**Blockchain for securing the communications in 5G**

Submitted by: Mani Sekhar Kothapalli

Instructor: Dipak Biscuitwala

Webster University

**Part-1**

**Introduction**

Human communication needs fifth-generation wireless networks (5G) to provide fast data transfer and improve connection while reducing latency because 5G must establish security measures against cyberattacks and data security infringements. The protection of sensitive information from unauthorized access requires immediate consideration since decentralized communication security needs persist in current times.

The 5G communication systems obtain powerful danger protection because of Blockchain technology integration. The distributed decentralized system functions of blockchain provides secure verified data exchange through tamper-proof transparent protocols because it operates as a distributed decentralized system. Blockchain's built-in data security characteristics including cryptography and consensus methods with immutable features prove to be an optimal solution for defending 5G networks (Nguyen et al., 2020). Blockchain technology applied to 5G networks enables a protected decentralized communication system which defends sensitive information from invasive access by unauthorized parties.

Through 5G network integration with blockchain technology we can achieve a revolutionary evolution in communication systems.In a Blockchain-powered 5G networks completely eliminate the need of middlemen and authorized central entities for creating secure operational telecommunications systems. The secure transmission of 5G networks becomes possible through blockchain technology which generates a visible platform for performing real-time traffic monitoring. The paper analyzes how blockchain applications serve to protect 5G communication systems. The paper assesses blockchain implementation in 5G spectrum while evaluating potential future integration barriers by identifying available deployment strategies. This study evaluates blockchain solutions developed for 5G networks as well as regulatory integration needs for the existing framework.

**Selecting the research topic**

**Area of intended research:**

The research consists of deploying blockchain technology to establish security solutions for 5G communication networks. Research analysis shows that blockchain technology allows 5G networks to maintain secure decentralized communication functions with transparency (Haddad, n.d.). The research evaluates blockchain implementations of data packet security and user access identity protection and access acquisition through 5G networks. The study examines blockchain technology deployment for 5G networks through an analysis of current blockchain usage together with its implementation spread across network frameworks and safety protocols and edge processing systems and distributed environments. Individual blockchain-based 5G network implementation scenarios with IoT security systems and decentralized edge computational infrastructure and network partition protection make up the research focus.

**Brief review of the literature:**

5G wireless networks of the fifth generation approach global implementation across the world. The 5G technology aims to provide numerous vertical applications by establishing network connectivity systems that enable heterogeneous devices and machines to share fast service quality improvements while using enhanced network capability and better system throughput (Nguyen, 2020). Security experts and organizations have recognized various challenges with 5G systems that involve network privacy weaknesses and distributed system architecture and poor information transparency and data integration issues. The traditional security strategies demonstrate inadequate abilities for managing 5G security requirements. The usage of 5G technology primarily exists in heterogeneous networks with massive ubiquitous devices which demands secure decentralized solutions.

Through the Internet-of-Things (IoT) ubiquitous computing enables Internet access in all application environments which include e-Health and smart cities and cyber physical systems etc. 5G network implementation enables real-time objects to obtain rapid data transfers through this technology. Data processing takes place after scheduled data collection runs to enable management of access through an exclusive network protocol that pulls information across various domains. A different entrance system is needed for industrial usage as present alternatives support only traditional central control networks. This complicated computing system results in deteriorating performance during device-to-device (D2D) transmission. The industrial sectors give prime importance to privacy and security fundamentals because they need these requirements to run their costly operations yet protect themselves against destructive cloud servers. Maximizing communication efficiency involves appropriate coordination of real-time objects with each other.

**Research Question:**

What are the effective approaches to unite blockchain systems with 5G networks for secure decentralized communication functions that resolve regulatory problems and deployment restrictions?

**Personal Interest and Narrow the scope**

The evaluation of "Blockchain for Securing Communications in 5G" holds my interest because I need daily access to Internet data storage services. I must prioritize network security because I handle cloud storage platforms and applications every day. The study focuses on blockchain technology as its major research subject to analyze its protection capabilities for 5G communication systems while omitting alternative security mechanisms during its investigation into network development for solid 5G infrastructure. My study investigates blockchain technology deployment in 5G security with the goal of discovering modern solutions to counteractive threats and vulnerabilities. Stakeholders who encompass telecom providers and policymakers and cybersecurity specialists will gain essential information from the research findings. My professional goal involves providing value so the 5G network ecosystem will have dependable security capabilities and operational safety.

**Research Problem Selection**

**IT Topic Area:**

Blockchain serves to safeguard 5G Communications Networks constituting an investigation area within Cybersecurity and Telecommunications research domains. The paper investigates blockchain system execution to boost 5G communications network security while improving dependability.

**Applicable Industries**:

The study highlights the blockchain technology which is used to secure the networks, that has great impact in cyber security fields, finance, telecommunication, healthcare and government sectors. The providers who are using this 5G network can use this blockchain to make sure that the system is more secure and reliable. The companies who need more security can develop blockchain tools to protect 5G networks from cyber threats. In various fields like banking and health care, the combination of 5G and blockchain creates a great network for mobile banking, telemedicine, remote health monitoring, and protecting medical records. It is a very important point to consider because it's secure infrastructure, public safety and national defense.

**Competitive Environment and Rationale**

The blockchain market segment for 5G network security solutions has experienced fast-paced change as multiple organizations from telecommunications to cybersecurity industries and tech corporations pursue market dominance. The growing popularity of blockchain technology has not been accompanied by sufficient research that investigates its application for 5G communications networks security. This research adds to current knowledge by carrying out a detailed examination of blockchain technology capabilities that boost 5G network security and reliability. This research investigates blockchain-based 5G network security solutions so stakeholders can make well-informed decisions to maintain their position in the swiftly developing 5G market.

**Premise and alignment with Core ITM Curriculum**

Research is based on the belief that blockchain technology presents major potential to transform 5G network security by establishing reliable applications necessary for building secure trustful 5G infrastructure. The research investigates blockchain technology for 5G network security while exploring advantages, barriers, open possibilities as well as innovative approaches to new threats and vulnerabilities in the network. The study fits directly into fundamental ITM educational objectives which focus on Information Technology Management, Telecommunications and Cybersecurity concepts. This investigation brings together blockchain technology with 5G and cybersecurity to fulfill key educational goals presented in the ITM curriculum about system analysis and technology assessment and developing practical solutions for IT challenges.

**Definitions**

1.     Blockchain: Blockchain is the distributed platform that safeguards multiple interaction histories on interconnected systems using parallel execution that delivers transparent documentation features (What Is Blockchain?, n.d.).

2.      5G Network: The advanced network technology is known as the fifth generation(5G ) that operates as a platform to boost data transmission speed and reduce delays and extend mobile connectivity possibilities (What Is a Decentralized Network?, 2022).

3.     Security Threat: Any incident creating data exposure risks through unidentified access attempts or cyber-attacks or harmful software that leads to system security breaches.

4.      Decentralized Network: A decentralized structure works through peer-to-peer linking where participants validate network transactions.

5.     Data Encryption: It is the technology in which simple text is converted into impenetrable ciphertext numbers to keep data protected against both unauthorized acquisition attempts and interception events.

**Delimitations**

* This study avoids discussions about diverse defense approaches and technical structures as it mainly focus on finding platform blockchain solutions for protecting 5G communication infrastructure standards.
* Withoutanalyzing regulatory compliance or financial impacts or social societal aspects of integration, this research only explores technical approaches to integrate blockchain systems with 5G networks.
* This study examines a standard 5G network with present using protocols and utilizes existing designs so don't provide information about alternative technological routes.
* The study functions under the assumption that blockchain development for 5G networks will take place in existing standards and protocol frameworks.
* Security hazards data breaches and cyberattacks and unauthorized access represent the whole focus in this research as different threats are excluded from study.
* The research accepts blockchain integration systems operating together using current prototypical data requirements and technical rules.

**Limitations**

* This study faces technical barriers because blockchain technology stands in its current development phase and 5G network integration efforts remain unfinished.
* The research assumes blockchain implementation which meets standard protocols while ignoring potential technical limitations.
* The implementation success of this research struggles due to insufficient 5G network security vulnerability and threat data which are inconsistent.
* This research uses primary research data and literature materials as its starting point but experimental evidence is needed to assess blockchain technology's integration with 5G networks.
* The research faces constraints from the theoretical frameworks used to study the security benefits of blockchain technology integration within 5G networks.
* This study uses frameworks and models which it takes code as accurate but fails to evaluate alternate theoretical views or operational principles.
* The research evaluates security advantages of blockchain within 5G networks but it does not explore application of discoveries to outside sectors or industries.

**Chapter- 2**

**Introduction to Research Methodology**

The research is mainly done to answer a few questions and solve various problems carefully by understanding and analyzing information. It is nothing but the way the researchers choose to conduct the study, which plays very important key role in completing the project on time. Creating a clear plan makes the research successful, it also shows as a guide to reach the research goals. Without a proper plan, the research might go out of track and it can affect the accuracy and the effectiveness. Hence, it is very important to use correct methods and follow schedules, that fits the topic. It explains the use of research methods in this research, including the tools, materials and ethical considerations that guides the study.

## Methodologies and Design of Research

The main aim of the research project is to study the topic and gather the appropriate information to get the results. But choosing the right method is very important, in finishing the study on time. Having a poor plan can make this research to mistakes and the entire project will be ineffective. Thus, the well structure and effective research plan is very important and acts as the map for completing the research successfully. It is also very important to use the right methods and create a plan that fits the specific research topic. This paper provides a clear explanation of the research methods used, the resources available, the problems and the study aims to solve.

## Primary Research Methodology

To become successful in this study choosing the right research method is very important. The research method is nothing but that helps us to understand the topic better and solve few issues of this study. They provide clear and accurate results, by answering the important questions of the research for this study. I am choosing a descriptive research method because it gives a detailed picture of the current situation and helps to identify the research problems in the current era. To get useful information, I plan to conduct a few surveys with the IT industry workers who are having real experience in few projects. This professional works on different software projects and has great experience on the applications they develop. The survey will help to identify the challenges that prevents employees from following security process in the organization. I will distribute these surveys to employees in my network and also include few questions to gather meaningful insights.

In addition to using questionnaire for my study, I also plan to apply these research techniques with the target group of 20 participants. These observations will be integrated into my research to strengthen this study and provide deep understanding of the issues that have been examined. The combination of surveys and observational research will give a comprehensive understanding of blockchain security. Hence this approach will help me to draw an insightful conclusion by ultimately enhancing the overall quality of the research.

## Secondary Research Methodology

The most important part of my study is the secondary research methods. It allows me to explore and build the knowledge and findings of experts in the field. In today's digital era, there is a huge amount of information available in books, research papers, journals, and websites that give valuable information on a particular topic. I plan to review various journal articles written by professionals and software testing experts. This is because to deepen my understanding and strengthen my research. The secondary research method is both flexible and cost effective that can make a practical way and also supports the primary research method.

The main goal of my study is not only to enhance the knowledge about the blockchain security, but also serve as an educational resource. The results of this research will give the impact of weak security practices, which can be practically beneficial for a few small businesses. By analyzing how large organizations have faced security issues due to their inadequate measures, the research can also help to raise such awareness and encourage adoption of strong security, protocols. Finally the research contributes to improvement of blockchain security standards.

**Research Methodologies:**

Primary research: Survey

Secondary research : Literature Review

**Design Research Instruments and data collection plan, Data analysis plan.**

## Data Collection

## The data collection method of my research involves two separate approaches to uncover more details about analyzing Blockchain technology security. The surveys implemented in my primary research allow me to engage with IT industry professionals. Both survey methods are distributed to the area residents. The primary information sources deliver real-time security procedures knowledge along with direct descriptions of blockchain technology limitations.

## Research at the secondary level enhances the initial discovery findings through indispensable supplements. The necessary achievement requires detailed analysis of academic papers together with scholarly magazines and reliable websites. I examine software instruments coming from established software technology companies. The findings from secondary research enhance first-hand data while presenting the complete picture of the study.

## Data Analysis

The result of research heavily depends on the analysis procedure. Useful information extraction from large data collections depends on this process. The analytical process reveals a full understanding when researchers thoroughly analyze and contrast findings obtained from primary investigations with those from secondary investigations. The analysis tools allow researchers to detect essential patterns and important data that solve the research issues. Researchers examine each type of data which includes responses from polls in addition to questionnaires as well as scholarly writing and business websites. This methodical research approach will lead me to well-found insights that build upon my understanding of Blockchain security value assessment.

**Part-2**

**Introduction**

The fast development of 5G communication networks has revolutionized industries because it provides speedier data sharing together with reduced delays and improved connections. 5G network advancements have brought forth major security problems that encompass data breaches together with cyberattacks and unauthorized system entry. Today's security solutions are insufficient for 5G networks because those networks have multiple centers and interconnect thousands of devices. Blockchains have risen as a likely technique to strengthen 5G network security. The distributed platform of blockchain establishes transparent authentication systems that protect exchanged data and defends networks from possible attacks. The study examines using blockchain technology to establish secure 5G network communications as it resolves key security challenges.

The evaluation of blockchain security solutions for 5G networks analyzes both opportunities and difficulties and deployment restrictions that exist when implementing these solutions. Blockchain technology achieves authentication combined with data protection through these three fundamental elements and smart contracts. The study examines how Information Technology Management (ITM) security planning and procurement and system analysis procedures facilitate blockchain implementation into 5G infrastructure. The study deduces blockchain effectiveness for securing next-generation networks through extensive research of existing documents. This investigation leads to enhanced security development of distributed and secure 5G telecommunication systems able to defend against present and future cyber threats.

**Thesis Statement:**

The research examines blockchain technology implementation to secure 5G communication networks including its ability to establish a secure decentralized transparent foundation for communication while overcoming data breach and cyber attack and unauthorized access threats. This research evaluates blockchain security applications within 5G networks through investigation of security benefits and implementation barriers that affect 5G communication security while exploring blockchain potential to strengthen security and enhance transparency and decentralization of 5G networks. The thesis works to develop safe decentralized 5G communication systems and supports regulatory standards which handle blockchain implementation in 5G networks.

**Role of Literature Review:**

The research paper critically depends on its literature review to catalog all blockchain technology uses for 5G communication security that academic literature supports. The literature review evaluates papers along with articles and books to determine both benefits and challenges of blockchain technology adoption in 5G networks with emphasis on applications and designs and security features.

Numerous studies explore current 5G security threats as well as unauthorized entry and data breaches in today's communication networks. The review explains how blockchain technology combat security risks. Research limitations in this analysis serve to develop vital conceptual design elements that secure 5G telecommunication systems by utilizing blockchain technology. The research paper builds its analysis of blockchain technology protection for 5G networks through the findings in the literature review.

Multiple Information Technology Management (ITM) components will be used to build secure blockchain networks that integrate with 5G systems. The objective of ITM security is to preserve data confidentiality and maintain its integrity together with availability. At the same time ITM management enables the planning and execution of blockchain-based security systems. The evaluation of vendors and solutions for procurement needs thoughtful assessment and the ITM system analysis and design process will deliver useful solutions matching system requirements.

**Literature Review:**

5G network stands as a primary foundation for multiple key industries that include IoT along with smart cities and virtual reality and others. 5G executes its operations through complex digital technologies including massive Multiple Input Multiple Output (mMIMO) while operating across higher radio frequencies. Network operators face new complexities with advanced 5G features and new technologies due to which Artificial Intelligence represents an effective solution to manage these complexities. Security challenges have emerged through AI implementation in 5G while the new network generation needs standardization adjustments to qualify its features. Implementation of Blockchain represents the solution to address these challenges(Azzaoui, 2020). Blockchain operates as a distributed technology to enable safe information distribution and resource exchange within multiple 5G network nodes. Blockchain enables support for other technologies such as AI-based 5G networks to develop cellular networks that achieve enhanced efficiency alongside improved security.

New opportunities emerge from smart transportation systems which create simultaneous challenges for vehicular ad-hoc networks (VANETs) during vehicular Internet of Things (IoT) service delivery. Network performance enhancement needs a viable security solution for trust management alongside comprehensive protection of user privacy. Many consider the emerging 5G mobile communication system to represent an exceptional technology for providing ultra-reliable wireless communication services with fast response times(Xie & Ding, 2019). The integration of software-defined network (SDN) architecture into 5G-VANET enables the system to obtain data from a worldwide scale and exercise network control. Real-time IoT services on transportation monitoring and reporting receive effective support from such systems. The innovative vehicular security system benefits from these two advancements.

Users trust fifth generation (5G) cellular network for its promising quality of services because security remains their main concern in applications like education banking and health etc. Both cellular networks depend on registration and authentication protocols and key agreements because subscribers verify their relationship with the network using shared encryption keys(Haddad, 2020). Third Generation Partnership Project (3GPP) developed security specifications for the user authentication with the provider. Research groups identified target protocols because security issues had not been resolved so they provided suggestions for authentication and key agreement procedures. Experts in present times consider blockchain as an essential emerging innovation that will dramatically transform human existence during forthcoming days. Blockchain grants its security properties such as authenticity and integrity to various applications such as bitcoin, smart contracts, etc.

High-quality user services are enabled by 5G cellular networks because of their rapid data transmission and minimal time delays. This upcoming network will manage IoT devices while creating new health-related services as well as banking and educational applications. To ensure their stability security remains mandatory given that exploitable vulnerabilities could disrupt operations with consequences for daily human life. Any cellular network faces cyberattacks most frequently against its Authentication and key agreement (AKA) as well as its handover (HO) protocols. Blockchain functions as a peer-to-peer network which operates to create an unalterable secure record system. Many applications will increasingly adopt this newly developed technology for their security needs(Haddad & Baza, 2021). The research undertakes a development of blockchain-based secure and efficient AKA schemes with uniform handover protocols for 5G networks. The proposed scheme keeps the home network (HN) outside AKA procedure and HO protocol operations for two reasons: first to defend HN from denial-of-service attacks and second to minimize communication and computational costs. Our HO protocol operates uniformly as it serves all scenarios of handover. The proposed method attains efficiency through its limited data requirements during operations. The proposed method enables forward/backward secrecy among its capabilities. The blockchain system functions to authenticate the public keys of the network nodes thus helping to protect our AKA scheme and HO protocol. The network needs the user location information for proper functioning therefore the system records these positions.

The fifth-generation (5G) technology now brings out IoT applications for smart transportation and healthcare alongside virtual and augmented reality experiences to build better Quality of Service (QoS) alongside user experience. 5G-enabled IoT revolution brings various attributes to the network through enhanced data rate along with decreased latency and better system capacity and reduced power usage. Such revolutionary changes result in substantial data growth thus creating an essential need for intelligent and effective data analytic operations throughout the network(Rathore, 2021). Data growth creates two significant challenges in network security and privacy because it increases the risks of data breach along with sensitive information loss. Traditional data analytic techniques together with security protocols fail to fulfill the requirements of 5G-enabled IoT due to its specific need for minimal delays and high bandwidth.

Mobile operators need subscriber authentication as their basic operation before they provide services to end users. The authors suggested a new blockchain implementation of the Authentication and Key Agreement (AKA) protocol to enable 5G network roaming services. Every Home Network supplies its autonomous smart contract information which helps other operators provide roaming functionalities to its subscriber base. The smart contract functions enable complete communication operations between the Home Network and Serving Network subscribers. The proposed protocol removes the requirement of a protected communication path between the HN and SN because this serves as the main demand of current 5G AKA systems(Hojjati, 2020). The HN and SN first need to create a secure session before using the AKA protocol as per secure channel standards. The proposed protocol benefits from blockchain functionality that includes audited logs as well as decentralized operation alongside Denial of Service (DoS) protection. The authors used ProVerif for formal verification to establish a security proof of their approach.

5G networks will form the communications backbone because they integrate with multiple services including SDN and NFV coupled with cloud computing and MIMO systems. The combination of various services with 5G networks creates vital security and privacy problems for these networks(Haddad, 2023). A security and privacy authentication protocol using pseudonyms and blockchain was proposed for 5G networks throughout this research. Security analysis results demonstrated the proposed scheme achieved security together with privacy protection against various attack methods. Performance evaluation indicates that the proposed scheme outperforms current existing specifications.

The 5G network provides quick Internet speeds while ensuring reduced network delays and coverage for both indoor and outdoor Smart City areas. The 5G wireless technology shows potential for changing Wi-Fi networks and replacing Bluetooth geolocation systems because of continuous network span construction which enhances IoT service delivery. The market already features Wi-Fi 6 as a solution for IoT applications(Serrano, 2020). New Smart City applications based on Big Data will function through 5G as their mobile Internet service provider thus removing the requirement for extra private network infrastructure or mobile network deployment. Better access to networks as well as improved device connection speeds create intrinsic risks to network security. Cyber attackers will receive more digital targets because wireless and mobile network access channels will be utilized by separate services.

Future wireless network technologies depend largely on two promising technologies which are Blockchain and AI. A resource sharing environment with secure decentralized characteristics emerges through blockchain functionality. The exploration of AI offers new solutions to problems that contain uncertain characteristics together with time-dependent and complex attributes. These technologies have become increasingly popular during the last period. By uniting these two techniques the performance achieved by wireless networks will receive additional improvements. This article suggests a secure intelligent next-generation wireless network design through blockchain and AI deployment in wireless systems and resource sharing function(Dai, 2019). The authors introduced a content caching problem solution which maximized system utility using blockchain technology along with deep reinforcement learning to develop a new caching scheme. The proposed scheme achieves favorable results according to numerical outcomes.

Balancing technology needs two revolutionary components: 5G supplies users with high speeds and quality of service and blockchain creates peer-based security and trust protocols. The requirements for speed and bandwidth and latency measurement differ among the applications which consider using 5G technology. The application of 5G technology for reliable and fast communication occurs primarily in augmented reality as well as self-driving vehicles and additional ioT applications (Praveen et al., 2020). The authors in this article explain the specific blockchain applications that could improve 5G service security and privacy delivery to users. The document discusses present obstacles related to 5G deployment as well as blockchain-based solutions for these challenges. Additionally the article includes a 5G blockchain implementation model for Multi-Operator Network Slicing in 5G networks.

**Hope to Learn from this Research Paper:**

The research paper explores "Blockchain for Securing Communications in 5G" to extend current understanding of blockchain applications used for 5G security. I aim to comprehend the advantages and technical limitations of implementing blockchain technology within 5G networking systems and the present security threats for 5G networks with insights into blockchain mitigation techniques for these security risks. My information acquisition focuses on how blockchain security solutions handle their design process and security implementation for 5G networks. The achievement of my learning goals depends on implementing ITM Security in combination with ITM Management and ITM Procurement along with ITM System Analysis and Design components. I will examine distributed blockchain security mechanisms for 5G networks through the study of encryption systems and authentication protocols and authorization processes in ITM Security. The analysis examines blockchain-based security solution management for 5G networks by studying planning execution control activities as well as organizing functions. Security solution procurement for 5G blockchain networks will receive separate detailed evaluation along with vendor selection and contract administration. The mixed-system architecture design along with security function analysis of blockchain-based 5G solutions will serve as the conclusion of my research. The Information Technology Management elements help me acquire thorough knowledge about blockchain technology security in 5G communications while discovering different implementation choices and research directions.

**References:**

Azzaoui, A. E. (2020). Block5GIntell. *IEEE*, *8*. 10.1109/ACCESS.2020.3014356

Dai, Y. (2019). Blockchain and Deep Reinforcement Learning Empowered Intelligent 5G Beyond. *IEEE*, *33*(3), 10-17. 10.1109/MNET.2019.1800376

Haddad, Z. (2020). Blockchain-based Authentication for 5G Networks. *IEEE*, 189-194. 10.1109/ICIoT48696.2020.9089507

Haddad, Z. (2023). Blockchain-enabled anonymous mutual authentication and location privacy-preserving scheme for 5g networks. *scienceDirect*, *35*(6). https://www.sciencedirect.com/science/article/pii/S1319157822004165

Haddad, Z., & Baza, M. (2021). Secure and Efficient AKA Scheme and Uniform Handover Protocol for 5G Network Using Blockchain. *IEEE*, *2*, 2616 - 2627. 10.1109/OJCOMS.2021.3131552

Hojjati, M. (2020). A Blockchain-Based Authentication and Key Agreement (AKA) Protocol for 5G Networks. *IEEE*, *8*, 216461 - 216476. 10.1109/ACCESS.2020.3041710

Praveen, G., Chamola, V., Hassija, V., & Kumar, N. (2020). Blockchain for 5G: A Prelude to Future Telecommunication. *IEEE*, *34*(6), 106-113. 10.1109/MNET.001.2000005

Haddad, Z. (n.d.). *Blockchain-based Authentication for 5G Networks*. IEEE. https://ieeexplore.ieee.org/abstract/document/9089507

Nguyen, D., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). *Blockchain for 5G and beyond networks*. ScienceDirect. https://www.sciencedirect.com/science/article/abs/pii/S1084804520301673

*Nguyen, D. C. (2020). Blockchain for 5G and beyond networks. ScienceDirect, 166.*

*What is a decentralized network?* (2022). 4soft. https://www.4soft.co/blog/what-is-a-decentralized-network-definition-benefits-and-challenges

*What Is Blockchain?* (n.d.). IBM. Retrieved January 24, 2025, from https://www.ibm.com/think/topics/blockchain

Rathore, S. (2021). Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT. *IEEE*, *9*, 90075 - 90083. 10.1109/ACCESS.2021.3077069

Serrano, W. (2020). The Blockchain Random Neural Network for cybersecure IoT and 5G infrastructure in Smart Cities. *ScienceDirect*, *175*. https://www.sciencedirect.com/science/article/abs/pii/S1084804520303696

Xie, L., & Ding. (2019). IEEE. *Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs*, *7*, 56656 - 56666. 10.1109/ACCESS.2019.2913682