ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 7, Issue 11, November 2018

# Development of New Smart City Applications using Blockchain Technology and Cybersecurity Utilisation

**Sakshi Sharma[1*], Natasha Dutta[2]**

Senior Project Manager, Midland Credit Management, San Diego, CA[1*]

Project Engineer, Online Micro Services, India[2]

**ABSTRACT:** In addition to integrating cutting-edge technologies to improve urban living, the quick expansion of smart cities poses serious cybersecurity challenges. With its decentralised and unchangeable structure, blockchain technology provides strong answers to these problems and guarantees the safe and effective administration of smart city applications. The use of blockchain technology to improve cybersecurity in developing smart cities is examined in this article. Among the key areas of focus are decentralised IoT networks, data privacy and protection, secure identity management, and the use of smart contracts for automated services. The essay illustrates how blockchain may be able to handle particular cybersecurity risks by means of thorough case studies and analysis, guaranteeing the robustness and integrity of smart city infrastructure. The findings suggest that blockchain technology not only enhances the security of smart cities but also drives innovation and efficiency, paving the way for more resilient and sustainable urban environments.

**KEYWORDS:** Blockchain, Blockchain applications, Blockchain use cases, distributed digital ledger technology, Data transparency, Cryptographic security, Public service delivery, Data authenticity.

## I. INTRODUCTION

Blockchain technology, a paradigm-shifting innovation, has emerged as a formidable tool capable of transforming various aspects of contemporary digital infrastructure. Fundamentally, blockchain is a decentralized and immutable ledger system that ensures transparency, security, and trust in data transactions. Each transaction is cryptographically secured and linked to the previous one, forming a chain of records that is resistant to tampering and fraud [1]. This characteristic of blockchain makes it particularly well-suited for addressing the multifaceted challenges faced by emerging smart cities. As urban centers evolve into complex ecosystems driven by interconnected technologies, the need for robust cybersecurity measures becomes paramount. Blockchain's decentralized nature eliminates single points of failure, thereby enhancing the resilience of smart city networks against cyberattacks. Moreover, its transparent and verifiable framework fosters greater trust among stakeholders by ensuring that data integrity is maintained across various smart city applications. This includes secure identity management systems that protect citizens' personal information, efficient and transparent public service delivery, and the creation of decentralized Internet of Things (IoT) networks that can operate autonomously while ensuring data authenticity. By integrating blockchain technology, smart cities can achieve heightened levels of security, efficiency, and transparency, ultimately leading to more sustainable and resilient urban environments [2]. This transformative potential positions blockchain as a cornerstone in the development of future-proof smart cities, capable of seamlessly integrating cutting-edge technology with everyday urban life to create a secure, efficient, and trust-driven urban landscape. Traditional ledger technologies necessitate the presence of a trusted third-party intermediary, such as a banking institution, as illustrated in Figure 1. Conversely, blockchain-based technology operates on a peer-to-peer network, as depicted in Figure 2, thereby obviating the need for a centralized trusted third party to manage transactions. Issues like double-spending are effectively mitigated through the consensus mechanisms employed by miners, ensuring the integrity of transactions without the intervention of an intermediary, as evidenced in Figure 2. This decentralized approach enhances security and trust, making intermediary entities redundant in the transaction management process.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 7, Issue 11, November 2018

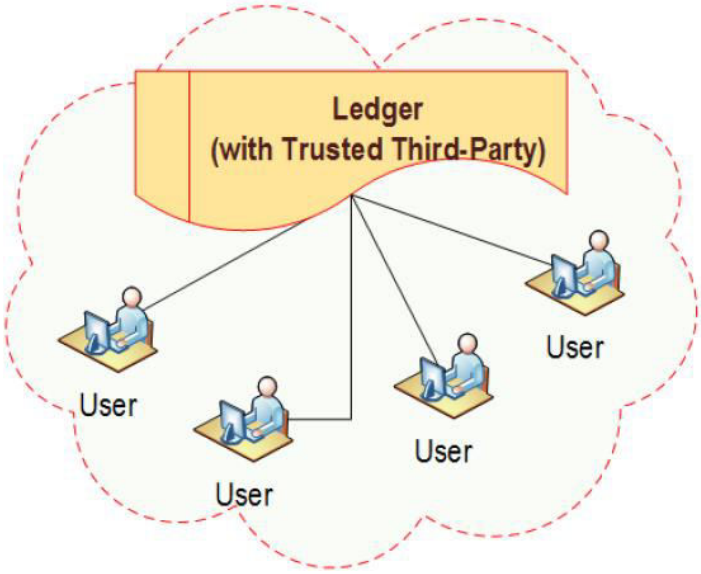


**Figure 1: Conventional centralized ledger technology reliant on a trusted third-party.**

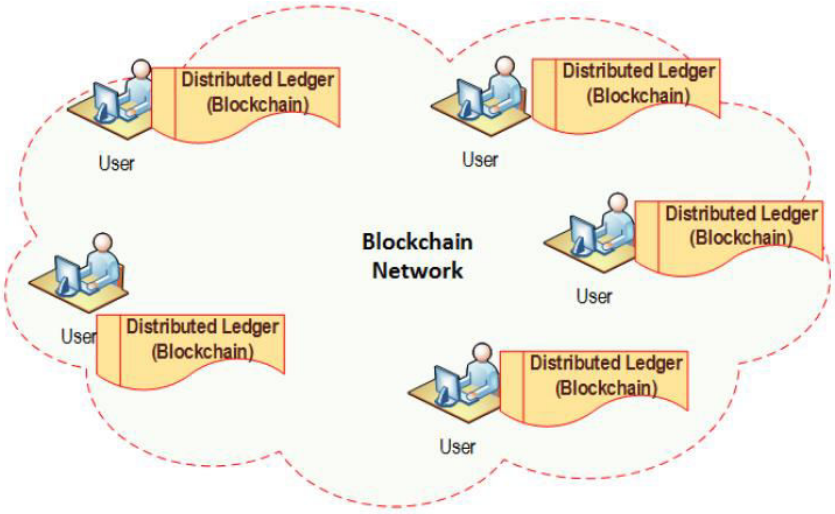


**Figure 2: A quintessential example of blockchain technology—distributed ledger technology—operating without a trusted third-party.**

While blockchain technology is predominantly associated with cryptocurrencies such as Bitcoin, its applications extend far beyond this realm. This transformative technology facilitates financial services without the need for traditional financial institutions, such as banks or other intermediaries, as illustrated in Figure 2. It can be harnessed to enable services like online payments, digital asset management, and remittance transactions. The core attributes of blockchain—decentralization, immutability, integrity, and anonymity—render it highly suitable for a wide array of non-financial applications. These include smart contracts, the Internet of Things (IoT), reputation systems, security services, wireless network virtualization, among many others. In this paper, we provide a succinct overview of the history and architecture of blockchain technology, followed by an exploration of its diverse applications and use cases across various domains. Despite the extensive discussion and acclaim this technology has garnered in both academic and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 7, Issue 11, November 2018

industry circles, comprehensive documentation of its emerging applications and use cases is sparse [3]. While several survey papers exist, they typically focus on either a specific subset of applications, security challenges, or a singular application domain. Here, we aim to bridge this gap by offering a broader perspective on the multifaceted potential of blockchain technology, underscoring its versatility and transformative impact across different sectors.

## II. ENHANCING CYBERSECURITY IN SMART CITIES WITH BLOCKCHAIN

In the intricate tapestry of smart city infrastructure, where diverse technologies converge to enhance urban living, cybersecurity emerges as a paramount concern. Blockchain technology offers a robust solution to these cybersecurity challenges through its intrinsic properties of decentralization, immutability, and transparency. In a smart city context, the decentralized nature of blockchain eliminates the reliance on a single point of control, thereby significantly reducing the risk of targeted cyberattacks. Each transaction within a blockchain is cryptographically secured and linked to the preceding one, creating an immutable ledger that is exceedingly difficult to alter or falsify. This ensures the integrity and authenticity of data across the myriad interconnected systems within a smart city. Moreover, the transparency provided by blockchain enables real-time verification and auditing of transactions, fostering a higher degree of trust among stakeholders [4-9]. The technology's capacity to create secure, decentralized networks can be particularly advantageous for managing Internet of Things (IoT) devices, which are often seen as vulnerable entry points for cyber threats. By using blockchain, each IoT device can be authenticated and authorized in a tamper-proof manner, safeguarding the entire network from unauthorized access and manipulation. Additionally, blockchain's smart contract functionality can automate and secure various urban services, from energy management to public transportation, ensuring that these services are both efficient and resilient against cyber threats. Thus, by embedding blockchain technology into the fabric of smart cities, we can fortify their cybersecurity posture, enabling these urban centers to thrive securely in an increasingly digital world.

### 2.1 Types of Blockchain and Consensus Mechanisms

Blockchains can generally be classified into permissioned and permissionless types.
Permissioned blockchains restrict access to a network where only pre-approved participants, designated by a controlling authority, are allowed to join. An example of a permissioned blockchain is the Quorum blockchain, which uses a consensus protocol known as Quorum Chain. This system relies on majority voting to reach consensus, making it relatively fast due to its efficient voting process.

Permissionless blockchains, on the other hand, are open to all participants. Bitcoin, which operates on a permissionless blockchain, uses a consensus mechanism called Proof of Work (PoW). This process requires all participants to contribute to the consensus, which can slow down the network due to the extensive computational work involved.

Blockchain technology encompasses various types, each tailored to specific use cases and operational paradigms, and employs diverse consensus mechanisms to validate and secure transactions within its network. Broadly, blockchains can be categorized into public, private, and consortium types. Public blockchains, such as Bitcoin and Ethereum, are characterized by their open, permissionless nature, allowing anyone to participate in the network as both users and validators, which enhances decentralization and transparency. Private blockchains, in contrast, are restricted to a select group of participants, providing greater control and efficiency but at the cost of some decentralization. Consortium blockchains represent a hybrid model where multiple organizations collaboratively manage the network, balancing decentralization with operational efficiency. Each type of blockchain employs distinct consensus mechanisms to achieve agreement on the state of the ledger, crucial for ensuring the integrity and security of transactions. Proof of Work (PoW), utilized by Bitcoin, relies on computationally intensive tasks to solve cryptographic puzzles, thus securing the network through significant resource expenditure. Proof of Stake (PoS) offers an alternative by selecting validators based on the amount of cryptocurrency they hold and are willing to "stake" as collateral, thereby reducing the environmental impact associated with PoW. Delegated Proof of Stake (DPoS) further refines this model by allowing stakeholders to elect a limited number of validators who are responsible for maintaining the blockchain, optimizing both scalability and efficiency [10-12]. Other mechanisms include Practical Byzantine Fault Tolerance (PBFT), which is employed in permissioned blockchains to achieve consensus through a voting process among pre-approved nodes, ensuring reliability even in the presence of faulty or malicious actors. Each consensus mechanism carries its own set of

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 7, Issue 11, November 2018

trade-offs concerning security, scalability, and decentralization, reflecting the diverse needs and priorities of blockchain networks across different applications.

### 2.2 Block Structure

Blockchain is a chronological sequence of block where each block holds a complete list of transactions, as shown in Figure 4. It follows the data structure of linked list, where each block points to a previous block through the reference of the hash value of the previous block, also called parent block. The first block of a Blockchain, the genesis block, has no block to point to. A block is composed of metadata (block header) and list of transactions (block body). The metadata includes block version, parent block hash, Merkle tree root hash, timestamp, and nonce [13]. Nonce is an arbitrary number which is used in the cryptographic communication within the user network.

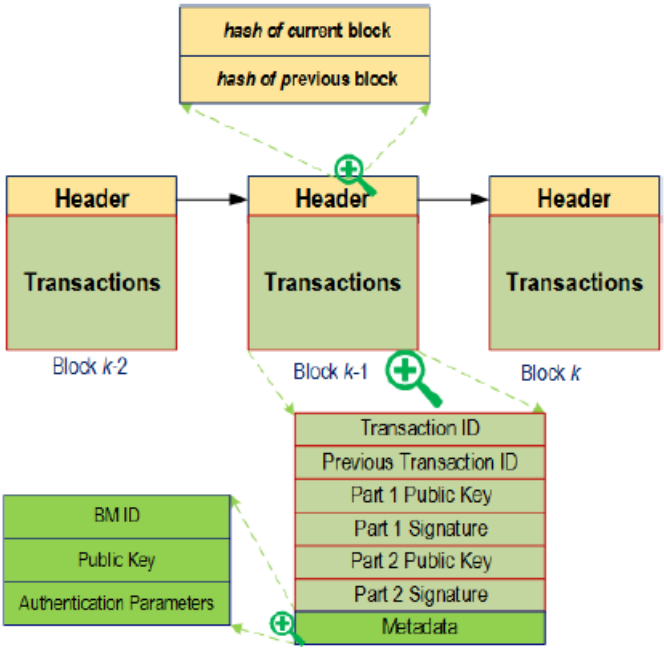


**Figure 3: Typical blocks in blockchain technology consist of a header and a transactions section.**

In blockchain networks, digital signatures are crucial for establishing secure communication between users. Each participant is provided with a pair of cryptographic keys: a public key and a private key. When a user initiates a transaction, they sign it with their private key, thereby authenticating its origin and ensuring its integrity. Recipients can then use the corresponding public key to verify the transaction's authenticity. This cryptographic approach safeguards the transaction's integrity within the network. A nonce (a number used only once) plays a critical role in the mining process within a blockchain [14-15]. It is an arbitrary value added to a block's hash to meet the network's difficulty requirements. The process of finding a valid nonce is computationally intensive and serves as a filter to exclude unqualified or less capable miners, thereby maintaining the network's security and efficiency.

## III. APPLICATIONS AND USE CASES OF BLOCKCHAIN

Following the successful deployment of blockchain technology in Bitcoin due to its notable features, blockchain has been proposed for a range of diverse applications and use cases, as illustrated in Figure 4. In the following section, we provide a concise overview of each of these domains.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 7, Issue 11, November 2018

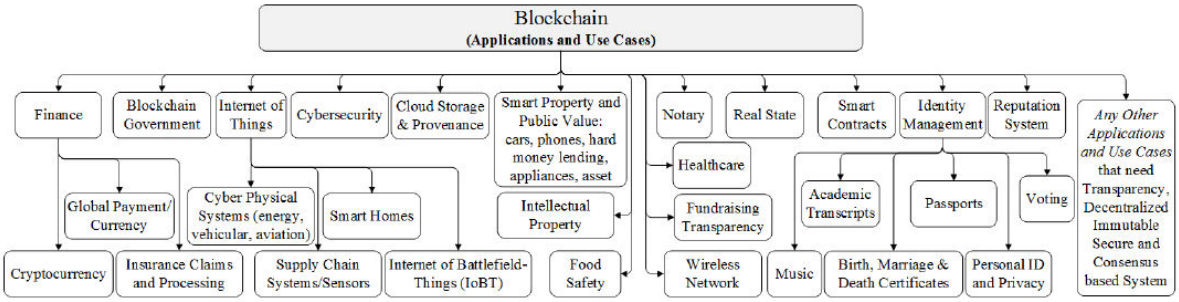


**Figure 4: Various applications and use cases of blockchain technology.**

### 3.1 Finance

Traditionally, financial transactions rely on intermediaries like banks, which can lead to inefficiencies and errors due to the need for multiple uncoordinated parties to manage and reconcile records. This centralization makes the process both costly and time-consuming. Blockchain technology addresses these issues by providing a distributed public ledger where transactions are verified through a "proof-of-work" consensus mechanism. Each node in the blockchain network maintains an updated copy of the ledger, ensuring transparency and immutability. Once a transaction is added to the blockchain, it cannot be altered, protecting it from tampering. In cases of conflicting chains, miners prefer the longest chain, which is considered more reliable. This decentralized and secure approach significantly enhances the efficiency and reliability of financial services.

#### 3.1.1 Cryptocurrency

Cryptocurrency, valued in the billions of dollars, is made possible by blockchain technology. Bitcoin, created by the pseudonymous programmer Satoshi Nakamoto, uses cryptographic techniques to enable secure transactions without the need for intermediaries like banks or PayPal. The Bitcoin network relies on a blockchain, a distributed public ledger, where new blocks are added through consensus mechanisms like Proof-of-Work. It is virtually impossible to derive someone's private key from their public key, preventing impersonation attacks. Transactions involve combining the recipient's public key and the sender's private key with the transaction amount. This transaction is broadcast to the network, where it is verified by other users who check the validity of the keys and ensure the sender has sufficient funds. This process makes it nearly impossible to create fraudulent transactions or spend someone else's bitcoins.

#### 3.1.2 Global Payments (Global Currency)

Global payments are often slow and costly due to the many intermediaries involved, leading to potential errors and inefficiencies. This centralization, where banks and financial institutions control and verify transactions, complicates the process. Blockchain technology addresses these issues by providing a decentralized public ledger and a robust verification method. In this peer-to-peer network, transactions are faster, verifiable, immutable, and more secure. Several remittance companies, such as Abra and Bitspark, are already leveraging blockchain technology to streamline their services.

#### 3.1.3 Insurance Claims and Processing

Insurance claims often face issues with fraud and the challenge of managing updated policies and data. Blockchain technology can streamline and secure this process using a distributed ledger. By requiring multiple participants to validate each transaction, blockchain effectively detects and prevents fraudulent claims. This ensures that legitimate claims are settled quickly and efficiently.

## IV. BLOCKCHAIN GOVERNMENT

Blockchain technology can enhance government operations by fostering transparency, accountability, and trust among stakeholders such as citizens, leaders, and officials. By providing a decentralized public ledger, blockchain allows for

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 7, Issue 11, November 2018

real-time access to government data, addressing accountability issues and exposing misconduct. According to McKinsey, making open data available can yield substantial economic benefits and enable the public to scrutinize services like healthcare and food supplies. However, releasing data infrequently limits its impact. Blockchain offers a solution by continuously distributing data on a public ledger and using smart contracts to ensure that elected officials fulfill their promises based on their electoral commitments. This approach enhances transparency and holds officials accountable.

### 4.1 Internet of Things (IoT)

The rapid growth in the number of electronic devices connected to the Internet is creating the Internet of Things (IoT), which has the potential to revolutionize daily life with concepts like smart homes. However, this surge in interconnected devices raises significant cybersecurity and privacy concerns. Blockchain technology can play a crucial role in securing the IoT by ensuring that data transmitted across these devices remains secure and that participants are accountable.

#### 4.1.1 Energy Cyber Physical System

Smart energy grids are evolving into complex cyber-physical systems with bidirectional interactions between power generation, distribution, utilities, and users. Blockchain technology offers a secure and verifiable framework to support these interactions within energy CPS.

#### 4.1.2 Vehicular Cyber Physical System

Vehicular cyber-physical systems are fundamental to intelligent transportation, unmanned aerial vehicles (UAVs), and autonomous driving, enhancing road safety and traffic efficiency. Given that vehicles are linked to sensitive personal information, security and privacy are critical concerns. Blockchain, with its decentralization, immutability, and cryptographic features, can create a smart and secure framework for autonomous transportation systems.

#### 4.1.3 Blockchain in Aviation Systems

In the aviation industry, blockchain can facilitate secure, collaborative partnerships among service and product providers. Smart contracts can streamline interactions between businesses and their various units.

#### 4.1.4 Supply Chain Systems/Sensors

Smart sensors are increasingly used by supply chain companies to track global shipments, with their numbers expected to grow rapidly. This will generate vast amounts of data that need to be collected and analyzed. Blockchain technology can significantly enhance the efficiency and security of supply chains by managing and securing this data.

#### 4.1.5 Smart Homes

Blockchain can enhance the security and reliability of smart home operations with IoT devices. However, implementing blockchain in these resource-constrained IoT systems is challenging due to the high resource demands of proof-of-work, limited storage, low latency, and scalability issues.

#### 4.1.6 Internet of Battle-Field Things (IoBT)

The Internet of Battlefield Things (IoBT) is essential for smart defense and warfare, integrating diverse devices like combat equipment, UAVs, ground vehicles, and sensors to provide real-time, secure, and immutable intelligence. This diversity presents challenges in ensuring secure, privacy-aware, and trustworthy battlefield operations. Blockchain technology can address these challenges, enhancing the security and reliability of IoBT systems.

### 4.2 Cybersecurity

Cybersecurity involves protecting computer systems, networks, and data from digital attacks, theft, and damage. It encompasses various measures and practices, including encryption, firewalls, and intrusion detection systems, to safeguard sensitive information and ensure the integrity, confidentiality, and availability of data. As cyber threats evolve, cybersecurity continuously adapts to address new vulnerabilities and safeguard against malicious activities.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 7, Issue 11, November 2018

### 4.3 Smart Property and Public Value

Blockchain technology can represent and track various assets such as houses, land, and automobiles by recording all operations and property records on a decentralized ledger. Once entered into the blockchain, records are shared with all relevant parties, facilitating contract creation and verification. This decentralized approach ensures that lost records can be quickly recovered and duplicated from the network.

#### 4.3.1 Hard Money Lending

Hard money lending helps people with short-term financial needs by using real estate as collateral. Ensuring the legitimacy of the collateral and agreement is crucial, as lenders risk losing money and borrowers may face property loss due to fraudulent policies. Blockchain can address these issues by encoding property details and policies on a transparent and secure ledger. This enables trustworthy transactions with strangers. Smart contracts on the blockchain can further ensure the integrity of these agreements.

#### 4.3.2 Cars and Phones

Personal devices and cars use authentication keys for security, but these methods can fail if keys are stolen or copied. Blockchain technology can address these issues by allowing users to replace and replicate lost credentials securely on the ledger.

#### 4.3.3 Smart Appliances

Smart appliances, equipped with cyber systems, can communicate information about their environment and usage, exemplified by a "talking toaster" that provides relevant usage data. A home with these connected devices is termed a smart home, where the cyber-physical system optimizes device functionality for user benefit. Encoding these smart appliances on a blockchain as smart property ensures clear ownership and management of these devices.

#### 4.3.4 Asset Management

Asset management involves multiple parties maintaining transaction records, leading to inefficiencies and errors, especially with cross-border transactions. A distributed ledger can address these issues by allowing each party to hold a copy of the complete transaction history, updated through cryptographic communication. This approach enhances efficiency and reduces costs by eliminating the need for intermediaries.

### 4.4 Cloud Storage and Provenance

Blockchain can record metadata on file creation and all operations, including access activities, and share this information with stakeholders. This data provenance is crucial for applications requiring accountability and forensics. For example, changes made to collaborative documents, like those in Google Docs, can be tracked and stored on the blockchain. This ensures integrity and accountability in cloud storage and processing by preserving a complete, immutable record of all edits and changes.

### 4.5 Intellectual Property

An Intellectual Property management system can use blockchain technology to enforce provable rights, providing verifiable, immutable, and secure records to resolve disputes.

### 4.6 Food Safety

Food safety is a major concern, with over 600 million people falling ill and around 1,167 dying daily from contaminated food. Blockchain technology can combat counterfeiting and enhance visibility throughout the food supply chain, allowing consumers to access accurate information about food content, origins, and expiration quickly. This improves control, accuracy, and transparency, enhancing overall food safety.

### 4.7 Blockchain Notary

Blockchain, utilizing distributed ledger technology and cryptography, replaces traditional trusted third parties like notaries. It automates the notary process, making it more cost-effective, transparent, and secure.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 7, Issue 11, November 2018

**4.8 Blockchain in Healthcare**
Blockchain can securely store personal health records with private keys for authorized access only, ensuring confidentiality and compliance with HIPAA laws. It facilitates secure data sharing between patients, insurance providers, and doctors.

**4.9 Fundraising and Transparency**
Blockchain enhances transparency, security, and integrity in fundraising by providing an immutable and verifiable ledger of transactions.

**4.10 Wireless Networks and Virtualization**
With the growth of IoT and CPS, blockchain can manage wireless resources like RF slices, ensuring verifiable allocation and preventing double spending.

**4.11 Real Estate**
Blockchain offers a modern solution for property title recording, replacing traditional methods with a distributed ledger system.

**4.12 Smart Contracts**
Smart contracts, encoded in Ethereum Virtual Machine bytecode, automate and enforce agreements without intermediaries. Miners verify transactions through consensus protocols like proof-of-work, ensuring decentralization and compliance.

**4.13 Identity Management**
Academic Records: Blockchain can store immutable and secure academic records.
Blockchain Music: It provides a transparent database of music rights and royalty distributions using smart contracts and digital currency.
Certificates: Birth, marriage, and death records can be securely encrypted and managed on blockchain.
Passports: Blockchain-based passports allow secure, verified identity sharing via digital signatures.
Personal Identity and Privacy: Blockchain can protect personal data by encrypting and securing it against unauthorized access.
Personal ID: Blockchain can consolidate various physical IDs into a single digital identity.
Voting: Blockchain can create secure, verifiable voting systems, allowing for confident and remote voting.
Reputation System: Blockchain can maintain a tamper-proof, distributed ledger of transactions, ensuring the integrity and fairness of reputation systems.

## V. SUMMARY

Blockchain technology has broad and transformative applications across various sectors. In healthcare, it secures personal health records and facilitates compliant data sharing. For fundraising, blockchain ensures transparency and integrity by providing an immutable ledger. In wireless networks, it manages resources efficiently, preventing double-spending. Real estate benefits from blockchain's ability to record property titles securely. Smart contracts automate and enforce agreements without intermediaries, with miners verifying transactions through decentralized consensus mechanisms. In identity management, blockchain enhances security and efficiency for academic records, music rights, certificates, and passports. It also consolidates personal IDs into a single digital format and can safeguard personal data and privacy. For voting, blockchain offers a secure and verifiable system for remote participation. Lastly, in reputation systems, blockchain maintains an unalterable record of transactions, ensuring fair evaluations and trustworthiness.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 7, Issue 11, November 2018

## REFERENCES

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf
2. Morris, D.Z. Bitcoin Hits a New Record High, But Stops Short of USD 20,000. 17 December 2017. Available online: http://fortune.com/2017/12/17/bitcoin-record-high-short-of-20000/
3. Asuvaran & S. Senthilkumar, "Low delay error correction codes to correct stuck-at defects and soft errors", 2014 International Conference on Advances in Engineering and Technology (ICAET), 02-03 May 2014. doi:10.1109/icaet.2014.7105257.
4. S. Senthilkumar, R. Nithya, P. Vaishali, R. Valli, G. Vanitha, & L. Ramachanndran, "Autonomous navigation robot", International Research Journal of Engineering and Technology, vol. 4, no. 2, 2017.
5. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.
6. Zhang, Y.; Wen, J. An IoT electric business model based on the protocol of bitcoin. In Proceedings of the 2015 18th International Conference on Intelligence in Next Generation Networks, Paris, France, 17–19 February 2015; pp. 184–191.
7. Sharples, M.; Domingue, J. The blockchain and kudos: A distributed system for educational record, reputation and reward. In European Conference on Technology Enhanced Learning; Springer: Berlin/Heidelberg, Germany, 2016; pp. 490–496.
8. Noyes, C. Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning. arXiv 2016, arXiv:1601.01405.
9. Malomo, O.O.; Rawat, D.B.; Garuba, M. Next-generation cybersecurity through a blockchain-enabled federated cloud framework. J. Supercomput. 2018, 74, 5099–5126. [CrossRef]
10. S. Senthilkumar, C. Nivetha, G. Pavithra, G. Priyanka,S. Vigneshwari, L. Ramachandran, "Intelligent solar operated pesticide spray pump with cell charger", International Journal For Research & Development In Technology, vol. 7, no. 2, pp. 285-287, 2017.
11. Rawat, D.B.; Alshaikhi, A. Leveraging Distributed Blockchain-based Scheme for Wireless Network Virtualization with Security and QoS Constraints. In Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 5–8 March 2018; pp. 332–336.
12. Divya, M.; Biradar, N.B. IOTA-next generation block chain. Int. J. Eng. Comput. Sci. 2018, 7, 23823–23826.
13. S. Senthilkumar, L. Ramachandran, R. S. Aarthi, "Pick and place of Robotic Vehicle by using an Arm based Solar tracking system", International Journal of Advanced Engineering Research and Science, vol. 1, no. 7, pp. 39-43, 2014.