Chapter 5
Blockchain for Digital Twin

Abstract Security and privacy are critical issues in digital twin edge networks. Blockchain, as a tamper-proof distributed database, is a promising solution for protecting data and edge resource sharing in digital twin edge networks. In this chapter, we first introduce the architecture of the blockchain-empowered digital twin edge network, to show the integration angles of the blockchain and digital twin techniques. Then, we show the block generation and consensus process in the developed blockchain-empowered digital twin edge network architecture.

5.1 Blockchain-Empowered Digital Twin

Blockchain is a chain structure of data blocks arranged in chronological order that is essentially a tamper-proof distributed database that uses cryptography to ensure the security of each transaction in a decentralized manner. A blockchain is composed of peer-to-peer networks, distributed storage, consensus mechanisms, cryptography, and smart contracts. Therefore, a blockchain has the advantages of decentralization, tamper resistance, anonymity, public verifiability, and traceability [61, 62]. Integrating blockchain and digital twin provides security guarantee, trusted traceability, accessibility, and immutability of transactions in digital twin edge networks. Specifically, building virtual twins and continuously updating twin models require core data that contain private user information, such as production parameters and users' personal information in industrial manufacturing and personal health data in healthcare. Therefore, the physical and virtual synchronization during virtual twin construction and maintenance needs to be recorded as transactions in the blockchain. This means the core data and edge resources can be governed by the blockchain in a decentralized and secure manner. In addition, virtual twins can simulate the behavioural features of physical components and generate virtual data. After the blockchain stores the generated virtual data in its distributed ledger, these virtual data become digital assets and their ownership can be proved. To achieve a secure and reliable digital

Y. Zhang, *Digital Twin*, Simula SpringerBriefs on Computing 16,
https://doi.org/10.1007/978-3-031-51819-5_5

twin edge network, the following blockchain-related security performances should be satisfied.

- *Security and trust:* In the developed blockchain-empowered digital twin edge network, the transactions are audited and verified by a set of verifiers by utilizing consensus algorithms [63], unlike traditional transaction management, which depends on a central infrastructure. Thus, the blockchain can guarantee security and trust for the transactions in a digital twin edge network in a decentralized manner without a trusted intermediary.
- *Unforgeability and immutability:* The decentralized authentication of transactions in the blockchain-empowered digital twin edge network ensures that no attacker can pose as a user to corrupt the blockchain. In addition, verifiers who execute the consensus algorithms are reluctant to misbehave or collude with each other, since all the verifiers' identities are revealed to the users in a digital twin edge network and would be scrutinized for any misconduct. Furthermore, an attacker cannot modify the audited and stored transactions in the blockchain, since each block is embedded with the hash value of its previous block, which ensures immutability [64].
- *Transparency and privacy protection:* In the blockchain-empowered digital twin edge network, all the kinds of information recorded in the blockchain are transparent and openly accessible to all participants. Moreover, end users can change their identity (i.e. public key) after each transaction in the blockchain to protect their identity privacy.
- *Scalability and interoperability:* Digital twins are digital replicas of physical entities, enabling close monitoring, real-time interactions, and reliable communications between digital space and physical systems. They provide rich information to reflect the states of physical entities, to optimize the running of physical systems [65]. Therefore, the blockchain needs to provide scalability and interoperability for various digital twin services. The scalability of blockchain provides end users simultaneous access to the digital twin edge network. Meanwhile, the interoperability allows different digital replicas of physical entities to interact with each other seamlessly.

The architecture of a blockchain-empowered digital twin edge network is shown in Fig. 5.1. In the physical plane, physical objects share information with each other. Various wireless/wired devices, such as sensors, radio frequency identification devices, actuators, controllers, and other tags can connect with IoT gateways, Wi-Fi access points, and base stations (BSs) supporting the communications between physical objects. In the virtual plane, the digital twin edge servers provide the necessary computing capability to generate virtual twins of the physical objects, as well as model the channel conditions and data transmission among the physical objects. Moreover, a physical object realizes information transmission with a virtual twin through wireless communication technologies and shares the data in real time and accepts feedback from the virtual twin. In the blockchain plane, BSs are distributed in a specific area to work as verifiers. Specifically, if data or network resources are successfully shared between a requester and a provider in both the physical and vir-

tual planes, the requester should create a transaction record and send it to the nearest BS. The BSs collect and manage local transaction records. The transaction records are structured into blocks after the consensus process among the BSs is completed, and then stored permanently in each BS. The detailed processes are as follows.

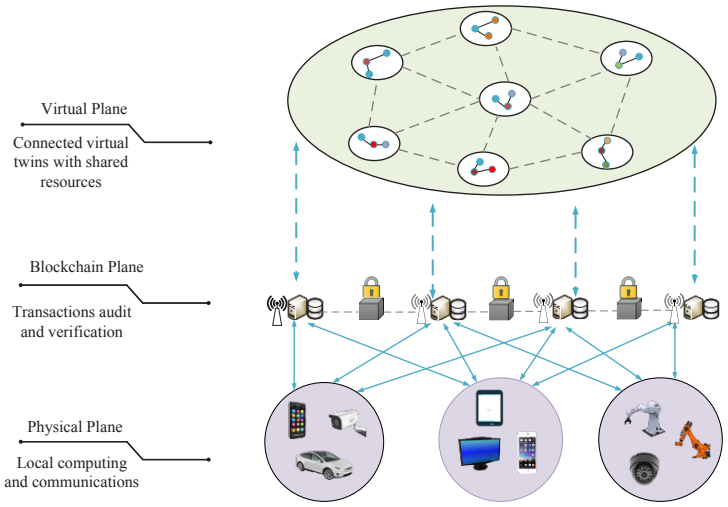

Fig. 5.1 The architecture of a blockchain-empowered digital twin edge network

- *System initialization:* For privacy protection, each device needs to register a legitimate identity in the initialization stage. In the blockchain-empowered digital twin edge network, an elliptic curve digital signature algorithm and asymmetric cryptography are used for initialization. A device can obtain a legitimate identity after its identity has been authenticated. The identity includes a public key, a private key, and the corresponding certificate.
- *Role selection for devices:* Devices in both the physical and virtual planes choose their roles (i.e. data or network resource requester and provider) according to their current available resources. Devices with surplus resources can become providers to provide services for requesters.
- *Transactions:* The existence of connections in the digital twin edge network poses new challenges for security and privacy. Therefore, communications in the physical and virtual planes can be considered transactions, which are recorded into the blockchain to achieve security and preserve privacy. Additionally, the blockchain can store the synchronization data between the physical and virtual planes, so that the data are secure and private. In addition, the blockchain enables edge servers belonging to different stakeholders to cooperatively process computation tasks without a trusted third party.
- *Building blocks:* BSs collect all the transaction records within a certain period and then encrypt and digitally sign them to guarantee their authenticity and accuracy.

The transaction records are structured into blocks, and each block contains a cryptographic hash of the prior block. To verify the correctness of a new block, the consensus algorithm is used. In the proof-based consensus process, one of the BSs is selected as the leader for creating the new block. Because of broadcasts, each BS can access the entire transaction record and has the opportunity to be the leader.

- *The consensus process:* The leader broadcasts the created block to the other BSs for verification and audit. All the BSs audit the correctness of the created block and broadcast their audit results. The leader then analyses the audit results and, if necessary, sends the block back to the BSs for another audit.

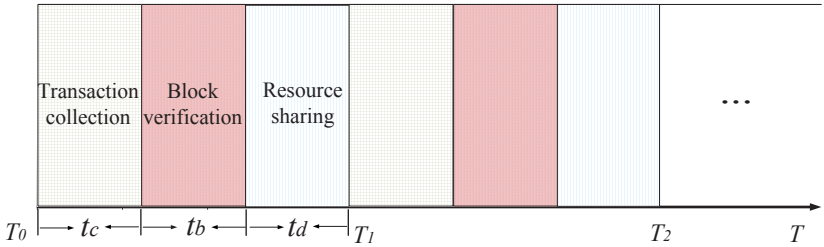

Fig. 5.2 The time sequence of the transaction confirmation procedure

5.2 Block Generation and Consensus for Digital Twin

In the developed blockchain-empowered digital twin edge network, the distinct characteristics of the blockchain introduce unique challenges for data and edge resource sharing. Specifically, Fig. 5.2 illustrates the time sequence of T rounds of the transaction confirmation procedure. In each round, the transaction confirmation time is divided into three time slots: a transaction collection slot, a block verification slot, and a resource sharing slot. For example, in the T_1 round, this consists of the slot t_c for transaction collection, the slot t_b for block verification, and the slot t_d for resource sharing among the edge devices. The requester can obtain the required resource from the provider only at the end of round T_1's transaction confirmation procedure, that is, when the block is appended to the blockchain. In practice, it could take a long time to successfully finish the transaction confirmation procedure, since both transaction collection and block verification are executed in a dynamic and stochastic wireless transmission environment. Transactions of edge devices in congested areas might not be successfully transmitted to the verifiers for verification in the transaction collection phase, which will lead to failure of the transaction confirmation procedure. On the other hand, the typical Nakamoto consensus protocol provides proof of work (PoW) [66], where the verifiers compete to solve a computationally difficult

cryptopuzzle. The fastest verifier that solves the cryptopuzzle will append its block to the blockchain. Nevertheless, the cryptopuzzle solving–based PoW consensus protocol consumes a large amount of computational and energy resources, which is not useful for resource-constrained edge devices, since they cannot undertake heavy computations. In addition, the audit and verification of the block among the verifiers can encounter impediments due to traffic congestion in the network. Therefore, the edge devices could suffer from long waiting times in resource sharing. A carefully designed transaction confirmation procedure is thus necessary for secure and privacy-protected resource sharing among edge devices while allowing for their resource sharing efficiency.

To enable edge devices to obtain the required resources in time, we present a block generation and consensus process in the developed blockchain-empowered digital twin edge network. The process is based on a relay-assisted transaction relaying scheme that facilitates transaction collection in congested areas, and a lightweight block verification scheme based on delegated proof of stake (DPoS) that is utilized to reduce the resource consumption of the verifiers during block verification.

- In the transaction collection phase, the local verifiers periodically collect transactions, verify the integrity and correctness of the transactions by validating their signature, and then process a number of validated transactions into a block.
- In the block verification phase, the local verifiers that would like to add a block to the blockchain send consensus requests to a verification set, which consists of a set of preselected verifiers, and executes block verification and audit by using a proof-based consensus protocol.

We develop two new schemes for transaction collection and block verification: (I) a relay-assisted transaction relaying scheme and (II) a DPoS-based lightweight block verification scheme. The work procedure for the developed schemes is shown in Fig. 5.3 and is illustrated in the subsequent discussion.

5.2.1 Blockchain Model

To enhance the security and reliability of digital twins from untrusted end users, the BSs act as blockchain nodes and maintain the running of the permissioned blockchain. The digital twins are stored in the blockchain and their data are updated as the states of the corresponding users change. The local models of the BS, also stored in the blockchain, can be verified by other BSs to ensure their quality. Thus, there are three types of records, namely, digital twin model records, digital twin data records, and training model records.

The overall digital twin blockchain scheme is shown in Fig. 5.4. The BSs first train the local training models on their own data and then upload the trained models to the MBS. The trained models are also recorded as blockchain transactions and are broadcast to the other BSs for verification. The other BSs collect the transactions and pack them into blocks. The consensus process is executed to verify the transactions

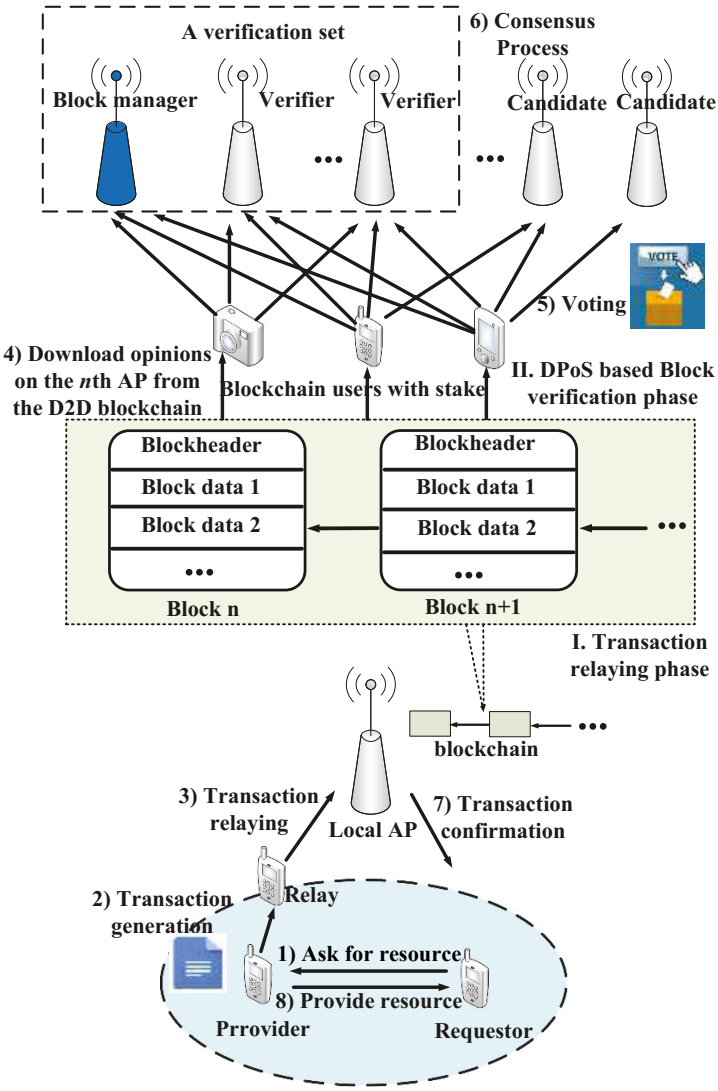

Fig. 5.3 Work procedure for transaction relaying and DPoS-based block verification

in blocks. Our consensus process is executed based on the DPoS protocol, where the

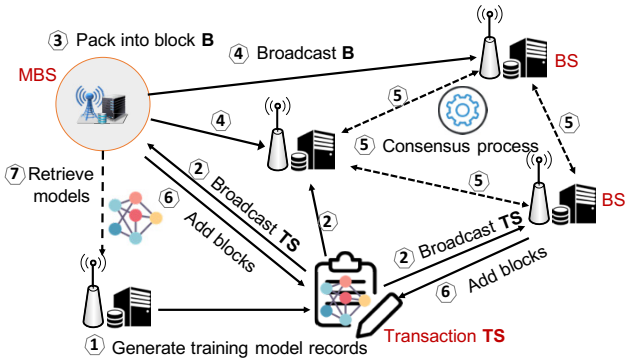

Fig. 5.4 The blockchain scheme for federated learning

stakes are the training coins. The initial training coins are allocated to BS i according to its data from digital twins, denoted as

$$S_i = \frac{\sum_{j=1}^{K_i} D_{DT_j}}{\sum_{k=1}^{M} D_k} S_{ini}, \tag{5.1}$$

where S_{ini} is an initial value and K_i is the number of digital twins associated with BS i.

The coins of each BS are then adjusted according to their performance in the training process. If the trained model of a BS passes the verification of the other BSs and the MBS, the coins will be awarded to the BS. Otherwise, the BS will receive no pay for its training work. A number of BSs are elected as block producers by all the BSs. In the voting process, all the BSs vote for the candidate BSs by using their own training coins. The elected BSs take turns to pack the transactions in a time interval T into a block B and broadcast the block B to other producers for verification.

In our proposed scheme, we leverage blockchain to verify the local models before embedding them into the global model. Due to high resource consumption required for block verification, the interval T should be set to multiple times the local training period; that is, the BSs execute multiple local training iterations before transmitting the local models to the MBS for global aggregation.

5.2.2 Relay-Assisted Transaction Relaying Scheme

As shown in Fig. 5.3, a requester that requires resources first sends a request to a nearby provider (Step 1). Then the provider generates a transaction (Step 2) and broadcasts its transaction for verification. A provider that would like to verify its

transaction in a congested area first sends a transaction relaying request. To facilitate peer discovery and reduce interference, the local verifier coordinates the transaction relaying link establishment; that is, the verifier selects a device near the provider as a relay device to assist in transaction relaying and reuses the channels of end users located far away in a different area (Step 3). We consider the time division multiple access technique in the transaction relaying transmission. However, the existence of a neighbour might not imply the stable establishment of the transaction relaying link, since the neighbour might not be willing to participate in transaction relaying due to the associated overhead, such as energy and bandwidth consumption. Thus, the local verifier needs to pay the relay devices a relay fee to motivate them to participate in transaction relaying.

5.2.3 DPoS-Based Lightweight Block Verification Scheme

DPoS has been demonstrated as a high-efficiency consensus protocol with moderate cost in which a part of the delegates (i.e. verifiers) are selected based on their stakes to perform the consensus process. Here, the stake is the accumulated time during which a delegate possesses its assets before using them to generate a new block. DPoS has been used in real scenarios, such as enterprise operation systems, BitShares, and the Internet of Vehicles. It is reasonable to consider that the DPoS can be utilized in the digital twin edge network and to develop a DPoS-based lightweight block verification scheme. Unlike computation-intensive PoW, the designed DPoS-based lightweight block verification scheme can leverage the stake of the verifiers as a mining resource to generate a block. The more stakes a verifier has, the higher its probability of finding a solution to generate a block. In addition, the verification and audit of the generated block are executed by only some of the preselected verifiers, thus keeping the computational complexity reasonably low. As shown in Fig. 5.3, the main steps in the DPoS consensus protocol in our lightweight block verification scheme involve verifying candidate generation, the verifier selection, the consensus process, and the transaction fee payment.

5.2.3.1 Verifying Candidate Generation

A verifier that wants to be a verifier first submits a deposit of stake to an account under public supervision. This deposit will be confiscated if the verifier behaves badly during a consensus process, for example, if it fails to generate a block in its turn or if it generates false block verification results.

5.2.3.2 Verifier Selection

The blockchain users, that is, the end users possessing stakes, download the opinions of the candidates from the blockchain (Step 4) and vote for their preferred candidates according to some criteria, for example, voting for candidates that can generate and verify a block quickly (Step 5). A blockchain user can vote for more than one candidate and can also persuade others to vote for their favourite candidates. The top k candidates with the most votes are selected to form a verification set, where k is an odd integer, such as 21 in enterprise operation systems. The k verifiers all take turns acting as the block manager during k block verification subslots.

5.2.3.3 Consensus Process

In each block verification subslot, the block manager carries out block management in its own consensus process round (Step 6). Specifically, the block manager first broadcasts the unverified block to other verifiers for verification and audit. Then, each verifier locally verifies the signature of each transaction in the block and replies to other audit results with its signature. Following the reception of the audit results, each verifier compares its audit result with those of the other verifiers and sends a commit message to the block manager. Considering Byzantine fault tolerance consensus conditions, the block manager sends the current audited block to all the verifiers and the local verifiers for storage (Step 7), providing it receives a commit message from more than two-thirds of the verifiers. Finally, the provider provides the required resources to the requestor (Step 8).

5.2.4 Conclusion

We first presented the architecture of a blockchain-empowered digital twin edge network that consists of a virtual plane, a blockchain plane, and a physical plane. Then, we illustrated the processes of the developed architecture and showed the integration angles of the blockchain and the digital twin edge network. Furthermore, we presented the block generation and consensus process in the developed blockchain-empowered digital twin edge network architecture.