International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 6, ISSN No. 2455-2143, Pages 436-441
Published Online October 2022 in IJEAST (http://www.ijeast.com)

REVIEW ON SMART CITY IOT SECURITY USING BLOCKCHAIN

Gurmanpreet Kaur Dhanju, Shobha Tyagi, Aditya Kumar, Ishaan Asthana, Aditya Taluja
Department of Computer Science and Engineering
Manav Rachna International Institute of research and studies

Abstract: **Blockchain has grown in popularity as a crypto currency in recent years. It can also be used to secure IoT devices, helping to keep personal information private. Cities are becoming smarter these days thanks to IT and IoT devices, yet the data they generate is insecure due to IoT devices' limited processing capability. This is where blockchain comes in to secure the IoT data it generates. Blockchain and smart cities are still in their infancy, thus further study is required to integrate them. This study examines the challenges of implementing IoT security in smart cities using blockchain.**

I. INTRODUCTION

Because of the Internet of Things, the number of networked devices is rapidly increasing (IoT). According to the 2020 census, there will be more than 25 billion IoT devices on the planet [1]. As the number of IoT devices grows, the key concern is security, which is both necessary and concerning. Faridabad has been designated as a smart city under the Indian government's ground-breaking flagship initiative, which intends to build 100 smart cities over a five-year period. The Ministry of Urban Development has started out on a mission to build communities with adequate infrastructure that provide a comfortable lifestyle for citizens while also safeguarding the environment. The mission's major goal is to give these communities with cutting-edge smart technology solutions like water recycling, solar energy, digitalization, waste management, and smart metering.

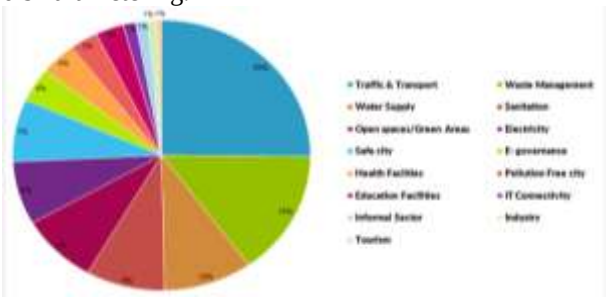

Fig 1: Applications of smart cities

As indicated in Figure 1, smart cities provide advanced services such as transportation, smart healthcare, e-voting, smart banking, and so on. In order to run these applications efficiently, security is essential. These applications aid in the improvement of personal and national standards. [2]. We employ blockchain to achieve standard security. This technology aids in security[1]. For IoT security and authentication, blockchain offers a feasible alternative. [3]. Bitcoin introduced blockchain to allow for the movement of digital payments between parties without the use of a central authority (CA) [1.]

Smart cities contain an environment that improves a person's lifestyle. One of the most important and major goals of a smart city is to provide services such as housing, transportation, and healthcare. By offering consistent security, blockchain aids the proper operation of these facilities[1].

II. IMPLEMENTATION CONCERN IN IOT SECURITY

The Internet of Things is a vast field with numerous applications. Smart Homes, Smart Cities, Smart-Driven Cars, IoT Retail Shops, Farming, and other applications are among them. IoT gadgets such as wearables, smart thermostat systems, air conditioners, and refrigerators that use Wi-Fi for remote control are already on the market. Apart from these benefits, IoT has several serious downsides that must be addressed prior to the installation of gadgets.

There have been a number of bugs discovered, and if hackers gain access to them, they can wreak havoc. They can use these flaws to undermine the system. Customers' privacy could be threatened, or they could be injured. Thus, before using IoT devices, evaluate the security of these systems to ensure that they are bug-free. [4].

III. AN INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

The blockchain is a decentralised database that keeps track of transactions. Every network transaction is recorded. Rather than relying on a central database like those used by banks or government entities. It has a distributed ledger spanning a network of computer nodes. This network, like the internet, can be open to the general public. It can be public or private, and anyone can access it from anywhere on the planet. It is only accessible to members of an organisation. The blockchain's decentralised cryptographic process allows users to trust one another and perform peer-

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 6, ISSN No. 2455-2143, Pages 436-441
Published Online October 2022 in IJEAST (http://www.ijeast.com)

to-peer transactions, eliminating the need for intermediaries or middlemen. This technology is not only practical, but also entertaining. The global economy, on the other hand, is influencing how we use the internet. also undergoing transformation [3].

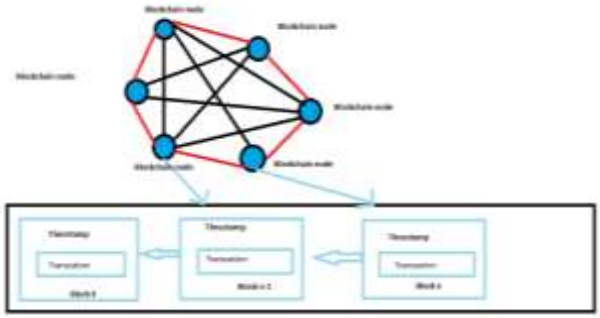

Fig 2: Blockchain database

3.1 Components of blockchain: -

The entire system of blockchain is made up of four key components.

1) Node Network: On a blockchain network, all nodes connected to the internet collaborate to keep track of all transactions. The protocol validates the transaction's legitimacy, eliminating the requirement for a trusted third party to do so. When the transaction is finished[15] Mining is the process of adding the records of a transaction to the ledger of prior transactions. The rest of the network's nodes must verify the proof of work.

2) Distributed database system: Each system node receives a copy of the database, which is made up of data blocks. Each block contains the information listed below. A transaction list is a list of all transactions made by a corporation.

3) Shared ledger: The ledger is updated every time a transaction is completed. It is entirely free and open to the general public. in corruptible, which gives the equation system more transparency.

4) Cryptography: It ties the information together with a sophisticated encryption method. Unauthorized users have tampered with the data using an encryption technique that is difficult to monitor or decrypt.

3.2: Security framework

1) Physical layer: Smart city devices include sensors and actuators that collect and transmit data to upper-layer protocols. Several of these gadgets, like the Nest thermostat and the Acer Fitbit, are vulnerable to security attacks because to inadequate encryption and access control methods. Furthermore, there is no smart device standard that permits data to be shared and integrated for cross-functionality. Vendors must agree on implementation and communication standards to resolve these challenges with smart devices.

2) Communication layer: Bluetooth, 6LoWPAN, Wi-Fi, Ethernet, 3G, and 4G are some of the communication technologies used by smart city networks to connect with one another. Blockchain protocols must be connected with this layer to guarantee security and anonymity for transferred data. For example, transaction records can be transformed into blocks and tele-hash broadcasted throughout the network. Protocols like BitTorrent provide peer-to-peer connectivity, while Ethereum allows for smart contract capabilities. However, because needs vary by application, combining existing communication protocols with blockchain is a significant problem. One approach is to use numerous blockchains with the help of a blockchain access layer to enable application-specific functionality.

3) Database layer: In blockchain, a distributed ledger is a type of decentralised database that saves records one by one. Each record in the ledger has a timestamp and a unique cryptographic signature. Any authorised user gets access to the whole transaction history of the ledger, which can be verified and audited. There are two types of distributed ledgers in practise: permissionless and permissioned. The key benefits of a permissionless ledger are its censorship resistance and openness. The public ledger, on the other hand, must keep complex shared records and requires more time to reach consensus than the private ledger. Furthermore, anonymous assaults can compromise public ledgers. As a result, private ledgers are recommended for real-time applications like traffic systems in smart cities because they enable scalability, performance, and security.

4) Interface layer: This layer contains a collection of intelligent programmes that collaborate to make sound decisions. The apps should, however, be tightly linked because weaknesses in one application could give intruders access to other processes that rely on it. [6]

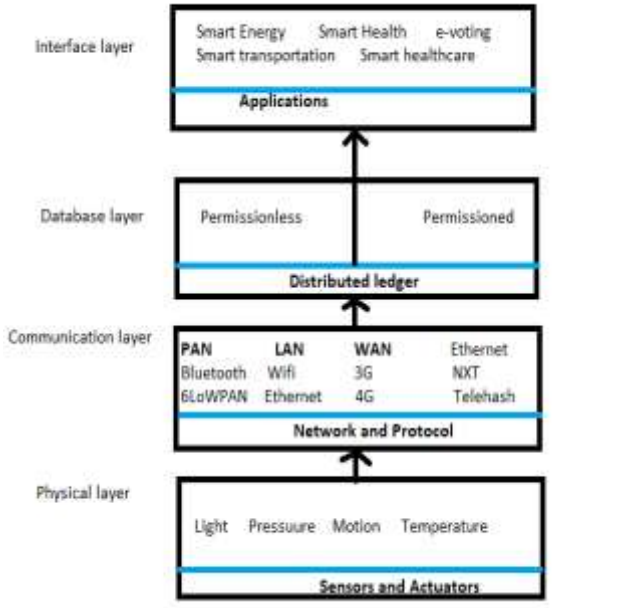

Fig 3: Security framework

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 6, ISSN No. 2455-2143, Pages 436-441
Published Online October 2022 in IJEAST (http://www.ijeast.com)

3.3 Construction of blockchain

A new digital transaction is generated, which is then transformed into a cryptographically secure block. Miners are members of the blockchain network who compete to validate transactions by solving complex programmed tasks. A prize is awarded to the first person to solve it (In the case of the bitcoin blockchain, the miner would get bitcoins).
The time-stamped and chronologically inserted block is then added to the chain. The hash of the previously accepted block is used by nodes to communicate their approval of a block by producing another block in the chain[14].

3.4 Implementing blockchain

1) Public: This is an open region where any node can send or receive transactions and participate in the consensus process without requesting permission. Here's where Bitcoin and Ethereum come into play.
2) Consortium area: Only specific nodes are allowed to participate in the consensus process. Reading and sending permissions can be made public or limited to a small number of authorised nodes.
3) Private: Only the entity that owns the blockchain network can write transactions in this authorization region. Transaction reading can be made public or restricted to a few nodes, depending on the requirements. This type of device is quite frequent.

IV. MARKET STATISTICS FOR BLOCKCHAIN AND SMART CITIES

According to IDC, blockchain adoption in the industry is widespread[5]. At least 25% of the world's 2000 largest public corporations are expected to embrace blockchain to ensure digital trust. Blockchain will be used by the majority of the world's leading banks, health institutions, and half of all manufacturers and merchants. The blockchain market is anticipated to grow from 3.0 billion USD to 39.7 billion USD by 2025.

4.1 Recent Advances in Blockchain Applications in Smart Cities

This section summarises recent research in blockchain-based smart cities and related smart environment disciplines. The purpose of this section is to critically assess and evaluate new research discoveries as potential smart city solutions based on blockchain technology. A smart city with several smart settings is depicted.

4.2 Smart electronic commerce

The purchasing and selling of products and services over the Internet or through online services is known as e-commerce. E-commerce technology includes mobile commerce, electronic money transfers, supply chain management, and the Internet. Automated data collection systems include marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. E-commerce, which is the largest sector of the electronics business, benefits from technological advancements in the semiconductor industry.
Although other technologies, such as e-mail, may be used, e-commerce often uses the internet for at least a portion of the transaction's life cycle. E-commerce transactions include the purchase of goods or services. Online retail, electronic markets, and online auctions are the three types of e-commerce. E-commerce is aided by electronic commerce.

4.3 E-commerce businesses may also employ some or all of the following

Conversational commerce involves live chat, chatbots, and voice assistants, as well as online retail sales to consumers via websites and mobile apps;
Providing or participating in online marketplaces that undertake third-party B2C or C2C transactions; buying and selling between businesses (B2B); Collecting and using demographic data through web contacts and social media; Electronic data transmission between businesses;
Marketing to new and existing customers via email or fax (for example, newsletters); Preparing new items and services for release; Online financial exchanges are offered for currency exchanges or trading.

4.4 Smart electronic voting

Electronic voting (sometimes known as e-voting) is a method of voting that use electronic equipment to assist in the casting and counting of votes. Many countries have stated that governments must go online and adopt electronic voting in elections.
Depending on the implementation, freestanding electronic voting machines (also known as EVMs) or PCs connected to the Internet may be used for e-voting. Electronic voting is a digital polling technique. Rather than utilising ballot papers, voters are validated for voting using biometrics through software systems. However, such electronic voting is vulnerable to cyber and manipulation attempts at the user and system levels. In terms of time and election costs, blockchain-based e-voting systems can improve voting efficiency[12]. The blockchain technology creates a network without a single point of failure. It is not under the control of any central authority and is not in danger of failing. Each user on the blockchain has their own private key, which they may use to digitally sign documents and add his transaction to a digital ledger that only allows appends. These blockchain properties can be employed in scalable blockchain-based e-voting. Each voter can be allocated a wallet with a private key for authentication when voting in blockchain-based e-voting. During each poll, a coin is credited to the wallet, which can only be used once to vote for a preferred candidate. The system protocol can be set up to allow voters to be validated while remaining anonymous until the final count is performed.

4.5 Smart transportation

To make transportation systems efficient, safe, fast, convenient, economical, lucrative, and linked, modern management methods and traffic management techniques are integrated with new technologies such as computing devices, sensor networks, wireless communications, and electronics. The smart transportation system includes traffic signal management systems, integration of the Speed Detection Camera System (SDCS), automatic number plate identification, real-time monitoring CCTV systems, and traffic ticket administration systems.

The BFT feature of blockchain can manage the problem of communication and collaboration in automobiles, roadside-connected devices and infrastructure, and pedestrian-owned cell phones in a fully distributed manner for smart transportation systems. Blockchain's resistance to "double spending" will aid in monetary transactions without the use of central middlemen, leading in the construction of an inbuilt financial system for ITS. Blockchain technology can help the ride-sharing transportation industry. It has the potential to create a peer-to-peer ecosystem, putting commercialised corporate-based transportation services like Uber, Careem, and Lyft under pressure. As a result, the economy will become more dispersed.

4.6 Smart HealthCare

Data-driven healthcare models have emerged as the volume of patient data shared between healthcare providers and insurance firms has expanded considerably in recent years [9]. The provision of high-quality health care to the general people is one of the smart city's main goals. The ability of health care services in a smart city to produce desired health outcomes at the individual and population levels is characterised as care quality. Blockchain technology could be beneficial to the healthcare industry. A blockchain-based healthcare system keeps medical records accurate and interoperable, improves insurance claim adjudication quality, and delivers high-quality patient-centric services[13]. The blockchain may store whole electronic health records (EHR), and each patient can be given a blockchain-based identification. Information access, identity identification, and privacy can all be addressed with smart contracts and blockchain-based access control technology. Access to the same information on a patient's medical history, diagnoses, and treatments is required by various stakeholders in the healthcare industry. For therapeutic purposes, blockchain's distributed architecture enables for data sharing and authorised access between Medicare systems. Furthermore, blockchain might be used to control the medical product supply chain from manufacturing to distribution at pharmacies, allowing for the detection and prevention of medicine counterfeiting by verifying the provenance of medical items.

A blockchain-based prototype named MedRec" is being used to store electronic health information for medical research. MedRec is a real-time, system-interoperable data storage platform for medical records that prioritises patient privacy while also improving the quality and amount of data available for medical research. The distributed ledger mechanism, like bitcoin POW, is well-established, and the medical record is saved using its cryptographic hash to avoid manipulation.

4.7 Smart Home

The term "smart house" refers to the sophisticated use of ICT, ubiquitous computing, and wireless sensor networks (WSN) for automated control and management of items like lights, thermostats, fire alarms, and entertainment systems. Smart houses demonstrate how new technologies are increasingly being used and integrated into home networks to improve people's quality of life [8]. It also has an intrusion detection system, access control, and emergency alarm systems to prevent cyber-physical threats. The home appliances are connected to the Internet through a local network for remote monitoring and control via a wall-mounted terminal or mobile/desktop apps. Smart houses promise to revolutionise living standards with domestic comfort, reliability, privacy, and leisure, with energy efficiency, increased Quality of Service (QoS), improved customer experience, and enhanced quality of life (QoL) as main goals. The Internet of Things (IoT) in the Smart House System (SHS) links to each other and local servers via the home local network, as well as to faraway servers via the home gateway, jeopardising privacy. To combat this, SHS use blockchain technology and smart contracts to ensure network security. Incorporating blockchain technology into smart homes has various advantages[11]. A homomorphic consortium blockchain solution for sensitive data privacy preservation was proposed in Traditional SHS (HCB-SDPP). The consortium blockchain offers expanded organisational jurisdiction as well as scalability and interoperability. The physical structure of the HCB-SDPP is made up of sensor nodes, gateway nodes, and verification nodes. Paillier Encryption, a type of homomorphic encryption, was employed for privacy and security. Blockchain Channels were used to keep separate ledgers for each community, which included many gateway nodes. A novel block data format based on homomorphic encryption was also developed (HEBDS). After a performance analysis based on data security, data availability, ledger storage security, and system resilience, the HCB-SDPP scheme was shown to be effective.

V. DISCUSSION, LIMITATIONS, AND FUTURE RESEARCH

Our study ideas should be seen as suggested starting points for further research rather than comprehensive overviews of the issue under consideration. Even though we believe our framework is complete at this moment, additional research fields may emerge in the future.

More research is needed to assess the usefulness of blockchain when combined with different architectures such as cloud, fog, and edge computing. This is especially true in terms of scalability solutions provided by such designs. Similarly, the combination of blockchain and artificial intelligence (AI) brings up interesting new research opportunities in a number of the disciplines discussed in this article. AI skills combined with data analytics could enable smart cities realise the benefits of blockchain technology in sectors such as health care, administration, energy production, and commerce, as well as corporate logistics and mobility.

Blockchain technology and smart cities share two characteristics: They are, first and foremost, large conceptions. Smart city research is a field of applied study whose goal is to make cities more liveable. Blockchain is a technology platform that may be used to power a variety of applications. Second, both industries are undergoing tremendous development, with significant advancements expected in the near future. In the blockchain sector, a variety of novel techniques are being investigated in order to provide more efficient solutions that preserve transaction scalability without relying on energy-intensive consensus mechanisms like proof of work. As a result, technological progress offers up new opportunities for smart cities, which will require more investigation.

VI. CONCLUSION

Blockchain has emerged as a disruptive option for secure P2P interaction in an untrustworthy environment, thanks to disintermediation. In this research, we looked at the role of blockchain in smart cities. We investigated the origins of blockchain technology, as well as its development and evolution. We discussed the various technologies that comprise blockchain technology. We looked at the various blockchain platforms and consensus algorithms that are currently available for use in smart city applications in the blockchain ecosystem. We undertook technical due diligence on potential blockchain applications as part of the conversation. We've outlined some of the most important factors to think about while selecting a blockchain platform. We conducted a thorough review of the literature on the usage of blockchain in common smart city applications. We demonstrated how blockchain was utilised to deliver trustworthy and secure services in smart cities using real-world case studies. The basic data-centric requirements for blockchain use in smart cities were investigated. The open research issues that are preventing blockchain from becoming a key instrument in smart city innovation were explored. In the data-driven era, we believe blockchain will be a key technology. In today's academic circles, blockchain technology breakthroughs and its implementation in smart cities to improve quality of life are a popular topic. Before blockchain may be employed in sustainable urban development initiatives, a variety of difficulties and needs must be investigated and overcome.

VII. REFERENCES

[1]. Umer Majeeda, Latif U. Khana, Ibrar Yaqoobb, S. M. Ahsan Kazmic, Khaled Salahb, Choong Seon Honga,(2017) .Blockchain for IoT-based Smart Cities: Recent Advances, Requirements, and Future Challenges. In IEEE (DOI: 10.1109/MCOM.2017.1600514)

[2]. Yang su , Jing wu, Chennain Long , Lijun Wei.(2020) Secure Decentralised Machine Identifiers for Internet of Things .(https://doi.org/10.1145/3390566.3391670)

[3]. Dongxing Li, Wenping Deng, Wei Peng Fangyu Gai,(2018). A Blockchain-based Authentication and Security Mechanism for IoT.In IEEE (DOI: 10.1109/ICCCN.2018.8487449)

[4]. Madhusudan Singh , Abihraj Singh , Shiho kim . (2018) Blockchain: A Game Changer for Securing IoT.IEEE 4th World Forum on Internet of Things (WF-IoT)(DOI: 10.1109/WF-IoT.2018.8355182)

[5]. IDC FutureScape: Worldwide IT Industry 2018 Predictions. URLhttps://www.idc.com/getdoc.jsp?containerId=US43171317

[6]. Kamanshis Biswas ,Vallipuram Muthukkumarasamy.(2016)Securing smart cities Using blockchain Technology. In IEEE (DOI: 10.1109/HPCC-SmartCity-DSS.2016.0198)

[7]. Mostafa, M.M.; El-Masry, A.A. Citizens as consumers (2013) Profiling e-government services' users in Egypt via data mining techniques. Int. J. Inf. Manag. (33, 627–641). [CrossRef]

[8]. Sripan, M.; Lin, X.; Petchlorlean, P.; Ketcham, M.(18–19 December 2012)Research and thinking of smart home technology. In Proceedings of the International Conference on Systems and Electronic Engineering (ICSEE'2012), Phuket, Thailand, (pp. 61–63)

[9]. Demirkan, H.(2013) A smart healthcare systems framework. IT Prof. (38–45). [CrossRef]

[10]. Horst Treibmaier; Abderahman rejeb; (2020), 3Anderas strebinger.Blockchain as a Driver for Smart City Development: Application Fields and a Comprehensive Research Agenda.(853–872.)

[11]. Ferdous, M.S.; Biswas, K.; Chowdhury, M.J.M.; Chowdhury, N.; Muthukkumarasamy, V., 2019; Volume 115 Chapter two—Integrated platforms for blockchain enablement. In Advances in Computers; Kim, S., Deka, G.C., Zhang, P., Eds.; Role of Blockchain Technology in IoT Applications; Academic Press: Cambridge, MA, USA, (pp. 41–72)

[12]. Li, J.; Greenwood, D.; Kassem, M. (2019), Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases. Autom. Constr. ,(102, 288–307.) [CrossRef]

[13]. Kundu, D. (2019) Blockchain and trust in a smart city. Environ. Urban. ASIA(31–43). [CrossRef].

[14]. Meinel, Holger, and Wolfgang Bösch, (2017) "Radar Sensors in Cars." Automated Driving. Springer International Publishing, 2.(245-261).

[15]. Humayed, Abdulmalik, (2017)"Cyber-Physical Systems Security—A Survey." arXiv preprint arXiv:1701.04525