Blockchain Technology and Its Components

Subjects: Others
Contributor: Yi Wang , Jason Zheng , Chidinma Dike , Stefan Pancari , George Giakos , Wafa Elmannai , Bingyang Wei

The Internet of Things (IoT) is a recent technology that uses smart connected systems to create a global network of physical devices that exchange and communicate data with each other. Blockchain is essentially a system for recording data that makes it much more difficult to change or hack. Blockchain uses a distributed networking system of machines that replicate and create a chain of data. This chain of data can be considered a ledger, with each of these becoming a block. This chain of data is turned into a block which is linked to the previous block creating a chain of blocks, hence the name blockchain.

IoT blockchain simulator

1. Blockchain Components

Blockchain technology, as previously stated, is characterized by its blocks which are formed into chains, hence the name blockchain. However, blockchain technology is much more complicated than just a collection of blocks and chains. It requires many other components to actually build the block and make sure that they will not be tampered with and will remain safe. Some of these important technologies include cryptographic hash functions, asymmetric-key cryptography, and ledgers [1].

The first main component of blockchain technology is the cryptographic hash functions. This is applied to data in a method called hashing. Hashing is a method used to calculate a unique output for an input of any size. The data is encrypted into a secure format which is unreadable unless the recipient has the keys. This allows individuals to take input data and hash the data to derive the same results. This proves that there has been no change to the data [1]. One of the most widely implemented hash functions in blockchain technology would be the Secure Hash Algorithm with an output of 256 bits, otherwise, known as SHA-256. The SHA256 algorithm takes inputs that have a length of less than 2^{64} bits and releases an output that has a length of 256 bits. It has a block size of 512 bits which are represented by sixteen 32-bit words. This block of 512 enters a message compression function in 32-bit words through a message scheduler. The message scheduler then expands the 512-bit message block into sixty-four 32-bit words. The SHA256 hashing algorithms are then performed on words that are 32 bits in length, using eight working variables that are also 32 bits in length. The values of the working variable are computed at every round and this is continued until 64 rounds have been completed [2].

SHA256 also takes a 256-bit initialization vector which is fixed for the first message block. The intermediate message digest obtained at the end of the first 64 rounds is used as the initialization vector for the next message

block. The SHA256 hash function is built using the Davies–Meyer construction where the initialization vector is added to the output of 64 rounds. After 64 rounds of message compression and the addition of the initialization vector, the algorithm produces an intermediate message digest of 256 bits. After the whole message block has been hashed, a value of 256 bits is obtained that is the final message digest of the input message. The SHA256 hashing algorithm is thus similar to a block cipher with a 256-bit message block size and a 512-bit key that is expanded into sixty-four 32-bit round keys using the message scheduler for each of the 64 rounds of this cipher [2].

A second important component of blockchain is asymmetric-key cryptography also known as public-key cryptography [3]. Asymmetric-key cryptography uses a pair of keys: one public and one private. The main purpose of this component is to be used in transactions such as those done in cryptocurrency. The public key is used to secure operations of the blockchain and give everyone access to the knowledge stored in the block such as the address of a single cryptocurrency in the entire network. The private key is much more restrictive and is used by an individual to digitally sign transactions.

The third important component of blockchain would be the ledger. A ledger would simply be a collection of transactions. These ledgers traditionally were centralized and operated by a single party. However, the distributed ledger is much more common in the case of blockchain [1]. Distributed ledgers are digital ledgers that are distributed across a network to all the nodes, which results in all the nodes having the same copy of the ledger. This ledger will update all nodes or holders on the network simultaneously. Distributed ledgers also authenticate information through cryptographic signature [4]. In the case of blockchain, distributed ledgers are made of blocks and all these blocks form a chain to create the entire ledger. **Figure 1** displays all different layers in a blockchain, which will be explained in detail in the next section.

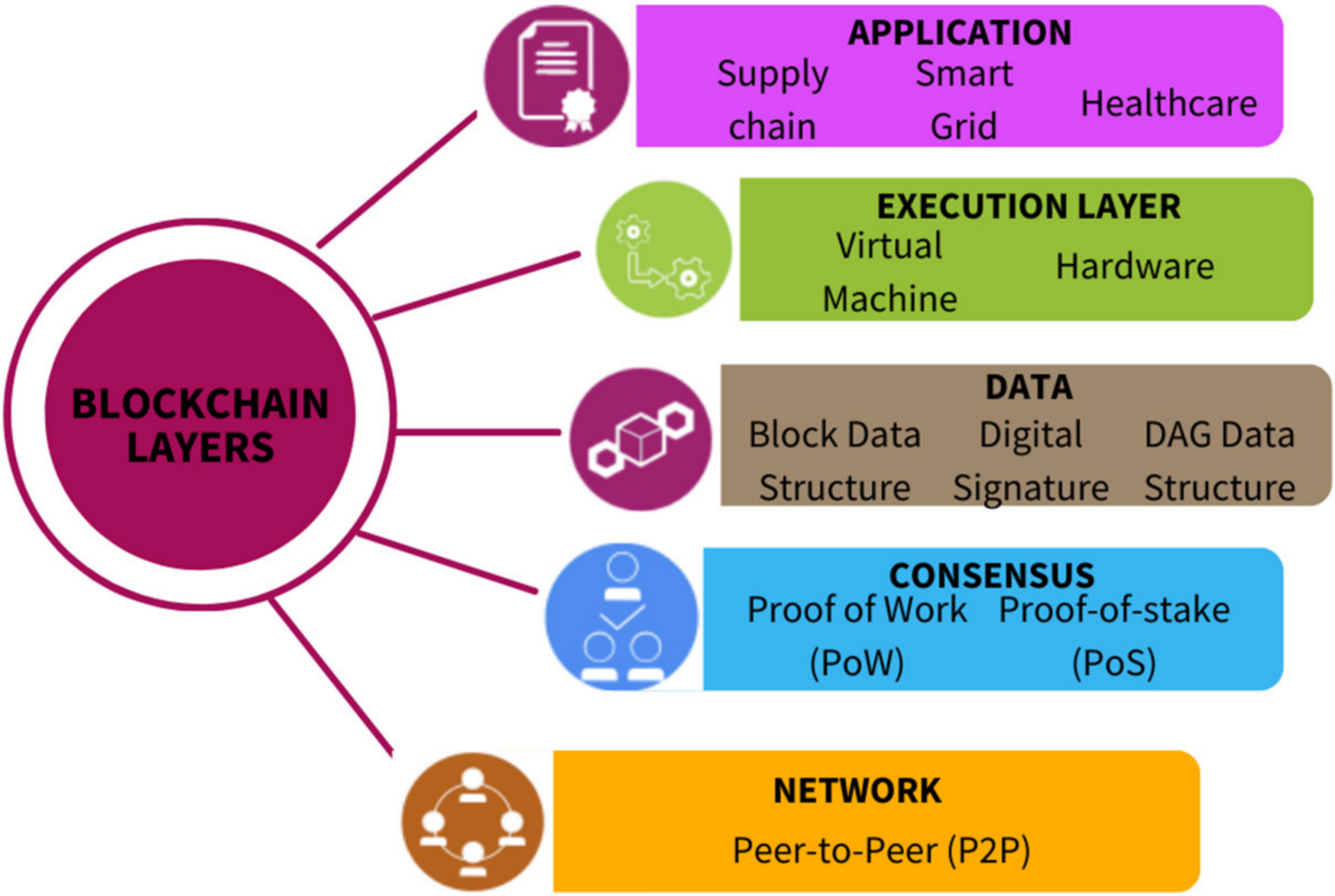

Figure 1. Five Different Layers of Blockchain.

2. Blockchain Layers

2.1. Network Layer

The first and bottom layer of the multi-layered Distribute Ledger Technology (DLT) stack would be the network layer. This layer consists of a peer-to-peer network in which participants share resources without a central authority, i.e., it is decentralized. While all participants in a P2P network are considered equal, participants are split into two basic types of nodes: light/lightweight nodes and full nodes. Full nodes are the main type of node that stores a complete copy of the ledger and takes care of all the mining, validations, and execution of consensus rules. Lightweight nodes are not able to act as a full ledger but rather are meant to supplement the full nodes of the network. Lightweight nodes store block headers and act as clients to issue transactions. The network layer is critical and takes care of peer discovery, transactions, and block propagation. Depending on the size of the blockchain, the speed of peer discovery, network delays, and propagation may have an impact on the performance of the DLT [5].

2.2. Consensus Layer

The consensus layer is very important in the DLT state system as its role is to get all the nodes of the system to reach an agreement. Two main consensus algorithms used by DLT systems are proof based and PBFT [6].

The proof-based consensus was first introduced on the bitcoin network as PoW or proof of work. This is the core mechanism on which the bitcoin network was based, a mechanism which relies on competition between nodes to compete to be the first to solve a mathematical problem [7]. This calculated block would then be broadcast by a node to other nodes, which must then mutually confirm the correctness of the hash value. Once this has been achieved, other miners would add this new block to their own blockchain. Quite similarly, this PoW is used by other cryptocurrencies such as Ethereum and Dogecoin. A drawback would be the waste of considerable computing resources. Proof of Stake (PoS) and Proof of Authority (PoA) are other two proof-based consensus algorithms.

PBFT or Practical Byzantine Fault Tolerance is an algorithm intended to handle up to ⅓ malicious byzantine replicas. The PBFT algorithm is divided into three phases: pre-prepare, prepare and commit. The pre-prepared and preparation phases are used to order requests sent in the same view even when the primary is faulty. The prepare and commit phase is used to ensure that requests that commit are totally ordered across views. For each phase, a node needs ⅔ votes from all nodes to proceed from one phase to the next. The PBFT algorithm relies on a fault tolerance calculated by the formula $(n - 1)/3$ to ensure activity and safety. An important feature of the PBFT consensus algorithm is that nodes are only partially trusted [8]. Hyperledger Fabric is an example that uses this type of consensus.

2.3. Data Layer

The data layer of the blockchain is typically used to describe the physical layer of the blockchain or DLTS. Included in this layer is practically the entire underlying technology of the blockchain. This includes data block and chain structure, hash function, Merkle tree, asymmetric public key data encryption, and time stamp technology [9]. Despite all of this technology included within the data layer, the most important aspect of this layer is storing data. The data layer is the blockchains database and safely stores all information in the form of data blocks. These data blocks, which are formed into chains, can be accessed by any full node.

In regard to data security, the blockchain system uses the previously mentioned Merkle tree structure to record transactions. Hashes of transactions are computed using the Merkle tree data structure and are stored as Merkle root. The Merkle root, previous hash, timestamps, and the decentralized nature of blockchain make it incredibly difficult to tamper with the system. Along with the security nature of the Merkle tree structure, it also allows transactions to be carried out safely between nodes in the case of decentralization. A drawback is that it can be very energy demanding and have slow processing [5].

2.4. Execution Layer

The execution layer has runtime environments such as virtual machines (VMs), containers, and compilers that are installed on nodes. This layer also implements smart contracts, through which it implements trust. These smart contracts run on the local VMs in each individual node on the network. The network then collects self-executing

computer instructions to ensure mutual consent between non-trusting parties [10]. A drawback of smart contracts would be the waste of computing resources due to the aborted transactions.

2.5. Application Layer

The application layer is the top layer of the blockchain network and is used to connect decentralized applications with the underlying blockchain technology [9]. The most popular use of blockchain technology is cryptocurrency. Typically, along with the cryptocurrency comes a lot of applications such as crypto wallets, smart contracts, and various other decentralized applications [6]. Smart contracts are widely used in cryptocurrency; however, they are designed to facilitate, verify, and enforce the execution of the contract.

Outside of cryptocurrency, the applicability of blockchain can be applied to IoT. Some examples are smart cars, smart healthcare, smart farming, and even smart cities. It is in the application layer that blockchain technology can be applied to IoT.

3. IoT Technology

IoT, which is known as the Internet of Things, simply refers to the physical objects and devices that are capable of connecting and exchanging data with other devices through the internet or other communication networks. IoT is one of the most important areas of future technology and is beginning to be implemented in multiple industries [11]. IoT devices are now not only able to connect to a network and communicate with one another but are also capable of collecting data from the environment and sharing that data to other devices for analytics, applications, and communication [12]. This is important for creating a smart environment as the connection of multiple devices and sharing information is a must.

A few examples of IoT being explored to be used in unexpected parts of our lives are transportation systems [13] and in supply chain operations [14]. When it comes to transportation systems, it has been suggested that we use sensors on vehicles, roads, and infrastructure to collect and store huge amounts of data, collectively known as big data. Using this big data traffic control, road conditions, and scheduled travel time can all be viewed and managed with the data collected by the IoT sensors [13]. Similarly, in supply chains, there have been some proposals to use machine learning and artificial intelligence algorithms in conjunction with smart sensors to monitor and collect data on remote equipment and provide suggestions on when maintenance is needed [14].

4. Blockchain Implementation in IoT

When it comes to implementing blockchain within an IoT environment, it can play an important role in more than just security. When used along with a smart contract, it can be used in managing, controlling, and securing IoT devices [15]. An example of this is for wines and spirit, where blockchain technology is being recommended for use in labeling and tracing these products to ensure quality and to prevent illegal trading and adulteration [16]. Blockchain technology in this case is being used to manage and control the smart sensors used to keep track of

these liquors and wines. In addition to its capability to make IoT device management more efficient, it allows for IoT devices to be removed from the control of a centralized authority who can manipulate or stop the system from working [17]. This makes attacks against the network a lot more difficult since the network does not revolve around an individual. In addition, the data received from IoT devices and stored in the blockchain network would also be less susceptible to plaintext and cipher attacks due to the hashing of data in the blockchain.

Figure 2 presents the proposed architecture for an IoT blockchain platform. It is composed of a large number of IoT devices and sensors, user devices, full nodes acting as local bridges, and data storage, all of which are linked to a peer-to-peer blockchain network. The IoT devices and sensors can be connected directly to the blockchain network or can connect to it through a full node. These IoT devices will collect useful data via sensors or user inputs and can request specific transactions through the blockchain network. Data can be sent or received by the IoT devices along with transactions. These data are then stored within the data storage which itself can be stored in two places. One place can be direct data storage, whether it be hardware or software. The second is the blockchain, where data are stored as blocks and can be viewed by anyone. Transactions, on the other hand, must be validated by a group of miners who in turn will receive some sort of reward for validating these transactions. These transactions will then be stored in existing blockchains and form new blocks that will be added to the ledger.

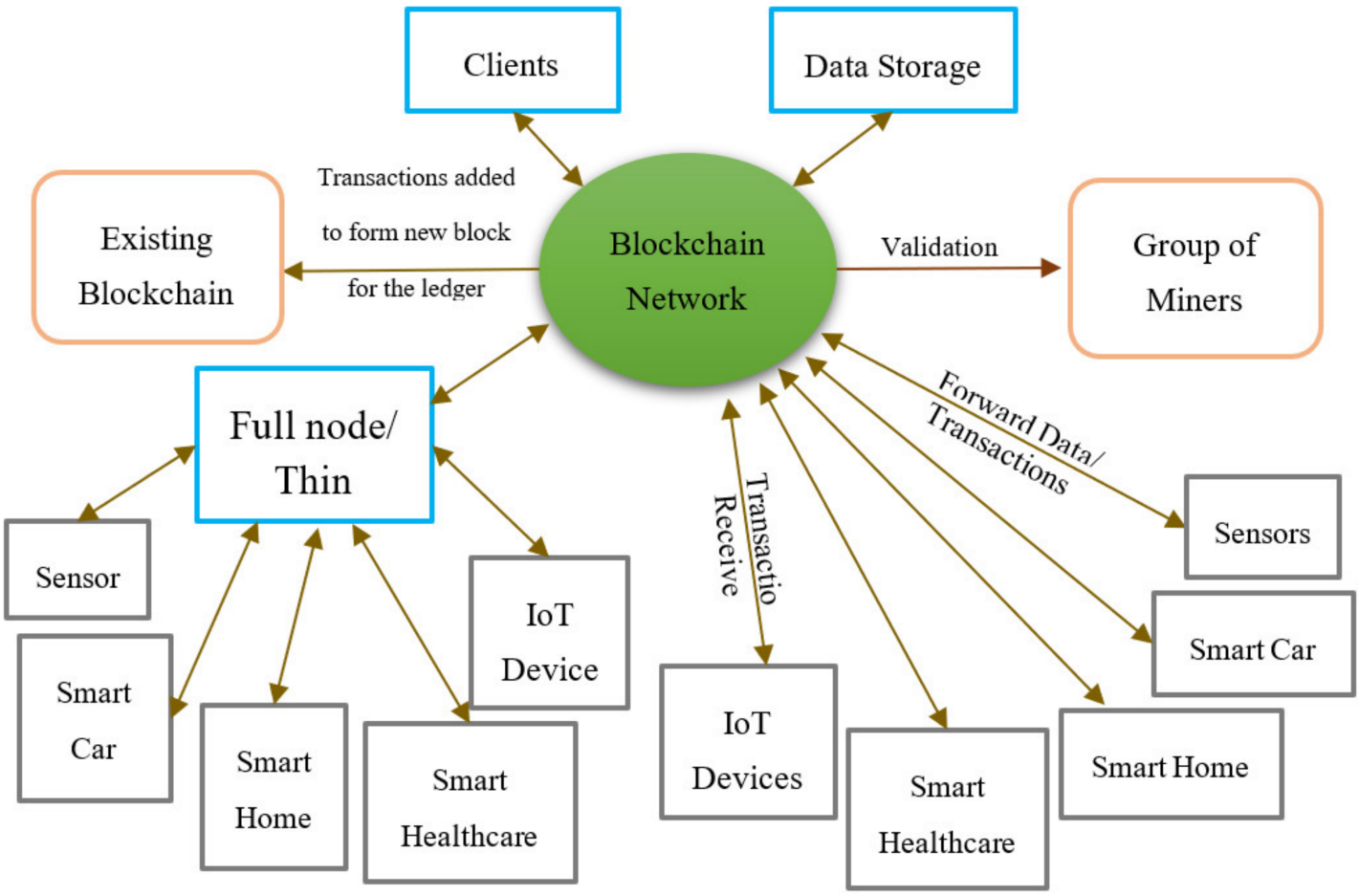

Figure 2. Proposed architecture for an IoT blockchain platform.

References

1. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain Technology Overview. Gaithersburg, MD: National Institute of Standards and Technology. Comput. Secur. Div. Inf. Technol. Lab. 2018, 31.
2. Naik, R.P.; Courtois, N.T. Optimising the SHA256 Hashing Algorithm for Faster and More Efficient Bitcoin Mining. MSc Inf. Secur. Dep. Comput. Sci. UCL 2013, 1–65.
3. Puthal, D.; Malik, N.; Mohanty, S.P.; Kougianos, E.; Das, G. Everything You Wanted to Know about the Blockchain: Its Promise, Components, Processes, and Problems. IEEE Consum. Electron. Mag. 2018, 7, 6–14.
4. Deshpande, A.; Stewart, K.; Lepetit, L.; Gunashekar, S. Distributed Ledger Technologies/Blockchain: Challenges, Opportunities and the Prospects for Standards. Overv. Rep. Br. Stand. Inst. 2017, 40, 40.
5. Paulavičius, R.; Grigaitis, S.; Filatovas, E. A Systematic Review and Empirical Analysis of Blockchain Simulators. IEEE Access 2021, 9, 38010–38028.
6. Polge, J.; Ghatpande, S.; Kubler, S.; Robert, J.; Le Traon, Y. BlockPerf: A Hybrid Blockchain Emulator/Simulator Framework. IEEE Access 2021, 9, 107858–107872.
7. Kaur, M.; Khan, M.Z.; Gupta, S.; Noorwali, A.; Chakraborty, C.; Pani, S.K. MBCP: Performance Analysis of Large Scale Mainstream Blockchain Consensus Protocols. IEEE Access 2021, 9, 80931–80944.
8. Nolan, S. PBFT—Understanding the Algorithm. Coinmonks (Blog). Available online: https://medium.com/coinmonks/pbft-understanding-the-algorithm-b7a7869650ae (accessed on 27 August 2020).
9. Xinyi, Y.; Yi, Z.; He, Y. Technical Characteristics and Model of Blockchain. In Proceedings of the 2018 10th International Conference on Communication Software and Networks (ICCSN), Chengdu, China, 6–9 July 2018; pp. 562–566.
10. Hao, Y.; Li, Y.; Dong, X.; Fang, L.; Chen, P. Performance Analysis of Consensus Algorithm in Private Blockchain. In Proceedings of the 2018 IEEE Intelligent Vehicles Symposium (IV), Changshu, China, 26–30 June 2018; pp. 280–285.
11. Lee, I.; Lee, K. The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises. Bus. Horiz. 2015, 25, 431–440.
12. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Gener. Comput. Syst. 2013, 29, 1645–1660.
13. Gayialis, S.P.; Konstantakopoulos, G.D.; Kechagias, E.P.; Papadopoulos, G.A. An Advanced Transportation System Based on Internet of Things. In Proceedings of the 10th Annual

International Conference on Industrial Engineering and Operations Management (IEOM 2020), Dubai, United Arab Emirates, 10–12 March 2020; pp. 10–12.

14. Gayialis, S.P.; Kechagias, E.P.; Konstantakopoulos, G.D.; Papadopoulos, G.A. A Predictive Maintenance System for Reverse Supply Chain Operations. Logistics 2022, 6, 4.
15. Khan, M.A.; Salah, K. IoT Security: Review, Blockchain Solutions, and Open Challenges. Future Gener. Comput. Syst. 2018, 82, 395–411.
16. Gayialis, S.P.; Kechagias, E.P.; Konstantakopoulos, G.D.; Papadopoulos, G.A.; Tatsiopoulos, I.P. An Approach for Creating a Blockchain Platform for Labeling and Tracing Wines and Spirits. In Proceedings of the IFIP International Conference on Advances in Production Management Systems, Nantes, France, 5–9 September 2021; Springer: Cham, Switzerland, 2021; pp. 81–89.
17. Alkhateeb, A.; Catal, C.; Kar, G.; Mishra, A. Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review. Sensors 2022, 22, 1304.