Chapter 14
Nullifying the Prevalent Threats in IoT Based Applications and Smart Cities Using Blockchain Technology

Lokesh Yadav, Milan Mitra, Akash Kumar, Bharat Bhushan, and Mustafa A. Al-Asadi

Introduction

The revolutionary population expansion in urban areas has been witnessed in the past few decades. Only 45% of the population is living in rural areas which will further reduce to 30% in the next 3 decades and 25% of the population would shift to urban cities (Department of Economic and Social Affairs 2014). This eruptive population growth would make it impossible for current methods to deal with economic, social, educational and other sorts of problems. To cope up with these inescapable problems, officials and chairpersons are moreover interested in implementing the smart cum sustainable methods to tackle both tangible and intangible (various sources of capital) assets (Bibri and Krogstie 2017). Thus, the idea of a smart city comes into play. A Smart city is a combination of various systems designed to deal with problems mentioned above by evolving and adapting to the changes and needs of the environment and other sorts of commodities with the help of data analysis thus reducing human involvement. Decentralization, transparency, privacy, security, and this interconnection are the main features of blockchain which could be tools to manage, develop, maintain and run smart cities. The elimination of mediators i.e. decentralization is the main objective of achieving sustainability (Makrushin and Dashchenko 2016).

While considering the security aspect, the major enhancement in IoT and wireless transmission has made it simple and easy for a range of devices to get interconnected

L. Yadav (✉) · M. Mitra · A. Kumar · B. Bhushan
School of Engineering and Technology, Sharda University, Greater Noida, India
e-mail: lokeshyadav4703@gmail.com

B. Bhushan
e-mail: bharat.bhushan@sharda.ac.in

M. A. Al-Asadi
Department of Computer Engineering, Selçuk University, Konyo, Turkey
e-mail: masadi@lisansustu.selcuk.edu.tr

D. K. Sharma et al. (eds.), *Low Power Architectures for IoT Applications*, Springer Tracts in Electrical and Electronics Engineering, https://doi.org/10.1007/978-981-99-0639-0_14

and even share data from distinct locations. However, the data which is open may contain sensitive information like financial, personal and other private information thus increasing the chances of security attacks and hence they must be able to repel these deadly attacks. As shown by Kaspersky Labs, smart terminals like self-service machines, bicycle rental terminals and information kiosks have many security gaps (Bhushan et al. 2020). Cybercriminals could target these devices and can further get access to the private and financial information of any user. It is important to note that the old security mechanism has failed to make the city's critical infrastructure smart. Thus, alternative and new solutions should be developed which provide data privacy, confidentiality and integrity which is based on the data type i.e. public or private. This article conceptualizes a security framework based on blockchain which would let the communication between entities of smart city to communicate without compromising the cost of privacy and security.

Due to variegated types of resources constrained in devices smart cities are vulnerable to many data security attacks. Therefore, identification of these kinds of important threats and their further leading consequences need to be identified to design a relevant solution. Numerous studies and research have been carried out in this area like Computer Emergency Response Teams (CERT) which provides graphical information about potential risks, Open Web Application Security Project (OWASP) mobilize common security attacks, G-Cloud which shows a collection of Cloud Computer Service Provider (CCSP) needs (OWASP Foundation 2013; Goyal et al. 2021; HMGovernment 2011). Major threats to smart cities are as follows- Integrity threats-this includes manipulation and alteration of critical data and information through unauthorized means. Authenticity threats—Access of resources and critical information by unauthorized means. Availability threats—Upholding of resources by unauthorized means. Accountability threats—Refusal of acceptance or transmission of messages by co-related entities. Confidentiality threats—Disclosure of critical information by unauthorized access (Biswas and Muthukkumarasamy 2016). The main contributions of this work are enumerated below.

- This paper presents the dimensions of smart cities, security framework and major cyberattacks launched in the realm of smart cities.
- This paper explores the working of blockchain, its type, its consensus protocols and motivation for its widespread deployment in smart cities.
- This paper presents the major recent advancements dedicated towards blockchain enabled secure smart cities.
- This paper also presents future advancements in securing smart cities with or without blockchain.

The remainder of this article is organized as follows: Sect. 14.2 presents an overview of the smart city dimension of smart cities, the security of the frameworks and layers involved in it. Section 14.3 highlights major cyberattacks on smart cities. Section 14.4 elaborates on the workings of blockchain, its types, its consensus protocols, and the motivation for its widespread deployment in smart cities. Section 14.5 highlights the recent advances in securing smart cities with blockchain. Finally, the

paper concludes itself in Sect. 14.6, highlighting the major open research directions and future discussion.

Overview of Smart City

Smart city includes various reliable frameworks and designs with the top most priority of user convenience according to primary needs compromising security, privacy, all shorts of solution to Urban problems along with secure transactions and other data monitoring features. The main reason for bringing up the smart city concept is to provide the most reliable and quality efficient development of infrastructure with the utilization of fore technologies like IoT and Machine Learning (ML) with Artificial Intelligence in order to develop a user-friendly ecosystem that provides interaction and deployment of digital services and devices interaction to uplift the quality of living of peoples. This integration provides a secure network that does not compromise security; moreover, as we further proceed with automation, the above-mentioned components should hold cyber security as one of the primary components (Alnahari and Ariaratnam 2022).

Smart Cities Dimensions

The four major pillars involved in the planning of smart cities are economic, social, physical, and institutional infrastructures. The main motive for the dimensions of smart cities is to support the above-mentioned pillars (Silva et al. 2018).

Smart Economy

Apostol et al. (2020) researched about smart economy projects and talked about strategies and suggestions that motivates creative vision along with scientific research, leading-edge technology, and the idea of sustainable development with regard to the environment. Zahi et al. (2016) described a smart economy as creative, full of statistics figures and data with the determination of competition and transmission technologies about the economy and its resources. Kumar (Bhushan and Sahoo 2017) studied smart economies and addressed the understanding of economies based on research in all factors, including heritage, industry, business, development, construction planning, and science. The smart economy has various forms in smart cities, along with different features, challenges, and remedies.

Smart Governance

Silva et al. (2018) explored the different dimensions of smart cities and their challenges and further showed that the governance of smart cities collaborated with offerings to various services, including public and social services, managing decisions along with governance with full transparency. The author defines governance as cooperation between institutions of administration and citizens. Also, maximum gain in the aspects of greater dependability, planning, and productiveness of services could be achieved with governance by a combination of public, and civil governing systems. Addressing governance with technology is critical because it makes sure to represent every service of the city via high-tech solutions. On the basis of a study on smart city features, he classifies different methods for expanding smart cities' creative potential (Silva et al. 2018). Nilssen focuses mostly on collective governance to upgrade creative transformation (Nilssen 2019). Collective governance can be achieved directly through e-governance. E-governance can be intensified by artificial intelligence (AI) and 5G technology. Collaborative governance with the help of information based on cloud services aids in the contribution, involvement, and splitting of information (Ismagilova et al. 2019).

Smart Living

The important components for smart living observed by the OECD which is a Better-Life Initiative framework called are the evolution and maintenance of natural, profitable, human capitals. Medical management can be achieved completely by actual time tracking of the requirements of care, and urgent sustenance activated by the ICT (Ismagilova et al. 2019; Mehta et al. 2022; Nižetić et al. 2020). Another important factor for smart living is the upshot of the smart economy. ICT is considered as a helping guide in smart living via automatic connectivity network-enabled living space processing, and merging security systems (Ande et al. 2020; Bhowmik et al. 2022). Author states that smart homes consist of applications that are linked to smart assistance and these applications grab individual information about their users even then no harm is done to any security system or privacy. Elahi et al. (2019) did research on the lucidity of products available in smart cities and labeled that provisions for smart applications along with setting standards are important to discover the probability of risks connected with these products.

Smart Mobility

Smart mobility centralizes majorly on the foundation of infrastructure and transport networks. The author discusses common issues such as overcrowding, long chain queues and hindrances which led to delays (Appio et al. 2019). They put forward the idea that the system should divert attention from the operation of private vehicles and come up with interrelated alternatives for people to relieve their travel schedule.

Actual real-time data on roads and time travelers' analysis is compiled using IoT (Silva et al. 2018). With the help of IoT, there is a linking of information in automobile means of transport and IOV helps in the functioning of traffic safety to reach smart mobility (Ismagilova et al. 2019). The universal operation of IoT and IOV maximizes the effectiveness needed to attain smart mobility. It also came up with a superior transport system (Porru et al. 2020). For the sanction of smart mobility, there is a need to allow technologies like AI, IoT, big data, and blockchain along with their developments and answers (Paiva et al. 2021).

Smart People

The main role in smart cities development is played by two important elements-social capital and human capital. The potentiality and skill of an individual or a mass are defined as Human Capital on the other side Social Capital points towards the caliber and numeral amount of relation linking in between social organizations. There is a high requirement for efficient human and social capital for fruitfulness and creativity in building smart cities. Human capital can only be developed by implementing the role of higher education in schools and universities. To become a wiser and smarter individual, one needs knowledge and understanding, which can only be gained through high educational institutes (Ismagilova et al. 2019). Smart applications such as AI and big data help to lift up the learning and teaching proficiency to upgrade a better grip on knowledge gaining (Radu 2020).

Security Framework

A data security framework is a defined approach to making data processing free from data security risks and data protection threats. Security frameworks in four different layers are discussed below.

Physical Layer

Devices used in the smart city come with sensors and actuators which accumulate and send data further to higher or upper levels. A few of such devices Acer Fitbit and Nest thermostat are more likely to have cyberattacks because of poor encryption and maybe access control structures. And then, there are no standards available for smart devices which can share and integrate data which is generated by the smart devices to bring forth cross functionality (Topal et al. 2020).

Communication Layer

Different types of communication mechanisms are used by smart city networks. For ex-Ethernet, Bluetooth, 4G and 3G to pass information between various systems. This layer must be integrated with blockchain protocols to bring forth the security and privacy of data (Arsh et al. 2021).

Database Layer

One after another, a decentralized database stores records, known as distributed ledger. Unique cryptographic signatures and timestamps are included in each record in the ledger. Any authorized user may verify and audit the ledger's whole transaction history. Distributed ledgers can be either permissionless as well as permissioned. The main advantages of a permissionless ledger are transparency and censorship resistance. However, compared to the private ledger, the public ledger takes a longer time to attain agreement and requires more maintenance of complex records. In addition, anonymous attackers may target public ledgers. Thus, to provide security, scalability, and speed in real-time applications like traffic systems in a smart city, it is advised to use private ledgers (Yu et al. 2018).

Interface Layer

This layer contains several intelligent applications that work together to make effective decisions. For instance, to turn on the air conditioner a few minutes before you arrive home, a smartphone application can deliver location to a smart home system. Although, vulnerabilities and bugs in one application might provide anonymous attackers access to dependent operations. So, the app should be carefully integrated (Hussain et al. 2018).

Attacks in IoT Enabled Smart City Applications

Nowadays, Cyber Attacks in smart cities are very common and exponentially increasing day by day. There are several types of cyberattacks, some of them are listed below in this section.

Data and Identity Theft

Unsecured smart city data facilitates vile behavior with an abundance of targeted sensitive data that can ultimately be used for suspicious transactions. An identity

thief that obtains a victim's credit or debit card or national insurance number may use it to make transactions or create accounts in the victim's name. Financial gain is the main purpose of the attack, a poll also revealed that a big majority of respondents place the greatest importance on their passwords. It may also be performed with an account that almost all people don't mind giving out like email (Burnes et al. 2020).

Distributed Denial-of-Service Attack (DDoS)

DDoS issue addressed in this study is that one or more devices transmit unusually enormous amounts of data in order to overwhelm a network. DDoS assaults are effective because they use several computer servers to attack web traffic. Personal computers that were potentially compromised are made up of networks which allows the attacker to manage them remotely. Once a botnet is created, delivering remote commands to each bot the attacker may conduct the attack (Khalaf et al. 2019).

Permanent Denial of Service (PDoS)

PDoS, also known colloquially as Phlashing, in this necessitating hardware replacement or reinstallation is required as this attack causes significant damage to the device (Bhushan and Sahoo 2017). An attacker bricks a device or damages firmware during such an attack, leaving the device or an entire network inoperable. Because the attacks are permanent, the attackers also couldn't demand a monetary payment to terminate the attack, but this generates problems for the victim.

Device Hijacking

The attacker controls the device or hijacks it by seizing control over everything. Because the attacker does not affect the basic functions of the device, these attacks can be more difficult to detect. Hackers may use browser security holes to induce victims to download their malware, commonly known as hijackware (Flynn et al. 2020). Various cyberattacks rely on some form of kidnapping, as well as other kidnappings such as B. Criminals hijacking planes or hijacking invulnerable transport vehicles.

Man-In-The-Middle (MITM)

In order to eavesdrop or impersonate one of the participants, the perpetrator puts themselves together into a dialogue between a user and a software. MITM is about

the certain data flowing between endpoints and the furtiveness and rectitude of the data itself (Al-shareeda et al. 2020). This attack is based on multiple parameters, including the attacker's location within the network, the nature of the conversation channel, and enactment techniques. Then, based on our taxonomy of pose techniques, we provide electrocution instructions for each MITM class.

Eclipse Attack

Controlling a victim's local Internet connection is part of the eclipse. To begin, the attacker obscures the merchant's view of the blockchain. Seemingly legitimate transaction H including payment for a good is sent to the merchant, and then a defective transaction F to the miners is transmitted which shifts the cash elsewhere. The attacker floods the network with rogue nodes and communicates with infected nodes (Liu et al. 2020).

Sybil Attack

Sybil's attack attacks the entire network, trying to affect the network by flooding it by including a large number of nodes with fictitious IDs. In this, Sybil nodes are closely connected with other Sybil nodes. The ability to interact with authentic nodes is not strong in a Sybil attack. There are a limited number of social connections between Sybil and honest nodes. The main goal is to wield popular options or reputation (Bhushan and Sahoo 2020). For example, in an online voting system, SA-1 can illegally impersonate many identities to act as a regular user and vote on partisan options.

Double Spending

The double-spend is a basic Bitcoin assault attack. In this, an attacker makes a transaction that moves money to a business's address. After the transaction is shown in the most recent block, the attacker gets ownership of the purchased goods. After that the attacker immediately releases two blocks, the first of which contains a transaction that sends the money to a second address owned by himself (Begum et al. 2020).

Race Attack

The attacker sends an unusual exchange to a victim while concurrently sending another transaction to the network. This gives the merchant the impression thinking his transaction might be the first, but the attacker never submits it to the blockchain network. First, the user logs out and requests a transaction through the user's wallet (Aggarwal and Kumar 2021). This unjustifiable transaction takes place in a pool of unjustifiable transactions, from which a miner selects his transactions, solves a complex numerical problem through the POW consensus, obtains a unique hash output, and sends it to Add blocks to the blockchain. Blocks are added only if other miners verify these hashes.

51% Attack

51% attack is a smart blockchain attack in which fifty percent of the total of the network's mining hash rate is dominated by a team of hackers, and these ruling parties have the power to modify the blockchain by owning 51% of the whole network's nodes (Ye et al. 2018). This attack begins by privately accomplishing a chain of blocks that is completely separate from any version of the chain. Later, the decoupled chains are granted to the network and built as real chains. This allows for double-spending attacks.

Blockchain Enabled Smart Cities

Smart cities offer various unique benefits including privacy, reliability, better scalability, efficiency and fault tolerance. Blockchain integrated Smart city provides more resistance to threats. Thus, integration of blockchain on all the available smart devices would create a web that would provide better reliable and secure communication.

Motivation for Deployment of Blockchain in IoT Based Smart Cities

Currently, popularity is gained by smart city projects, and many nations and cities such as Manchester, Amsterdam, Madrid, Singapore, Barcelona, etc. are actively planning and making strategies to convert normal cities into smart cities (Xie et al. 2019). Also, a variety of smart city testbeds were developed to evaluate and simulate the proposed solutions for smart cities (Lanza et al. 2015). Some of them are listed below:

- SmartSantander is a well known testbed in which RFID tag labels/2000 popular QR codes, 200 GPRS modules, and 2000 IoT devices are successfully deployed in Santander, Spain (Latre et al. 2016). Additionally, eight use cases are implemented, including free parking, traffic monitoring, augmented reality, mobile perimeter monitoring, perimeter monitoring, outdoor parking management and participatory sensing.
- A new smart city testbed called City of Things is in Antwerp, Belgium (https://www.ibm.com/in-en/topics/what-is-blockchain#:~:text=Blockchain%20defined%3A%20Blockchain%20is%20a,patents%2C%20copyrights%2C%20branding). It arranges validation of advanced experiments of smart cities at the two users along with the technology level.
- NYUAD is developed by Abu Dhabi Center for Cyber Security (CCS-AD), a smart city test bed that aims to give a realistic and real-time environment of a smart city (Biswas and Muthukkumarasamy 2016). These environments further can be used by researchers or developers to study and rate the models they provide.

Blockchain Technology Overview

Blockchain ledger which is shared and records transactions, tracks assets (tangible and intangible), agreements, and contracts (Qiu et al. 2018). Originally developed to guide cryptocurrency transactions, but can also be used in all short-term transactions except the mediator. The major convenience of the blockchain is that to give up the hash power of the network, 51% of the system must be compromised. Hence, concluding the impracticality of succeeding in an attack over the blockchain network. Whenever any transaction happens over a blockchain network it is categorized as a block containing proof of work, record of transactions, number of the block, and also previous block's number to each and every entity involved in this network. The block gets cross checked by the entities and when 50% plus of them approve the transaction then it becomes successful and hence gets included in the current chain.

Types of Blockchain

The four major categories of blockchains are described in subsections below.

Public Blockchain

Public blockchains do not need any permissions and further allow any random person to join, they are also 100% decentralized. In these types of blockchain access rights, node creation rights, as well as validation rights are the same for every node. Till date, all sorts of transactions including mining and exchange of cryptocurrencies are done over the public blockchain. By computing hard cryptographic equations the

nodes over the public blockchain mine crypto over most familiar coins like Bitcoin, In exchange these nodes are rewarded with small amounts of cryptocurrencies, where they act as bank tellers who get the reward for transaction formulation.

Private Blockchains

Private blockchains also known to be managed blockchains are called so because a single organization controls them and they also require specific permissions. A node to be part of the blockchain is totally determined by the central authority, and the functional rights may not be necessarily same for each and every node. Since public access is restricted over managed blockchains they are not fully decentralized. Many B2B digital currency exchanges like ripple are examples of private blockchains. Private and public blockchain have their own disadvantages—private blockchains are more likely to be scams whereas public blockchains are time taking for the validation of any new data.

Consortium Blockchains

Consortium blockchains are similar in terms of requiring permissions like private blockchains. They also differ from private blockchains as they are in control by a group of organizations, rather than any individual entity. Thus, making it more decentralized and further increasing the security. The involvement of a number of groups makes it challenging to operate since every group may not have all the required infrastructure as well as technology required to implement blockchain and also it creates a trust risk.

Working of Blockchain

In recent years, we may have recorded that many companies around the world have integrated blockchain technology in late new years. But how does it work? Is it one major change or a simple extension? Blockchain progress is just beginning and has revolutionary potential in the future. So let's start debunking this technology. Figure 14.1 shows the Process of transaction in a blockchain.

Blockchain is a solution of three main technologies: A Peer-to-Peer network with shared ledger, Cryptographic keys, and a computing device that stores network transactions and records.

Cryptography keys consist of two keys—a public key and a private key. These keys make every transaction between two parties successful. Everyone carries the above-mentioned two keys for creating a secure digital identity reference. This aspect of Blockchain is the most critical secured identity. In the cryptocurrency world, this identification is known as a "virtual signature" and is used to authorize and manage transactions. Digital signatures are integrated in peer-to-peer networks. Various

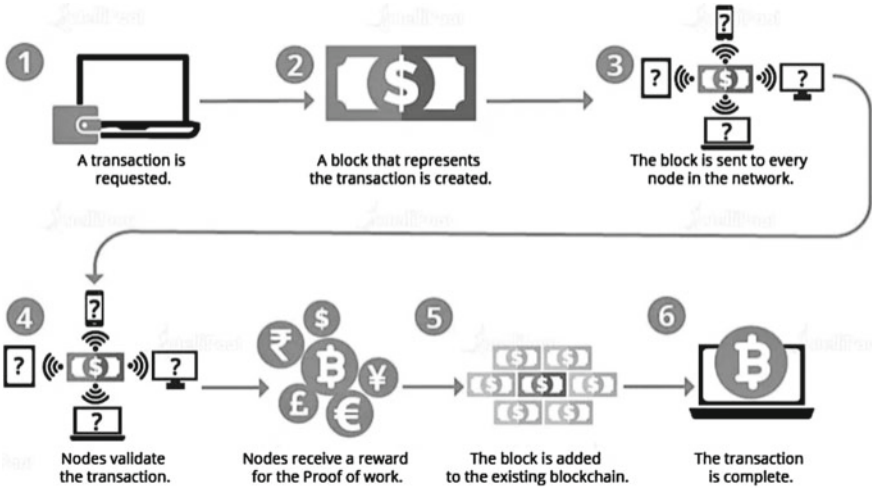

Fig. 14.1 Process of transaction in a blockchain

people assist as high-level advisors create agreements on transactions using digital signatures. Once they authorize the transaction, the numerical checks prove it and the transaction is acknowledged and protected between two parties associated with the network. In short, blockchain users practice cryptographic keys to conduct various kinds of digital communications over peer-to-peer networks. In summary, blockchain users use cryptographic keys to conduct various kinds of digital intercommunication over peer-to-peer networks.

Whenever a blockchain is included in a new blockchain transaction or a new block needs to be added to the blockchain, typically multiple nodes in the same blockchain implementation are required to run algorithms for evaluation, testing, and processing. Blockchain block history: A new block of a blockchain transaction is added to the ledger and a new block of all-inclusive data is combined with the blockchain once most nodes have authenticated the history and signature of the block. Blocks will be rejected for addition to the blockchain if consensus is not reached. This dispersed consensus model allows the blockchain to act as a distributed ledger without the need for a central authority or unified authorization to approve the blockchain transactions as shown in Fig. 14.1. Blockchain transactions are therefore very secure.

Consensus Protocols

The blockchain consensus protocol can be found in several definitive goals, such as achieving consensus, working together, collaboration, equal rights of all nodes, and compulsory participation of all nodes in the consensus process. Different types of Consensus protocols are described in further sections below.

PoS (Proof of Stake)

In this, the stake that is held determines which node is selected to build each new block, not the computational power. The major difference between PoW and PoS is that the simple way to find the solution is to find out the stake amount instead of adjusting the nonce several times. Hence, we can say that PoS uses energy efficiently. Similarly to PoW, this is also called as probabilistic-finality consensus protocol.

DPoS (Delegated Proof of Stake)

DPoS works on the basic principle of letting the nodes holding a stake vote on the choice of block validators. With this type of voting, stakeholders get the right to create blocks for the representatives they support and not create blocks themselves, thus reducing consumption power to 0. In comparison to PoS and PoW, this consensus protocol is low-cost and provides high efficiency.

PoW (Proof of Work)

Bitcoin and Ethereum have adopted PoW etc. In each consensus round, PoW selects a node and builds a different block using competition for computational power. The nodes which take part in the competition have to decode the cryptographic puzzle. Permission to create new blocks is only given to all nodes that tackle the puzzle first. Solving a PoW puzzle is very complex. A Higher level of computational power is required by the nodes to auto-adjust the value to find the right answer.

Ripple

Ripple is an open source based payment protocol[i]. In this, with the help of tracking or validating nodes clients initiate the transactions which are then broadcasted in the entire network, node validation performs the consensus process, and each node has a list of trusted nodes known as the Unique Node List (UNL). Votes for transactions are awarded to delegates backed by UNL nodes.

PoI (Point of Importance)

In PoS, the users who have more coins have higher chances that they will mine the next block. Similarly in PoW, to increase the computational power, parallel AISCs (application specific integrated circuits) chips are deployed by the miners. Whereas in PoI to overcome these limitations, the users which have a high number of transactions and the users who have high net stakes are rewarded. In this, an important value is assigned to every node. The node with the higher important value has higher priority

to mine the next block even if the stake value of that node is lower than the other nodes.

PoET (Proof of Elapsed Time)

PoET is an improvement over the PoW protocol where the selection of the mining node depends on the node which has the lowest waiting time. The same can be achieved by assigning a random timer value to each node. The earliest node (whose timer runs out earliest) generates a signed certificate which allows the node that in the current iteration this node will be the block leader.

PoC (Proof of Capacity)

The mechanism of PoC is such that based on the availability of the free memory capacity of HDD (external) a minor node is chosen. More possible solutions to nonce problems can be stored in the node which has a large capacity, before the beginning of the mining. The overall complexity and the difficulties in managing the nodes in PoW can be improved with the help of PoC.

PoB (Proof of Burn)

In PoB protocol, to access the mining rights to the authorized source the virtual cryptocurrency is burned by the nodes. This is quite similar to the PoW but the difference is that the assets in PoB are in terms of cryptocurrency. Whereas in PoW, the assets are in terms of the computing power of nodes. Here the burning coins shows us the node's commitment to be honest in the entire network as to gain the mining rights it has burned the original coins.

PoP (Proof of Proof)

To protect Sybil and attacks in blockchain a modification in PoS is made which is known as PoP. In standard PoS a recently developed mechanism is introduced, which states that after every successful transaction, every node in the entire network should get incentives. This reward policy is an incentive based which depends on the quality of work, amount of work and chain performance. The nodes can use the earned rewards as stakes to mine the new blocks.

FRChain (Fault Resilient Chain)

These types of algorithms are highly used in case of permissioned blockchains. This algorithm tries its best to make the network irrepressible from failures. These are scalable. It replaces faulty or malicious nodes with the good nodes after crashes with high efficiency. The security is provided to the network with the help of collective signing which is based on routing of oral messages over multicast trees. After a root is selected, validation and block propagation is conducted in the blockchain.

Recent Advancements in Blockchain Assisted IoT and Smart City Applications

Liang et al. (2018) proposed a framework of security that integrates smart devices with blockchain technology to make smart cities a secure communication platform. Noh and Kwon (2019) presented a use case where Blockchain promises to balance security and privacy. Montes et al. (2019) discussed how the integration of healthcare and smart cities will use information and technology in healthcare and medical practice around the world. Al-Abbasi and El-Medany (2019) examined potential security issues in integrating blockchain technology into smart city infrastructure and provided blockchain-based solutions ensuring the security and resilience of smart cities. Yetis and Sahingoz (2019) intended to look into the institutional and technical frameworks for the adoption of safe urban living using blockchain technology. In this project, Majdoubi et al. (2020) focused on the Supply-He-Chain Operational Oriented Document of Understanding (DOU) contract, which serves as a framework for interaction between consumers of services and their suppliers.

Begam et al. (2020) examined the architecture of blockchain technology platforms, the security stability and vulnerability of the technology, and how it addresses the critical areas of information security integrity, availability, and confidentiality. Thanh et al. (2020) proposed an allocated node structure for blockchain systems and attempted to set up an authentication system for IoT devices using the blocks stored in these nodes. Nguyen et al. (2020) proposed measures to comply with the requirements of major data protection laws and regulations, in particular the European Union's General Data Protection Regulation. Finally, he proposed a Proof of Reputation (PoR) consensus scheme based on a multidimensional trust model. Jha et al. (2019) proposed a consensus-based decentralized blockchain solution to address e-FIR data integrity and registration errors related to police stations in a constitutional database as a key component of smart city environments.

Sharma et al. (2019) offered an innovative and efficient security protection architecture that uses digital video on the Blockchain network to conceal sensitive information. It has been demonstrated that the suggested framework could safeguard digital video content with high accuracy and efficiency. Sharma et al. (2020a) established a secure communication platform in smart cities. The purpose of this article is

to combine blockchain and IoT. This will be done by creating a secure decentralized architecture. Dansana et al. (2020) proposed the Temporal Pattern Attention-Based LSTM (TPA-LSTM) natural gas performance prediction illustrative to enable the system to detect changes in natural gas supply capacity. Malik et al. (2021) studied a case for how the creation and growth of smart cities will alter both the way that cities are created today and how people live in future. Smart cities have grown to be an inevitable fashion of world development.

Sharma et al. 2020b) proposed a way to combine IoT and blockchain along the Consensus Algorithm Framework (BCIoT-CAF) to address the problem and ensure riskless data exchange in smart cities. Dansana et al. (2021) used a machine learning (ML) method in our proposed consensus protocol to accomplish effective leader election, and a novel dynamic block construction mechanism was created as a result. Each transaction's hash value is initially generated using the Merkle hash tree (Table 14.1).

Future Research Directions

On the basis of the review of this paper, few research could be carried out on smart city, a few similar concepts are mentioned below. Sharma et al. (2020b) came up

Table 14.1 Summary of recent advancements

Reference	Year	Major Contribution
Liang et al. (2018)	2016	Proposed security framework that integrates smart devices with blockchain
Noh and Kwon (2019)	2018	Presents a use case where Blockchain promises to balance security and privacy
Montes et al. (2019)	2018	Discussed how the integration of healthcare and smart cities will use information and technology in healthcare
Al-Abbasi and El-Medany (2019)	2018	Examined potential security issues in integrating blockchain technology into smart city infrastructure and provided blockchain-based solutions
Yetis and Sahingoz (2019)	2019	Intended to look into the institutional and technical frameworks for the adoption of safe urban living
Majdoubi et al. (2020)	2019	Focused on the Supply-He-Chain Operational Oriented Document of Understanding (DOU) contract
Begam et al. (2020)	2019	Examined the architecture of blockchain technology platforms, the security stability and vulnerability of the technology

(continued)

Table 14.1 (continued)

Reference	Year	Major Contribution
Thanh et al. (2020)	2019	Proposed an allocated node structure for blockchain systems and attempted to set up an authentication system
Nguyen et al. (2020)	2020	Proposed measures to comply with the requirements of major data protection laws and regulations
Jha et al. (2019)	2020	Proposed a consensus-based decentralized blockchain solution to address e-FIR data integrity and registration errors related to police stations
Sharma et al. (2019)	2020	Offered innovative and efficient security protection architecture that uses digital video
Sharma et al. (2020a)	2020	Established a secure communication platform in smart cities. The purpose of this article is to combine blockchain and IoT
Dansana et al. (2020)	2020	Proposed the Temporal Pattern Attention-Based LSTM (TPA-LSTM) natural gas performance prediction illustrative
Malik et al. (2021)	2021	Studied a case for how the creation and growth of smart cities will alter both the way cities are created today
Sharma et al. (2020b)	2021	Proposed a way to combine IoT and blockchain along the Consensus Algorithm Framework (BCIoT-CAF) to address the problem and ensure riskless data exchange
Dansana et al. (2021)	2022	Proposed consensus protocol to accomplish effective leader election

with few tools and techniques in order to evaluate smart cities on the basis of their management sustainability and smartness to operate. Sharma et al. (2020b) conducted a comparison of different tools and further pointed out the lackings and strengths. According to these authors, better development of smart cities assessment tools could be the main focus of further research and also the assessing the measures which would increase their performance. IoT is a leading tech used to apply smart cities in various dimensions. Scientists such as Sharma et al. (2020b) noted his use of IoT in areas such as transportation, waste management, healthcare and power transmission.

What is still lacking, however, is the integration of IoT across multiple dimensions and the further use of blockchain technology and AI to improve multiple dimensions of smart cities. This kind of research could help to eliminate the problems of cyber threats and security issues in smart cities. Dansana et al. (2021), highlighted that available risk assessment and management approaches are not comprehensive. Available tools do not appropriately consider non-technology-associated uncertainty. His research emphasized assessing technology-associated uncertainty without looking at

non-technology-associated risks. In addition, it is important to consider all aspects and their interrelationships, as these aspects are not practically separate in reality. Therefore, in-depth research into the risk landscape, proprietary assessment methodologies, and non-technology and technology-based risk management are critical. Such approaches can leverage AI technology and blockchain to predict and identify triggers to resolve manual disruptions, semi-autonomous, or autonomous. Since smart cities are bottom-up businesses, they adopt the enterprise architecture approach proposed by Helfert and Singh et al. can be considered for further analysis. Such advances will help advance a burgeoning program risk management pathway that can be deployed in a variety of smart city domains by taking a few precautions.

Conclusion

In this paper, we propose a security framework that uses blockchain technology to ensure reliable intercommunication between smart cities and ensure their security. Along with various unique benefits including privacy, reliability, better scalability, efficiency and fault tolerance. Blockchain integrated Smart city provides more resistance to threats. Thus, integration of blockchain on all the available smart devices would create a web which would provide better reliable and secure communication. Further work on this technology aims at designing the system model, authenticating its operability, and testing.

References

Aggarwal S, Kumar N (2021) Attacks on blockchain. In: Advances in computers, vol 121, pp 399–410. Elsevier

Al-Abbasi L, El-Medany W (2019) Blockchain security architecture: a review technology platform, security strength and weakness. In: 2nd smart cities symposium (SCS 2019), pp 1–5. https://doi.org/10.1049/cp.2019.0190

Alnahari MS, Ariaratnam ST (2022) The application of blockchain technology to smart city infrastructure. Smart Cities 5(3):979–993

Al-shareeda MA, Anbar M, Manickam S, Hasbullah IH (2020) Review of prevention schemes for man-in-the-middle (MITM) attack in vehicular ad hoc networks. Int J Eng Manag Res 10

Ande R, Adebisi B, Hammoudeh M, Saleem J (2020) IoT: evolution and technologies from a security perspective. Sustain Cities Soc 54(February 2019):101728. https://doi.org/10.1016/j.scs.2019.101728

Appio FP, Lima M, Paroutis S (2019) Understanding smart cities: innovation ecosystems, technological advancements, and societal challenges. Technol Forecast Soc Chang 142(1–14):2018. https://doi.org/10.1016/j.techfore.2018.12.018

Apostol D, Balaceanu C, Constantinescu EM (2015) Smart—Economy concept—Facts and perspectives. HOLISTICA J Bus Public Admin 6(3):67–77

Arroub A, Zahi B, Sabir E, Sadik M (2016) A literature review on smart cities: paradigms, opportunities and open problems. In: Proceedings—2016 international conference on wireless networks and

mobile communications, WINCOM 2016: green communications and networking, pp 180–186. https://doi.org/10.1109/WINCOM.2016.7777211

Arsh M, Bhushan B, Uppal M (2021) Internet of Things (IoT) toward 5G NETWORK: design requirements, integration trends, and future research directions. In: Advances in intelligent systems and computing, pp 887–899.https://doi.org/10.1007/978-981-15-9927-9_85

Begam SS, JV, Selvachandran G, Ngan TT, Sharma R (2020) Similarity measure of lattice ordered multi-fuzzy soft sets based on set theoretic approach and its application in decision making. Mathematics 8:1255

Begum A, Tareq A, Sultana M, Sohel M, Rahman T, Sarwar A (2020) Blockchain attacks analysis and a model to solve double spending attacks. Int J Mach Learn Comput 10(2):352–357

Biswas K, Muthukkumarasamy V (2016)Securing smart cities using blockchain technology. In: 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS), pp 1392–1393. https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198

Bhowmik T, Bhadwaj A, Kumar A, Bhushan B (2022) Machine learning and deep learning models for privacy management and data analysis in smart cities. In: Balas VE, Solanki VK, Kumar R (eds) Recent advances in Internet of Things and machine learning. intelligent systems reference library, vol 215. Springer, Cham. https://doi.org/10.1007/978-3-030-90119-6_13

Bhushan B, Sahoo G (2020) Requirements, protocols, and security challenges in wireless sensor networks: an industrial perspective. In: Handbook of computer networks and cyber security, pp 683–713.https://doi.org/10.1007/978-3-030-22277-2_27

Bibri SE, Krogstie J (2017) Smart sustainable cities of the future: an extensive interdisciplinary literature review. Sustain Cities Soc 31:183–212. https://doi.org/10.1016/j.scs.2017.02.016

Burnes D, DeLiema M, Langton L (2020) Risk and protective factors of identity theft victimization in the United States. Prevent Med Rep 17:101058

Biswas K, Muthukkumarasamy V (2016) Securing smart cities using blockchain technology. https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198

Bhushan B, Sahoo C, Sinha P, Khamparia A (2020) Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions. Wirel Netw. https://doi.org/10.1007/s11276-020-02445-6

Bhushan B, Sahoo G (2017) Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. Wirel Pers Commun 98(2):2037–2077. https://doi.org/10.1007/s11277-017-4962-0

Dansana D, Kumar R, Das Adhikari J, Mohapatra M, Sharma R, Priyadarshini I, Le D-N (2020) Global forecasting confirmed and fatal cases of COVID-19 outbreak using autoregressive integrated moving average model. Front Public Health 8:580327. https://doi.org/10.3389/fpubh.2020.580327

Dansana D, Kumar R, Parida A, Sharma R, Adhikari JD et al (2021) Using susceptible-exposed-infectious-recovered model to forecast coronavirus outbreak. Comput, Mater Continua 67(2):1595–1612

Department of Economic and Social Affairs (2014) World urbanization prospects: The 2014 revision, highlights (ST/ESA/SER.A/352). United Nations: Department of Economic and Social Affairs, Population Division, Tech. Rep. https://esa.un.org/unpd/wup/Publications/Files/WUP2014-Highlights.pdf

Elahi H, Wang G, Peng T, Chen J (2019) On transparency and accountability of smart assistants in smart cities. Appl Sci (Switzerland) (24):9. https://doi.org/10.3390/app9245344

Flynn T, Grispos G, Glisson W, Mahoney W (2020) Knock! Knock! Who is there? Investigating data leakage from a medical IoT hijacking attack. In: Proceedings of the 53rd Hawaii international conference on system sciences

Goyal S, Sharma N, Kaushik I, Bhushan B (2021) Blockchain as a solution for security attacks in named data networking of things. In: Security and privacy issues in IoT devices and sensor networks, pp 211–243.https://doi.org/10.1016/b978-0-12-821255-4.00010-9

HMGovernment (2011) Government cloud strategy, pp 1–24
Hussain M, Al-Haiqi A, Zaidan AA, Zaidan BB, Kiah M, Iqbal S, Iqbal S, Abdulnabi M (2018) A security framework for mHealth apps on Android platform. Comput Secur 75:191–217
https://www.ibm.com/in-en/topics/what-is-blockchain#:~:text=Blockchain%20defined%3A%20Blockchain%20is%20a,patents%2C%20copyrights%2C%20branding
Ismagilova E, Hughes L, Dwivedi YK, Raman KR (2019) Smart cities: advances in research—An information systems perspective. Int J Inf Manag 47(88–100):2018. https://doi.org/10.1016/j.ijinfomgt.2019.01.004
Jha S et al (2019) Deep learning approach for software maintainability metrics prediction. IEEE Access 7:61840–61855
Khalaf BA, Mostafa SA, Mustapha A, Mohammed MA, Abduallah WM (2019) Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. IEEE Access 7:51691–51713. https://doi.org/10.1109/ACCESS.2019.2908998
Lanza J, Sánchez L, Muñoz L, Galache JA, Sotres P, Santana JR, Gutiérrez V (2015) Large-scale mobile sensing enabled internet-of-Things testbed for smart city services. Int J Distribut Sensor Netw 11(8). Article 785061. https://doi.org/10.1155/2015/785061
Latre S, Leroux P, Coenen T, Braem B, Ballon P, Demeester P (2016) City of things: an integrated and multi-technology testbed for IoT smart city experiments. In: 2016 IEEE International Smart Cities Conference (ISC2). https://doi.org/10.1109/isc2.2016.7580875
Liang X, Shetty S, Tosh D (2018)Exploring the attack surfaces in blockchain enabled smart cities. In: 2018 IEEE international smart cities conference (ISC2), pp 1–8. https://doi.org/10.1109/ISC2.2018.8656852
Liu Y, Hei Y, Xu T, Liu J (2020) An evaluation of uncle block mechanism effect on ethereum selfish and stubborn mining combined with an eclipse attack. IEEE Access 8:17489–17499
Majdoubi DE, El Bakkali H, Sadki S (2020) Towards smart blockchain-based system for privacy and security in a smart city environment. In: 2020 5th international conference on cloud computing and artificial intelligence: technologies and applications (CloudTech), pp 1–7. https://doi.org/10.1109/CloudTech49835.2020.9365905
Makrushin D, Dashchenko V (2016) Fooling the 'Smart City.' Technical Report, Kaspersky Lab, pp 1–22
Malik PK, Sharma R, Singh R, Gehlot A, Chandra Satapathy S, Alnumay WS, Pelusi D, Ghosh U, Nayak J (2021) Industrial Internet of Things and its applications in industry 4.0: state of the art. Comput Commun 166:125–139. ISSN 0140-3664. https://doi.org/10.1016/j.comcom.2020.11.016
Mehta S, Bhushan B, Kumar R (2022) Machine learning approaches for smart city applications: emergence, challenges and opportunities. In: Balas VE, Solanki VK, Kumar R (eds) Recent advances in internet of things and machine learning. Intelligent Systems Reference Library, vol 215. Springer, Cham. https://doi.org/10.1007/978-3-030-90119-6_12
Montes JM, Ramirez CE, Gutierrez MC, Larios VM (2019) Smart contracts for supply chain applicable to smart cities daily operations. In: 2019 IEEE international smart cities conference (ISC2), pp 565–570. https://doi.org/10.1109/ISC246665.2019.9071650
Nguyen PT, Ha DH, Avand M, Jaafari A, Nguyen HD, Al-Ansari N, Van Phong T, Sharma R, Kumar R, Le HV, Ho LS, Prakash I, Pham BT (2020) Soft computing ensemble models based on logistic regression for groundwater potential mapping. Appl Sci 10:2469
Nilssen M (2019) To the smart city and beyond? Developing a typology of smart urban innovation. Technol Forecast Soc Change 142:98–104. https://doi.org/10.1016/j.techfore.2018.07.060. July 2018
Nižetić S, Solić, P, Lopez-de-Ipi´na˜ Gonzalez-de-Artaza´ D, Patrono L (2020) IoT (IoT): opportunities, issues and challenges towards a smart and sustainable future. J Clean Prod 274.https://doi.org/10.1016/j.jclepro.2020.122877

Noh Jh, Kwon Hy (2019) A Study on smart city security policy based on blockchain in 5G Age. In: 2019 international conference on platform technology and service (PlatCon), pp 1–4. https://doi.org/10.1109/PlatCon.2019.8669406

OWASP Foundation (2013) OWASP top 10-2013: the most critical web application security risks

Paiva S, Ahad MA, Tripathi G, Feroz N, Casalino G (2021) Enabling technologies for urban smart mobility: recent trends, opportunities and challenges. Sensors 21(6):1–45. https://doi.org/10.3390/s21062143

Porru S, Misso FE, Pani FE, Repetto C (2020) Smart mobility and public transport: opportunities and challenges in rural and urban areas. J Traffic Transp Eng (English Edition) 7(1):88–97. https://doi.org/10.1016/j.jtte.2019.10.002

Qiu J, Liang X, Shetty S, Bowden D (2018)Towards secure and smart healthcare in smart cities using blockchain. In: 2018 IEEE international smart cities conference (ISC2), pp 1–4. https://doi.org/10.1109/ISC2.2018.8656914

Radu LD (2020) Disruptive technologies in smart cities: a survey on current trends and challenges. Smart Cities 3(3):1022–1038. https://doi.org/10.3390/smartcities3030051

Sharma R, Kumar R, Kumar Sharma D, Hoang Son L, Priyadarshini I, Thai Pham B, Tien Bui D, Rai S (2019) Inferring air pollution from air quality index by different geographical areas: case study in India. Air Qual Atmos Health 12:1347–1357 (2019)

Sharma R, Kumar R, Singh PK, Raboaca MS, Felseghi R-A (2020a) A systematic study on the analysis of the emission of CO, CO_2 and HC for four-wheelers and its impact on the sustainable ecosystem. Sustainability 12:6707

Sharma R, Kumar R, Satapathy SC, Al-Ansari N, Singh KK, Mahapatra RP, Agarwal AK, Le HV, Pham BT (2020b) Analysis of water pollution using different physicochemical parameters: a study of Yamuna River. Front Environ Sci 8:581591. https://doi.org/10.3389/fenvs.2020.581591

Silva BN, Khan M, Han K (2018) Towards sustainable smart cities: a review of trends, architectures, components, and open challenges in smart cities. Sustain Cities Soc 38(697–713):2017. https://doi.org/10.1016/j.scs.2018.01.053

Thanh V, Rohit S, Raghvendra K, Le Hoang S, Binh Thai P, Bui Dieu T, Ishaani P, Manash S, Tuong L (2020) Crime rate detection using social media of different crime locations and twitter part-of-speech tagger with brown clustering. 1 Jan. 2020:4287–4299

Topal OA, Demir MO, Liang Z, Pusane AE, Dartmann G, Ascheid G, Kur GK (2020) A physical layer security framework for cognitive cyber-physical systems. IEEE Wirel Commun 27(4):32–39

Xie J, Tang H, Huang T, Yu FR, Xie R, Liu J, Liu Y (2019) A survey of blockchain technology applied to smart cities: research issues and challenges. IEEE Commun Surv Tutor 21(3):2794–2830. https://doi.org/10.1109/comst.2019.2899617

Ye C, Li G, Cai H, Gu Y, Fukuda A (2018). Analysis of security in blockchain: case study in 51%-attack detecting. In: 2018 5th international conference on dependable systems and their applications (DSA). IEEE, September, pp 15–24

Yetis R, Sahingoz OK (2019)Blockchain based secure communication for IoT devices in smart cities. In: 2019 7th international Istanbul smart grids and cities congress and fair (ICSG), pp 134–138. https://doi.org/10.1109/SGCF.2019.8782285

Yu Y, Li Y, Tian J, Liu J (2018) Blockchain-based solutions to security and privacy issues in the IoT. IEEE Wirel Commun 25(6):12–18