International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 02 | Feb 2019 www.irjet.net p-ISSN: 2395-0072

A SURVEY ON IOT REFERENCE ARCHITECTURE WITH BLOCK CHAIN FOR AUTOMATIC SUPPLY CHAIN MANAGEMENT

Nikhil[1], Aditya Sinha[2], Bhupendra Pratap Singh[3], S. Karthikeyan[4]

[1]PG Student, Dept. of ECE, Sathyabama Institute of Science and Technology, Chennai, India
[2]Joint Director, CDAC ACTS, Pune, India
[3]Project Engineer, CDAC ACTS, Pune, India
[4]Assistant Professor of SIST, Chennai, India

ABSTRACT: *Internet of Things implies that physical articles will have the capacity to collaborate and impart by means of installed frameworks. This will prompt a dispersed system of gadgets that can speak with the two people and one another. One application zone is in enhancing supply chain management. Usage of IoT will have numerous advantages yet it likewise raises security issues that can influence respectability, security and protection for the two people and organizations. Blockchain is a record of realities, information isn't put away in just a single system with a typical processor, yet it is conveyed among every one of the customers on the system. blockchain can be utilized to anchor information administration inside some random supply chain that utilizes IoT innovation, yet blockchain ought to be viewed as an apparatus, and not as an entire arrangement. A considerable lot of the security issues inside IoT are identified with the gadgets and blockchain won't have the capacity to give an answer for these issues. Blockchain can anyway be utilized for taking care of data, anchoring personalities, traceability of products, exchanges being made without human communication, computerized capacity administration and time stepped activities to name a few models. There are still boundaries to make these advantages work in all actuality however there is a considerable measure of research as of now on-going, attempting to get it going. This paper investigates breakthrough research of blockchain and IoT with the reason to examine blockchain as a potential answer for secure IoT information administration inside supply chains. Both blockchain and IoT are generally new research zones with small existing examination, which bolster our utilization of a subjective inductive technique. In this paper, we depict the open doors for uses of blockchain for the IoT and inspect the difficulties engaged with architecting Blockchain-based IoT applications, at that point this innovation might be an answer for a few issues that IoT are confronting.*

Keywords: *Blockchain, Internet of Things, supply chain, device, smart contract, private/public blockchain.*

I. INTRODCUTION

The Internet of Things (IoT) speaks to a standout amongst the most noteworthy troublesome innovations of this century. Over the most recent couple of years, we have seen the capability of Internet of Things to convey energizing administrations over a few divisions, from online life, business, shrewd transportation and savvy urban communities to the ventures [1], [2], [3]. Satoshi Nakamoto established the framework for the Blockchain innovation in 2008 by showing an answer for decentralized trust among obscure elements [1]. IoT consistently interconnects heterogeneous gadgets with assorted functionalities in the human-driven and machine-driven systems to meet the advancing necessities of the prior specified parts. In any case, the noteworthy number of associated gadgets and gigantic information activity turn into the bottleneck in meeting the required Quality-of-Services (QoS) due to the computational, stockpiling, and data transfer capacity compelled IoT gadgets. It is a characteristic advancement of the Internet (of PCs) to implanted and digital physical frameworks, "things" that, while not clearly PCs themselves, by the by have PCs inside them. With a system of modest sensors and interconnected things, data accumulation on our reality and condition can be accomplished at a considerably higher granularity. In reality, such point by point learning will enhance efficiencies and convey propelled benefits in an extensive variety of utilization areas including unavoidable medicinal services and keen city administrations. Be that as it may, the undeniably undetectable, thick and unavoidable gathering, preparing and scattering of information amidst individuals' private lives offers ascend to genuine security and protection concerns [1]. From one viewpoint, this information can be utilized to offer a scope of modern and customized administrations that give utility to the clients. Then again, installed in this information will be data that can be utilized to algorithmically develop a virtual life story of our exercises, uncovering private conduct and way of life designs. The protection dangers of IoT are exacerbated by the absence of essential security defends in a significant number of the original IoT items available. Various security vulnerabilities have been distinguished in associated gadgets going from shrewd locks [2] to vehicles [3]. A few characteristic highlights of IoT enhance its security and protection challenges

including: absence of focal control, heterogeneity in gadget assets, numerous assault surfaces, setting mindful and situational nature of dangers, and scale.

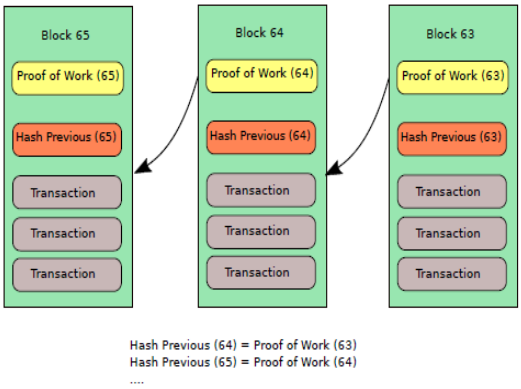

Fig. 1. Blockchain structure.

As shown in Fig. 1, the blockchain structure is composed of a sequence of blocks, which are linked together by their hash values. BitCoin, the first decentralized digital currency, impacted financial institutions, and a wide-number of cryptocurrencies entered the market in the following years. The majority of blockchain applications currently involve digital cryptocurrencies, where the users exchange monetary value with each other through the decentralized framework. Enabling decentralized trust through a consensus protocol and distributed storage through a tamper-proof ledger are the critical features of the Blockchain technology. Any application that involves multiple stakeholders can benefit from these features because it enables transparent interactions without requiring a trusted third party. IoT applications in the context of smart cities and supply chain management consist of numerous stakeholders, where the Blockchain technology can be used to strengthen the confidence among the involved entities and organizations. Although the technology has been around for almost a decade, its technical underpinnings are made clearer only in the last two years. On the one hand, architects designing IoT applications are fully aware of the limitations and capabilities of contemporary IoT platforms and technologies. On the other hand, Blockchain developers and enthusiasts understand the practical details of the Blockchain frameworks and their viability on different classes of computation and storage platforms. We notice a gap between the two communities, and it is essential to bridge this gap to fully exploit the capabilities of blockchain technology beyond cryptocurrencies and FinTech applications. This paper presents the promises of Blockchain for IoT and describes the challenges and limitations of the blockchain by correlating the architectural elements of IoT with the Blockchain. Furthermore, the paper also discusses the fundamental design questions for the application developers who are designing and implementing applications at the intersection of Blockchain and IoT.

Section 2 provides an overview and the architecture of IoT. Building blocks and architectural elements of the blockchain are presented in Section 3. Section 4 discusses the opportunities for applying blockchain for the IoT. Section 5 describes the challenges and open questions. Finally, Section 7 concludes the paper.

II. RELATED WORK

Wang et al [1] proposed the Crowdsensing applications utilize the pervasive smartphone users to collect large-scale sensing data efficiently. The quality of sensing data depends on the participation of highly skilled users. To motivate these skilled users to participate, they should receive enough rewards for compensating their resource consumption. Available incentive mechanisms mainly consider the truthfulness of the mechanism, but mostly ignore the issues of security and privacy caused by a 'trustful' center. In this paper, we propose a privacy-preserving blockchain incentive mechanism in crowdsensing applications, in which a cryptocurrency built on block chains is used as a secure incentive way. High quality contributors will get their payments that are recorded in transaction blocks. The miners will verify the transaction according to the sensing data assessment criteria published by the server. As the transaction information can disclose users' privacy, a node cooperation verification approach is proposed to achieve k-anonymity privacy protection.

Johan Älvebrink et al[2] this paper looks into up to date research of blockchain and IoT with the purpose to study blockchain as a potential solution to secure IoT data management within supply chains. Both blockchain and IoT are relatively new research areas with little existing research, which support our use of a qualitative inductive method. Semi-structured interviews, which will be further explained in the methodology section below, have been conducted with people working within the fields of blockchain, IoT and supply chain. The result indicates that blockchain can be used to secure data management within any given supply chain that uses IoT technology.

Kun Yang et al[3] explained about ***t***he Internet of Things (IoT), an emerging global network of uniquely identifiable embedded computing devices within the existing Internet infrastructure, is transforming how we live and work by increasing the connectedness of people

and things on a scale that was once unimaginable. In addition to increased communication efficiency between connected objects, the IoT also brings new security and privacy challenges. Comprehensive measures that enable IoT device authentication and secure access control need to be established. Existing hardware, software, and network protection methods, however, are designed against fraction of real security issues and lack the capability to trace the provenance and history information of IoT devices. To mitigate this shortcoming, we propose an RFID-enabled solution that aims at protecting endpoint devices in IoT supply chain. We take advantage of the connection between RFID tag and control chip in an IoT device to enable data transfer from tag memory to centralized database for authentication once deployed.

Pradip Kumar Sharma et al[4] Proposed architecture, security must automatically adapt to the threat landscape, without administrator needs to review and apply thousands of recommendations and opinions manually. These issues are caused by key mechanisms being distributed to the IoT network on a large scale, which is why a distributed secure SDN architecture for IoT using the blockchain technique (DistBlockNet) is proposed in this research. It follows the principles required for designing a secure, scalable, and efficient network architecture. The DistBlockNet model of IoT architecture combines the advantages of two emerging technologies: SDN and blockchains technology. In a verifiable manner, blockchains allow us to have a distributed peer-to-peer network where non-confident members can interact with each other without a trusted intermediary. A new scheme for updating a flow rule table using a blockchains technique is proposed to securely verify a version of the flow rule table, validate the flow rule table, and download the latest flow rules table for the IoT forwarding devices.

Simone Figorilli et al[5] This is the first work to introduce the use of blockchain technology for the electronic traceability of wood from standing tree to final user. Infotracing integrates the information related to the product quality with those related to the traceability [physical and digital documents (Radio Frequency IDentification—RFID—architecture)] within an online information system whose steps (transactions) can be made safe to evidence of alteration through the blockchain. This is a decentralized and distributed ledger that keeps records of digital transactions in such a way that makes them accessible and visible to multiple participants in a network while keeping them secure without the need of a centralized certification organism. This work implements a blockchain architecture within the wood chain electronic traceability. The infotracing system is based on RFID sensors and open source technology. The entire forest wood supply chain was simulated from standing trees to the final product passing through tree cutting and sawmill process. Different kinds of Internet of Things (IoT) open source devices and tags were used, and a specific app aiming the forest operations was engineered to collect and store in a centralized database information (e.g., species,date, position, dendrometric and commercial information).

R. B. Dhumale et al described about supply chain is a network of facilities and distribution options that performs the functions of procurement of materials, transformation of these materials into intermediate and finished products and the distribution of these finished products to customers. Supply chains exist in both service and manufacturing organizations, although the complexity of the chain may vary greatly from industry to industry and firm to firm. In this project the service is provided to customers by giving specific products or materials to particular customer or user. For providing such services to the customers there are two types of techniques are used. These techniques are Internet of Things (IoT) and Radio Frequency for Identification (RFID). Internet of thing technology is used for keeping all records related of products e.g. products delivery and updating information about products such as the cost of products, delivery date of products, products name, products delivery is to be done or not.

Lun Li et al[6] In this paper, we endeavor to resolve these two issues through proposing an effective announcement network called CreditCoin, a novel privacy-preserving incentive announcement network based on Blockchain via an efficient anonymous vehicular announcement aggregation protocol. On the one hand, CreditCoin allows nondeterministic different signers (i.e., users) to generate the signatures and to send announcements anonymously in the nonfully trusted environment. On the other hand, with Blockchain, CreditCoin motivates users with incentives to share traffic information. In addition, transactions and account information in CreditCoin are tamper-resistant. CreditCoin also achieves conditional privacy since Trace manager in CreditCoin traces malicious users' identitiesin anonymous announcements with related transactions. CreditCoin thus is able to motivate users to forward announcements anonymously and reliably.

Kai Fan et al[7] life is full of vast amount of information, the era of information has arrived. So the content-centric networks face severe challenges in dealing with a huge range of content requests, bringing protection and sharing concerns of the content. How to protect information in the network efficiently and securely for the upcoming 5G era has become a problem. The authors propose a scheme based on a blockchain to solve the

privacy issues in content-centric mobile networks for 5G. The authors implement the mutual trust between content providers and users. Besides, the openness and tamper-resistant of the blockchain ledger ensure the access control and privacy of the provider. With the help of a miner, selected from users, the authors can maintain the public ledger expediently. Also, in return, the authors share the interesting data with low overhead, network delay and congestion, and then achieve green communication.

Alexander Yohan et al[8] described with this being the case, a lot of IoT devices are manufactured and the applications of IoT are increasing drastically in the past five years. Improper device management and firmware distribution from the device manufacturer could harm the IoT environment. In this paper, a firmware update framework for IoT devices based on blockchain technology is proposed. The proposed framework aims to securely verify the firmware deployed by the device manufacturer and to securely distribute the firmware to the end-device. A PUSH-based firmware update method is adopted to deliver the new version of firmware from the legitimate vendor. In addition, smart contract and consensus mechanism from blockchain technology are utilized to preserve the integrity of the distributed firmware.

YI LIU et al [9]explained aboutBitcoin combines a peer-to-peer network and cryptographic algorithm to implement a distributed digital currency system, which keeps all transaction history on a public blockchain. Since all transactions recorded on the blockchain are public to everyone, Bitcoin users face a threat of leaking financial privacy. Many analysis and deanonymization approaches have been proposed to link transaction records to real identities. To eliminate this threat, we present an unlink able coin mixing scheme that allows users to mix their bitcoins without trusting a third party. This mixing scheme employs a primitive known as ring signature with elliptic curve digital signature algorithm (ECDSA) to conceal the transfer of coins between addresses. The mixing server is only able to check whether the output addresses belong to its customers, but it cannot tell which address owned by which customer. Customers do not have to rely on the reputation of a third party to ensure his money will be returned and his privacy will not be leaked.. Privacy of our mixing scheme are ensured through the standard ring signature and ECDSA unforgeability.

Hu et al[10] proposed to take advantage of the delay-tolerant nature of blockchains to deliver banking services to remote communities that only connect to the broader Internet intermittently. Using a base station that offers connectivity within the local area, regular transaction processing is solely handled by blockchain miners. The bank only joins to process currency exchange requests, reward miners and track user balances when the connection is available. By distributing the verification and storage tasks among peers, our system design saves on the overall deployment and operational costs without sacrificing the reliability and trustworthiness. Through theoretical and empirical analysis, we provided insights to system design, tested its robustness against network disturbances, and demonstrated the feasibility of implementation on off-the-shelf computers and mobile devices.

III. BLOCKCHAIN IN SUPPLY CHAINS

Worldwide exchange work has been especially the equivalent since the presentation of the delivery compartments in 1956. Manual paper-based procedures are as yet normal and data about the state/details of products is secured away hierarchical property. Delivery conveys about 90% of all products inside the worldwide exchange today. The multifaceted nature and offer volume of point-to-point correspondence moderates the inventory network process down over an inexactly coupled place where there is transportation suppliers, governments, ports and sea bearers. Handling the data for a compartment shipment is evaluated to cost more then twice than the genuine expense of the physical transportation. (IBM, 2017a)

Today, parties in the supply chainutilizes different frameworks for keeping up their records, this prompts each gathering have an alternate form about the current state. The records can comprises of various mediums like messages, telephone messages and paper archives prompting a powerless framework since reports can get lost and individuals can mess with data. Blockchain can help with this in light of the fact that each believed gathering in the supply chain will approach a similar data in the meantime. All gatherings can concur of the current state and there will be no errors and contentions. (IBM, 2017b)

Blockchain can be utilized in supply chains with its conveyed records, with the end goal to anchor trust with each exchange being made. Each record of each exchange is time stepped and joined to the occasion before it. By this blockchain offers points of interest in the inventory network like perceivability, streamlining and request. People that are approved can just access the records on the blockchain. This implies the records can be shared and anchored in the meantime. Perceivability and following of products can be guaranteed with the assistance of sensors and by consolidating this data with blockchain innovation; chiefs can get to information with lessened hazard. (IBM, 2016)

Wu et al. (2017) proposes a model for supply chains where data that streams between gatherings will be upheld by both private and open records. The private record will be utilized for shipments where every shipment is related with a particular record that just the gatherings engaged with the shipment will approach. This is on account of data about delicate merchandise like pharmaceutical items is better kept private. This private record incorporates data about occasions related to that particular shipment. The second kind of record is general society record and that comprises of the considerable number of occasions presented on the private records. This record can approve the area of a truck and interface the shipments through the data on the private record. General society record incorporates hash estimations of the private occasions and the records of these occasions are kept up by presenting the hash esteems on people in general record. The general population record is available to everybody dissimilar to the private records.

IV. COMPARISION WITH EXISTING METHOD

SNO	AUTHOR	MODEL	ADVANTAGE	DISADVANTAGE
1	Wang et al	Blockchain based incentive mechanism	Resist the impersonation attacks in the open and transparent blockchain	The collusion attacks is not analyzed.
2	Johan Älvebrink et al	Blockchain with supply chain	blockchain can be used to secure data management within any given supply chain that uses IoT technology	There are still barriers to make these benefits work in reality
3	Kun Yang et al	supply chain called ReSC-2.	By binding the RFID tag and the identified device together with a one-to-one mapping, potential split attacks (i.e., separating tag from product, swapping tags, etc.) can be detected;	ReSC-2 is resistant to denial-of-service attack since the RFID reader can only update the tag memory after passing the tag's authentication.
4	Pradip Kumar Sharma et al	SDN and blockchains technology- Dist Block Net model	DistBlockNet is capable of detecting attacks in the IoT network in real time with low performance overheads	Double-spending attacks is not considered.
5	Simone Figorilli et al	Radio Frequency IDentification—RFID	blockchain is perfect for applications in other contexts related to the agri-food industry	blockchain seems to suffer from technical limitations and a lack of practical applications.
6	Lun Li et al	Blockchain based incentive Mechanism	Maintains the reliability of announcements, Achieve Sybil-resistance	Location privacy is not considered.
7	Kai Fan et al	The blockchain is a public, tamper-resistant ledger	Backward security Forward security	The Sybil-resistance is not considered
8	Alexander Yohan et al	PUSH-based firmware update	secure verification mechanism is applied to securely distribute the firmware binary from the repository of device	Adaptation with the Blockchain is not analyzed.

			manufacturer to the requesting IoT device.	
9	Liu et al	The blockchain based on the ring signature with elliptic curve digital signature algorithm (ECDSA)	Resistant to DoS attacks Prevent the mixing server from mapping input Transactions Anonymity and scalability.	Double-spending attacks is not considered
10	Hu et al.	The Ethereum Blockchain	Low-cost, accessible, reliable and secure payment scheme	Accountable traceability is not considered

V. RESULT AND DISCUSSION

5.1 BLOCKCHAIN FOR THE IOT WITH SUPPLYCHAIN

5.1.1 OPPORTUNITY: Record exchanges for record and review: The information from IoT applications are transported through foundation possessed by various associations. Supply chain checking centers around following and observing resources all through the supply chain process. Conventional inventory network checking frameworks depend on an incorporated engineering, wherein every one of the information from resources are put away in a focal database. Utilizing blockchain for account the information in a decentralized record expands the trust while moving resources (genuine or computerized) through framework possessed by various and differing partners.

5.1.2 CHALLENGES: IoT applications in the space of supply chain observing comprise of cell phones with discontinuous availability. Likewise, the end-gadgets running on batteries utilize obligation cycling to draw out the lifetime. Moreover, the gadgets working on the remote groups managed by ETSI and FTC needs to hold fast to the data transfer capacity constraints authorized government specialists. In such situations, the gadgets associate with a server or edge-gadget irregularly to trade information. Expecting a design in which the server is going about as a lightweight hub for chronicle the IoT information to a blockchain, the server needs to download and store the headers of the blockchain to keep itself synchronized. For discontinuously associated IoT gadgets, the expense of running a lightweight hub for account IoT information in a blockchain system may exceed the advantages due to the data transfer capacity, calculation, and capacity costs. New blockchain conventions and structures are basic for lessening the framework cost when utilizing blockchain for account IoT exchanges and DAG-based conventions, for example, IOTA give segment resistance by making it simple to combine exchanges from divided parts of the system.

VI. CONCLUSION

Blockchain innovation has officially had a huge effect in the digital currency applications. The principal building squares - conveyed record, accord instruments, and open key cryptography - of blockchain innovation is promising for IoT and supply chain observing applications. We have talked about the design of IoT applications and mapped the utilitarian squares of the blockchain innovation to uncover the building difficulties associated with applying blockchain for the IoT. Next, we have exhibited open doors for applying blockchain for the IoT. At last, we finished up with the difficulties which should be routed to completely misuse the advantages of blockchain advancements in the IoT area. In spite of the difficulties, blockchain innovations are profoundly encouraging for settling security, protection, and trust issues in multi-partner application situations.

REFERENCES:

1) J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications," IEEE Access, vol. 6, pp. 17 545–17 556, 2018.
2) P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," IEEE Commun. Mag., vol. 55, no. 9, pp. 78–85, 2017.
3) Simone Figorilli, Francesca Antonucci , Corrado Costa „ Federico Pallottino, "A Blockchain Implementation Prototype for the Electronic Open Source Traceability ofWood along the Whole Supply Chain", Sensors 2018, 18, 3133; doi:10.3390/s18093133.
4) L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles," IEEE Trans. Intell. Transp. Syst., pp. 1–17, 2018.
5) K. Fan, Y. Ren, Y.Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving

and data sharing scheme of content-centric network in 5G," IET Commun., vol. 12, no. 5, pp. 527–532, Mar. 2018.

6) Alexander Yohan, Nai-Wei Lo, Suttawee Achawapong, "Blockchain-based Firmware Update Framework for Internet-of-Things Environment", Int'l Conf. Information and Knowledge Engineering | IKE'18 |
7) Y. Liu, X. Liu, C. Tang, J. Wang, and L. Zhang, "Unlinkable Coin Mixing Scheme for Transaction Privacy Enhancement of Bitcoin," IEEE Access, vol. 6, pp. 23 261–23 270, 2018.
8) Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, A. Seneviratne, and M. E. Ylianttila, "A Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain," jan 2018. [Online]. Available: http://arxiv.org/abs/1801.10295
9) A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy," IEEE Commun. Mag., vol. 55, no. 12, pp. 119–125, dec 2017.
10) A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems," IEEE Internet Things J., vol. 4, no. 6, pp. 1832–1843, dec 2017.
11) J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains," IEEE Trans. Ind. Informatics, vol. 13, no. 6, pp. 3154–3164, dec 2017.
12) Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in 2017 IEEE 28th Annu. Int. Symp. Pers. Indoor, Mob. Radio Commun. IEEE, oct 2017, pp. 1–5.
13) J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications," IEEE Access, vol. 6, pp. 17 545–17 556, 2018.
14) Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," IEEE Trans. Ind. Informatics, pp. 1–1, 2017.
15) T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in Proc. IEEE Technology & Engineering Management Conference (TEMSCON), June 2017.
16) J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "GridMonitoring: Secured sovereign blockchain based monitoring on smart grid," IEEE Access, vol. 6, pp. 9917–9925, 2018.
17) G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks," IEEE Trans. Smart Grid, pp. 1–1, 2018.
18) N. Zhumabekuly Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams," IEEE Trans. ependable Secur. Comput., pp. 1–1, 2016.
19) N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," Telecommunications Policy, vol. 41, no. 10, pp. 1027–1038, Nov. 2017.
20) T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of bloc