Distributed-Proof-of-Sense: Blockchain Consensus Mechanisms for Detecting Spectrum Access Violations of the Radio Spectrum

Article *in* IEEE Transactions on Cognitive Communications and Networking · June 2023

DOI: 10.1109/TCCN.2023.3291366

Pramitha Fernando
Vrije Universiteit Brussel

Keshawa Dadallage
Washington State University

Tharindu Gamage
University of Ruhuna

An Braeken
Vrije Universiteit Brussel

Distributed-Proof-of-Sense: Blockchain Consensus Mechanisms for Detecting Spectrum Access Violations of the Radio Spectrum

Pramitha Fernando, *Student Member, IEEE,* Keshawa Dadallage, Tharindu Gamage, Chathura Seneviratne, *Member, IEEE,*, An Braeken, Arjuna Madanayake, and Madhusanka Liyanage, *Senior Member, IEEE*

Abstract—**The exponential growth in connected devices with Internet-of-Things (IoT) and next-generation wireless networks requires more advanced and dynamic spectrum access mechanisms. Blockchain-based approaches to Dynamic Spectrum Access (DSA) seem efficient and robust due to their inherited characteristics such as decentralization, immutability and transparency. However, conventional consensus mechanisms used in blockchain networks are expensive to be used due to the cost, processing and energy constraints. Moreover, addressing spectrum violations (i.e., unauthorized access to the spectrum) is not well-discussed in most blockchain-based DSA systems in the literature. In this work, we propose a newly tailored energy-efficient consensus mechanism called "Distributed-Proof-of-Sense (DPoS)" that is specially designed to enable DSA and detect spectrum violations. The proposed consensus algorithm motivates blockchain miners to perform spectrum sensing, which leads to the collection of a full spectrum of sensing data. An elliptic curve cryptography-based zero-knowledge proof is used as the core of the proposed mechanism. We use MATLAB simulations to analyze the performance of the consensus mechanism and implement several consensus algorithms in a microprocessor to highlight the benefits of adopting the proposed system.**

Index Terms—**Spectrum Management, Dynamic Spectrum Access, Spectrum Sensing, Spectrum Misuse, Blockchain, Consensus Mechanism, Elliptic Curve Cryptography, Zero Knowledge Proof**

I. Introduction

The exponential growth in connected devices with IoT, Device-to-Device (D2D) communication, and next-generation wireless networks needs a more advanced and dynamic spectrum access mechanism [1], which is not currently available in fixed spectrum allocation. The scarcity of electromagnetic radio spectrum fuels this idea. In conventional static spectrum assignment, a government regulatory body such as Federal Communications Commission (FCC) sells the spectrum to Mobile Network Operators (MNOs) in a primary market [2], providing the MNO exclusive rights to the specific frequency range. However, license holder MNOs barely use some frequency bands or use them sporadically, resulting in spectrum holes [1] [3]. These spectrum holes appear and disappear across a vast time scale, ranging from a few milliseconds to several weeks [4]. Since the static model is unable to address these flaws, demand for spectrum continues to climb, despite the fact that the radio spectrum is already overburdened [5]. Furthermore, conventional spectrum allocation is outmoded and unable to meet the high bandwidth, ultra-low latency connectivity needs of future networks. To address these problems, the research communities introduce DSA concepts.

Over time various approaches have been adopted to achieve efficient and effective spectrum allocation. Cognitive Radio (CR) technology is proposed to solve this problem by dynamically allocating spectrum holes to Secondary Users (SUs), while technologies like Co-Primary Spectrum Sharing (CoPSS) solves this problem by assigning a non-exclusive band to several potential operators for shared use [6]. In CRs, frequency coordination systems such as Spectrum Access System (SAS) in Citizens Broadcast Radio Services (CBRS) are used to handle the coordination. New models of DSA could possibly rise with the localized infrastructure-based services such as Local 5G Operators (L5GO), where a local regulator can lease spectrum dynamically.

Spectrum misuse (i.e., fraud) is a common problem in shared spectrum access models. We define spectrum fraud as unlawful access (intentional or unintentional) to licensed radio spectrum, causing interference to rightful spectrum owners. Fraud in a DSA system will reduce service quality and may result in significant financial losses. Such negative impacts may dissuade operators from using DSA. Therefore, it is critical in a DSA system to ensure that these misuses do not occur to maintain its reliability.

In a conventional system, a trustworthy third party (i.e., a mediator) must manage the sharing system as the stakeholders are unlikely to trust each other, and due to third-party commissions and fees, this process incurs additional costs for operators and customers indirectly. Furthermore, current DSA approaches do not support automatic detection of unauthorized spectrum usage. Spectrum fraud detection is critical for maintaining a reliable DSA system because these violations can significantly impact the system's QoS. At present, usually, the spectrum regulatory body manually

Pramitha Fernando is with the Faculty of Engineering, Vrije Universiteit Brussel, Brussels, Belgium. e-mail: Warnakulasuriya.Pramitha.V.Fernando@vub.be

Keshawa Dadallage, Tharindu Gamage and Chatura Seneviratne are with the Department of Electrical and Information Engineering, University of Ruhuna, Galle, Sri Lanka. e-mail: keshawa.dadallage@eie.ruh.ac.lk, tharindu@eie.ruh.ac.lk, chatura@eie.ruh.ac.lk

An Braeken is with the Industrial Engineering Department of the Vrije Universiteit Brussel, Brussels, Belgium. e-mail: an.braeken@vub.be

Arjuna Madanayake is with the Florida International University (FIU), Miami, Florida, USA. e-mail: amadanay@fiu.edu

Madhusanka Liyanage is with the School of Computer Science, University College Dublin (UCD), Ireland, e-mail:madhusanka@ucd.ie

This work is partly supported by European Union in the CONFIDENTIAL-6G project (Grant ID. 101096435) and by Science Foundation Ireland under CONNECT phase 2 (Grant no. 13/RC/2077_P2) project.

attends to these complaints, which is neither efficient nor practical. Investigating such violations by hand will not be possible with the more frequent spectrum sharing events in upcoming technologies. Moreover, traditional spectrum sharing methods do not support real-time marketplaces for MNOs to buy and sell spectrum in real-time. As a result, the existing spectrum sharing mechanisms are inefficient and time-consuming. Spectral whitespaces appear and disappear at millisecond time scales, implying that automated high-frequency spectrum trading as part of DSA is a viable option. The FCC phrased secondary markets as a means to correct potential inefficiencies caused by the primary market and an alternative for responding to the changing technologies [2]. Furthermore, traditional mechanisms lack global-level reputation management systems that can rate Primary Users (PUs) and SUs based on their performance or network quality. Such information is critical for stakeholders in identifying responsible parties to establish spectrum sharing agreements.

Our Contribution: This paper presents a novel Consensus Mechanism (CM) that will help to alleviate the limitations of existing DSA systems. The proposed *Distributed-Proof-of-Sense* consensus mechanism operates based on spectrum sensing, and it is specifically designed to build a superior DSA system. The novel consensus mechanism has the potential to deliver all of the benefits of blockchain technology while collecting additional data for spectrum analysis. The DSA system can use these data to identify and track down system-wide infractions of spectrum rules. Aside from that, this information is useful in determining customer behavior patterns and trends. This paper discusses the design of the new consensus mechanism, along with its implementation in a DSA system. Furthermore, we describe the software simulations and practical testbed implementations of the proposed system. We use simulations and implementation to examine the performance of the proposed system under a variety of different scenarios. Furthermore, the proposed consensus mechanism is compared with existing consensus algorithms to compare the characteristics.

Outline: The remainder of this article is structured as follows. Section II discusses the related works and their strengths and weaknesses. Section III describes the proposed dynamic spectrum management system and the Distributed-Proof-of-Sense operating principles. Section IV discusses the proposed system's performance evaluations and simulations. Section V goes over the experiments that were carried out on the testbed. Finally, Section VI brings this article to a conclusion.

II. Related Works

Several DSA systems powered by blockchain have been developed in [4], [7], [8], [9], and [10]. Weiss et al. in [7] broadly explained the utilization of blockchain for spectrum sharing and discussed its benefits and limitations under four categories. The authors highlighted how the primary benefits of blockchain technology: decentralization, transparency, immutability, availability, and security, are well-suited for spectrum sharing. Further, the authors highlighted that massive energy expenditures, scalability, governance, and interoperability are major challenges in blockchain systems. The authors concluded that a new consensus algorithm could be a potential solution to resolve some of these challenges. Hao Xu et al. in [11] discussed the potentials of blockchain technology for resource management and sharing in 6G networks by considering multiple application scenarios, including spectrum sharing. The authors compared the consensus mechanisms regarding latency, complexity, security, energy consumption, and scalability. The authors also pointed out the role of SCs in automated resource management. Further, they highlighted that choosing a suitable consensus mechanism is critical for making a secured and efficient blockchain system. Tharaka Hewa et al. in [12] explained the possibilities of using blockchain in intelligent resource management for 6G networks, including spectrum sharing. They highlighted the new intriguing challenges in 6G and appraised the potential of blockchain technology to mitigate some of them. In [13], Ali Hussain Khan et al. discussed the potential of blockchain and 6G for future communication, emphasising their synergy. The authors have highlighted the importance of spectrum management in meeting the high data rate requirements of 6G applications and how a blockchain-based spectrum-sharing framework can help address them. Furthermore, the authors emphasised that using a consortium blockchain and appropriate consensus mechanisms will make the framework more secure.

Seppo Yrjölä in [14] investigated blockchain use cases for spectrum sharing. The study discussed the CBRS spectrum sharing concept's implementation considerations and how blockchain can be applied as a potential solution. The author highlighted that a successful blockchain deployment has the potential to improve the efficiency of the dynamic spectrum sharing concepts and produce new business opportunities. Kotobi and Bilén in [8] proposed using blockchain for enabling and securing the spectrum sharing process between CRs. The authors show that the proposed blockchain-based medium access protocol can outperform the current conventional system. Here authors have defined a special virtual currency called Specoins, and users can use it to buy the spectrum or earn it by making the blockchain. Further, in [9] Kotobi and Bilén evaluated the concept of moving CR networks.

Thirasara Ariyarathna et al. in [4] proposed a digital token-based DSA system using blockchain and SCs. The authors evaluate the proposed system under two circumstances: advertising-based DSA and sensing-based DSA. In the advertising-based scenario, spectrum owners advertise the availability of frequency bands for lease to potential buyers. In the sensing-based scenario, buyers request spectrum from owners when they need it. In [15], Nguyen Cong Luong et al. proposed to use the blockchain with the mining pool to support IoT services based on CR networks. The authors developed a Deep Q-Learning (DQL) algorithm to optimize the transaction transmission policy for a secondary user. Sicheng Han and Xiaorong Zhu in [16] proposed a consortium blockchain that allows operators to trade their spectrum directly. The blockchain is used to authenticate secondary users and record all the transactions in a tampered-free database. Junfei Qiu et al. in [17] exploited a blockchain-based spectrum trading framework for Unmanned-Aerial-Vehicle (UAV) assisted cellular networks. Using the proposed system, MNO and UAV operators could trade spectrum in a credible environment without relying on a trusted third party. Yueyue Dai in [18] proposed a secure and intelligent architecture for next-generation wireless networks. The authors integrated AI and blockchain technologies into wireless networks to facilitate flexible and secure resource sharing, including the spectrum.

All of the above proposals use blockchain as a service to enable the spectrum trading process. Therefore, the blockchain operates as a separate service that operators can use to transfer payments and store transaction information. As a result, these systems still suffer from excessive and additional energy utilization for the computation heavy mining process. Furthermore, none of the proposals has discussed a practical approach to eliminate spectrum violations in such systems.

A. *Comparison with Existing Work*

Table I shows a feature comparison between existing blockchain-based and non-blockchain-based spectrum sharing systems with the proposed DSA system. Here, the *Extra Cost of Mining* represents the additional energy usage for spectrum data collection. Traditional consensus algorithms, such as proof-of-work and proof-of-stake, need additional energy to collect these data, while customised mechanisms, like [19] and this paper, do not need extra energy because collecting spectrum data is built into the consensus mechanisms (i.e., collecting spectrum data is a part of the consensus mechanism). The *Computational Complexity* represents the complexity of the algorithms used to execute different transactions, such as contracts and spectrum allocation. Sections IV, V, and VI present the analysis of these features.(**L** → Low, **M** → Medium, **H** → High, • → Not Relevant/Not Available)

Most blockchain-based systems outperform non-blockchain systems by providing inherited features like transparency, immutability, and decentralization, which improve the system's reliability, security, and availability. Furthermore, by utilizing the SCs that run on the network, blockchain-based systems provide additional features such as a spectrum sharing marketplace and automated services. Most blockchain-based systems, however, have limitations such as high computational complexity and the additional cost of mining. The proposed DSA system, with its specially tailored Proof-of-Sense consensus mechanism, can overcome some limitations in existing blockchain-based systems.

III. Proposed Dynamic Spectrum Management System

This section presents the proposed dynamic spectrum management system, which brings the power of blockchains, concepts of dynamic spectrum access, and the elegance of ECC (Elliptic Curve Cryptography (ECC))-based Zero-Knowledge Proofs (ZKPs) to create a new paradigm in spectrum management. The resultant is a blockchain-based dynamic spectrum sharing platform powered by a novel consensus mechanism specially tailored for DSA systems. Fig. 1 describes the nodes and overall functionality of the proposed system.

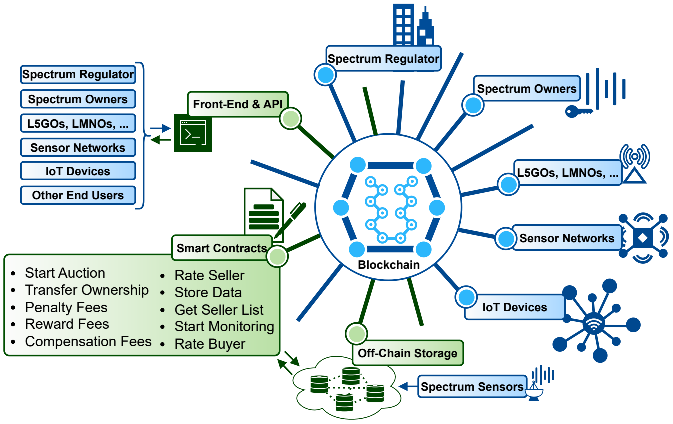


Fig. 1: Overall Functionality and Nodes of the Network

A. *Stakeholders of the System*

There are several stakeholders in any DSA system, such as spectrum regulatory bodies, MNOs, third-party spectrum sensors, and consumers. Since we deploy the system as a consortium blockchain, all the miners must register to become a stakeholder. MNOs (with an exclusive right to spectrum) and regulators can lease the spectrum for IoT devices, sensor network hubs, local network operators (L5GOs, LMNOs), or other MNOs. Through the blockchain network, the regulators can monitor the trading of spectrum and transactions in the network. Also, third-party spectrum sensors can monitor the network to detect misuse. The stakeholders can interact with the system via front-end application and Application Programming Interface (API). The system implements several SCs to conduct auctions, rate users and handle currency transactions.

The proposed system provides a real-time spectrum marketplace where nodes such as IoT devices, sensor network hubs, local network operators, and MNOs can purchase the spectrum from others. On the other hand, regulatory bodies are aware of these trades as they are also network nodes. The regulatory bodies are usually government entities who give the exclusive right to some MNOs in the first place.

B. *Adversary model and security features*

1) Adversary model: We assume the existence of a passive and active adversary capable of replaying, removing, changing, and inserting (parts of the) messages, cf. the Dolev-Yao model [24]. In addition, a lack of trust among the nodes is also inherently present in this particular scenario, and thus sufficient evidence of a well-behaving node should be provided. Therefore, protection should be provided against the most well-known attacks [25], [26] in this adversary model.

- Impersonation attack or man-in-the-middle attack: This type of adversary can act as one or other nodes and thus automatically has an advantage when constructing the final key when it knows more than one share. In order to guarantee that a node sends only one point to the network, we add a signature on the package. In addition, a counter is included to ensure they are not reused later.
- Replay attack: A replay adversary can send the messages at a later moment and tries to reuse previously known information, which would then result in a false key

TABLE I: Features Comparison with Key Existing Works

Features	[20]	[6]	[19]	[7]	[4]	[9]	[10]	[21]	[22]	[23]	Ours
Blockchain based	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Spectrum Trading Marketplace	✓	✗	✓	✓	✗	✗	✓	✓	✗	✓	✓
Automated Services	✗	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓
Spectrum Sensing	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✓
Spectrum Fraud Detection	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓
Off-Chain Storage	•	•	✗	✗	✗	✗	✗	✓	✗	✗	✓
Tailored Consensus	•	•	✓	✗	✗	✗	✗	✗	✓	✓	✓
Extra Cost of Mining	•	•	L	H	H	H	H	H	L	L	L
Computational Complexity	L	M	L	H	H	H	H	H	L	L	L

construction. In the proposed model, a counter in the certificate issued for B_is and a timestamp TS in the ZKP are used to avoid such attacks.

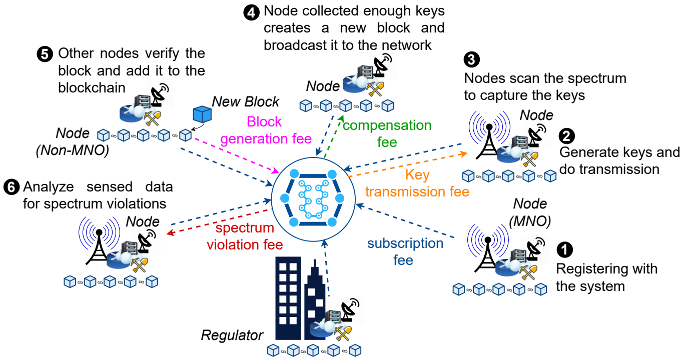
C. Security features

In order to overcome the above attacks, the following security features need to be satisfied by the protocol.

- Confidentiality: Only the node sharing the public key data (for individual shares and the resulting final key) should be aware of the corresponding private key data.
- Authenticity: An adversary cannot claim to knows the winning key without possessing each individual shares.
- Integrity: An adversary should not be able to change content to the message without being noticed.

D. Operation of the Proposed Platform

We can describe the overall operation of the proposed DSA system in six steps, as illustrated in Fig. 2. Furthermore, the arrows in Fig. 2 show the flow of transactions in the network.



4 Node collected enough keys creates a new block and broadcast it to the network
5 Other nodes verify the block and add it to the blockchain
3 Nodes scan the spectrum to capture the keys
Node
New Block
Block generation fee
compensation fee
Node (Non-MNO)
Node
2 Generate keys and do transmission
Key transmission fee
6 Analyze sensed data for spectrum violations
Node
Node (MNO)
spectrum violation fee
subscription fee
1 Registering with the system
Regulator

Fig. 2: The High-Level View of the Proposed DSA System

Step 1 All the stakeholders join as nodes by registering with the blockchain network. Stakeholders are supposed to pay a subscription fee.

Step 2 The proposed system uses a new consensus mechanism (details in section III-F). The blockchain creates and assigns individual keys to each node to transmit via random channels. Later we describe the message structure and countermeasures against attacks in the network. The system encourages key transmission by offering a transmission reward.

Step 3 The goal of the nodes is to sense the spectrum to capture these keys while collecting other spectrum sensing information.

Step 4 Whoever collects enough keys will create a new block. The node will transfer sensed data to off-chain storage and broadcast the new block to the network via a known channel.

Step 5 Other nodes will verify the new block and add it to the blockchain. The system rewards the winner miner with a block generation reward.

Step 6 Automated spectrum violation detection algorithms will run on the sensed data and collect penalties from spectrum misusers. The system also provides additional rewards for the node, which has added the relevant sensed data to discover the misuse. Moreover, the system grants a compensation to nodes whose spectrum is misused.

E. Deployment of the Blockchain

All the stakeholders except consumers in the system are nodes in the network. However, the set of tasks performed by each node would be different based on their role. All the mining nodes (MNO and non-MNO) must possess a Radio-Frequency (RF) spectrum sensor network with the ability to detect waveforms, modulations, energy levels and perform additional tasks such as running ML algorithms. Generally, we do not expect the regulatory bodies to purchase the spectrum. Nevertheless, they can still sell the spectrum at auctions. On the other hand, non-MNO miners may not possess the long-distance state-of-the-art transmitting antennas to participate in the key transmission process. Therefore, we expect to exclude them in the key transmission process. However, MNO miners must transmit the keys, and it is rewarded with a fee. Also, the transmitted key must reach most of the nodes in the network. Therefore, we assume that more than half of the network will recover a key transmitted by a node. We propose to rate the nodes based on their activities (i.e., key transmission, recording spectrum data, violation detection, spectrum auctions, etc.) and use these ratings to control access to the system's privileges, such as spectrum marketplace and various rewards. Since there is a specific set of hardware and software requirements to become a node in the network, it is more practical to use a consortium blockchain for the proposed system.

F. Consensus Mechanism: ***Distributed-Proof-of-Sense***

The DPoS consensus mechanism proposed in this paper is a decentralized key generation and verification process with non-interactive ECC-based ZKP following the Schnorr scheme

[27]. In the protocol steps, we have considered all the verifier nodes in the network as a single verifier for the simplicity of explanation. But in the proposed system, even though it has only a single prover, all the other nodes in the network will act as verifiers.

In the proposed system, miners (nodes) scan the spectrum and analyze the sensory data to capture the keys. Since each node transmits its key, miners need to collect at least *t-out-of-n* (where n is the total no. of keys and t is the threshold) keys to become the winner. The miner who captures t keys creates the next block and broadcasts it to the network for verification. Then, other miners can verify the solution and the block, and finally, the verified block is added to the existing chain. The system operates based on a distributed key generation and verification mechanism. The values for t and n are system parameters that need to be decided by the spectrum regulator. Variables such as the number of miners and the network's difficulty may influence t and n. We can briefly describe the overall operation of the consensus mechanism using five steps. Fig. 3 illustrates the workflow of the proposed mechanism.

Step 1 **Key Generation:** Each node in the network generates a point B_i (i.e., $B_i = a_iG$) on the elliptic curve. Here, we can consider B_i as the public key and a_i as the private key of the i^{th} node for a session.

Step 2 **Key Sharing:** Then, each node signs and transmits its key (a_i) in a randomly selected frequency. At the same time, nodes put B_i in the network so that every node in the network knows it.

Step 3 **Spectrum Sensing:** Nodes scan the spectrum and analyze the sensory data to capture the keys. Miners need to collect at least t keys to become the winner. Miners store these sensory data in an off-chain storage (eg: IPFS - InterPlanetary File System). The system uses this data to identify anomalies or violations in the system.

Step 4 **Winning Miner and Block Creation:** The miner who first captured the required number of key parts (i.e., threshold), multicasts it to the network.

Step 5 **Verification:** Other nodes in the network start the verification process. Once the network verifies the key, the new block is added to the chain and the winner node can earn a reward for that.

The main functions of the proposed system are as follows.

1) Key Generation: All the MNO nodes are responsible for key generation. Nodes need to agree on a standard EC (Elliptic Curve) E and generate points on that curve. Let a_i be the key of the i^{th} node and it expires at the end of each session. A session is the period it takes to generate a new block. A new session starts when a block is generated, and nodes generate new key pairs (B_i and a_i) for each session. If there are n number of nodes, then the final key a is the collection of all these keys (equation (1)). However, since we use a *t-out-of-n* threshold scheme, the winner node needs only to collect t keys ($t < n$).

Fig. 4 depicts the proposed structure of an individual key. Packets for both keys a_i and B_i has the same structure. A key is 192-bit in size (because we use *secp192r1* curve), with a 64-bit slot and two 32-bit slots reserved for the timestamp, node ID, and counter, respectively. All the mentioned fields are inputs to a hash function that produce a 128-bit hashed output (such as *SHA-2*). Finally, the packet is signed with the node's private key. The timestamp and counter collectively provide the resistance against replay attacks. At the same time, the block signature ensures that an adversary cannot claim it knows the winning key (which is generated using individual collected keys) since other nodes can check the signatures during the verification process.

2) Key Sharing: After key generation, all the MNO nodes transmit it via a random channel. Other miners (nodes) in the system do not know this random channel, and they must listen to the spectrum to capture these keys. Apart from the key, the transmitted message contains several other components as shown in Fig. 4. According to the proposed method, once a node collects t keys, it can create the next block. A node repeatedly retransmits its key for the ongoing session until a new block is generated and marks the end of the session. The retransmission interval also affects the block time of the network. Further research is needed to determine the best retransmission interval, and it is left for future work.

3) Spectrum Sensing: Miner nodes in the system use spectrum sensors (e.g., Software-Defined Radios) to listen to and capture the spectrum data. These sensors could be a network spread over a wide geographical area to collect additional and precise information. The miners can design sensors based on the area they want to cover and the frequency range. While continuously monitoring the spectrum for the keys, miners also collect valuable spectrum usage information. In general, RF spectrum sensors can collect information such as the geographical location of transmission, power and energy levels, and modulation rates [28]. Furthermore, sensor networks can capture some upper-layer details like protocol, wavelength, and waveform standards. Nodes temporarily store the data collected by sensors in the local storage until they get an opportunity to mine a block. The SCs that drive these violation detection algorithms may also optionally contain CR physical layer reconfiguration information, such as VITA49 hardware adaptations for each spectrum band and user scenario.

The recovery difficulty determines how hard it is to recover the keys successfully. This also affects the block time of the network. In DPoS, we use the characteristics of wireless channels to control the recovery difficulty. Table II presents the parameters that can affect the recovery difficulty.

4) Winning Miner and Block Generation: As per the proposed DPoS, the first miner that recovers at least t keys becomes the winner node. Fig. 5 shows the communication among nodes in the network from the key transmission to adding the new block. The winning miner generates the next block of the chain and is entitled to a reward after the verification. While creating the new block, the winner node also stores the collected spectrum data. The node uploads the sensed data separately in off-chain storage, and adds a pointer (e.g., IPFS hash) in the block. Fig. 6 presents the proposed block structure for the DSA system. After block generation, the winner node will broadcast the new block via a known channel to other nodes. This new block creation will trigger the start of a new session.

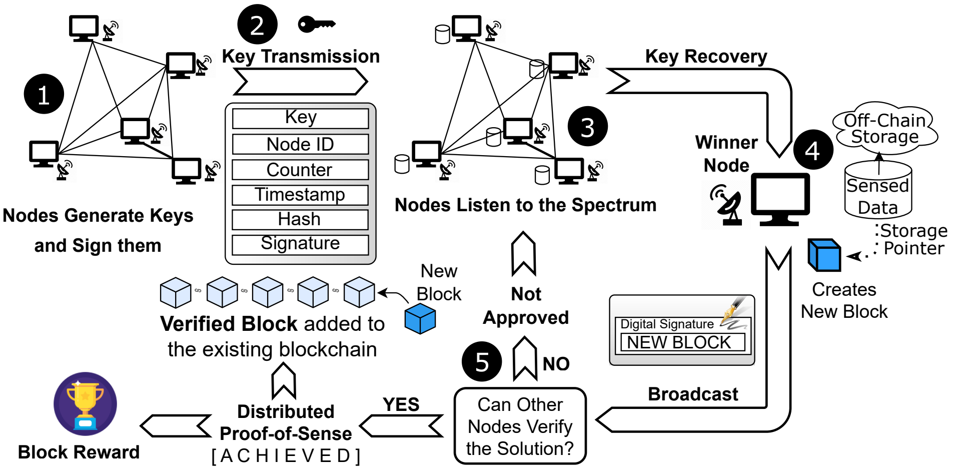


Fig. 3: The Workflow of Consensus Mechanism

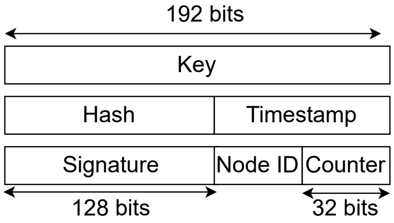


Fig. 4: Structure of an Individual Key

TABLE II: Key Recovery Difficulty

Component	Feature	Effect on Recovery Difficulty
Key	Key Length	Increase with size
	Total Nodes (N)	Decrease with N
	Threshold (t)	Increase with t
Wireless Channel	Free space losses	Increase with Losses
	Multi-path Fade	Increase with Fade
	Diffraction	Increase
	Absorption	Increase
	Reflection	Increase
	Atmospheric Losses	Increase
	Interference	Increase
Transmitter, Receiver	Modulation	Depend on Scheme
	Coupling Losses	Increase with Losses
	Error Correction	Decrease

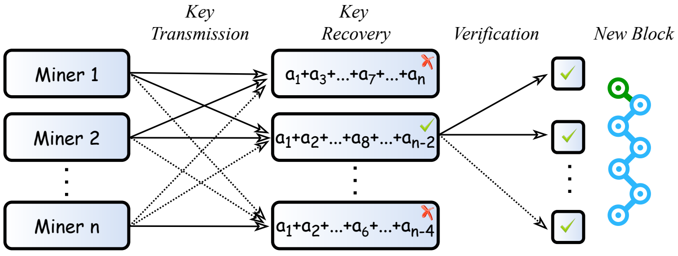

Key Transmission
Key Recovery
Verification
New Block
Miner 1
Miner 2
Miner n
$a_1+a_3+...+a_7+...+a_n$
$a_1+a_2+...+a_8+...+a_{n-2}$
$a_1+a_2+...+a_6+...+a_{n-4}$

Fig. 5: Communications in Distributed-Proof-of-Sense

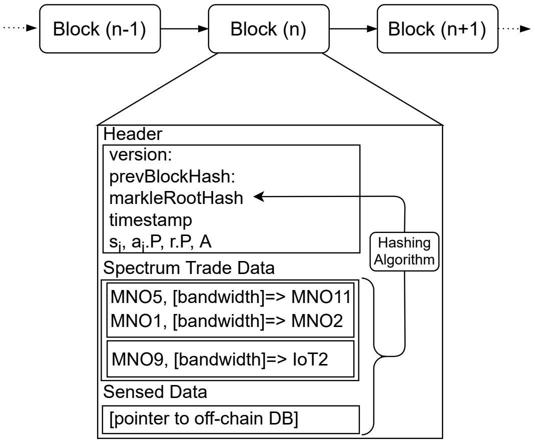


Fig. 6: The Block Structure

5) Verification: The verification process starts when the nodes receive a new block from a node. Fig. 7 presents the message flow for the verification process.

The message exchange proposed in ZKP (See Appendix B) uses the prover-verifier combination to demonstrate the verification process. However, in the proposed DPoS, multiple verifiers verify the solution simultaneously. This section explains the verification process with multiple verifiers.

In order to become the winner, a miner node needs to possess at least *t-out-of-n* key parts. In the single prover-verifier case, both parties know B (i.e., $B = aG$), the public key of the transmitter node. Since we use a threshold scheme, and every node transmits its key, the prover must prove more than one key in a verification session. Therefore, the verifier node creates a new key from the recovered keys. Equation (1) gives the final key as a combination of all captured keys. Together with this key, the verifier also sends the node IDs of the recovered keys.

$$a = a_1 + a_2 + ... + a_n \tag{1}$$

Then, other verifier nodes indirectly check the following expression to confirm the prover's claim to be true.

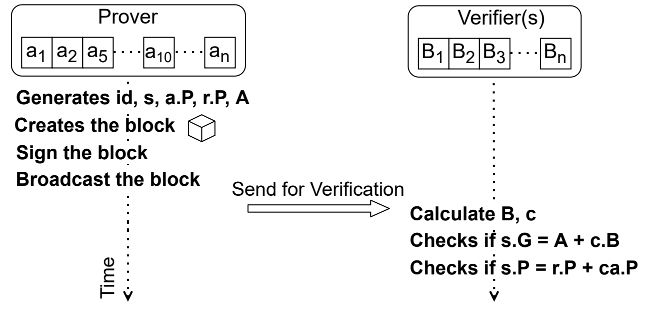


Fig. 7: The Message flow of the Verification Process

$$\begin{aligned} aG &= a_1G + a_2G + ... + a_nG \\ &= B_1 + B_2 + ... + B_n \end{aligned} \tag{2}$$

Since we propose a threshold scheme for the system, there is no need to construct the complete final key with all a_i s. A minimum of t keys is enough for a node to claim his achievement and become the prover. Then, the verification process takes place, and if verifiers can verify the solution, the prover becomes the winner. With the threshold scheme, the final key would not be the same for every node because there is no guarantee that every node can collect all parts due to the difficulty of the network (see Table II). For example, let $n = 10$ and $t = 6$. Then we can have 210 different combinations according to equation (3).

$$C_r^n = \binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{n!}{t!(n-t)!} \tag{3}$$

For the verification process with multiple verifiers, we use the protocol described below. This method allows us to build the system with the proposed threshold scheme.

First, the prover node generates a list that includes the IDs of transmitter nodes whose keys were recovered. Then, the prover calculates the a as in equation (1) and other parameters required for the verification. After receiving the data from the prover, the verifier can identify the respective nodes from the node ID list and calculate the public key as in equation (2). Note that the public keys (B) are known by everyone.

Prover

- Generate node ID list
  id = {node IDs of recovered a_i}
- Calculate a
  $a = a_1 + a_2 + ... + a_r + ... + a_n$
- Generates random r and compute A, such that $A = rG$
- Computes c = Hash ($aP|rP|A|id$)
- Computes s = r + ca
- Sends id, s, aP, rP, A to the verifier

Verifier

- Identify corresponding B_is from id list
- Calculate B
  $B = B_1 + B_2 + ... + B_r + ... + B_n$
- Computes c = Hash($aP|rP|A|id$)
- Checks if sG = A + cB
- Checks if sP = rP + caP

G. Spectrum Fraud Detection

The system analyses the data stored by miners in the key capturing process to identify unauthorized accesses (intentional or unintentional) to the spectrum. These data contain much information about the events that occurred in the system. The fraud detection mechanism can detect violations of MNO level sharing agreements and accessing the restricted spectrum in an area. The system uses SCs to automate this process. The governing ML algorithms for this process are yet to be determined. ML-based device identification schemes such as radio fingerprinting have shown some impressive results in recent studies [29] [30]. Implementing fraud detection mechanisms and ML algorithms is beyond the scope of this paper. Since we have the data now, that will be the next step of this research.

H. Miners Rewards and Other Payments

Several money transactions are involved in the system, including subscription fees, key transmission fees, block generation fees, fines for spectrum violation, and compensation for spectrum violation. Earnings from the nodes help to maintain a healthy amount of money for the system's continuous operation. The system spends earnings for transmission fees, block generation rewards, and compensations.

1) Subscription fee: All the nodes in the network are obligated to pay this fee. This fund collection helps to maintain a financially stable system. The system uses this money to pay other fees in the system.

2) Transmission Reward: Nodes that transmit keys for sessions are eligible for this reward. Transmission fees encourage the nodes to transmit keys continuously for every session.

3) Block Generation Reward: At the end of every new block generation, the winner node is eligible for this reward. Block generation fees encourage the nodes to scan the spectrum more and more precisely to become the winner.

4) Fraud Detection Reward: Nodes, whose spectrum data were used in identifying the violation are eligible for this.

5) Fines for Spectrum Violation: The nodes which are committing spectrum violations will be charged this fine. Spectrum violation fees discourage the users from breaking spectrum agreements and rules in the system

This paper does not cover the implementation of payment handling mechanisms. We left it for future work and we continue our research on designing the best method for handling currency transactions in the system.

IV. Numerical Analysis

This section presents the numerical analysis of the proposed DPoS. First, we present a comparison of the performance of the proposed DPoS with existing mechanisms such as PBFT, PoW, and Raft. The performance is evaluated in terms of communication complexity, spectrum requirement, transaction throughput, scalability and security bounds. Next, we discuss some features of the proposed blockchain network, such as forks, chain growth, and chain quality.

A. Performance Comparison with Existing Mechanisms

The four most important metrics to measure blockchain performance are security bound, node scalability, transaction throughput, and latency [31]. The consensus mechanism plays a vital role in determining those metrics. In [31], authors discuss the performance of consensus mechanisms for a wireless blockchain network, and Table III presents the comparison of different consensus mechanisms. Here, f is the number of faulty (malicious) nodes in the network, N is the total nodes, and t is the threshold of the proposed DPoS. Threshold (t) can vary from 1 to N, and it changes the communication complexity (see Fig. 5) of the network accordingly (considering the minimum requirements to achieve the consensus). The security bound of the network is the same as in the PoW. The scalability of the network is medium due to the Nt term in the communication complexity. When t goes to N, the scalability of the network reduces. However, in a practical deployment, t will always be less than N. The main purpose of the system is to collect spectrum data and detect spectrum violations. As a result, most nodes in this system will be spectrum sensors. The communication complexity is increased only by increasing the number of key transmitting nodes in the network, not by increasing the spectrum sensors.

1) Communication complexity: The communication complexity of a network refers to the number of communications between transmitter and receiver nodes. Fig. 8 illustrates the communication complexity of different consensus mechanisms presented in Table III. Here, we consider $t = N$ and $t = N/2$ cases for the proposed DPoS. The PBFT consensus mechanism required a $2N^2 + N$ communications making it the highest in Fig. 8. The proposed DPoS has a lower communication complexity in both $t = N$ and $t = N/2$ cases than BPFT because PBFT relies on three main stages to achieve an agreement among the nodes. In each stage of PBFT, broadcast communication is needed to exchange information among nodes. Therefore PBFT is more suited for a consortium or private blockchain networks that consist of a limited number of nodes. In Raft, the communication complexity $2N$ comes from communication between the head and follower nodes (uplink) and again from follower nodes and head (uplink). For PoW, $2N$ comes from broadcasting client request to all other nodes and broadcasting the winner miner's hash results to all other nodes. In the proposed DPoS, the Nt term represents the keys received by the winner node, and N is for the broadcast from the winner node to all other nodes.

2) Spectrum Requirement: The spectrum requirement of a wireless blockchain network refers to the needed spectrum resource for communication. While communication complexity is made of the number of receiver processes, spectrum requirement is the number of transmitter processes [31]. Even though this metric is only valid for a wireless blockchain network, the proposed consensus mechanism can be used in a wireless or regular blockchain network. Fig. 9 represents the spectrum requirement for different CMs presented in Table III. It is important to note that here we consider the simplest case in which one's radio power covers all nodes. The spectrum requirement can further vary with the network topology. Under these conditions, the spectrum requirements for PBFT, RAFT, PoW, and ours are $2N + 1$, $N + 1$, 2, and $N + 1$ respectively. In PBFT, $2N + 1$ consists of $2N$ spectrum resources for the communication among nodes in prepare and commit stages of the consensus mechanism and one resource for the pre-prepare stage where the leader node broadcasts a message to the rest of the nodes. For Raft, one spectrum resource is required for the downlink communication from head to followers, and N resources are required for the uplink communication from each follower node to the head. The spectrum requirement for the PoW is constant as it does not depend on the number of nodes in the network. This is because PoW consists of two broadcast messages: broadcast transactions and broadcast hash result of the winner node. The proposed DPoS requires N resources for key transmission and one resource for broadcasting the captured keys of the winner node.

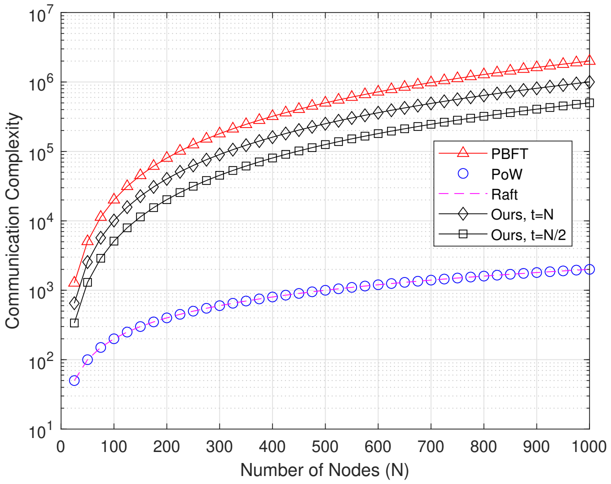


Fig. 8: Communication Complexity of CMs

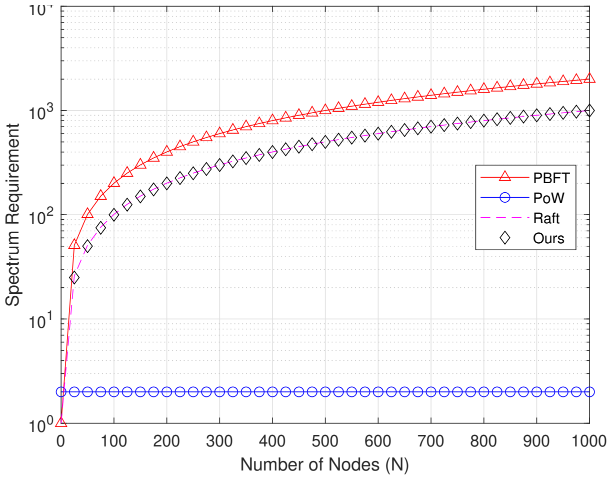


Fig. 9: Spectrum Requirements of CMs

3) Transaction Throughput: Transaction throughput denotes the number of transactions processed per second (TPS) in the system. Because of its computationally difficult hash puzzles, PoW has a low throughput. The proposed DPoS is based on spectrum sensing and is not as computationally difficult as PoW. However, the verification process takes some

TABLE III: Performance Comparison with Commonly Used Consensus Mechanisms

Consensus Mechanism	Suitable Type of Blockchain	Transaction Throughput	Scalability	Security Bound	Communication Complexity	Spectrum Requirement
PBFT [32]	Private/Consortium	High	Low	$3f+1$	$2N^2+N$	$2N+1$
Raft [33]	Private	Very High	Medium	$2f+1$	$2N$	$N+1$
PoW [34]	Public	Low	High	$2f+1$	$2N$	2
Ours	Private/Consortium	High	Medium	$2f+1$	$Nt+N$	$N+1$

Note: f = number of faulty nodes, N = total nodes, t = threshold for the proposed DPoS.

extra time due to ECC operations (overhead due to $Nt+N$ communication complexity of the network). As a result, we can conclude that it has a high-to-medium throughput. On the other hand, voting-based mechanisms have a higher throughput (100 to 1000 TPS) [31].

4) Scalability: The ability of the consensus mechanism to handle an increasing number of nodes is referred to as scalability. In theory, PoW has excellent scalability and can support as many users as the network allows. However, given the spectrum requirements of a wireless blockchain network, it is impossible to keep as many users. Voting-based mechanisms, on the other hand, rely heavily on inter-node communication. As a result, both PBFT and Raft have limited scalability. Because the number of message exchanges increases with the number of nodes in the network, the proposed DPoS has medium scalability. However, given the number of nodes in a DSA system, we believe scalability is adequate for the application in question.

5) Security Bound: The maximum number of faulty nodes tolerated by the consensus mechanism is known as the security bound. In general, the security bound for PoW is considered to be $2f+1$. As a result, a blockchain network based on PoW will compromise if a single entity controls more than 50% of the network's resources. If more than half of the nodes verify the constructed key, the proposed DPoS achieves consensus. As a result, DPoS shares the same security constraints as PoW. However, voting-based consensus mechanisms like PBFT and Raft define the number of faulty nodes in the network as inactive or malicious nodes [31]. These nodes send false information in order to jeopardize the network's stability. PBFT typically has a security bound of $3f+1$ (allowing 1/3 of faculty nodes) and Raft has a security bound of $2f+1$.

6) Impact of Transmission Power: This section analyzes the relationship between transmission power and the number of faulty nodes in the wireless blockchain network. In [35], authors study the viable area of a PBFT wireless blockchain network in terms of transmission power. We take a similar approach to investigate the minimum transmission power required to manage the proposed DPoS successfully. Here, we consider all nodes are having equal transmission power, receiver sensitivity and coverage radius.

First, we derive expressions for the constraints in the system and then study the relationships. Let us consider N nodes uniformly distributed in a circular area with a radius of R_0. The node distribution density (λ) can be expressed as,

$$\lambda = \frac{N}{\pi R_0^2} \tag{4}$$

Furthermore, let us assume the wireless network is noise-limited and all the nodes have the same receive sensitivity β. Then based on the maximum long-term averages of channel power, the coverage range of a node can be expressed as [36],

$$R = d_0 \left(\frac{P\kappa}{\beta}\right)^{\frac{1}{\gamma}} \tag{5}$$

where R is the radius of the circular coverage area, P is the transmission power of the node, κ is a unit-less constant that depends on the antenna characteristics and the average channel attenuation, d_0 is the reference distance for the antenna far-field, and γ is the path loss exponent. All the nodes within the transmission range receive the broadcast messages.

Constraint 1: Given that there are total N nodes and f faulty nodes in the blockchain network, in order to become a valid transaction it must be verified by at least $2f+1$ nodes. Therefore, once a node collect t keys, its solution must be verified by at least $2f+1$ nodes.

$$A_1\lambda \geqslant 2f+1 \tag{6}$$

Substituting from equation (5) to equation (6),

$$\begin{gathered}\pi R_1^2\lambda \geqslant 2f+1 \\ \pi d_0^2 \left(\frac{P_1\kappa}{\beta_1}\right)^{\frac{2}{\gamma}} \lambda \geqslant 2f+1\end{gathered} \tag{7}$$

Constraint 2: The total non-faulty nodes in the network is the different between total nodes (N) and faulty nodes (f), and it must be always greater than or equal to the threshold (t) of the consensus mechanism to ensure that a node receive at least t keys.

$$N - f \geqslant t \tag{8}$$

Constraint 3: When multiple nodes transmit simultaneously, there is an intersection area where nodes receive all these transmissions. Considering the minimum requirements, there should be at least one node in this intersection area in order to successfully go to the verification stage.

$$A_2\lambda \geqslant 1 \tag{9}$$

However, it is not practically possible to derive a general equation to describe the common intersection area of t circles, having the same radius R without knowing the distance between centers of each node. Therefore, we consider a simplified case in which the centers of all t nodes lay on vertices of a regular polygon that have t sides. This way, we can ensure the distance between two adjacent centers is always equal, and it should be small enough to create a intersection between all t circles. Furthermore, when circles intersect this way, the intersection area is the summation of t equal circular segments and a regular polygon with t sides.

The area of a regular polygon can be calculated using $n \times s \times a/2$, where n is the number of sides, s is the length of a side and a is the apothem. Apothem is the distance of a perpendicular line from any side of the polygon to its center and gives by $(s/2)\cot(\pi/n)$. Therefore, we can calculate the area of a regular polygon having t sides as follows,

$$A_{t\_sides} = \frac{ts^2 \cot\frac{\pi}{t}}{4} \tag{10}$$

We can calculate the area of circular segments using the angle θ expressed in radians where θ is the angle two intersection points of a circle creates with its center. Under the given assumptions, the total circular segment area is,

$$A_{t\_seg} = t \times \frac{R^2}{2}(\theta - \sin\theta) \tag{11}$$

By combining equations (10) and (11), we can create a equation to calculate the total intersection area,

$$A_2 = \frac{tR^2}{2}\left[\theta - \sin\theta + 2\sin^2\frac{\theta}{2}\cot\frac{\pi}{t}\right] \tag{12}$$

For example, using equations (12), the intersection area of three circles (A_{3C}) having the same radius R and their centers are equal distance apart can be expressed as in equation (13). Fig. 10 illustrate the intersection of circles.

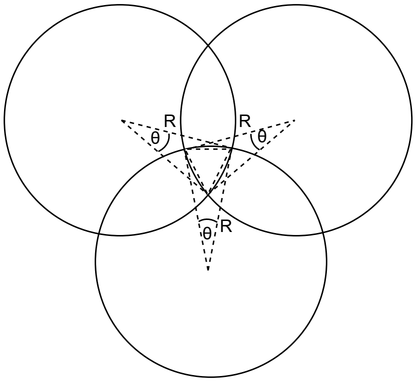


Fig. 10: Intersection of Three Circles

$$A_{3C} = \frac{3R^2}{2}\left[\theta - \sin\theta + \frac{2}{\sqrt{3}}\sin^2\frac{\theta}{2}\right] \tag{13}$$

Finally, by substituting from equation (12) and (5), the constrain 3 can be expressed as follows,

$$\frac{t\lambda}{2}d_0^2\left(\frac{P_1\kappa}{\beta_1}\right)^{\frac{2}{\gamma}}\left[\theta - \sin\theta + 2\sin^2\frac{\theta}{2}\cot\frac{\pi}{t}\right] \geqslant 1 \tag{14}$$

Fig. 11 illustrate the relation between faulty nodes and transmission power for the proposed DPoS and PBFT. The constraints and equations for PBFT consensus mechanism are taken from [35]. We use MATLAB to find the minimum transmission power required to achieve each mechanism's consensus successfully. The network coverage radius is taken as $R = 1000$ and nodes are uniformly distributed in the considered area with density $\lambda = \frac{1}{1000\pi} nodes/m^2$. The intersection points create an angle $\theta = \frac{\pi}{6}$ rad with the center of the transmitter node. The other system parameters are as follows, $\kappa = 1$, $d_0 = 1$, $\gamma = 4$, and $\beta = -84.5$ dBm. The PBFT graph is plotted based on the equations and parameters in [35] using MATLAB fmincon nonlinear optimization. According to results in Fig. 11, we can conclude that PBFT is better in terms of power. However, the proposed DPoS is better in terms of spectrum requirements since PBFT has multiple communication stages, which consume more spectrum resources.

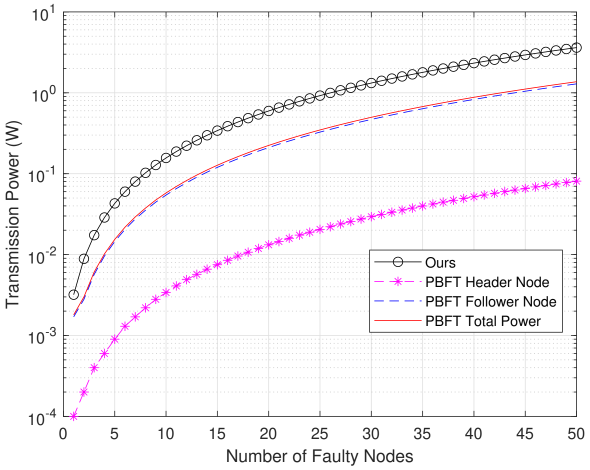


Fig. 11: Transmission Power of Ours vs PBFT

B. Forks in the Network

It is called a blockchain fork if a blockchain network has multiple heads at a time. During a blockchain fork, the nodes in the network do not agree on which block is the current head of the blockchain [37]. A blockchain fork may be extended by network partitions discovering more blocks building on their respective blockchain heads. One branch will eventually be longer than the others, and the partitions that did not adopt this branch as their own will switch to it. When it comes to this point, the fork is resolved, and the ledger replicas are consistent all the way up to the blockchain head. The blocks that are discarded in this process are known as orphan blocks.

C. Decker and R. Wattenhofert in [37] discussed in detail the information propagation in and forks in the Bitcoin network. Authors have calculated the probability for a blockchain fork in Bitcoin as 1.78% using their model. Furthermore, the authors observed a blockchain fork rate of 1.69%, which is close to the calculated probability. The authors collected information of blocks that have been propagated in the network between a height (i.e., the distance between a block and the genesis block) of 180,000 and a height of 190,000 (a total of 10,000 block intervals) and found 169 blockchain forks. Authors claim that the main reason a blockchain fork occurs is the network's significant propagation delay. For example, the Bitcoin network has more than 100 000 nodes, making it harder to propagate a block or transaction created at one end of the network to the rest.

In the context of the proposed blockchain network with a tailored consensus mechanism, the total number of nodes in the network is far smaller than in the Bitcoin network (because the network's transmission capabilities restrict the network's geographical stretch). Furthermore, Bitcoin has a size limit of 500kB for the block size [37], and typically a block contains more than 1000 transactions. However, in the proposed network, there will be fewer transactions due to a lower number of nodes, which infers the block size will be smaller than 500kB. Therefore, based on these metrics described in [37], we can extrapolate that the fork probability in the proposed network will be lower than that of Bitcoin (i.,e., < 1.69 %). A large amount of statistical information, such as average block size, probability of a random node finding a block, and probability of a network partition finding a conflicting block, is required to estimate a precise value [37].

C. Chain Growth

Chain growth expresses the minimum rate at which the chains of honest parties grow [38]. The idea of chain growth is motivated by an attacker who wishes to slow down the transaction processing time of the network. In [38], the chain growth property Q_{cg} is defined with parameters $\tau \in \Re$ (chain speed coefficient) and $s \in \mathbb{N}$ states that for any round $r > s$, where honest party has chain C_1 at round r and chain C_2 at round $r - s$, it holds $\mid C1 \mid - \mid C2 \mid \geq \tau.s$. The Bitcoin backbone protocol satisfies this property by parameter τ being equal to γ (γ is the probability of a round being successful or uniquely successful, where successful means at least one honest miner computers a solution in the current round, and uniquely successful means exactly one honest miner compute a solution in the current round). Because all legitimate miners choose the longest chain they see, and successful rounds occur at a rate γ, chains of these miners will grow at least at this rate [38] [39]. Since miners in the proposed network will also select the longest chain as the legitimate chain, we can reasonably assume Proof-of-Sense also satisfy the chain growth property (also, given the size of the proposed network compared to Bitcoin and this is a permissioned blockchain, we can be sure that all honest miners see the legitimate ledger without significant propagation delays).

D. Chain Quality

The chain quality parameter refers to the fraction of blocks in the chain that is mined by compliant (i.e., honest) miners. Because of the poor chain quality, attackers can replace other miners' blocks from the blockchain with their own [40]. As Rez Zhang and Bart Preneel highlighted in [40], Bitcoin's Nakamoto Consensus fails to achieve perfect chain quality. All other PoW protocols derived from the Nakamoto Consensus of Bitcoin have different design improvements to solve problems by increasing chain quality or developing defence mechanisms against the absence of perfect chain quality. In [40], chain quality Q is expressed as the expected lower bound on the fraction of blocks in the main chain mined by honest miners, given that the attacker holds a fraction of total mining power α_a. Given the compliant miners have mined B_c blocks on the main chain, attackers mined B_a blocks, and s is the strategy of attacker, we can define chain quality,

$$Q(\alpha_a) = \min_s \lim_{t \to \infty} \frac{B_c}{B_a + B_c} \tag{15}$$

Ideally, $Q(\alpha_a) = 1 - \alpha_a$, considering the attackers control main chain blocks at most proportional to the attacker's mining power α_a. In [40], authors have calculated the chain quality of several protocols, such as Nakamoto Consensus, uniform tie-breaking, smallest-hash tie-breaking, and unpredictable deterministic tie-breaking. As the discussion highlighted, to date, no protocol surpasses Nakamoto Consensus in all the assessed metrics if attackers have no propagation advantage. Like Nakamoto Consensus, Distributed-Proof-of-Sense also selects the longers chain (i.e., the most challenging chain to produce) as the tiebreaker. All miners discard orphaned blocks that are not on the longest chain.

V. Simulation Results

This section presents the performance evaluation of the proposed DPoS using MATLAB simulations. We assess the key recovery ability of the proposed DPoS under different keying strategies and wireless channel characteristics by simulating one transmitter node and one receiver node.

The key recovery probability of the system determines the block time and performance of the blockchain network. It can be calculated by counting the number of successful key recoveries against the total number of keys transmitted. The parameters mentioned in Table II describe the identified factors influencing the key recovery probability. We use MATLAB to investigate the effects of some of these factors on the key recovery probability. We calculate the average recovery probability considering the transmission of 10000 OFDM symbols. Note that we have not used any error correction mechanism in simulations, which will further increase the recovery probability.

We use ECC-based ZKPs as the core of the proposed consensus mechanism. The private key length is taken as 192 bits in the simulations because we use *secp192r1* curve for all the simulations and experiments. We use IEEE 802.11ax [41] for orthogonal frequency-division multiplexing (OFDM) transmission with 256 subcarriers, and it consists of 242 populated subcarriers, 11 sideband subcarriers, and 3 DC subcarriers [41]. In this section, we study the effect of modulation technique and channel conditions on the key recovery probability. Binary phase-shift keying (BPSK) and quadrature phase-shift keying (QPSK) are used as the modulation schemes, and each is tested under additive white Gaussian noise (AWGN), Rayleigh, and Rician (k factor = 10) channels. Fig. 12, Fig. 13 and Fig. 14 illustrate the key recovery probability under different channel conditions, modulation techniques, and thresholds, respectively. The results clearly show that we can change the key recovery probability by varying the parameters in Table II and ultimately control the block time.

A. Effects of Wireless Channel

The results in Fig. 12 show that simulations under AWGN channel conditions have a much higher recovery probability. This happens due to the absence of the fading effects. In Rician channel conditions, we take the k-factor as 10. Due to the presence of a dominant component (eg. line-of-sight, ground reflection) in Rician fading, it shows a higher recovery probability in contrast with Rayleigh fading. The Rayleigh fading is a special case of Rician fading with no dominant component (i.e., k-factor = 0), and due to this reason, the key recovery probability is lower under Rayleigh fading.

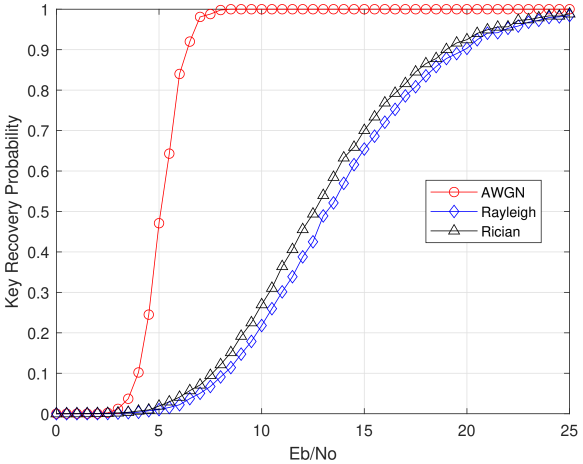


Fig. 12: The Key Recovery Probability under Different Channel Conditions

B. Effects of Modulation

The results in Fig. 13 show that the OFDM with QPSK modulation has a higher key recovery probability. The reason for the higher recovery probability is QPSK modulation encodes two bits per symbol, and therefore, one OFDM symbol can transmit multiple copies of the key. In contrast, BPSK only encodes one bit per symbol. Fig. 13 confirms that the key recovery probability varies depending on the modulation technique. Here, we only took into account two modulation methods, which amply show that the recovery difficulty varies with the modulation technique.

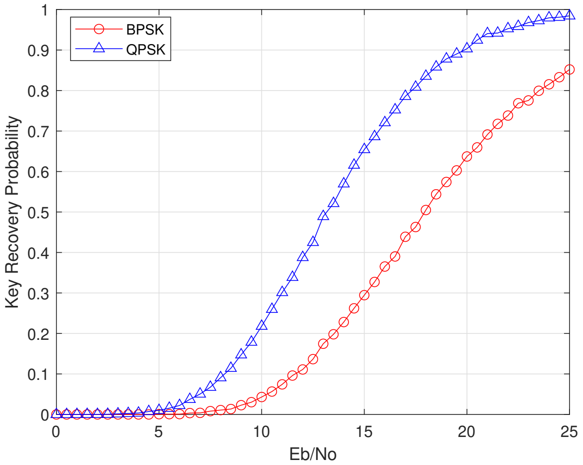


Fig. 13: The Key Recovery Probability under Different Modulations

C. Effects of Key Components

Fig. 14 illustrate the effect of key components (threshold). Here, we let the total key components be 30 and change the threshold from 10 to 30. Figure contains three curves drawn for $E_b/N_0 = 15$, $E_b/N_0 = 20$ and $E_b/N_0 = 25$. We plot all the curves using QPSK modulations in a Rayleigh fading channel. The results clearly show that it is easy to recover under a lower threshold.

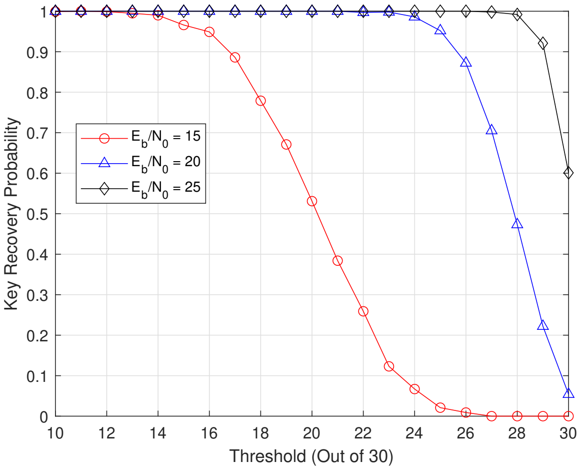


Fig. 14: Effect of Threshold for Key Recovery Probability

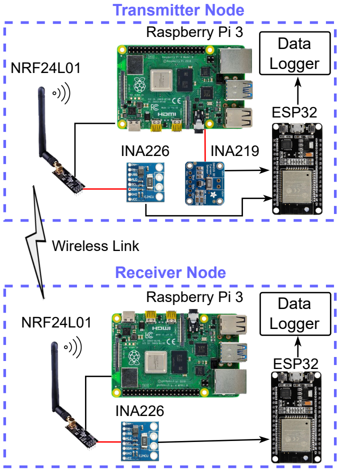


Fig. 15: High-Level View of the Testbed Arrangement

VI. Experimental Testbed and Results

We evaluate the performance of the proposed system using the experimental testbed shown in Fig. 15. Two Raspberry Pi 3 modules, two nRF24L01 transceivers, two ESP32 microcontroller units (MCUs), and three bi-directional current/power monitor modules (2 x INA226, 1 x INA219) comprise the testbed. The Raspberry Pi 3 module serves as the system's processor, performing computational tasks. The nRF24L01 is a single-chip radio transceiver with a maximum transmission distance of 1 km that operates in the 2.4 - 2.5 GHz band. The radio frond-end in the nRF24L01 uses Gaussian Frequency-Shift Keying (GFSK) modulation, and the frequency channel and air data rate are both configurable. During the experiments, we set the air data rate to 250 kbps. The INA226 and INA219 bi-directional current/power monitor Integrated Circuits (ICs) from Texas Instruments are current shunts and power monitors with an I2C interface. Table IV shows the parameters of the experiment. When measuring the energy consumption of algorithms, we use a single node to take all the measurements, and values are averaged after taking 100 readings.

We use the two INA226 ICs for the transceivers and INA219 IC for the Raspberry Pi module. We use INA219 IC for the processor because it can measure very low-level increments in the current, and the sensing range is 0 to 3.2A, which is essential to precisely measure the power without overflowing. The number of samples per average is set to 2, and the conversion time to 532 µs. The conversion time settings and averaging mode combinations both have trade-offs. By effectively filtering the signal, the chosen combination reduces measurement noise and increases measurement accuracy. We did, however, increase the sampling rate to 500 samples per second. We used several MCUs to ensure that the power measurement process did not interfere with the main processor's operation. As a result, we can assume that the main processor's power readings are caused solely by the instructions that run on it.

TABLE IV: Experimental Parameters

Parameter	Value
Frequency	2.4GHz
Modulation	GFSK
Data Rate	250kbps
Distance	1km

A. *Energy Utilization*

Table V presents the energy consumed by the Raspberry Pi for executing different operations associated with EC and ZKP. All the values presented in tables in this section are averaged after recording 100 readings of each operation. It is clear that public key generation (EC multiplication) has consumed more energy as it repeatedly solves coordinate geometry problems to find the point on the curve.

TABLE V: Execution Time and Energy for Basic EC and ZKP Operations

Operation	Execution Time (ms)	Energy (mJ)
Private Key Generation	0.3737	1.0248
Public Key Generation	315.5171	855.8680
Curve Points Addition	1.0950	3.1642
Private Key Addition	0.0186	0.0528
Private Key Multiplication	0.0212	0.0605
SHA-256 Hash	0.06069	0.1726

Table VI exhibits the energy consumption for major phases of the proposed consensus algorithm. Here, we set the key transmission distance to 1km and use two nodes.

TABLE VI: Energy Consumption for Distributed-Proof-of-Sense

Phase	Time (S)	Energy (J)
Key Pair Generation	1.25	3.5
Key Transmission	0.54	10.4
Key Recovery	0.54	6.5
Verification	2.94	8.1

We executed three different consensus mechanisms in the processor for the next experiment to determine the energy required to achieve the consensus. It is important to mention that, here, we did not implement a fully operational blockchain network. Instead, we implement only the winner-choosing mechanism and verification mechanism. In table VII, we can see the energy consumed by different consensus mechanisms. For the PoW, we set the difficulty level of the network to start the hash puzzle with six zeros.

PoS consensus mechanism has a relatively less complex winner-choosing mechanism. However, it requires energy to create the stake. Generally, PoS-based blockchain networks use cryptocurrency as the stake (for example, Ether in Ethereum network). That will add extra cost of operation for the DSA system. Therefore, existing PoS-based blockchain networks are highly expensive than the proposed system. If we want to create a low-cost PoS, it is possible to replace the stake with spectrum-sensed data. Thus, here we consider the stake as the spectrum-sensed data stored by the node. Under such a scheme, the power consumption for PoS in table VII is comprised of energy for the consensus mechanism and energy for the stake.

TABLE VII: Energy Consumption Comparison

Consensus Mechanism	Execution Time (S)	Energy (J)
Proof-of-Work [7] [21]	860.57*	1994.53
Proof-of-Stake [7] [21]	0.39*	29.81
Distributed-Proof-of-Sense	15.71	28.45

* The block time of a real PoS/PoW blockchain network can be higher than this due to propagation delays and sophisticated winner selection mechanisms.

TABLE VIII: Variation of Power Consumption with Difficulty

Difficulty Level	Execution Time (S)	Energy (J)
’0’	0.00134	0.0034
’00’	0.01421	0.0358
’000’	0.23439	0.6014
’0000’	4.19905	11.3850
’00000’	48.7342	134.1675
’000000’	860.574	1994.5301
’0000000’	20979.2	57646.5894

Based on the results in table VII, PoW uses the highest energy to achieve the consensus. This happens because solving the hash puzzle requires a lot of computational resources. Table VIII shows the time and energy needed by PoW vs. the number of zeros in the hash puzzle. On the other hand, PoS based blockchain system with the stake defined as spectrum sensed data is not yet practically implemented. Implementation of such systems needs to address the challenge of data verification. Since miner nodes can create faulty or dummy data to increase their stakes, stake pre-verification or pre-validation is necessary. For instance, ML/AI-based data verification methods may need to utilize here. This complex process will consume energy for this stake generation and verification process. Moreover, if we implement a DSA system with PoW, the system still consumes additional energy for spectrum sensors. However, with the proposed DPoS, we will be using an already implemented antenna and spectrum sensors for the consensus mechanism. Therefore, we can get an additional advantage of using the same infrastructure to support the blockchain. Therefore, we can conclude that the proposed mechanism is significantly more energy efficient than PoW and provide similar or improved performance than PoS.

B. Block Time

Using the testbed, we determined the average block time of the proposed system. The block time is the summation of key transmission, key recovery, and verification times. For the time measurements, we used a prototype network of ten nodes ($N = 10$) equipped with RF transceivers. Each node generates a key pair and transmits it over the wireless medium, and the verification can begin when a node collects t of them. The spectrum scanning algorithm determines whether the node executes a sequential search, random search, or another approach. For the experiment, we set $t = 7$ and scanning algorithms in a way that the node first scans the expected frequency bands sequentially and then starts random scanning. If the node finds keys in the scanning process, it will remember that frequency band and not scan it again for the keys until the session ends. Once the other nodes verify the winner's solution, the winner node can generate the next block and earn a reward. The experiment was carried out inside a 20-meter-radius circle with no obstacles where prototype nodes were randomly placed inside. Fig. 16 shows the results of the experiment for 100 block times. The average block time is 15.71 seconds, and the shortest block time is 14.03 seconds. We can see a variation in the block time around the average line. This is due to the interferences caused by the wireless medium. Furthermore, we slightly changed the arbitrary positions of the nodes within the 20- meter-radius circle during the 100 tests to get a better average block time. That also causes a change in the effect of interference and a change in the block time.

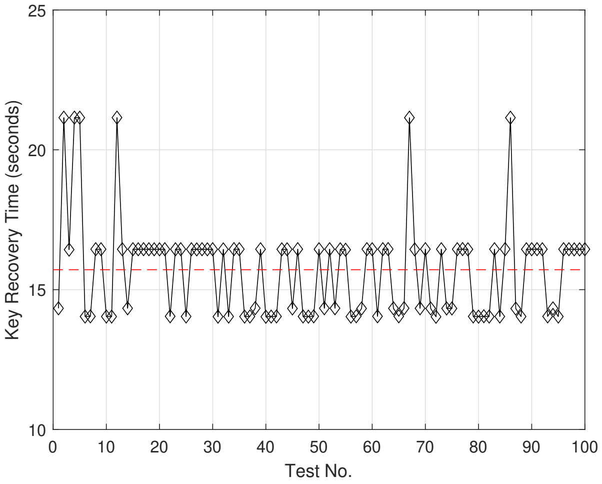


Fig. 16: E2E Delay of the Proposed System

VII. Conclusion

This paper proposed a blockchain-based DSA system with a novel consensus mechanism tailored specifically for the use case. The new Distributed-Proof-of-Sense consensus mechanism is based on ECC-based ZKP, which is lightweight and secure. Instead of resource-intensive cryptographic operations, the proposed consensus mechanism is based on wireless spectrum sensing processes. As a result of its tailored features, the proposed system is energy efficient and outperforms existing systems. We demonstrated the system's performance using MATLAB simulations of IEEE 802.11ax with 256 subcarriers. The results show that by changing specific parameters, we can control the network's block time and difficulty. Then, in a testbed, we implemented various consensus algorithms and measured the energy consumed by each mechanism. The results clearly demonstrate that the proposed mechanism is effective. Aside from energy consumption, the new mechanism allows for the detection of network fraud using sensed data. In general, our DSA system increases spectrum utilisation and ensures interference-free service. When compared to existing DSA systems, the system can save a significant amount of money on management costs. This paper covers the implementation of the consensus mechanism and fundamental performance evaluations. The development of a complete blockchain-based DSA system that runs with the proposed consensus mechanism and includes features such as analysing the collected sensed data using ML/AI algorithms is left for future work. Furthermore, the development of services such as conducting spectrum auctions, bidding for spectrum, and handling payments need to be implemented using smart contracts in future work.

References

[1] V.-D. Nguyen and O.-S. Shin, "Cooperative prediction-and-sensing-based spectrum sharing in cognitive radio networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 4, no. 1, pp. 108–120, 2018.

[2] M. Gomez, M. Weiss, and P. Krishnamurthy, "Improving Liquidity in Secondary Spectrum Markets: Virtualizing Spectrum for Fungibility," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 2, pp. 252–266, 2019.

[3] V. Valenta, R. Maršálek, G. Baudoin, M. Villegas, M. Suarez, and F. Robert, "Survey on spectrum utilization in europe: Measurements, analyses and observations," in *2010 Proceedings of the Fifth International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, 2010, pp. 1–5.

[4] T. Ariyarathna, P. Harankahadeniya, S. Isthikar, N. Pathirana, H. D. Bandara, and A. Madanayake, "Dynamic spectrum access via smart contracts on blockchain," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2019, pp. 1–6.

[5] H. Griffiths, S. Blunt, L. Cohen, and L. Savy, "Challenge problems in spectrum engineering and waveform diversity," in *2013 IEEE Radar Conference (RadarCon13)*, 2013, pp. 1–5.

[6] B. Cho, K. Koufos, R. Jäntti, and S. Kim, "Co-Primary Spectrum Sharing for Inter-Operator Device-to-Device Communication," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 1, pp. 91–105, 2017.

[7] M. B. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, "On the Application of Blockchains to Spectrum Management," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 2, pp. 193–205, 2019.

[8] K. Kotobi and S. G. Bilén, "Blockchain-enabled spectrum access in cognitive radio networks," in *2017 Wireless Telecommunications Symposium (WTS)*. IEEE, 2017, pp. 1–6.

[9] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *ieee vehicular technology magazine*, vol. 13, no. 1, pp. 32–39, 2018.

[10] M. Khan, M. Jamali, T. Maksymyuk, and J. Gazda, "A Blockchain Token-Based Trading Model for Secondary Spectrum Markets in Future Generation Mobile Networks," *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1–12, 08 2020.

[11] H. Xu, P. V. Klaine, O. Onireti, B. Cao, M. Imran, and L. Zhang, "Blockchain-Enabled Resource Management and Sharing for 6G Communications," *Digital Communications and Networks*, vol. 6, no. 3, pp. 261–269, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864820300249

[12] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6g: Challenges, opportunities and research directions," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.

[13] A. H. Khan, N. Ul Hassan, C. Yuen, J. Zhao, D. Niyato, Y. Zhang, and H. V. Poor, "Blockchain and 6g: The future of secure and ubiquitous communication," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 194–201, 2022.

[14] S. Yrjölä, "Analysis of blockchain use cases in the citizens broadband radio service spectrum sharing concept," in *International Conference on Cognitive Radio Oriented Wireless Networks*. Springer, 2017, pp. 128–139.

[15] N. C. Luong, T. T. Anh, H. T. T. Binh, D. Niyato, D. I. Kim, and Y.-C. Liang, "Joint transaction transmission and channel selection in cognitive radio based blockchain networks: A deep reinforcement learning approach," in *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2019, pp. 8409–8413.

[16] S. Han and X. Zhu, "Blockchain based spectrum sharing algorithm," in *2019 IEEE 19th International Conference on Communication Technology (ICCT)*, 2019, pp. 936–940.

[17] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 451–466, 2019.

[18] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5g beyond," *IEEE Network*, vol. 33, no. 3, pp. 10–17, 2019.

[19] Y. Liang, C. Lu, Y. Zhao, and C. Sun, "Interference-based consensus and transaction validation mechanisms for blockchain-based spectrum management," *IEEE Access*, vol. 9, pp. 90 757–90 766, 2021.

[20] S. K. Jayaweera and T. Li, "Dynamic Spectrum Leasing in Cognitive Radio Networks via Primary-Secondary User Power Control Games," *IEEE Transactions on Wireless Communications*, vol. 8, no. 6, pp. 3300–3310, 2009.

[21] T. Maksymyuk, J. Gazda, M. Volosin, G. Bugar, D. Horvath, M. Klymash, and M. Dohler, "Blockchain-Empowered Framework for Decentralized Network Management in 6G," *IEEE Communications Magazine*, vol. 58, no. 9, pp. 86–92, 2020.

[22] J. Ye, X. Kang, Y.-C. Liang, and S. Sun, "A trust-centric privacy-preserving blockchain for dynamic spectrum management in iot networks," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13 263–13 278, 2022.

[23] Z. Cheng, Y. Liang, Y. Zhao, S. Wang, and C. Sun, "A multi-blockchain scheme for distributed spectrum sharing in cbrs system," *IEEE Transactions on Cognitive Communications and Networking*, vol. 9, no. 2, pp. 266–280, 2023.

[24] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[25] A. Braeken, "A. public key versus symmetric key cryptography in client–server authentication protocols," *Int. J. Inf. Secur.*, vol. 21, pp. 103–114, 2022.

[26] T. Hewa, A. Braeken, M. Ylianttila, and M. Liyanage, "Blockchain-based automated certificate revocation for 5g iot," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–7.

[27] C. P. Schnorr, "Efficient Signature Generation by Smart Cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, Jan 1991. [Online]. Available: https://doi.org/10.1007/BF00196725

[28] Y. Arjoune and N. Kaabouch, "A Comprehensive Survey on Spectrum Sensing in Cognitive Radio Networks: Recent Advances, New Challenges, and Future Research Directions," *Sensors*, vol. 19, no. 1, 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/1/126

[29] A. Al-Shawabka, F. Restuccia, S. D'Oro, T. Jian, B. Costa Rendon, N. Soltani, J. Dy, S. Ioannidis, K. Chowdhury, and T. Melodia, "Exposing the Fingerprint: Dissecting the Impact of the Wireless Channel on Radio Fingerprinting," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, 2020, pp. 646–655.

[30] K. Sankhe, M. Belgiovine, F. Zhou, L. Angioloni, F. Restuccia, S. D'Oro, T. Melodia, S. Ioannidis, and K. Chowdhury, "No Radio Left Behind: Radio Fingerprinting Through Deep Learning of Physical-Layer Hardware Impairments," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 1, pp. 165–178, 2020.

[31] L. Zhang, H. Xu, O. Onireti, M. A. Imran, and B. Cao, "How much communication resource is needed to run a wireless blockchain network?" 2021.

[32] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, ser. OSDI '99. USA: USENIX Association, 1999, p. 173–186.

[33] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference*, ser. USENIX ATC'14. USA: USENIX Association, 2014, p. 305–320.

[34] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Cryptography Mailing list at https://metzdowd.com*, 03 2009.

[35] O. Onireti, L. Zhang, and M. A. Imran, "On the viable area of wireless practical byzantine fault tolerance (pbft) blockchain networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.

[36] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[37] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *IEEE P2P 2013 Proceedings*, 2013, pp. 1–10.

[38] A. Kiayias and G. Panagiotakos, "Speed-Security Tradeoffs in Blockchain Protocols," Cryptology ePrint Archive, Paper 2015/1019, 2015, https://eprint.iacr.org/2015/1019. [Online]. Available: https://eprint.iacr.org/2015/1019

[39] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Advances in Cryptology - EUROCRYPT 2015*, E. Oswald and M. Fischlin, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 281–310.

[40] R. Zhang and B. Preneel, "Lay down the common metrics: Evaluating proof-of-work consensus protocols' security," in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 175–192.

[41] Q. Qu, B. Li, M. Yang, Z. Yan, A. Yang, D.-J. Deng, and K.-C. Chen, "Survey and Performance Evaluation of the Upcoming Next Generation WLANs Standard - IEEE 802.11ax," *Mobile Networks and Applications*, vol. 24, 10 2019.

Pramitha Fernando (STM'17) received B.Sc degree in electrical and information engineering from University of Ruhuna, Galle, Sri Lanka. He is reading for the M.Sc in applied computer science at Vrije Universiteit Brussel (VUB), Belgium. His research interests are information security, blockchain, and wireless communication.

Keshawa Dadallage received his B.Sc. degree in electrical and information engineering from the University of Ruhuna, Galle, Sri Lanka in 2017. His research interests are wireless communication, sensors and transducers, IoT, blockchain, and network security.

An Braeken is full time professor at VUB-INDI. Her interests include lightweight security and privacy protocols for IoT, cloud and fog, blockchain and 5G security.

Tharindu Gamage is currently working as a Lecturer in the Department of Electrical and Information Engineering, University of Ruhuna, Sri Lanka. His research interests are IoT, Embedded Systems, High Performance Computing and Medical Image Processing. URL: http://eie.eng.ruh.ac.lk/team/tharindu-gamage

Chatura Seneviatne (S11, M18) is currently working as a Senior Lecturer in the Department of Electrical and Information Engineering, University Ruhuna, Sri Lanka. His research interests include signal processing, data aggregation and wireless communication. URL: http://eie.eng.ruh.ac.lk/team/chatura-seneviratne/

Arjuna Madanayake (M'03) received Ph.D. degree in Electrical Engineering from the University of Calgary, AB, Canada in 2008. Dr. Madanayake is an Associate Professor of Electrical and Computer Engineering at Florida International University (FIU), Miami, Florida,. His research interest including wireless communications, spectrum, radar and phased-arrays, electronic systems, digital signal processing, mm-wave receivers, antenna array processing, and analog CMOS computing.

Madhusanka Liyanage (STM'07–M'16–SM'20) is an Assistant Professor/Ad Astra Fellow and Director of Graduate Research at the School of Computer Science, University College Dublin, Ireland. Dr. Liyanage's research interests are 5G/6G, SDN, IoT, Blockchain, MEC, mobile, and virtual network security. More info: www.madhusanka.com