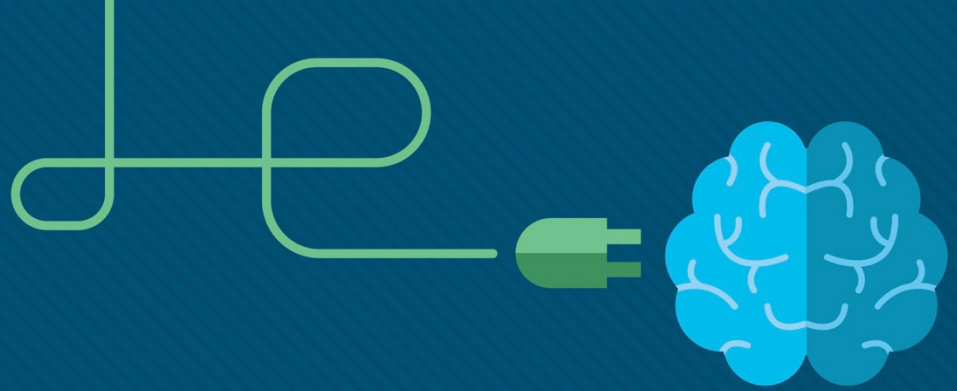
Cognitive NETWORKS



Blockchain for Dynamic Spectrum Management

Lector Materials

gabriel.bugar@tuke.sk – BN 32, č.d. 515

Lessons content

Key Topics

Week	Topic description
7.	Cognitive Radio for Dynamic Spectrum Management
8.	OSA and Spectrum Sensing Theories and Methods
9.	Assignments for elaboration - performance and discussions
10.	Blockchain for Dynamic Spectrum Management
11.	Artificial Intelligence for Dynamic Spectrum Management
12.	ML for Spectrum Sharing, ML for Signal Classification, Deep Reinforcement Learning for Dynamic Spectrum Access
13.	

Week 10. Lector Content

This chapter covers the following content:

- Blockchain and DSM
  - Key functions and basic model
- Blockchain Technologies
  - Overview of Blockchain
  - Blockchain structure
  - Consensus Algorithm – PoW, PoS, PBFT
  - Workflow of Blockchain, features and potential attacks
- Blockchain for Spectrum Management

1.1 Blockchain and DSM

- 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**.

Blockchain

- 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.

Blockchain

- Some characteristics of blockchain make it beneficial in many areas in communications, for examples:
  - **encryption algorithms**, blockchain has been used to guarantee the integrity of data in the Internet of Things (IoT) [1],
  - **traceability**, blockchain has been used to design a collaborated video streaming framework for Mobile Edge Computing [2].
- Moreover, blockchain is seen as a promising technology to achieve more efficient dynamic spectrum management (DSM) [3, 4].
- 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 [5].

1.2 Blockchain Technologies

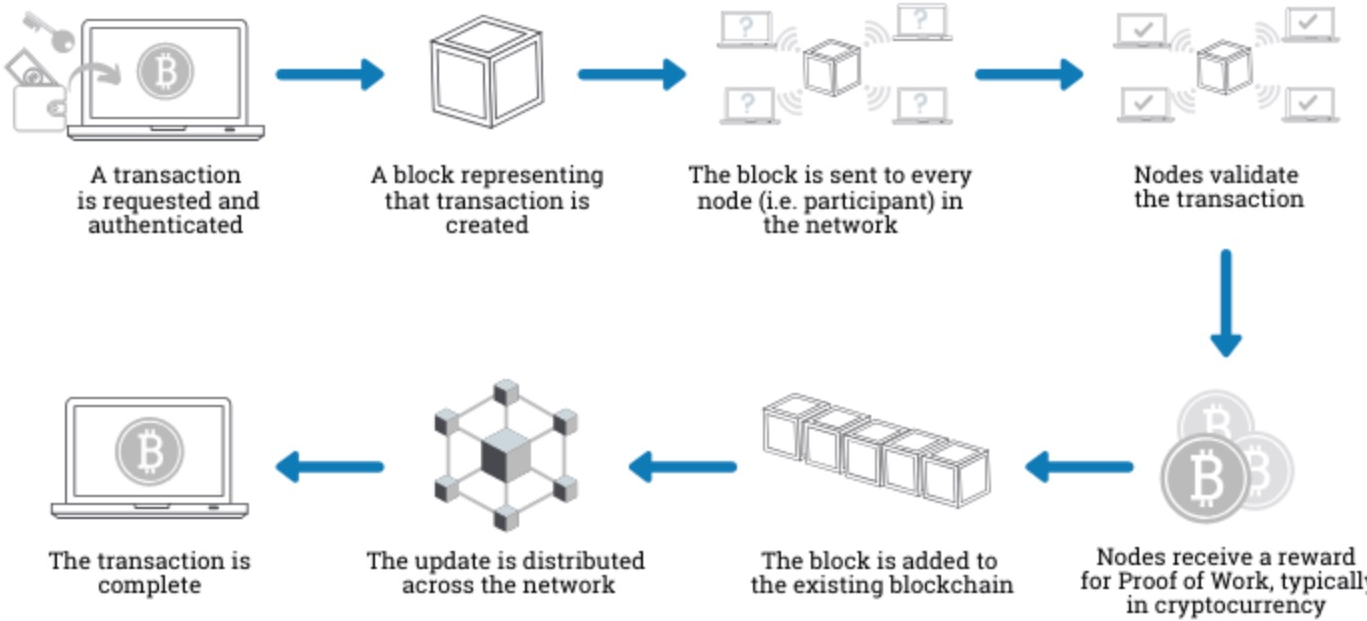
- Blockchain is essentially an open and distributed database maintained by nodes in a Peer-to-Peer (P2P) network.
- When a blockchain is used to record transactions between nodes, it can be seen as a distributed ledger.
- Through cryptographic techniques, the transactions recorded in a blockchain are 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.

Overview of Blockchain

- We give an overview of blockchain from the following 5 aspects:
    1. Blockchain structure
    2. Consensus algorithm
    3. Solution of discrepancy in the nodes
    4. Digital signature and types of blockchain
- Finally, we will illustrate the work flow of a blockchain.

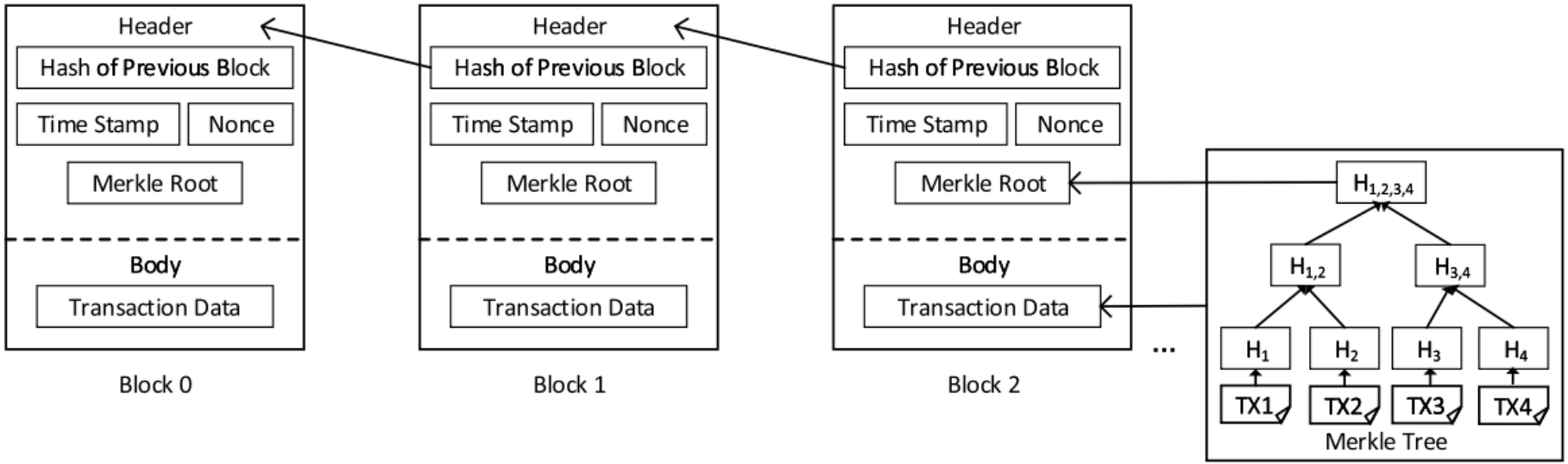
Blockchain Structure

- In a blockchain network, transactions are validated by a community of nodes and then recorded in a block



Blockchain Structure

- As shown in Fig, a block is composed of a Header and a Body, in the latter of which the transaction data is stored.



Blockchain Structure

- The block header contains the **Hash of the previous block**, a **Time Stamp**, **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 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.

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.

Consensus Algorithm - PoW

- 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.

Consensus Algorithm - PoW

- 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.

Consensus Algorithm - PoS

- 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.

Consensus Algorithm - PoS

- 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.
- With PoS, the computational resources one node occupies no longer determine the probability that it successfully finds a new block
- thus the computational resources required to reach a consensus can be largely reduced.

Consensus Algorithm - PBFT

- Practical Byzantine Fault Tolerance is a practical voting-based algorithm that allows a consortium of nodes to reach consensus without the assumption of synchronization among them.
- With a PBFT, 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.

Consensus Algorithm - PBFT

- 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 $\lfloor n-1 \rfloor$ byzantine nodes, where n is denoted as the 3 number of nodes which participate in the consensus process.

Consensus Algorithm - PBFT

- 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, 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.

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 public 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.

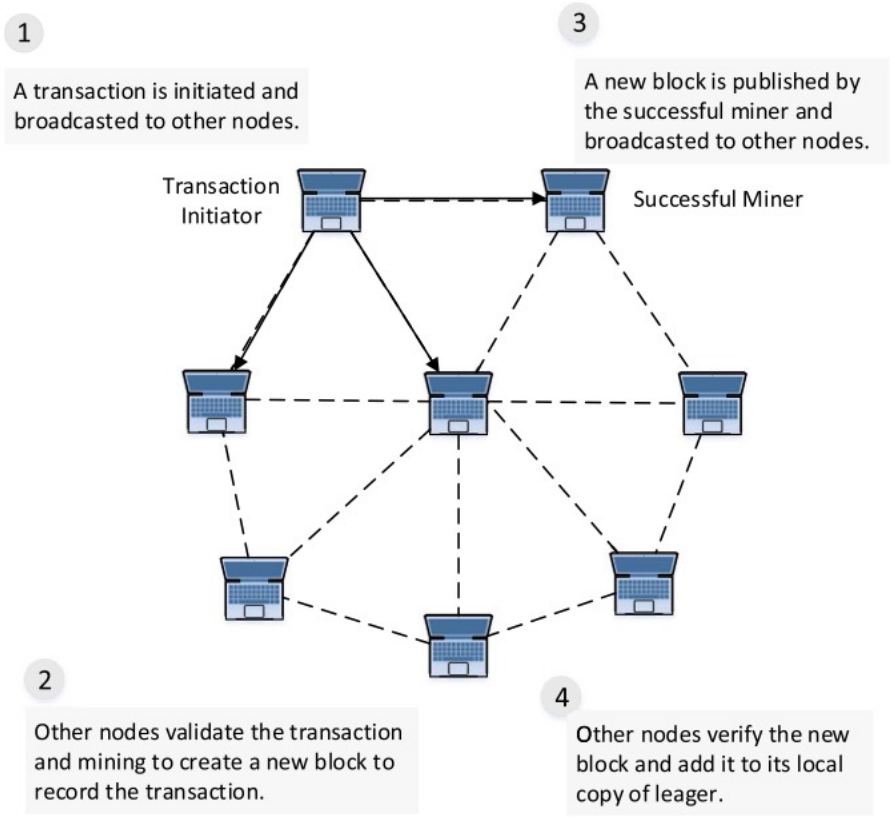
Types of Blockchain

- 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
- 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.
- 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.

Types of Blockchain

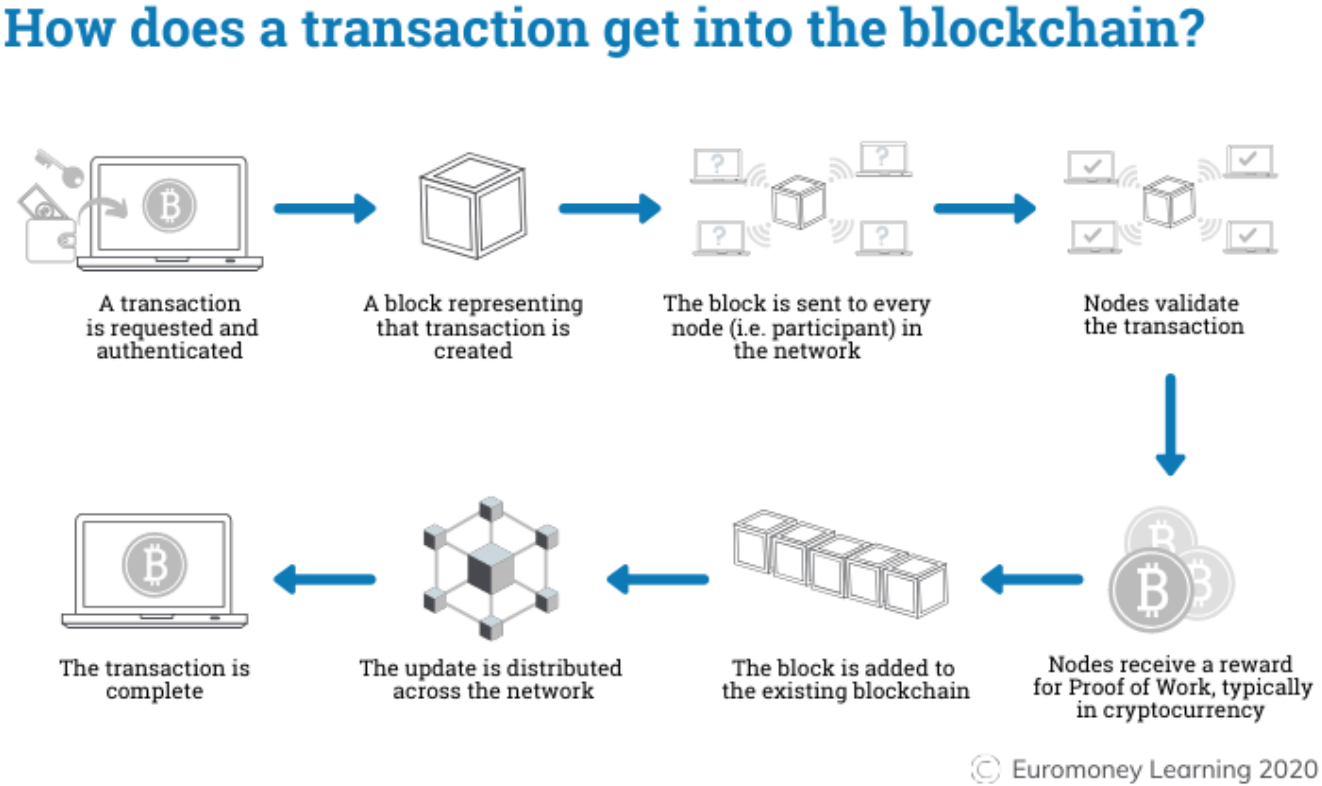
- A permissioned network is thus established, in which only the authorized nodes can access certain transactions of the blockchain or participate in working to publish new blocks. In this way, the privacy of the transactions is highly improved and the decentralization of authority of transaction validation 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.
- 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.

Workflow of Blockchain



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

Workflow of Blockchain – new Transaction



Features and the Potential Attacks on Blockchain

- Decentralization
- Trustless
- Immutability
- Non-repudiation
- Transparency
- Traceability

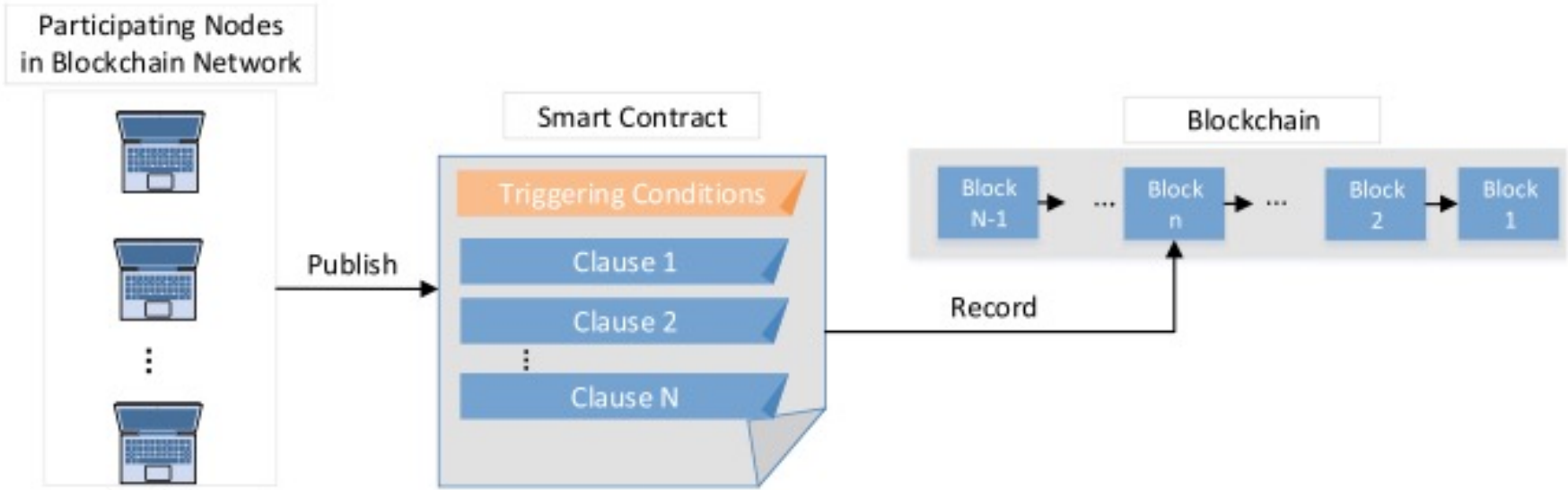
- The blockchain is still under the risk of multiple kinds of attacks:
  - Selfish Mining
  - Majority Attack
  - Denial of Service Attack

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 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.

Smart Contracts Enabled by Blockchain

- The generation procedures of a smart contract are shown in Figure, and the work flow of the smart contracts is demonstrated as follows.



Smart Contracts Enabled by Blockchain

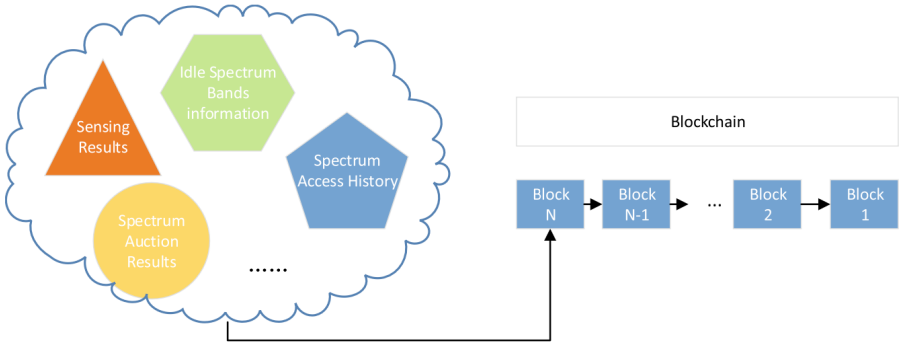
- The involved nodes first negotiate to agree upon and sign contractual clauses.
- The approved clauses are further recorded in a transaction.
- Similar as other transactions, such a transaction which records the smart contract will be verified by other nodes and then appended to other transactions in 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.

1.3 Blockchain for Spectrum Management

Cognitive NETWORKS

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.
- Based on this, one potential trend of applying blockchain to spectrum management is to record the information about spectrum management.



- One main reason of this application is that blockchain makes such information accessible to all the **secondary users (SUs)**.

Blockchain as a Secure Database for Spectrum Management

- **Information of TV White Spaces** and other underutilized spectrum bands can be dynamically recorded in a 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.

Blockchain as a Secure Database for Spectrum Management

- **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.

Blockchain as a Secure Database for Spectrum Management

- **Spectrum Auction Results** can also be recorded in a blockchain.
- Auction mechanisms have been shown as an efficient way for dynamic spectrum allocation. Among the spectrum auctions, the secondary auctions are used when the licensed PU shares the spectrum with SUs.
- The sealedbid 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.

Blockchain as a Secure Database for Spectrum Management

- **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.

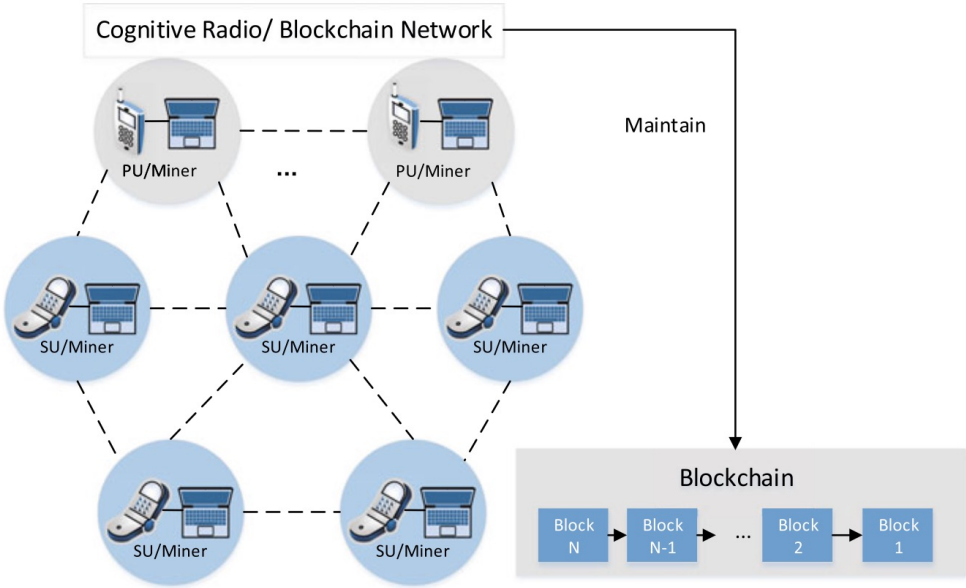
Deployment of Blockchain over Cognitive Radio Networks

- 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.

Deployment of Blockchain over Cognitive Radio Networks

- The first way is to **directly deploy a blockchain network** over a communication network, as shown in Figure.

- Specifically, since the information regarding the spectrum management, which needs to be recorded in the blockchain, is produced or 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

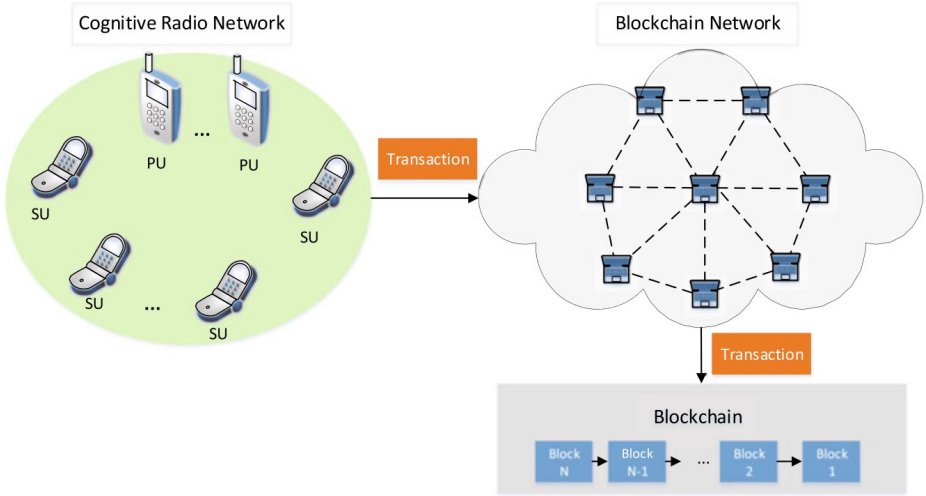


Deployment of Blockchain over Cognitive Radio Networks

- 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.

Deployment of Blockchain over Cognitive Radio Networks

- 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 Figure:



Deployment of Blockchain over Cognitive Radio Networks

- 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. 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.

References

1. 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. 212, 1676–1717 (2018)
2. M.Liu,F.R.Yu,Y.Teng,V.C.Leung,M.Song,Distributedresourceallocationinblockchain-based video streaming systems with mobile edge computing. IEEE Trans. Wirel. Commun. 18(1), 695–708 (2018)
3. 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)
4. M.B.Weiss,K.Werbach,D.C.Sicker,C.Caicedo,Ontheapplicationofblockchainstospectrum management. IEEE Trans. Cogn. Commun. Netw. (2019)
5. FCC's Rosenworcel Talks Up 6G? (2018), https://www.multichan-nel.com/news/fccs-rosenworcel- talks- up- 6g

Next lessons content

Cognitive
NETWORKS

Next lessons content

Key Topics

Week	Description
9.	Concurrent Spectrum Access
10.	Blockchain for Dynamic Spectrum Management
11.	Artificial Intelligence for Dynamic Spectrum Management
12.	ML for Spectrum Sharing, ML for Signal Classification, Deep Reinforcement Learning for Dynamic Spectrum Access
13.	-

Cognitive
NETWORKS