Medicon Engineering Themes
Volume 4 Issue 4 April 2023
Article Type: Editorial Note
ISSN: 2834-7218

Securing Cognitive Radio Networks with Blockchain: Opportunities and Challenges

Debabrata Dansana*[1,2]

[1]*Department of Computer Science and Applications, Utkal University, Vani Vihar, Bhubaneswar, Odisha*

[2]*Rajendra University, Balangir, Odisha*

***Corresponding Author:** Debabrata Dansana, Department of Computer Science and Applications, Utkal University, Vani Vihar, Bhubaneswar, Odisha; Rajendra University, Balangir, Odisha.

Received: March 23, 2023; **Published:** March 29, 2023

1. In recent years, cognitive radio ad-hoc networks (CRAN) have become increasingly popular due to their ability to improve spectrum utilization and enhance wireless communication. CRANs are becoming increasingly popular due to their ability to improve spectrum utilization and enhance wireless communication; security remains a significant challenge. However, security in CRAN remains a considerable challenge, with malicious actors capable of causing disruptions and stealing data. One promising solution to this problem is using blockchain technology to secure CRANs. The paragraph sets the stage for discussing how blockchain technology can help solve this problem.
2. Blockchain technology, initially developed for the cryptocurrency Bitcoin, has evolved into a sophisticated tool for secure and transparent data management. The blockchain is essentially a decentralized, distributed ledger that records transactions in a tamper-proof manner. This technology can potentially transform the security of CRANs by providing a secure and transparent way to manage communication and ensure data privacy.

a. Spectrum Management: This section explains how blockchain technology can enhance security in CRANs by providing a secure and transparent method for spectrum management. In a typical CRAN, nodes may compete for available frequencies, leading to interference and reduced network performance. However, using blockchain, nodes can reach a consensus on spectrum usage, ensuring each node gets a fair share of the available spectrum. This can help to reduce interference and improve network performance.

   For example, imagine a group of devices in a park that want to use the same frequency band to communicate with each other. Without a centralized authority to manage spectrum usage, these devices could interfere with each other and cause communication issues. However, by using blockchain technology, the devices could come to a consensus on which frequency band each device can operate at a given time, ensuring that there is no interference and that communication is reliable.

3. One-way blockchain technology can enhance security in CRANs is by providing a secure and transparent method for spectrum management. In a typical CRAN, nodes may compete for available frequencies, leading to interference and reduced network performance. Using blockchain, nodes can reach a consensus on spectrum usage, ensuring each node gets a fair share of the available spectrum. This can help to reduce interference and improve network performance.

b. Identity Management: This section explains how blockchain technology can enhance security in CRANs by providing a secure and transparent method for identity management. In a typical CRAN, nodes may be vulnerable to spoofing and impersonation attacks, leading to data theft and network disruptions. However, using blockchain, nodes can authenticate each other using public- key cryptography, ensuring that only authorized nodes can access the network. This can help to prevent unauthorized access and protect against malicious attacks.

   For example, consider a group of intelligent sensors in a building that are communicating with each other to monitor temperature and humidity levels. Without a secure method of identity management, a malicious actor could spoof the identity of one of the sensors and gain access to the network, potentially stealing data or disrupting communication. However, using blockchain technology, each sensor can be authenticated using public-key cryptography, ensuring that only authorized sensors can commu-

nicate with each other.

4. Another way blockchain technology can enhance security in CRANs is by providing a secure and transparent method for identity management. In a typical CRAN, nodes may be vulnerable to spoofing and impersonation attacks, which can lead to data theft and network disruptions. By using blockchain, nodes can authenticate each other using public-key cryptography, ensuring that only authorized nodes can access the network. This can help to prevent unauthorized access and protect against malicious attacks.

c. Data Management: This section explains how blockchain technology can enhance security in CRANs by providing a secure and transparent method for data management. In a typical CRAN, data may be vulnerable to interception and tampering, leading to data theft and network disruptions. However, using blockchain, data can be encrypted and stored securely, ensuring that only authorized nodes can access it. Additionally, the decentralized nature of blockchain technology ensures that data is stored redundantly, making it difficult for attackers to compromise the network.

For example, imagine a group of drones using a CRAN to communicate with each other to complete a mapping mission. The data transmitted between the drones is sensitive and needs to be kept secure. By using blockchain technology, the data can be encrypted and stored securely, ensuring that only authorized nodes can access it. Additionally, because the data is stored redundantly on multiple nodes in the network, it is difficult for a single point of failure to bring down the entire network.

5. Finally, blockchain technology can enhance security in CRANs by providing a secure and transparent method for data management. In a typical CRAN, data may be vulnerable to interception and tampering, leading to data theft and network disruptions. Using blockchain, data can be encrypted and stored securely, ensuring that only authorized nodes can access it. Additionally, the decentralized nature of blockchain technology ensures that data is stored redundantly, making it difficult for attackers to compromise the network.

   As CRANs become more prevalent, we must continue to explore innovative solutions to enhance their security, and blockchain technology is a promising option. Overall, blockchain technology has the potential to improve security in CRANs by providing a secure and transparent method for spectrum management, identity management, and data management. While challenges remain to be addressed, such as the scalability of blockchain technology, the benefits are clear.

6. In conclusion, the use of blockchain technology in CRANs has the potential to transform the security of these networks by providing a secure and transparent method for spectrum management, identity management, and data management. While challenges remain to be addressed, such as the scalability of blockchain technology, the benefits are clear. As CRANs become more prevalent, we must continue to explore innovative solutions to enhance their security, and blockchain technology is a promising option.

Volume 4 Issue 4 April 2023