International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

xx

COPY RIGHT

IJIEMR Transactions, online available on 23th May 2024. Link
https://www.ijiemr.org/downloads/Volume-13/ISSUE-5

10.48047/IJIEMR/V13/ISSUE 05/42

TITLE: EMPLOYING BLOCKCHAIN TECHNOLOGY TO STRENGTHEN SECURITY OF WIRELESS SENSOR NETWORKS

Volume 13, ISSUE 05, Pages: 402-412

Paper Authors **MR. MAHESH BABU CHERUKURI, KANDHALA ANANTH PAL REDDY, TIRUVEEDULA BADRINATH, SURAKANTI KAVYA REDDY, BIRADAR SWETHA**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

International Journal for Innovative Engineering and Management Research

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

EMPLOYING BLOCKCHAIN TECHNOLOGY TO STRENGTHEN SECURITY OF WIRELESS SENSOR NETWORKS

MR. MAHESH BABU CHERUKURI, KANDHALA ANANTH PAL REDDY, TIRUVEEDULA BADRINATH, SURAKANTI KAVYA REDDY, BIRADAR SWETHA

ASSISTANT PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY
saimahesh912@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY
ananthpalreddy.kandhala@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY
badrinath888@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY
2610skr@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGYswethabiradar111@gmail.com

Abstract: The significant motivation behind this task is to work on the security of Wireless Sensor Networks (WSNs) by using Blockchain innovation. To achieve this reason, the drive use Blockchain innovation to store sensor information in an alter safe configuration. Each piece of information is saved as a block, which are connected along with novel hash codes. This safeguards the information's respectability and security. Any work to change the information would bring about a crisscross of hash codes, making altering simple to distinguish. The undertaking's original part is the plan of sensor nodes into gatherings, each with its own Mobile Database Node (MDN). These MDNs take information from sensor hubs, dissect it, and safely store it on the blockchain. This procedure further develops information security by lessening wellsprings of chance and guaranteeing that information is obtained and protected in a controlled and climate. To make it simpler to store and recover sensor information on the Blockchain, the task makes shrewd agreements with Robustness code. Brilliant agreements will be arrangements in which the arrangements of the agreement are straightforwardly written in code. In this specific situation, they portray capabilities that safeguard information and control the way things are kept and gotten to. The venture includes an easy to use web server interface that permits clients to get to IoT sensor information over the Blockchain securely. This connection point smoothes out client associations, simplifying it for anybody to join, sign in, and access information. It further develops information security as well as builds the openness of

WSN information, making it more helpful for various applications.

***Index terms** -Blockchain, mobile database, embedded system, mobile web server, big data analysis, sensor.*

1. INTRODUCTION

The utilization of blockchain innovation in conventional wireless sensor networks is a novel exploration approach. This study expands on the enhancements in [1] with additional specialized developments, and more exploratory outcomes are portrayed [2]. When a blockchain-based method is utilized with a web administration, it results in a blockchain-based site page framework [3], [4]. The benefit of blockchain is decentralization, which infers that information isn't subject to a solitary server. Reliance on a solitary server requires that sensor information be gathered and handled in one area. Involving a blockchain-based method for record dispersal diminishes the dangers associated with the information storehouse [5]. This study presents a blockchain-based procedure that is integrated into the WSN structure. The blockchain-based arrangement has demonstrated to be reliable and can possibly turn into the most inventive IoT innovation [6], [7].

The equipment gadgets on the left are sensors that action temperature, moistness, and air quality. The examination utilizes an assortment of microcontroller-gadget models for estimating natural information, as well as related artificial intelligence (AI) calculations for major information arranging [8]. Following essential arranging, the information are saved in the data set framework utilizing a cloud-end association in view of their sort. The methodology also processes information for investigation and afterward makes an interpretation of the information into continuous website page pictures utilizing Python and JavaScript codes. Then, the proposed framework might give a graphical translation of the sensor information. The proposed strategy permits a distant administrator to notice the discoveries while likewise signing into the framework. Since the information from these sensors can be recovered by means of web program applications, this arrangement isn't restricted to any cell phone working frameworks. However long the cell phone has a program application, the far off administrator may effortlessly sign into the framework and view sensor information and graphical examination [9], [10].

This study exploits a few of the advantages of blockchain. The main angle is that decentralized correspondences are challenging to alter. Because of the utilization of conveyed bookkeeping and stockpiling, there is no requirement for a concentrated gadget or organization association, the limitations of any hub are coordinated, and the blocks of information in the exploration are together kept up with by the hubs with scrambling capabilities [11], [12]. At the point when sensor information is approved and added to the block of the proposed blockchain-based method, it is saved persistently [13]-[15]. At the point when programmers deal with over 51% of the hubs immediately, the blockchain-based framework endures. In any case, changing the data set on a solitary hub makes no difference, making blockchain information very powerful and reliable. Accordingly, the sensor information in the proposed arrangement in light of blockchain innovation is exhaustive consistently and from any area [16]-[19].

2. LITERATURE SURVEY

This work utilizes blockchain innovation to deal with portable information bases as blocks. Sensor information from each block will be distinguished first. Block-level sensor information is connected utilizing blockchain innovation [1, 8]. Notwithstanding their singular estimation information, these connected sensor information contain all earlier block sensor information [1]. Each block hub saves the remote organization's sensor information once the framework associates each block. Versatile data sets are consolidated in Raspberry Pi equipment. This module likewise introduces a web server. This versatile web server utilizes WoT settings. This versatile data set works on information gathering while at the same time safeguarding security. This versatile web server can create different diagram sorts on the site page and send them to the cloud. A confidential cloud server farm can be made on a similar inserted equipment module as the versatile web server. After large information examination, the proposed framework would show sensor information and build the expected diagram. This framework's website page server is based on an implanted working framework to make demonstrating and envisioning illustrations in Python or JavaScript more straightforward.

A power supply shrewd agreement was displayed to arrange request age valuing pre-season of-purpose and settle and pay post-season of-purpose [3]. The brilliant agreement was tried with 1000 burdens/generators and lognormal likelihood circulations. It includes store installment, gauge based estimating discussion, use based settlement, and digital money installments. [3] Clients that fair the framework are compensated in settlement. Solidity was utilized to compose the shrewd agreement and test rpc and go-ethereum to emulate the Ethereum blockchain. In the experiment, a cost was settled and paid.

We construct a consortium blockchain engineering [2, 4, 5, 6] with a recognizing consortium chain shared by test individuals and a public chain shared by clients to distinguish hazardous codes in malware and gather proof from cell phones. Specifically, we utilize factual investigation to recreate Android malware families' product bundle, authorization and application, and capability call properties. Our Android-based malware recognition and arrangement utilizes multi-include discovery to diminish misleading positive rates and improve malware variation identification [5]. We make a blockchain-based truth base of dispersed Android unsafe projects. The new strategy has more noteworthy location precision significantly quicker and lower bogus positive and misleading negative rates than prior calculations, as indicated by tests.

Clinics oversee Electronic Health Records (EHRs), making it hard to think about medical clinic proposals. Patients should focus on their heath and recover clinical information the board. [8, 9, 10] Blockchain innovation is quickly propelling populace medical services, including clinical records and patient information. The innovation gives patients complete, permanent records and free EHR access from specialist co-ops and treatment sites. In this paper [7], we present a characteristic based signature conspire with numerous specialists to check blockchain-embodied EHRs. A patient underwrites a message as per the quality while revealing no other data. Without a confided in focal power to issue and circulate patient public/confidential keys, various specialists stay away from the escrow issue and follow blockchain conveyed information capacity. An intrigue attack from N compromised specialists is forestalled by giving mystery pseudorandom capability seeds. We further demonstrate that our characteristic based signature strategy is protected in the irregular prophet model for the trait endorser's unforgeability and ideal security under the computational bilinear Diffie-Hellman suspicion. The proposed approach is contrasted with past examination' philosophies for productivity and qualities.

The cyber physical system (CPS) has succeeded in enormous scope appropriated reconciliation. In such frameworks, sensor gadgets gather information that is dependably shipped off totally intrigued actual world cooperators. Be that as it may, CPS's very capricious climate, for example, network middleware limitations, makes protected and reliable information dispersion administrations troublesome. This study [9] proposes secure pub-sub (SPS) without center product, a blockchain-based fair installment with notoriety design. In SPS, distributers post a point on the blockchain and endorsers store to demonstrate interest. In the event that the interest message fits the subject, the distributer sends the encoded material to the blockchain [1, 10] so supporters might unravel and assign the distributer as its standing. At long last, endorsers pay the distributer. The new idea guarantees information protection, endorser obscurity, and distributer supporter installment reasonableness. Since we use blockchain, no believed outsider is involved, not normal for conventional bar sub frameworks. The arranged SPS's security is surveyed. Carrying out the convention utilizing Ethereum smart contract proves SPS.

3. METHODOLOGY

i) Proposed Work:

The recommended approach looks to incredibly work on the security of Wireless Sensor Networks (WSNs) [6, 7] by using Blockchain innovation. This clever method incorporates decentralized, carefully designed information capacity, which guarantees the respectability of procured data. Furthermore, sensor hubs are organized into bunches with Mobile Database Nodes (MDNs) to give safe information social affair and capacity inside the Blockchain. An easy to understand web interface makes information access simpler, which further develops security and information openness in WSN applications, making it a comprehensive answer for information security and organization uprightness [13, 14]. The utilization of Blockchain innovation further develops information security and trustworthiness by using carefully designed information capacity and cryptographic confirmation, thus diminishing the risk of undesirable access and information control. Sensor hubs organized into bunches utilizing MDNs and secure information stores inside Blockchain decrease likely marks of shortcoming, making it more hard for assailants to penetrate the organization. An easy to understand web interface improves on information access, making it more open to clients while guaranteeing security, and expanding the value of WSN information for different applications. Savvy contracts make information capacity and recovery more straightforward, further develop control and admittance to put away data, and smooth out managerial exercises all through the organization.

ii) System Architecture:

The framework engineering comprises of WSNs [7] and a Sink Node, which fills in as a main issue for information gathering from sensors. The obtained information is in this manner sent by means of the Web. Here, the Blockchain System comes right into it, going about as a decentralized and secure record for putting away and controlling sensor data. The blockchain framework gives information trustworthiness and sealing. Subsequent to being saved money on the blockchain, clients and examination devices might get to the information for inside and out exploration and bits of knowledge. This engineering incorporates the Web with blockchain innovation to construct a thorough and secure climate for making due, putting away, and breaking down information from WSNs [6].

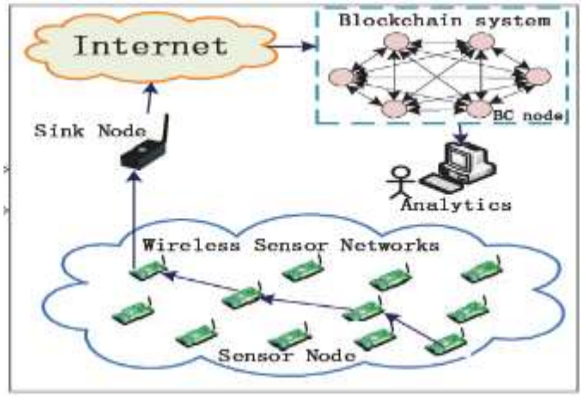


Fig 1 Proposed Architecture

iii) Processing:

Rather of relying upon a single central server, blockchain innovation stores information across a few hubs in a circulated network. The decentralization further develops information security and accessibility. In this venture, the MDN fills in as an extension between minuscule sensors and the blockchain. It mines blocks with the SHA-256 calculation, which produces one of a kind exchange hash codes for information. This safeguards the information's security and honesty. Each block in a blockchain is doled out a one of a kind Hashcode. These blocks are put away on a few hubs or servers. Prior to putting away new passages, blockchain actually takes a look at each block's Hashcode. Assuming any block information is refreshed, the Hashcode changes, producing security alerts and guaranteeing the information's respectability and unchanging nature. Clients have safe admittance to WSN [6] information recorded on the blockchain. This entrance guarantees the legitimacy and security of information, permitting clients to acquire and associate with it certainly. Smart contracts created in SOLIDITY code oversee information on the blockchain. They indicate how information is saved and gotten to, ensuring solid and secure activities. Without real IoT sensors, reproduction hubs are used to make mimicked temperature information. This information looks like veritable sensor readings and is safely kept on the blockchain, permitting the security framework to be tried and approved.

vi) Modules:

WSNSimulation: these are the modules in WSN Simulation

- **Start WSN Simulation:** This module begins a recreation of WSN [13, 14]. Simulated nodes produce arbitrary information, as temperature estimations, that imitates the way of behaving of certified IoT-associated sensors.
- **Stop Simulation:** This choice permits us to stop the WSN recreation when it is not generally needed.
- **Transaction Processed Graph:** This module shows a graphical portrayal of the time expected to execute every exchange in the framework. It assists us with perceiving how effectively the framework processes information exchanges.

Web Server:

- **New User Signup:** In this module, new users might make accounts by joining. Users give their data to make a safe record for review IoT sensor information put away on the Blockchain.
- **User Login:** This option allows registered users to log into their accounts. After successfully logging in, users will have access to the project's features and data.
- **Access Blockchain WSN [7]:** This module enables users to safely access IoT sensor data stored on the Blockchain. Users may choose which sensors or data points to examine and interact with.

4. EXPERIMENTAL RESULTS

Fig 2 WSN simulation

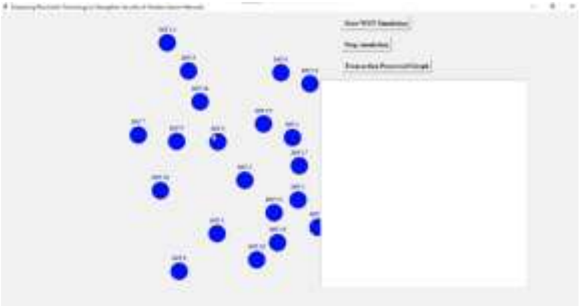


Fig 3 Start WSN simulation

Fig 4 Stop simulation

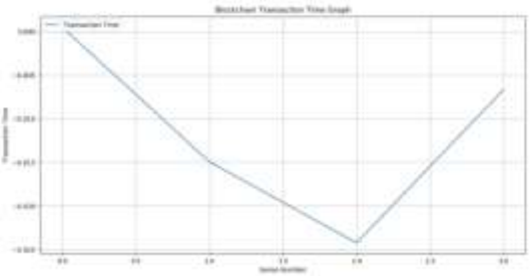
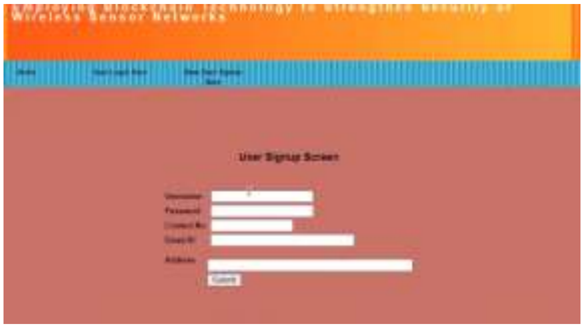


Fig 5 Transaction processed graph

Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks

Fig 6 Home screen

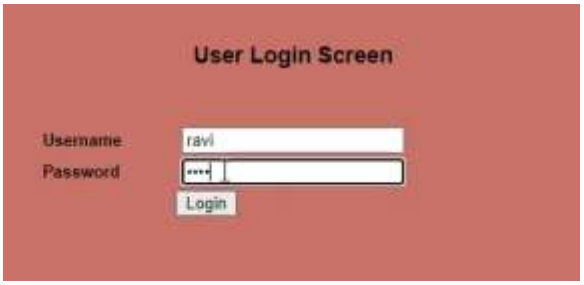


Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks

User Signup Screen

Username
Password
Contact No
Email ID
Address
Submit

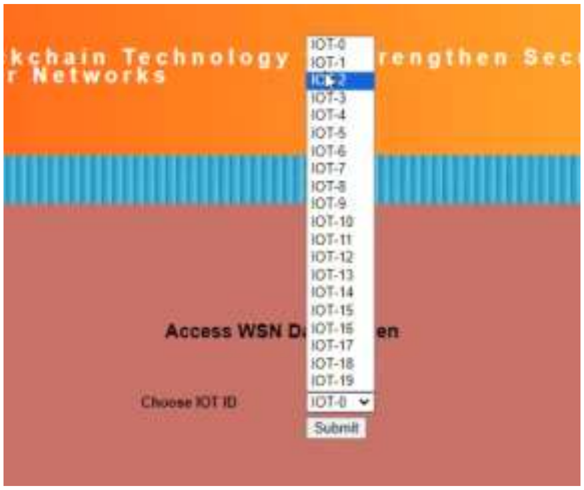
Fig 7 User signup



User Login Screen

Username ravi
Password ••••
Login

Fig 8 User login



kchain Technology rengthen Sec
r Networks

Access WSN D en

Choose IOT ID IOT-0
Submit

Fig 9 Access WSN bloackchain

5. CONCLUSION

The investigation exhibited how Blockchain innovation may significantly work on the security of Wireless Sensor Networks (WSN) information [6, 7, 13, 14]. By disseminating information north of a few nodes in a decentralized style, the venture effectively disposed of the dangers related with brought together servers. This diminished the risk of information control and unlawful access. It was basic to Keep up with information honesty. Information was safely saved in alter safe blocks, each with its own hash code, which expanded the constancy of the data. In spite of the absence of genuine IoT WSN sensors, the task utilized reenactment hubs to completely test and approve the blockchain-based security component. Making and conveying smart contracts written in Robustness offered a strong structure for handling and recovering sensor information from the blockchain. The undertaking's web server connection points were made in light of convenience, letting clients to securely see and associate with IoT [16] sensor information. We completely explored what amount of time exchanges required to outwardly finish and showed this information. This study permitted us to survey how successfully the framework was performing, guaranteeing that information assortment stayed fast and proficient. At last, the examination uncovered that consolidating blockchain innovation may impressively work on the security and uprightness of information procured from IoT-associated sensors, guaranteeing its constancy and dependability for various applications.

6. FUTURE SCOPE

Research might focus on working on the versatility and effectiveness of blockchain-based WSNs to help a more prominent number of hubs and information exchanges, guaranteeing the framework's steadiness in enormous scope organizations. Investigating the combination of arising advances, for example, artificial intelligence and machine learning with blockchain in WSNs can empower improved information examination and navigation, opening up new roads for information driven bits of knowledge [26-28]. Executing and working on smart contracts in the blockchain-based WSN design might robotize and authorize safe information moves and associations across sensor nodes, thus speeding network tasks. True tests and contextual investigations in an assortment of use circumstances can assess the proposed framework's exhibition, reliability, and plausibility, offering valuable bits of knowledge for certifiable organizations. These examination regions help to create and advance protected and solid remote sensor networks with blockchain innovation, supporting development in the field of IoT and sensor-based applications [16].

REFERENCES

[1] S.-Y. Wang, Y.-J. Hsu, and S.-J. Hsiao, ‘‘Integrating blockchain technology for data collection and analysis in wireless sensor networks with an innovative implementation,’’ in Proc. Int. Symp. Comput., Consum. Control (ISC), Dec. 2018, pp. 149–152.

[2] 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.

[3] L. Thomas, C. Long, P. Burnap, J. Wu, and N. Jenkins, ‘‘Automation of the supplier role in the GB power system using blockchain-based smart contracts,’’ CIRED-Open Access Proc. J., vol. 2017, no. 1, pp. 2619–2623, Oct. 2017.

[4] 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.

[5] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, ‘‘Consortium blockchain-based malware detection in mobile devices,’’ IEEE Access, vol. 6, pp. 12118–12128, 2018.

[6] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, ‘‘The blockchain as a decentralized security framework [future directions],’’ IEEE Consum. Electron. Mag., vol. 7, no. 2, pp. 18–21, Mar. 2018.

[7] R. Guo, H. Shi, Q. Zhao, and D. Zheng, ‘‘Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems,’’ IEEE Access, vol. 6, pp. 11676–11686, 2018.

[8] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, ‘‘When intrusion detection meets blockchain technology: A review,’’ IEEE Access, vol. 6, pp. 10179–10188, 2018.

[9] Y. Zhao, Y. Li, Q. Mu, B. Yang, and Y. Yu, ‘‘Secure pub-sub: Blockchainbased fair payment with reputation for reliable cyber physical systems,’’ IEEE Access, vol. 6, pp. 12295–12303, 2018.

[10] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, ‘‘An anti-quantum transaction authentication approach in blockchain,’’ IEEE Access, vol. 6, pp. 5393–5401, 2018.

[11] 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.

[12] J.-H. Lee, ‘‘BIDaaS: Blockchain based ID as a service,’’ IEEE Access, vol. 6, pp. 2274–2278, 2018.

[13] H. Jang and J. Lee, ‘‘An empirical study on modeling and prediction of bitcoin prices with Bayesian neural networks based on blockchain information,’’ IEEE Access, vol. 6, pp. 5427–5437, 2018.

[14] Q. Lu and X. Xu, ‘‘Adaptable blockchain-based systems: A case study for product traceability,’’ IEEE Softw., vol. 34, no. 6, pp. 21–27, Nov. 2017.

[15] A. Anjum, M. Sporny, and A. Sill, ‘‘Blockchain standards for compliance and trust,’’ IEEE Cloud Comput., vol. 4, no. 4, pp. 84–90, Jul. 2017.

[16] P. K. Sharma, M.-Y. Chen, and J. H. Park, ‘‘A software defined fog node based distributed blockchain cloud architecture for IoT,’’ IEEE Access, vol. 6, pp. 115–124, 2018.

[17] M. E. Peck, ‘‘Blockchain world–do you need a blockchain? This chart will tell you if the technology can solve your problem,’’ IEEE Spectr., vol. 54, no. 10, pp. 38–60, Oct. 2017.

[18] M. E. Peck and S. K. Moore, ‘‘The blossoming of the blockchain,’’ IEEE Spectr., vol. 54, no. 10, pp. 24–25, Oct. 2017.

[19] P. Fairley, ‘‘Blockchain world–feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous,’’ IEEE Spectr., vol. 54, no. 10, pp. 36–59, Oct. 2017.

[20] A. Nordrum, ‘‘Govern by blockchain dubai wants one platform to rule them all, while Illinois will try anything,’’ IEEE Spectr., vol. 54, no. 10, pp. 54–55, Oct. 2017.

[21] M. E. Peck and D. Wagman, ‘‘Energy trading for fun and profit buy your neighbor’s rooftop solar power or sell your own-it’ll all be on a blockchain,’’ IEEE Spectr., vol. 54, no. 10, pp. 56–61, Oct. 2017.

[22] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, ‘‘Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm,’’ IEEE Access, vol. 7, pp. 9714–9723, 2019.

[23] K. Kotobi and S. G. Bilen, ‘‘Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access,’’ IEEE Veh. Technol. Mag., vol. 13, no. 1, pp. 32–39, Mar. 2018.

[24] A. Islam, M. B. Uddin, M. F. Kader, and S. Y. Shin, ‘‘Blockchain based secure data handover scheme in non-orthogonal multiple access,’’ in Proc. 4th Int. Conf. Wireless Telematics (ICWT), Jul. 2018, pp. 1–5.

[25] K. Kotobi and S. G. Bilen, ‘‘Blockchain-enabled spectrum access in cognitive radio networks,’’ in Proc. Wireless Telecommun. Symp. (WTS), Apr. 2017, pp. 1–6.

[26] X. Feng, J. Ma, T. Feng, Y. Miao, and X. Liu, ‘‘Consortium blockchainbased SIFT: Outsourcing encrypted feature extraction in the D2D network,’’ IEEE Access, vol. 6, pp. 52248–52260, 2018.

[27] Z. Wang, Y. Tian, and J. Zhu, ‘‘Data sharing and tracing scheme based on blockchain,’’ in Proc. 8th Int. Conf. Logistics, Informat. Service Sci. (LISS), Aug. 2018, pp. 1–6.

[28] Q. He, Y. Xu, Y. Yan, J. Wang, Q. Han, and L. Li, ‘‘A consensus and incentive program for charging piles based on consortium blockchain,’’ CSEE J. Power Energy Syst., vol. 4, no. 4, pp. 452–458, 2018.

[29] H. Xie, Z. Yan, Z. Yao, and M. Atiquzzaman, ‘‘Data collection for security measurement in wireless sensor networks: A survey,’’ IEEE Internet Things J., vol. 6, no. 2, pp. 2205–2224, Apr. 2019.

[30] S. A. Sert, E. Onur, and A. Yazici, ‘‘Security attacks and countermeasures in surveillance wireless sensor networks,’’ in Proc. 9th Int. Conf. Appl. Inf. Commun. Technol. (AICT), Oct. 2015, pp. 201–205.

[31] A. Sharma and S. Chauhan, ‘‘Sensor fusion for distributed detection of mobile intruders in surveillance wireless sensor networks,’’ IEEE Sensors J., vol. 20, no. 24, pp. 15224–15231, Dec. 2020.

[32] A. Yazici, M. Koyuncu, S. A. Sert, and T. Yilmaz, ‘‘A fusion-based framework for wireless multimedia sensor networks in surveillance applications,’’ IEEE Access, vol. 7, pp. 2169–3536, Jul. 2019.

[33] X. Gou, C. Zhao, T. Yang, L. Zou, Y. Zhou, Y. Yan, X. Li, and B. Cui, ‘‘Single hash: Use one hash function to build faster hash based data structures,’’ in Proc. IEEE Int. Conf. Big Data Smart Comput. (BigComp), Jan. 2018, pp. 278–285.

[34] M. Kidon and R. Dobai, ‘‘Evolutionary design of hash functions for IP address hashing using genetic programming,’’ in Proc. IEEE Congr. Evol. Comput. (CEC), Jun. 2017, pp. 1720–1727.

[35] N. Veeraragavan, L. Arockiam, and S. S. Manikandasaran, ‘‘Enhanced encryption algorithm (EEA) for protecting users’ credentials in public cloud,’’ in Proc. Int. Conf. Algorithms, Methodol., Models Appl. Emerg. Technol. (ICAMMAET), Feb. 2017, pp. 1–6.

[36] A. Mustafa and Hendrawan, ‘‘Calculation of encryption algorithm combination for video

encryption using two layers of AHP,’’ in Proc. 10th Int. Conf. Telecommun. Syst. Services Appl. (TSSA), Oct. 2016, pp. 1–7.

[37] A. A. Moldovyan, N. A. Moldovyan, A. N. Berezin, and P. I. Shapovalov, ‘‘Randomized pseudo-probabilistic encryption algorithms,’’ in Proc. 20th IEEE Int. Conf. Soft Comput. Meas. (SCM), May 2017, pp. 14–17.

[38] F. S. Wu, ‘‘Research of cloud platform data encryption technology based on ECC algorithm,’’ in Proc. Int. Conf. Virtual Reality Intell. Syst. (ICVRIS), Aug. 2018, pp. 125–129.

[39] B. T. Baker, R. F. Silva, V. D. Calhoun, A. D. Sarwate, and S. M. Plis, ‘‘Large scale collaboration with autonomy: Decentralized data ICA,’’ in Proc. IEEE 25th Int. Workshop Mach. Learn. Signal Process. (MLSP), Sep. 2015, pp. 1–6.

[40] K. Xie, W. Luo, X. Wang, D. Xie, J. Cao, J. Wen, and G. Xie, ‘‘Decentralized context sharing in vehicular delay tolerant networks with compressive sensing,’’ in Proc. IEEE 36th Int. Conf. Distrib. Comput. Syst. (ICDCS), Jun. 2016, pp. 169–178.

[41] K. Nomura, M. Mohri, Y. Shiraishi, and M. Morii, ‘‘Attribute revocable attribute-based encryption for decentralized disruption-tolerant military networks,’’ in Proc. 3rd Int. Symp. Comput. Netw. (CANDAR), Dec. 2015, pp. 491–494.

[42] Y. He, M. Yan, M. Shahidehpour, Z. Li, C. Guo, L. Wu, and Y. Ding, ‘‘Decentralized optimization of multi-area electricity-natural gas flows based on cone reformulation,’’ IEEE Trans. Power Syst., vol. 33, no. 4, pp. 4531–4542, Jul. 2018.