engineering proceedings

MDPI

Proceeding Paper

An Analytical Model for Dynamic Spectrum Sensing in Cognitive Radio Networks Using Blockchain Management †

Nikhil Kumar Marriwala [1,*], Sunita Panda [2], Chandran Kamalanathan [2], Narayanan Sadhasivam [3] and Vootla Subba Ramaiah [4]

[1] Department of Electronics & Communication Engineering, University Institute of Engineering & Technology, Kurukshetra University, Kurukshetra 135001, Haryana, India
[2] Department of Electrical, Electronics and Communication Engineering GITAM School of Technology, GITAM Deemed to be University, Bengaluru Campus, Bengaluru 561203, Karnataka, India; spanda3@gitam.edu (S.P.); kchandra@gitam.edu (C.K.)
[3] Department of Computer Technology, Bannari Amman Institute of Technology, Sathyamangalam 638401, Tamil Nadu, India; sadhasivamn82@gmail.com
[4] Department of CSE, Mahatma Gandhi Institute of Technology, Gandipet 500075, Telangana, India; vsubbaramaiah_cse@mgit.ac.in
* Correspondence: nmarriwala@kuk.ac.in
† Presented at the International Conference on Recent Advances on Science and Engineering, Dubai, United Arab Emirates, 4–5 October 2023.

Abstract: Recent advancements in wireless communication technology have brought about the pressing issue of increasing spectrum scarcity. This challenge in spectrum allocation arises from ongoing research in the field of wireless communication. Unfortunately, a significant portion of the spectrum remains underutilized within wireless networks. Cognitive radio (CR) presents an innovative solution to this problem by enabling unlicensed secondary users to coexist with licensed primary users within allocated spectrum bands without causing interference to the primary users' communications. This paper promises to address the spectrum redundancy challenges and substantially improve the spectrum utilization efficiency. Cognitive radio networks (CRNs), alternatively known as dynamic spectrum access networks, are comprised of multiple CR nodes and are frequently referred to as next generation (XG) communication networks. These XG communication networks are expected to offer high-speed data transmission capabilities to adaptable users through a variety of wireless architectures and dynamic access protocols. Since CRNs share similarities with traditional wireless networks but operate in an external wireless medium, they are more susceptible to various types of attacks compared to their wired counterparts. This vulnerability stems from the fact that wireless media can be intercepted or exploited, potentially leading to channel congestion or data interception. This paper presents two key approaches: the node evaluation and selection (NES) algorithm and the secure spectrum sensing mechanism, which incorporate the user's interaction history and connection distance, that are recorded in a public ledger and managed by a blockchain management system. The proposed algorithm facilitates the central aggregation point for selecting nodes with outstanding performance for cooperative sensing, thus enhancing the network's security against malicious node attacks.

Keywords: blockchain; cognitive radio network; error rate; NES algorithm; spectrum sensing; dynamic spectrum access

Citation: Marriwala, N.K.; Panda, S.; Kamalanathan, C.; Sadhasivam, N.; Ramaiah, V.S. An Analytical Model for Dynamic Spectrum Sensing in Cognitive Radio Networks Using Blockchain Management. *Eng. Proc.* **2023**, *59*, 163. https://doi.org/10.3390/engproc2023059163

Academic Editors: Nithesh Naik, Rajiv Selvam, Pavan Hiremath, Suhas Kowshik CS and Ritesh Ramakrishna Bhat

Published: 15 January 2024

1. Introduction

Blockchain adoption is rapidly gaining momentum, driven by the ever-evolving industry landscape. Numerous startups have embarked on blockchain projects, and investments in this technology have surged significantly. Despite blockchain's ongoing development in terms of technological maturity, there is a continuous surge in innovative experimental

adoption and customization [1]. Blockchain possesses the potential to disrupt established innovations and reshape industries or create entirely new ones [1]. The initial trends in the emergence of cryptocurrencies have already demonstrated that blockchain technology is a disruptive force in the banking and financial services sectors [2]. Notably, cryptocurrencies have the potential to challenge centralized banking systems by eliminating the transaction fees typically associated with credit and debit card usage [3]. Recent developments suggest that blockchain is transitioning from a disruptive technology to a sustaining one [4]. Its significant potential extends well beyond the realm of finance and is poised to have a substantial impact on supply chain management, healthcare, the Internet of Things (IoT), education, and public services. The commercial feasibility and acceptance of blockchain are steadily increasing [3]. The patent landscape further underscores the growing influence of blockchain, with more than 3021 patent families associated with blockchain applications falling into four sub-categories: payments and transaction systems, financial services business, administration, and e-commerce [5]. Blockchain's high level of security is attributed to its extensive use of cryptography and decentralization. Concerns about privacy, often associated with public blockchains, can be addressed by implementing blockchains in a controlled manner, known as permissioned blockchain, as shown in Figure 1.

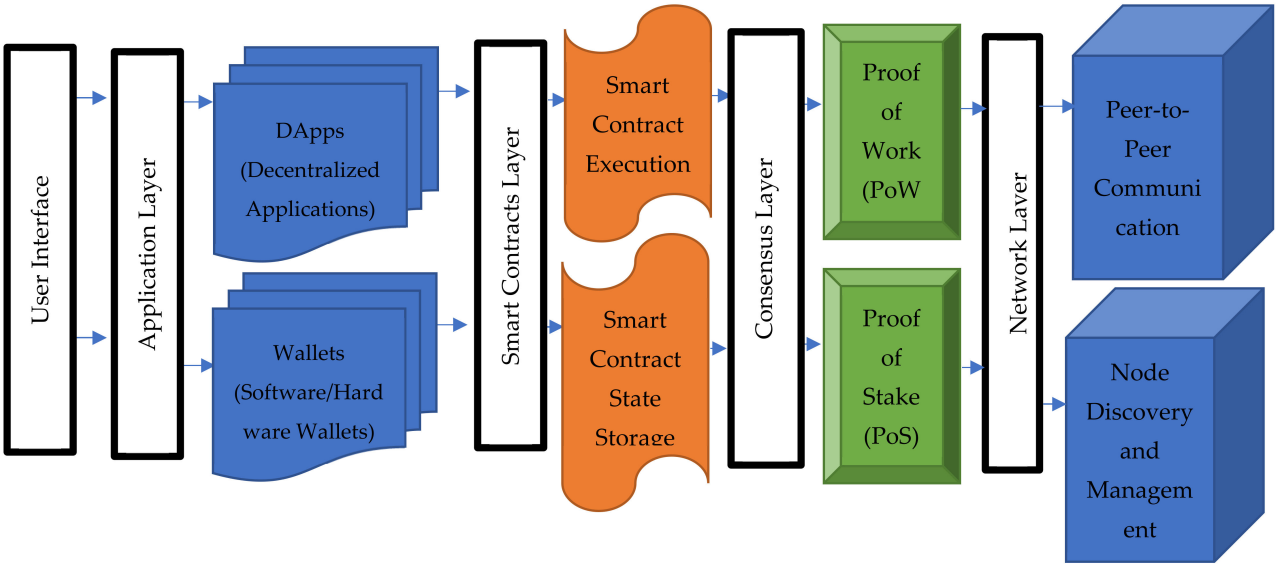

Figure 1. An overview of the blockchain architectures.

Blockchain has the capacity to record various types of transactions, contracts, data assets, or virtually any information that can be stored digitally [6]. Blockchain records possess enduring qualities and are digitally structured, transparent, and easily accessible, as shown in Figure 1. Each newly generated "block" is appended to the end of an existing "chain," and the initiation, validation, storage, and distribution of each block are governed by a predefined protocol [7]. This technology eliminates the necessity for third-party intermediaries, as participants within the blockchain network execute complex algorithms to verify the integrity of the records within the block. Blockchain presents an intriguing alternative to conventional data storage methods [8]. Historically, databases have been the primary means of data storage. While databases offer speed and user-friendliness, they also come with limitations and challenges, such as the absence of immutability [1,9]. Table 1 outlines the key distinctions between blockchain and traditional databases. Blockchain databases offer distinct advantages and trade-offs, making them suitable for different use cases based on specific requirements for data security, transparency, immutability, and decentralization [10]. A blockchain system comprises various integral components that collaborate to facilitate business transactions and operations [6].

Table 1. Comparison of databases with blockchain [1].

Aspect	Blockchain	Databases
Record immutability	Records are immutable once added to the chain, making them highly resistant to tampering or alteration.	Records can be modified or deleted by authorized users, compromising data integrity.
Decentralization	Operates in a decentralized manner, distributing control and data across a network of nodes.	Typically, databases are centralized, with a single authority or server managing data access and control.
Trust and transparency	Offers transparency, as all participants can view the entire transaction history, enhancing trust.	Access permissions in databases can limit visibility, potentially raising trust issues.
Security	Employs cryptographic techniques to ensure data security, making it robust against cyber threats.	Security measures in databases may vary, and vulnerabilities can be exploited by skilled attackers.
Consensus mechanism [11]	Achieves consensus through complex algorithms and validation by network participants.	Relies on a central authority or predetermined rules to maintain data consistency.
Transaction speed	Transaction processing speed can vary depending on the blockchain's design and network size.	Traditional databases often offer faster transaction processing.
Data recovery	Recovery options may be limited, as immutability may hinder data modification in the case of errors.	Data recovery and modification are more flexible in databases.
Cost efficiency	May involve transaction fees, especially in public blockchains, impacting cost-effectiveness.	Databases may have lower operational costs but can entail licensing fees.
Use cases	Ideal for scenarios requiring trust, transparency, and security, such as financial transactions and supply chain tracking.	Well suited for applications where data modification and retrieval are frequent, like content management systems.

Each of these elements plays a distinct role within the blockchain ecosystem.

a. Node: A node refers to a computational unit within the blockchain network with the capability to initiate, receive, or validate transactions [11]. It operates using software applications designed for specific business use cases. Typically, blockchains feature two types of nodes.
b. Validator Nodes: These nodes possess enhanced capabilities, allowing them to initiate, receive, and validate transactions.
c. Member Nodes: Member nodes, on the other hand, are limited to initiating and receiving transactions.
d. Transaction: In the context of a blockchain, a transaction is a collection of various data items that convey information about the exchange of assets, services, entities, events, or anything of value.
e. Block: A block is a data structure tasked with storing a collection of transactions. After undergoing successful verification, each block is distributed to all the nodes across the blockchain network.
f. Block Number: This identifier uniquely identifies blocks within the chain of blocks.
g. User Nodes: User nodes are primarily responsible for initiating transactions and do not engage in block verification.

These components collectively form the foundation of a blockchain system, enabling secure, transparent, and tamper-resistant transactions and data management. Several well-known consensus algorithms are Proof of Work (PoW), Proof of Stake (POS), Proof of Activity (POA), which combines elements of both POW and POS [12], and Proof of Capacity (POC).

2. Blockchain-Based CRN Security Technique

Blockchain is a basic innovation preoccupied via Bitcoin. It is another use of conventional innovation in the web period that incorporates conveyed information stockpiling innovation, remote organizations, agreement systems, and cryptography [7]. Table 2 A, B represents the block structure in a blockchain radio network. As a decentralization

public data set, blockchain utilizes public keying cryptographical calculations, hashing capacities, agreement instruments, and different innovations to fabricate a decentralized non-verification framework that could be utilized in internet business to guarantee client data security [7,13]. It would additionally advance the course of monetary globalization and would enormously affect the current monetary marketing design and, surprisingly, social design [5]. Blockchain innovation enjoys the benefits of the lowest exchange costs, solid straightforwardness, and the highest securities. Normal issues like a significant expense, low effectiveness, and low information stockpiling security in the normalized data set give groundbreaking thoughts [13,14]. Blockchain is a carefully designed, full history information base stockpiling innovation that ordinarily utilizes highlight direct innovation to coordinate every hub. Every hub understands the elements of steering, and a new hub distinguishes proof and information dispersal via multicast. By utilizing cryptography, it can create related information blocks. The created information could look at the legitimacy of the data and likewise understand the solid connection via the following information [15]. Taking into account the benefits of blockchain innovation, this paper gives a psychological remote organization security calculation dependent on blockchains [11].

Table 2. (A, B) Block structure in a blockchain radio network summary [1].

(**A**)					
Block	# 1				
Nonce	36,584				
Transaction	Rs 65	from	Ravi	to	Mohit
	Rs 30	from	Pankaj	to	Vishal
	Rs 45	from	Ravi	to	Mohit
	Rs 50	from	Rohit	to	Sonu
	Rs 30	from	Mohit	to	Kunal
Previous	00000000000000000000				
Hash	0000ab2des234f453f4r5tfe34				
(**B**)					
Block	# 2				
Nonce	82,549				
Transaction	Rs 25	from	Mohit	to	Priya
	Rs 30	from	Sonu	to	Reena
	Rs 15	from	Kunal	to	Ravi
	Rs 25	from	Ravi	to	Sonu
	Rs 30	from	Pankaj	to	Kunal
Previous	0000ab2des234f453f4r5tfe34				
Hash	0000rgtf3r4r45t6y6hfrett56y5				

Algo Design Structure

Clients speak via the block chain framework in the combination place. The particular construction is displayed in Figure 2. The IoT gadget sends its hub data to the combination place, and the combination community inquiries the blockchain framework for the presence of its hub data. Afterwards, the hub sends the information endorsed via the private keying to the combination place, and checks when the detecting hub had a relating private keying paired signature.

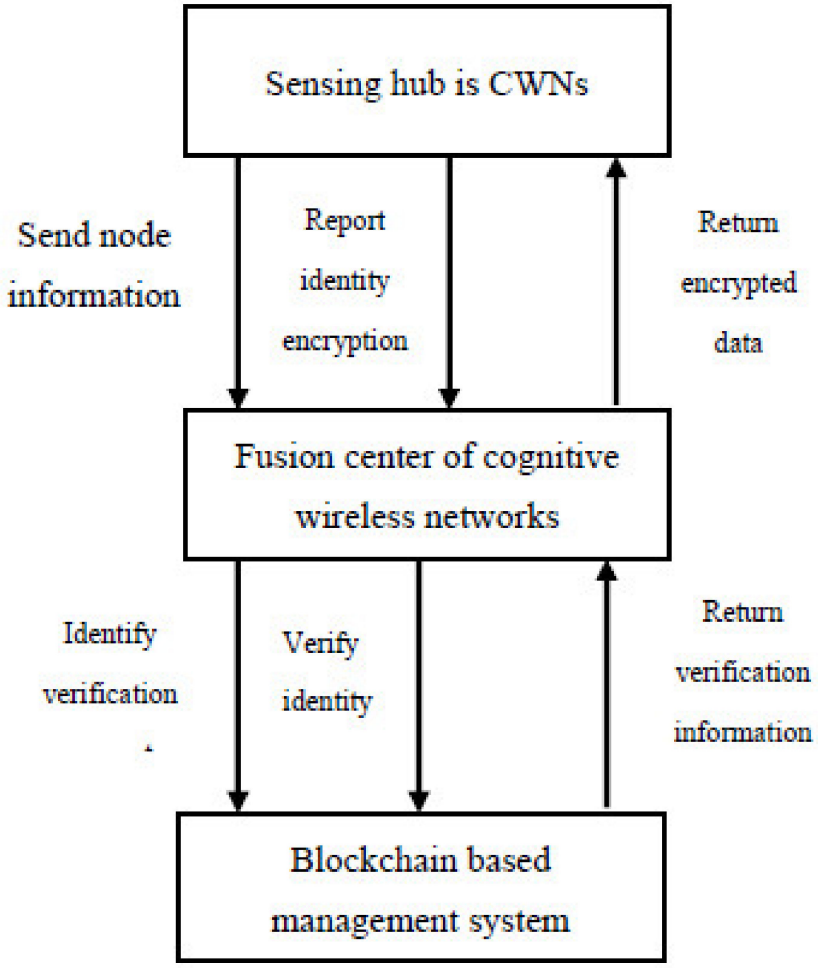

Figure 2. Security calculation construction of the intellectual remote organization.

Assuming is the above, the hub's solicitation is forwarded to the blockchain framework, and the reaction of the blockchain framework is sent back to the detecting hub. Some potential research gaps identified in CRN security are in the field of physical layer security, machine learning-based attacks and defenses, security in spectrum sensing, coexistence with legacy systems, dynamic key management, privacy preservation, cross-layer security, resilience against jamming and spoofing, blockchain and distributed ledgers, secure localization, and security education and awareness [16].

3. Blockchain Technology Blockchain-Based Secure Spectrum

This paper presents blockchain innovation and a notoriety system into the range detecting measure. Another safe range detecting strategy was proposed. This security detecting strategy incorporated the assessment of the client's immediate standing and suggestion notoriety.

To stay away from conspiracy assault and malevolent hub conduct, the detecting results were more precise. The particular working course of the safety range detection dependent on blockchain innovation is displayed in Figure 3. The value was determined using Equation (1).

$$T_i = \frac{N_i}{k}\theta\omega_i \quad (1)$$

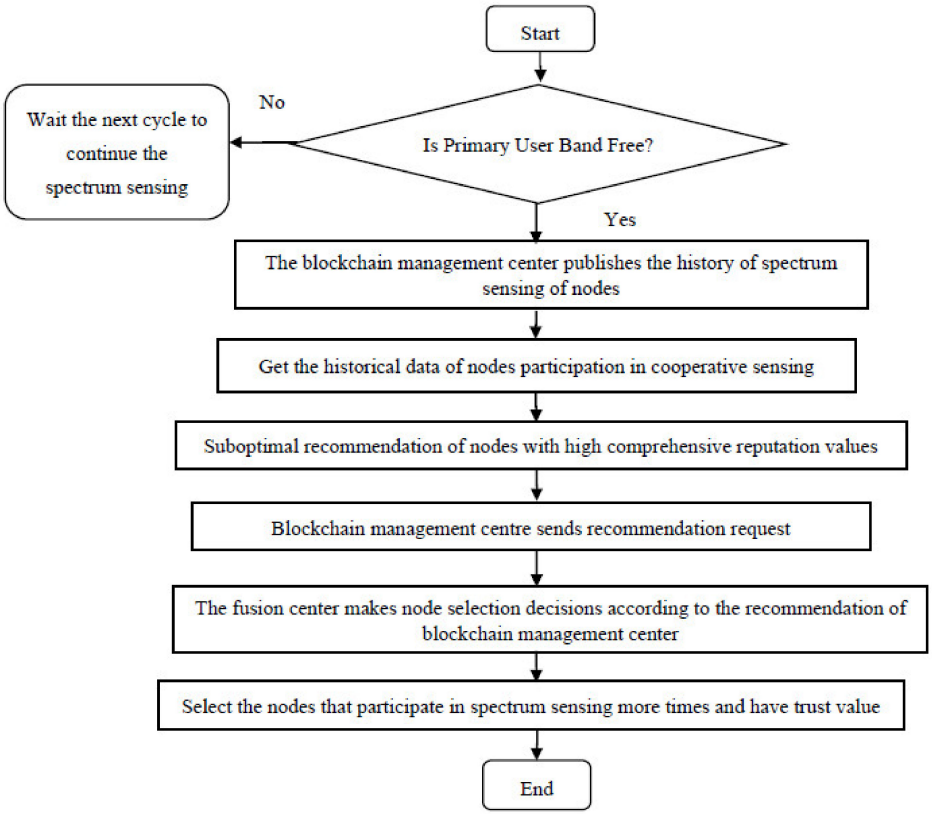

Figure 3. Flow chart depicting the security enhancement in CRNs through the blockchain-based spectrum sensing algorithm.

In Equation (1), T_i addresses the ith detecting period, N_i is the quantity of all the detecting periods up to the T_i time frame. The significance of k is equivalent to and shows the right number of intuitive detections in the history, θ implies the detecting activity force, its worth is determined by ω_i, which is the impact coefficient of the detecting times in the public record book. Its worth is determined by Equations (2) and (3).

$$\theta = 1 - e^{|-\frac{k}{mn}|} \tag{2}$$

$$\omega_i = \sum_{i=1}^{n} \left| \frac{h_1}{m} . \frac{l}{n} \right| \tag{3}$$

where h_1 is the number of cooperations in l period, m is the size of the detecting period in every period, and n is the all-out association time frame. It can be seen from the equation that the nearer the cooperation history in the public record book, the more prominent the extent, and the effect on the trust worth will increment as needed. At the point when the trust worth of the hub is not in the front line, with everything being equal, the hub is chosen by figuring the extensive trust esteem, and the thorough trust worth of the hub is determined by Equation (4).

$$T_{i,c} = \varnothing T_i + \varphi | T_i + \theta \sum_i w_i | \tag{4}$$

The blockchain can contribute to improving CRN security for immutable transaction records, secure spectrum allocation, consensus mechanisms, decentralization, secure identity and authentication, transparency and trust, and resilience to sybil attacks and data integrity.

By integrating blockchain technology into CRNs, network operators can enhance security, transparency, and trust in spectrum allocation and access. It provides a robust foundation for managing spectrum resources and mitigating various security threats commonly

associated with dynamic and shared spectrum environments [17]. The NES algorithm plays a crucial role within the context of dynamic spectrum sensing in CRNs. Its primary purpose is to effectively and intelligently evaluate and select the nodes that will participate in the spectrum sensing process, ultimately improving the overall efficiency and reliability of spectrum utilization [18]. The NES algorithm aims to address the challenges of dynamic spectrum sensing in CRNs, where multiple nodes must collaboratively sense and share information about the available spectrum bands. Its core purposes are node evaluation, node selection, efficiency enhancement, and reliability improvement. In dynamic spectrum sensing scenarios [19], where the availability of spectrum bands can change rapidly, the NES algorithm is highly relevant and valuable. The NES algorithm serves as an intelligent mechanism for selecting nodes in CRNs, ensuring that spectrum sensing is efficient, reliable, and adaptable to the dynamic nature of the spectrum availability. It plays a vital role in optimizing resource usage and improving the overall performance and trustworthiness of dynamic spectrum sensing in CRNs [20]. Various sectors, including satellite services, government agencies, and industries like broadcasting and aerospace, also rely on the spectrum [21]. Balancing the needs of these sectors with the demand for wireless data can lead to challenges in spectrum allocation. The scarcity of available spectrums can limit the ability to conduct experiments, trials, and research on new wireless technologies and applications. These trends and statistics highlight the pressing need for continued research in spectrum management, allocation, and optimization. As technology advances and new applications emerge, the urgency to find innovative solutions to address spectrum scarcity becomes even more critical.

4. Result Analysis

In this section, we conduct a thorough analysis of the outcomes derived from the integration of blockchain technology within the context of the cognitive radio network. To provide a comprehensive understanding of our findings, we reference and elaborate upon the simulation parameters, as outlined in Table 3. The simulation area for the network was defined as a circular region with a radius of 'm'. Within this area, primary users were positioned at arbitrary locations along the circumference of the circle. In the given system, the signal power was 100 MW (megawatts), and the bandwidth was 100 kHz (kilohertz). There were 15 nodes in the system, with SNRs (signal-to-noise ratios) of -18 dB and -14 dB for some of the nodes. The noise used in this system was additive white Gaussian noise (AWGN). The system parameters included an average detection time of 10,000 and the presence of three auxiliary nodes. The spectrum detection method employed was energy detection. The cognitive radio topology is defined in Figure 4. The different number of primary and secondary users was placed in a particular geometry. The range of the network was between -500 to 500 m. There was one primary user and multiple secondary users. The primary user was located at the center of the area while the secondary users were located around the primary users within the specific pattern. The total error rate is depicted in Figure 5, commencing at 15% within the first second. Figure 5 shows that the total error rate progressively rose to 20.05% over a period of 2 s. Subsequently, there was a sudden decline, bringing the total error rate down to 10%.

A similar Analysis of Security in Cognitive Radio is displayed in Figure 6. It tends to be seen from Figure 6 that when the NES and SSSB calculations are utilized in the mix, as expanding the number of associations between the detecting hub, combination focus and blockchain the board community, the security file of the psychological remote organization rises fundamentally quickly. Figure 7 depicts the analysis of the energy consumption in terms of the proposed algorithm vs. the NES algorithm. Figure 7 clearly demonstrates that when the number of detection cycles exceeded 60, the energy consumption associated with the algorithm presented in this study was markedly lower compared to that of the conventional algorithms. Increasing the number of detection cycles resulted in longer detection times, ultimately leading to greater energy conservation. This significantly benefitted the cognitive wireless network by extending its operational lifespan. The reason

behind this was that the algorithm presented in this paper consistently selected the node with the optimal performance for timely participation in cooperative detection, thereby saving more energy when the detection performance surpassed that of the traditional methods. In comparison to the NES algorithm, the proposed algorithm demonstrated superior energy efficiency. The results for the organization of traffic are presented in Table 4. Query per second (QPS) assessments offer numerous advantages when examining traffic utilization. To illustrate that the new algorithm did not increase network overhead, a deliberate organization traffic test was conducted. The proposed solution outlined a protocol or algorithm used to manage network traffic within a blockchain network. It aimed to maintain optimal network performance by routing requests appropriately, monitoring traffic conditions, and ensuring timely responses. This test aimed to evaluate the algorithm without introducing any variables related to character data in this segment.

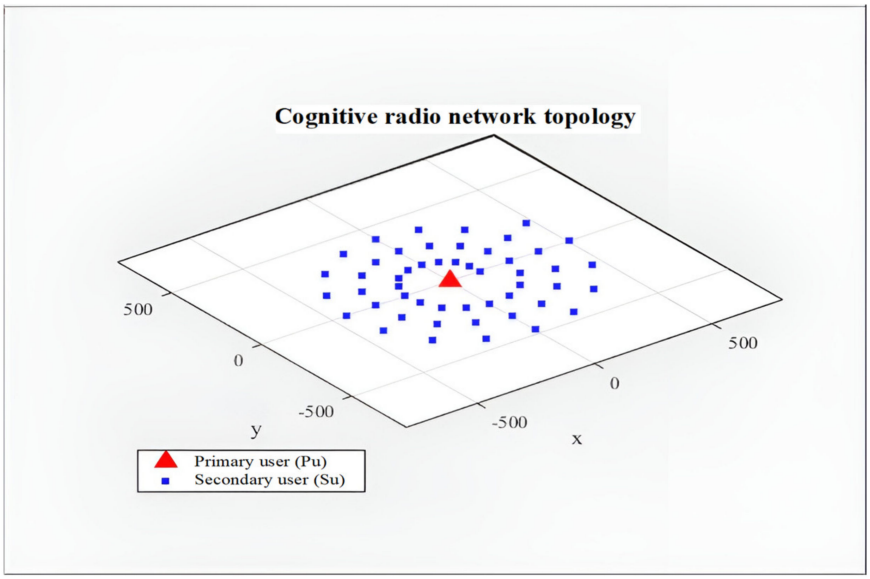

Figure 4. Cognitive radio topology.

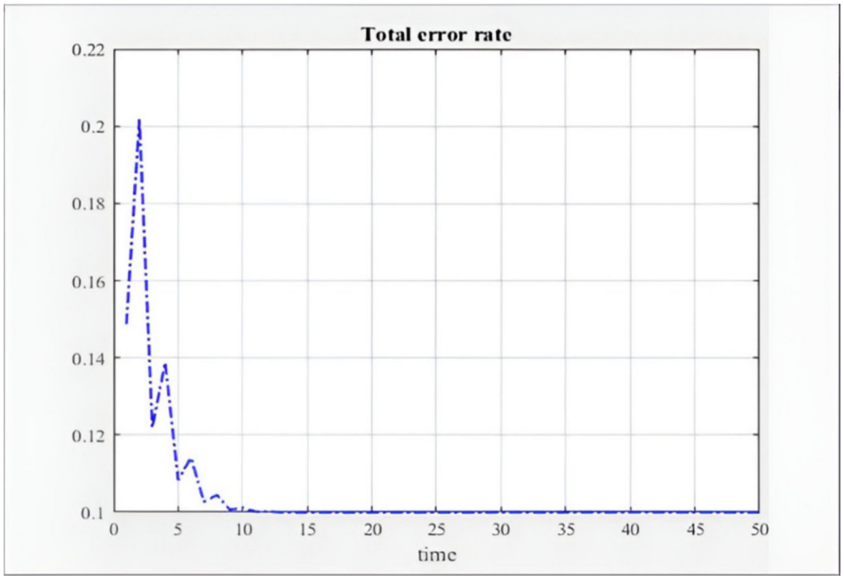

Figure 5. Total error rate.

Table 3. Specific simulation parameters.

Sr. No.	Parameter	Value
1	Configuration of the simulation area	A circular area with a radius of m
2	Primary user	Positioning a primary user at any location along the perimeter of the circular area
3	Operational parameters of a primary user	Utilizing a BPSK signal with a power level of 100 MW and a bandwidth of 100 kHz.
4	Number of nodes	Randomly distributing 15 nodes, with five nodes having SNR of −18 dB and the remaining nodes with SNR of −14 dB.
5	Configuration of noise	AWGN
6	Average detection time	10,000
7	Auxiliary node	3
8	Spectrum detection method of the node front end	Energy detection

Its primary objective was to compare network traffic disparities between remote gateways. If the traffic surpassed a certain predefined threshold, a specific action was taken, and the query or request was directly routed to the blockchain. This approach could be employed to alleviate network congestion or ensure that critical queries are handled promptly by the blockchain, bypassing any potential bottlenecks in the network. The selection of service nodes was also mentioned as a part of this process. Scenarios such as location spoofing, resource exhaustion attacks, authentication and key management vulnerabilities, rogue spectrum access points, primary user protection attacks, jamming attacks, spectrum sensing data falsification and primary user emulation illustrated the potential security risks in CRNs, emphasizing the need for robust security mechanisms, such as authentication, encryption, intrusion detection, and intrusion prevention, to mitigate these threats and ensure the safe and reliable operation of CRNs. The basic architecture, as discussed above, outlined the key components and processes for integrating blockchain into CRNs to enhance security and spectrum access management. By leveraging blockchain technology, CRNs can achieve greater transparency, trust, and efficiency in spectrum allocation and management while mitigating security risks. It's essential to customize this architecture according to specific CRN use cases and regulatory frameworks. Integrating blockchain technology into CRNs can bring several benefits, but it also introduces potential overheads and performance trade-offs that network operators and architects need to consider. Integrating blockchain into CRNs can significantly enhance security and spectrum access management. Blockchain-enabled CRNs can offer both advantages and pose challenges in terms of aligning with current spectrum regulations and policies. While blockchain-enabled CRNs offer significant potential for enhancing spectrum management, there are hurdles to overcome in aligning these systems with current spectrum regulations and policies. Collaboration, adaptation, and a balanced approach to privacy and transparency are key to successfully integrating blockchain technology into the regulatory framework of CRNs. Mitigating security vulnerabilities in CRNs requires a multifaceted approach that combines technological, operational, and regulatory measures.

Table 4. Network traffic test results.

QPS	Direct Interactive Traffic (MB/S)	Encrypted Authentication Traffic (MB/S)	Traffic Utilization (%)
1	1	1	100
2	2	2.001	99.95
5	5	5.002	99.96
10	10.001	10.005	99.96
20	20.002	20.011	99.955
40	20.004	20.02	99.95

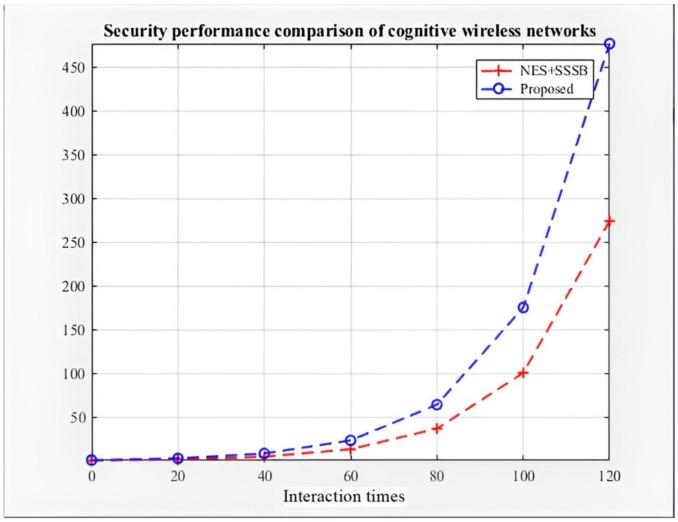

Figure 6. Comparative analysis of security in cognitive radio.

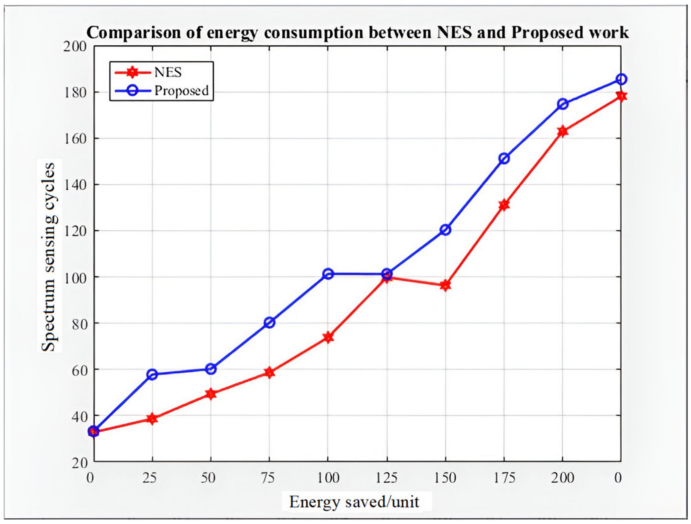

Figure 7. Analysis of the energy consumption: the proposed vs. NES algorithms.

By implementing practical strategies and countermeasures, such as authentication and authorization, spectrum sensing security, jamming detection and mitigation, primary user protection, secure spectrum allocation, intrusion detection, and response, redundancy and resilience, CRN operators can enhance the security and resilience of their networks.

5. Conclusions

In real-world applications for cognitive wireless networks, it is common to encounter genuine errors in data detection through network nodes, leading to deviations from the expected range of detection values. Additionally, there are instances where some nodes intentionally transmit incorrect data to the central aggregation point. In response to these security concerns, this paper presents two key approaches: the NES algorithm and the secure spectrum sensing mechanism. The proposed techniques incorporate the user's interaction history and connection distance, which are recorded as a public ledger and managed by a blockchain management system. The proposed algorithm facilitates the central aggregation point in selecting nodes with outstanding performance for cooperative sensing, thus enhancing the network's security against malicious node attacks.

Author Contributions: Conceptualization, N.K.M. and S.P.; methodology, N.K.M. and C.K.; software, N.K.M. and N.S.; validation, V.S.R., N.K.M. and N.S.; formal analysis, S.P.; investigation, N.K.M.;

writing—original draft preparation, N.K.M. and C.K.; writing—review and editing, N.S. and V.S.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data is contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
2. Bayhan, S.; Zubow, A.; Gawlowicz, P.; Wolisz, A. Smart Contracts for Spectrum Sensing as a Service. *IEEE Trans. Cogn. Commun. Netw.* **2019**, *5*, 648–660. [CrossRef]
3. Xiao, L.; Han, D.; Meng, X.; Liang, W.; Li, K.-C. A Secure Framework for Data Sharing in Private Blockchain-Based WBANs. *IEEE Access* **2020**, *8*, 153956–153968. [CrossRef]
4. Chen, R.; Park, J.-M.; Reed, J.H. Defense against Primary User Emulation Attacks in Cognitive Radio Networks. *IEEE J. Sel. Areas Commun.* **2008**, *26*, 25–37. [CrossRef]
5. Kumar, T.; Harjula, E.; Ejaz, M.; Manzoor, A.; Porambage, P.; Ahmad, I.; Liyanage, M.; Braeken, A.; Ylianttila, M. BlockEdge: Blockchain-Edge Framework for Industrial IoT Networks. *IEEE Access* **2020**, *8*, 154166–154185. [CrossRef]
6. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for 5G and beyond networks: A state of the art survey. *J. Netw. Comput. Appl.* **2020**, *166*, 102693. [CrossRef]
7. Taneja, S.; Marriwala, N. Block Chain Based Cognitive Wireless Networks: Challenges Applications. In Proceedings of the 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 7–9 October 2021; pp. 811–816. [CrossRef]
8. Pang, Y. A New Consensus Protocol for Blockchain Interoperability Architecture. *IEEE Access* **2020**, *8*, 153719–153730. [CrossRef]
9. Choi, M.K.; Yeun, C.Y.; Seong, P.H. A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology. *IEEE Access* **2020**, *8*, 118732–118740. [CrossRef]
10. Roy, C.; Misra, S.; Pal, S. Blockchain-Enabled Safety-as-a-Service for Industrial IoT Applications. *IEEE Internet Things Mag.* **2020**, *3*, 19–23. [CrossRef]
11. Zhang, H.; Leng, S.; Wei, Y.; He, J. A Blockchain Enhanced Coexistence of Heterogeneous Networks on Unlicensed Spectrum. *IEEE Trans. Veh. Technol.* **2022**, *71*, 7613–7624. [CrossRef]
12. Tariq, S.; Akhtar, N.; Afzal, H.; Khalid, S.; Mufti, M.R.; Hussain, S.; Habib, A.; Ahmad, G. A Novel Co-Training-Based Approach for the Classification of Mental Illnesses Using Social Media Posts. *IEEE Access* **2019**, *7*, 166165–166172. [CrossRef]
13. Ni, W.; Zhang, Y.; Li, W. Optimal admission control for secondary users using blockchain technology in cognitive radio networks. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019; pp. 1518–1526. [CrossRef]
14. Pawar, A.; Jawale, M.; William, P.; Chhabra, G.; Rakshe, D.S.; Korde, S.K.; Marriwala, N. Implementation of blockchain technology using extended CNN for lung cancer prediction. *Meas. Sensors* **2022**, *24*, 100530. [CrossRef]
15. Kalra, M.; Vohra, A.; Marriwala, N. Hybrid blockchain-based spectrum sharing algorithm for dynamic channel selection in cognitive radio. *Meas. Sensors* **2023**, *25*, 100648. [CrossRef]
16. Cai, L.; Cao, K.; Wu, Y.; Zhou, Y. Spectrum Sensing Based on Spectrogram-Aware CNN for Cognitive Radio Network. *IEEE Wirel. Commun. Lett.* **2022**, *11*, 2135–2139. [CrossRef]
17. Khan, A.U.; Abbas, G.; Abbas, Z.H.; Khan, W.U. On Reliable Key Performance Indicators in Cognitive Radio Networks. *IEEE Netw. Lett.* **2021**, *4*, 11–15. [CrossRef]
18. Papadopoulos, A.; Chatzidiamantis, N.D.; Georgiadis, L. Network Coding Techniques for Primary-Secondary User Cooperation in Cognitive Radio Networks. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 4195–4208. [CrossRef]
19. Sharifi, A.A. Attack-Aware Defense Strategy: A Robust Cooperative Spectrum Sensing in Cognitive Radio Sensor Networks. *Iran. J. Sci. Technol. Trans. Electr. Eng.* **2018**, *43*, 133–140. [CrossRef]
20. Ding, G.; Jiao, Y.; Wang, J.; Zou, Y.; Wu, Q.; Yao, Y.-D.; Hanzo, L. Spectrum Inference in Cognitive Radio Networks: Algorithms and Applications. *IEEE Commun. Surv. Tutorials* **2017**, *20*, 150–182. [CrossRef]
21. Jararweh, Y.; Salameh, H.A.B.; Alturani, A.; Tawalbeh, L.; Song, H. Anomaly-based framework for detecting dynamic spectrum access attacks in cognitive radio networks. *Telecommun. Syst.* **2017**, *67*, 217–229. [CrossRef]