Converging Blockchain and Internet of Things

David Nettikadan, Riya T Raphael, Blessy Daise Paul

Abstract*: Internet of Things (IoT) ecosystem is expanding at an unimaginable pace and is applied to every aspect of life. Though no one questions the impact and usefulness of this technology, many criticisms have been coming up these days as many security and privacy issues are made public. At the same time having a central system capable of controlling and maintaining a large number of devices is also an issue faced by the IoT ecosystem. The solution proposed by most of the researchers and industries is to converge the IoT ecosystem with the technology underlying the most secure cryptocurrency Bitcoin, which is called as Blockchain. A blockchain in short is an immutable distributed ledger system. It enables the IoT devices to have data security and privacy without needing a central authority. This paper studies what are the issues IoT ecosystem is currently facing and how a blockchain can help to solve it, the relevance of blockchain-IoT convergence, and the areas where this can be applied. The companies who are developing products based on this new technology and various challenges this technology is facing right now is also explored in this paper.

Keywords: Blockchain, De-centralization, Distributed Systems, Internet of Things, Security.

I. INTRODUCTION TO INTERNET OF THINGS

Internet of Things (IoT) is a network of everyday objects often called as 'things', which are interconnected to each other. It is used to make everyday objects smarter. IoT is used in smart homes, to monitor the environmental and security conditions of the home and to control home appliances automatically. IoT has been used in enterprise based applications such as a factory setup for automation, climate control, and automation. It is also used for providing utilities like energy via smart grid and smart metering, water, and other utilities. Smart transportations and logistics are another domain of application of IoT. The live traffic situation is sensed using various sensors and the traffic lights and routing are controlled accordingly. Another main area of application is healthcare where the diagnosis can be automated to large extent. [1]

A. Challenges Faced by IoT Ecosystem

But as the application scenarios of IoT are exponentially increasing, the issues concerning IoT are also increasing. The challenges IoT ecosystem faces can be primarily categorized into three areas: security, scalability, and privacy. [2] The data IoT devices generate and process contains sensitive information. For example, a security camera or camera as part of a smart TV can be used to monitor the presence of people in a home. So these devices are always an appealing target for cyber-attacks. The security systems are not equipped to accommodate the large ecosystem which has resulted in various catastrophes.

Security Issues. A DNS provider named Dyn faced cyber-attack in October 2016, where the attack originated from 'tens of millions of IP addresses' and a considerable amount of the traffic was from IoT devices like webcams, baby monitors, home routers. Those devices were infected with malware named Mirai, which used those devices to launch a DDoS (distributed denial of service) attack on the server. This attack demonstrated how vulnerable the security of the IoT devices is. [3]

The IoT devices are usually of low energy and lightweight in nature. In IoT devices, most of the CPU resources are allocated to execute the core application functionalities. To attain security and privacy additional cryptographic support for devices is needed. This will need additional resources which will result in price hikes which will6 not be in the general interests of the manufacturers and consumers. Securing IoT network is also a major issue since there is a wide range of communication standards, protocols, and device capabilities. The network is getting more complex making it more difficult to secure it. Though many security mechanisms for IoT exist right now it's not equipped to address present challenges. [4]

Need of Central Server. It is predicted that the IoT devices will cross 20 billion in numbers by 2020. Present IoT solutions are depended on centralized server-client architecture which won't be able to accommodate the present growth of IoT devices. To accommodate the increasing number of IoT devices, the capacity of the central server has to be increased, which in case increase the price dramatically. So we need some decentralized architecture depending on Peer-to-Peer structure. For this, some new technology has to be adopted.

Privacy Issues. After the Edward Snowden leaks the customers cannot trust the technological partners who give access and control to authorities to collect and analyze their data which risks the privacy and anonymity of the user. To increase the trust factor and transparency they should adopt open-source approaches. [5] A new technology called blockchain can be a solution to the problems faced by the IoT ecosystem right now.

Revised Manuscript Received on May 28, 2019.

David Nettikadan, Assistant Professor, Department of Electronics and Communication Engineering, Jyothi Engineering College, Thrissur, India.

Riya T Raphael, M.Tech Scholar, Department of Electronics and Communication Engineering, Sahrdaya College of Engineering and Technology , Thrissur, India

Blessy Daise Paul, M.Tech Scholar, Department of Electronics and Communication Engineering, Sahrdaya College of Engineering and Technology , Thrissur, India

II. INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

Bitcoin and the technology underlying it called blockchain is a buzzword today not only in the financial sector but even to the industrial and academic world because of its wide range of future application scenarios. Satoshi Nakamoto in 2009 proposed a peer-to-peer version of electronic cash system which does not need a third party financial institution to authenticate it. [6]

Similar to IoT we cannot find a standard definition on the blockchain. The National Institute of Standards and Technology (NIST) in their paper defines blockchain as "immutable digital ledger systems implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority". [7] The blockchain use cases are diverse like finance, healthcare, distribution, agriculture, manufacturing and much more.

A. Blockchain Architecture

Blockchain can be said as a sequence of the block, where each block contains a list of transaction records. Each block has two part block header and block body. The block header contains block version (set of block validation rules to follow), Merkle tree root hash (hash value of all transactions in the block), Time (current time as seconds), nBits (target threshold of a valid block hash), Nonce (4-byte field counter), and parent block hash (256-bit hash value point to previous block). The body of the block consists of transaction counter and transactions. A block is connected to the previous block using the parent block hash in the header and thus forms a chain. [8] Figure 1 shows a sample continuous sequence in a blockchain.

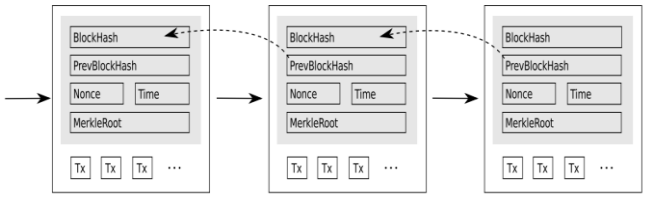

Figure-1. Architecture of blocks in blockchain and a sample sequence of block. [9]

B. Consensus Mechanisms

Blocks are generated frequently and there must be a mechanism to validate block to ensure the proper functioning of the blockchain. It is done by consensus, a mechanism that determines the condition to reach an agreement regarding the validation of blocks to be added to a blockchain. The most popular one is the one that was introduced by Satoshi Nakamoto called the proof of work (PoW). In proof of work, persons so-called miners will compete for each other to solve a difficult cryptographic puzzle. Who can solve the puzzle first wins a prize and the block which holds the transactions will be added to the chain. The process is called mining. But the problem is that it will take a lot of energy and time for computing which is a waste. To avoid it another popular consensus mechanism is the proof of stake (PoS) where no one races for the prize. Instead, a 'validator' invests the coins in the stem and those having a large number of coins will be picked to create the next block of the chain. There are many other consensus mechanisms like proof of activity, Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), Ripple consensus algorithm which is beyond the scope of this paper. [8][9]

C. Types of Blockchain

Nature of blockchain is usually explained in the terms of private/public and permissioned/unpermissioned blockchain. Blockchain provides a distributed ledger technology, where the copies of the ledger can be kept by different users. But the difference lies in who can access the ledgers. Private blockchain restricts the read/write access to preselected group of people to maintain the integrity of system. A permission structure can also be implemented for accessing the chain. Private blockchains will be more private and secure and public blockchain will be having advantages in terms of interoperability, operational costs and time and network traffic. [8]

There can be three types of blockchain using this taxonomy. A) Permissioned, private shared ledger: Here the permission to make additions to the chain is limited to the owner group of the chain. Eg: Bankchain, a clearing and settlement network. B) Permissioned, public shared ledger: Here the permission to use the ledger is given to a group or a person who is validated as the trusted ledger owners or actors. Eg: Ripple, a global financial transaction system. C) Unpermissioned, public shared ledger: Here any user can make transactions with consensus, no special authorization is needed. Eg: Bitcoin, the crypto currency. [8]

III. CONVERGING BLOCKCHAIN AND INTERNET OF THINGS

Some characteristics of blockchain are favorable to be used in an IoT ecosystem. Table 1 shows various challenges faced by IoT ecosystem and how blockchain can overcome those situations.

A. Securing Data

The most important characteristic is that blockchain is immutable. Once the transaction is packed in the block, it cannot be tampered. This introduces the elements of honesty and trust factor to the customers. It enables devices to have transactions and communications as trusted parties. Though the devices may not know each other, the immutability of records enables the devices to trust and cooperate. It introduces the trust factor not only on a device level but also even in the level of an organization. It also ensures the data is secure and not even the service providers or the manufacturers can tamper any information.

B. Reducing Cost

The IoT blockchain convergence results in the elimination of the middleman from the system enabling communication and data exchange on a peer-to-peer basis. This removes overhead costs of additional protocols or high-performance servers. This also helps in reducing the overall cost of the

system. If a network is large the central server should be large enough to accommodate it. This server becomes a probable target of attack as it contains a large amount of data. The additional cost must be spent to make it more secure. This can be reduced by decentralizing the system using blockchain. At the same time, it improves the device identification and authentication as the devices in the network can be easily identified and authenticated without the need of a central server. This is useful in setting up ad hoc networks.

C. *Speeding up Transactions*

Blockchain can also be used to instruct a system on what to do, and the steps to execute the instruction. The smart contract can be said as a computer algorithm that can be automatically executed when the terms and conditions of the contract are met. This improves the reliability of the system and users as well as the speed of transactions. The information exchanges are automated and don't need third parties to execute it accelerate the data exchanges.

Table -I. How blockchain can address Internet of Things (IoT) challenges. [3]

Challenge	Explanation	Potential blockchain solution
Costs and capacity constraints	It is a challenge to handle exponential growth in IoT devices: by 2020, a network capacity at least 1,000 times the level of 2016 will be needed.	No need for a centralized entity: devices can communicate securely, exchange value with each other, and execute actions automatically through smart contracts
Deficient architecture	Each block of IoT architecture acts as a bottleneck or point of failure and disrupts the entire network; vulnerability to distributed denial-of-service attacks, hacking, data theft, and remote hijacking also exists.	Secure messaging between devices: the validity of a device's identity is verified, and transactions are signed and verified cryptographically to ensure that only a message's originator could have sent it.
Cloud server downtime and unavailability of services	Cloud servers are sometimes down due to cyber attacks, software bugs, power, cooling, or other problems.	No single point of failure: records are on many computers and devices that hold identical information.
Susceptibility to manipulation	Information is likely to be manipulated and put to inappropriate uses.	Decentralized access and immutability: malicious actions can be detected and prevented. Devices are interlocked: if one device's blockchain updates are breached, the system rejects it.

IV. APPLICATION SCENARIOS AND USE CASES

The areas in which IoT can be applied are diverse and all of them become relevant when it is combined with the power of blockchain and at the same time it becomes more secure. Blockchain IoT can be used in following Scenarios: Government, Democracy & Law Enforcement, Energy, Transportation, Smart Objects, Fleet Monitoring and Management, Industry 4.0, Personal Sensing, Healthcare, Smart Cities, Collaborative and Crowd Sensing, Financial Transactions, Farming, Defense & Public Safety, and Telecommunications & Information Systems.[5]

A. *Supply Chain*

The most popular industrial application where it can be used is the supply chain or fleet monitoring and management. In a supply chain industry, every transaction can be made transparent and traceable. The usual scene of manufacturing and supply chain is that the company maintains ledgers of their transactions only and doesn't know what happens afterward. But when applied to blockchain the complete details will be recorded and the copy is kept by each and every participant. It can be used to track the complete life cycle of a product like the wheat cultivated in the farm, to the company where the bread is manufactured, to the store where the bread is sold. Tracking a product from manufacturer to the customer and beyond helps the customer to check the fake consumer market. [10]

B. *Healthcare*

Healthcare which is a rapidly advancing IoT application can also be made private, fast and secure by converging it with blockchain technology. In the present scenario, the medical records of patients are spread out in hospitals, labs, pharmacies etc., and it's practically impossible to get a consolidated overview. Blockchain enables to securely store the data in a time-stamped block of data, which cannot be tampered with. It can be reviewed only by the authorized personnel who have the permission to do so, using a permissioned blockchain, thus avoiding the misuse of the data. It helps medical industry indirectly through providing services in areas such as billing and claims management using smart contracts, medical asset tracking, medicine supply chain management etc. [11]

C. *Energy Distribution*

In the current scenario energy creation and distribution to the consumer is done using some agencies like the electricity board of the state or nation. In present scenario where individual homes are able to generate electricity by itself, there must be some mechanisms through which houses can sell and buy electricity from others. It can be done even without a centralized system done using blockchain. Also there is a lack of electric charging infrastructure, which will be a major requirement in coming years. The charging can be done using smart contracts to share and charge electric vehicles using micropayments. [12]

D. *Others*

There are many other areas in which IoT-blockchain can be used. In agriculture the food safety is ensured by keeping track of the agro-food supplied. It can be used to have a secure

vehicular network without having a central trusted authority. It can be used in smart cities and Industrial applications so that the data is private and secured. Wherever financial transactions have to be done without having a central banking system cryptocurrencies can be relied upon. [5]

V. COMPANIES IN PLAY

A. IBM

We can say the blockchain-IoT convergence is only in its infancy stage, but the big tech companies have already started working on these technologies. The first giant player who has entered the field is IBM blockchain. IBM has already launched an IBM Blockchain Platform, which provides blockchain-as-a-Service (BaaS). By providing the blockchain service through the cloud it allows the clients to develop, govern and operate any network with high-security performance. It uses the Hyperledger fabric to provide the services. [13] IBM is planning to combine the power of IoT, blockchain and artificial intelligence which opens a great number of opportunities. An advantage of IBM Blockchain Platform is that the customers need not develop applications from scratch. It provides a number of industry use case scenarios from which they can start with. IBM has teamed up with various companies and have developed many Blockchain based solutions for large companies in various domains like supply chain, healthcare management, energy management, IoT devices etc.

B. Filament

A company named Filament have developed both hardware and software solutions for Blockchain-IoT convergence. They have developed a low-cost chip named Blocklet which is IoT optimized and can be powered by a coin-cell. In a small footprint, it provides trusted execution environment. Along with the hardware chip they have also provided software with the same name designed for embedded systems. It can provide a cryptographic chain of custody ledger from the beginning of production to delivery of product and even on-site provisioning. [14]

C. Everledger

Everledger is a UK based startup which uses IoT, blockchain, smart contract and machine vision to track the provenance of high-value assets. Their hyperledger based distributed ledger they made has enabled the manufacturers, retailers and consumers to track the whole life cycle of the diamond from origin to the end customer. They have developed a 'Diamond Time-Lapse Protocol' in 2017 which is a ledger which records the country of origin, and the list of persons who chose, architected, laser cut, crafter and groomed the diamond with the profile of each person. The detail of the agency who graded the diamond and the report is also provided. This helps in identifying the 'blood diamond' made using forced labor or stolen diamonds. They have teamed up with Sightholder of De Beers Group of Companies and Alliance of Alrosa and have made a database of more than two million diamonds.[15]

D. Others

There are many startups working in applying blockchain into medical industry. Healthbank is a Swiss startup, which has provided a blockchain based Electronic Medical Record System (EMR). It collects medical data from number of medical devices, assimilates it. The personal health data can be shared to medical professional or family members if permitted by the user.[16] Guardian is an Estonian company, who has developed blockchain Keyless Signature Infrastructure (KSI). It can provide authentication in large scale and using it they are going to record the complete medical records in the country of Estonia. New companies like MedRec, Medicalchain, UnitedHealth Group, Camelot Consulting Group, joining the game which will perfect the technology in due time. Many The Chinese government is collaborating with Alibaba and Russian Ministry of Health partner with Vnesheconobank government initiatives have been also started like that in Estonia. The Chinese government is collaborating with Alibaba and Russian Ministry of Health partner with Vnesheconobank, a state-owned bank to apply blockchain in the medical sector.

Slock is a company which provides a smart locking system based on smart contracts. They made a physical technology that can be embedded into any smart devices like smart door, vehicles etc. The aim of the company is to promote a shared economy. For example, you want to lease a room or a cycle for a limited period. The deal can be made using a smart contract which leaves out the necessity of an intermediary. [17]. IoT chain has developed a light, secure operating System called ITC for IoT devices based on blockchain technology. It can be used for payment, digital transaction, shared economy and secure access.[18] Other companies like Blockchainofthings, BitSE, Chronicled, Kinno, Iota, Io3energy, SolarCoin have entered the market exploring new application scenarios where blockchain can be merged with IoT.

VI. CHALLENGES FOR BLOCKCHAIN-IOT CONVERGENCE

Though we were discussing various benefits and possibilities of blockchain-IoT convergence there exists various challenges in making this convergence a full reality. IoT devices are mainly embedded systems which having many design constraints like speed, power consumption, storage, cost, size etc. The Blockchain technology is developed envisioning the general computers in mind which don't have the above-said constraints. So merging the two technologies has its own cons. Various articles like [2, 5, 19, 20] propose various challenges in implementing the system. The prominent challenges are Scalability, Energy consumption, Processing time, Storage needed and legal compliances.

A. Scalability

As the network size and number of transaction increases, many issues come into existence. As most of the blockchain services are provided as cloud service, the limited bandwidth can cause a problem in real time processing of the data. The

transaction fees, data storage necessary and the cost and risk of potential downtime will also increase as the network grows. Some companies propose many solutions to make the architecture simpler like side-chains, tree-chains, and mini-blockchains.

B. Energy Consumption

Blockchain technology was always criticized from its early days for the energy consumption especially in the context of Bitcoin mining. A lot of computations have to be done for encrypting and verifying blocks. This has resulted in a large amount of processing energy consumption. But as an embedded system IoT has to always consider the issue of energy consumption especially in the devices which are battery powered.

C. Processing Time

As mentioned above the encryption and hashing process is very much computation intensive which does not only consume much power but also takes more time to process. Time or speed of the system is also constrained in designing an IoT or embedded system. Different systems will be having different computational capabilities and some of the devices may not be able to run the encryption algorithm in the required speed, which makes the system working not as smooth as expected.

D. Storage

Main advantage of blockchain technology is that it doesn't need a central server to store the device ID's and transactions conducted. It is made possible by having distributed ledgers, ie, each device or nodes need to have its own copy of the ledger. Though initially, the ledger size would be small, the ledger starts to grow when more devices are included in the network. In some situations, the size of ledger passes the storage provided in the IoT devices, which have only very low storage. Adding extra storage will incur a high cost to the device. As the size of block grows, there may be the need for a central server to store it, which doesn't serve the complete purpose of the blockchain.

E. Legal Compliance Issues

One of the main aims of blockchain technology is to provide trust without a central authority to control or regulate the system. Though it seems like a brilliant idea it presents a system without any legal or compliance code to follow. The main issue is the many lack clear monetary policies and regulations about crypto currencies, though some countries are making a genuine effort on this issue. The more serious issue in the realm of IoT is about the legal uncertainty in privacy, data access, and ownership. It causes many problems to the service providers and manufacturers and scares off many clients in taking up the new technology.

F. Others

Beyond the above mentioned there exists some other challenges or issues in implementing the system. To make the system work in industries like supply chain and logistics, there must be a mutual agreement among a large number of players in the ecosystem. The personnel who are expert in blockchain technology is only a few and who is also well versed in IoT is fewer which make the development of the technology very slow. There may be many hidden challenges and risks involved in the system which cannot be seen at the time of development, but made only visible when deployed to work in realworld conditions. Ability to interconnect multiple networks (interoperability) is also an issue when multiple chains especially private and public blockchains have to be integrated. So there hurdles have to be overcome to make the new technology a reality. As technology is evolving, one can assume that the above said challenges can be overcome in due time.

VII. CONCLUSION

IEEE has initiated a committee with an intention to develop definitions and protocols for implementing blockchain within IoT framework in June 2018. The framework needs to address the scalability, security and privacy challenges. The framework must also include permissioned and permissionless IoT blockchain and also blockchain tokens, smart contracts etc. Developing a standard will promote common understanding and interoperability between blockchain platforms. [21]

Though we cannot say always that a blockchain is the best solution for issues in IoT, there are many cases where it can be applied. When an IoT application demand decentralization or in cases where communication among peers at node level is required like cases in intelligent swarms, blockchain is an optimum solution. When the data from IoT network is collected and stored sequentially, blockchain assures the data is secure and not altered and allows traceability. Blockchain can also be used where some economic transactions must be done without needing a trust bank or middleman. The Blockchain-IoT combination is powerful enough to transform many industries and when combined with artificial intelligence and big data the impact is going to be larger.

Modifications are also needed for proper blockchain-IoT convergence. The proof of work consensus needs high computing power which needs to be changed to other consensus mechanisms. Each consensus mechanism has its own pros and cons, so which to choose depends on individual use cases. The requirement of Public Key Infrastructure (PKI) must be overcome by using hash-based signatures or Merkle-tree schemes. The size of the ledger is large to be saved in a memory constrained IoT devices which necessitate a pruned and compressed ledger, where only device-relevant transaction and data must be saved. Blockchain allows ad-hoc networking, but may not be needed in many use cases. In those situations, anonymous network joining and leaving can be avoided by incorporating group signatures using a pre-shared key. [22] New architectures enabling Blockchain-IoT convergences have to be developed which will be done in near future.

REFERENCES

1. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, 2013, pp. 1645-1660.
2. M. A. Khan, and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, 2018, pp. 395-411.
3. N. Kshetri, "Can blockchain strengthen the internet of things," *IT professional*, vol. 19, no. 4, 2017, pp. 68-72.
4. M. Banerjee, J. Lee, and K. K. R. Choo, "A blockchain future to Internet of Things security: A position paper, Digital Communications and Networks," 2017. Available: *http://www. sciencedirect. com/science/article/pii*.
5. T. M. Fernández-Caramés, and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access*, vol. 6, 2018, pp. 32979-33001.
6. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronics Cash System, 2008. Available: https://bitcoin.org/bitcoin.pdf.
7. D. Yaga, P. Mell, N. Roby, and K. Scarfone. "Blockchain technology overview. NIST Internal or Interagency Report (NISTIR)," *National Institute of Standards and Technology*, 2018. Available: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.
8. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," In *IEEE International Congress on Big Data (BigData Congress)*, 2017, pp. 557-564.
9. F. Tschorsch, and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, 2016, pp. 2084-2123.
10. K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," In *proceedings of the 50th Hawaii international conference on system sciences*, 2017, pp. 4182-4191.
11. M. Pilkington, "Can Blockchain Improve Healthcare Management? Consumer Medical Electronics and the IoMT," 2017. Available: .
12. T. Lundqvist, A. De Blanche, and H. Robert, "Thing-to-thing electricity micro payments using blockchain technology," In *2017 Global Internet of Things Summit (GIoTS)*, 2017, pp. 1-6.
13. "IBM Blockchain Platform: Technical Overview". *IBM White Paper*, 2018. Available: https://www.ibm.com/downloads/cas/Q9DGBLV7.
14. "Filament v3.0: Thing Nirvana," *Filament White Paper*, 2018. Available: https://filament.com/wp-content/uploads/2018/12/Filament-v3.0-White-Paper.pdf.
15. Diamonds Everledger Homepage. Available: https://diamonds.everledger.io/.
16. Healthbank Homepage. Available: https://www.healthbank.coop/.
17. Slock Homepage. Available https://slock.it.
18. "IoT Chain: A high security lite IoT OS," *IoT Chain Whitepaper*, 2018. Available: https://iotchain.io/whitepaper/ITCWHITEPAPER.pdf.
19. A. Banafa, "IoT and blockchain convergence: Benefits and challenges," *IEEE Internet of Things*, 2017. Available: https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html.
20. H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. Wills, "Blockchain with internet of things: Benefits, challenges, and future directions," *International Journal of Intelligent Systems and Applications*, vol.10, no. 6, 2018, pp. 40-48.
21. "P2418: IEEE Standard for the framework of Blockchain use in Internet of Things (IoT)," 2017. Available: https://standards.ieee.org/project/2418_1.html.
22. A. Stavrou, "Leveraging Blockchian-based protocols in IoT system," 2017. Available: https://blockchain.ieee.org/images/files/pdf/201710-iot-blockchain_-_a-stavrou.pdf.

AUTHORS PROFILE

David Nettikadan: Received the B.Tech. degree in Electronics and Communication Engineering from Govt. Engineering College, Thrissur, under University of Calicut, Kerala, India, in 2002 and M.Tech degree in Embedded Systems from Sahrdaya College of Engineering and Technogy, Kodakara, under APJ Abdul Kalam Technological University, Kerala, India in 2018. After doing internship in the Inter-disciplinary Programme in Educational Technology at IIT Bombay, he pursued his passion in the career in teaching. At present he is working as Assistant Professor in Department of Electronics and Communication Engineering. He is an active member of IEEE and IEDC. He is interested in Embedded System Design, Internet of Things, Blockchain, Artificial Intelligence and Machine Learning. He has published 3 papers in International Conferences and Journals.

Riya T Raphael: Received B-Tech degree in Biomedical engineering under Calicut University in 2017 and currently pursuing Master's in Embedded systems under APJ Abdul Kalam Technological university from Sahrdaya College of Engineering and Technology, Thrissur, India. She is interested in Embedded system design, Biomedical instrumentation and Artificial implants design. She have presented paper in IEEE conference held at SCAD institute, Tirupur and received the best paper award.

Blessy Daise Paul: Received B-Tech degree in Electronics and communication engineering from Calicut University in 2017 and pursuing M.Tech in embedded systems under APJ Abdul Kalam Technological University from Sahrdaya College of Engineering and Technology, Thrissur, India in 2019. She is interested in Digital communication electromagnetic and embedded systems. Her current research is concentrated in the field of image processing of medical images.