CHAPTER 11

Blockchain-based secured payment in IoE

S.B. Gopal[1], C. Poongodi[2] and D. Nanthiya[3]
[1]Department of Electronics and Communication Engineering, Kongu Engineering College, Perundurai, Tamil Nadu, India
[2]Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Thiruchengode, Tamil Nadu, India
[3]Department of Computer Technology-UG, Kongu Engineering College, Perundurai, Tamil Nadu, India

11.1 Introduction

Internet of things (IoT) includes the IoE as a subset. The IoT is built on the foundation of network intelligence, which is referred to as IoE. The Internet of Everything's (IoE's) spurpose is to transform data into actions, allowing for data-driven decision-making and introducing new capabilities and experiences. Machines to machines, machines to people, and technology-assisted people to people are all connected via the IoT. IoE is more complicated than IoT since it encompasses the IoD (Internet of Digital), IoH (Internet of Human), and IoT.

The Internet of things (IoT) is a collection of networked physical devices and things that collect and exchange data across wireless networks. The IoT is made up of two parts: the "Internet," which acts as the connection's backbone, and the "Things," which refers to real things and equipment. It connects the internet's power, data processing and analytics, and decision-making to physical items in the real world [1]. The IoT aims to build a network of linked objects and physical devices. Alternatively, you may create an ecosystem in which everything is interconnected. The IoT allows machines to communicate with one another. IoT is less advanced than IoE since it is considered a component of the wider IoE ecosystem. Wearable health monitoring, linked appliances, self-driving farming equipment, energy management systems that are more efficient, and smart surveillance are just a few examples. Bitcoin is one of the most well-known instances of Blockchain in operation [2]. This is a cryptocurrency (a type of digital cash). Bitcoin Atom (BCA) is a fork of Bitcoin

Smart Energy and Electric Power Systems
DOI: https://doi.org/10.1016/B978-0-323-91664-6.00009-7
© 2023 Elsevier Inc.
All rights reserved.

that offers a genuinely decentralized alternative to trade cryptocurrencies with no trading fees or exchange hacks.

11.2 Blockchain

11.2.1 Working of blockchain

In cryptography, a private key and a public key are used. These keys help in the efficient execution of two-party transactions. These two keys are personal and are used to build a secure digital identification reference for each user. Secure identification is the most important aspect of Blockchain technology. In the bitcoin world, this identity is referred to as a "digital signature," and it is used to authorize and monitor transactions. The peer-to-peer network is paired with the digital signature; the digital signature is used by a large number of individuals acting as authorities to reach an agreement on transactions and other issues.

11.2.2 Decentralization

No one member (user) controls the transaction in a peer-to-peer network, and power is distributed across all network users, suggesting that no single stakeholder has the ability to hack, manipulate, halt, or shut down the chain of blocks [3]. This blockchain network is free of hackers and fraud owing to its distributed (decentralized) nature.

11.2.3 Integrity

All members in a blockchain-powered network have the right to make judgments; faith in the system is not imposed, but is entirely led by human intuition. The way each user is rewarded for their efforts, as well as the way this entire P2P network runs, demonstrates the high level of honesty.

11.2.4 Cryptography: fair to all

The primary premise of blockchain is to offer the user with a high level of security and authenticity [4]. It makes use of cryptography to maintain strict security and data integrity. The blockchain transaction process is advantageous and profitable for a trustworthy user, but it is extremely punitive for irresponsible users. The blockchain system is fair to all users who act well and rewards them accordingly. However, if you use it with the wrong intention, you will be punished.

11.2.5 Security

Because blockchain is a distributed network, there is no single point of failure, and no single person can destroy the entire chain by acting recklessly. Any damage caused by a single password breach will be limited to that single individual [5]. Unless you are a fool and leak your private key, your transaction over the network is extremely safe thanks to the blockchain PKI (public key infrastructure) encryption mechanism, for which no technology has a solution. As a consequence, you can trust Blockchain technology to conduct your transactions in a secure manner.

11.2.6 Inclusive

In its methodology, the blockchain is inclusive, allowing anybody to participate in the global economy without prejudice. Because a bank account is no longer required, Bitcoin allows anybody, rich or poor, to invest in their skills and participate in the global economy. They have the freedom to deal with anyone they choose without the need for a third party, and they can do it for free or for a very low transaction cost. Blockchain, in my opinion, is a link that will liberate and unite all people without discrimination. The major contribution of the blockchain to the world will be to enable everyone to participate in a global economy that is fair, safe, secure, and just to everyone.

11.2.7 Blockchain respects your privacy

Data privacy has grown crucial in a digital age when consumers and businesses trade online for a number of purposes, including purchasing, paying bills, and validating information [6]. Its strong hash key encryption is very secure, letting you to send and receive data over the internet while being anonymous. When you use the blockchain P2P network to conduct business, your identity is never disclosed [7]. As you become a member of the blockchain ecosystem, your rights and freedom become apparent and enforceable. The Smart Contract on the Blockchain is an excellent approach to carry out any agreement between two parties, as it allows transactions to take place only once certain predetermined benchmarks have been satisfied and both parties have consented.

11.2.8 Challenges in block chain

11.2.8.1 Scalability

The blockchain industry's capacity to handle a large number of users at once remains a hurdle. To conduct a single transaction, blockchain

technology uses numerous sophisticated algorithms. The overall number of coinbase users was estimated to be 11.7 million as of October 2017. The typical transaction has grown considerably as more individuals have become accustomed to it. It had a significant impact on transaction processing speed since a larger number of individuals means more computers writing and accessing the network, resulting in a more cumbersome system overall.

11.2.8.2 Hackers and shadow dealing

The lack of governmental control in the blockchain business makes it a volatile environment and an easy target for market manipulation. For example, the famed one coin hoax, in which many investors lost money believing it to be the next breakthrough digital currency, turned out to be a Ponzi scheme. No matter how knowledgeable you are about cryptocurrencies, there is always the risk that your online wallet will be hacked or blacklisted by the authorities owing to unethical behavior.

11.2.8.3 Complex to understand and adopt

The complexity of blockchain technology makes it difficult for a layperson to comprehend and understand its benefits. Before going into this ground-breaking program, one must first read it and grasp the concepts of encryption and distributed ledger [8]. Another factor that makes blockchain difficult to implement is that, in comparison to the expenses associated with blockchain, financial institutions are capable of providing secure payment gateways and other services at reasonable pricing.

11.2.8.4 Privacy

Blockchain is an open ledger that can be viewed by anybody. In many circumstances, it is necessary, but when employed in a delicate context, it becomes a hazard [9]. Blockchain technology still has a long way to go before it is widely embraced. The ledger has to be redesigned in such a manner that it can only be accessed by those who are permitted to see it.

11.2.8.5 Costs

Blockchain is typically used to eliminate costs associated with third parties and intermediaries involved in the value transfer process. Despite its numerous benefits, blockchain technology is still in its early stages of development, making it challenging to integrate into current systems.

It changes into an expensive affair in general, preventing it from being adopted by both the government and commercial businesses.

11.2.8.6 Blockchain is still a distant dream

The blockchain technology, its benefits, and how it is reshaping the architecture of emergent technologies like InsurTech and others have market commentators enthralled. However, these obstacles are still difficult to overcome, and it will take some time before blockchain becomes an intrinsic component of all businesses.

11.2.9 Application of block chain

11.2.9.1 Money transfers

The initial notion behind blockchain technology's creation is still a fantastic use. Traditional methods of money transfer may be more expensive and time consuming than using the blockchain. This is particularly true in the case of cross-border transactions, which are notoriously delayed and costly [10]. Money transfers between accounts can take days in the existing US banking system, but it takes minute to complete the transaction.

11.2.9.2 Financial exchanges

Over the last several years, a slew of firms have sprung up to provide decentralized bitcoin exchanges. When it comes to exchanges, blockchain enables for speedier and less expensive transactions. Furthermore, because a decentralized exchange does not force investors to deposit their funds with a centralized authority, they have more control and security. While bitcoin is the primary focus of blockchain-based exchanges, the concept might be extended to other traditional assets as well.

11.2.9.3 Insurance

Customers and insurance providers can benefit from more transparency by using smart contracts on a blockchain. Customers would be prevented from filing repeated claims for the same occurrence if all claims were recorded on a blockchain. Furthermore, the use of smart contracts can expedite the payment procedure for claimants.

11.2.9.4 Real estate

To verify financial facts and ownership, as well as transfer deeds and titles to new owners, real estate transactions need a large amount of documentation. Real estate deals are being recorded using blockchain technology

can improve the security and accessibility of ownership verification and transfer. This can help you save time and money by speeding up transactions and reducing paperwork.

11.2.9.5 Data storage

When blockchain technology is used in conjunction with a data storage system, it may improve security and integrity. Because data is maintained decentralized, Hacking into and wiping out all of the data on the network will be more difficult, whereas a centralized data storage provider may only have a few points of redundancy. It also suggests that data is more available because access is not restricted to the actions of a single organization. In certain circumstances, storing data on blockchain might be as less expensive as other types of storing data.

11.2.9.6 Gambling

Blockchain might be used by the gaming industry to benefit gamers in a variety of ways. The transparency that operating a casino on the blockchain delivers to potential players is one of the main advantages. Bettors can see that the games are fair and that the casino pays out because every transaction is recorded on the blockchain. Furthermore, using blockchain eliminates the need for personal information such as a bank account, which may deter some would-be gamblers. Because users may wager anonymously and the decentralized network is not subject to government closure, it provides a workaround for regulatory constraints.

11.3 Internet of everything (IoE)

IoE proposes a scenario in which billions of items are connected via public or private networks utilizing standard and proprietary protocols to detect, measure, and analyze their state as shown in Fig. 11.1.

Need for IoE

11.3.1 Benefits of the Internet of things

- More information improves overall conclusions.
- The ability to keep track of and monitor events
- Automate your tasks to reduce your workload.
- Saves money and resources, resulting in increased efficiency.
- Better quality of life

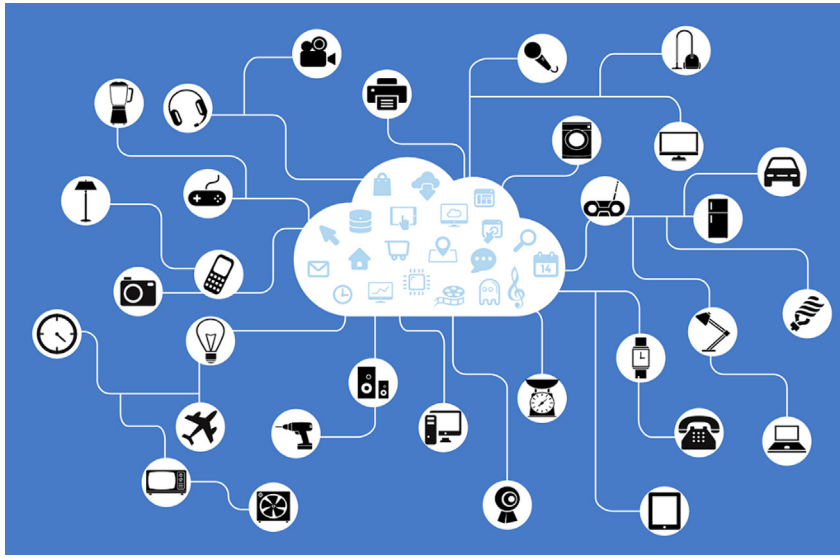


Figure 11.1 Internet of everything.

11.3.2 Challenges in privacy and security

IoE is a system with several domains. IoE is made up of a large number of connected devices and services that share data. Every domain has its own set of norms for security, privacy, and trust [11].

The following are some of the current problems in IoE securities: privacy of user and protection of individual data in

- Authentication and administration of identities
- Integrating policies and managing trust
- Access control and authorization
- Point-to-point security
- Security solution that is resistant to attacks

11.3.3 Communication between Machine to Machine

Machine to Machine (M2M) is a communication technology that allows wireless and wired equipment to connect with one another. In industrial automation, M2M connections are commonly utilized for machine monitoring and instrumentation. The "Internet of verything" (IoE) is a collection of people, processes, data, and objects that collaborate to improve the utility and relevance of networked interactions. IoE encompasses both M2M and IoT technologies, and its pervasiveness allows it to be utilized

to achieve a wide range of goals for a wide range of people, including first responders as shown in Fig. 11.2.

IoE has taken the role of the IoT. Nowadays, security in an IoE network is critical. The key hurdles in IoE are security and privacy concerns. The numerous IoE security standards are beneficial in automating systems in various areas such as home automation, smart cities, smart agriculture, and so on.

11.3.4 Application

11.3.4.1 Smart city

To collect and analyze data, smart cities rely on IoE devices such connected sensors, lights, and meters. Cities then utilize the information to enhance their infrastructure, public utilities, and other areas of their operations [12]. The Internet of Things (IoE) solutions available in the smart city sector serve to handle a variety of city-related issues, such as traffic congestion, air and noise pollution reduction, and city safety.

11.3.4.2 Smart grids

The smart grid is part of an IoT architecture that may be used to monitor and control everything from lighting to traffic signals, traffic congestion, parking spots, road alerts, and early detection of things like earthquake-induced power surges [13]. The smart grid distributes transmission lines, smart meters, distribution automation, substations, transformers, sensors, software, and more to companies and families around the city [14].

11.3.4.3 Health

In the healthcare industry, the most recent IoE trends are being used. IoE software supports patients in decreasing health-related dangers and hospital

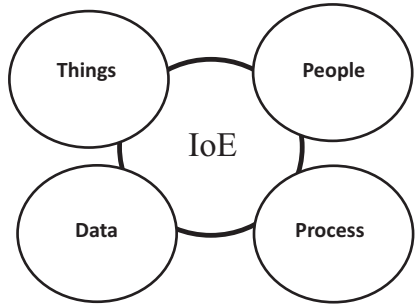


Figure 11.2 IoT with M2M. *IoT*, Internet of things; *M2M*, Machine to Machine.

expenses by gathering patient information and analyzing data using cloud services to exchange data sources.

11.3.4.4 Retail

Retail enterprises may now evolve into smart shops that collect data on consumers' preferences, requirements, and behaviors in real time thanks to the IoT. This allows merchants to understand client behavior and deliver the items and services they desire.

11.3.4.5 Smart supply chain

For a number of years, supply networks have been growing smarter [15]. Tracking things while they are on the road or in transit is one of the most popular services, as is supporting suppliers with inventory information exchange. Factory equipment with embedded sensors may send data about many factors, such as pressure, temperature, and machine usage, using an IoE enabled system [16]. The IoE system may also enhance performance by processing operations and changing equipment settings.

11.3.4.6 Smart farming

The IoE can monitor a vast number of farming activities and also lot of livestock that farmers goes through it, all of them which can transform the way farmers operate day to day.

11.4 Secure payments in IoE

11.4.1 IoE with blockchain: security challenges

Despite the fact that blockchain technology greatly improves the dependability and concerns are always developing [17]. This article examines the security flaws that have arisen as a result of the confluence of blockchain and IoT, as well as possible remedies [18].

The following security problems in implementing dispersed IoT are highlighted in this article: (1) Network security as well as communication; (2) identity management and verification; (3) dispersed consensus protocol with good dependence; (4) distributed cooperation and establishment of trust; (5) transferring data privacy and security (P2P) mode which is peer to peer method, which allows nodes to interact with each other autonomously without the use of a central server platform, is used heavily in the architecture of IoT. One of the important technologies for resolving the aforesaid security issue is cryptographic algorithms. In the IoT, (PKIs)

make identity association and verification easier as shown in Fig. 11.3. At the moment, the most widely used PKIs are (CAs) and web of trust based on somewhat excellent privacy.

11.4.2 A secures energy transaction prototype

The communication related infrastructure, 5G components are discussed in this project as shown in Fig. 11.4. Here 5G-V2X network model for the EVBlocks trading scheme is shown. We analyze mm Wave channel-based communication in the 5G-V2X ecosystem, which works in the thirty to three hundred GHz range. Nodes N1 and N2 connect with

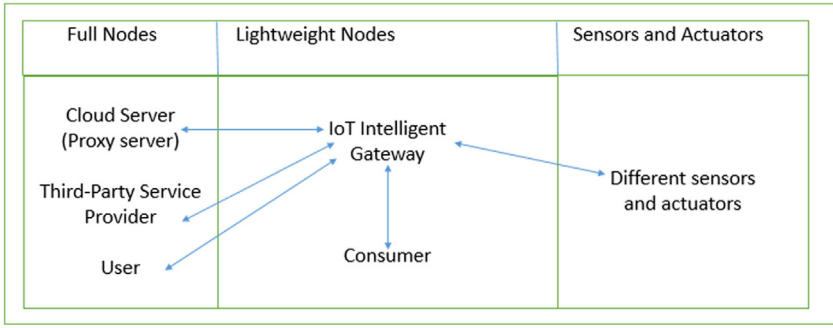


Figure 11.3 IoE with blockchain.

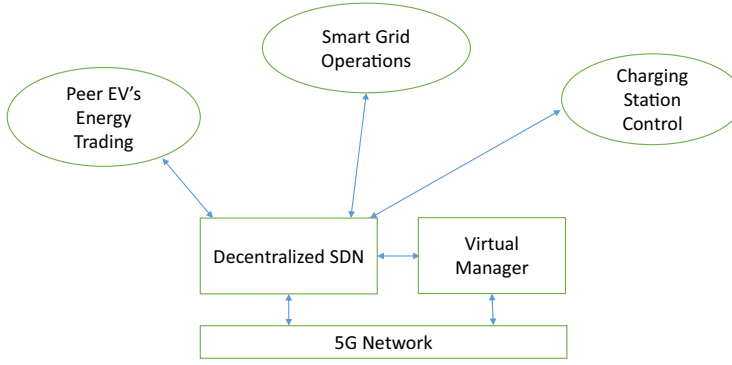


Figure 11.4 Secured energy transaction.

each other using transmitting and receiving antennas in C-V2X. The SDN-leveraged CBC resource-trading model and the accompanying problem formulation are seperated. Layer from 1, 2 and 3 are the layers of the resource-trading model [19]. EVs communicate with CS situated GS with the necessary frequency range for energy exchange. Micro-grids of small in size, known as location aggregators (LAGs), are located within each GS to help with load-balancing.

11.4.3 Internet of entities (IoE): a blockchain-based distributed paradigm to security

It is an effective workflow for the localization of people and things that takes advantage of the vast number of existing wireless-based devices to overcome the limitations while maintaining user privacy.

A tracker device is used for detection, a distributed ledger is used for recording the collected data [20] as shown in Fig. 11.5. With a focus on the characteristics of current wireless technologies capable of performing these activities. It formalises the structures of the data and procedures involved in software is capable of combining information connected to the participating entity and devices used for tracking, resulting in a structure of data that represents the statistics to be stored on the distributed ledger. Localization of elements: it thoroughly outlines the work carried out, introducing certain methodologies and a set of rules for localization targeted at directly or indirectly exploiting the information accessible on the blockchain (Fig. 11.6).

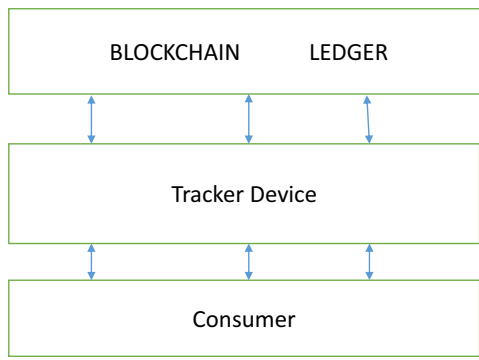


Figure 11.5 Blockchain-based distributed paradigm.

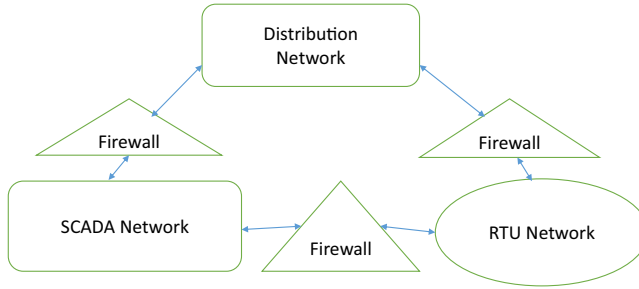


Figure 11.6 Secured blockchain prototype.

11.4.4 A secured blockchain prototype

The smart RTUs of SCADA are used to gather, transmit, and receive customized signal data between the communication and physical layers. The RTU-nodes are used to connect the communication paths. Only authorized individuals with communication access can confirm data collecting and processing for reports or signaling of various processes used in the production environment as shown in Fig. 11.6. The proposed decentralized data security solution relies heavily on advanced metering infrastructure (AMI).

11.4.5 Role of software in securing Internet of things/IoE

The purpose of this article is to analyze the current importance of security needs in modern cultures.

The above mentioned methods were used to collect primary and secondary data: (1) obtaining a large amount of unidentified practical data about software security vulnerabilities from a cyber intelligence company that works in a many countries; (2) conducting interviews that are informal with two well-known cyber intelligence workers [21] as shown in Fig. 11.7.

11.4.6 Role of IoE/Internet of things in vehicular networks

This research will aid researchers in gaining a thorough understanding of the taxonomy of automotive network security challenges, which can then be used to develop novel solutions. This knowledge will also aid in the development of new research avenues, which will aid in the design of new tactics for dealing with attacks more effectively.

Cars and electric vehicle charging grids are all part of VANETs [3,5,22]. In VANETs, there are two types of communication: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), as well as infrastructure-to-vehicle

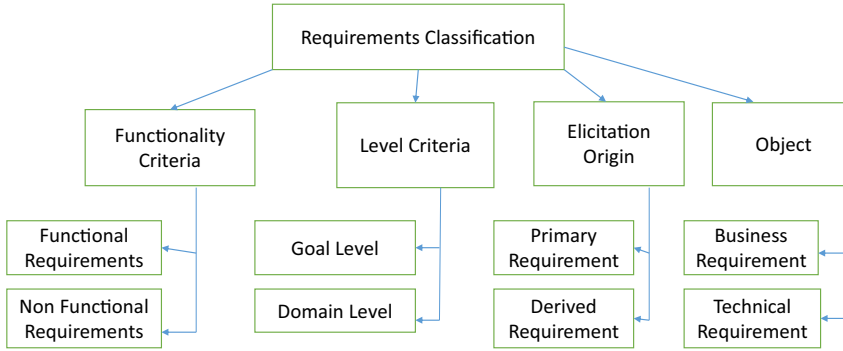


Figure 11.7 Secured blockchain prototype.

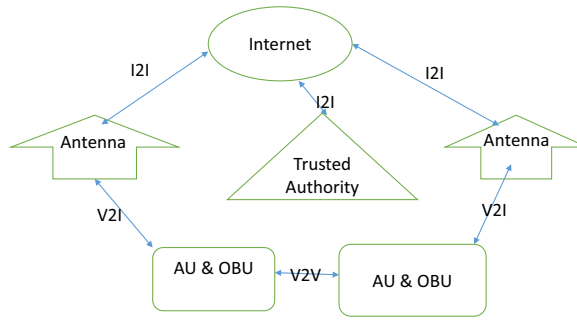


Figure 11.8 IoT in vehicular networks. *IoT*, Internet of things.

(IV) (I2V). Communication between roadside units and base stations is known as infrastructure-to-infrastructure (I2I) as shown in Fig. 11.8. As a backbone, they rely on the internet.

11.4.7 IoE with privacy

Rootstock (RSK), Sidechain Overlay Block Manager (OBM), and 2 Way Peg are the names of our proposed IoE architecture (WP). OBM is a company that manages an integrated blockchain that operates on one or more sidechains and is in charge of generating, verifying, and storing individual transactions. A two-way peg (2WP) protocol is one that allows a bitcoin to be transferred from one blockchain to another inside a third-party trust as shown in Fig. 11.9.

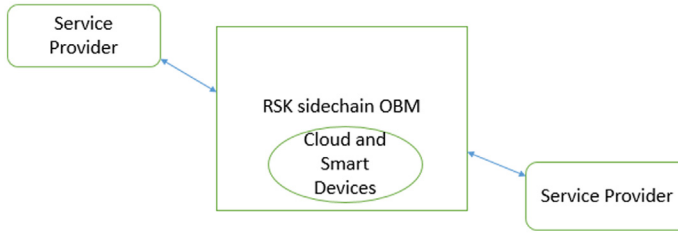


Figure 11.9 IoE with privacy.

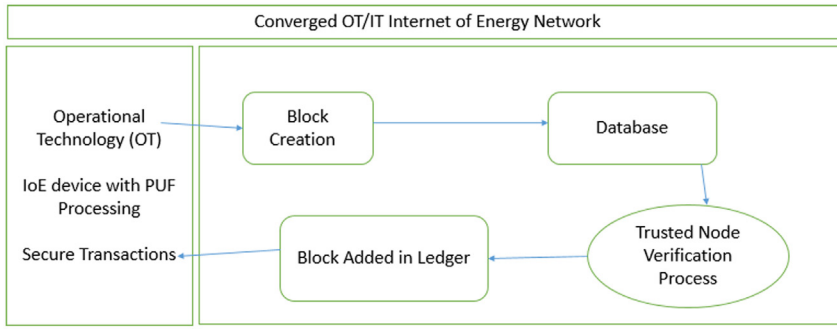


Figure 11.10 PUF enabled secured blockchain. *PUF*, Physical unclonable function.

OBM is a company that manages an integrated blockchain that runs on one or more sidechains and is in charge of generating, verifying, and storing individual transactions. A 2WP protocol is one that allows a bitcoin to be transferred from one blockchain to another inside a third-party trust. We wish to analyze existing 2WP approaches like Federation, Sidechain, and Drivechain, as well as hybrid ways, to determine which is best suited for the RSK platform's 2WP at each level of adoption. Rootstock was developed and tested to give two methods for constructing and confirming SPV proofs. The Rootstock 2WP smart contract creates two separate indicators to lock and unlock cryptocurrencies like bitcoin.

11.4.8 Physical unclonable function enabled secured blockchain

This paper provides a thorough examination of the technological features of blockchain and physical unclonable functions (PUFs). It defines a developing blockchain idea that uses PUFs to incorporate security in hardware primitives to address bandwidth, integration, scalability, latency, and energy needs for Internet-of-Energy (IoE) devices as shown in Fig. 11.10.

Blockchain, which is based on Proof-of-PUF verification, data stored which is encrypted with same PUF-derived keys and attributes, providing immutable assurance that data have not been changed with, as well as traceability and simple auditing capabilities. The shuffling of the PUF technology, as mentioned in the preceding sections, is crucial to the PUF Chain's defence. The amount of 0 and 1 s should be the same for PUF answers to be highly consistent and impervious to the cyber assaults.

References

[1] M. Moness, A.M. Moustafa, A survey of cyber-physical advances and challenges of wind energy conversion systems: prospects for internet of energy, IEEE Internet of Things Journal 3 (2016) 134–145.

[2] A. Verma, et al., The security perspectives of vehicular networks: a taxonomical analysis of attacks and solutions, Applied Sciences 11 (10) (2021) 4682.

[3] N.Z. Aitzhan, D. Svetinovic, Security and privacy in decentralized energy trading through multisignatures, blockchain and anonymous messaging streams, IEEE Transactions on Dependable and Secure Computing 15 (5) (2018) 840–885.

[4] M.T. Hammi, et al., Bubbles of trust: a decentralized blockchain-based authentication system for IoT, Computers & Security 78 (2018) 126–142.

[5] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Computer Networks 57 (10) (2013) 2266–2279.

[6] Z. Liu, et al., On emerging family of elliptic curves to secure internet of things: ECC comes of age, IEEE Transactions on Dependable and Secure Computing 14 (3) (2017) 237–248.

[7] A. Satsiou, L. Tassiulas, Reputation-based resource allocation in P2P systems of rational users, IEEE Transactions on Parallel and Distributed Systems 21 (4) (2010) 466–479.

[8] A. Kiayias et al., Ouroboros: A provably secure proof-of-stake blockchain protocol, in Proc. Annu. Int. Cryptol. Conf., 2017, pp. 357–388.

[9] Z. Lu, et al., A privacy-preserving trust model based on blockchain for VANETs, IEEE Access. 6 (2018) 45655–45664.

[10] Y. Zhang, R.H. Deng, X. Liu, D. Zheng, Blockchain based efficient and robust fair payment for outsourcing services in cloud computing, Information Sciences 462 (2018) 262–277.

[11] S.B. Gopal, C. Poongudi, D. Nanthiya, A. Jeevanantham, D. Sumithra, P. Tharani, et al., Secured smart home using blockchain technology, Gedrag & Organisatie Review (2020)ISSN:0921-5077.

[12] X. Fang, S. Misra, G. Xue, D. Yang, Smart grid—the new and improved power grid: a survey, IEEE Communications Surveys & Tutorials 14 (4) (2012) 944–980.

[13] N. Bui, A.P. Castellani, P. Casari, M. Zorzi, The internet of energy: a web-enabled smart grid system, IEEE Network 26 (2012) 39–45.

[14] V.C. Gungor, B. Lu, G.P. Hancke, Opportunities and challenges of wireless sensor networks in smart grid, IEEE Transactions on Industrial Electronics 57 (10) (2010) 3557–3564.

[15] Y. Yan, Y. Qian, H. Sharif, D. Tipper, A survey on smart grid communication infrastructures: Motivations, requirements and challenges, IEEE Communications Surveys & Tutorials 15 (1) (2014) 5–20 (2013).

[16] F. Mwasilu, J.J. Justo, E.-K. Kim, T.D. Do, J.-W. Jung, Electric vehicles and smart grid interaction: a review on vehicle to grid and renewable energy sources integration, Renewable & Sustainable Energy Reviews 34 (2014) (2014) 501–516.
[17] L. Wei, J. Wu, C. Long, Y.B. Lin, The convergence of ioe and blockchain: security challenges, IT Professional 21 (5) (2019) 26–32.
[18] S.B. Gopal, D. Nanthiya, P. Keerthika, S.B. Kayalvizhi, T. Raja, R. Snega Priya, SVM Based DDoS Attack Detection in IoT Using Iot-23 Botnet Dataset, Innovations in Power and Advanced Computing Technologies (I-PACT) (2021) 1–7.
[19] P. Bhattacharya, S. Tanwar, U. Bodkhe, A. Kumar, N. Kumar, EVBlocks: a blockchain-based secure energy trading scheme for electric vehicles underlying 5G-V2X ecosystems, Wireless Personal Communications (2021) 1–41.
[20] R. Saia, S. Carta, D.R. Recupero, G. Fenu, Internet of entities (IoE): a blockchain-based distributed paradigm for data exchange between wireless-based devices, SENSORNETS (2019) 77–84.
[21] F.F.S. Flores, S.R. de Lemos Meira, Ethical software engineering: a critical review about software engineering in face of security requirements in the IoT/IoE society, in: 2021 IEEE International Systems Conference (SysCon), 2021.
[22] M. Suarez-Albela, et al., A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications, Sensors 17 (9) (2017). 2017, Art. 1978.