Exploration of Blockchain Teaching Based on Case Library and Project Driven

Liuping Feng[a]*, Lifang Yu[b], Zhihong Dong[c]

{*Corresponding author: [a]lpfeng@bigc.edu.cn, [b]yulifang@bigc.edu.cn, [c]dongzhihong@bigc.edu.cn}

School of Information Engineering, Beijing Institute of Graphic Communication, Beijing, China

Abstract. In the teaching process of blockchain, in order to enable the students to quickly grasp the basic knowledge and key technologies of blockchain, this paper adopted case teaching, which is a practical teaching mode to deepen students' theoretical knowledge and cultivate their ability to solve problems. This paper decomposes the knowledge points of blockchain technology and establishes a case library. Students can use the case library to quickly grasp the basic knowledge of blockchain. Combining graduation project and utilizing project driven approach, to enable students to master the development of blockchain systems. Through these practical activities, students' programming skills have been improved, and the configuration and development process of blockchain systems has been gained, which has increased their interest in blockchain technology.

Keywords: Constructivism, Active Learning, Blockchain, Case Library, Project Driven

1 Introduction

Blockchain is a cutting-edge technology of information security, which has gradually gained widespread attention from domestic and foreign industry. Blockchain encompasses multiple disciplines such as computer networks, cryptography, mathematics, and even social sciences, and is a comprehensive innovation involving various technologies. Blockchain technology has strong practicality and many application scenarios, such as digital currency, evidence preservation, copyright protection, etc. The development of blockchain is very rapid, and it involves a lot of content. The related concepts of blockchain are abstract and easily confused, which brings challenges to the teaching of blockchain.

Constructivism believes that teachers are not only transmitters of knowledge in the teaching process, but also need to help students construct their knowledge system and cultivate their habit of self-directed learning. Students should actively apply their existing knowledge and experience to create new knowledge frameworks, rather than passively engage in learning. The cultivation of innovation awareness is the key to cultivating students' innovation ability.

Constructivism theory believes that the process of mastering knowledge is the process in which learners actively use their own cognitive schema to construct knowledge in their subjective world through assimilation. The process of students constructing course knowledge is an active one, and guiding students to actively learn can effectively improve teaching effectiveness. The teaching method of allowing students to learn with questions can effectively guide students to actively learn.[1].

ITEI 2023, November 24-26, Zhengzhou, People's Republic of China

DOI 10.4108/eai.24-11-2023.2343550

Constructivism theory has guiding significance for exploration of blockchain teaching, and cultivating students' learning and innovation ability is also an important content of teaching reform.

Case teaching, as a teaching method, has been applied in various fields of teaching practice for many years and has become relatively mature in theory and practical operation. It is a teaching method that combines theory and practice and many people have explored this area. For example, the paper [2] introduces a practical case of introducing Bayesian inference into introductory statistics courses. Through this case study, it was found that students enjoy "real games", which means they enjoy imitating what they will do as professionals.

Project and Problem based Learning (PBL) are some examples of educational approaches that take in account student-centred learning. With project-based learning students work together in teams to solve large-scale open-ended projects[3].

From the perspective of modern teaching theory, case teaching method and PBL can truly shift the teaching mode from teacher centered to student centered. The teaching content not only focuses on imparting knowledge, but also emphasizes students' abilities.

The application of blockchain technology has strong theoretical significance, and also has high requirements for engineering practice and application, which emphasizes both theory and practice. This is consistent with the teaching objectives of case teaching method and PBL. In order to enable students to quickly grasp the basic theories and application technologies of blockchain and apply them to scientific research, this paper explores the blockchain teaching based on case library and project driven.

2 The case library

Case teaching is a teaching method centered on guiding students to participate in practice. It mainly introduces simulated data and system development processes to inspire students to think, interact, summarize, and ultimately achieve the requirement of cultivating students' ability to combine theory and practice. The research of paper [4] is based on three factors: individual students, case analysis expectations, and preference to case materials that affect the effectiveness of case teaching. It attempts to demonstrate and clarify the potential factors that affect students' attitude towards case teaching. The research results show that students' attitude towards case teaching is mainly directly influenced by the factors of preference to case materials. Therefore, the construction of a case library is very important.

2.1 Blockchain architecture

From Bitcoin, which was the earliest to apply blockchain technology, to Ethereum, which first introduced smart contracts in blockchain, to the most widely used alliance chain Hyperledger Fabric, although they have different specific implementations, they have many commonalities in the overall architecture[5].

Taking Ethereum as an example, blockchain can generally be divided into several parts, such as data layer, network layer, consensus layer, incentive layer, and application layer (as shown in Figure 1), among which the data layer, network layer, consensus layer, and incentive layer constitute the basic blockchain structure. The smart contract layer can be said to be unique to

Ethereum. The smart contract layer encapsulates a virtual machine that can execute Turing's complete scripting language, and can be deployed as a smart contract in the Ethereum blockchain to achieve application decentralization.

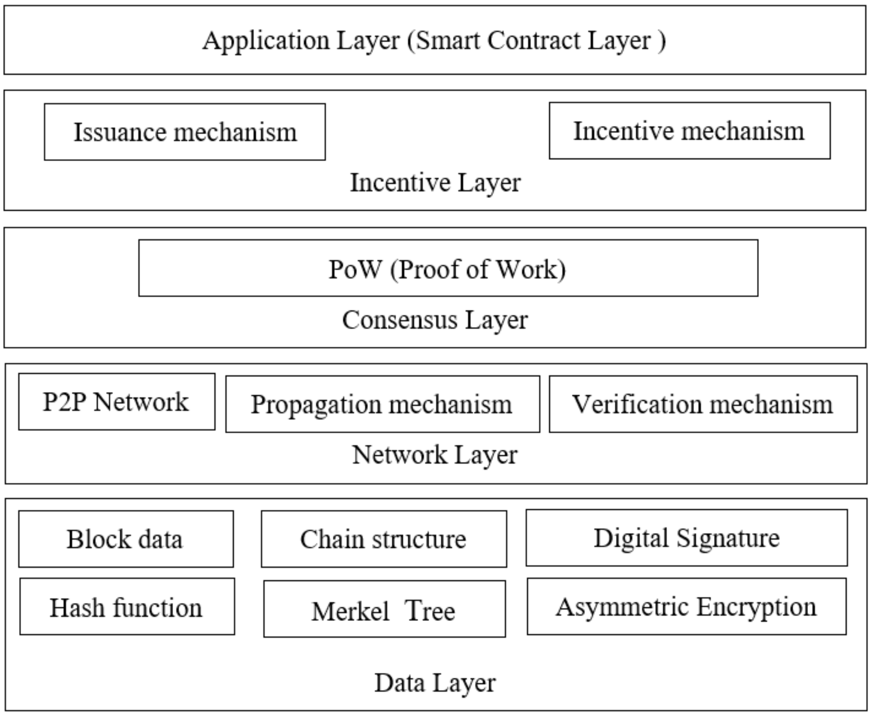


Figure 1. Ethereum blockchain architecture.

At the data layer, Ethereum maintains the correlation of blocks through hash functions and uses MPT (Merkle Patricia Tree) to achieve efficient verification of account status. At the network layer, a decentralized peer-to-peer transmission network is implemented through P2P networks. The consensus layer mainly achieves consensus on transactions and data among all nodes in the entire network. Ethereum adopts two consensus mechanisms, namely PoW (Proof of Work) and PoS (Proof of Stake). The incentive layer mainly implements the issuance and allocation mechanism of Ethereum, and running smart contracts and sending transactions requires paying certain fees. The application layer implements the function of smart contracts by running code through EVM (Ethereum Virtual Machine), adding a front-end interface that can interact with users on the smart contract, forming a DAPP (Decentralized Application).

2.2 Construction of the case library

In order to carry out practical teaching of blockchain technology and enable students to master the basic knowledge and key technologies of blockchain, we have established a teaching case library. Based on the analysis above, we have decomposed the knowledge points of blockchain, mainly including the following aspects:

(1) Basic data structure of blockchain

The structure of a blockchain consists of two parts: a block header and a block body. Figure 2 shows the block structure of Ethereum, where the block header includes the previous block's hash value (PreHash), state root hash value (stateRoot), transaction tree root hash value (TransactionRoot), receipt tree hash value (ReceiptRoot), timestamp (Timestamp), random number (Nonce), etc. The timestamp records the generation time of the block, ensuring its orderliness and preventing tampering with the block data source. The transaction tree root is the Mercle tree root node of the block body transaction information, which stores the transaction information within the block.

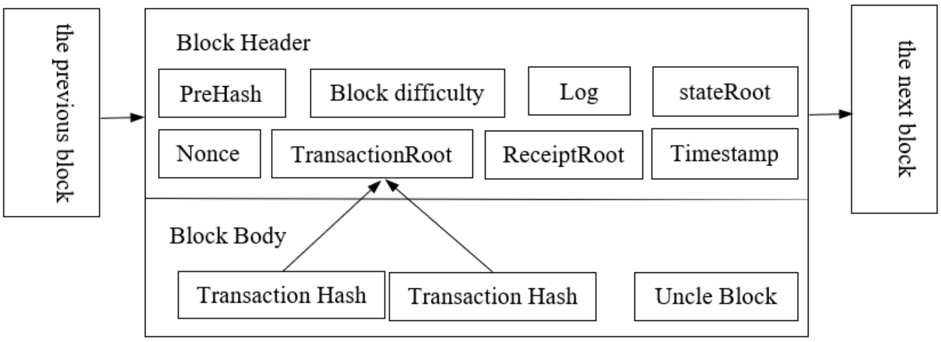


Figure 2. Ethereum block structure

(2) Cryptology Techniques

Cryptography technology is one of the core foundations of blockchain, serving as the underlying support for verification of immutability and decentralized features. In blockchain systems, there are two commonly used cryptographic techniques: hash functions and digital signatures.

(3) Consensus algorithms

Consensus algorithm is the core mechanism and key technology of blockchain systems, aiming to solve the problem of data consistency among nodes in distributed systems. Since the development of blockchain, various consensus mechanisms have evolved, including PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of Stake), and PBFT (Practical Byzantine Fault Tolerant), etc.

(4) Smart contract

Smart contracts are one of the important applications of blockchain technology, which automate the execution and interaction of contracts through programming code. It operates in a decentralized network and does not rely on the trust of third-party institutions, providing more secure, transparent, and efficient trading methods for all parties.

We construct the case library based on these main knowledge points of blockchain. Therefore, the case library consists of the following instances:

(1) Basic blockchain structure

The case library uses Go language to define the data structure of blockchain. In order to help students grasp the principles of blockchain as soon as possible, we have simplified the program without considering the situation of transaction data, that is, we will not process the Merkle tree.

```
type Block struct {    //definition of blockchain header types
   BlockNum  int       //block identifier
   TimeStamp string    //time stamp
   PreHash string      //hash value of the previous block
   HashCode string     //hash value of the current block
   Data string         //transaction data information
   Diff int            //target difficulty coefficient
   Nonce  int          //random number
   root MerkleTree     //MerkleTree root
}
```

On the basis of blockchain knowledge, the definition of Merkle tree is added, and the case library includes content such as the creation of Merkle tree, traversal of Merkle tree, and simulation program for blockchain construction.

```
//Defining the Node Structure of Merkle Trees
type MerkleTreeNode struct{
   Left *MerkleTreeNode
   Right *MerkleTreeNode
   Data []byte
}
```

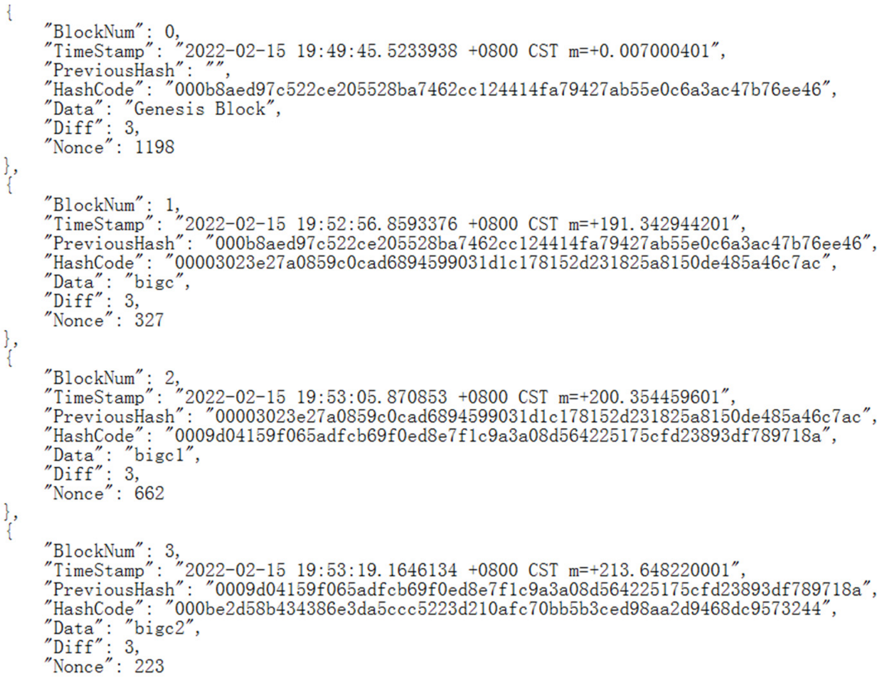
(2) Basic hash algorithm and digital signature algorithm

The hash algorithm instances in the case library include several commonly used hash algorithms such as SHA-256 algorithm, Keccak algorithm, SM3 algorithm, etc. Through learning examples, students can understand the characteristics and algorithm principles of several different hash functions, and understand the meanings of parameters such as message length, group length, and iteration rounds.

Digital signature algorithms mainly include classic algorithms such as ElGamal digital signature algorithm, Schnorr digital signature algorithm, RSA digital signature algorithm, and DSA Algorithm. There are also digital signature algorithms based on elliptic curves, such as ECDSA algorithm and SM2 digital signature algorithm.

(3) Main consensus algorithms

The case library includes several basic consensus algorithms: PBFT algorithm, PoS algorithm, and PoW algorithm. Figure 3 shows an instance of using PoW consensus algorithm under the condition of a target difficulty coefficient of 3[6].



```
{
    "BlockNum": 0,
    "TimeStamp": "2022-02-15 19:49:45.5233938 +0800 CST m=+0.007000401",
    "PreviousHash": "",
    "HashCode": "000b8aed97c522ce205528ba7462cc124414fa79427ab55e0c6a3ac47b76ee46",
    "Data": "Genesis Block",
    "Diff": 3,
    "Nonce": 1198
},
{
    "BlockNum": 1,
    "TimeStamp": "2022-02-15 19:52:56.8593376 +0800 CST m=+191.342944201",
    "PreviousHash": "000b8aed97c522ce205528ba7462cc124414fa79427ab55e0c6a3ac47b76ee46",
    "HashCode": "00003023e27a0859c0cad6894599031d1c178152d231825a8150de485a46c7ac",
    "Data": "bigc",
    "Diff": 3,
    "Nonce": 327
},
{
    "BlockNum": 2,
    "TimeStamp": "2022-02-15 19:53:05.870853 +0800 CST m=+200.354459601",
    "PreviousHash": "00003023e27a0859c0cad6894599031d1c178152d231825a8150de485a46c7ac",
    "HashCode": "0009d04159f065adfcb69f0ed8e7f1c9a3a08d564225175cfd23893df789718a",
    "Data": "bigc1",
    "Diff": 3,
    "Nonce": 662
},
{
    "BlockNum": 3,
    "TimeStamp": "2022-02-15 19:53:19.1646134 +0800 CST m=+213.648220001",
    "PreviousHash": "0009d04159f065adfcb69f0ed8e7f1c9a3a08d564225175cfd23893df789718a",
    "HashCode": "000be2d58b434386e3da5ccc5223d210afc70bb5b3ced98aa2d9468dc9573244",
    "Data": "bigc2",
    "Diff": 3,
    "Nonce": 223
```

Figure 3. Blockchain instance

(4) Smart contract instance

In the case library, the instances of smart contract cases are programmed using Solidity language, which is the preferred language for the development of Ethereum smart contracts. The instances include as electronic voting systems, blind auction systems, secure remote purchase contracts, and micropayment channels.

The case library has played a positive role in blockchain teaching. Based on the construction of the case library, we have compiled two textbooks: "Go Language and Blockchain Development" [6] and "Blockchain Technology and Applications".

2.3 Case based teaching

Constructivism theory suggests that the process of students' learning can be divided into three stages: conflict stage, construction stage, and application stage. In the conflict stage, teachers should actively create problem situations to trigger cognitive conflicts of students, while students actively search for old cognitive structures to lay the foundation for the transformation of cognitive structures; In the construction stage, students analyze, summarize, compare, and reason new problems that arise in conflicts, and use effective learning and thinking strategies to solve conflicts, achieving assimilation and adaptation of the conflict process; In the application stage, students consolidate and improve their new cognitive structure through variant exercises, achieving smooth transfer[7].

According to constructivist learning theory, in case based teaching, we let the students to implement instances of the case library on the Ethereum platform. Firstly, the students learn to build a local Ethereum private network based on Ganache and Metamask[8]. Ganache provides a very simple method for building Ethereum private networks, and through a visual interface, various parameters can be intuitively set, and account and transaction data can be viewed. Metamask is a lightweight Ethereum wallet.

Students can gain a perceptual understanding of the abstract concepts of blockchain and have also sparked interest in learning. For example, by analyzing several examples of smart contracts and demonstrating the language characteristics of Solidity from the shallower to the deeper, students can understand how Solidity writes smart contracts.

Then, students debug and run instances of the case library on the Ethereum platform, and solve the problems encountered through discussion and communication. Through these case studies, students have mastered the basic knowledge and key technologies of blockchain.

Case teaching is a process from theory to practice, and then from practice to theory. Students should first learn relevant knowledge points. Then they will further deepen their understanding through the presentation of instances in the case library, discussion and exchange of ideas. Finally, they should summarize the solutions to such type of problems. Case based teaching enable students to quickly grasp the basic knowledge and key technologies of blockchain.

In the next stage, through project driven practice, students will enter the application stage and develop an application program according to the requirements, which means using these basic knowledge and key technologies to solve practical problems.

3 Project driven practice

The key features of the PBL aim at fostering student-centeredness, teamwork, interdisciplinarity, development of critical thinking and competencies related to interpersonal communication and project management[9]. By learning through projects and teamwork, students move from merely listening and reading about abstract concepts to working with their teammates in applying those concepts in order to solve real-world problems[10].

Therefore, on the basis of mastering the basic knowledge and key technologies of blockchain, combined with the graduation project, project driven practice is carried out.

3.1 Content of practical projects

Graduation project is an important stage in practical teaching and an opportunity to enhance students' ability to solve complex engineering problems. From project requirements analysis to design and development, a series of problems that students encounter will promote the improvement of their abilities. Considering various aspects of blockchain applications, The content of practical projects mainly includes the following options:

(1) Implementation and Analysis of Blockchain Consensus Algorithm

Build a blockchain framework using Go language, implement PoS and Raft consensus algorithms on this framework, analyze and compare their performance.

(2) Design of PBFT Algorithm as Ethereum Consensus Mechanism

Explore the use of more efficient PBFT algorithm instead of PoW algorithm in Ethereum, design and implement an Ethereum consensus mechanism based on improved PBFT algorithm, and analyze its performance.

(3) Design and Implementation of Smart Contracts Based on Blind Signature Technology

Research on smart contracts based on blind signature technology and implement a smart contract model based on blind signature technology to improve the privacy security of smart contracts.

(4) Digital copyright protection system based blockchain

Utilizing the blockchain characteristics of decentralized, tamper proof, and transparent, design and implement a digital copyright protection system on Ethereum, to solve the security problems brought by centralized management of traditional digital copyright protection systems.

(5) Decentralized Weibo based on Ethereum blockchain

Design and implement a decentralized Weibo platform on Ethereum, using blockchain technology to ensure the authenticity and immutability of Weibo information, as well as the traceability of all data and behaviors.

(6) A Voting System Based on Ethereum Blockchain

Design and implement a voting system on Ethereum that utilizes transfer transactions in blockchain to replace the voting process, in order to solve the security problems of existing online voting systems.

3.2 Implementation of the projects

Ethereum and Bitcoin are both blockchain based systems, and there is no essential difference between the core of them. However, Ethereum belongs to blockchain 2.0 and fully implements smart contract functionality. Ethereum is widely used to support complete application development, which enables blockchain technology to adapt to more application scenarios. Therefore, Project driven practice is carried out on Ethereum platform.

Firstly, analyze the requirements of the project. At this stage, students should discuss the project functions and determine a detailed plan for the project. For example, to develop a digital copyright protection system based blockchain. According to the requirements, the students divided the functional modules, and designed login modules, content management modules, content incentive modules, etc.

Secondly, configure the environment for the project implementation platform, namely Ethereum. The digital copyright protection system includes the front system and the back system. On the Truffle framework, students develop, test and deploy the smart contracts to realize various functions required by the digital copyright protection system. The front system interacts with the smart contract using the Web3.js framework and presents various data with a visual front interface. Students need to patiently complete the process of environmental configuration. When they encounter errors and problems, they need to find a solution to the problems. In the process of solving problems, their practical abilities have been enhanced.

Then, the students began writing smart contracts for the backend system. Smart contracts are written in Solidity language, which is the preferred language for Ethereum smart contract development. With the Truffle development tool, smart contract code can be compiled into bytecode, which can be run on EVM (Ethereum Virtual Machine). Through these practices, students have gained a further understanding of abstract concepts such as smart contracts, EVM, and bytecode. They complete project functionality by programming and debugging smart contracts. After the project is completed, they summarize and communicate with each other.

Through the project, students have mastered the process and technology of blockchain development. The implementation of the project has stimulated students' learning interest and subjective initiative. Students are able to actively discuss and think about problems encountered during the project development process, and work together to promote the implementation of the project.

4 Conclusion

Blockchain is a system that involves multiple technologies and programming languages. In order to help students master blockchain technology as soon as possible, this paper decomposes the knowledge points of blockchain technology and establishes a case library to enable students to quickly grasp the basic knowledge and key technologies of blockchain. On this basis, combined with the graduation project, project driven practice is utilized to enable students to develop blockchain systems. Through these practical activities, students' programming skills have been improved, and a comprehensive understanding of the configuration and development process of blockchain systems has been gained, which has increased their interest in blockchain technology.

Acknowledgments. This paper is supported by the Discipline Construction and Graduate Education Project of Beijing Institute of Graphic Communication (No. 21090323010, No. 21090123009).

References

[1] Fengchun Xie: Constructivism and the Teaching of the Basic Theory Courses of Engineering. Research in Higher Education of Engineering. pp151-155 (2010)

[2] Stangl D K.: A Case Study for Teaching Bayesian Methods. Proceedings of the Annual Meeting of the American Statistical Association, August 5-9, (2001)

[3] Fernandes, Goncalves S R.: Preparing Graduates for Professional Practice: Findings from a Case Study of Project-based Learning (PBL).Procedia - Social and Behavioral Sciences, 2014, 139: pp219-226. (2014)

[4] Junhui, G., Xuhua C., and Fuzhong W. : The Exploration of the Optimal Model for Case Teaching Effect. Research in Higher Education of Engineering.pp140-144 (2010).

[5] Qifeng Shao, Cheqing Jin, Zhao Zhang, et al.: Blockchain: Architecture and Research Progress. Chinese journal of computers. Vol 41, No.5, pp969-986(2018)

[6] Liuping F., Lanzhen C., Guichun Y., Tingting L.: Go Language and Blockchain Development. Science Press. (2022)

[7] Qingmei W. , Ge Z.: An Overview on Case Method Researches at Home and Abroad. Journal of Ningbo University(Educational Science Edition), 2009,31(03):7-11. (2009)

[8] Liuping F., Lifang Y., Wenqiu L., Zhihong D.: Exploration on Practical Teaching of Blockchain Technology on Ethereum Platform. Proceedings of the 2023 4th International Conference on Education, Knowledge and Information Management. pp. 631-639 (2023)

[9] Helle, L., Tynjälä, P., and Olkinuora, E. : Project-based learning in post-secondary education - theory, practice and rubber sling shots. Higher Education, 51:2, 287-314. (2006)

[10] Michaelsen, L., Knight, A., Fink, L. : Team-Based Learning. A Transformative Use of Small Groups in College Teaching. Stylus Publishing. (2004).