Achieving Fair and Accountable Data Trading Scheme for Educational Multimedia Data Based on Blockchain

Xianxian Li[1,2], Jiahui Peng[1,2], Zhenkui Shi[1,2(✉)], and Chunpei Li[1,2]

[1] College of Computer Science, Guangxi Normal University, Guilin, China
lixx@mailbox.gxnu.edu.cn
[2] Guangxi Key Lab of Multi-source Information Mining Security, Guilin, China
shizhenkui@gxnu.edu.cn

Abstract. Educational resources have a higher need for copyright protection to avoiding illegal redistribution. The transactions of educational multimedia data resources can effectively promote the development of educational informatization and solve the island situation of educational resources. In the process of traditional transactions for educational multimedia data, there is always a third parties, which may lead to dispute and distrust. And the copyright is not well protected. In this paper, we propose a fair and accountable trading scheme for educational multimedia data. The scheme is based on blockchain to achieve accountability and secure storage with IPFS. And we aim to construct a relatively strong copyright protection model through digital fingerprint and watermark technology. We implemented and evaluated the scheme in Ethereum. The results show that our scheme can achieve well copyright protection and preserve the users' privacy. The overall overhead is reasonable.

Keywords: Blockchain trading · Educational multimedia data · Copyright confirmation

1 Introduction

The era of big data has promoted the development of online education. More and more students would like to obtain knowledge through the Internet. Digital educational resources such as teaching plans, handouts, teaching videos and other multimedia data become the key to the development of online education. The transactions of high quality resources have become one of the effective

The work is partially supported by the National Natural Science Foundation of China (No. 61672176), the Guangxi "Bagui Scholar" Teams for Innovation and Research Project, the Guangxi Talent Highland Project of Big Data Intelligence and Application, the Guangxi Science and Technology Plan Projects No. AD20159039, the Guangxi Young and Middle-aged Ability Improvement Project No. 2020KY02032, the Innovation Project of Guangxi Graduate Education No. YCSW2020110.

X. Yuan et al. (Eds.): QShine 2021, LNICST 402, pp. 111–125, 2021.
https://doi.org/10.1007/978-3-030-91424-0_7

ways to solve the island of educational multimedia data. Educational multimedia resources are easy to be copied. This will lead to them to be pirated easily [1]. Many challenges need to be solved in the transaction of multimedia data in the network, such as the fairness of educational multimedia data transaction, the digital copyright protection after the transaction of educational multimedia data, and the large storage problems of educational multimedia data. It will affect the development of educational informatization to some extent.

Our scheme focuses on multimedia data in the transaction of educational resources, which includes educational audios and videos, teaching plans. Whereas handouts are not considered in our scheme. We summarize the challenges of educational multimedia data transaction as follows:

- **Copyright confirmation:** When the data owner wanted to sell data in our system, he may only want to sell right to buyers to use data instead of data ownership. That is, the data consumers are not allowed to sell data for the second time after getting the data. The data consumers can sell the data again after obtaining the permission of the data owner, who needs to purchase ownership of the data before them can sell the purchased data, otherwise buyers can only have the right to use the data.
- **Secure storage:** Educational multimedia data is mainly based on teaching videos which are generally generated through the whole school year and teaching books. And the contents are very rich. These educational multimedia data need to use large storage resources. It is obviously impractical to store such huge multimedia data directly on the blockchain. And it is also not secure to store in the cloud server because of the dishonest or curious cloud server. There may be security issues [2,3].
- **Reasonable pricing:** In the current scheme of data trading, the price of data is set by the data owner. Unreasonable price will affect the profit of data, the higher price will lead to unsatisfactory data sales, on the contrary, lower price will also affect the income of data owner. Data buyers also hope to have a price negotiation mechanism, which can realize the bargaining process of commodities trading in order to achieve the best balance of both sides.
- **Fair transaction and privacy.** In the traditional multimedia data transaction process, privacy and fairness is an issue that has to be considered. The fairness we mentioned is defined as follows:

- **Real-time.** The data owner obtained the token and buyer got the data completing their act of trading. After the buyer passed the verification, the data owner should obtain the transaction amount corresponding to the data immediately.
- **Independence.** Cheating by one of the parties in the transaction will not affect the other party's benefits negotiated before the transaction.
- **Reasonable rewards and punishments.** Users who have participated in transactions in the system can apply for arbitration for cheating during the transaction. Once it is determined to be cheated, the cheating party will be punished (such as forfeiting the deposit).

As one of the most representative emerging technologies in the 21st century, blockchain has become an indispensable technology for distributed transactions because of its decentralized, traceable and tamper proof characteristics. The use of blockchain technology can help to realize the fairness of the transaction process and can effectively prevent security and privacy issues caused by tampering of transaction data. The role of blockchain technology is not only limited to transactions, but also helps to confirm and trace data rights in the process of transactions. At present, copyright protection works focus on digital fingerprint and digital watermark technology. The digital watermark can confirm the ownership of copyright, and digital fingerprint can confirm the owner of copyright [4]. Combining blockchain and digital fingerprint can help the confirmation work of copyright in the process of transaction more credible.

Our scheme realizes a fair and accountable transaction process of educational multimedia resources, and uses blockchain combined with digital fingerprint and watermark technology to confirm copyright of educational data. In terms of privacy protection, we use the enclave module of SGX to protect the privacy of smart contracts, which protects users' private information, and proves the feasibility of our proposed scheme through efficiency. Our contributions mainly include the following:

- Compared with the previous work requiring the participation of a trusted third party, our scheme uses blockchain technology to realize a decentralized data right confirmation model. The symmetric fingerprint scheme is optimized by homomorphic encryption to protect the privacy of transaction participants, and the process of right confirmation and accountability is completed by smart contract;
- Reasonable pricing model combines with fair mechanism of trading were designed by using smart contract, and our scheme used Trusted Execution Environment SGX to protect users' privacy.
- We implement and evaluate our scheme on Ethereum. The results show the solution works well.

2 Related Work

Blockchain technology was first proposed by Nakamoto in his paper [5] in 2008. The emergence of the first Genesis block marks that blockchain technology has entered the development of Internet, blockchain technology has been developed for thirteen years. Smart contract [6] and the consensus mechanism [7,8] is the key technologies of blockchain. In particular, the use of smart contract makes blockchain not only used for transaction bookkeeping, but also provides blockchain with the ability to deal with complex computer problems, which provides a good technical foundation for the application of blockchain.

Blockchain technology has been used for transactions since its inception, the recent works were more about privacy and security issues in the transaction process [9,11]. For example, [12] uses the anonymous mechanism which is

implemented on the blockchain to protect users' privacy, and the dynamic price negotiation model is implemented by using the Robin Stein bargaining model, and the proxy re-encryption technology is used to realize the secure storage of data. The work is completed by smart contract, but the smart contract has the problem of privacy leakage in the process of public operation because it is publicly executed. The anonymous mechanism is implemented by elliptic curve encryption algorithm, and each execution of the smart contract needs to verify the identity information. So it may be not efficient enough. [13] proposed an auction transaction framework with copyright protection, and blockchain is used to implement the copyright protection protocol. However, the complexity of the protocol is $log(m)$ in the process of right confirmation, and m is the number of users who participated in the transaction. If the number of users is large, the protocol will be inefficient and cannot meet the requirements of actual transaction application scenarios. [14] uses the trusted execution environment SGX combined with blockchain technology to implement a secure transaction scheme. The scheme puts the smart contract into Software Guard Extensions (SGX) for execution, which protects the privacy of sensitive information of the smart contract. SGX is responsible for outputting the final result, while the execution process is confidential to all participants.

The main current works of copyright protection are through digital fingerprint and watermark. Digital watermark technology can confirm the ownership of copyright, but it can not confirm the responsible person in the process of piracy tracking [15]. On the contrary, digital fingerprint technology can determine the owner of copyright which can be divided into three kinds: symmetric fingerprint [16], asymmetric fingerprint [17] and anonymous fingerprint [18]. Symmetric fingerprint may lead seller to frame the buyer, while the asymmetric fingerprint refers to the asymmetric encryption technology to solve the problem of anti frame, and the anonymous fingerprint realizes the identity hiding on the basis of the asymmetric fingerprint. In copyright protection aspect, there are some work combined with Digital Rights Management (DRM) system [19–21]. But DRM system is a centralized management system, privacy information may be tampered by administrator. Meanwhile, DRM system will charge the management fee, which will add the transaction cost to a certain extent. In the copyright confirmation work, we hope to achieve a copyright management system without the third party, which can protect users' privacy and finish the transaction with fair process.

Due to its technical characteristics, the copyright protection work of blockchain technology combined with digital fingerprint and watermark is less. The representative work is the work [22] which used zero knowledge proof, protocol of oblivious transfer, secret sharing and digital watermark technology to realize data tracking. This work can still track the copyright in the case of partial data leakage. However, it used many encryption technologies, the scheme is inefficient in the case of large volume data. It can not be applied to the scene of multimedia data which is large. [23] uses local sensitive hashing and traditional hashing technology to achieve copyright detection, but this work introduces a

third-party organization for copyright confirmation, which deviates from our efforts to achieve the copyright confirmation without the third party. [13] as we said before, because it needs to compare with all the users participating in the transaction in the detection process, it can not be applied to the actual scenarios.

To sum up, there is a lot of work on the blockchain transaction, but there is little work on the data right confirmation in the transaction process. Copyright protection researches have been carried out for many years, and digital fingerprint and watermark technology have been mature. How to combine the blockchain technology with digital fingerprint and watermark technology to realize a data transaction scheme with right confirmation can help solve the increasingly obvious piracy in the process of trading for educational resources, so as to improve motivation of resources providers and promote a better and faster development of educational informatization.

3 Proposed Framework

3.1 Preliminaries

Blockchain and Smart Contract: Blockchain technology [24] is widely used in data transactions due to its decentralized, tamper-proof, and traceable characteristics. Blockchain is a distributed shared ledger and database, which can effectively solve the problem of information asymmetry, and achieve collaborative trust and concerted action among multiple subjects.

Smart contracts are a computer program that automatically executes after setting predetermined rules and terms. It is used to process transaction steps in the blockchain, which was the key to the development of blockchain to the 2.0 stages, which can help blockchain to realize more complex program and provide a good foundation for large-scale application to real scenes.

Bilinear Map: Suppose there is a mapping e: $G_1 \times G_2 \rightarrow G_t$ is bilinear map, it has properties as follow:

- There is the same order g which is shared by G_1 and G_2.
- If there have $x, y \in \mathbb{Z}_q$ and $g, q \in G_1$,$e(g^x, q^y) = e(g, q)^{xy}$ can be calculated correctly.
- If there have g belong to G_1 and q is generated by be G_1,e(g,q) is generated by G_2.

Homomorphic Encryption: Using the Homomorphic Encryption [25] base on RSA, which can perform operations without decrypting them. When give the key K, it satisfies: $H(Enc(M_1, M_2)) = Enc(f(M_1, M_2))$, where H() and f() can be seen as the addition and multiplication operations. Let $\otimes$ and $\oplus$ represents addition and multiplication operations. For $\forall x, y \in$ prime field ψ_q,$x \otimes y \stackrel{def}{=} xy$ mod q and $x \oplus y \stackrel{def}{=} x + y$ mod q.

Diffie-Hellman Key Exchange Protocol: Diffie-Hellman key exchange protocol can exchange secret keys in non-secure channels for encrypting subsequent communication information.

- **Setup:** In order to exchange the shared secret key, both parties of the exchange rely on a finite cyclic group G and the generator g of the group, and both parties also need to generate random numbers x and y respectively.
- **Exchange:** Alice generates a random number x and sends g^x to Bob. Similarly, Bob generates a random number y and sends g^y to Alice. Alice calculates $Key_{AB}Y_{B^x}(modp) = (g^y)^x modp$ and Bob calculates $Key_{BA}Y_{A^y}(modp) = (g^x)^y modp$, where p is a large prime number.
- **Verify:** Both parties judge whether they have received the correct parameters by calculating $Key_{AB} = Key_{BA}$.
  The Diffie-Hellman key exchange protocol can effectively solve the problem of safe key transmission in the transaction process and further enhance the reliability of the transaction.

Trusted Execution Environment: Intel Software Guard Extensions (SGX) [26] are currently under investigation in the area of privacy protection. SGX provides a hardware environment where code runs in a memory area known as an enclave. SGX is currently used to perform some privacy protection for smart contracts which involved sensitive information [27].

IPFS: InterPlanetary File System is a File System that enables distributed storage of large files, with technical features that are faster, more secure, and more open. The goal of IPFS protocol is to replace the traditional Internet protocol HTTP and store large files on IPFS in the system. Blockchain only stores the address hashes returned by IPFS. The integration with blockchain technology can effectively reduce the pressure of storage on blockchain [27].

RobinStein Model: In 1982, Rubinstein proposed the bargaining model of alternating offers [28], which belongs to the cooperative model of game. The simplified scenario assumes that there are two players 1 and 2 who shared the cake with a size of 1 unit. 1 moves first and puts forward the allocation plan, which is called "bid first". 2 then chosen to accept or reject the proposal proposed by 1 after finishing step. If the proposal is rejected, 2 will propose his own proposal of allocation, which is called the "counter-offer" of 2, and then 1 will consider whether to accept it or not. If 1 accepts, the game is over, otherwise 1 bid again,..... , until one party's offer is accepted by the other.

3.2 The Overview of Our Scheme

As shown in Fig. 1, our framework consists of five entities: Schools/Teachers, Data Buyers, SGX enclave, smart contracts, and IPFS.

Schools/Teachers (ST): The ST collects and sells educational multimedia data in the system, participates in data processing, stores data, and initiates smart contracts for data transactions to complete the transaction process.

Data Buyers (DB): The DB searches the data in the blockchain network according to the data description to meet the purchase requirements, then purchases the data, verifies the data and completes the transaction process.

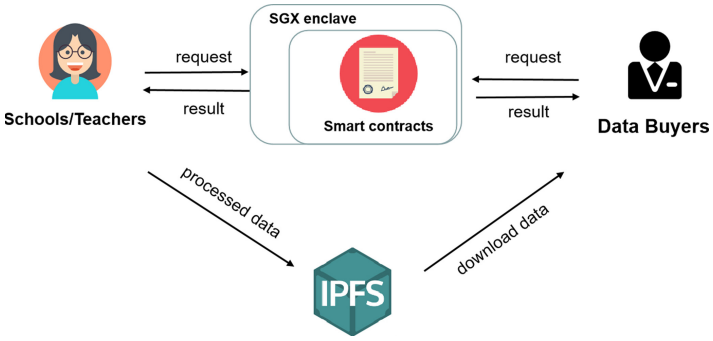

Fig. 1. System framework

Smart Contract: Smart contract completes the execution of the steps of the transaction process. Our scheme includes the following smart contracts:

- **Query:** The DB searches for data that met the requirements.
- **Bargaining process:** Execute the process of ST and DB's bargaining game on data price, in which each bid is protected by SGX to protect the privacy of both parties, in order not to be cheated after the other party knows its price.
- **Data trading:** Perform fair steps of data transaction.
- **Transaction receipt store:** Perform transaction receipt store.
- **Private key verification:** Smart contract uses zero knowledge proof to verify whether the private key of DB meets the transaction requirements. It should be noted that because there are many secret keys in system, using zero-knowledge proof can quickly identify whether the private key meets the requirement.
- **Piracy detection:** Fingerprint comparison of pirated multimedia data to determine if there is a piracy behavior.

SGX Enclave: Since the execution of smart contracts is public, enclave is used to help prevent privacy issues during the execution of smart contracts and to prevent cheating during transactions.

IPFS: Distributed storage of large-capacity educational multimedia data. After the storage is complete, return an address hash to smart contract for saving.

4 Our Fair and Copyright-Preserving Data Trading Scheme

This section elaborates on our fair and copyright-protected data transaction framework. Table 1 lists the symbols used in scheme and their specific meanings. Figure 2 shows the workflow of our scheme.

Table 1. Symbols appearing in the scheme and their explanation

Symbol	Description
FP_{ST}	ST's fingerprint
FP_{DB}	DB's fingerprint
dep_{ST}	ST's deposit
dep_{DB}	DB's deposit
PK_{ST}	Public key of ST
SK_{ST}	Secret key of ST
PK_{DB}	Public key of DB
SK_{DB}	Secret key of DB
encFP	DB's fingerprint used private key to encrypt
$Receipt_0$	Receipt required by DB to purchase data
$Receipt_1$	Receipt required for ST to withdraw tokens
Add_{Hash}	Hash of data storage address returned by IPFS
Price	The price of the data

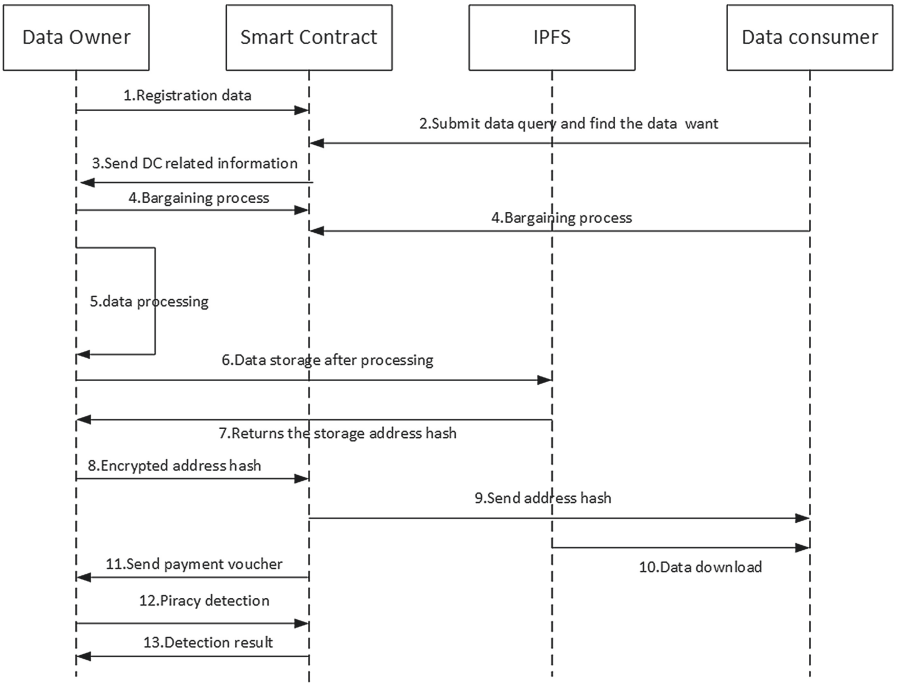

Fig. 2. System workflow

4.1 Participants Registration

If DB wants to buy data in system, he submitted search request to query SC, SC returns the most similar data to DB. Before the transaction, data should be processed as following:

1. ST and DB register in the blockchain network, and obtain a public-private key pair $(PK_{ST}, SK_{ST}||PK_{DB}, SK_{DB})$ issued by the CA center by Bilinear Map by the following formula:$SK = a, PK = a * G$, a is a prime number. The public-private key pair will be used in data processing and transaction processes.

2. If the DB wants to buy data, he should submit the set$\{dep_{DB}, encFP_{DB}\}$ to smart contract, deposit dep_{DB} which is equal to the data price, EncFP_{DB} is the encrypted fingerprint.

3. If the ST wants to sell educational multimedia data, he needs to register in the blockchain and submit the set$\{FP_{ST}, dep_{ST}, price\}$to smart contract.

Before the data is submitted, our scheme allows the price to be agreed as follows:

DB invokes the remote enclave for executing the bargain smart contract. Because our pricing is the priority of the seller, the price at the beginning is set by the seller, which means that the seller always makes the first bid, and each bid of the seller cannot be higher than the price of the previous round. The price offered by the buyer each time cannot be lower than the last price. We define the authentication of the bidding parties as following:

$$Verify_{bar} = (Bid, Hash(Bid), Sig_{SK}(Hash(Bid))) \tag{1}$$

According to Rubinstein bargaining game theory, the perfect equilibrium of the price negotiation between the two parties is calculated as:

$$M = \frac{(1-\delta_2)(S_i^{ST} - S_{i+1}^{DB})}{1-\delta_1\delta_2} + S_{i+1}^{DB} \tag{2}$$

The recommended bidding mechanism for the contract is based on predicting that both parties have enough patience to participate in the data negotiation process, so the selected initial discount factor for both parties is $\delta_1 = \delta_2 = 0.9$.

The recommended price of the smart contract guides the bidder's quote in the next stage to reach the perfect equilibrium price as soon as possible, helping both parties complete the price negotiation efficiently and fairly. When both parties complete the stage of bidding, the discount factor will change, representing that the best balance of the price negotiation between the two parties decreases.

4.2 Data Trading

Setup: ST invokes the remote enclave for trading smart contract execution. ST and DB exchange shared key g^{xy} through the Diffie-Hellman key exchange method, where x and y correspond to random numbers generated by ST and DB, respectively. The ST and DB verify to each other by the shared key which received by each other using formulas 3 and 4.

$$Enc(g^{xy}, Sig(SK_{ST}, H(g^x)||H(g^y))) \tag{3}$$

$$Enc(g^{xy}, Sig(SK_{DB}, H(g^y)||H(g^y))) \tag{4}$$

DB can decrypt x generated by the ST through the random number: $x = SK_{DB} * r^{-1}(mod\varphi(n))$,where $r * r^{-1} \equiv 1(mod\varphi(n))$.

Payment Receipt Generation:

1. Generated payment receipt for DB's purchase data:

$$Receipt_0 = PK_{DO}||Price_{Data}||Time||E_{PK_{DB}}(r)||Hash(r) \tag{5}$$

Where $Time$ is the time when the receipt is generated,$E_{PK_{DB}}(r)$ is the random number r encrypted with the DB's public key, which is generated by the traditional random number algorithm, and $Hash(r)$ is the hash value of the random number r.

2. The DB uses his private key to sign the receipt and send it to the smart contract for transaction authentication.

$$Receipt_1 = Sig(Receipt_0, SK_{DB}) \tag{6}$$

Data Exchange: After the above steps, ST and DB will exchange the data.

1. The ST and the DB should submit deposit dep_{ST} and dep_{DB} for corresponding data price respectively.

2. The DB queries the SC to find the matching data, initiates the transaction request, and confirms the matching ST via the random number x of the Diffie-Hellman key exchange method.

3. The ST initiates the transaction, encrypts the hash value Add_{Hash} of the data address using the shared key g^{xy}, and sends it to SC.

4. DB sends $Receipt_1$ and PK_{DB} to SC.

5. The ST uses PK_{DB} to verify $Receipt_1$ to get $Receipt_0$ from SC, uses SK_{ST} to decrypt $E_{PK_{DB}}(r)$ to get r', and sends r' to SC for verification.

6. SC compares r'with $Hash(r)$, the purpose is to identify the ST. The tokens in the receipt will be sent to the ST account if the verification is successful.

7. The ST confirms the transaction, the SC sends the encrypted address and data hash value to the DB, and the DB decrypts the data, verifies the data hash to confirm the data which he bought, and finally closes the transaction.

8. Both the ST and the DB can initiate arbitration before closing the deal. The arbitration contract validates the process and cheating party will forfeit the deposit.

4.3 Traitor Tracing

Like work [13], we also divide the piracy tracking process into two examples. It should be noted that an ST may correspond to multiple data, but since the fingerprint embedded in each data is unique in our scheme, there is no problem that the fingerprint of each file is different.

Case 1: When a data owner finds illegal pirated data $data_{pira}$ after the trading. He gets the fingerprint FP^* = extract($data_{pira}$). Find the illegal consumer from

on-chain trading records and the request of the corresponding ID user, then gets EncFP_{DB} according to the request, if EncFP_{DB} = Enc(FP^*,PK_{DB}) the consumer is the pirate. Then the seller submits the evidences to the arbiter for accountability. Arbiter verifies the evidences through the Ethereum to make a judgment.

Case 2: When a seller uploads the data hash path to smart contract: data owner downloads the $data_i$ from IPFS. If data owner can detect a encrypted fingerprint FP' that: $FP' = Enc(FP_{ST}, PK_{DB})$ which can show this seller is a pirate because he wanted to resell the data from others.

5 Security Analysis

In this chapter, we will carry out security analysis on the proposed scheme and give corresponding defense scheme against the attack.

Single Point of Failure: Single point of failure refers to the failure or outage of some nodes of the system that affects the operation of the whole system. Our scheme is implemented with pow consensus algorithm for data synchronization, allowing up to 1/2 of the nodes to fail.

Users' Info Security and Privacy: All smart contracts designed for user privacy or affecting the fairness of transactions are executed in SGX Enclave. The transaction parties or other participants can only see the final result of the transaction rather than the data information of the transaction process, which greatly protects the privacy of parties and guarantees the security of the transaction.

Problem of Framing: Our copyright confirmation scheme uses homomorphic encryption combined with digital fingerprint, which is similar to asymmetric fingerprint. In addition, the information of both sides of the transaction is stored on the blockchain to prevent tampering, and there is no case of the seller embedding other fingerprints to frame the buyer.

6 Performance Evaluation

We test our scheme on Ethereum with Intel Core i7 CPU with 16 GB RAM with 1 TB hard drive with bandwidth 50 Mbps and 100 Raspberry Pi Nodes. We tested the efficiency of 1 GB–6 GB of educational multimedia data stored in IPFS to evaluate whether our proposed solution can meet actual needs.

6.1 Smart Contract Efficiency

We tested the gas consumption and execution time of the smart contracts in the Ethereum environment, where we used Ganache to create private chain and maintained the account using MetaMask. Tables 2 shows the execution results and gas costs of smart contracts and Fig. 3 shows the execution time. The 1–6

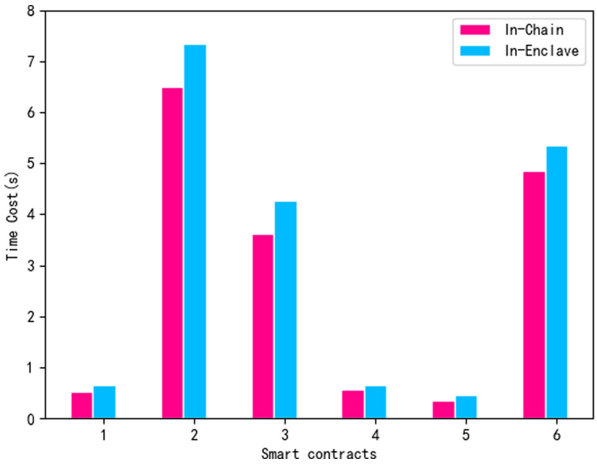

Fig. 3. Smart contracts perform

Table 2. Gas consumption of smart contracts

	Gas used	Gas cost (Ether)
Data query	98525	0.0019
Bargaining process	3029521	0.0589
Data trading	254253	0.0050
Transaction receipt	39558	0.0007
Private key verification	39000	0.0007
Piracy detection	2959512	0.0563

abscissas of Fig. 3 respectively represent the smart contract: Data query, Bargaining process, Data trading, Transaction receipt, Private key verification and Piracy detection. Through the chart analysis, we can know that our scheme meets the efficiency requirements of actual transaction scenarios.

6.2 IPFS Storage Data Efficiency

In order to show the efficiency of IPFS in storing large-capacity educational multimedia resources, we tested the upload speed of IPFS, and the data size of tested was 1 GB–5 GB as shown in Fig. 4. In the evaluation, the upload time of 1 GB compressed data is 16 s, and the upload time of 5 GB compressed data is 68 s. The experiment shows the efficiency and feasibility of using IPFS to store large data. In addition, ours also tested the impact of the number of folders on the storage efficiency of IPFS. Experiments show that the number of folders has little effect on upload speed, and the time efficiency of the impact is within the acceptable range.

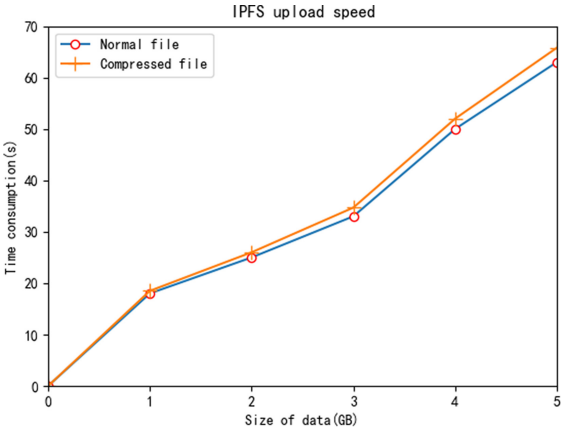

Fig. 4. IPFS upload speed

7 Conclusion

In this article, we propose a fair and accountable educational multimedia data transaction scheme based on blockchain. A detailed solution is designed using Ethereum, smart contract, IPFS, digital fingerprint/watermark technology to provide a safe and reliable educational multimedia data transaction and traceability digital copyright protection scheme. Blockchain technology mainly provides decentralized traceability, using smart contracts to complete the entire transaction process, some transactions using SGX to complete the privacy protection of sensitive information, and testing the feasibility of the entire platform through the implementation of smart contracts. In future work, we plan to continue to improve the platform performance and security.

References

1. Zhao, H.L., Xu, Y.P., Yang, Y.: Technology research of mobile internet digital rights management security authorization. In: Proceedings of the 19th National Youth Communication Academic Conference, pp. 299–309 (2014)
2. Song, H., Li, J., Li, H.: A cloud secure storage mechanism based on data dispersion and encryption. IEEE Access **9**, 63745–63751 (2021)
3. Shi. Z., Fu, X., Li, X., et al.: ESVSSE: enabling efficient, secure, verifiable searchable symmetric encryption. IEEE Trans. Knowl. Data Eng. (2020)
4. Shen, J.: Blockchain technology and its applications in digital content copyright protection. In: Yuan, C., Li, X., Kent, J. (eds.) Proceedings of the 4th International Conference on Economic Management and Green Development. AEPS, pp. 18–25. Springer, Singapore (2021). https://doi.org/10.1007/978-981-16-5359-9_3
5. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Manubot (2019)
6. Mermer, G.B., Zeydan, E., Arslan, S.S.: An overview of blockchain technologies: principles, opportunities and challenges. In: 2018 26th Signal Processing and Communications Applications Conference (SIU), pp. 1–4. IEEE (2018)

7. Fullmer, D., Morse, A.S.: Analysis of difficulty control in bitcoin and proof-of-work blockchains. In: 2018 IEEE Conference on Decision and Control (CDC), pp. 5988–5992. IEEE (2018)
8. Castro, M., Liskov, B.: Practical byzantine fault tolerance. In: OSDI, vol. 99, pp. 173–186 (1999)
9. Li, Z., Kang, J., Yu, R., et al.: Consortium blockchain for secure energy trading in industrial Internet of Things. IEEE Trans. Ind. Inform. **14**(8), 3690–3700 (2017)
10. Gai, K., Wu, Y., Zhu, L., et al.: Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Trans. Ind. Inform. **15**(6), 3548–3558 (2019)
11. Aitzhan, N.Z., Svetinovic, D.: Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans. Dependable Secure Comput. **15**(5), 840–852 (2016)
12. Hu, D., Li, Y., Pan, L., et al.: A blockchain-based trading system for big data. Comput. Networks **191**, 107994 (2021)
13. Sheng, D., Xiao, M., Liu, A., et al.: CPchain: a copyright-preserving crowdsourcing data trading framework based on blockchain. In: 2020 29th International Conference on Computer Communications and Networks (ICCCN), pp. 1–9. IEEE (2020)
14. Dai, W., Dai, C., Choo, K.K.R., et al.: SDTE: a secure blockchain-based data trading ecosystem. IEEE Trans. Inf. Forensics Secur. **15**, 725–737 (2019)
15. Savelyev, A.: Copyright in the blockchain era: promises and challenges. Comput. Law Secur. Rev. **34**(3), 550–561 (2018)
16. Tulyakov, S., Farooq, F., Govindaraju, V.: Symmetric hash functions for fingerprint minutiae. In: Singh, S., Singh, M., Apte, C., Perner, P. (eds.) ICAPR 2005. LNCS, vol. 3687, pp. 30–38. Springer, Heidelberg (2005). https://doi.org/10.1007/11552499_4
17. Charpentier, A., Fontaine, C., Furon, T., Cox, I.: An asymmetric fingerprinting scheme based on Tardos codes. In: Filler, T., Pevný, T., Craver, S., Ker, A. (eds.) IH 2011. LNCS, vol. 6958, pp. 43–58. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24178-9_4
18. Farooq, F., Bolle, R.M., Jea, T.Y., et al.: Anonymous and revocable fingerprint recognition. In: 2007 IEEE Conference on Computer Vision and Pattern Recognition, pp. 1–7. IEEE (2007)
19. Liu, Q., Safavi-Naini, R., Sheppard, N.P.: Digital rights management for content distribution. In: Proceedings of the Australasian Information Security Workshop Conference on ACSW Frontiers 2003-Volume 21, pp. 49–58 (2003)
20. Ma, Z., Jiang, M., Gao, H., et al.: Blockchain for digital rights management. Future Gener. Comput. Syst. **89**, 746–764 (2018)
21. Kenny, S., Korba, L.: Applying digital rights management systems to privacy rights management. Comput. Secur. **21**(7), 648–664 (2002)
22. Huang, C., Liu, D., Ni, J., et al.: Achieving accountable and efficient data sharing in industrial Internet of Things. IEEE Trans. Ind. Inform. **17**(2), 1416–1427 (2020)
23. Chen, Z., Wang, Y., Ni, T., et al.: DCDChain: A Credible Architecture of Digital Copyright Detection Based on Blockchain. arXiv preprint arXiv:2010.01235 (2020)
24. Underwood, S.: Blockchain beyond bitcoin. Commun. ACM **59**(11), 15–17 (2016)
25. Yi, X., Paulet, R., Bertino, E.: Homomorphic encryption. In: Homomorphic Encryption and Applications. SCS, pp. 27–46. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-12229-8_2
26. Brasser, F., Müller, U., Dmitrienko, A., et al.: Software grand exposure: SGX cache attacks are practical. In: 11th USENIX Workshop on Offensive Technologies (WOOT 17) (2017)

27. Bowman, M., et al.: Private data objects: an overview. arXiv preprint arXiv:1807.05686 (2018)
28. Rubinstein, A.: Perfect equilibrium in a bargaining model. Econometrica J. Econometric Soc. 97–109 (1982)