On the application of blockchains to spectrum management

Martin Weiss, Kevin Werbach, Douglas Sicker, Carlos Caicedo, Amer Malki

Abstract

Spectrum sharing mechanisms have evolved to meet different needs related to increasing spectrum use efficiency. At first, decentralized and opportunistic cognitive radios (and cognitive radio networks) were the primary focus of research for these mechanisms. This gradually transitioned towards the development of cooperative sharing methods based on databases, typified by TV White Spaces databases. Spectrum sharing is now the basis for the dynamic and fine-grained spectrum rights regime for the Citizen's Band Radio Service (CBRS) as well as for License Shared Access (LSA).

The emergence of the cryptocurrency Bitcoin has stimulated interest in applying its underlying technology, blockchain, to other applications as well, such as securities trading and supply chain management. This paper explores the application of blockchain to radio spectrum management. While blockchains could underlie radio spectrum management more broadly, we will focus on dynamic spectrum sharing applications. Like the cooperative approaches currently in use, blockchain is a database technology. However, a blockchain is a decentralized database in which the owner of the data maintains control. We consider the benefits and limitations of blockchain solutions in general, and then examine their potential application to four major categories of spectrum sharing. The use of blockchain technology in spectrum management could have significant implications for stakeholders.

I. INTRODUCTION

Blockchain has been heralded as a technology that could be as important as the Internet [2]. Secure distributed ledgers and cryptocurrencies based on blockchain technologies could have many applications and be broadly disruptive. This paper examines one potential use case, exploring the ways this technology might be applied to spectrum sharing.[1]

[1] While in this paper we focus on blockchain as it applies to spectrum sharing, there may be situations where blockchain could be applied to non-sharing-based approaches, such as its use in spectrum license databases or possibly as part of a spectrum usage application.

This paper is structured as follows. Section II provides an introduction to the concepts of distributed ledgers based on blockchain technology. Section III provides a general description of how distributed ledgers could impact spectrum sharing. Section IV describes how distributed ledgers for spectrum management could be implemented in different spectrum access scenarios, and discusses the pros and cons of using blockchain in each scenario. Section V discusses the implications for various stakeholder groups of blockchain-based distributed ledgers in spectrum management. Section VI presents our conclusions and recommendations for future work.

II. DISTRIBUTED LEDGER TECHNOLOGY

Technically, blockchain technology implements a distributed ledger: A secure decentralized form of a database where no single party has control [36]. It offers a resilient, reliable, transparent and decentralized way of recording and manipulating data across all the nodes of a network of interested parties that want to keep the distributed ledger up to date. Blockchain is best known as the basis of Bitcoin, a private digital "cryptocurrency" that can function as money despite not being issued by any government [23]. However, distributed ledgers have many more uses. There are now other services operating on the Bitcoin blockchain, independent blockchains with their own cryptocurrencies (such as the Ethereum and Ripple), and distributed ledgers with no native currency.

The transactions stored on a distributed ledger could represent anything: holdings of a digital currency (as with Bitcoin), the movement of goods across a global supply chain, syndicated loans among financial institutions, or land title records, to name just a few applications under development. Just as relational databases accessed through client-server computing were the foundation for the business revolution built around the World Wide Web, blockchain, as a distributed ledger, is a foundational technology that could have far-reaching impacts [17].

The distinctive feature of blockchain distributed ledgers is that each node connected to the blockchain network can maintain its own copy of the distributed ledger and control over its own data, yet everyone sees the same ledger. There is no need for a master copy or clearinghouse. This property, known as consensus, may be achieved through several technical mechanisms, which are discussed in more detail in Appendix A. The advantages of a consensus-based system depend on the particular application, but they may include: resistance to censorship or tampering, avoidance of the need to trust a central government or private institution, elimination of inefficiencies and errors in reconciling transactions across a network, and an immutable transaction record.

Once information is stored on a blockchain, it can be acted upon through "smart contracts" [8]. Smart contracts are special-purpose code that can execute instructions on a blockchain [36]. They can execute contractual logic, such as paying beneficiaries according to the terms of a will, or granting rights to start a car if the lease is paid up. Bitcoin uses a very simple set of smart contract functions limited for security reasons to moving currency tokens between accounts. Other systems go farther. Smart contracts mean that virtually any activity that can be

represented in software could, in theory, be implemented in an automated and distributed form on a blockchain. This idea was proposed by Szabo in the 1990s [32], but was not well-known until the emergence of cryptocurrencies [7].

There are two primary types of distributed ledger networks: public and permissioned [31]. Which approach is best depends on the application scenario.[2] In public (permissionless) blockchain systems such as Bitcoin, anyone can join the network, so all nodes are treated as potential attackers. Producing a reliable consensus involves significant performance overhead. Permissioned blockchains limit participation to identified users. While this restriction simplifies security and governance, it could make it easier for one or a small number of participants to exercise control.

Table 1 summarizes key characteristics of blockchain-based distributed ledgers.

Benefit	Description
Decentralization	No trusted party or intermediary is needed to validate transactions. Users control their own data.
Transparency	The history of transactions and the software algorithms governing the blockchain network are typically public for anyone to review.
Immutability	It is extremely difficult to change data recorded on a blockchain.
Availability	Blockchain ledgers are replicated among many nodes, making them highly available even if some nodes become inaccessible.
Security	All entries in the ledger are cryptographically secured. All transactions are digitally signed, and access is through public/private cryptographic key pairs.

Table 1. Characteristics of a blockchain

III. BLOCKCHAINS FOR SPECTRUM SHARING

As a general-purpose database-type technology, blockchain can in theory be applied to virtually any business context. However, the potential benefits of distributed ledgers come with costs. Blockchain technology is not the best solution for every scenario. The first step in assessing the usefulness of blockchain is to ask whether its features — decentralization, transparency, immutability, availability, and security — are relevant for the application at hand. The World Economic Forum suggests a similar approach [39]. If all relevant data are to remain under the control of a single trusted party, for example, there is no need for a decentralized solution. The FCC table of spectrum frequency allocations [12] published on a blockchain would be no better than the document published in the Federal Register.

[2] For purposes of this paper we differentiate the two general categories, although there are many gradations and hybrids of public and permissioned blockchains under development.

From this high-level perspective, spectrum sharing seems like a promising candidate for blockchain technology, as shown in Table 2.

Benefit	Potential Application to Spectrum Sharing
Decentralization	Eliminate the need for trusted third parties such as spectrum licensees, band managers, and database/SAS administrators.
Transparency	Better localized visibility into spectrum usage; auditability of activity for effective implementation of spectrum sharing rules.
Immutability	Permanent records prevent tampering, facilitate accurate auditing/enforcement, and can ensure accurate implementation of rules.
Availability	More reliable accessibility of spectrum sharing databases.
Security	As communications infrastructure, wireless systems need strong security against attacks. Secure ledgers also foster reliable enforcement of sharing regimes.

Table 2. Blockchain characteristics applied to spectrum sharing

In contrast with traditional exclusive frequency allocations, spectrum sharing by definition involves multiple entities with rights to use the spectrum. Management mechanisms using databases are being employed for spectrum sharing regimes such as TV White spaces (TVWS) and the Citizens Band Radio Service (CBRS). Since blockchains are a form of database, it is worth exploring whether they could be used to enhance the effectiveness of various forms of spectrum sharing.

Information about access rights and usage can be recorded on a distributed ledger, and managed using smart contracts. Distributed ledgers offer benefits compared to centralized databases for tracking property rights and assets which could make them effective tools for spectrum management. Some of the benefits we foresee are:

- Increased speed in the evaluation of available spectrum resources (in a given area) and registering spectrum use without incurring the processing delay of an authorization from a regulator. Service operators participating in a blockchain for spectrum management interactions (e.g., sharing and trading) could check their own local copy of the distributed ledger to decide what spectrum resources to use.
- Regulators can use the information in the distributed ledger for evaluating spectrum access efficiency, computing fees for spectrum use, and enforcing spectrum access regimes.
- With the use of smart contracts, dynamic and rule-based spectrum use interactions can be tracked and enabled such as: changing the fees for the use of spectrum based on time of day, automatic transfer and reconciliation of spectrum use fees, facilitation of spectrum trading interactions between service providers.

As a more concrete example, DiPascale et al propose a smart contract system for providers of "small cell as a service" to implement service level agreements (SLAs) for mobile network operators in localized areas [12]. This use case could in theory be implemented either on licensed spectrum or through unlicensed frequencies using a mechanism such as LSA to provide quality of service guarantees. The authors focus on how the smart contract could automate the processes of payment and enforcement of the SLA, making it easier for individuals or other small-scale antenna operators to implement these arrangements with operators.

Table 3 offers a high-level comparison of public and permissioned blockchain-based approaches to the primary spectrum management approaches in use today.

There are a number of issues that would need to be considered to implement blockchain-based spectrum sharing. Mobile devices would likely not have the processing power and battery capacity to operate as full blockchain nodes, but fixed devices might, depending on the consensus protocol used.

One additional issue is that unless limited to nodes that have a wired network connection, the distributed ledger would likely also use spectrum resources for the communications needed to validate transactions. This could create capacity issues, especially if the blockchain uses broadcast communications among nodes, as Bitcoin does. High-performance distributed permissioned ledgers may have significantly lesser communications requirements, because nodes are trusted [31]. In addition, the inherent unreliability of wireless communication, which is magnified in a primary non-cooperative sharing environment, will likely require adaptation of blockchain protocols in the same way that wireless communications devices must incorporate greater error correction and buffering than wired ones.

There are a various other practical implementation questions that we only address here in a cursory way, such as who would operate and govern the blockchain networks, how they would be funded, and how they would be deployed. Because the effects of wireless transmissions are localized, a blockchain would need to have sufficiently dense information to be useful.

	Technical Benefits	Business Benefits	Limitations
FCC exclusive licensing	Clear boundaries between allocations Receivers can be inexpensive	Auctions get spectrum to those who value it most, and raise revenue Licensees have confidence about rights	Limited flexibility Fails to maximize spectrum utilization Potential for licensee spectrum hoarding
Unlicensed	Encourages innovation Devices improve with hardware and software	Permissionless entry Device purchases replace recurring service charges	No guaranteed transmission quality Potential for "tragedy of the commons" No ability to protect primary users
3rd Party DB/SAS	Allows both guarantees for primary users and open access Mandatory rules provide certainty compared to unlicensed	Added capacity without new auctions/clearing Allows heightened protection/override for government uses Flexibility for market participants	Database provider controls data Need to convince incumbents of value proposition Accuracy of database records not guaranteed
Public blockchain	Transparent ledger for spectrum management and auditing Strong security High availability	Users control data Facilitates spectrum access fees Complex arrangements via smart contracts Cryptocurrencies can incentivize cost-based activities	Significant overhead of consensus protocols Uncertain governance Anonymity of users could pose enforcement challenges
Permissioned blockchain	High performance Defined governance rules Transparent ledger for spectrum management and auditing Strong security High availability	Users control data Facilitates spectrum access fees Complex arrangements via smart contracts	Questionable benefits relative to traditional databases Require identification of network participants

Table 3. Benefits and limitations of spectrum sharing mechanisms

IV. APPLICATION TO SPECIFIC FORMS OF SPECTRUM SHARING

There are many ways in which researchers have proposed sharing spectrum. Each approach makes different assumptions and may have different functional requirements to support it. Even if blockchain technology is useful for spectrum sharing generally, its value may depend on matching implementation details with sharing scenarios. However, we propose that it is not necessary, at this point anyway, to consider the functional requirements for *each* spectrum sharing scheme that has been proposed and that it is sufficient to consider *classes* of approaches.

	Non-Cooperative	Cooperative
Primary	Unlicensed	Secondary Markets
Secondary	Opportunistic	Cooperative Sharing

Table 4. Modes of spectrum sharing

To this end, we consider the typology for spectrum sharing proposed by Weiss and Lehr in [35], reproduced in Table 4 as a guide for this discussion. It should be noted that there are approaches and technologies that arguably fall between the categories listed, so these four categories are best seen as archetypical with the possibility that some forms of sharing do not neatly fit into any one of these categories.

The term "primary sharing" in Table 4 means that all users have equivalent (or equal) rights to access the spectrum, as is the case, for example, in the unlicensed bands. In contrast, a secondary sharing regime implies a hierarchy of rights, where incumbents/primary users/license holders have superior rights to spectrum entrants/secondary users. TV white spaces and the Citizen's Broadband Radio Service (CBRS) as well as Licensed Shared Access (LSA) are examples of this kind of rights relationship. Much of the research in spectrum sharing assumes a secondary sharing regime. In the table, "cooperative" sharing means that ex ante agreements have been struck between the sharing parties regarding sharing. Secondary markets that involve voluntary exchange can be thought of as cooperative sharing, as sharing techniques such as LSA. Finally, in non-cooperative sharing, users do not coordinate their use ex ante.

It is important to keep context in mind when applying a simple framework such as the one in Table 4. For example, while TVWS can be seen as a form of cooperative secondary sharing when the relationship between the class of secondary users and the class of primary users is considered, sharing among secondary users may be non-cooperative. Similarly, sharing between primary users in this case is cooperative (through the licensing process) and primary.

We will use this framework to explore if and how blockchain technology might be applied for spectrum sharing.

A. Primary non-cooperative sharing

In this kind of sharing, users do not coordinate their usage of the spectrum in advance and they have equal (or equivalent) rights to transmit and receive. The most straight-forward example of this type of sharing would be the open access spectrum sharing as typified by the unlicensed ISM bands (even though some uses of these bands implement cooperation in their medium access protocols). There are two sub-categories of primary non-cooperative sharing:

1. *Open Access Commons*: In open access commons, any spectrum user that meets the technical requirements of the band may operate. No user is guaranteed any additional protection against interference. In such an environment:
    - Spectrum users must be able to find stations to communicate with (whether base stations or other mobile users in an ad hoc network)
    - Spectrum users need to be able to detect and deal with other stations who are transmitting and who may or may not be "polite". This is, in part, what MAC protocols do.
2. *Private Commons:* In a private commons, access may be governed, meaning that an additional function will be determining who gets to use the spectrum and when (as suggested in [34]). For private commons, additional functions come into play:
    - Spectrum users must have a way of managing the commons and allowing and disallowing access (i.e., exercising collective action rights as described in [31]);
    - Spectrum users must have a way of determining others' usage for enforcement purposes.

The success of WiFi in the ISM bands shows that databases are not necessary for effective primary non-cooperative sharing, at least in some usage contexts. However, they might improve the efficiency of spectrum utilization in such environments or facilitate business models such as mesh networks that have been widely explored by researchers but slow to develop commercially. In a rapidly changing communications environment, spectrum use will change as mobile devices alter their location and fixed devices go in and out of service. Each spectrum user will only need to know about its local environment at any given moment to determine the availability of spectrum resources. All spectrum use data recorded on a blockchain can be timestamped and geocoded, either by the device itself or the node in the blockchain network that first recorded the information. Based on this information, devices or network controllers could develop a near real-time map of the local spectrum environment depending on the latency of the blockchain to attain consensus on the validity of recorded spectrum use entries. Such information could be used to decide whether to admit new users to a private commons.

In essence, blockchain would be used to keep a dynamic record of the users operating in the band. However, having each device register its location on the blockchain would generate

significant overhead. The practical question is whether the benefits in terms of spectrum re-use and improved device performance would exceed the costs.

Open access commons might lend themselves more to public blockchain networks, because they are open to anyone. Spectrum users in an open access environment are untrusted. Users cannot assume that other users (or more precisely, MAC layers of their devices) will be polite. On the other hand, blockchains for this category of spectrum sharing are likely to handle a relatively high volume of transactions. If the blockchain is dynamically recording all users of a band as they operate and move, it will need scalable real-time processing capacity. This tends to be more difficult on public blockchains, because they use complex consensus mechanisms in place of trusted identity of participants.

Furthermore, on an open access commons, no particular protocol is required of devices, so participation in a blockchain-assisted system would not be guaranteed. Users or devices would need sufficient incentives to contribute to, and check with prior to transmission, a blockchain distributed ledger. A related question is who would be willing to operate the nodes of such a network. One answer might be to use a cryptocurrency. Device operators could pay to participate in a blockchain-mediated real-time tracking system that would improve performance, and node operators would be compensated for maintain and verifying transactions on the ledger.

Finally, a blockchain could aid regulators in assessing activity, and in pursuing enforcement against users who violate the transmission standards for the band. However, it is unclear whether sufficient information would be stored in the blockchain to support an enforcement action.

Most of the same benefits of blockchain for open access commons would apply to the private commons scenario. In the case of a private commons, a permissioned blockchain would be a good fit, because all users must be identified in order to access the spectrum. There might be efficiencies of having the operator of the commons also manage the blockchain, although a third party could handle it too. The operator could use the blockchain to manage individual devices efficiently, or to develop longer-term analytics about the spectral environment.

In a private commons, compliance with coordination standards is required by the commons manager. Therefore, enforcement is not just a matter of baseline requirements set by regulators, but of the specific terms set for the private commons. Because every device would have to register and be identified, smart contracts could be used to establish payment mechanisms from devices to the commons manager. They could also operate as a “kill switch” for devices that fail to meet applicable requirements.

The following table summarizes the benefits, drawbacks and characteristics of using a blockchain that keeps a record of the wireless users operating in a primary non-cooperative sharing environment

Primary non-cooperative Sharing	
Open Access Commons	**Private Commons**
Benefits(+) and drawbacks(-)	
(+) Enhanced spectrum use efficiency (+) Near real-time map of local spectrum use can be built (+) Blockchain can be used to confirm presence of a node and verify its identity (-) Overhead to run the blockchain, no reward incentive for nodes to maintain the blockchain	(+) Enhanced spectrum use efficiency (+) Near real-time map of local spectrum use can be built (+) Blockchain facilitates the enforcement of spectrum access rights
Blockchain type to use	
Public blockchain. However, likely infeasible due to the overhead and network structure needed to operate it.	Permissioned blockchain

Table 5. Benefits and drawbacks of blockchains for primary non-cooperative spectrum sharing

B. Primary cooperative sharing

In *primary, cooperative* sharing, users coordinate their uses ex ante. The best example of this might be the (as yet hypothetical) real time spectrum markets, as studied by [7] [33]. The functions that this kind of sharing implies are:

- Spectrum users need to be able to find transmission opportunities that map to their needs
- Spectrum users need to be able to exchange usage rights rapidly

Many aspects of blockchains for primary cooperative sharing will be similar to primary non-cooperative environments. When used to identify stations to communicate with or to supplement sensing of the local environment, a ledger in a cooperative environment would have similar properties to those described in the previous section. The major difference is that in cooperative sharing, uses are coordinated and rights are allocated before transmission occurs. The primary function of a distributed ledger in an environment of real-time spectrum markets would be to record and enforce market transactions.

For TVWS and the 3.5 GHz SAS, databases essentially memorialize a fixed set of rights: two-tier secondary sharing rules for the case of TVWS, and three-tier SAS based operations for 3.5 GHz. Secondary or lower tier users must query the database to protect the primary users. In the case of primary cooperative sharing, a database would serve a slightly different purpose. Because all users are primary, no one can transmit without first obtaining transmission rights. On the other hand, those with transmission rights need not account for others.

A ledger for primary cooperative sharing must therefore be able to record transactions for transmission rights where additional logic could use the records in enforcing those rights among devices. Spectrum access coordination and maintenance of the ledger could be

performed by a modified SAS or a band manager [7]. The band manager would read requests for spectrum entered on the blockchain by the nodes from entities that want to operate in a given location. The requests would specify the spectrum requirements of the node (i.e. bandwidth, central frequency, location, time, etc.). The band manager proceeds to determine if the request can be satisfied and proceeds to record a spectrum assignment in the blockchain that the requesting node can afterwards read and enable. For a real time spectrum trading market operation such as that described in [7] the band manager would instead become a spectrum exchange that would record requests and offers of spectrum and perform the exchange of transmission rights via smart contracts.

Different types of contracts and their related spectrum trades could be enabled. As an example, in a time limited spectrum use trade, when the contract terminates or the rights-holder negotiates a new agreement, the blockchain can be used to enforce the new allocation of transmission authorizations. The flexibility of smart contracts would allow for transactions of arbitrary levels of sophistication. For example, a spectrum rights-holder might grant another user transmission rights limited by time, geography, transmission characteristics, or throughput. Transactions could be contingent on verification of payment, or verification that devices are compliant with transmission protocols.

For many instances, the use of smart contracts on spectrum management blockchains will require access to external information to execute the logic of the contract. Smart contracts can reference information outside the blockchain in two ways. They can incorporate oracles, which are automated systems that verify information (such as a stock price on a given date) [4]. Or they can incorporate human arbitrators. Most blockchain-based systems, including Bitcoin, support a feature called *multisig*, in which the approval of transactions require the submission of M out of N cryptographically signed approval messages (most commonly 2 out of 3) [24]. If each party to a transaction has one signature key and a neutral arbitrator has the third, the arbitrator's decision can bind the parties and activate the enforcement mechanism of the smart contract. A smart contract for primary cooperative spectrum sharing might, for example, require a user to submit to verification that its devices meet certain criteria by a third-party firm, which would control the private signing key needed to enforce the smart contract.

In addition to the flexibility and automation of smart contracts, blockchains for primary cooperative sharing could also provide a transparent, auditable, unified record of transactions. This would provide the same benefits in the spectrum sharing context as blockchains in other industries. For example, having a single shared ledger means that each spectrum user doesn't have to maintain its own database, verify that its records accord with its counterparties, and/or trust the accuracy of a central clearinghouse. The fact that the government or a monopoly private contractor would not be needed to operate the transaction clearinghouse could address concerns about biases and excessive charges that have arisen in analogous contexts such as telephone numbering administration and internet domain name registration. With a blockchain, each party controls its own data, but everyone is able to see the entire ledger. Assuming the ledger is transparent, market participants as well as regulators can perform audits and observe market trends. Regulators could also use the blockchain to tax transactions

as a funding mechanism. If transactions are considered competitively strategic, a permissioned ledger could be made non-transparent, or could only be viewed by the regulator.

Blockchains for the primary cooperative sharing category would require less transaction throughput than the real-time spectrum map described in the previous section. They would only be recording explicit transactions between spectrum rightsholders, rather than tracking the activity of every device. In a real-time spectrum marketplace, the volume of transactions would not be trivial, and the system would have to update its state quickly enough for devices to receive accurate information. However, blockchain operations introduce latency in registering transactions, in particular because of block latency which is incurred by nodes in the blockchain having to wait for enough requests and/or assignment transactions to have been issued before a block can be built and deemed a candidate to be incorporated in the blockchain and submitted to the consensus algorithm used in a particular blockchain implementation. Thus, only near-to-real time operations can be enabled, but if the block size to speed tradeoff is carefully balanced, a spectrum marketplace using a blockchain could be feasible, although research is still needed to be certain.

Blockchain use in Primary Cooperative Sharing
Benefits (+) and drawbacks (-)
(+) Enables spectrum trading markets
(+) Enables different types of spectrum trading transactions with the use of smart contracts
(+) Provides an auditable, unified record of transactions
(-) True real-time spectrum market is not feasible due to latency in the blockchain. A near-real-time market could be feasible but needs to be carefully designed.
Blockchain type to use
Public or permissioned blockchain could be used. However, a permissioned blockchain would be simpler to manage, faster, and can better protect transaction information that could be used for competitive purposes. The regulator would need to have access to the blockchain to guarantee fair market operation.

Table 6. Benefits and drawbacks of blockchains for primary cooperative spectrum sharing

C. Secondary non-cooperative sharing

S*econdary, non-cooperative* sharing is the opportunistic sharing case typified by cognitive radios [15], where secondary users do not coordinate their usage in advance with primary users. This approach has been widely studied. Functions implied by this kind of sharing include:

- Determination of where transmission is possible (spectrum hole detection)
- Determination of other opportunistic users who are using the same band
- Detection of when transmission is no longer possible

There have also been proposals, such as the Cognitive Pilot Channel (CPC) [29], that enable a degree of cooperation between the incumbent (primary user) and the entrant (secondary user). A blockchain could be used as a secure implementation of this channel, providing a history of incumbent interventions to the community. Basically, the CPC would provide information to radio terminals so that they can decide how to (opportunistically) use spectrum. The

information could include, a list of available frequency bands and which primary operators are active at a given time and space. This history is useful for entrants to determine their risk [9]. TVWS could also be seen as a kind of hybrid, since coordination with the primary is cooperative while sharing available channels is opportunistic.

The most prominent uses of blockchains for secondary non-cooperative sharing would likely be to enhance the ability of opportunistic devices to identify transmission opportunities, and to automate the process of auditing and enforcement for those opportunistic users. As with primary non-cooperative sharing, even if unlicensed devices are not required to follow a particular protocol, they would benefit from richer information about primary users. The decentralization, availability, and security of blockchain distributed ledgers could be an improvement over the centralized databases in existing systems such as TVWS. They might allow for systems analogous to TVWS where the primary users' transmitters are not fixed, or their transmission patterns are more complex than television broadcasting.

The ultimate question here is whether an opportunistic/non-cooperative environment lends itself to the use of some feature(s) of blockchain. Does non-cooperation means not using blockchain services? We see that from a binary (yes/no) perspective it might seem that a noncooperating device would not use blockchain services, but there is no need to assume such strict categories and it is likely that there are many shades of gray to consider in terms of these definitions of cooperative and non-cooperative. Maybe there is a model for having a "non-cooperative" environment where devices participate in a blockchain for spectrum sharing to acquire environmental input, or possibly simply participate because the spectrum policy mandates participation for reasons of producing a log of activities for any potential enforcement review that might arise.

Smart contracts could further enhance such a system. They could be used to implement geo-specific transmission masks to limit the ability of secondary devices to interfere with primary users, while leaving them the flexibility to transmit when, where, and how they choose. If primary users experience interference, a blockchain-based ledger recording the activities of secondary devices could be used to assess violations, or even impose penalties through smart contracts.

One of the challenges with the current TVWS system is that some primary users provide inaccurate information that artificially reduces the scope for secondary users [25]. While a blockchain verifies consistency of information on a distributed basis, it does not necessarily solve this problem. The blockchain itself has no way to determine if the information provided by authorized users is truthful. Once information is added to the blockchain, it cannot easily be tampered with, but garbage in is still garbage out.

Additional verification and identity/reputation layers could theoretically be built on top of the ledger to deal with this "fake news" problem. There is widespread experimentation with "token curated registries" [15] and other mechanisms that employ the economic incentive structures of cryptocurrencies and the immutable recording of blockchains to improve information

quality. In essence, these approaches make it profitable to be truthful and unprofitable to be untruthful, so long as a majority of users are honest. Further study is required to evaluate whether such solutions might be useful for spectrum access ledgers.

Blockchain use in Secondary non-Cooperative Sharing
Benefits (+) and drawbacks (-)
(+) Provides a record of primary user operations against which opportunistic access operations can be executed
(-) Additional overhead and little differentiation with non-Cooperative access approaches for secondary users such as those used for TVWS.
Blockchain type to use
Public or permissioned blockchain could be used. As discussed above, there are questions as to what defines a non-cooperative device and how this device might interact with blockchain services.

Table 7. Benefits and drawbacks of blockchains for secondary non-cooperative spectrum sharing

D. Secondary cooperative sharing

In *secondary cooperative sharing*, users coordinate their use ex ante. Mobile Virtual Network Operators (MVNOs) behave in this way, but so do users under the License Shared Access (LSA) regime or the Citizen's Band Radio Service (CBRS) recently proposed by the FCC. Also, this mode of sharing might also be useful to describe users of a commercial mobile service, where the usage is controlled through the access system (e.g., HSPA, LTE).

Secondary cooperative sharing is likely a rich domain for blockchain implementation. Most of the discussion in Section B about blockchains and smart contracts for primary cooperative sharing would also apply to the secondary model. The major difference is the greater variety of transactions possible in a secondary cooperative sharing environment. Rightsholders are not simply transacting to give all or nothing primary rights to other parties. They can subdivide their rights under any set of arrangements they choose.

The issue of who operates the blockchain may also have a different resolution in this category. There need not be one blockchain for the entire band. An incumbent, for example, might operate a private blockchain to manage its MVNOs or its implementation of LSA. The blockchain could coordinate among secondary users subsidiary to that incumbent, but wouldn't necessarily affect others.

There are a few applications in particular to consider in this spectrum sharing category:

- Registration/authorization of devices: Base stations of a radio access network provider that dynamically allow devices associated with previously authorized entities to use the base station resources. It is possible to imagine this association to occur via a smart contract, which would result in a blockchain implementation
- Spectrum Access Systems (SAS) can be seen as an approach to the governance of shared spectrum [34]. WinnForum has identified some information sharing principles that apply particularly to sharing information between SASs. It is possible that blockchain based

systems can support these design goals naturally. Especially those related to CBSD registration data captured by a SAS and that will need to be shared with regulators and other SAS entities.

In the particular case of blockchain supported SAS operations. A distributed ledger would be useful in SAS to SAS interactions that aim at maintaining a unified view of the devices registered for CBRS operation in a particular region (or set of regions) where two or more SASs may be offering spectrum access services. Similarly, the interactions between the operators of ESC (Environmental Sensing Capability) devices and SAS operators could be secured and managed in a blockchain based distributed ledger.

….

Blockchain use in Secondary Cooperative Sharing
Benefits (+) and drawbacks (-)
(+) Enables secure, distributed handling of spectrum usage rights
(+) Enables different types of secondary spectrum use transactions with the use of smart contracts
(+) Provides an auditable, unified record of transactions
(-) Latency in blockchain operation would limit the rate at which new spectrum use transactions can be validated
Blockchain type to use
Public or permissioned blockchain could be used. However, a permissioned blockchain would be simpler to manage, faster, and can better protect transaction information that could be used for competitive purposes. The regulator would need to have access to the blockchain to guarantee fair market operation and efficient use of spectrum resources.

Table 8. Benefits and drawbacks of blockchains for secondary cooperative spectrum sharing

V. Implications for stakeholders

A blockchain-based spectrum management model could have a broad set of implications for different entities in the spectrum ecosystem. Here we briefly consider several of the major stakeholder in this space.

Incumbents

Incumbent holders of spectrum might view blockchain as a negative if it ushers in the sharing of their current exclusively held spectrum. Such sharing might increase concerns over interference issues, but more significant it might result in decrease value to exclusively held spectrum. On the other hand, there might be blockchain models that the incumbents use as a coordination tool for their users, or possibly to coordinate leasing of a given band. We generally believe incumbents will be more concerned about the potential increase in sharing, loss of control, and negative impact on spectrum values, than in the opportunities to improve management of the spectrum they control.

Entrants

New entrants would likely have the most to gain if blockchain-based spectrum management was adopted. It could allow for easier, more coordinated access to spectrum and enable access to shared (possibly free or low cost) spectrum. As mentioned above, it is possible that spectrum could be accessed in some form of coordinated leasing or new unlicensed models, lowering the high bar often associated with obtaining adequate spectrum. Cryptocurrencies could support new economic arrangement involving micropayments and automated smart contracts, which might foster broader and better-quality access on an unlicensed foundation.

Spectrum Managers

The blockchain model poses a direct threat to spectrum management functions, such as database operator or band managers. In blockchain systems, many of the functions performed by these entities would be implemented in a decentralized model that does not have a significant role for them.

Policymakers

The implications of blockchain on spectrum management are probably biggest on policymakers and spectrum regulators. While this approach could enable new access and new business models, relieving demand by improving access, it could also lessen the current command and control model of spectrum management in a way that some regulators would be unwilling to consider. Blockchain might also have a negative impact on spectrum revenues if it allows for easier and cheaper access to what has been managed as a scarce resource.

One of the more interesting applications could be blockchain as a tool for coordination between governments. For example, blockchain could be employed as a management layer when US troops are using spectrum during times of friendly occupancy (a major issue for DoD). Lastly, it is worth noting that blockchain could be part of a more involved process of policing for interference events. Here, a log would exist indicating who was using bands at what time/place and this could help in resolving interference events. Of course, it isn't clear that blockchain would be needed for such monitoring, but it would provide some useful attributes for such a process.

International Implications

At an international level, it is unclear just how this would play out. It could be that agreements would be put in place to allow blockchain as an enabler of cross border access to spectrum. It could be that blockchain be used as a monitoring (accounting) tool in certain bands or used as a tool for coordination during times of joint use of spectrum. The biggest concern is that this approach might raise sovereignty issues by disintermediating the power and role of the national regulator by differing to a distributed permissionless approach. Each nation state could decide whether blockchain-connected devices would be allowed to operate in its territory. However, because blockchains are decentralized (especially public blockchains), it might not be easy for a government to prohibit operation of the blockchain itself to record information for spectrum-sharing applications.

VI. CONCLUSIONS

This paper takes a broad look at the application of blockchain to spectrum sharing. We demonstrate that a number of areas are worth of deeper research. It is too early to declare with confidence that blockchain will be superior to conventional database technology, or even that useful blockchain-mediated spectrum sharing is technically feasible. However, the primary benefits of blockchain-based distributed ledgers—decentralization, transparency, immutability, availability, and security—are all well-suited to spectrum sharing. By drilling down into four modes of spectrum sharing, we have identified a number of scenarios for productive implementation of blockchain technology.

As situations suitable for blockchain-based approaches in the spectrum sharing universe are identified, some additional questions arise that require further research. From a technical perspective, the question is whether blockchain performs "better" than alternate implementations. In this analysis, it would be critical to identify the correct objective function; it would be one thing to compare two systems based on technical requirements and quite another if socio-technical goals were to be considered.

There are also several general challenges for blockchain technology that remain to be resolved. Major public blockchains such as Bitcoin and Ethereum use a consensus mechanism, proof of work, that requires massive energy expenditures by the miners who compete to verify transactions. Alternatives such as proof of stake do not yet have a track record of operating securely at scale. Scalability, governance, and interoperability are major challenges for all blockchain system, especially public blockchains. A number of solutions are under active development, such as new consensus algorithms and "layer 2" solutions that rely on the blockchain for security but are not limited to its performance characteristics. Cryptocurrencies tend to be extremely volatile, and attack both scams and theft. While these may not directly affect blockchain systems designed for applications such as spectrum sharing, a major cryptocurrency crash could have negative fallout on development activity and adoption.

Permissioned blockchains, on the other hand, need to demonstrate that they offer significant differentiation from traditional approaches. If a database-driven system such as an advanced SAS is not being deployed today, for whatever reasons, it is not obvious that a permissioned blockchain would cause a different result. And there are many different consensus mechanisms and network configurations under the permissioned blockchain heading, just as for public blockchains. A fragmented situation in which different groups push for their preferred solution could eliminate potential benefits of a universal shared ledger. Finally, deployment and operation of blockchain networks and the associated decentralized applications and smart contracts is not costless. There would need to be economic models, whether through internal

cryptocurrencies or external funding, to support deployment of the systems described in this paper.

Blockchain is an ideology as much as it is a technical approach. Further work is needed to assess how consistent this ideology is with spectrum sharing, or rather, when it is. From an initial observation, the emphasis on decentralized coordination that animates blockchain communities seems like a strong fit for spectrum sharing. Given the high level of development activity and interest in blockchain technology today, and the continued need for enhanced spectrum access and utilization methods, blockchain approaches to spectrum sharing deserve further investigation.

REFERENCES

[1] A. M. Antonopoulos, "Mastering Bitcoin: unlocking digital cryptocurrencies," O'Reilly Media, Inc., 2014.

[2] M. Andreessen, "Why Bitcoin Matters," New York Times, January 21, 2014

[3] A. Back et al., "Hashcash-a denial of service counter-measure," 2002.

[4] J. Buck, "Blockchain Oracles, Explained," CoinTelegraph, October 18, 2017, https://cointelegraph.com/explained/blockchain-oracles-explained.

[5] V. Buterin, "A next-generation smart contract and decentralized application platform," White Paper, 2014.

[6] R. Caetano, Learning Bitcoin: embrace the new world of finance by leveraging the power of crypto-currencies using Bitcoin and the Blockchain. Birmingham: Packt Publishing, 2015.

[7] C. Caicedo and M. B. Weiss, "The viability of spectrum trading markets," IEEE Communications Magazine, vol. 43, no. 3, pp. 46–52, 2011.

[8] M. Crosby, P. P. Nachiappan, S. Verma, and V. Kalyanaraman, "Blockchain technology beyond bitcoin," http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf, Sutardja Center for Entrepreneurship & Technology Technical Report. UC Berkeley, Tech. Rep., 16 October 2015, accessed: 05-31-2016.

[9] L. Cui, M. B. Weiss, B. Morel, and D. Tipper, "Risk and decision analysis of dynamic spectrum access," Telecommunications Policy, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0308596117300460

[10] J. S. Czepluch, N. Z. Lollike, and S. O. Malone, "The use of block chain technology in different application domains," 2015.

[11] "Vumi for developers," http://vumi.org/developers/, Developers. Praekelt Foundation, accessed: 6-17-2016.

[12] E. Di Pascale, J. McMenamy, I. Macalusa, and L. Doyle, "Smart Contract SLAs for Dense Small-Cell-as-a-Service," https://arxiv.org/pdf/1703.04502.pdf

[13] Federal Communications Commission, FCC Online Table of Frequency Allocations, https://transition.fcc.gov/oet/spectrum/table/fcctable.pdf

[14] G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain." Retrieved from https://www.researchgate.net/profile/Georgios_Foroglou/publication/276304843_Further_applications_of_the_blockchain/links/5556f20608ae6fd2d8237a34/Further-applications-of-the-blockchain.pdf

[15] M. Goldin, Token-Curated Registries 1.0, Medium, September 14, 2017, https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7

[16] S. Haykin, “Cognitive radio: Brain-empowered wireless communications,” IEEE Journal on Selected Areas in Communication (JSAC), vol. 23, no. 2, pp. 201– 220, 2005.

[17] M. Iansiti and K.R. Lakhani, “The Truth About Blockchain”, Harvard Business Review, January–February 2017 issue (pp.118–127).

[18] S. King and S. Nadal, “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake,” self-published paper, August, vol. 19, 2012. https://pdfs.semanticscholar.org/0db3/8d32069f3341d34c35085dc009a85ba13c13.pdf

[19] D. Kraft, “Difficulty control for blockchain-based consensus systems,” Peer-to-Peer Networking and Applications, pp. 1–17, 2015.

[20] J. Mattila, “The blockchain phenomenon,” Berkeley Roundtable on the International Economy (BRIE), 2016.

[21] D. Mazieres, “The stellar consensus protocol: A federated model for internet-level consensus,” Draft, Stellar Development Foundation, 15th May, available at: https://www. stellar. org/papers/stellarconsensus-protocol. pdf (Accessed 3rd June, 2016), 2015.

[22] M. Miller, The ultimate guide to Bitcoin, 1st ed. Indianapolis, Indiana: Pearson Education, 2014.

[23] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[24] A. Narayanan, J. Bonneau, E. Felton, A. Miller, “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction” (2016).

[25] National Association of Broadcasters, “Emergency Motion for Suspension of Operations and Petition for Rulemaking”, 2015, available at: http://www.nab.org/documents/newsRoom/pdfs/031915_TVWS_Emergency_Petition.pdf.

[26] A. Narayanan and Jeremy Clark, “Bitcoin’s Academic Pedigree,” Communications of the ACM, December 2017, Vol. 60 No. 12, Pages 36-45.

[27] S. Pearl, “Distributed public key infrastructure via the blockchain,” 2015.

[28] W. Reijers, F. O’BrolchA¡in, and P. Haynes, “Governance in blockchain technologies & social contract theories,” Ledger, vol. 1, no. 0, pp. 134–151, 2016. [Online]. Available: http://ledgerjournal.org/ojs/index.php/ledger/article/view/62

[29] O. Sallent, J. Perez-Romero, R. Agusti, and P. Cordier, “Cognitive pilot channel enabling spectrum awareness,” in 2009 IEEE International Conference on Communications Workshops, June 2009, pp. 1–6.

[30] M. Swan, “Blockchain: Blueprint for a New Economy,” O’Reilly Media, Inc., 2015.

[31] T. Swanson, “Consensus as a Service: A Brief Report on the Emergence of Permissioned Distributed Ledger Systems,” http://www.ofnumbers.com/2015/04/06/consensus-as-a-service-a-brief-report-on-the-emergence-of-permissioned-distributed-ledger-systems/

[32] N. Szabo, “Formalizing and securing relationships on public networks,” First Monday, vol. 2, no. 9, 1997.

[33] M. Weiss, P. Krishnamurthy, L. Doyle, and K. Pelechrinis, “When is electromagnetic spectrum fungible?” in IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2012.

[34] M. B. H. Weiss, W. H. Lehr, A. Acker, and M. M. Gomez, “Socio-technical considerations for spectrum access system (sas) design,” in Dynamic Spectrum Access Networks (DySPAN), 2015 IEEE International Symposium on, Sept 2015, pp. 35–46.

[35] M. B. Weiss and W. H. Lehr, “Market based approaches for dynamic spectrum assignment,” Working Paper http://d-scholarship.pitt.edu/2824/, 2009.

[36] K. Werbach, “The Blockchain and the New Architecture of Trust,” MIT Press, 2018.

[37] K. Werbach and N. Cornell, “Contracts Ex Machina,” 67 Duke Law Journal 313 (2017).

[38] WinForum, “Webinar 19: Spectrum sharing committee SAS to CBSD and SAS to SAS protocols,” 23 February 2017.

[39] World Economic Forum, “Blockchain Beyond the Hype,” April 23, 2018, https://www.weforum.org/whitepapers/blockchain-beyond-the-hype.

[40] S. T. Zargar, M. B. Weiss, C. E. Caicedo, and J. B. Joshi, “Security in dynamic spectrum access systems: A survey,”University of Pittsburgh, Working Paper, December 2009. [Online]. Available: http://d-scholarship.pitt.edu/2823/

APPENDIX A: BLOCKCHAIN TECHNOLOGY

Blockchain takes advantage of cryptographic methods to guarantee both trust and reliability of data. All data entries to the blockchain are digitally signed. As the name suggests, data is stored in chains of blocks, each of which incorporates a cryptographic hash function linking it to the prior block. Each new block of transactions is appended to the end of the chain. The nodes that participate on the distributed ledger network broadcast transactions to each other and validate each new block as it is added.

Strictly speaking, not all distributed ledger platforms use the blockchain data structure. R3's Corda platform, for example, combines a blockchain-type consensus mechanism with a traditional relational database for information storage. Following the standard usage, we employ the term "blockchain" for immutable distributed ledgers that use a consensus algorithm so that no entity has control over transaction validation.

As a classic example of a permissionless distributed ledger, Bitcoin uses randomized selection to achieve consensus, backed by an approach called proof of work [1] [23]. Proof of work is designed to make attacks costly for the attackers to subvert the voting-based consensus process. In proof of work, "miners" authenticate blocks by competing repeatedly amongst each other to solve a computationally difficult mathematical puzzle that is related to the information contained in the block. The greater the miner's processing power, the greater the chance of finding the solution and winning. If a miner solves the mathematical puzzle, the miner broadcasts the block of the digital actions to all the nodes of the network to be approved. All the other nodes in the network check the block and if a majority of nodes agree, that block of digital-actions is added to the blockchain. The "winning" miner for each block receives Bitcoin as a reward. Proof of work makes attacks costly, because a dishonest node is competing against the total processing power of the network [36]. Because each block is linked to the previous ones, it becomes more and more difficult to falsify a block as time goes on.

Not all blockchains use proof of work. It requires immense computing power and its associated electricity. Although Bitcoin's proof of work system has worked successfully for since 2009 as the currency went from zero to an aggregate value of over $120 billion at mid-2018 exchange rates, concerns about potential vulnerabilities and misbehavior by miners remain. Proof of stake, which avoids the need for mining and its colossal waste of energy, is being actively explored as the future consensus mechanism for Ethereum, the second most valuable public blockchain [20] [36]. Table A describes the characteristics of a few consensus protocols.

Permissioned blockchains can use more lightweight consensus protocols. In these networks, only authenticated parties can process transactions. The network may be open to anyone meeting specified criteria, or it may be limited to a private consortium. Either way, because nodes are known, they can more easily be trusted. A variety of permissioned blockchains such as Ripple, Stellar, Hyperledger, Symbiont, and R3 Corda use consensus mechanisms based around voting processes among nodes [20] [21]. This can typically be done far more quickly

than proof of work or proof of stake, making it easier to scale permissioned blockchain networks for high transaction volume applications. On the other hand, permissioned blockchains do not offer the same level of decentralization as public systems.

Voting Tool	Advantages	Disadvantages	Resources	Model
Proof-of-Work (PoW)	• Decentralized control	• Power and process consumption	Solving the mathematical puzzle→ processor power→ energy consumption	Bitcoin
Proof-of-Stake (PoS)	• Decentralized control • Low latency • Ease of rule	• Lack of flexible trust	Certificate of Deposit	NXT (Registry, asset exchange, secure messaging, and stake allocation)
Stellar Consensus Protocol (SCP)	• Decentralized control • Low latency • Flexible trust	• Manual broadcasting for the root token	Quorum vote (peer standing)	Vumi (Under development)
Ripple Consensus Protocol	• Decentralized control	• Network monitoring	Exceptional node list based on peer reputation	Ripple

Table A: Several consensus approaches (adapted from [20])