework and purchasing the related resources, developers can create the blockchain node via BSN portal and connect the node to the BSN network [1].

It should be noted that the nature of the public blockchain may work against or not conform to local laws and regulations, in which case the public chain would cause some difficulties when it is implemented. For instance, Internal Revenue Service of United States requires taxpayers who hold cryptocurrencies to declare their cryptocurrency income [3]. However, there is no governing authority censoring the public blockchain due to the anonymity of its inherent characteristics, some transaction of cryptocurrency therefore cannot be identified [4]. Based on this point, BSN proposed Open Permissioned Blockchain (OPB), which combines the technical advantages of the public blockchain and the consortium blockchain. It can support distributed public ledger services in an untrusted environment and provide a compliant and good development setting for applications.

2.3. BSN portal

When developers purchase cloud resources and publish applications on the Internet, they can operate in any cloud service portal. Compared with the Internet, the service network also adopts the multi-portal strategy. Companies with corresponding resources such as cloud, framework and application developer resources can apply to establish BSN portal [1].

DOI: 10.54254/2755-2721/6/20230463

2.4. BSN Network Operations Platform

BSN Network Operations Platform can be regarded as the management system of BSN, the main functions of it include public city node management, application management, maintenance management, billing and settlement management, Certificate Authority (CA) management, etc. [1].

Due to the limited data there are about BSN network operation platform, this paper only focuses on the security analysis of public city node, blockchain framework and BSN portal.

3. Security issue of public city node

The study shows that the blockchain infrastructure is more subject than ever to vulnerabilities [5]. it is critical to analyse the security of PCN for its integral role as the infrastructure of BSN. In view of the functions of PCN, that is to provide computation, storage and bandwidth resources to support blockchain applications, the security issue is mainly in networking level.

3.1. BGP hijacking

Border gateway protocol (BGP) handles routing between multiple Autonomous System (AS). Attackers can leverage the BGP to intercept or manipulate blockchain's traffic by gaining control of the network from network operators. As network is an essential part of PCN, it will consequently inflict security hazard onto PCN. By analysing the node-level and network-wide attacks on routing, Apostolaki et al. stated that the impact of attack depends on the distribution of the computation power, if it is highly centralised, the range and seriousness of the impact will be significantly massive [6]. Also, it is also a time-consuming and complex task to recover from the BGP hijacking attack as the BGP configuration need to be reconfigured manually [7]. To prevent the BGP hijacking attack, monitoring system and prefixed filter need to be deployed for blockchain operator to inspect and intercept suspicious traffic because the security extension of BGP is not widely implemented and different networks adopt varying security solution. Additionally, the RPKI (Resource Public Key Infrastructure) is also a feasible solution, which can provide the trusted mapping for BGP to minimising the occurrence of the BGP Hijacking attack [6, 8].

3.2. Eclipse attack

Due to the decentralised trait of blockchain, not every node connects to each other. Instead, in order to improve efficiency, a given node will be connected to a group of selected nodes, so that the node is linked to the group to which the selected nodes belong. By leveraging this mechanism, eclipse attack is able to isolate the victim node from other groups in the network [9], attacker can make the target waste computing power through isolation or use the computing power of victim to conduct malicious damage. Although the eclipse attack takes advantages of this attribute of blockchain, it is essentially a network attack for the target is the node. In 2018, Yves-Christian et al. launched an eclipse attack in their experiment, the result demonstrated that the connection of the victim is monopolised, and denial of service is realised for the victim [10]. Besides, Heilman et al. believed that eclipse attack can become the basis of other secondary attacks, thus causing further damage [11]. However, not every secondary attack is likely to happened in BSN because BSN does not have the function of mining coins, which means attacks against mining may not work in BSN, thus, 0-confirmation double spend is the only one secondary attack may occur in BSN.

3.3. Other attacks

In addition to BGP hijacking and eclipse attack, other attacks exist, such as DDoS (Distributed Denial of Service) and sybil attack. DDoS implements massive number of visits at the same time, causing victim to be unable to carry out normal activities [12], while sybil attack aims to destroy the trust foundation of the blockchain network and control voting by creating multiple nodes [13, 14]. Despite these attacks setting the network as target, these attacks are not universal to different blockchains, thus, details of these attacks will be discussed in section 4.

DOI: 10.54254/2755-2721/6/20230463

4. Security issue of blockchain frameworks

Currently, the BSN adopts 3 different blockchain frameworks: public blockchain, consortium blockchain and open permissioned blockchain. Taking into account the specific characteristics and application scenarios, different kinds of frameworks use corresponding consensus algorithms to conduct their daily business, the attacker may exploit the shortcoming of the consensus algorithm to perform their attack. The analysis in this section revolves around these 3 kinds of frameworks.

4.1. Consortium blockchain framework

For consortium blockchain framework, BSN adopts Hyperledger Fabric, FISCO BCOS, ConsenSys Quorum and Hyperledger Besu as its consortium blockchain frameworks. The consensus algorithms of each framework are presented in table 1. Among those consensuses, PBFT (Practical Byzantine Fault Tolerance) and IBFT (Istanbul Byzantine Fault Tolerance) belong to BFT (Byzantine Fault Tolerance) [15]. By exploiting the principle of BFT, the sybil attack can be conducted, attackers can destroy the trust foundation and Redundancy Strategy of the blockchain network by creating multiple identity nodes and manipulating the voting of the blockchain [13, 14]. Moreover, regardless of the consensus algorithm, owing to the characteristic of consortium chain, the whole network knows the identity of node, which provides a gateway for DoS attack. In 2019, Andola et al. found that the endorser can be DoS-attacked under the Hyperledger Fabric framework because the identity of endorser is known to all member of the network [16].

Table 1. Frameworks and corresponding consensus algorithms.

Framework	Consensus	Reference
Hyperledger Fabric	Raft	[17]
FISCO BCOS	PBFT, Raft	[18]
ConsenSys Quorum	IBFT, QBFT	[19]
Hyperledger Besu	PoW, IBFT, QBFT, etc.	[20]

4.2. Public blockchain framework

For public blockchain framework, the general consensuses are PoW (Proof of Work) and PoS (Proof of Service) [15]. BSN adopts various kind of public chain frameworks and the consensus with the corresponding frameworks are shown in table 2, it is worth noting that some of frameworks may adopt the modified consensus. For instance, the Nervos framework uses a consensus based on PoW named NC-MAX, but in general, it belongs to PoW. In BSN, as it does not have mining function, attacks that exploit the weakness of PoW and PoS will not work, as a result, most of attack against public chain can be avoided. This does not mean the public chain framework is absolute safe especially for some frameworks using BFT consensus, where the sybil attack may occur.

Table 2. Consensus algorithms and corresponding frameworks.

Framework	Consensus	Reference
PoW based	Nervos	[21]
PoS based	ETH, Algorand, Oasis Network, Polkadot, Near, EOS, IRISNET	[22-28]
BFT based	Casper, Solana, Cypherium, Klaytn, Tenzos, Findora	[29-34]

4.3. Open permissioned blockchain

Open permissioned blockchain combines the advantages of public blockchain and consortium blockchain. The authority control of nodes is added to the public chain, meanwhile the mechanism of

DOI: 10.54254/2755-2721/6/20230463

paying GaS with virtual currency is cancelled, which creates the form similar to the consortium chain. Under this framework, the anonymity of blockchain can be reserved and the regulation can also be ensured. Currently, 5 kinds of open permissioned blockchains have been put into operation, and chains and consensuses on which they are based is shown in table 3, although the consensus algorithm of Tangshan and Guangyuan chain is unknown, for the chain using Tendermint, PBFT and dBFT, the risk of being attack nonetheless exists because those 3 consensus algorithms are based on BFT, and the weakness of BFT can be abused by sybil attack.

Table 3. Open permissioned blockchain with its basis and consensus.

Name	Based on	Consensus	Reference
Wenchang	IRITA	Tendermint	[28]
Tai'an	FISCO BCOS	PBFT	[18]
Wuhan	ETH	PoA	[22]
Tangshan	DBChain	Unknown	
Guangyuan	Everscale	Unknown	
Zhongyi	EOS	DPoS	[27]
Jiuquan	NEO	dBFT	[35]

5. Security issue of BSN portal

In BSN, the portal is responsible for the implementation of applications. When a new application comes out, for different business scenarios of the applications, the smart contracts also vary accordingly, which on the other hand induces risks for attacks. There is another dilemma between the need for data transaction supervision and sensitive information leak. So, it is critical to ensure the smart contract is correctly and securely implemented against attack [36].

5.1. Criminal smart contract

Criminals may leverage the smart contract to commit malicious deeds, the Criminal Smart Contract (CSC) can cause the leakage of sensitive information and real-world crimes. By utilising the CSC, criminals may produce the 0-day vulnerability data transactions [37]. Although it is possible to delete the CSC after being exposed, it will be very difficult to offset the damage caused by CSC because the malicious transaction can hardly be deleted. The approach of deleting CSC is to roll back the recorded data transaction, however, the new consensus needs to be called among members, by doing that, the credibility of the system may be impaired [38].

5.2. Vulnerability of smart contract

The key issue of blockchain application is smart contract's code level security [36]. For legal smart contract, some program defects may cause the security vulnerabilities. Atzei et al. investigated the vulnerabilities of smart contract and summarised them into 12 categories [36]. Since the BSN does not has the function of mining, the categories of possible vulnerabilities are reduced from 12 to 8, as shown in table 4. In fact, it is rare to find them in the real-world scenario because when smart contracts are applied to more complex situations, the complexity and technical difficulty of contract codes may also increase correspondingly.

DOI: 10.54254/2755-2721/6/20230463

Table 4. Smart contract vulnerabilities.

Level	Vulnerability	Caused by
Solidity	Call to the unknown	The function called does not exist
	Gasless send	Callee's fallback is executed
	Exception disorders	Exception handling is irregular
	Type casts	Type check error when executing contract
	Re-entrancy	Function re-enters before terminating
EVM	Immutable bugs	Change contract after deployment
	Stack size limit	The number of values in the stack exceeds 1024
Blockchain	Unpredictable state	Change the state of the contract before calling

6. Conclusion

In this paper, the security issues of BSN are analysed and determined, which mainly revolves PCN, blockchain frameworks and BSN portal, each further specifically with regards to networking, consensus algorithm and smart contract. From the analysis, the security issue on public city node cannot be mitigated because the attack is against underlying resources such as routing. For blockchain frameworks and BSN portal, owing to the function of mining is abandoned, attacks against virtual currency and mining are unlikely to be implemented.

Although security issues still exist, compared with traditional blockchain, there are fewer security issues. However, this analysis still has its shortcomings. The BSN network operation platform was not covered due to lack of useful information. Also, the blockchain framework was only analysed in the perspective of consensus algorithm. In the future, the research of BSN security issue can focus on BSN network operation platform to analyse the governance effectiveness of BSN. Likewise, assessing the blockchain framework from other perspective may draw different conclusion, it deserves the effort to explore.

References

[1] Red Date Technology Limited. (2020a). Blockchain-based Service Network (BSN) Introductory White Paper.

[2] Red Date Technology Limited. (2020b). Blockchain-based Service Network (BSN) Technical White Paper.

[3] Internal Revenue Service. (2014). *Notice 2014-21*.

[4] Treasury Inspector General for Tax Administration. (2016). As the Use of Virtual Currencies in Taxable Transactions Becomes More Common, Additional Actions Are Needed to Ensure Taxpayer Compliance.

[5] Goldfeder, S., Gennaro, R., Kalodner, H., Bonneau, J., Kroll, J., Felten, E., & Narayanan, A. (2015). *Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme*.

[6] Apostolaki, M., Zohar, A., & Vanbever, L. (2017, May). Hijacking bitcoin: Routing attacks on cryptocurrencies. In *2017 IEEE symposium on security and privacy (SP)* (pp. 375-392). IEEE.

[7] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems*, *107*, 841-853.

[8] Goldberg, S. (2014). Why is it taking so long to secure internet routing?. *Communications of the ACM*, *57*(10), 56-63.

[9] Singh, A. (2006). Eclipse attacks on overlay networks: Threats and defenses. In *IEEE INFOCOM*.

[10] Yves-Christian, A. E., Hammi, B., Serhrouchni, A., & Labiod, H. (2018, October). Total eclipse: How to completely isolate a bitcoin peer. In *2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)* (pp. 1-7). IEEE.

[11] Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse attacks on {Bitcoin's} {peer-

DOI: 10.54254/2755-2721/6/20230463

to-peer} network. In *24th USENIX Security Symposium (USENIX Security 15)* (pp. 129-144).

[12] Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer networks*, *44*(5), 643-666.

[13] Dinger, J., & Hartenstein, H. (2006, April). Defending the sybil attack in p2p networks: Taxonomy, challenges, and a proposal for self-registration. In *First International Conference on Availability, Reliability and Security (ARES'06)* (pp. 8-pp). IEEE.

[14] Swathi, P., Modi, C., & Patel, D. (2019, July). Preventing sybil attack in blockchain using distributed behavior monitoring of miners. In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE.

[15] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). IEEE

[16] Andola, N., Gogoi, M., Venkatesan, S., & Verma, S. (2019). Vulnerabilities on hyperledger fabric. *Pervasive and Mobile Computing*, *59*, 101050.

[17] *Hyperledger Architecture, Volume 1*. (2017). https://www.hyperledger.org/wp-content/uploads/2017/08/HyperLedger_Arch_WG_Paper_1_Consensus.pdf

[18] *Consensus algorithm — FISCO BCOS EN v2.9.0 documentation*. (n.d.). Fisco-Bcos-Documentation.readthedocs.io. Retrieved June 18, 2022, from https://fisco-bcos-documentation.readthedocs.io/en/latest/docs/design/consensus/index.html

[19] *Consensus protocols - GoQuorum*. (n.d.). Consensys.net. Retrieved June 18, 2022, from https://consensys.net/docs/goquorum/en/stable/concepts/consensus/

[20] *Consensus protocols - Hyperledger Besu*. (n.d.). Besu.hyperledger.org. Retrieved June 18, 2022, from https://besu.hyperledger.org/en/stable/private-networks/how-to/configure/consensus/

[21] *Consensus | Nervos CKB*. (n.d.). Docs.nervos.org. Retrieved September 18, 2022, from https://docs.nervos.org/docs/basics/concepts/consensus/

[22] *Consensus mechanisms*. (n.d.). Ethereum.org. Retrieved March 27, 2022, from https://ethereum.org/en/developers/docs/consensus-mechanisms/

[23] *Pure Proof-of-Stake*. (n.d.). Www.algorand.com. Retrieved November 16, 2021, from https://www.algorand.com/technology/pure-proof-of-stake

[24] *Consensus Layer | Oasis Network Documentation*. (n.d.). Docs.oasis.io. Retrieved June 18, 2022, from https://docs.oasis.io/core/consensus/

[25] *Polkadot Consensus · Polkadot Wiki*. (n.d.). Wiki.polkadot.network. Retrieved June 18, 2022, from https://wiki.polkadot.network/docs/learn-consensus

[26] *Consensus | NEAR Protocol Specification*. (n.d.). Nomicon.io. Retrieved June 18, 2022, from https://nomicon.io/ChainSpec/Consensus

[27] *Consensus Protocol*. (n.d.). Developers.eos.io. Retrieved June 18, 2022, from https://developers.eos.io/welcome/v2.0/protocol-guides/consensus_protocol

[28] *General Concepts | IRISnet Documents*. (n.d.). Www.irisnet.org. Retrieved June 18, 2022, from https://www.irisnet.org/docs/concepts/general-concepts.html

[29] *The Casper Network Highway Consensus Protocol*. (2021, January 12). CasperLabs Blog. https://blog.casperlabs.io/the-casper-network-highway-consensus-protocol/

[30] Yakovenko, A. (n.d.). Solana: A new architecture for a high performance blockchain v0.8.13. https://solana.com/solana-whitepaper.pdf

[31] Cypherium. (2020, May 8). *Cypherium | Hotstuff Consensus Algorithm*. Medium. https://cypherium.medium.com/what-is-hotstuff-and-why-is-it-a-big-deal-213f39696763

[32] *Consensus Mechanism - Klaytn Docs*. (2022). Klaytn.foundation. https://docs.klaytn.foundation/klaytn/design/consensus-mechanism

[33] *The Tezos Consensus Algorithm - Tezos Agora Wiki*. (2016). Tezosagora.org. https://wiki.tezosagora.org/learn/baking/proofofstake/consensus

[34] *Consensus | Findora Wiki*. (n.d.). Wiki.findora.org. Retrieved June 18, 2022, from

DOI: 10.54254/2755-2721/6/20230463

https://wiki.findora.org/docs/components/Staking/Consensus/

[35] neo-project. (n.d.). *Neo Documentation*. Docs.neo.org. Retrieved June 18, 2022, from https://docs.neo.org/docs/en-us/basic/consensus/dbft.html

[36] Atzei, N., Bartoletti, M., & Cimoli, T. (2017, April). A survey of attacks on ethereum smart contracts (sok). In *International conference on principles of security and trust* (pp. 164-186). Springer, Berlin, Heidelberg.

[37] Juels, A., Kosba, A., & Shi, E. (2016, October). The ring of gyges: Investigating the future of criminal smart contracts. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 283-295).

[38] Mavridou, A., & Laszka, A. (2018, February). Designing secure ethereum smart contracts: A finite state machine based approach. In *International Conference on Financial Cryptography and Data Security* (pp. 523-540). Springer, Berlin, Heidelberg.