Chapter 5
Blockchain for Dynamic Spectrum Management

Abstract Blockchain is believed to bring new opportunities to dynamic spectrum management (DSM). With features of blockchain, the traditional spectrum management method, such as the spectrum auction, can be improved. It can also help to overcome the challenges about the security or the lack of incentive mechanisms for collaboration in DSM. Moreover, with blockchain, spectrum usage of the DSM system can be recorded in a decentralized manner. In this chapter, we will discuss the potentials of blockchain for spectrum management in a systematic way and using multiple case studies.

5.1 Introduction

Recently, blockchain has received increasing attention, with bitcoin [1] supported by it being the most famous cryptocurrency. Blockchain is essentially an open and distributed ledger, with some key characteristics such as immutability, transparency, decentralization and security. The main idea behind blockchain is to distribute the validation authority of the transactions to a community of the nodes and to use the cryptographic techniques to guarantee the immutability of the transactions. Far from being used only as a ledger, blockchain has been able to support various kinds of cyptocurrencies and smart contracts, which autonomously executes agreements reached between nodes in blockchain networks.

The aforementioned characteristics of blockchain make it beneficial in many areas in communications. For examples, with the encryption algorithms, blockchain has been used to guarantee the integrity of data in the Internet of Things (IoT) [2], and with the traceability, blockchain has been used to design a collaborated video streaming framework for Mobile Edge Computing (MEC) [3]. Moreover, blockchain is seen as a promising technology to achieve more efficient dynamic spectrum management (DSM) [4, 5]. According to Federal Communications Commission (FCC), blockchain could be used to reduce the administrative expenses of dynamic spectrum access systems and thus increase the spectrum efficiency [6].

As a secure ledger, blockchain has been introduced to record the spectrum auction initiated by the licensed users [7]. With the use of blockchain, spectrum transactions

Y.-C. Liang, *Dynamic Spectrum Management*, Signals and Communication Technology, https://doi.org/10.1007/978-981-15-0776-2_5

are recorded and maintained by all the users in an immutable and verifiable manner. Moreover, a dynamic spectrum access system featuring secure cooperative sensing is proposed with the use of blockchain [8]. In such a system, the opportunity of spectrum access is first explored by cooperative sensing and the access right is then allocated through an auction, with all the information of the spectrum auction being securely stored in a blockchain. Besides, the use of a smart contract, which is built on the top of blockchain, has also been explored to execute the spectrum sensing service provided for secondary users [9].

In this chapter, we first give a brief overview of blockchain. Then, from a systematic view, we give some basic principles to illustrate how and why blockchain can be used in DSM, and also address the cost and challenges of using the blockchain. Several instances of blockchain for DSM are then introduced. Finally, a conclusive summary of this chapter is given.

5.2 Blockchain Technologies

Blockchain is essentially an open and distributed database maintained by nodes in a Peer-to-Peer (P2P) network. When a blockchain is used to record transactions between nodes, it can be seen as a distributed ledger. Through cryptographic techniques, the transactions recorded in a blockchain are tamper-resilient; and by distributing copies of the ledger to all the nodes in the network, a blockchain is robust to single point of failures compared to a centralized ledger. In this section, we will give an overview of the blockchain technology, summarize its features and introduce the smart contract, which is an important application of blockchain.

5.2.1 Overview of Blockchain

We give an overview of blockchain from the following five aspects, including the blockchain structure, consensus algorithm, solution of discrepancy in the nodes, digital signature and types of blockchain. Finally, we will illustrate the work flow of a blockchain.

Blockchain Structure: In a blockchain network, transactions are validated by a community of nodes and then recorded in a *block*. As shown in Fig. 5.1, a block is composed of a header and a body, in the latter of which the transaction data is stored. The block header contains the hash of the previous block, a timestamp, Nonce and the Merkle root. The hash value is calculated by passing the header of the previous block to a hash function. With the hash of the previous block stored in the current block, blockchain is thus growing with new blocks being created and linked to it. Moreover, this guarantees that tampering on the previous block will efficiently detected. The timestamp is to record the time when a block is created. Nonce is used in the creation and verification of a block. The Merkle tree is a binary tree with each leaf node

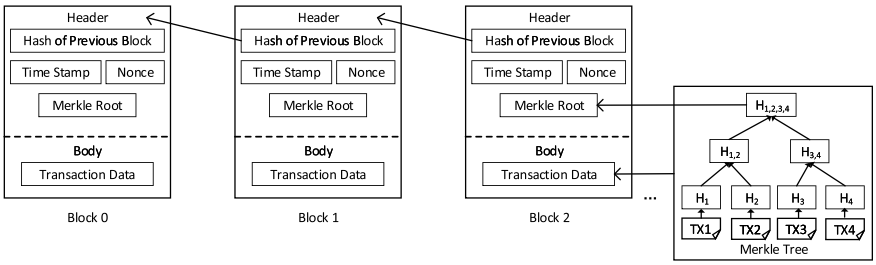

Fig. 5.1 The structure of a Blockchain. A block is composed of a header and a body, where a header contains the hash of previous block, a timestamp, Nonce and the Merkle root. The Merkle root is the root hash of a Merkle tree which is stored in the block body. We denote a transaction as TX and take the 3-th block, which only contains four transactions, as an example to illustrate the structure of a Merkle tree

labelled with the hash of one transaction stored in the block body, and the non-leaf nodes labelled with the concatenation of the hash of its child nodes. Merkle root, i.e., the root hash of a Merkle tree, is used to reduce the efforts to verify the transactions in a block. Since a tiny change in one transaction can produce a significantly different Merkle root, the verification can be completed by simply comparing the Merkle root instead of verifying all the transactions in the block.

Consensus Algorithm: As a distinctive feature, blockchain eliminates the need for a trusted third-party to validate the transactions. Instead, a *consensus* is reached between all the nodes before a block, recording multiple transactions, is included into the blockchain. Essentially, a consensus algorithm is used to regulate the creation of a block in an unbiased manner to resist malicious attack. There are different consensus algorithms, such as Proof of Work (PoW), Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT), to adapt to the blockchain of different types and the performance requirements in different applications.

PoW is widely used in blockchain networks such as bitcoin. With PoW, a new block is created when a random number called *Nonce* is found. The nonce can be verified by checking if the hash of the block header, added with Nonce, satisfy certain conditions. Due to the characteristic of hash function, Nonce is easy to verify but can only be found by trial and error. Thus, devoting computation resources to find a valid Nonce can be seen as a form of *work* to create a new block. The success of finding Nonce is thus the *proof* of the work one node has done. To incentivize the nodes to participate in mining, network tokens and transaction fees will be rewarded to the miner which successfully publishes a block. The process of creating a new block is thus called *mining* and the node who participates in mining is called a *miner*.

PoS is another consensus algorithm, with the objective to reduce the intensive computation in the PoW algorithm. PoS is first used in Peercoin, in which the right to publish a new block is still granted by allowing nodes to compete to solve a mathematical problem as in PoW, i.e., to find a valid Nonce. However, the difference lies in the difficulty of solving the problem, which is inversely proportional to the tokens and the holding time of these tokens that a node has. In particular, with

more tokens and longer time of holding the tokens, the difficulty of mining for a node reduces. Further, the problem-solving process is eliminated in the latter PoS algorithms, and the block creator is elected based on the stakes the nodes hold [10]. With PoS, the computational resources one node occupies no longer determine the probability that it successfully finds a new block, and thus the computational resources required to reach a consensus can be largely reduced.

PBFT [11], is a practical voting-based algorithm that allows a consortium of nodes to reach consensus without the assumption of synchronization among them. With a Byzantine Fault Tolerance (BFT), nodes can still reach consensus even when there are some faulty nodes, i.e., byzantine nodes which can behave arbitrarily. There are two kinds of nodes in the PBFT algorithm, including a primary node and backup nodes. One node in the network, acting as a *client*, first issues transactions, as a *request* to the primary node, and the primary node decides the execution order of the request and then broadcasts it to all the other backup nodes. After receiving the request, the backup nodes check the authentication of the request, decide whether to execute the request and send replies to the clients. The consensus of the transaction is reached after the client receives $f+1$ (f is denoted as the number of byzantine nodes) replies from different backup nodes with the same results. PBFT algorithm guarantees the security and liveness, i.e., a request from a client will eventually be replied, when there are less than $\lfloor \frac{n-1}{3} \rfloor$ byzantine nodes, where n is denoted as the number of nodes which participate in the consensus process. PBFT eliminates the heavy computation as in PoW to elect a node to publish a new block. However, the benefit comes at the cost of requiring a high level of trust between the nodes to resist the *sybil attacks* [12] where a malicious party can create many nodes to bias the consensus toward itself. Thus, PBFT algorithm is usually used in consortium blockchain networks, e.g., Hyperledger Fabric.

Solution to Discrepancy: Since a blockchain is built upon a distributed network, it might take some time for all nodes in such a network to update a new block. Besides, there are multiple nodes mining at the same time. The latency of distributing a new block and the probability that another block is created during the latency make it possible that there exists more than one chains in the network at the same time. In this case, discrepancy about which chain is valid between the nodes arises. Specifically, nodes need to decide to believe one chain by working to extend it with a new block. The discrepancy is solved with the longest chain rule, i.e., the longest chain will be accepted with the other chains being discarded. A simple rationale behind this solution is that the longest chain is the chain that the majority of the nodes trust and work on extending. Over the long time scale, the solution guarantees that only one chain prevails.

Digital Signature: To verify the authentication and integrity of transactions, digital signatures based on asymmetric encryption are used in blockchain networks. Each node in a blockchain network has two keys, including a public key and a private key, and the content encrypted by the private key can only be decrypted by the private key. Before a node initiates/broadcasts a transaction, it first signs the transaction with its private key. Other nodes in the network can then verify the authenticity of the transaction using the public key. With the private key kept confidential to its

owner and the public key accessible by all nodes, the authenticity and the integrity of transactions can be easily verified. Thus, one cannot masquerade as others to initiate transactions or to forge the contents in the initiated transactions.

Types of Blockchain: Based on the rule to regulate which nodes can access, verify and validate the transactions initiated by other nodes, blockchains are typically categorized into public blockchains, private blockchains and consortium blockchains to satisfy the requirements in different applications.

1. *A Public Blockchain* is designed to be accessible and verifiable by all the nodes in the network. Specifically, all nodes in a public blockchain network can verify transactions, maintain a local replica of the blockchain, and publish a new block into the blockchain. By granting the authority of maintaining a ledger to all the nodes, public blockchains are fully distributed. Such a blockchain is widely used in anonymous trading. However, the system suffers from the low speed of transaction validation, and requires certain level of computation to secure that an unbiased block is created. Bitcoin [1] is one of the most popular cryptocurrency supported by a public blockchain.
2. *A Private Blockchain* is usually maintained by a single organization. The rights to access the blockchain and to verify the transactions are granted through a central controller to the permissioned nodes. A permissioned network is thus established, in which only the authorized nodes can access certain transactions of the blockchain or participate in working to publish new blocks. In this way, the privacy of the transactions is highly improved and the decentralization of authority of transaction validation is under the control of the organization. Moreover, with a high level of trust among the nodes in the permissioned network, the computation-intensive consensus algorithm is not needed.
3. *A Consortium Blockchain* is similar to a private blockchain in the sense that they are both maintained in a permissioned network. The difference is that in consortium blockchain, there involve multiple organizations to share the right to access and validate the transactions. Although these organizations might not fully trust each other, they can work together by altering the consensus algorithm based on the level of trust among them.

Work Flow of Blockchain: In Fig. 5.2, we show the work flow of a blockchain using the PoW consensus algorithm. Firstly, a transaction is initiated and broadcast to other nodes in the network. The nodes which receive the transaction use the digital signature to verify the authentication of the transaction. After verified, the transaction is appended to the list of valid transactions in the nodes. To record the verified transactions, nodes in the network work to publish the new block, i.e., find Nonce. Once one node finds a valid Nonce, it is allowed to publish a block which contains the initiated transaction. The other nodes then verify transactions in the block received by comparing the Merkle root, and once the transactions in the newly published block are proven to be authenticated and not tampered, the new block is added to the local replica of the blockchain. The update of the blockchain has been completed.

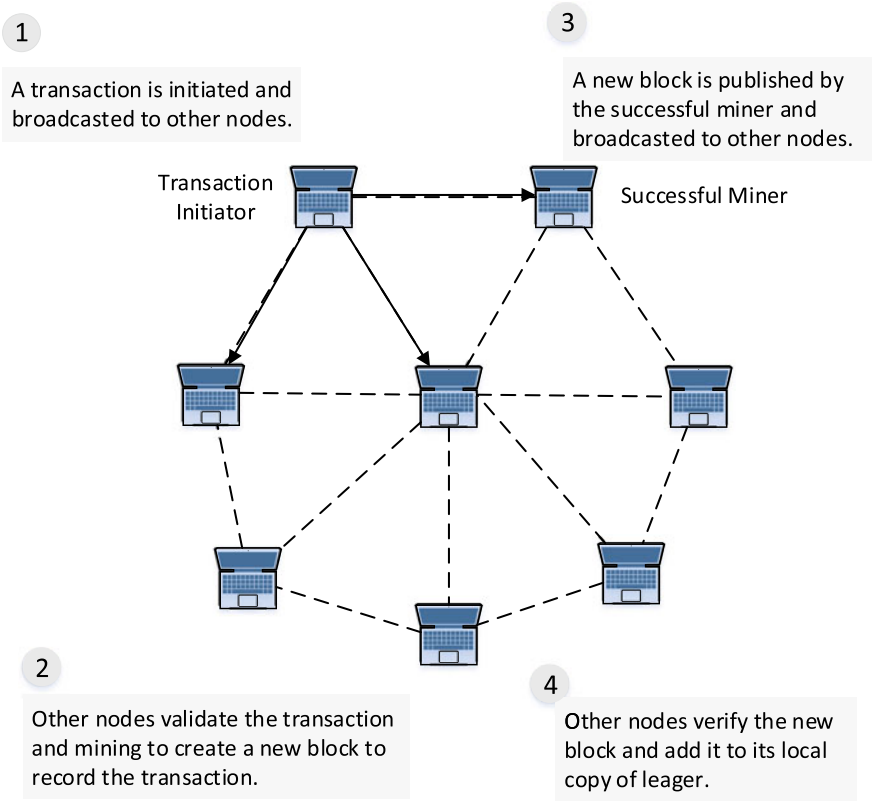

Fig. 5.2 The work flow of a blockchain network

5.2.2 Features and the Potential Attacks on Blockchain

The features of a public blockchain are summarized below.

- *Decentralization*: In a public blockchain network, the transactions are recorded by all the nodes in the network and each node has a local copy of the ledger in which transactions are recorded. In this way, the distributed ledger is protected against the single point of failures.
- *Trustless*: In a blockchain network, a trusted third party is not needed to validate the transactions, neither should one node need to trust others before they can transact. The consensus algorithm in the blockchain is used to validate and record the transactions in a more democratic manner than the centralized approach.
- *Immutability*: Using a one-way cryptographic hash function, any modification of the previous blocks in a blockchain invalidates all the consequently generated blocks. Thus, to tamper transactions recorded in a previous block, the malicious node needs to create a new block and replicate all the following blocks. With other

nodes continuing to create new blocks, the manipulation is hard to achieve, which makes the blockchain immutable.

- *Non-repudiation*: A transaction is cryptographically signed with a private key before broadcast to others. The authentication of transactions can be verified by others via the corresponding public key which is accessible to other nodes. Since the private key is kept by its owner, one node cannot masquerade others to initiate transactions and one verified transaction cannot be denied by its initiator.
- *Transparency*: In a public blockchain network, every node can access the transactions stored in the blockchain and verify the initiated transactions. Data stored in blockchain is thus transparent to the public.
- *Traceability*: The block header is attached with a timestamp which records the time when the block is created. Nodes can thus easily verify and trace the origin of the historical blocks.

Although relatively secure, the blockchain is still under the risk of multiple kinds of attacks, such as selfish mining attack, majority attack and Denial of Service (DOS) attack [13].

- *Selfish Mining* is applied by the malicious nodes to withhold the blocks they have successfully mined or to hold and then release the blocks. In this way, the nodes can make other miners waste their computational resources to find the Nonce which has been found by the attackers. On the other hand, by withholding a mined block, the attacker can start earlier than others to find the Nonce of the next block.
- *Majority Attack* might happen when one node or a coalition of nodes possesses more than 50% of the computational resources of all the nodes in the network. With the PoW consensus algorithm, such nodes have a probability larger than 0.5 to successfully mine and publish a new block. Thus, they can arbitrarily reverse or halt the transactions by publishing new blocks. The majority attack can also be performed by an attacker without such a high proportion of computational resources. Specifically, they can employ other nodes to help it privately extend a chain with a block published by itself. Once the private chain is longer than the existing one in the network, the attacker can make the new chain public. Based on the longest chain rule, the new chain will be accepted by other nodes in the network, and the transactions in the newly accepted blockchain, which might favor the attacker, will also be accepted.
- *Denial of Service Attack* happens when malicious nodes completely occupy the resources to verify or to transmit the blocks and transactions. Specifically, malicious nodes can initiate plenty of transactions to other nodes to disable the transmission and verification of transactions from other nodes.

5.2.3 Smart Contracts Enabled by Blockchain

Smart contracts, enabled by the blockchain technology, are self-executing contracts without extra enforcement. The contractual clauses between nodes are converted

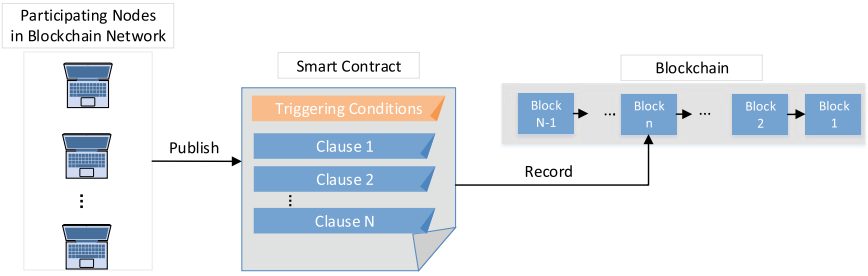

Fig. 5.3 The generation and recording of smart contracts

into computer programs in a form such as "If-Then" statements. The executable computer programs are then securely stored in the blockchain. When the predefined conditions in smart contract are satisfied, the clauses in smart contracts will be executed autonomously, and the execution will be recorded as an immutable transaction in the blockchain.

The generation procedures of a smart contract are shown in Fig. 5.3, and the work flow of the smart contracts is demonstrated as follows. The involved nodes first negotiate to agree upon and sign contractual clauses. The approved clauses are further recorded in a transaction. Similar as other transactions, such a transaction which records the smart contract will be verified by other nodes and then appended to other transactions in a block. With the consensus algorithm, a block contains the smart contract will be added into the blockchain. The smart contract will then be allocated with a unique address, through which the nodes in the network can access or interact with it. Once some node sends transactions to that address or the conditions in the smart contract are satisfied, the corresponding clause in the smart contract will be strictly executed.

Bitcoin is known as the first cryptocurrency that supports basic smart contract in the sense that the network allows one user to transfer value to another. However, the limited programmability makes it impossible to support a smart contract with complex logic. Ethereum is the first public blockchain-based platform which supports the advanced smart contracts which are encoded by high level programming implementation.

5.3 Blockchain for Spectrum Management: Basic Principles

In this section, we will first provide the potential aspects from which the application of the blockchain technology can benefit DSM. Note that we mainly consider the spectrum management in a sharing use. If not specifically mentioned, all blockchains in this section are public blockchains. Then, we outline three different ways to deploy

a blockchain network over a cognitive radio network. Finally, we will bring up and discuss challenges in the application of blockchain to DSM.

5.3.1 *Blockchain as a Secure Database for Spectrum Management*

Blockchain, as essentially an open and distributed database, can be used to record any kind of information as a form of transaction. On the other hand, spectrum management can benefit from the assistance of a database, such as a geo-location database for the protection of incumbent users in TV white spaces [14]. Based on this, one potential trend of applying blockchain to spectrum management is to record the information about spectrum management (Fig. 5.4).

One main reason of this application is that blockchain makes such information accessible to all the secondary users. Such kinds of information include the TV White Spaces, the spectrum auction results, the spectrum access history and the spectrum sensing results. Here, we discuss the benefits of recording these kinds of information on spectrum management.

Information of TV White Spaces and other underutilized spectrum bands can be dynamically recorded in a blockchain. In a secure blockchain, the information including interference protection requirements of the primary users and the spectrum usage with respect to time, frequency and geo-location of TV white spaces can be recorded. Compared to a traditional third party database, blockchain allows users directly control the data in the blockchain and thus guarantees the accuracy of data. Another concern of spectrum management is its dynamic characteristic. With the mobility of mobile secondary users or the variation of traffic demands of the primary users, the availability of spectrum bands might change dynamically. With the decentralization of blockchain, the information of idle spectrum bands can be dynamically recorded by primary users and easily accessed by all the unlicensed users. Moreover, by initiating a transaction, SUs can inform others their departure or arrival to some area, to help others to capture the potential spectrum opportunities in the area where they are located, to finally optimize their transmission strategies. Thus, the efficiency of spectrum utilization can be improved.

Spectrum Access History of the unlicensed spectrum bands can be recorded in a blockchain. With the existing access protocol such as Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA) and Listen-Before-Talk (LBT), the access is not needed to be coordinated. However, the access history needs to be recorded in the blockchain to achieve the fairness in all the users. For example, with the autonomous implementation of smart contracts, the users which are recorded to access the unlicensed spectrum bands up to a frequency threshold will be not allowed to access the same spectrum bands in a fixed period.

Spectrum Auction Results can also be recorded in a blockchain. Auction mechanisms have been shown as an efficient way for dynamic spectrum allocation [15]. Among the spectrum auctions, the *secondary auctions* are used when the licensed primary user (PU) shares the spectrum with secondary users (SUs). The sealed-bid spectrum auctions, where the SUs as bidders send their bids to the PU who is auctioneer privately, can improve the efficiency of spectrum auction. Moreover, the second-price sealed-bid auction, can guarantee the *truthfulness* of spectrum auctions, which means that SUs will obtain optimal utilities by submitting the bid with respect to their true valuation of the spectrum bands, instead of deceiving the auctioneer. Although sealing the spectrum auction results can be beneficial from the above aspects, recording the auction results such as the bids and the *hammer price*, at which the SUs and the PU make a deal, after the auction is completed, is also important. Blockchain provides an secure and verifiable way to record such information. Specifically, recording of spectrum auction results in a blockchain can be beneficial from the following aspects.

1. *Prevent the frauds from a PU*. The lack of transparency of bids and the hammer price can lead to the occurrence of frauds. For example, it is possible that one dishonest PU charges the winning SU with a forged price or grants more than one SUs the exclusive access right of spectrum bands, to increase its revenues. However, this kind of frauds cannot be detected by the SUs since the bids are sealed. With the use of blockchain, the bids and hammer price can be immutably recorded as a transaction after the auction is ended and the information can be verified and accessible by all the SUs. It is thus easy to detect and prevent the frauds of a PU.
2. *Guarantee the non-repudiation of auction payment*. Since that the transaction which records the bids and hammer prices is verified by all SUs before being recorded in a blockchain, the wining SU cannot repudiate the bid they submit. Thus, the PU as the spectrum resource provider, can be secured to obtain its rightful payment after the auction is completed.
3. *Prevent the unauthorized access of SUs*. Recorded in a blockchain, the results of spectrum auctions are accessible to all the SUs. To ensure the fairness of spectrum auctions, all SUs can collaboratively supervise and prevent the unauthorized access. In this way, no SU can access the spectrum without participating in and wining the spectrum auctions.

Spectrum Sensing Results are another kind of information which can be stored in a blockchain. The sensing results stored in the blockchain can be used to map the spectrum usage of the primary networks and hence provide them an additional tool for monitoring and maintaining of their networks. Moreover, this could potentially encourage more licensed users to allow shared use of spectrum. Without the help of secondary users to submit the sensing reports, however, a cellular network operator can achieve the above objective by deploying a sensor network to monitor and record the spectrum usage in a blockchain. On the other hand, the sensing results recorded in the blockchain can be used as prior information when SUs need to choose which licensed spectrum bands to sense and access. In particular, SUs can estimate the

utilization rate of different spectrum bands from the historical sensing results, and SUs can thus choose the spectrum bands with a relatively low utilization rate.

5.3.2 Self-organized Spectrum Market Supported by Blockchain

With the tamper-proof record of transactions, the autonomous contract execution and payment settlement enabled by smart contracts, blockchain is a powerful platform to construct a self-organized spectrum market, to provide the following applications.

Services Implementation: A smart contract, which is a self-executing contract built upon a blockchain, can be used in spectrum management, with the clauses in the smart contract being autonomously executed and immutably recorded. Moreover, the payment process can also be autonomously completed by smart contracts. Thus, with the usage of smart contracts, services such as spectrum sensing service [9], the trading of transmission capabilities can be explored to be securely executed between the users in the blockchain network.

Identity Management: Besides executing the services with smart contracts, blockchain can also provide an identity management mechanism in the spectrum market. Specifically, a consortium blockchain as an intermediary first collects and records the information from the service seekers, such as SUs, to complete the registration process. The blockchain can then be used to authenticate the registered users and to only allow the registered users to access the data recorded in it. To protect the privacy of the users, the blockchain only provides the pseudonymous identity of the users when the service providers seek for the user identity authentication. Such a configuration is first proposed in [16], where an Identity and Credibility Service (ICS) is built upon a consortium blockchain.

5.3.3 Deployment of Blockchain over Cognitive Radio Networks

Blockchain, as a distributed ledger, is maintained by all the nodes in the network. However, it can be energy-consuming for a node to maintain the blockchain. For example, in the blockchain using the PoW consensus algorithm, the nodes need to devote computational resources to publish a new block. Thus, the deployment of blockchain network with the communication network should be studied. Here, we outline three ways to deploy the blockchain network to the cognitive radio network and analyze the pros and cons of these ways.

The first way is to directly deploy a blockchain network over a communication network, as shown in Fig. 5.5. Specifically, since the information regarding the spectrum management, which needs to be recorded in the blockchain, is produced or

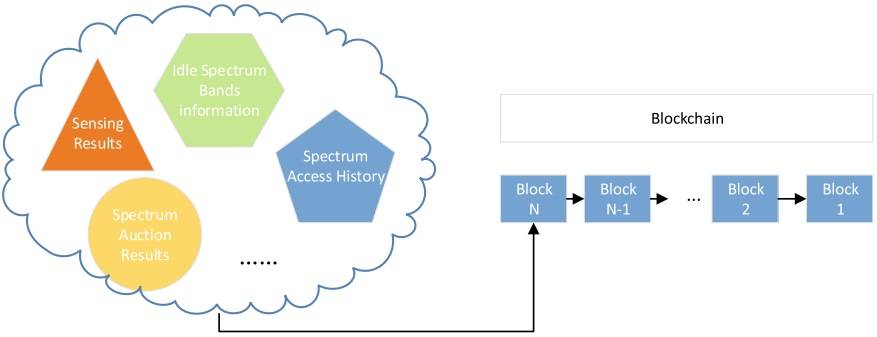

Fig. 5.4 Blockchain as a secure database for spectrum management. The information such as spectrum sensing results, spectrum auction results, spectrum access history and the idle spectrum bands information can be securely recorded in blockchain

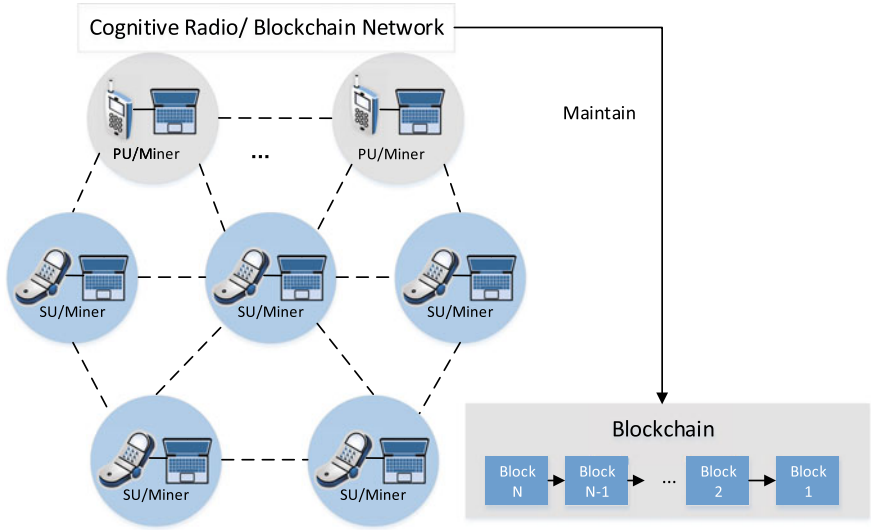

Fig. 5.5 Deploy the blockchain network directly on a cognitive radio network

obtained by the nodes in the communication network, i.e., SUs and PUs, it is intuitive for the nodes in the cognitive radio network to also act as nodes in the blockchain network. To deploy the blockchain in this way, the SUs and PUs should be equipped with the mining and other functions in the blockchain. Thus, all the functions of the blockchain, such as the distributed verification of transactions, can be performed by all the users. However, such kind of deployment requires a control channel through which the users can transmit the transactions and blocks. If a wireless control channel is used, there exists the risk that the control channel is jammed by the malicious users. Once the control channel is paralyzed, the blockchain network cannot function.

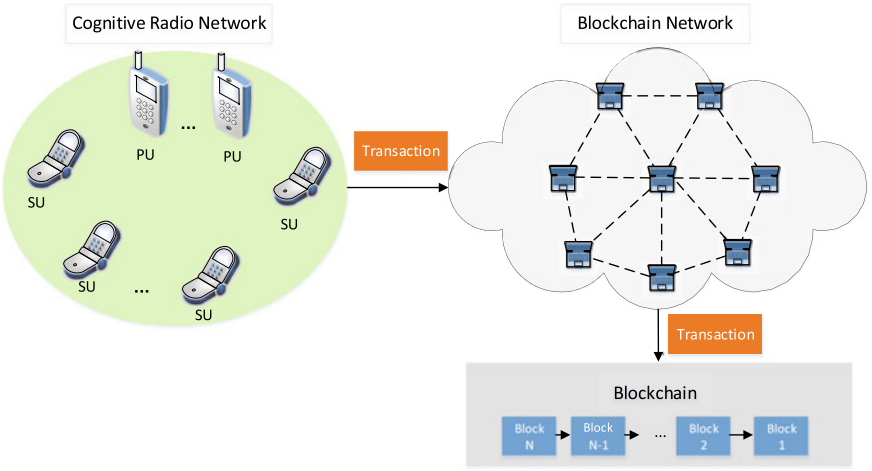

Fig. 5.6 The coexistence of a dedicated blockchain network and a cognitive radio network

Another way is to use a *dedicated blockchain network* to help record the relevant information. For users in the cognitive radio network, the limited computational capabilities make it difficult for them to access the spectrum bands and maintain the blockchain at the same time. Specifically, mining, which might consume a lot of energy, is impractical for SUs with constrained battery to implement. To overcome this challenge, one possible way is to allow users to offload the task of recording transactions to a dedicated blockchain network, as shown in Fig. 5.6. In this way, the blockchain functions as an independent database. However, the transaction cannot be verified directly by users and the overhead of transmitting the transactions to the dedicated blockchain network also increases. Moreover, the nodes lose the control over information recorded in the blockchain. To this end, a more practical way for the users is to only offload the mining task, which is energy-consuming, to a cloud/edge computing service provider, and to record the transaction into the blockchain by themselves. Researchers have designed auction mechanisms to allocate computing resources in this case [17]. However, the offloading of mining task might lead to a malicious competitions between the users, which also needs to be considered when a blockchain network is deployed in this way.

Besides the cognitive radio network and the blockchain network, there sometimes exists a third network, e.g., a sensor network, where sensors can be deployed to perform cooperative spectrum sensing to obtain the diversity gain. Under the same principle of dedicated blockchain, the above three networks can coexist and interact with others. Traditionally, the third network such as the sensor network directly communicates with the cognitive radio network. Blockchain network, however, can become an intermediate of the two networks.

5.3.4 Challenges of Applying Blockchain to Spectrum Management

The application to blockchain in spectrum management is promising. However, there remain a few challenges with respect to, for example, transaction cost, the latency and the privacy leakage. Generally, the challenges can be solved by trading off different characteristics of a blockchain, which is shown in Fig. 5.7. As it can be seen, the decentralization of blockchain is helpful to guarantee the non-repudiation, transparency and immutability, while decreasing the privacy and the scalability, and increasing the latency and transaction cost in the blockchain network. We introduce the challenges and discuss their potential solutions as follows.

Transaction Cost: The transaction cost for a node in a blockchain network includes the cost to publish a new block and the communication overhead to transmit the transactions initiated by all the nodes. The consensus algorithm, through which a new block is published, such as PoW, is too computationally intensive to be sustainable for cognitive devices with limited computational resources and battery. Although users can upload the mining task to a cloud/edge computing provider to save their energy, it still costs them to pay for the computing service. Another solution is to adopt or design a more suitable consensus algorithm to lower the cost of maintaining the blockchain. However, an energy-efficient consensus algorithm usually required

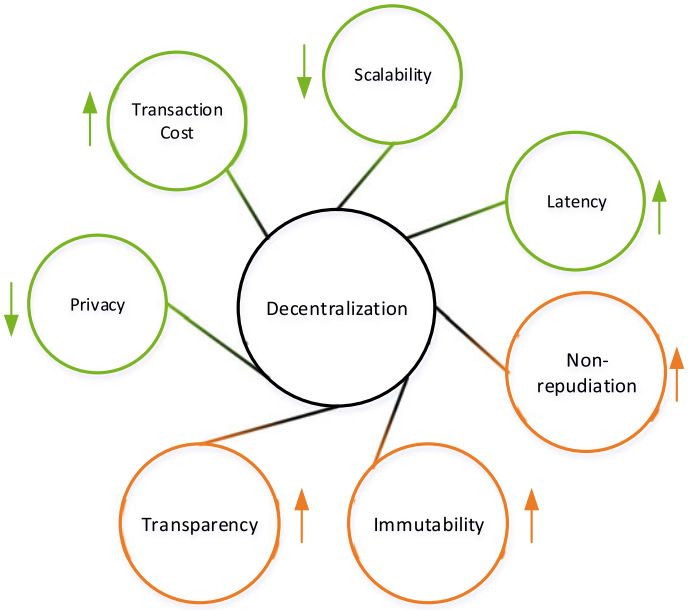

Fig. 5.7 The tradeoffs in different characteristics in a blockchain network

a higher level of trust between nodes in the network to guarantee the security, which limits the flexibility of the blockchain network.

Another cost in maintaining a blockchain is caused by the transmission of transactions. A transaction, initiated by one node in a blockchain network, needs to be broadcast and verified by other nodes before it can be recorded in a new block. After that, the new block is also needed to be broadcast to other nodes for verification and storage. In the case when the generation of transactions is frequent, the overhead of transaction transmission cannot be neglected. On the other hand, the transmission of transactions usually requires a control channel, which is under the risk of being jammed by the malicious nodes. The risk also increases the cost of transaction transmission. To conclude, tradeoff of the cost and the benefits should be considered when applying the blockchain to spectrum management.

Latency and Synchronization: The latency in a blockchain network is caused by two phases including the mining process, and updating local blockchain of all the users. Firstly, the mining process, e.g., PoW consensus algorithm, is energy-consuming and time-consuming to guarantee unbiased selection of nodes to publish a new block. Moreover, after a block is published, it still requires some time for the successful miner to broadcast the new block and all other nodes to verify and add the new block to their local replicas of the blockchain. The high latency in the blockchain network might make it unsuitable to the applications with stringent latency requirements. For example, the latency of writing the results of an spectrum auction in the blockchain can delay the execution of spectrum access. This will impair the revenues for the secondary users and increase the latency for transmission. On the other hand, the latency can also lead the fork of a blockchain, i.e., the existence of multiple blockchains in a network. In the fork of a blockchain, multiple auction results such as the recorded winner and its allocated spectrum bands might be different from that of the original blockchain. This will lead to the discrepancy in the spectrum access allocation among the users and even result in interferences between the users when they simultaneously access the same spectrum bands. Although this discrepancy could eventually be solved by the longest chain rule, the effect on secondary users can not be reversible. To conclude, the delayed spectrum access caused by the latency of the blockchain impairs its revenue and further discourages the users from participating in the spectrum auctions.

Privacy Leakage: A blockchain guarantees its security by distributing the authority of maintaining the database to all the nodes in the network. As a result, any node can access and verify the data stored in the blockchain. In DSM, the data can be some private information collected by users, which might leak their location or other features. However, the easy and open access to the public blockchain might prevent users from recording any private information in it. Although a private blockchain, in which the access to blockchain is distributed only to permissioned nodes, can be employed to improve the privacy of data recorded in blockchain, this will reduce the decentralization of blockchain and increase the administration cost to supervise the nodes in the blockchain network.

Scalability: A newly published block needs to be broadcast to all the other nodes and stored in the local replica of all nodes. Thus, the number of transactions in a block

is limited since containing too many transactions might make it be *orphaned*, which occurs when it can not be included to the local blockchain replica of all the nodes on time. On the other hand, in public blockchains, there is usually a pre-defined *block interval*, which can be adjusted by setting the difficulty of block creation. Reducing the block interval can increase the transaction throughput. However, it also increases the risk of creating blockchain forks and thus reduces the security. Thus, the scalability of blockchain, defined as the transaction throughput per second, is limited. To solve this, a more efficient consensus algorithm can be adopted to decrease the block interval, or a private/consortium blockchain can be used instead of a public blockchain, to decrease the number of nodes which need to store a local blockchain copy, and to increase the speed of propagation of a new block to all the nodes.

Attacks on Blockchain: The major kinds of attacks on a blockchain are introduced in Sect. 5.2. These attacks can degrade the security or increase the latency of the blockchain, to further affect the dynamic spectrum management which uses the blockchain. Take the selfish mining attacks as an example. In an application which uses a blockchain to record the spectrum auction results, the selfish mining attacks will delay the time for a transaction, i.e., spectrum auction results, to be successfully recorded in the blockchain. Thus, the allocation of spectrum bands cannot be executed on time. The denial of services (DoS) attacks can also be implemented by jamming the control channel, through which the transactions are transmitted.

5.4 Blockchain for Spectrum Management: Examples

In this section, we give some examples to show how the blockchain technologies can be applied to DSM. Firstly, using the consensus algorithm, researchers have enhanced the performance of traditional spectrum access or developed new spectrum access protocol. Besides, the spectrum auctions secured by a blockchain will also be introduced. Moreover, we introduce a novel cooperative-sensing-based spectrum access protocol, which is also enabled by the blockchain technologies.

5.4.1 Consensus-Based Dynamic Spectrum Access

A consensus algorithm adopted in the competition of mining in blockchain, such as the PoW algorithm, is used to select one node to create a new block in an unbiased and distributive manner. They can be also used to manage the spectrum access where the coordination of the access requests from SUs is needed to avoid collision. Furthermore, with the use of Distributed Ledger Technology (DLT), the queue derived using a consensus algorithm can be distributively recorded. Overall, using the consensus algorithm, we can either enhance the performance of traditional access

protocols or propose new access protocols. Here, we introduce two instances of the consensus-based dynamic spectrum access (DSA).

It is noted that in traditional spectrum auctions, the computational complexity to derive the optimal bid might be high for cognitive devices limited computational capabilities, and the time to derive the optimal bid might occupy the time for transmission. In [18], authors proposed a puzzle-based auction to improve the efficiency of spectrum auctions. The essence of the puzzle-based auction mechanism is to make SUs win the spectrum auction by competing to solve a complex math problem, rather than through traditional bidding. Specifically, in a puzzle-based auction, an auctioneer advertises an access opportunity, and SUs who are interested then respond to the auctioneer to obtain a math problem and will be charged with an entry fee. The involved SUs then start working on solving the math problem. The first SU who submits the correct answer of the problem to the auctioneer will be granted to access the advertised spectrum band. To guarantee the fairness of the auction, the math problem is set to be non-parallelizable, e.g., to find the n-th digit of π, meaning that the problem cannot be computed in a parallel manner. By doing so, the SUs cannot devote more parallel computational resources to obtain a greater chance to win the auction, which ensures the fairness and prevents the malicious competition of the spectrum auction. Since the competition of winning one puzzle-based auction is similar to the mining process, the auction can be seen as a centralized consensus algorithm, where the verification of the winner of the auction is performed only by the PU.

In [19], with the use of the DLT, the authors proposed a distributed DSA protocol, so called *consensus-before-talk* in which the access requests of the SUs are stored as transactions and queued with a consensus which is distributively achieved between all the nodes by a pre-defined rule. The system is shown in Fig. 5.8. In such a system, the collision of SUs is avoided by distributively queuing the access requests from different users and the latency of transmission for SUs can thus be reduced. Specifically, an SU first generates an access request as a form of transaction and uses the gossip-of-gossip protocol to spread the transaction. The SU who receives the transaction then verifies the authentication of the request through digital signature and adds its verification time to the transaction, and finally sends the modified transaction to another SU. After all the SUs have verified the transaction, the SUs spread the transaction again. Lastly, each SU has a copy of the transaction with the verification/generation time from all SUs and each SU can calculate the consensus time using the verification and generation time of the transaction. After that, the transactions are added to their local ledger in a order decided by the calculated consensus time. Through these procedures, a consensus, which regulates the queue of spectrum access, is distributively reached among all the SUs.

5.4.2 Secure Spectrum Auctions with Blockchain

Auction mechanisms have been proven to be an efficient way for dynamic spectrum management. However, the security of the spectrum auctions is mainly guaranteed

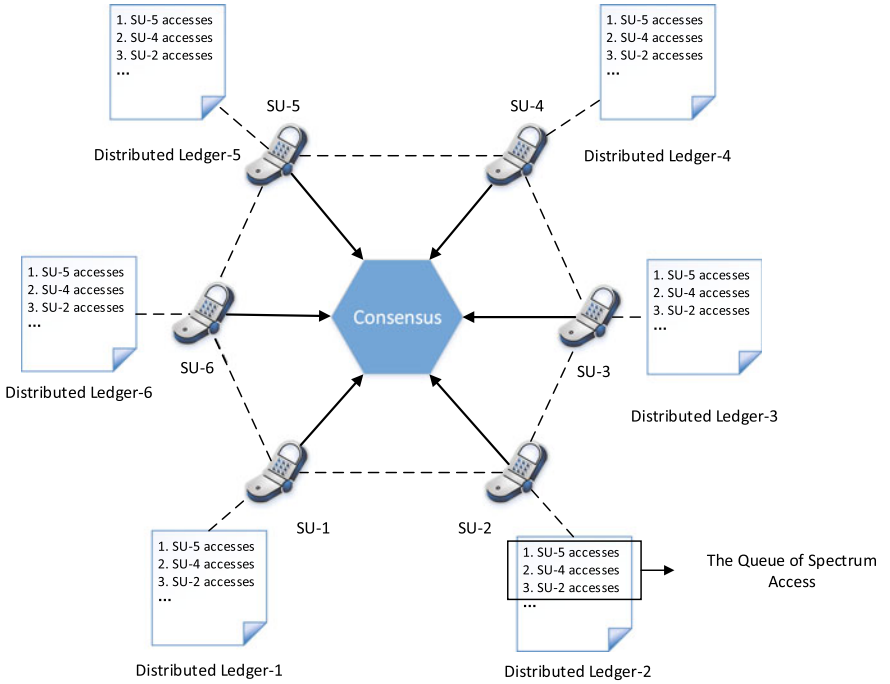

Fig. 5.8 A consensus-based dynamic spectrum access framework

by third-party entities [15]. On the other hand, there usually lacks validation of the transactions in a traditional spectrum auction. Although some centralized validation mechanisms, which are executed by a centralized authority, are proposed, such mechanisms are vulnerable to single point of failures [7]. A distributed validation mechanism, which is accessible to and verifiable by all the users in the network, is thus desired. Blockchain, as a distributed ledger, can be used to overcome the security challenges in the spectrum auctions.

In [7], authors proposed a blockchain-enabled DSA scheme based on the puzzle-based auction. In such a DSA system, SUs are seen as both sensing nodes in the cognitive radio network and mining nodes in the blockchain network. A PU leases its idle spectrum to the SUs through a blockchain without an auctioneer. Leveraging on the blockchain, the spectrum transactions are recorded and verified in immutable and distributed manner by the SUs. The procedures of the spectrum auction system in [7] are introduced below. Firstly, the advertisement of spectrum opportunity is broadcast by an PU through a control channel, and a puzzle-based auction is used to determine the winner of the auction. If the the winner has sufficient tokens to sustain the pre-defined spectrum payment, then the access is granted. Otherwise, the auction is restarted, and the malicious bidder, i.e., the SU who takes part in the auction but has an insufficient budget, will be deprived of the bidding right. After the auction is completed, a new transaction recording the auction result needs to be

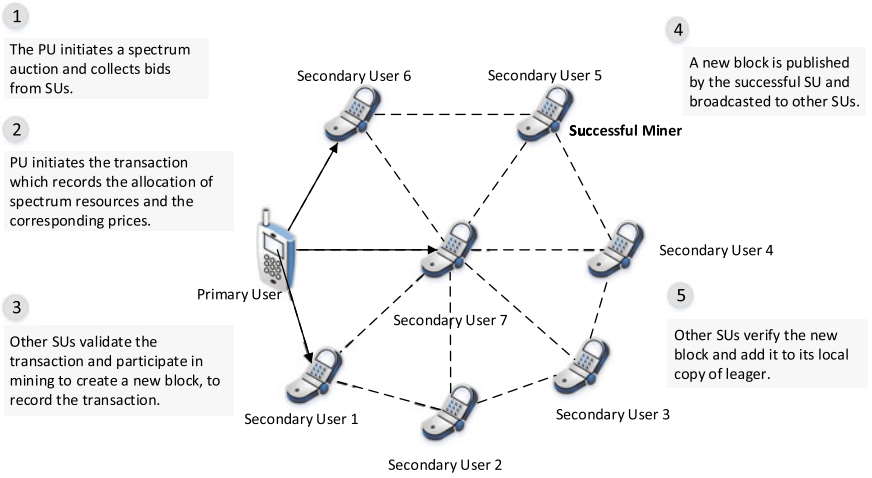

Fig. 5.9 Procedures in a blockchain-secured spectrum auction

recorded in the blockchain. SUs then work to create a new block via mining. The SU which successfully publishes a block will be rewarded with the tokens, named as *specoins*, in the network. With the PoW consensus mechanism, the difficulty of creating a new block increases as the blockchain grows longer. To prevent the creation of a new block from being impossible for SUs which are equipped with limited computational capabilities, the blockchain will be reset at a fixed frequency. The reset can be achieved by creating the first block of a new blockchain, in which the balances of SUs and the PU are recorded.

Although [7] uses the puzzle-based auction to reduce the complexity and thus to improve the efficiency of spectrum auctions, it is straightforward to extend this system to adapt to other auction mechanisms since a blockchain is only used to verify and record the result of a spectrum auction. A more general blockchain-secured spectrum auction system is depicted in Fig. 5.9, where we omit the detailed procedures of spectrum auction.

Enabled by the blockchain technologies, the security of spectrum auctions using a blockchain has been improved with the following features.

- *Decentralization*: The spectrum transactions are verified and recorded in a distributed and immutable manner. Compared to the centralized auction system, where the transaction is verified and stored by a trusted third-party, the blockchain-enabled auction system is robust against the single point of failures.
- *Accessibility*: With a mechanism to help exchange the real currency with the cryptocurrency, and using the public blockchain which is accessible to any node in the public, any interested SU can participate in the spectrum auction. Moreover, the registration procedures of users and the reliance on the trust between the user and the auctioneer are eliminated. In this way, the spectrum resource is more accessible by all the users.

- *Verification of User Identity*: With the use of the digital signature in each transaction, the authentication of SUs and PUs can be verified by all the users. Thus, malicious user cannot impersonate another SU to submit bid in the spectrum auctions or impersonate the PU to initiate an auction. The account of users can thus be secured.
- *Fraud Prevention*: The transparency of transactions prevents the frauds of a PU, e.g., overcharging the winning SU with a forged price.

5.4.3 Secure Spectrum Sensing Service with Smart Contracts

In [9], the authors use smart contracts to autonomously execute the spectrum sensing service. It is known that without the cooperation of PUs, the access opportunity can only be obtained by spectrum sensing. However, due to the adverse channel fading effect, the sensing result of a single SU might be incorrect. Cooperative sensing by multiple SUs can be used to improve the sensing performance. However, when an SU does not need to access the spectrum, there lacks incentive for it to participate in the cooperative sensing, which is energy-consuming. To this end, in [9], authors proposed to improve the sensing performance by deploying multiple sensing nodes, so called *helpers* to provide the SUs with the sensing service and to use the smart contract to implement the spectrum sensing service. In this way, an SU can offload its sensing task to the sensing helpers, and the sensing helpers can obtain revenues by charging the SUs. Specifically, the SU firstly broadcasts the smart contract, in which a sensing quality requirement is recorded, to the sensing helpers. Then, the sensing helper checks if it satisfies the requirement and then decides whether to provide the sensing service. After that, smart contract selects the helpers and collects the sensing reports from them. Moreover, the algorithms to detect and remove the malicious sensing helpers, which reports a false or random sensing report, can be also executed autonomously by smart contract. The last procedure in the smart contract is to autonomously pay the service provider. From the above execution process, it is noted that with the use of smart contract, the sensing service can be implemented and supervised in an autonomous and immutable way, and with the use of a permissionless blockchain, an elaborate registration of sensing helpers is eliminated.

5.4.4 Blockchain-Enabled Cooperative Dynamic Spectrum Access

Cooperative sensing is used to improve the accuracy of spectrum sensing, which gives the SUs a better chance for opportunistic access. To achieve cooperative sensing, a centralized approach is to deploy a fusion centre to collect and fuse the sensing reports from SUs. Moreover, the fusion centre can analyze the collected sensing

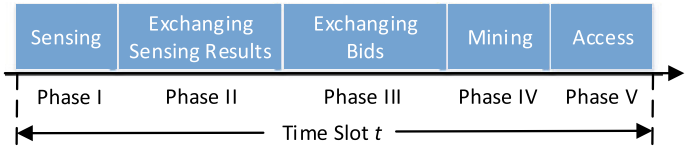

Fig. 5.10 The sequence of operations in a time slot

reports to detect the malicious SUs which report false or random reports for maximizing its own benefits. Although easy to be implemented, this centralized scheme is vulnerable to single point of failures. In particular, the cooperative sensing scheme will break down when the fusion centre is hacked. In this case, the whole secondary network is no longer secure. Moreover, there exits a potential type of attacks in which an attacker emulates an SU to report false sensing results to the fusion centre. Thus, the authentication of SUs should verified [20]. A decentralized and secure cooperative sensing scheme to address the above concerns is thus desired. Furthermore, cooperative sensing also needs an incentive mechanism to encourage the SUs to spend the additional energy for cooperative sensing.

Here, we propose a decentralized cooperative sensing scheme, where the sensing reports of SUs are spread collaboratively by all the SUs, and once an SU collects all the sensing reports, it derives the final result by its local fusion rule. Moreover, the sensing results are securely recorded as a transaction in the blockchain. To achieve this, one SU acts as both a sensing node and a mining node. However, the energy consumed by sensing and mining might prevent SUs from collaboration. To this end, we propose an effective incentive mechanism which guarantees that the efforts of SUs paid to cooperatively sensing and mining are proportional to their chances to access one cooperatively sensed the idle spectrum band. Specifically, the SUs which participate in cooperative sensing and win the mining will be rewarded with tokens in a virtual currency and the SUs can bid for the access opportunity using the tokens they earn. Note that the virtual currency will be supported and secured by the blockchain. In this sense, by fairly allocating the cooperatively obtained access opportunity, SUs are effectively incentivized to participate in cooperative spectrum sensing and mining, and a DSA framework is thus established.

The proposed DSA framework includes a protocol that specifies a time-slotted five-phase operation by the SUs to obtain an access to the spectrum, as shown in Fig. 5.10. Specifically, the SUs first choose whether to sense the primary channel according to its sensing policy (*Phase I*). Then, SUs exchange their sensing results through a control channel (*Phase II*). If the fused sensing result shows that the spectrum is idle, SUs decide the bid for the access according its bidding policy and exchange their bids (*Phase III*). Then, SUs decide whether to work on mining according to its mining policy, and the successful miner will create and broadcast a new block that records the sensing results, bids of SUs and the wining bidder (*Phase IV*). Finally, the winning SU accesses the spectrum to transmit its packets (*Phase V*).

The benefits of the proposed cooperative-spectrum-sensing-based DSA framework are as follows:

- By allocating the spectrum band through auctions, it prevents the collision of SUs which sense and access the same spectrum band.
- With the help of hashing and digital signature in the blockchain technology to distributively verify the authentication of SUs, the proposed DSA framework thwarts the SU emulation attack in the cooperative sensing.
- The decentralized cooperative sensing scheme in the DSA framework is free from single point of failures by eliminating the need of a fusion centre.
- The virtual currency, secured by the blockchain, provides an effective mechanism to incentivize SUs to cooperative sensing and mining.
- The use of blockchain helps to securely record the historical sensing, bidding, and access results.
- The recorded historical sensing results in the blockchain can be used by SUs to predict the spectrum usage or to detect the dishonest/malicious SUs which send random/false reports. Moreover, they can be used for PUs to monitor and maintain the usage of its licensed spectrum bands.

According to the DSA framework, three policies are important for the SUs to finally obtain the spectrum access opportunity. For each SU, to maximize its token revenues, it needs to sense and mine in all the time slots. However, it might be a waste of energy for all SUs to always sense and mine. In this sense, we propose a set of heuristic policies for SUs to distributively make the sensing, bidding and mining decisions.

1. *Sensing Policy* $a_i(t)$: By a sensing policy, denoted as $a_i(t)$, SU i determines whether it should sense the primary channel, with $a_i(t) = 1$ and $a_i(t) = 0$ representing sensing and not sensing, respectively. We consider a probabilistic sensing policy by which each SU decides whether to sense in t-th time slot with a fixed probability P_s, i.e.,
$$a_i(t) = \begin{cases} 1, \text{ with probability } P_s, \\ 0, \text{ with probability } 1 - P_s. \end{cases} \tag{5.1}$$

2. *Bidding Policy* $b_i(t)$: By a bidding policy, denoted as $b_i(t)$, SU i determines how many tokens that it should use to bid for the spectrum access. Denote $n_i(t)$ as the balance of SU i's wallet. Then the bid that an SU can place is limited by the maximum number of tokens that it has, i.e., $b_i(t) \leq n_i(t)$. We consider a bidding policy that is based on its current buffer occupancy ratio and its currently available token values. Mathematically, the bid of SU i in t-th time slot is determined to be
$$b_i(t) = \frac{q_i(t)}{Q_i} n_i(t), \tag{5.2}$$
where $q_i(t)$, Q_i denote the number of packets in the buffer and the buffer size of SU i, respectively. Under this bidding policy, an SU dynamically adapts its bid to its current buffer state, which represents its urgency to access. Thus, when its

buffer occupancy ratio is high, it is allowed to submit a high bid to obtain a better chance to access.

3. *Mining Policy* $c_i(t)$: By a mining policy, denoted as $c_i(t)$, SU i determines whether it should work on mining to update the blockchain, with $c_i(t) = 1$ and $c_i(t) = 0$ representing mining and not mining, respectively. Similarly with the sensing policy, we consider a probabilistic mining policy according to which each SU randomly decides whether to participates in mining in the t-th time slot with a fixed probability P_m, i.e.,

$$c_i(t) = \begin{cases} 1, \text{ with probability } P_m, \\ 0, \text{ with probability } 1 - P_m. \end{cases} \tag{5.3}$$

5.5 Future Directions

The application of the blockchain technologies to dynamic spectrum access is still at its infancy. As mentioned in the preceding sections, there still exist many challenges to be addressed. In this section, we will give some future directions of work so the benefits of the blockchain technology can be better harvested to support more efficient dynamic spectrum access in the future.

- *Incentive Mechanisms Using Blockchain*: Blockchain has successfully supported many kinds of cryptocurrency. With cryptocurrency, it is convenient to design incentive mechanism for users to contribute to the spectrum management. For example, tokens in the cryptocurreny can be rewarded to the users which participates in the spectrum sensing, to help explore the access opportunity or monitor the spectrum utilization efficiency of licensed bands. The tokens can also be used to obtain the access opportunity or to get other services provided by other users.
- *Design of Consensus Algorithms*: Besides the properties including correctness, consistency, termination and total order [21], which a consensus algorithm needs to satisfy, the latency and computational cost of the consensus algorithm should also be considered when applying blockchain to dynamic spectrum management. Generally, a computationally efficient consensus algorithm is needed to reduce the computation consumption of users with the limited battery. On the other hand, the PoW consensus algorithm, with which the nodes reach the consensus by devoting computational resources to solve a puzzle, costs the nodes in the network to perform *useless* computation, i.e., finding a random number by trial and error. To this end, proof of useful work [22] can be employed to let the users solve a practical puzzle to increase the usefulness of computation to reach the consensus.
- *Flexibility of Blockchain Networks*: With the communication overhead of transaction transmission determined by the distance of the users, it is needed for the users in the blockchain network to stay in a relative small area. On the other hand, same spectrum bands can be allocated to users in different areas since the interference of them reduces with the increase of their distance. To control the transaction cost

and improve the utilization of spectrum resources, it is thus practical to design different blockchain networks to manage the spectrum resources in different areas. However, it is not suitable to use private blockchain network which needs to verify the identity of nodes in the network and assign the permission to the trusted nodes. This is because the mobile users can frequently change its locations and need to be permissioned once they get into a new private blockchain network. Thus, how to adopt or design an efficient blockchain to guarantee the flexibility should be considered in the future researches.

- *Allocation of Energy and Maximization of Revenue*: With the consensus algorithm such as PoW, the creation of block can be computationally intensive. It is thus crucial for users to allocate their limited computational resources/energy between mining and data transmission. The former helps the users to obtain the revenue from token rewards and transaction fees, while the latter helps to obtain the revenue by providing the transmission service. With limited energy, there exits a tradeoff between the revenue from the blockchain and the revenue from data transmission service provisioning. Specifically, if one node spends more energy on mining, it is more probable for them to mine a new block and obtain the token reward. However, the power for transmission is reduced which degrades the performance of transmission. Although the mining task can be offloaded to an edge computing service provider, the balance should be considered between the cost on the computing service and the revenue from the transmission service. An interesting trade-off on the achievable throughput arises when the tokens rewarded by mining can be used for purchasing the spectrum access license. That is, if a user spends more energy in mining, although its probability to obtain the spectrum access opportunity increases, the transmission performance such as achievable throughput will be degraded as the energy left for transmission will be less.
- *Frequency of Blockchain-based Spectrum Auctions*: One application of blockchain to dynamic spectrum management is in the spectrum auction, which is designed to dynamically allocate the spectrum resources to improve the spectrum utilization efficiency. Besides the merits such as security, transparency and accessibility, using the blockchain to hold and record the spectrum auction can reduce the administration cost on it. However, the cost of blockchain to validate the transactions cannot be ignored. Although increasing the frequency of spectrum auctions can achieve better utilization of the spectrum resources, the cost of recording the increasing number of transactions also increases. Under some circumstances, the increase of frequency to hold the spectrum auctions can even affect the execution of spectrum auction results. Specifically, if the frequency of spectrum auctions is so high that there is not enough time for all the users to validate and record the transactions, the results of auctions cannot be executed on time. To conclude, the frequency of blockchain-based spectrum auction should be optimized to tradeoff between the spectrum utilization efficiency and the cost of recording transactions in the blockchain.

5.6 Summary

In this chapter, we have investigated the applications of blockchain to dynamic spectrum management. We have first briefly introduced blockchain technologies. We have then given the basic principles which illustrate how and why it is helpful to apply blockchain technologies to dynamic spectrum management, with challenges summarized at last. Moreover, we have introduced some instances of blockchain for dynamic spectrum management. Finally, we have discussed the future directions.

References

1. S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008)
2. M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the internet of things: a comprehensive survey. IEEE Commun. Surv. Tutor. **21**2, 1676–1717 (2018)
3. M. Liu, F.R. Yu, Y. Teng, V.C. Leung, M. Song, Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing. IEEE Trans. Wirel. Commun. **18**(1), 695–708 (2018)
4. Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, Y. Zhang, Blockchain and deep reinforcement learning empowered intelligent 5G beyond. IEEE Netw. **33**(3), 10–17 (2019)
5. M.B. Weiss, K. Werbach, D.C. Sicker, C. Caicedo, On the application of blockchains to spectrum management. IEEE Trans. Cogn. Commun. Netw. (2019)
6. FCC's Rosenworcel Talks Up 6G? (2018), https://www.multichan-nel.com/news/fccs-rosenworcel-talks-up-6g
7. K. Kotobi, S.G. Bilen, Secure blockchains for dynamic spectrum access: a decentralized database in moving cognitive radio networks enhances security and user access. IEEE Trans. Veh. Technol. Mag. **13**(1), 32–39 (2018)
8. Y. Pei, S. Hu, F. Zhong, D. Niyato, Y.-C. Liang, Blockchain-enabled dynamic spectrum access: cooperative spectrum sensing, access and mining. *Proceedings of the IEEE Global Communications Conference (GLOBECOM'19)*, 2019, pp. 1–6
9. S. Bayhan, A. Zubow, A. Wolisz, Spass: spectrum sensing as a service via smart contracts, in *Proceedings of the IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN'18)*, 2018, pp. 1–10
10. C.T. Nguyen, D.T. Hoang, D.N. Nguyen, D. Niyato, H.T. Nguyen, E. Dutkiewicz, Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE Access **7**, 85727–85745 (2019)
11. M. Castro, B. Liskov et al., Practical byzantine fault tolerance, in *OSDI* , vol. 99(1999), 1999, pp. 173–186
12. J.R. Douceur, The sybil attack, in *International Workshop on Peer-to-Peer Systems*. (Springer, 2002), pp. 251–260
13. Z. Liu, N.C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, D.I. Kim, A survey on blockchain: a game theoretical perspective, IEEE Access **7**, 47615–47643 (2019)
14. D. Gurney, G. Buchwald, L. Ecklund, S.L. Kuffner, J. Grosspietsch, Geo-location database techniques for incumbent protection in the TV white space, in *Proceedings of the IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN'08)*. IEEE, 2008, pp. 1–9
15. Y. Zhang, C. Lee, D. Niyato, P. Wang, Auction approaches for resource allocation in wireless systems: a survey. IEEE Commun. Surv. Tutor. **15**(3), 1020–1041 (2012)

16. S. Raju, S. Boddepalli, S. Gampa, Q. Yan, J.S. Deogun, Identity management using blockchain for cognitive cellular networks, in *IEEE International Conference on Communications (ICC)*, 2017, pp. 1–6
17. Y. Jiao, P. Wang, D. Niyato, K. Suankaewmanee, Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks. IEEE Trans. Parallel Distrib. Syst. (2019)
18. K. Kotobi, P.B. Mainwaring, S.G. Bilen, Puzzle-based auction mechanism for spectrum sharing in cognitive radio networks, in *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2016, pp. 1–6
19. H. Seo, J. Park, M. Bennis, W. Choi, Consensus-before-talk: distributed dynamic spectrum access via distributed spectrum ledger technology, in *Proceedings of the IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN'18)*, 2018, pp. 1–7
20. Z. Gao, H. Zhu, S. Li, S. Du, X. Li, Security and privacy of collaborative spectrum sensing in cognitive radio networks. IEEE Wirel. Commun. **19**(6), 106–112 (2012)
21. W. Wang, D.T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, D.I. Kim, A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access **7**, 22328–22370 (2019)
22. M. Ball, A. Rosen, M. Sabin, P.N. Vasudevan, Proofs of useful work. IACR Cryptol. ePrint Arch. **2017**, 203 (2017)