Exploration on Practical Teaching of Blockchain Technology on Ethereum Platform

Liuping Feng(✉), Lifang Yu, Wenqiu Luo, and Zhihong Dong

School of Information Engineering, Beijing Institute of Graphic Communication, Beijing, China
{lpfeng,yulifang,luowenqiu,dongzhihong}@bigc.edu.cn

Abstract. In order to meet the demand for blockchain talents, this paper explores the practical teaching of blockchain technology. Taking Ethereum as the platform and combining the application of blockchain technology in the field of digital copyright protection, we guide students to conduct research projects, so that students have a deep understanding of some abstract concepts of blockchain and master the methods of blockchain development.

Keywords: Blockchain · Ethereum · smart contract · Practical teaching · Digital copyright protection

1 Introduction

Blockchain is a distributed ledger for transactions. However, Blockchain technology is currently being successfully applied not only financial markets, but also quite a few non-financial applications, such as education, medical care.

China's spending on blockchain technology will see rapid growth in the coming years to reach over $2 billion in 2023, a report by global market intelligence firm IDC showed. The country's expenditures on blockchain technology will see a compound annual growth rate of 65.7% from 2018 to 2023, the company estimated [1].

With the development of blockchain technology, the demand for talents is also growing. Consulting firm Gartner estimates China is facing a talent gap of more than 750,000 people in blockchain technology [2]. However, many universities have not set up blockchain majors, or have no plans to cultivate blockchain talents.

Blockchain technology is not a single information technology, it is an integrated innovation of mathematics, cryptography, computer science and even social science. Blockchain covers a variety of technologies, and the related concepts are easy to be confused, and there are many application scenarios, which brings certain difficulties to the teaching of blockchain. Blockchain technology is highly practical, involve a lot of content and develop rapidly, which is a challenge to teaching.

Without practical teaching, students often cannot fully understand the complex technical structure and lack the ability of application and practice. For the blockchain technology and application course, practice can enable students to quickly master the blockchain theory system and its application scenarios [3].

X. Yuan et al. (Eds.): ICEKIM 2023, AHCS 13, pp. 631–639, 2023.
https://doi.org/10.2991/978-94-6463-172-2_67

Beijing Institute of Graphic Communication is characterized by printing and publishing. This paper discusses the blockchain practice teaching mode, taking Ethereum blockchain as the platform and combining digital copyright protection technology, to guide students to carry out research projects.

2 Blockchain Technology and Digital Copyright Protection

2.1 Blockchain Structure

Blockchain is a chain structure that combines data blocks in sequence (as shown in Fig. 1). Block is the basic unit of blockchain. Each block consists of block head and block body. The block head stores the PrevBlockHash, TimeStamp, Nonce, Merkle Root, etc.; The block body contains the complete transaction information of a block, which is organized together in the form of Merkle tree.

Each block contains the Hash value of the previous block PrevBlockHash, which is continuously linked, it can well ensure that the information on the chain will not be modified. Once the information of one block is modified, it will not pass the verification of the next block, and the modified information will not be certified.

1) **Consensus mechanism.**

Blockchain is a decentralized distributed structure and consensus mechanism is the core technology of blockchain. In the process of information transmission and value transfer, the consensus mechanism solves and ensures the consistency and correctness of every transaction on all accounting nodes. Common consensus algorithms in blockchain include POW (Proof of Work), POS (Proof of Stake),

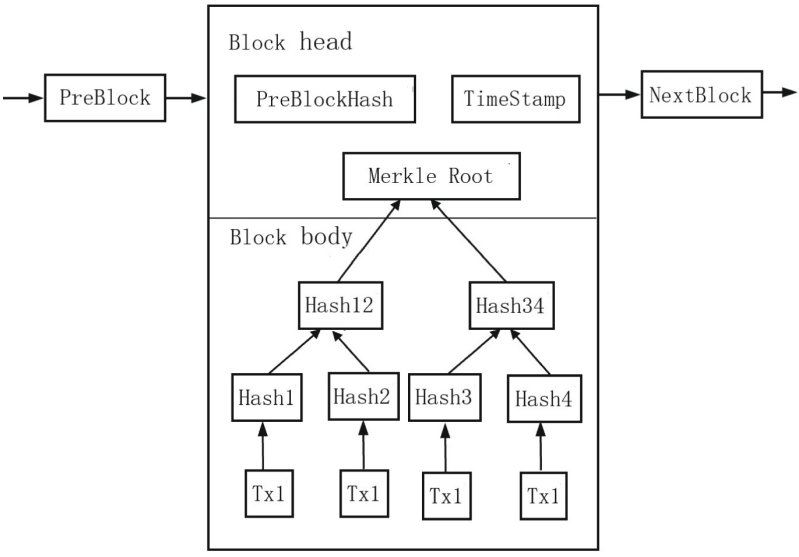

Fig. 1. Blockchain structure

DPOS (Delegated Proof of Stake), PBFT (Practical Byzantine FaultTolerance), and RAFT.

Each algorithm has its own advantages, which are adopted in a specific environment and time period. For different blockchain scenarios, the appropriate algorithm is the best algorithm.

2) **Smart contract.**

Smart contracts are can automatically execute some predefined rules and terms based on trusted and tamper proof data on the blockchain. When the pre-defined rules are met, the agreement is automatically enforced. The smart contract code verifies and enforces the performance of an agreement or transaction.

2.2 Ethereum Platform

Although there is no essential difference between the core of Ethereum and Bitcoin system, Ethereum has fully implemented the smart contract function, making the blockchain technology go beyond the application limitations of currency and adapt to more application scenarios. Therefore, we use Ethereum to guide students to conduct blockchain research.

1) **Account.**

An account is the basic unit of Ethereum. It is an entity with an Ethereum balance. It can send transactions on Ethereum. It can be controlled by users or deployed as a smart contract. Each account has a 20 bytes address.

The accounts of Ethereum blockchain can be divided into two types: external owned account (EOA) and contract account (CA).

2) **Transaction.**

An Ethereum transaction refers to an action initiated by an external owned account. The transaction includes the receiver of the message, the signature to confirm sender, the Ether account balance, the data to be sent, and two values called startGas and gasPrice.

3) **Transaction cost.**

Ethereum introduced the Gas mechanism in the transaction execution to quantify the complexity of the transaction and ensure fairness. Every transaction on the Ethereum blockchain will incur a cost, which Gas is the measurement unit of computing resources on the Ethereum platform. Once the Gas is exhausted, the contract will be terminated.

2.3 Digital Copyright Protection Based on Blockchain

The blockchain can record the release and use of digital works, prove copyright ownership, conduct copyright transactions, effectively restrict the use of works through smart contracts, and ensure that creators can obtain the benefits of works (as shown in Fig. 2). [4]

Firstly, the blockchain technology can provide the copyright owner with identification and copyright proof through timestamp and Merkle tree, so as to realize the traceability of the whole process of digital copyright; Secondly, the blockchain technology can solve the problem of data consistency between digital rights trading network

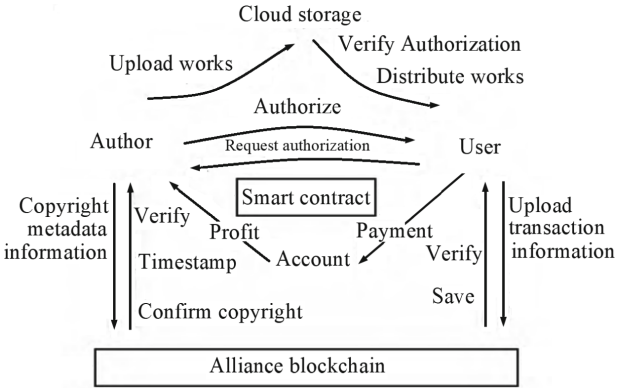

Fig. 2 Basic framework of digital copyright protection

nodes through the consensus mechanism to ensure the credit of digital rights trading; Finally, smart contracts can set rules in advance, reduce human intervention in the trading process, and enhance the transparency of digital copyright trading information.

Many foreign companies, such as Monegraphy, DECENT, and Colu, use the blockchain to help copyright owners achieve copyright protection and transactions, and obtain the rights and interests due to the distribution of works. Many domestic enterprises have also carried out this work. For example, Baidu has launched a blockchain-based stock photo service Totem. According to CoinDesk, it uses blockchain that's been named PicChain to timestamp and verify submissions for photographs in real time to make sure that they are original submissions [5]. Tencent uses blockchain technology to establish an tamper proof digital certificate. The Hangzhou blockchain judicial system developed by Alibaba's Ant Financial Services team has been launched.

The academic literature on the blockchain application of copyright protection mainly focuses on the basic theory of content distribution, tracking and copyright trading of various digital works. We can feel the prospect for blockchain application in the field of copyright protection.

3 Practice Teaching of Blockchain

In recent years, we have carried out research on blockchain based copyright protection projects, and combined with these projects, we have carried out practical teaching of blockchain technology for students.

3.1 Research on Consensus Algorithm

1) **Basic consensus algorithm.**

In order to make students understand the operation mechanism and basic consensus algorithm of blockchain, we guide students to establish a blockchain model with GO language, and implement the consensus algorithm.

Firstly, students installed the GO language development tool Goland on the Windows system and configured the environment variables. For the configuration of environment variables, it needs to be completed patiently. When students encounter errors in environment configuration, they need to find solutions to problems. In this process, they have developed their practical ability.

On this basis, students established a blockchain system and implement PoS consensus algorithm. In this process, students need to learn some new knowledge, such as how to establish and add mining nodes, the role of coin age, and how to conduct virtual mining. Through the learning of these knowledge, students have a basic understanding of blockchain and consensus algorithms, and at the same time, they have also developed their ability to learn independently.

Furthermore, students implemented consensus algorithms such as RAFT, PoS and PBFT.

2) **Improvement of consensus algorithm.**

The core of blockchain technology is consensus algorithm, which ensure data consistency. The PBFT (Practical Byzantine Fault Tolerant) algorithm is a consensus algorithm widely used in the alliance blockchain, but it has problems such as high communication overhead and consensus time extension, which cannot meet the needs of digital copyright protection. Therefore, we guided the graduate student to improve the original PBFT consensus algorithm.

On the basis of the original PBFT algorithm, the voting mechanism is introduced, and the master node is selected from the consensus nodes to dominate the consensus process, so as to ensure the reliability of the consensus results to the greatest extent. And the consensus process of PBFT algorithm is optimized. The consensus process is simplified into three stages, which reduces the complexity of the algorithm and improves the efficiency of consensus.

The improved PBFT algorithm has good performance in communication overhead and consensus delay. With the increase of the number of nodes in the traditional PBFT algorithm, the interaction between nodes also increases, so the time to reach consensus is also increasing. The improved PBFT algorithm classifies nodes, under the same number of nodes, the number of nodes for consensus is less than that of the traditional PBFT algorithm. Although the number of nodes increases, it will have an impact, but the overall consensus time is relatively stable.

Therefore, when the number of nodes is relatively large, the optimized algorithm has more obvious advantages (as shown in Fig. 3) [6] .

3.2 Realization of Smart Contract

The smart contract deployed on Ethereum is a program that runs in EVM (Ethereum Virtual Machine). The program can automatically perform operations according to certain rules agreed in advance.

MetaMask is a browser plug-in used as Ethereum wallet. Ganache is a rapid development tool provided by Truffle Suite for decentralized applications built on Ethereum. Users can deploy contracts, decentralized applications and program debugging on Ganache.

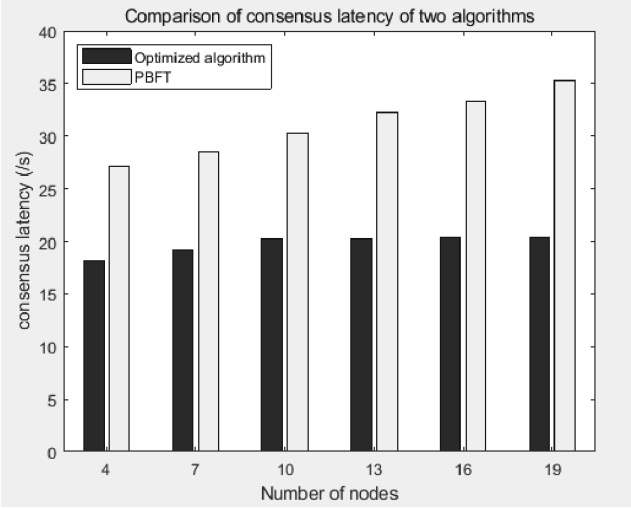

Fig. 3 Consensus delay comparison of two algorithms

In order to make students familiar with the development of blockchain applications on Ethereum, we have designed several topics, such as decentralized microblogging, voting system based on Ethereum blockchain, etc. In combination with digital copyright protection, we have designed the topics of copyright storage system on Ethereum, the digital copyright protection system based on blockchain.

For example, the students have developed a copyright certificate system on Ethereum. The smart contract model uses the Ganache private chain and connects the metamask wallet plug-in through the private key of the account. The system includes the front system and the back system. The front system uses the Web3.js framework to interact with the contract. The back system uses Solidity language to program contract code.

Firstly, the students learn to build a local Ethereum private network based on Ganache and Metamask. Through Ganache, the students can view the current status of the account, including address, private key, transaction and balance (as shown in Fig. 4). The abstract blockchain concepts are presented to students in a vivid form, which stimulates students' interest in project development.

Then, they use Solidity language to program the smart contract, and compile the smart contract (as shown in Fig. 5). After the smart contract is compiled, the corresponding bytecode is obtained. Only bytecode can be run on the Ethereum virtual machine, and the generated bytecode file will be stored in the build folder. Through this operation, students have a further understanding of such abstract concepts as virtual machine and bytecode.

After the compilation, complete the deployment of the smart contract through the "shuffle migrate" command (as shown in Fig. 6). After the smart contract is successfully deployed, the corresponding migration script will be generated in the migrations folder. When deploying the contract, Gas will be paid by default Account 0. Entering Ganache,

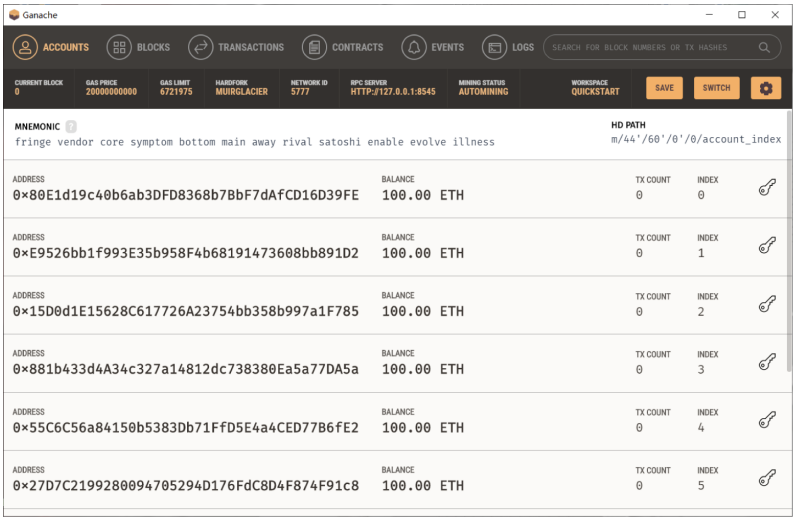

Fig. 4. View the current status of the account

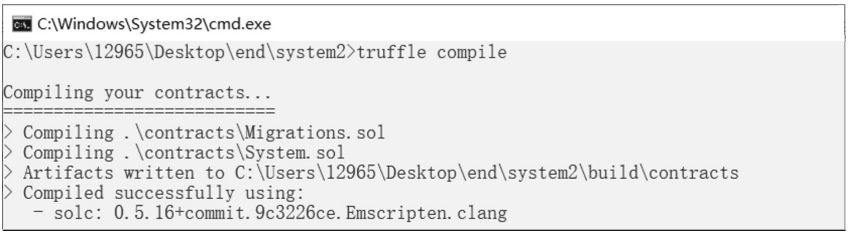

Fig. 5. Compilation of smart contracts

the students found that the 100 test coins in Account 0 were less, so they had a deep understanding of the Gas concept.

Furthermore, a decentralized digital copyright protection application platform is completed on Ethereum. According to the actual needs, the user login module, digital content management module, and other functions are designed and developed using smart contracts. Use the Truffle framework to program smart contracts to realize various functions required by the copyright protection system, and present various data with a visual front interface.

Through these topics, students mastered the design and programming of smart contracts on Ethereum.

3.3 Teaching Case Library

In order to carry out practical teaching of blockchain technology, we have established a teaching case library. Take scientific research and teaching achievements as source materials, and strive to combine theory with practice. The teaching case base has played

Fig. 6. Deployment of smart contracts

an active role in blockchain teaching, improving students' practical ability and enriching their academic quality. During the epidemic situation, through case base teaching, students are guided to carry out project research, and good results are achieved.

4 Conclusion

In order to adapt to technological development and social needs, this paper explores a practical ability training model driven by research topics. Through practical teaching, students are guided to carry out blockchain research, which enables students to have a deep understanding of blockchain technology, effectively improves the depth and breadth of students' scientific research, and greatly improves their engineering practice ability.

Acknowledgements. This paper is supported by the Discipline Construction and Graduate Education Project of Beijing Institute of Graphic Communication (No. 21090122013)

References

1. Xinhua. China blockchain spending to surpass $2B in 2023. China.org.cn/business/2019–11/11/content_75394040.htm.2019–11–11.
2. Su Xinbo. China's blockchain industry embraces influx of young talents. https://news.cgtn.com/news/2021-05-04/China-s-blockchain-industry-embraces-influx-of-young-talents-ZYPKpIUAo0/index.html. 2021–05–4.
3. H. Sun. Exploration of interdisciplinary practical courses under the background of new engineering -- Taking the course *Blockchain Technology and Application* as an example. Journal of Higher Education. 2020(04): 75-77.

4. L. Jiang. Research on Digital Copyright Protection and Knowledge Resource Sharing Mode Innovation in “Web 3.0” Era. Library Work and Study. 2022, 318: pp.65–69
5. Kishalaya Kundu. China’s Baidu Launches Blockchain-based Stock Photo Service ‘Totem’. https://beebom.com/china-baidu-blockchain-totem .2018–4–12.
6. G. C. Yuan, L. P. Feng, J. Ning, X. Y. Yang. Improvement of Practical Byzantine Fault Tolerant Consensus Algorithm Blockchain. Proceedings of IEEE 3rd International Conference on Frontiers Technology of Information and Computer. 2021