



| | |
|-------------------------------------|---|
| Title | Proof-of-Sense: A Novel Consensus Mechanism for spectrum Misuse Detection |
| Authors(s) | Fernando, Pramitha, Dadallage, Keshawa, Gamage, Tharindu, Liyanage, Madhusanka, et al. |
| Publication date | 2022-12 |
| Publication information | Fernando, Pramitha, Keshawa Dadallage, Tharindu Gamage, Madhusanka Liyanage, and et al. "Proof-of-Sense: A Novel Consensus Mechanism for Spectrum Misuse Detection." IEEE, December 2022. https://doi.org/10.1109/tii.2022.3169978 . |
| Publisher | IEEE |
| Item record/more information | http://hdl.handle.net/10197/12982 |
| Publisher's statement | © 2022 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. |
| Publisher's version (DOI) | 10.1109/tii.2022.3169978 |

Downloaded 2026-05-02 01:18:03

The UCD community has made this article openly available. Please share how this access benefits you. Your story matters! (@ucd_oa)



© Some rights reserved. For more information

Proof-of-Sense: A Novel Consensus Mechanism for Spectrum Misuse Detection

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

Abstract—Optimal use of scarce radio spectrum is essential in the proliferation of beyond 5G networks, and promising blockchain technology offers various benefits for the spectrum management. However, existing blockchain-based solutions are expensive, non-optimized, and lack spectrum fraud detection. This paper proposes a novel consensus mechanism for a blockchain-based Dynamic Spectrum Access (DSA) system. The proposed “Proof-of-Sense” consensus mechanism operates based on spectrum sensing procedures rather than cryptographic calculations. It is specially designed to address fraudulent/unauthorized access to the spectrum by analyzing the sensed spectrum data. The core of the consensus mechanism is a cryptographic key sharing mechanism inspired by Shamir’s secret sharing scheme. Moreover, the proposed DSA system can enable different micro-services such as automated spectrum auctions, payment and penalty handling, and spectrum fraud detection. A proof-of-concept based on experimental approaches coupled with Matlab simulations is presented to analyze the performance of the proposed consensus mechanism.

Index Terms—Blockchain, Consensus Algorithm, Dynamic Spectrum Access, Smart Contracts, Spectrum Management, Spectrum Sensing, Spectrum Misuse

I. INTRODUCTION

THE electromagnetic radio spectrum is a valuable and scarce natural resource in wireless communication. The popularity of telecommunication services causes increased capacity needs, leading to a rapid increase in bandwidth. Furthermore, billions of connected IoT devices and massive growth of services in 5G/6G wireless networks fuel the need

Manuscript received December 29, 2021; revised March 16, 2022; accepted April 12, 2022. This work has been performed under the framework of 6Genesis Flagship (grant 318927) project. Paper no. TII-21-5844. (Corresponding author: Madhusanka Liyanage)

Pramitha Fernando is with the Faculty of Engineering, Vrije Universiteit Brussel (VUB), Brussels, Belgium. e-mail: warnakula-suriya.pramitha.v.fernando@vub.be

Keshawa Dadallage, Tharindu Gamage, and Chathura 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, chathura@eie.ruh.ac.lk

Arjuna Madanayake is with the Department of Electrical and Computer Engineering, 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, the Centre for Wireless Communications, University of Oulu, Finland, and the Department of Electrical and Information Engineering, University of Ruhuna, Galle, Sri Lanka. e-mail: madhusanka@ucd.ie, madhusanka.liyanage@oulu.fi

for efficient, robust, and secure spectrum management mechanisms to prevent interference and offer guaranteed network conditions.

In today’s wireless world, spectrum allocation is based on the static assignment of the spectrum controlled by regulatory bodies, for example, the Federal Communications Commission (FCC) in the United States. Static assignments often lead to an underutilized spectrum. Therefore, several Dynamic Spectrum Access (DSA) concepts have been proposed to mitigate these issues in conventional spectrum allocation systems.

Cognitive Radio (CR) is an emerging technology that relies on DSA principles. CR proposes to manage the licensed spectrum dynamically by allowing unlicensed Secondary Users (SU) to opportunistically access the licensed spectrum that belongs to Primary Users (PU) without causing harmful interferences [1]. Spectrum Access System (SAS) is an example of a DSA system. In SAS, an automated frequency coordinator entity manages the spectrum sharing on a dynamic, as-needed basis across three tiers: incumbent access, priority access, and general authorized access. The idea of SAS was sustained in 2015 when the FCC adopted rules for shared commercial use of the 3.5 GHz band (3550-3700 MHz) [2].

Co-Primary Spectrum Sharing (CoPSS) is a dynamic spectrum sharing method in which the regulator allocates a non-exclusive band of the spectrum to several potential operators for shared use [3]. Multiple operators jointly use the allocated spectrum under rules and conditions (policies) laid down in a mutual agreement between all the parties. The allocation of the 3.5GHz band for fixed Broadband Wireless Access (BWA) in 2004/5 by the German Regulator (REGTP) is an example for the CoPSS model [4].

A. Limitations of Existing Dynamic Spectrum Sharing Systems

Today, a trustworthy third party (i.e., a mediator) must manage the sharing management systems as the stakeholders may likely not trust each other. Moreover, this process costs extra money for the operators and indirectly for customers due to third-party commissions and fees. Spectrum fraud detection is essential to maintaining a reliable DSA system. Spectrum fraud refers to unlawful access to licensed radio spectrum with intentional or unintentional harmful interference to rightful spectrum users by violating agreements. Spectrum violations significantly affect the Quality of Service (QoS) in

the PUs' systems and ultimately discourage operators from using dynamic spectrum sharing. However, the existing DSA approaches still do not support the automatic detection of unauthorized spectrum usage.

Detecting spectrum violations is always challenging because deploying sensors for Mobile Network Operators (MNOs) and spectrum regulators is difficult and expensive. With demanding requirements of highly localized services to meet the ultralow latency, high-speed requirements of critical IoT services such as in healthcare [5], telecommunication service providers need to use local network operators. With arising local operator concepts such as Local 5G Operators (L5GOs), Local Mobile Network Operators (LMNOs), Mobile Virtual Network Operators (MVNOs), there will be more spectrum tradings. Furthermore, DSA could have potential applications for wireless sensors networks, IoT data transmissions, Device-to-Device (D2D) communications. Since most of the mentioned entities do not have an exclusive right to the spectrum, they can rent frequency bands via the DSA system to transmit data to another location. All these potential use cases highlight the possibility of more frequent spectrum violations and the need for a superior DSA system.

B. Role of Blockchain for Dynamic Spectrum Sharing

Blockchain is a time-stamped series of immutable data records managed by a cluster of distributed computers not owned by a single entity. Blockchain offers several advantages such as decentralization, transparency, and immutability, which are useful in many applications, including dynamic spectrum sharing [6]. Recently, blockchain and smart contracts have been regarded as an emerging key enabler in the Internet of Things (IoT) ecosystem to provide a trusty system [7]. In DSA, blockchain can primarily store data securely with non-repudiation and automate complex activities, such as conducting automated, fast spectrum auctions using Smart Contracts (SCs). SCs is a small self-executable application that runs on a blockchain similar to micro-services. When the conditions defined in an SC are met, the code inside the contract will be executed automatically. The introduction of a marketplace to exchange the spectrum is the most intended use case of blockchain in the DSA domain [8] [9]. SCs can automate the auctioning functions and establish fair and dynamic agreements between stakeholders in such spectrum exchange marketplaces. Stakeholders can directly use the blockchain because of its inherent properties that make the need for trust obsolete. As a result, it vastly reduces the operation cost of the system. Moreover, the lack of transparency can be solved as all the stakeholders can check the history of spectrum usage and agreements from the immutable ledger records.

Several blockchain-based DSA systems have been developed in the literature. Weiss *et al.* in [6] proposed utilization of blockchain for spectrum sharing and discussed its benefits and limitations such as massive energy expenditures, scalability, governance, and interoperability are the major challenges in blockchain systems. T. Maksymuk *et al.* in [10] discussed the opportunities and challenges of the integration of blockchain into 6G mobile networks in terms of spectrum and

infrastructure sharing. The authors highlighted tokenization of spectrum and infrastructure and implementing smart contracts for service provisioning with intelligent spectrum trading as key implementation aspects of blockchain for 6G. M. Khan *et al.* in [11] proposed a Secondary Spectrum Market (SSM) with an automated pricing model using a blockchain token called spectrum dollar. The authors claimed that by applying the floor-and-trade rule, the system could regulate the token pricing based on the performance of the overall trades in SSM, and this methodology minimized the monitoring overhead. H. Huang *et al.* in [12] proposed a Network Functions Virtualization (NFV) and blockchain-enabled 5G architecture for ultra-reliable and low-latency (URLLC) communications. The authors discussed a spectrum sharing mechanism built on NFV, blockchain, and software-defined networking. In [13], authors proposed an interference-based consensus mechanism for blockchain-based spectrum management. It is based on comparing aggregated interference experienced by each node. The node that suffers the most aggregated interference will obtain the accounting right as a compensation.

In most of the existing blockchain-based DSA approaches, multipurpose consensus mechanisms such as Proof-of-Work (PoW) and Proof-of-Stake (PoS) operate as a separate service. Such consensus mechanisms based DSA systems suffer from excessive and additional energy utilization for the computation heavy mining process. The lack of a suitable and tailored consensus mechanism is the main limitation of existing blockchain-based spectrum sharing systems. Moreover, none of the existing blockchain or non-blockchain solutions offer automatic spectrum fraud detection and mitigation.

C. Our Contribution and Outline

This paper proposes a new consensus mechanism for a blockchain-based DSA system to mitigate the limitations in existing DSA systems. The new "*Proof-of-Sense*" consensus mechanism can eliminate the additional cost of unnecessary computational overhead and motivates the miner to collect helpful spectrum sensing information for spectrum management and fraud detection. This paper explains the operation of the Proof-of-Sense consensus mechanism, such as cryptographic key sharing mechanism, the key recovery process, block generation and verification process, and collection of spectrum data. Moreover, the performance of the proposed solution is analyzed using MATLAB simulations and hardware implementation. We compare the performance of the new consensus mechanism with existing schemes.

The remainder of this article can be outlined as follows. Section II introduces the proposed Proof-of-Sense consensus mechanism and the DSA system. Section III describes the testbed and simulations used to evaluate performance of the proposed mechanism and it further discuss the simulation results. Section IV compares the proposed system with related works. Finally section V contains the conclusion.

II. THE OPERATION OF THE PROPOSED PROOF-OF-SENSE CONSENSUS MECHANISM

This section presents the design of the proposed consensus mechanism, which combines DSA and spectrum sensing with

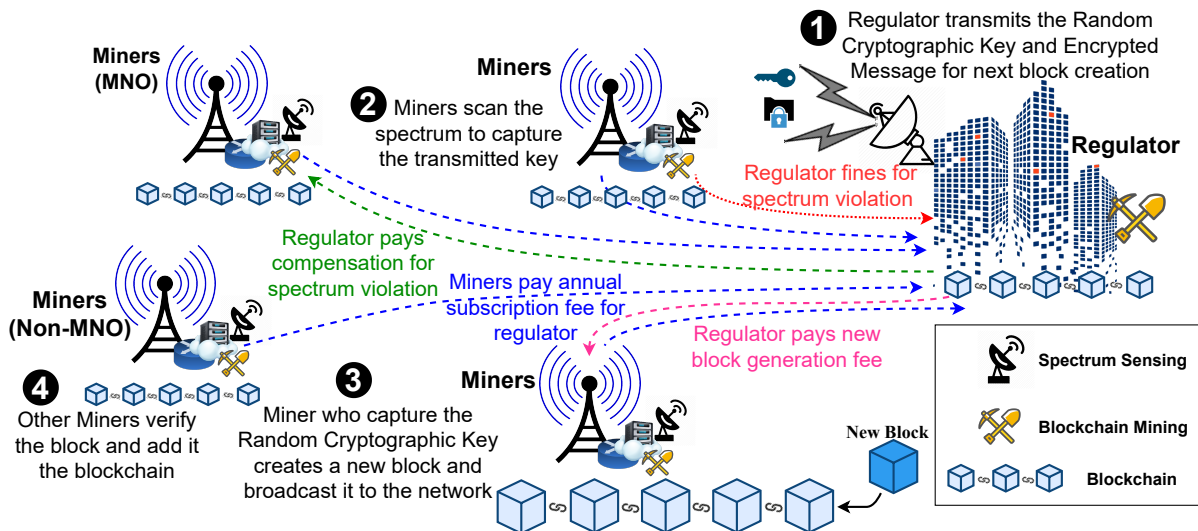


Fig. 1. The High-Level View of the Proposed Architecture

blockchain to create a new paradigm of spectrum management.

A. Stakeholders of the Proposed System

There are several stakeholders in the DSA ecosystem, such as MNOs, SUs, spectrum regulators, and third-party spectrum sensors. Note that not all the stakeholders have the same functionalities/responsibilities in the network. MNOs are the entities that lease spectrum chunks to the SUs. An MNO can also be a SU that buys spectrum from another MNO. A spectrum regulator is usually a government entity that governs the spectrum regulation within the country. The regulator sells the licenses for the spectrum to the MNOs, which give exclusive rights to use the particular spectrum. The spectrum regulator also can lease spectrum chunks for SUs. However, the most crucial role of the regulator is to monitor the spectrum transactions that happen in the network via the blockchain. Furthermore, the regulator can have higher authority than other nodes when imposing penalty fees after detecting a spectrum violation as it represents an independent government body. Finally, the third-party spectrum sensors are non-MNO individual miners in the network. They do not sell, lease or buy spectrum and their functionality is limited to collecting spectrum data and analyzing them.

B. Spectrum Sensing Process

The proposed DSA system contains the spectrum sensors deployed by MNOs and other third-party miners. These spectrum sensors continuously sense the radio spectrum and capture whitespace information. This spectrum sensing process is motivated by a reward scheme, and the sensors act as the miners of the blockchain network.

The “regulator” transmits a secret key called Random Cryptographic Key (RCK) in a randomly selected frequency band. All the sensors try to capture this key by sensing the spectrum. The first miner who successfully recovers the RCK can create the next block, receiving the mining reward. While continuously monitoring the spectrum, the sensors also collect

spectrum usage information. The system uses such information to identify spectrum violations (i.e., fraud). Miners can obtain additional rewards for their sensed data if fraud is detected based on that.

Thus, the system encourages spectrum sensors to collect and store information such as transmitter characteristics, the geographical location of the transmission, timestamps, frequency ranges, transmit power, and modulation rates [14]. Moreover, sensors can capture some upper layer details such as protocol, wavelength, waveform standard (i.e., 4G/5G).

C. Deployment of the Blockchain Nodes

In the proposed system, the “regulator” is the entity that transmits the session key in a randomly selected frequency band, which may be narrow or wide, inside the total licensed spectrum without interfering with the regular operation. All the mining nodes (MNO and non-MNO) must have Radio-Frequency (RF) spectrum sensors with wideband, high-sensitivity, multi-beam receivers, and additional capabilities such as waveform detection, running AI/ML algorithms and modulation recognition to perform the mining function of the proposed blockchain system. Since specific hardware resources are needed from the participating spectrum miners, it is not practical to deploy the proposed DSA system as a public blockchain network. Therefore, we propose to use a *private blockchain* for the proposed DSA system.

D. Operation of the Proposed DSA System

Fig. 1 presents the high-level deployment view of the proposed architecture. Here, the spectrum sensing and block generation process can be explained in four steps.

- Step 1:** Regulator transmits the RCK and an encrypted message in a randomly selected frequency band selected within the range of interest.
- Step 2:** Miners scan the spectrum and try to capture the transmitted key by analysing the sensed data.

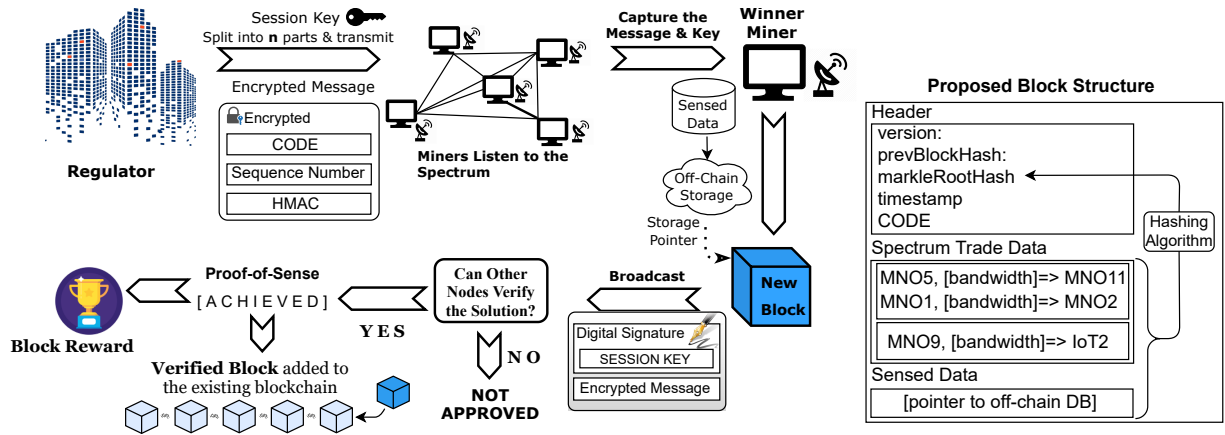


Fig. 2. The Workflow of the Proposed Proof-of-Sense

- Step 3:** The miner who captures the RCK creates a new block and multicast it to the network.
- Step 4:** Other miners verify the block and add it to the blockchain. The winner miner is entitled to any block rewards. The miner adds a pointer (e.g., IPFS hash) to its sensed data stored in off-chain storage in the block.

E. Proof-of-Sense: Novel Consensus Algorithm

Based on the literature, we noticed that the consensus algorithms, such as PoW, are based on cryptographic hashing functions (Ex: Bitcoin cryptocurrency uses an SHA-256 hashing-based puzzle), which are costly to operate in DSA systems. There are also growing concerns about the impact of energy usage of blockchains on the global carbon footprint. On the other hand, consensus mechanisms like PoS need pre-mined coins or start with PoW. Since we expect to trade only using spectrum, and the primary purpose is to develop a mechanism to detect fraud, none of the existing mechanisms is cost-effective and efficient. Therefore, we propose a new consensus mechanism based on spectrum sensing (i.e., *Proof-of-Sense*). In this mechanism, nodes have to perform a challenging process of precise spectrum sensing across many directions across a wide band to recover the RCK. RCK uses a symmetric key to encrypt the regulator's message and acts as a session key. A session is the time duration between the generation of two adjacent blocks. Once a particular session is expired, the corresponding session key gets invalid. The process of creating a new block dictates the expiration time of the session key. Once the network verifies the block, the regulator transmits a new message encrypted using a new RCK.

Simultaneously, the regulator transmits an encrypted message in a known channel. Therefore, every node can capture it. The regulator's encrypted message contains a "CODE", a sequence number, and a Hash-based Message Authentication Code (HMAC). Proof-of-Sense uses this encrypted message for the verification process. CODE is the hash of the RCK signed with the regulator's private key. Since all the nodes have the regulator's public key, nodes can verify the ownership. Along with a CODE, a sequence number and an HMAC are

sent to avoid reply attacks and protect the content's integrity. The miners scan the spectrum to capture the transmitted encrypted message and the RCK. Whoever captures the RCK first becomes the winner and can mine the next block. The nodes can maintain more than one spectrum sensor to increase the probability of finding the RCK. Fig. 2 further describes the workflow of the proposed *Proof-of-Sense* algorithm.

As an aside, note how, unlike hashing-based PoW, the proposed spectrum sensing Proof-of-Sense achieves the additional useful function of detecting whitespace while powering the blockchain, thereby better justifying its energy usage for applications beyond the distribution of trust.

1) Cryptographic Key Sharing: For the RCK sharing process, we propose using a key sharing scheme presented in [15], commonly known as Shamir's secret-sharing scheme. Shamir introduced the concept of secret sharing through threshold schemes, and his model is based on polynomial interpolation: given a set of t points $(x_1, y_1), \dots, (x_t, y_t)$, where the x_i s are all distinct, in a 2D plane, there is one and only one polynomial $f(x)$ of degree $t - 1$ such that $f(x_i) = y_i$ for all i [15]. To divide the data K (secret) into pieces K_i we can use a random polynomial $f(x)$ of degree $t - 1$ in which $a_0 = K$ and evaluate,

$$K_1 = f(1), \dots, K_i = f(i), \dots, K_n = f(n) \quad (1)$$

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1} \quad (2)$$

If some node has t shares $(i, f(i))$, the node can reconstruct the $f(x)$ using Lagrange polynomial interpolation in (3), and find a_0 , which is the secret. However, since we only interested in a_0 , there is a computationally efficient approach to calculate a_0 without reconstructing $f(x)$. We can substitute $x = 0$ in (3) and get (4). Although the original method uses integer arithmetic, the security can further be improved by using finite field arithmetic (a field of size $p \in \mathbb{P}$).

$$f(x) = \sum_{j=0}^{t-1} y_j \prod_{\substack{m=0 \\ m \neq j}}^{t-1} \frac{x - x_m}{x_j - x_m} \quad (3)$$

$$f(0) = \sum_{j=0}^{t-1} y_j \prod_{\substack{m=0 \\ m \neq j}}^{t-1} \frac{x_m}{x_m - x_j} \quad (4)$$

Therefore, a t -out-of- n threshold scheme is a method in which n pieces of information, known as *shares*, in a secret key K are distributed so that the secret can be reconstructed from any t or more shares and otherwise not. The parameter t is known as the *threshold* of the scheme.

We use Shamir’s concept to control the capturing difficulty of the key. The regulator transmits the n pieces of information of the session key (*RCK*) in multiple frequency bands, and miners need to collect t pieces to recover the session key. Algorithm 1 shows the pseudo code for generating transmission information. The recovery difficulty of the key depends on many variables such as the key length, shares, threshold, transmitter and receiver characteristics, and wireless channel characteristics. Once the regulator transmits the key, it waits for a specific interval and then re-transmits it until at least one node recovers the key. Since the regulator is also a miner node in the blockchain network, it will know when a node successfully recovers the key via blockchain. Algorithm 2 shows the pseudo code for reconstructing the RCK using t pieces of information.

Algorithm 1 Generating transmission information

```

Input: Secret key ( $a_0$ ), Total shares ( $n$ ), Threshold ( $t$ )
Output:  $n$  information pieces, Encrypted message
1:  $CODE \leftarrow$  hash of the secret key ( $a_0$ )
2: Generate the message with CODE, Sequence no. and HMAC
3: Encrypt the message using secret key
4: Generate  $t - 1$  random integer numbers
5: for  $i = 1$  to  $t - 1$  do
6:    $a_i \leftarrow$  random integer
7: end for
8: Generate the polynomial  $f(x)$ 
9:  $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}$ 
10: Generate  $n$  points  $\kappa_{x-1} = (x, f(x))$  from the polynomial
11: for  $j = 0$  to  $n - 1$  do
12:    $\kappa_j \leftarrow (x_j, f(x_j))$ 
13: end for
14: Transmit encrypted message in a known frequency
15: Transmit  $n$  key parts ( $\kappa_0, \kappa_1, \dots, \kappa_{n-1}$ ) in random  $n$  frequency bands within a agreed range
    
```

In a consensus mechanism, there should be a method to control the block time. In *Proof-of-Sense*, the recovery of RCK is directly impacting the block time. In the proposed system, the RCK can be embedded with or without a degree of obfuscation, using a multitude of modulation and coding schemes, across multiple bandwidths with parameters depend on the level of spectrum mining difficulty desired across the network. We quantitatively analyze the impact of some parameters on key recovery difficulty in section III-B. Table I provides an estimation of the impact of several parameters on recovery difficulty.

The effect of RCK on recovery difficulty depends on three main features, namely key length, total shares (n), and threshold (t). When we increase the size of the key, the receiver needs to recover additional data bits. Also, when we increase

Algorithm 2 Key Reconstruction

```

Input:  $t$  information pieces, Encrypted message
Output: Reconstructed key
1: Received:  $(x_0, y_0), (x_1, y_1), \dots, (x_t, y_t)$ 
2:  $p = 1, s = 0$ 
3: for  $j = 0$  to  $t - 1$  do
4:   for  $m = 0$  to  $t - 1$  do
5:     if  $j! = m$  then
6:        $p = p * (x_m) / (x_m - x_j)$ 
7:     end if
8:   end for
9:    $s = s + (p * y_j), p = 1$ 
10: end for
11: Secret key ( $a_0$ )  $\leftarrow s$ 
    
```

TABLE I
EFFECT OF DIFFERENT PARAMETERS ON KEY RECOVERY DIFFICULTY

| Component | Feature | Effect on Recovery Difficulty |
|-----------------------|----------------------|-------------------------------|
| Key | Key Length | Increase with size |
| | Total Shares (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 |

the t (keeping n and key length as constants), the receiver needs to recover additional key shares. Therefore, recovery difficulty increases with both key length and threshold. If we increase n (keeping t and key length as constants), the receiver needs fewer data bits to reconstruct the key. Therefore, recovery difficulty decreases with n . The effect of the wireless channel is mainly based on different types of losses and interference in the channel. All these qualities of wireless channels cause losses in data transmission [16], and therefore, recovery difficulty increases with free space losses, fading, diffraction, absorption, reflection, atmospheric losses, and interferences. We investigate the effect of some of these features in section III-B.3. Finally, transmitter and receiver characteristics such as modulation, coupling losses, and error correction mechanisms also affect the recovery difficulty. Coupling losses increase the recovery difficulty as they cause losses in the data being transmitted or received. Error correction mechanisms can improve the system’s ability to self-correct error bits without retransmissions, decreasing recovery difficulty. The effect of modulation is dependent on the modulation technique. In section III-B.2, we investigate the effect of two modulation schemes on the recovery probability. The system can adjust some of these parameters to complicate the recovery process sufficiently, and at the same time, it is not computationally challenging.

2) *Block Generation*: As per our consensus algorithm, the miner that recovers the RCK first becomes the winning node. The winning node can create the next block of the blockchain and earn a reward for that. While creating the block, the miner put the spectrum trade data and sensed data into the new block. Instead of storing sensed data into the blockchain, the node stores data in off-chain storage and stores a pointer to the data in the block. The block header contains the hash values, version, timestamp, and CODE (from the decrypted message). The proposed structure of a block is presented in Fig. 2. Then, the node broadcasts the newly mined block to the network for verification.

3) *Verification*: When a miner receives a new block from the winner node, it initiates the verification process. The miner first verifies the cryptographic key. Since every other node in the network has the regulator's encrypted message, they can decrypt the message with the winner node's key and verify the solution. The hash of RCK sent by the winner node should be equivalent to the hash of RCK in the encrypted message (CODE) sent by the regulator. Since the hash of RCK in the encrypted message is signed by the regulator, the winner node cannot claim victory with a fake RCK. This proposed process is cost-effective as there are no computationally challenging puzzles to solve. In addition, sensing measurements in the block must match up with the other miner nodes' measurements. This process is equivalent to transaction validation, and it ensures the integrity of the sensed data. Only the verified blocks will be added to the blockchain. Algorithm 3 shows the pseudo code of verification.

Algorithm 3 Verification

Input: Reconstructed Key

Output: True or False

```

1: Decrypt the message with the prover's key
2:  $K \leftarrow$  CODE inside the message
3:  $H \leftarrow$  hash of the prover's key
4: if  $K == H$  then
5:   True                                     ▷ Key is verified
6: else
7:   False                                    ▷ Key is not verified
8: end if

```

F. Database for Spectrum Sensing Data

Apart from the keys, spectrum sensors collect an enormous amount of other spectrum data in the key capturing process. Nodes store these spectrum data locally until they can create the next block. Once a node becomes the winner, the node adds a pointer for these data in the generated block. The sensed data is stored off-chain (e.g., IPFS - InterPlanetary File System) to avoid the excessive growth of the chain

G. Spectrum Fraud Detection

The fraud detection mechanism focuses on detecting the unauthorized (i.e., fraudulent) use of the licensed spectrum. Miners in the network store sensed data in the blockchain

during block generation. The system analyzes this data to identify spectrum violations using yet-to-be-determined Machine Learning (ML) algorithms. The system can use SCs to automatically trigger fraud detection and ensure the integrity of used ML algorithms. The fraud detection system checks both MNO level sharing agreement and spectrum regulation on restricted spectrum bands. Thus, the proposed DSA system with Proof-of-Sense can potentially detect unauthorized use of the restricted spectrum as well. Guaranteeing the accuracy and trustworthiness of the sensed data is one of the major challenges in the system. We propose to achieve this by cross-validating results with nearby sensors. The system will only take action against the discovered frauds if discoveries can be verified with cross-validating. In the literature, there are several approaches to ensure the efficiency, trustworthiness, and security of IoT/WSN data collection [17]. This paper does not intend to investigate such aspects of data collection.

Identifying the transmitter ID is very important as authorities can use it to trace fraud into the origin. However, it is challenging to capture the transmitter's ID by monitoring the spectrum data when the transmitter does not broadcast its ID. However, it is possible to use radio fingerprint-based identification mechanisms [18] [19] to identify the transmitter's ID. Due to the electronic level imperfections of transmitters semiconductor electronics, even though they are made of nominally identical components, there are differences in their radio fingerprints that have been detected using ML methods. The system can possibly use such radio fingerprints based identification mechanisms on identifying the devices [18] [19]. However, it is out of the scope of this paper, and it is left for future work.

H. Patently Payment and Rewards for Miner

Once the system identifies a spectrum violation, the particular transmitter will be fined based on pre-defined criteria according to the degree of a breach. Then, the system pays compensation to the spectrum owner, whose spectrum was accessed in an unauthorized manner. In addition, the system will use a part of the penalty to pay the block generation rewards and pay for the miners who contributed (i.e., by providing sensing information) to detect that particular infringement. The system can automate the compensation process by using SCs. When the number of frauds decreases, the available revenue to maintain the system will also decrease. Thus, it is necessary to implement a subscription fee for MNOs, or the regulators should pay a fee to maintain the system. The penalties may also scale, perhaps exponentially, with the severity of the fraud.

I. Role of Smart Contracts

Overall, SCs handle all payment instances of the proposed system, such as subscription fees, penalties, compensation and block rewards. Apart from financial aspects, SCs can conduct spectrum auctions, sublet spectrum, analyze stored spectrum data, detect infringements, rate users and other functionalities. Because they inherit blockchain properties, SCs add autonomy, trust, safety and efficiency to the network.

III. PERFORMANCE ANALYSIS

This section presents the performance evaluation of the Proof-of-Sense consensus mechanism. First, we measure the energy usage of the proposed consensus mechanism using a testbed and compare it with some of the existing consensus mechanisms. Then, we use MATLAB to evaluate the difficulty of reconstructing the key under different characteristics of the key sharing scheme and the wireless channel. Finally, we calculate the average block time under different noise conditions using MATLAB.

A. Energy Usage Comparison

We evaluate the performance of the proposed system using the experimental testbed comprised of two Raspberry Pi 3 modules connected with nRF24L01 transceivers, two ESP32 Microcontroller Units (MCUs), and two bi-directional current/power monitor modules (INA226). The Raspberry Pi 3 module performed the computational tasks at both transmitter's and receiver's end. The nRF24L01 is a transceiver with a maximum transmission distance of 1km and operates in the 2.4 - 2.5 GHz band. During the experiment, the air data rate was set to 250 kbps. The INA226 bi-directional current/power monitor IC is a current shunt and power monitor with an I2C interface.

Table II presents the power consumption of the processing unit (i.e., Raspberry Pi 3 module) for different steps of the Proof-of-Sense mechanism. In the experiment, we set the total shares as six ($n = 6$) and the threshold as three ($t = 4$) and four ($t = 4$). The values in Table II are averaged by taking 100 samples. The spectrum scanning and key capturing consume the most energy in Proof-of-Sense as it takes more time to sweep the interested frequency range. During this time transceiver is listening to the spectrum, consuming a considerable amount of energy. When $t = 4$, it consumes more energy than $t = 3$ as it needs to scan for one additional key share to reconstruct the key. On the other hand, the verification process consumes the lowest energy as it simply compares the hash values. The energy consumption for this step is equal in both $t = 3$ & $t = 4$ as the hash values of both cases are equal in size. In key generation and reconstruction steps, the $t = 4$ case consumes slightly higher energy due to the involvement of one additional key share.

TABLE II
ENERGY CONSUMPTION IN DIFFERENT PHASES OF PROOF-OF-SENSE FOR DIFFERENT THRESHOLDS

| Operation | $t = 3$ | $t = 4$ |
|--|-----------|-----------|
| Key Shares Generation and Transmission | 60.29 mJ | 69.10 mJ |
| Scan and Capture Key Shares | 18494 mJ | 24658 mJ |
| Key Reconstruction | 120.55 mJ | 146.17 mJ |
| Verification | 7.71 mJ | 7.71 mJ |

Table III shows the power consumption of different consensus mechanisms. It is important to note that it is not the energy for a fully operational blockchain network. We measure only the energy of a single node to run the underlying consensus algorithm. The results presented in the Table III are averaged by taking 100 samples. For PoW, we use SHA-256 as the

hashing algorithm with a 32-bit nonce. The difficulty of the network is set to six zeros. The testbed measures the time and energy needed for the processing unit to calculate the target hash value. For PoS, we take the amount of sensed data as the stake instead of a cryptocurrency asset. The more data a node captured, the higher the chance of creating the next block. However, in such an approach, we need to develop sophisticated mechanisms to verify the credibility of the sensed data, which is out of the scope of this paper. We also consider the coin age in selecting the winner node, apart from the stake weight. The testbed measures the time and energy needed to select the node with the highest coin age * stake weight value. For the proposed Proof-of-Sense mechanism, we set $n = 6$ and $t = 4$ for these measurements. The testbed measures the time and energy needed to capture the key parts, reconstruct the key and verify it.

According to Table III, PoW needs the highest energy to achieve the consensus because it involves solving hash puzzles that consume many computational resources. On the other hand, PoS has the lowest execution time because of the algorithm's simplicity. In the testbed, we consider the time needed to select the node with the highest coin age * stake weight value as the execution time. Note that in a real PoS based blockchain network, several other parameters affect the final block time of the network. The energy of PoS is the summation of algorithm execution energy and energy to create the sensed data-based stake. Moreover, even we implement a DSA system with PoW or PoS, the system still consumes additional energy for spectrum sensors. With Proof-of-Sense, we can get an additional advantage of using the same infrastructure (i.e., spectrum sensors) to support the blockchain.

TABLE III
ENERGY CONSUMPTION COMPARISON OF DIFFERENT CONSENSUS MECHANISMS

| Consensus Mechanism | Execution Time (seconds) | Energy (J) |
|-------------------------|--------------------------|------------|
| Proof-of-Work [6] [10] | 860.57 | 1994.53 |
| Proof-of-Stake [6] [10] | 0.39 | 29.81 |
| Proof-of-Sense | 9.06 | 24.88 |

B. Difficulty Analysis of Consensus Algorithm

The performance of the proposed *Proof-of-Sense* consensus algorithm depends on the RCK recovery probability, which is calculated by counting the number of successful RCK recoveries against the total number of RCK transmissions. The RCK recovery probability heavily relies on the factors given in Table I. Here, we use MATLAB to investigate the impacts of these factors on the RCK recovery probability.

In our simulations, we use Shamir's secret sharing scheme [15] to generate a total number of six shares (i.e., $n = 6$) for RCK in key distribution and to recover RCK from t number of shares (threshold). A 16 bits binary code represents each of these shares. Therefore, we need to transmit 96 information bits corresponding to an RCK. For this purpose, we adopt an OFDM transmission scheme having 64 subcarriers. Here,

we use 48 data subcarriers (out of 64 subcarriers) to transmit BPSK/QPSK symbols over different channel conditions. Fig. 3 illustrates the effects of threshold (t), modulation, and channel conditions on the key recovery probability. The results are averaged over 1000 random realization of AWGN, Rayleigh, and Rician channels.

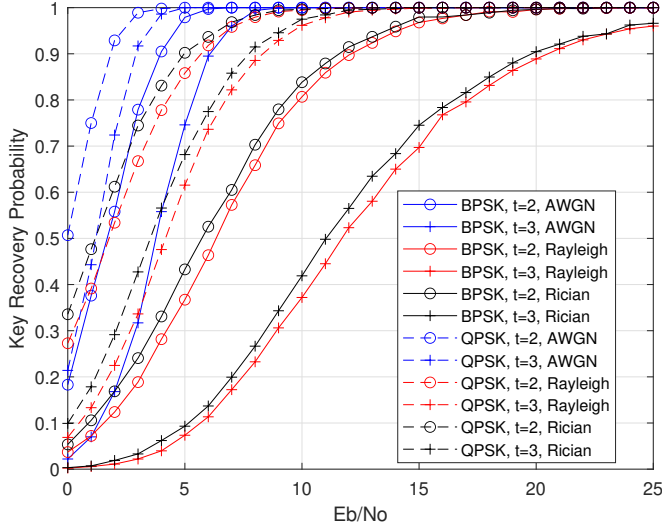


Fig. 3. Key Recovery Probability under Different Conditions

1) *Effects of Threshold*: We observe that the RCK recovery probability increases at lower t values for a given signal to noise ratio (E_b/N_0) as it is required a lesser number of shares for the recovery. When we increase the threshold, the receivers need to accurately collect more shares of the key at the given E_b/N_0 . Although this can delay the successful key recovery, the security of the RCK can greatly increase. Further research should be conducted to determine the best n (shares) and t (threshold) values to optimize recovery time and security.

2) *Effects of Modulation*: The results in Fig. 3 show that the OFDM system with QPSK modulation has a higher RCK recovery probability in both $t = 2$ and $t = 3$ cases. It is known that QPSK modulation encodes two bits per symbol and uses gray coding to reduce the bit error rate, while BPSK only encodes a single bit per symbol. Therefore, it is possible to assign all 96 information bits corresponding to all six RCK shares to one OFDM symbol when QPSK modulation is used. Hence, there is a better chance to correctly recover the required number of shares from all six shares in one OFDM symbol duration. However, we can assign only three shares (48 information bits) to one OFDM symbol when we use BPSK modulation. This reduces the recovery probability as it requires to correctly recover the required number of shares from three shares during one OFDM symbol duration. Therefore, there is a clear effect from the modulation for the RCK recovery probability.

3) *Effects of Wireless Channel*: When considering the effect of the wireless channel, the recovery probability is much higher when we only use AWGN channel conditions. This occurs due to the absence of the fading effects. Then, we consider the RCK recovery probability under the fading conditions by considering Rician and Rayleigh fading channel

models. Here, we consider the Rician model with a Rician K-factor of 0.6. Since there is a strong dominant component (ex: line-of-sight, ground reflection) in Rician fading, it shows a higher recovery probability than Rayleigh fading. Rayleigh fading is a special case of Rician fading where there is no line-of-sight (LOS) signal. Due to the absence of a LOS signal, the RCK recovery probability is lower under Rayleigh fading channel conditions. We also consider the effects of threshold t ($t = 2$ and $t = 3$) for these channel conditions, and it is clear that in every scenario, the more shares required, the lower the recovery probability. It is important to mention that we have not used any error correction mechanism in simulations, which will further increase the recovery probability.

C. End-to-End Delay

We implement the proposed system in software by using Ganache (an Ethereum blockchain), Python and Matlab. We use Ganache to upload the dummy sensed data to the IPFS network and measure the time for that process, Python to construct a small blockchain network with 10 mining nodes to measure the time for verification process, and MATLAB to simulate the key transmission and receiving process. In particular, we consider OFDM based QPSK symbol transmission scheme under Rayleigh fading channel conditions for RCK distribution. Here, the RCK is retransmitted until a successful RCK recovery occurs at a miner node. We take the OFDM symbol duration as $3.2\mu\text{s}$ (IEEE 802.11) [20], and we set the interval between two successive RCK transmissions to 200ms. After miners verify the key, winner node uploads the sensory data to the off-chain IPFS network and hash it. In our simulations, we assume the sensory data collection rate as 0.5 MB/s to create dummy data.

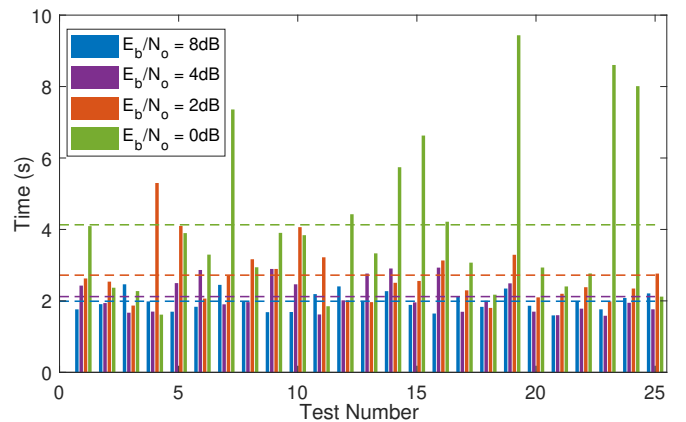


Fig. 4. End-to-End Delay for Different E_b/N_0 Values

The End-to-End (E2E) delay of the system is the summation of key recovery time, time to get the IPFS hash, and verification time. Fig. 4 depicts the E2E delay variations for different E_b/N_0 values. Here, we carry out 25 tests for each E_b/N_0 . The dotted lines in Fig. 4 show the average E2E delay values. Since the key recovery time varies according to the wireless channel conditions, the E2E delay varies at different E_b/N_0 values. In particular, the average E2E delay is 1.99s when E_b/N_0 is 8dB, and it is the smallest among all others

due to the low noise level. When E_b/N_0 is 4dB, 2dB, and 0dB, the average E2E delays are increased to 2.12s, 2.72s, and 4.13s, respectively. This shows exponential growth in the E2E delay with the decrement of E_b/N_0 values. The variances of the E2E delays for four cases are $0.07s^2$, $0.22s^2$, $0.67s^2$ and $4.95s^2$ respectively, and therefore, we can conclude that the inconsistency of the E2E delay increases with the decrement of E_b/N_0 value. It is further important to note that the time it takes to get the IPFS hash (i.e., a pointer to off-chain sensed data) also increases with the RCK recovery time because it collects more data with time.

IV. DISCUSSION

A. Feature Comparison

Table IV summarizes a feature comparison between existing blockchain-based and non-blockchain-based spectrum sharing systems with the proposed system. (Here, **L** → Low, **M** → Medium, **H** → High, - → Not Relevant/Not Available)

TABLE IV
FEATURES COMPARISON WITH KEY RELATED WORKS

| Features | [1] | [3] | [4] | [6] | [8] | [9] | [10] | [11] | [13] | Ours |
|------------------------------|-----|-----|-----|-----|-----|-----|------|------|------|------|
| Blockchain based | X | X | X | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Spectrum Trading Marketplace | ✓ | X | X | ✓ | X | X | ✓ | ✓ | ✓ | ✓ |
| Automated Services | X | X | X | ✓ | ✓ | X | ✓ | ✓ | ✓ | ✓ |
| Spectrum Sensing | X | X | X | X | ✓ | X | X | X | X | ✓ |
| Spectrum Fraud Detection | X | X | X | ✓ | ✓ | X | X | X | X | ✓ |
| Off-Chain Storage | - | - | - | X | X | X | ✓ | X | X | ✓ |
| Tailored Consensus | - | - | - | X | X | X | X | X | ✓ | ✓ |
| Extra Cost of Mining | - | - | - | H | H | H | H | H | L | L |
| Computational Complexity | L | M | L | H | H | H | H | H | L | L |

Most blockchain-based systems outrun the non-blockchain system by providing the features like spectrum sharing marketplace and automated services. Blockchain-based systems can enable these features using SCs. Still, most blockchain-based systems suffer from limitations such as high computational complexity and the extra cost of mining. The proposed DSA system eliminates some of these limitations in existing blockchain-based systems by introducing the specially tailored Proof-of-Sense consensus mechanism.

B. Complexity and Performance Comparison

The consensus mechanism plays a vital role in determining the performance of a blockchain, and security bound, scalability, transaction throughput, and latency are four of the most essential performance metrics [21]. Table V presents a performance comparison of blockchain consensus mechanisms considering a wireless blockchain network [21]. Here, N is the total nodes, f is malicious nodes, and n is the total key shares in Shamir’s secret sharing scheme. The value n is far less the N . Therefore, we can assume that the scalability of the network is high because the effect of n is minimal in both communication complexity and spectrum requirement. The security bound of the proposed consensus mechanism is as same as in the PoW.

1) *Security Bound*: Security bound can be defined as the maximum number of faulty nodes tolerated by the consensus mechanism. In general, the security bound for PoW is considered as $2f + 1$. Therefore, a blockchain network implemented with PoW will compromise if a single entity possesses more than 50% of the resources in the network. The proposed blockchain with Proof-of-Sense achieves consensus if more than 50% of the nodes verify the RCK. Therefore, Proof-of-Sense has the same security bound as PoW. However, voting-based consensus mechanisms such as Practical Byzantine Fault Tolerance (PBFT) and Raft define the number of faulty nodes as inactive or malicious nodes in the network [21]. These nodes send misinformation to jeopardize the healthy operation of the network. Typically, PBFT has a security bound of $3f + 1$ (allowing 1/3 of faulty nodes), and Raft has $2f + 1$.

2) *Scalability*: Scalability indicates the ability of the consensus mechanism to handle the increasing number of nodes. In theory, PoW has excellent scalability and can hold as many users within the network. However, it is impossible to keep as many users considering the spectrum requirements in a wireless blockchain network. On the other hand, voting-based mechanisms heavily rely on inter-node communications. Therefore both PBFT and Raft have poor scalability. The Proof-of-Sense mechanism has higher scalability because the number of total shares (n) is independent of the number of nodes in the network.

3) *Transaction Throughput*: Transaction throughput indicates the transaction per second (TPS) in the system. PoW has a low throughput due to its computationally hard hash puzzles. Proof-of-Sense is not computationally hard as in PoW and is based on spectrum sensing. However, the verification process takes some extra time. Therefore, we can conclude it has a medium throughput. On the other hand, voting-based mechanisms like PBFT and Raft have a greater throughput (in the range of 100 to 1000 TPS) [21].

4) *Communication complexity*: The communication complexity refers to the number of communications between transmitter and receiver nodes. Table V presents the communication complexity of different consensus mechanisms for a wireless blockchain network. PBFT requires $2N^2 + N$ communications and it is the highest communication complexity shown in the Table V as all nodes have to communicate to all other nodes in all three stages (pre-prepare, prepare and commit). In Raft, the communication complexity $2N$ represents the communication between the head and follower nodes (uplink) and again from follower nodes and head (uplink). In PoW, $2N$ comes from broadcasting client request to all other nodes and broadcasting the winner miner’s hash in the verification process. In Proof-of-Sense, $N \times n$ term represents the key shares received by the nodes, and $2N$ represents the encrypted message and the winner’s key broadcast message. Therefore proposed consensus mechanism has a communication complexity of $N(n + 2)$.

5) *Spectrum Requirement*: The spectrum requirement of a wireless blockchain network refers to the spectrum requirement for communication in the network. While communication complexity is made of the number of receiver processes, spectrum requirement is the number of transmitter processes in

TABLE V
PERFORMANCE COMPARISON WITH COMMONLY USED CONSENSUS MECHANISMS [21]

| Consensus Mechanism | Suitable Type of Blockchain | Transaction Throughput | Scalability | Security Bound | Communication Complexity | Spectrum Requirement |
|-----------------------|-----------------------------|------------------------|-------------|----------------|--------------------------|----------------------|
| PBFT [22] | Private/Consortium | High | Low | $3f + 1$ | $2N^2 + N$ | $2N + 1$ |
| Raft [23] | Private | Very High | Medium | $2f + 1$ | $2N$ | $N + 1$ |
| PoW [24] | Public | Low | High | $2f + 1$ | $2N$ | 2 |
| <i>Proof-of-Sense</i> | Private | Medium | High | $2f + 1$ | $N(n + 2)$ | $n + 2$ |

Note: f = number of faulty nodes, N = total nodes, n = total key shares

the wireless blockchain network [21]. Since PoW consists of two broadcast messages (broadcast transactions and broadcast hash result of the winner node), and it is independent of the nodes in the network, PoW has a constant spectrum requirement. Proof-of-sense also has a spectrum requirement independent of the total nodes in the network. The total number of shares (n) is a characteristic of the RCK and does not relate to the total nodes in the network. In PBFT, $2N$ spectrum resources are needed to communicate among nodes in prepare and commit stages. In the pre-prepare stage, the leader node broadcasts a message to the rest of the nodes. Therefore PBFT has a total of $2N + 1$ spectrum requirement. For Raft, spectrum resources are required for the broadcast message in downlink communication from head to followers and the uplink communication from each follower node to the head. Therefore, Raft has an $N + 1$ spectrum requirement.

V. CONCLUSION

This paper presents Proof-of-Sense, a new consensus mechanism for a blockchain-based DSA system. Proof-of-Sense consensus mechanisms can address the efficiency issues in existing consensus mechanisms and detect unauthorized spectrum access frauds. The proposed mechanism is built based on a wireless spectrum sensing process rather than resource-consuming mathematical puzzles. Furthermore, we have adopted Shamir's secret sharing scheme to be used in the key sharing process of the proposed system. The performance of the proposed system is examined using thorough simulations and implementations. The results verify that the key recovery probability, which corresponds to the block time of the Proof-of-Sense mechanism, can be changed by modifying the wireless channel and transmitter and receiver characteristics. The results verify that the proposed mechanism is more efficient in terms of energy consumption. Additionally, the proposed mechanism provides a more DSA friendly consensus mechanism while collecting spectrum data to detect spectrum violations. The scope of this paper is limited only to the evaluation of the proposed consensus mechanism. Developing a DSA system with the proposed mechanism with features such as analyzing the collected sensed data and developing required microservices (e.g., spectrum auctions, payments) based on smart contracts is left for future work.

REFERENCES

- [1] 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, p. 3300–3310, Jun 2009.
- [2] M. D. Mueck, S. Srikanteswara, and B. Badic, "Spectrum Sharing: Licensed Shared Access (LSA) and Spectrum Access System (SAS)," *Intel White Paper*, pp. 1–26, 2015.
- [3] B. Cho, K. Koufos, R. Jantti, 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.
- [4] Y. Teng, Y. Wang, and K. Horneman, "Co-Primary Spectrum Sharing for Denser Networks in Local Area," *9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, pp. 20–24, 2014.
- [5] T. Wang, L. Qiu, A. K. Sangaiah, A. Liu, M. Z. A. Bhuiyan, and Y. Ma, "Edge-computing-based trustworthy data collection model in the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4218–4227, 2020.
- [6] 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.
- [7] B. Cao, M. Li, L. Zhang, Y. Li, and M. Peng, "How Does CSMA/CA Affect the Performance and Security in Wireless Blockchain Networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4270–4280, 2020.
- [8] T. Ariyaratna, P. Harankahadeniya, S. Isthikar, N. Pathirana, H. D. Bandara, and A. Madanayake, "Dynamic Spectrum Access via Smart Contracts on Blockchain," *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, 2019.
- [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] 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.
- [11] 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, Aug 2020.
- [12] H. Huang, W. Miao, G. Min, J. Tian, and A. Alamri, "NFV and Blockchain Enabled 5G for Ultra-Reliable and Low-Latency Communications in Industry: Architecture and Performance Evaluation," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5595–5604, 2021.
- [13] 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.
- [14] Y. Arjoun 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>
- [15] A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, p. 612–613, Nov. 1979.
- [16] S. Salous, D. Gaillot, J.-M. Molina-Garcia-Pardo, R. He, K. Saito, K. Guan, M. Barbiroli, J. Pascual-Garcia, and K. Haneda, "Chapter 3 - iracon channel measurements and models," *Inclusive Radio Communications for 5G and Beyond*, C. Oestges and F. Quitin, Eds. Academic Press, 2021, pp. 49–105. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/B9780128205815000092>
- [17] T. Wang, L. Qiu, A. K. Sangaiah, G. Xu, and A. Liu, "Energy-Efficient and Trustworthy Data Collection Protocol Based on Mobile Fog Computing in Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3531–3539, 2020.
- [18] 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,” *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, 2020, pp. 646–655.

- [19] 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.
- [20] E. Khorov, A. Kiryanov, A. Lyakhov, and G. Bianchi, “A Tutorial on IEEE 802.11ax High Efficiency WLANs,” *IEEE Communications Surveys Tutorials*, vol. 21, no. 1, pp. 197–216, 2019.
- [21] L. Zhang, H. Xu, O. Onireti, M. A. Imran, and B. Cao, “How Much Communication Resource is Needed to Run a Wireless Blockchain Network?” *IEEE Network*, vol. 36, no. 1, pp. 128–135, 2022.
- [22] 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.
- [23] 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
- [24] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Cryptography Mailing List* at <https://metzdowd.com>, 03 2009.



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. He is currently working as a Teaching Assistant at the Department of Electrical and Information Engineering of the University of Ruhuna, Sri Lanka, and as an external project consultant. His research interests are wireless communication, sensors and transducers, IoT, blockchain, and network security.



Tharindu Gamage received his first degree from the Department of Computer Science and Engineering, University of Moratuwa, Sri Lanka in 2009. He worked as a research assistant for several years in the Department of Electronic and Telecommunication Engineering and obtained his M.Sc. from the same department of University of Moratuwa in 2014. He 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.



Chatura Seneviatne (M’11) received B.Sc. degree in electrical and information engineering from the University of Ruhuna, Sri Lanka in 2006 and the M.Eng. degree in information and communications technologies from the Asian Institute of Technology, Thailand in 2009. He completed his Ph.D. degree in Electrical and Computer Engineering in the University of Calgary, Canada. He subsequently completed a Post-doctoral Fellowship in the University of Calgary and worked on a chaos-based covert signaling project funded by the Office of Naval Research (ONR), USA. He is currently working as a Senior Lecturer in the Department of Electrical and Information Engineering, University of Ruhuna. His research interests include signal processing, data aggregation and wireless communications.



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, since 2018. He was with the University of Akron, Ohio, USA, between 2010-2015. Professor Madanayake leads the RF, Analog, and Digital (RAND) laboratory for Advanced Signal Processing Circuits (ASPC) at FIU. He has been recently supported by US National Science Foundation, Office of Naval Research, Defense Advanced Research Projects Agency, National Institute of Health, and NASA for scientific work in multiple areas, including wireless communications, spectrum, radar and phased-arrays, electronic systems including FPGAs and VLSI, digital signal processing, algorithms, 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. He is also acting as a Docent/Adjunct Professor at the Center for Wireless Communications, University of Oulu, Finland, and an Honorary Adjunct Professor at the Department of Electrical and Information Engineering, University of Ruhuna, Sri Lanka. He received his Doctor of Technology degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016. He was also a recipient of the prestigious Marie Skłodowska-Curie Actions Individual Fellowship and Government of Ireland Postdoctoral Fellowship during 2018-2020. In 2020, he received the “2020 IEEE ComSoc Outstanding Young Researcher” award by IEEE ComSoc EMEA. Dr. Liyanage’s research interests are 5G/6G, SDN, IoT, Blockchain, MEC, mobile, and virtual network security. More info: www.madhusanka.com