2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom)

2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom) | 978-1-6654-8066-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/CSCloud-EdgeCom54986.2022.00014

Current Status and Prospects of Blockchain Security Standardization

Xiaofeng Chen
Hangzhou Qulian Technology Co., Ltd.
Blockchain Research Center,
Zhejiang University
Hangzhou, China
12021185@zju.edu.cn

Zunbo Wei
Hangzhou Qulian Technology Co., Ltd.
Hangzhou, China

Xiangjuan Jia
Hangzhou Qulian Technology Co., Ltd.
Hangzhou, China

Peiyu Zheng
Hangzhou Qulian Technology Co., Ltd.
Hangzhou, China

Mengwei Han
Hangzhou Qulian Technology Co., Ltd.
Hangzhou, China

Xiaohu Yang
Blockchain Research Center,
Zhejiang University
Hangzhou, China
yangxh@zju.edu.cn

***Abstract*—In recent years, blockchain technology has become one of the key technical innovation fields in the world. From the simple Bitcoin that can only be transferred at first to the blockchain application ecology that is now blooming, blockchain is gradually building a credible internet of value. However, with the continuous development and application of blockchain, even the blockchain based on cryptography is facing a series of network security problems and has caused great property losses to participants. Therefore, studying blockchain security and accelerating standardization of blockchain security have become the top priority to ensure the orderly and healthy development of blockchain technology. This paper briefly introduces the scope of blockchain security from the perspective of network security, sorts out some existing standards related to blockchain security, and gives some suggestions to promote the development and application of blockchain security standardization.**

Keywords—blockchain security, attack event, development status, blockchain standard, security standard

I. Introduction

Blockchain is considered as a distributed ledger maintained by participants. The ledger adopts cryptography technology to ensure the security of transmission and access, and can achieve the purposes of data consistency, non-tampering and traceability. With the continuous attempts and applications of blockchain technology in all walks of life, blockchain security issues have gradually surfaced [1 ~ 3].

Currently, blockchain has many limitations in key management, consensus mechanism, smart contract and other technologies, which leads to the endless network attacks on blockchain platforms and blockchain-based applications [4].

On Feb. 7th, 2014, MtGox issued a statement saying that its security software was flawed, and immediately announced the suspension of all transactions including BTC and ETH. Two weeks later, the official website of MtGox suddenly disappeared and then filed for bankruptcy. The security incident caused huge losses to MtGox, and the lost 850,000 bitcoins were worth 470 million dollars at that time [5].

On June 17th, 2016, hackers attacked The Dao project, stealing more than 3 million ETH, which caused Ethereum to be forced to make a hard fork. In addition, because the values of community members failed to reach a consensus, after the original Ethereum forked, two chains were formed. One was the original chain recognized by a few community members (Ethereum Classic, ETC), and the other was the new chain recognized by most community members including Vitalik Buterin, founder of Ethereum [6].

On Aug. 10th, 2021, the cross-chain protocol Poly Network issued a statement saying that it was attacked by hackers, which led to heavy losses of O3 Swap using this protocol. All the digital assets on the three networks of Ethereum, Binance Smart Chain and Polygon were stolen by hackers, and none of them survived. According to the transfer records on the blockchain browser, the hackers transferred 302 million USDT, 55,000 ETH, 2,000 BTC and other assets in just about half an hour, with a total value of 610 million dollars. The scale of theft of this magnitude is the highest in history [7].

When conducting data security supervision, the characteristics of decentralization and anonymity of blockchain are very unfriendly, which brings great pressure to regulators. Successive blockchain security incidents have sounded the alarm for people and attracted the attention of practitioners in various fields, such as government, industry, university, and scientific research institution. Major countries and regions around the world have begun to pay attention to and study blockchain security.

As early as 2016, while actively promoting the cooperation and common development of all sectors of society, Britain also proposed that attention should be paid to the development of standards related to blockchain and DLT (distributed ledger technology), and proposed a new mode of blockchain supervision, that is, relying on technology as the main supervision mode instead of legal supervision [8].

The United States maintains a vigilant and friendly attitude towards blockchain, and pays great attention to the application of blockchain in the field of network security, and actively encourages the research on blockchain security. In 2017, then US President Trump signed a $700 billion defense policy bill, which included a study on blockchain security. At the same

This work was supported by the National Key R&D Program of China (Grant No. 2020YFB1005400).

978-1-6654-8066-6/22/$31.00 ©2022 IEEE
DOI 10.1109/CSCloud-EdgeCom54986.2022.00014

time, Trump also advocated the investigation of potential blockchain and DLT attacks and defensive countermeasures, and supported the United States *Department of Homeland Security* (DHS) to develop tools for tracking, forensics and analysis of cryptocurrency [9]. Linux Foundation, Accenture, Microsoft and other companies have launched their own products and solutions in blockchain hardware security module and blockchain cloud environment security.

China has successively promulgated 3 Laws [10], as shown in TABLE I. These laws put forward higher requirements for the security supervision of the blockchain industry.

TABLE I. REGULATORY LAWS OF CHINA

	Name of Law
1	Cybersecurity Law of the People’s Republic of China
2	Data Security Law of the People’s Republic of China
3	Personal Information Protection Law of the People’s Republic of China

Although the blockchain has produced many technical branches and applied to more and more scenes, the development degree of each branch is not balanced enough because the blockchain has only been born for 10+ years [11], and the same technology may have different understandings in different countries or regions. In addition, there are differences in blockchain system architecture and evaluation standards, which are not uniform. These have hindered the development, application and industrialization of blockchain security technology.

Therefore, accelerating the development of blockchain security standardization has become the consensus of many practitioners in the industry.

Our contributions in this paper are as follow:

1) First, we analysis the security of blockchain system on six levels: network, password, data, consensus mechanism, smart contract and appplication ecological.

2) Then, we summary the current standardization status of blockchain security in China and International.

3) Finally, the prospects of blockchain security standardizaiton are proprosed.

II. BLOCKCHAIN SECURITY

With the continuous development of blockchain technologies and the continuous improvement of blockchain ecology, in addition to traditional network security issues, many unique cyber-attack means and methods of blockchain have emerged in the blockchain field.

The overall architecture of blockchain roughly includes core layer, network layer, consensus layer, incentive layer, smart contract layer and application layer. It is precisely because blockchain has unique and innovative design architecture, technology and application that blockchain security can become an indispensable branch in the field of network security [12].

According to the general views of relevant practitioners in the field of blockchain security and the comprehensive analysis of security incidents in the field of blockchain, blockchain security generally includes network security, password security, data security, consensus mechanism security, smart contract security, application ecological security and so on.

A. Network security

Security on Network layer [13] is an extremely important part in the blockchain security field and even in the computer field. With the continuous development of blockchain technology based on P2P networks, the security control of network layer becomes more and more important. Network security in the blockchain field mainly includes witch attacks, eclipse attacks and *Distributed Denial of Service* (DDoS) attacks in the design layer. Traditional DDoS attacks are generally divided into two steps: the first step, using Trojan horse, buffer overflow [14], virus, Phishing and other attack means [15] to inbreak and control a large number of hosts, making them become botnets; Secondly, the attacker conducts a DDoS attack on the target through the controlled botnet.

B. Password security

Cryptographic mechanisms [16-18] such as asymmetric encryption and hash algorithm have solved the problems of message tamper-proof and privacy information protection, and are the foundation on which blockchain can be created and gradually developed and apply. However, these cryptographic mechanisms are not perfect, and there is still the risk of being attacked or even cracked. The related attacks of password security mainly include the following 3 aspects:

1) It threatens the user's digital assets by stealing the private key.

2) There may be security risks in complex encryption algorithms such as ECC and RSA as well as in the specific implementation process, thus endangering the security of the whole blockchain system and various applications carried on it.

3) It may be attacked by quantum computing. With the advent of quantum products such as quantum computers, quantum chips and quantum computing service systems, it has become a reality to crack the factorization of large numbers in asymmetric cryptographic algorithms in seconds.

C. Data security

It is one of the main features of blockchain that data is difficult to tamper with, but this feature also brings risks in data privacy [19-21] when it brings benefits. For example, harmful information can't be deleted after it is uploaded, which causes some bad effects, and the privacy leakage of sensitive data [22-24] after it is uploaded, etc. M. Qiu and his group had proposed novel secure data sharing approaches with blockchain-enhanced key management in untrusted clouds [25,26].

D. Consensus mechanism security

Consensus mechanism is the basis for the orderly operation of blockchain system. Blockchain nodes that have not established trust relationship can jointly verify the correctness of information written in new blocks through consensus mechanism. Blockchain has produced many consensus mechanisms so far, and the mainstream consensus mechanisms include *Proof of Work* (PoW), *Proof of Stake* (PoS), *Delegated Proof of Stake* (DPoS), *Byzantine Fault Tolerance* (BFT) and so on.

At present, the PoW, PoS and DPoS mechanisms have been tested in practice for a long time, and are relatively mature. However, in the long-term development and application of the blockchain consensus mechanism, there have also appeared many attack methods specifically aimed at the consensus mechanism, mainly including double flower attack, 51% computing power attack, selfish mining, replay attack and so on.

E. Smart contract security

Smart contract is automatically executed according to established rules, and its operation object is usually valuable digital assets. However, the artificially written code is not perfect after all, and it can even be said that there must be some light or heavy security problems. From previous security incidents, many blockchain security incidents are caused by smart contracts. The vulnerabilities of smart contract mainly include conditional competition, re-entrancy attack, logic design defects and so on. Besides the risks of the smart contract itself, the risks of virtual machines running smart contracts can’t be ignored. Because a large number of nodes in a blockchain system often use the same or similar virtual machines, a single virtual machine vulnerability is likely to endanger the whole system.

F. Application ecological security

Blockchain application ecology refers to various applications related to blockchain technologies, such as blockchain platforms, digital wallets, digital currency exchanges, *Decentralized Applications* (DApps), etc. These applications not only need to face the same security risks, but also need to face "tailor-made" vulnerability attacks. Moreover, with the continuous expansion of the ecological scope of blockchain, the security risks of blockchain application ecology are also increasing.

III. Blockchain Security Standardization

A. Current status of blockchain security standardization in China

Since 2016, China has gradually started the development of blockchain and DLT group standards, local standards, industry standards and national standards. Although there is no published national standard related to blockchain and DLT, there are a number of national standards under development are being accelerated. In addition, a number of industry standards, local standards and group standards related to blockchain and DLT have been published.

TABLE II. NATIONAL STANDARDS OF BLOCKCHAIN SECURITY IN CHINA

	Name of National Standard
1	Information security technology — Security specification for information service of blockchain
2	Information security technology — Security framework for blockchain technology

In view of the frequent chaos of blockchain security issues, domestic enterprises and institutions have begun to pay attention to blockchain security issues, and reached a consensus on speeding up the development of national standards related to blockchain security [27-29]. At present, there are two national standards related to blockchain and DLT security under development in SAC/TC260, shown in TABLE II, *Information security technology — Security specification for information service of blockchain* led by Institute of Information Engineering, Chinese Academy of Sciences and *Information security technology — Security framework for blockchain technology* led by Tsinghua University. These two standards have both entered the stage of soliciting comments.

Because finance is naturally suitable for blockchain, the earliest blockchain-based applications are appeared in financial industry in China, which makes the financial-related blockchain and DLT standard planning earlier and progressing faster [30]. In 2020, two industry standards led by the People's Bank of China, shown in TABLE III, were published and implemented one after another, thus achieving a breakthrough of zero industry standards in the blockchain security field and even the whole blockchain field.

TABLE III. INDUSTRY STANDARDS OF BLOCKCHAIN SECURITY IN CHINA

No.	Name of Industry Standard
JR/T 0184-2020	Financial distributed ledger technology security specification
JR/T 0193-2020	Financial application of blockchain technology – Evaluation rules

Since 2020, local standards have gradually increased in blockchain standardization. Among them, Hunan Province issued the first batch of local standards for blockchain security technology, which was officially implemented on Jan. 27th, 2021. There are 6 local standards in this batch, shown in TABLE IV, which are focus on evaluation requirements on the aspects of network, encryption, data, contract, consensus and application.

TABLE IV. LOCAL STANDARDS OF BLOCKCHAIN SECURITY IN CHINA

	Name of Local Standard
1	Information security technology — Evaluation requirements for blockchain network security technology
2	Information security technology — Evaluation requirements for blockchain encryption security technology
3	Information security technology — Evaluation requirements for blockchain data security technology
4	Information security technology — Evaluation requirements for blockchain contract security technology
5	Information security technology — Evaluation requirements for blockchain consensus security technology
6	Information security technology — Evaluation requirements for blockchain application security technology

TABLE V. GROUP STANDARDS OF BLOCKCHAIN SECURITY IN CHINA

	Name of Group Standard
1	Blockchain CA service interface specification and security requirements
2	Blockchain cryptography service interface specification and security requirements
3	Cryptographic test specification for blockchain

The number and scope of group standards are ahead of national standards, industry standards and local standards. Guangdong province, Zhejiang province, Shanghai and other regions, due to the strong support of the government, talent gathering and being good at innovation, have made the blockchain industry in these regions more mature, and the lead units of group standards are mostly distributed here [31]. The published blockchain standards match the application scenarios of industry and are more targeted, shown in TABLE V.

In addition, a number of group standards have been published in the field of privacy computing, which contributes to the security of blockchain, shown in TABLE IV, mainly focus on technical requirements, performance requirements testing methods of TEE(Trusted Executive Environment), Privacy-preserving Computation, Federated Learning and Secure Multi-party Computing.

TABLE VI. GROUP STANDARDS OF PRIVACY COMPUTING IN CHINA

	Name of Group Standard
1	Data computational platform based on trusted executive environment: Technical requirements and testing methods
2	Privacy-preserving Computation products assisted by Blockchain: Technical requirements and testing methods
3	Data circulation products based on federated learning: Technical requirements and testing methods
4	Performance requirements and testing methods of privacy-preserving computing — secure multi-party computing products
5	Performance requirements and testing methods of privacy-preserving computing — federated learning products
6	Privacy-preserving Computation Cross-platform Interconnection — Part 1: Framework

B. *Current status of international blockchain security standardization*

From the perspective of international standards of blockchain, influential organizations around the world such as *International Telecommunication Union* (ITU), *International Organization for Standardization* (ISO), *Institute of Electrical and Electronics Engineers* (IEEE) have successively set up blockchain standard working groups or committees to promote the development of international standards for blockchain technologies and promote the healthy development of blockchain industry.

TABLE VII. INTERNATIONAL STANDARDS OF BLOCKCHAIN SECURITY IN ITU-T

No.	**Name of ITU-T Standard**
X.1401	Security threats of distributed ledger technology
X.1402	Security framework for distributed ledger technology
X.1403	Security guidelines for using distributed ledger technology for decentralized identity management
X.1404	Security assurance for distributed ledger technology
X.1405	Security threats and requirements for digital payment services based on distributed ledger technology
X.1406	Security threats to online voting systems using distributed ledger technology
X.1407	Security requirements for digital integrity proofing service based on distributed ledger technology
X.1408	Security threats and requirements for data access and sharing based on the distributed ledger technology

ITU is an important specialized agency of the United Nations and the oldest international organization among the United Nations organizations. ITU has several departments, such as ITU-R and ITU-T. According to the information published on the official website of ITU [32], as of May 2022, ITU-T has published 19 standards related to blockchain and DLT, such as security technology, Internet of Things technology, data management and so on. Among them, there are 8 security-related standards, shown in TABLE VII.

ISO is an international non-governmental organization in the field of standardization. It is composed of national standardization organizations in more than 100 countries around the world. The General Assembly is the highest authority of ISO, the Council is an important decision-making body of ISO, and China is a permanent member state of ISO.

According to the information published on the official website of the ISO (https://www.iso.org/), as of May 2022, ISO has published 7 international standards and technical reports related to blockchain, which is less than the number of standards published by ITU [33]. The published standards and technical reports include blockchain terminology concept, system overview, privacy protection and personnel safety management. The specific standard names are shown in TABLE VIII, in which privacy protection and personnel safety management are closely related to blockchain security.

TABLE VIII. INTERNATIONAL STANDARDS OF BLOCKCHAIN SECURITY IN ISO

No.	**Name of ISO Standard/Technical Report**
23244:2020	Blockchain and distributed ledger technologies – Privacy and personally identifiable information protection considerations
23576:2020	Blockchain and distributed ledger technologies – Security management of digital asset custodians

IEEE is an international association of electronic technology and information science engineers, the largest non-profit professional technology society in the world and the most authoritative international academic organization in the field of electronic information. Its IEEE Standards Association is the world's leading standard-setting organization.

In the field of blockchain, IEEE has successively established specialized agencies responsible for the establishment, review and approval of standards related to blockchain/distributed ledger, including C/BDL - Blockchain and Distributed Ledger Standards Committee, CTS/BSC - Blockchain Standards Committee and so on. China Electronic Standardization Institute is the chairman of IEEE C/BDL. According to the information published by the IEEE standard website(https://standards.ieee.org/), as of May 2022, IEEE has issued the relevant standards for blockchain and DLT including data management [34], data format [35], electronic contracts [36], evidence collecting [37], cryptocurrency [38] and other subdivision directions. It is not difficult to see that IEEE attaches great importance to blockchain technology, and its standard range is broader. Although the security part of blockchain and DLT has not been covered in IEEE published standards, it has gradually included the security part of blockchain in the research standards.

We can see that there are some differences in the standards mentioned above. First, domestic standards like to use the word blockchain, while international standards use distributed ledger technology more. In addition, some standards focus on the security of blockchain and DLT itself, while others focus on the security of other areas that integrate blockchain and DLT.

IV. PROSPECTS OF BLOCKCHAIN SECURITY STANDARDIZATION

A. *Integration with privacy computing and intelligent data*

The integration of blockchain technology and privacy computing is a major trend today. We can see that data in the blockchain needs to be protected by privacy algorithm, while privacy computing can use blockchain technology to record and trace data sets, algorithm models and calculation processes in multi-party collaboration, and evaluate and agree on the final results to continuously optimize collaboration efficiency. Therefore, the future blockchain security will be inseparable from the assistance of privacy computing, intelligent data [39-41]. And even blockchain security standards including privacy computing will be gradually drafted and published.

B. *Strengthen the development of group standards and industry standards*

Group standards, local standards and industry standards of blockchain will have a lot of ideological collisions when they are formulated, and only through such ideological collisions can we form a result that everyone agrees with, which also lays the foundation for the development of national standards. The influence and application scope of national standards are larger and wider, so it is an essential step to learn from the experience and lessons in the development of group standards and industry standards. Therefore, when developing blockchain standards with the aid from artificial intelligence [42-44], the nations of the world shall make careful arrangements based on the use and acceptance of these standards.

C. *Encourage innovation and exploration*

On this basis, the nations of the world still need to continue to deeply participate in international standards related to blockchain and lay out the future international standard system of blockchain in advance. At the same time, it is also necessary to increase the support of leading enterprises in terms of policies and funds, carry out blockchain security development competitions, offensive and defensive competitions, testing and evaluation activities, encourage technological innovation and exploration of blockchain enterprises, and actively land a number of marketable and valuable blockchain applications, such as brain-based computer interface [45-46], to enhance the influence in the industry

D. *Education and Experts*

Although the application scope of blockchain is expanding rapidly from finance to supply chain, social welfare, culture and entertainment and other industries and fields. However, on the whole, the applications of blockchain is still in the early stage of unbalanced development, and there is still a long way to go before the applications of various industries and scenarios is mature. Therefore, in the process of standard development, the nations of the world shall carefully identify industry risks, effectively avoid application cases that may cause misunderstandings, and develop perfect, highly applicable and universal blockchain security-related standards.

Secondly, the domestic and international blockchain security standardization work has just started, so the nations of the world shall strengthen the training of talents in the blockchain security field, especially in the international standardization work.

If the nations of the world want to participate in the international standardization work substantially, they must cultivate compound professionals who understand security technology, understand the international standardization work flow and pass the language test. Therefore, enterprises and research institutes related to blockchain industry shall pay attention to the cultivation of blockchain security talents.

V. CONCLUSION

This paper analyzed six security aspects on blockchain systems, combined with the standardization status on blockchain security in China and International. The paper also proposed four ways to enhance the standardization of blockchain security.

REFERENCES

[1] H. Qiu, M. Qiu, et al., A dynamic scalable blockchain based communication architecture for IoT, International Conference on Smart Blockchain, 159-166,2018

[2] K. Gai et al., Differential privacy-based blockchain for industrial Internet-of-Things, IEEE TII, pp. 4156-4165, 16(6), 2019

[3] Z. Tian, M. Li, et al. Block-def: A secure digital evidence framework using blockchain, Information Sciences 491 (2019) 151-165.

[4] China Blockchain Technology and Application Development White Paper, [online] Available: http://www.shujuju.cn/lecture/detail/2134.

[5] The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster, [online] Available: https://www.wired.com/2014/03/bitcoin-exchange/.

[6] A History of 'The DAO' Hack, [online] Available: https://coinmarketcap.com/alexandria/article/a-history-of-the-dao-hack.

[7] Cross-Chain DeFi Site Poly Network Hacked, [online] Available: https://www.coindesk.com/markets/2021/08/10/cross-chain-defi-site-poly-network-hacked-hundreds-of-millions-potentially-lost/.

[8] Distributed Ledger Technology: beyond block chain, [online] Available: https://assets.publishing.service.gov.uk/government/uploa-ds/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

[9] $700 Billion Senate Defense Bill Calls for Blockchain Cybersecurity Study, [online] Available: https://www.coindesk.com/markets/2017/09/19/700-billion-senate-defense-bill-calls-for-blockchain-cybersecu-rity-study/.

[10] PRC: personal data protection, [online] Available: https://www.lex-ology.com/library/detail.aspx?g=3634f282-2f0e-4209-b5e0-5b6d88678fa6.

[11] 2018 China Blockchain Industry White Paper, [online] Available: http://www.chinatft.org/static/temimg/948298.pdf.

[12] Analysis Report on the Security Vulnerability of Open Source Software Source Code - Blockchain Topic, [online] Available: https://www.ccvalue.cn/article/27279.html.

[13] M. Qiu, J Deng, E. Sha, "Failure rate minimization with multiple function unit scheduling for heterogeneous WANs," IEEE GLOBECOM, 1-5, 2008

[14] Z. Shao, C. Xue, Q. Zhuge, et al., "Security protection and checking for embedded system integration against buffer overflow attacks via hardware/software", IEEE Transactions on Computers 55 (4), 443-453, 2006

[15] M. Qiu, L. Zhang, Z. Ming, et al., "Security-aware optimization for ubiquitous computing systems with SEAT graph approach", J. of Comp. and Sys. Sci., 79(5), 518-529, 2013

[16] H. Qiu, M. Qiu, R. Lu, "Secure V2X communication network based on intelligent PKI and edge computing," IEEE Network 34 (2), 172-178, 2019

[17] H. Qiu, M. Qiu, M. Liu, Z. Ming, "Lightweight selective encryption for social data protection based on EBCOT coding," IEEE Trans. on Compu. Social Systems 7 (1), 205-214, 2019

[18] H. Qiu, M. Qiu, Z. Lu, "Selective encryption on ECG data in body sensor network based on supervised machine learning," Information Fusion 55, 59-67, 2020

[19] M. Qiu, K. Gai, H. Zhao, M. Liu, "Privacy-preserving smart data storage for financial industry in cloud computing," Concurrency and Computation: Practice and Experience 30 (5), e4278, 2018

[20] M. Qiu, K. Gai, Z. Xiong, "Privacy-preserving wireless communications using bipartite matching in social big data", FGCS, 87, 772-781,2018

[21] K. Gai, M. Qiu, H. Zhao, "Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing," IEEE Trans. Big Data 7(4): 678-688, 2021

[22] H. Qiu, K. Kapusta, Z. Lu, M. Qiu, G. Memmi, "All-Or-Nothing data protection for ubiquitous communication: Challenges and perspectives," Information Sciences, 502, 434-445,2019

[23] H. Qiu, H. Noura, M. Qiu, Z. Ming, G. Memmi, "A User-Centric Data Protection Method for Cloud Storage Based on Invertible DWT," IEEE Trans. Cloud Comput. 9(4): 1293-1304, 2021

[24] K. Gai, M. Qiu, S. Elnagdy, "A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance," IEEE BigDataSecurity 2016

[25] M. Qiu, H. Qiu, H. Zhao, M. Liu, B. Thuraisingham, "Secure Data Sharing Through Untrusted Clouds with Blockchain-enhanced Key Management," Conf. SmartBlock, 11-16, 2020

[26] H. Qiu, M. Qiu, M. Liu, G. Memmi, "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0", IEEE journal of biomedical and health informatics 24 (9), 2499-2505, 2020

[27] Blockchain White Paper (2018), [online] Available: http://www.caict.ac.cn/english/research/whitepapers/202003/P020200327550628685790.pdf.

[28] Interpretation of blockchain technology security framework, [online] Available: https://netfreeman.com/2021/08/20210818040258753F.html.

[29] China has put forward 30 standards related to blockchain, [online] Available: http://www.zqrb.cn/jrjg/hlwjr/20200612/A159195460922 5 .html.

[30] W. Pan, M. Qiu, Application of blockchain in asset-backed securitization, IEEE 6th Conf. BigDataSecurity, 2020

[31] Blockchain Security White Paper—Technology Application Edition(2018), [online] Available: http://www.huanjing100.com/p-10095.html.

[32] ITU-T Recommendations, [online] Available: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14092&lang=en.

[33] ISO/TC 307 Blockchain and distributed ledger technologies, [online] Available: https://www.iso.org/committee/6266604.html.

[34] "IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management," in IEEE Std 2144.1-2020 , vol., no., pp.1-20, 18 Jan. 2021, doi: 10.1109/IEEESTD.2021.9329260.

[35] "IEEE Standard for Data Format for Blockchain Systems," in IEEE Std 2418.2-2020 , vol., no., pp.1-32, 23 Dec. 2020, doi: 10.1109/IEEESTD.2020.9303503.

[36] "IEEE Standard for Blockchain-based Electronic Contracts," in IEEE Std 3801-2022 , vol., no., pp.1-26, 1 April 2022, doi: 10.1109/IEEESTD.2022.9745868.

[37] "IEEE Standard for Application Technical Specification of Blockchain-based E-Commerce Transaction Evidence Collecting," in IEEE Std 3802-2022 , vol., no., pp.1-24, 1 April 2022, doi: 10.1109/IEEESTD.2022.9745865.

[38] "IEEE Standard for General Requirements for Cryptocurrency Exchanges," in IEEE Std 2140.1-2020 , vol., no., pp.1-18, 4 Nov. 2020, doi: 10.1109/IEEESTD.2020.9248667.

[39] Y. Li, Y. Song, L. Jia, et al., "Intelligent fault diagnosis by fusing domain adversarial training and maximum mean discrepancy via ensemble learning", IEEE Trans. on Industrial Informatics 17 (4), 2833-2841, 2020

[40] H. Qiu, Q. Zheng, G. Memmi, J. Lu, M. Qiu, B. Thuraisingham, "Deep residual learning-based enhanced JPEG compression in the Internet of Things," IEEE Trans. on Industrial Informatics, 17 (3), 2124-2133, 2020

[41] H. Qiu, T. Dong, T. Zhang, J. Lu, G. Memmi, M. Qiu, "Adversarial attacks against network intrusion detection in IoT systems," IEEE Internet of Things Journal 8(13), 10327-10335, 2020

[42] C. Li, M. Qiu, "Reinforcement Learning for Cyber-Physical Systems: with Cybersecurity Case Studies," Chapman and Hall/CRC, 2019

[43] H. Qiu, Y. Zeng, S. Guo, T. Zhang, M. Qiu, B. Thuraisingham, "Deepsweep: An evaluation framework for mitigating DNN backdoor attacks using data augmentation," ACM Asia Conf. on Comp. and Comm. 2021

[44] Y. Zeng, H. Qiu, G. Memmi, M. Qiu, "A Data Augmentation-Based Defense Method Against Adversarial Attacks in Neural Networks, " Conf. ICA3PP (2), 274-289, 2020

[45] M. Qiu, S.Y. Kung, K Gai, "Intelligent security and optimization in Edge/Fog Computing," Future generation computer systems 107, 1140-1142, 2020

[46] S. Li, M. Qiu, "Authentication Study for Brain-Based Computer Interfaces Using Music Stimulations," Conf. ICA3PP, 663-675, 2020