Demo: Radio Spectrum Data Collection with Distributed-Proof-of-Sense Blockchain Network

***Abstract*—Dynamic Spectrum Access (DSA) addresses the underutilized spectrum allocation issues associated with static spectrum allocation. Blockchain is a critical enabler for implementing a DSA system because it allows untrusted parties to conduct business, such as spectrum buying and selling, without the involvement of a trusted third party. A blockchain system is implemented using the Proof-of-Sense consensus algorithm, which is designed to facilitate DSA while also providing several additional benefits, such as spectrum data collection.**

***Index Terms*—Dynamic Spectrum Access (DSA), Blockchain, Consensus**

I. Introduction

The exponential growth in wireless devices needs a more flexible and robust spectrum access mechanism [1], which is not available in the current fixed spectrum allocation. In fixed spectrum allocation, a government spectrum regulatory body sells this scarce resource to Mobile Network Operators (MNOs), providing the MNO exclusive rights to a particular band. Given that the electromagnetic radio spectrum is a scarce natural resource, some MNOs barely use some frequency bands or use them sporadically, resulting in spectrum holes [2], which highlights the underutilisation issue that comes with the fixed allocation model. To address these problems, the research communities introduce Dynamic Spectrum Allocation/Access (DSA) concepts. In the literature, there are several blockchain-based and non-blockchain-based solutions to implement a spectrum management system.

Nevertheless, blockchain-based solutions have several key advantages, such as the elimination of a trusted third party to conduct deals (reduced operational cost), guaranteed integrity (accurate auditing), and transparency (better visibility into spectrum usage). However, one major shortcoming of such designs is the blockchain network's high resource consumption (e.g., energy and computational power). Additionally, existing DSA systems still need to address how to detect unauthorised spectrum usage in the shared model and how to collect spectrum data.

The Distributed-Proof-of-Sense (DPoS) consensus algorithm was introduced in [3] to address these identified shortcomings. DPoS is a tailored consensus algorithm created specifically to provide a more appropriate consensus algorithm for blockchain-based DSA systems. DPoS incentivises nodes to collect spectrum data as part of its consensus mechanism. Spectrum data collection is an important component of any DAS system because it detects which bands are not being used and when someone is accessing the spectrum in an unauthorised manner (also known as spectrum misuse, spectrum fraud, or spectrum violation).

Unauthorised access poses the risk of causing interference to subscribers of a wireless network. Spectrum misuse in DSA includes activities such as accessing the spectrum beyond the allocated time, transmitting within unauthorised bands, accessing restricted frequencies, breaching allowed energy levels, and contravening permitted modulation techniques and standards. Fraudulent activities in a DSA system can potentially diminish service quality and may lead to substantial financial losses. Therefore, the collection and analysis of spectrum data are indispensable for identifying and mitigating such issues.

II. System Architecture

In this demonstration, we implement the DPoS algorithm in a prototype network and present how spectrum-sensing-enabled nodes collect data and share it with the network using a DPoS-based blockchain network. As shown in Fig. 1, HackRF One Software Defined Radio (SDR) is used as the spectrum sensor, and a Raspberry Pi 4 device is used as the node, which runs the blockchain client and handles spectrum data processing. The blockchain network is built using the Substrate blockchain framework, with DPoS running as the consensus mechanism.

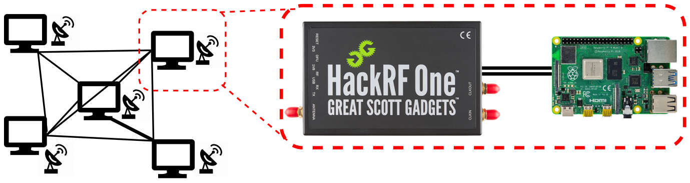

Fig. 1. A Node in the Blockchain Network

A. Consensus Mechanism

The DPoS consensus mechanism this platform utilises is a decentralised key generation and verification process based on non-interactive Elliptic Curve Cryptography (ECC) based Zero-Knowledge Proof (ZKP) following the Schnorr scheme [4]. Here, some basic terminologies and operations are described to explain the demonstration.

B. Key Generation

Each node generates a point $B_{i,j}$ (i.e., $B_{i,j} = a_{i,j}G$) on the elliptic curve (E). Here, $B_{i,j}$ is considered the public key, and $a_{i,j}$ as the private key of the i^{th} node for the j^{th} session.

C. Key Sharing

A node signs and transmits its private key (a_i) in a random frequency band. Additionally, the node shares B_i with the network to become shared knowledge. Also, E, G and P (another point on the curve) are considered shared knowledge.

D. Final Key Construction

A node must collect at least t-out-of-n keys (where t = threshold, n = total nodes) to become the winner and create the next block. The final key is a combination of keys transmitted by other nodes ($a = a_1 + a_2 + ... + a_n$).

E. Verification

Other nodes can indirectly check the final key to confirm the prover's claim to be correct by utilising the ECC-based ZKP. The prover must also generate additional parameters, as illustrated in Fig. 2.

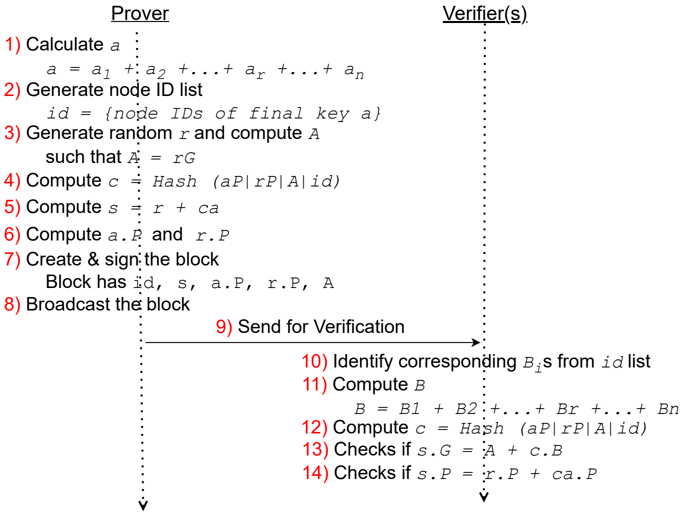
Prover
Verifier(s)
1) Calculate a
$a = a_1 + a_2 +...+ a_r +...+ a_n$
2) Generate node ID list
id = {node IDs of final key a}
3) Generate random r and compute A
such that $A = rG$
4) Compute $c = Hash\ (aP|rP|A|id)$
5) Compute $s = r + ca$
6) Compute $a.P$ and $r.P$
7) Create & sign the block
Block has id, s, a.P, r.P, A
8) Broadcast the block
9) Send for Verification
10) Identify corresponding B_is from id list
11) Compute B
$B = B1 + B2 +...+ Br +...+ Bn$
12) Compute $c = Hash\ (aP|rP|A|id)$
13) Checks if $s.G = A + c.B$
14) Checks if $s.P = r.P + ca.P$

Fig. 2. Messages Exchanged in the Verification Process

The operations device performed in this blockchain-based DSA system can be explained as follows.

Step 1 A node register with the DSA system.

Step 2 Node generates and transmits a session key in a random frequency band.

Step 3 Node scans the radio spectrum to collect session keys from other nodes. Nodes collect valuable spectrum data while scanning for the keys.

Step 4 Nodes that collect enough keys -to create the final key- will create a new block. The node stores the sensed data in an off-chain storage and puts the hash address of that data in the new block. The node then broadcasts the new block to the network.

Step 5 Other nodes verify the block using ECC ZKPs and add it to the local blockchain. This marks the end of a session and nodes go to Step 2 again.

III. Demonstration

The described system is set up in a prototype network of five nodes. Each node corresponds to a Mobile Network Operator (MNO) responsible of gathering radio spectrum data. These nodes run on a custom Substrate core, which includes a modified consensus library optimized for the DPoS consensus algorithm. The demonstration includes several key steps. Initially, a node is registered in the system and integrated into the network. The node then starts collecting radio spectrum data while playing the consensus game to add the next block to the network. After accumulating enough keys to generate the final key, the node can append the next block, along with the collected spectrum data. Following that, the block is verified by other nodes via ECC-based ZKPs. After successful verification, the block is added to each node's local chain. Furthermore, the demo showcases the real-time collection and sharing of spectrum data using HackRF One devices. It illustrates how this data seamlessly integrates into the blockchain.

Thus, the demonstration highlights key components of the proposed system and its novel blockchain network. The collected data serves as the foundation for future work, which will include analysis to detect available spectrum and unauthorized access.

IV. Conclusion

This demo paper describes a DSA system that allows network users to share radio spectrum efficiently and autonomously. The novel consensus mechanism encourages users to collect spectrum data, which will then be analysed to detect unauthorised spectrum access. The demo provides insight into how the DSA system operates. It demonstrates how the nodes compete to add the next block to the chain while also gathering valuable spectrum data.

Future work will include analysing the collected spectrum data to detect violations and designing rentable tokens that can be used to purchase and sell radio spectrum chunks.

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] 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.

[3] P. Fernando, K. Dadallage, T. Gamage, C. Seneviratne, A. Braeken, A. Madanayake, and M. Liyanage, "Distributed-Proof-of-Sense: Blockchain Consensus Mechanisms for Detecting Spectrum Access Violations of the Radio Spectrum," *IEEE Transactions on Cognitive Communications and Networking*, 2023.

[4] 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