

Blockchain for Digital Rights Management of Design Works

Zihao Lu, Youqun Shi, Rao Tao and Zhaohui Zhang

School of Computer Science and Technology

Donghua University

Shanghai, China

2171739@mail.dhu.edu.cn, {yqshi, taoran, zhzhong}@dhu.edu.cn

Abstract—A design work not only has a complex functional composition, but also has special trading needs. These all result in the difficulties in content protection, copyright protection and the trading of works. To solve these problems, this paper proposes a scheme for digital rights management of design works using blockchain. Unlike existing digital rights management methods, this scheme binds the off-chain design work and its copyright record in the blockchain. The display of design effects, the confidentiality of design details and the compatibility with relevant laws are all taken into account. A new proof-of-delivery method is also proposed to ensure the fairness of the trade. By using smart contracts and public key cryptography, it has no need for active operation from participants in the trade. The scheme is evaluated, analyzed, and compared with other methods from multiple respects to demonstrate its rationality and effectiveness. Finally, a proof-of-concept experiment is described by taking digital garment design as an example.

Keywords—*blockchain; DRM; content protection; smart contracts; proof of delivery*

I. INTRODUCTION

Design work is a description of the designer's intention, which standardizes the manufacturing or construction process. Design works often have high commercial value. However, related legal protection measures are sometimes hard to use. Taking clothing design as an example, the application of the Patent Law and the Copyright Law has limitations such as untimely protection [1], incomplete protection [2], and difficulty in evidence collection [3].

Protecting the rights of design works through digital technology is a good solution. However, digital files are easy to be copied and pirated [4]. It poses new challenges for copyright protection. To protect the copyright of digital content and provide related trading methods, Digital Right Management (DRM) has always been a hot issue in academic and industrial research [5-6].

Most DRM methods deal digital content as one whole item. Digital watermark and encryption are the two mostly used methods. However, due to the particularity of digital design works, these technical means are not fully suitable for design works. If you only add digital watermarks to your design, you can't prevent the leakage of design content. For example, design drawings can be stolen by taking photos. While, if you

encrypt the whole design work, you can't provide useful information to the potential purchaser. This is not convenient for the business. For example, the purchaser may give up buying since he cannot see the design effect.

In addition, DRM methods mostly require owners to upload all the details of the copyrighted content for registration. This approach easily leads to the leakage of important design content and does not provide psychological security for designers [7]. Besides, the practice of providing digital content after payment is sometimes damaging to the buyer's interests, especially when the design work is fake or damaged [8].

Due to the above special characteristics of digital design works, a new technical means is needed for rights management. Blockchain has the nature of decentralization, traceability and a tamper-proof ledger. It has a natural advantage in copyright protection issues [9]. To solve the limitations of the aforementioned laws and technical means, this paper proposes a scheme for DRM of digital design works using blockchain. In the scheme, the methods for copyright registration, query and verification, trading of the works, proof-of-delivery check are all detailed. The digital garment design is taken as an example for illustration.

The rest of this paper is organized as follows: Section 2 introduces base knowledge and related works. Section 3 provides an overview of the proposed scheme. Section 4 presents the method for copyright protection in the scheme. Section 5 presents the trading method for digital design works. Section 6 describes the proof-of-concept experiment and its result. Section 7 evaluates the proposed scheme. Section 8 presents the conclusion and discusses the future work.

II. BASE KNOWLEDGE AND RELATED WORK

A. Design Work

A design work mainly consists of three parts: effect design drawing, structure design blueprint, and specification/working sheet. Take garment design as an example, these three parts are described as follows:

- **Effect Design Drawing:** The visual effect of the design. It is also known as style design drawing.

Sponsored by Natural Science Foundation of Shanghai under grant 19ZR1401900.

Sponsored by Guangdong Provincial Cooperation Innovation and Platform Environment Construction Special Fund of China under grant 2014B090908004.

978-1-7281-0945-9/19/\$31.00©2019 IEEE

- **Structure Design Blueprint:** The description of the opening method and sewing method for a garment clothing piece. It is an essential structural description file for production process.
- **Specification/Working Sheet:** The description of the specific parameters of a garment, such as the size, fabrics used, and proportion of materials. It is an indispensable file for production process.

At present, there are few technical protection methods for design works. Y. Chen and L. Peng studied a copyright protection method for the style design drawing of garments by adding digital watermarks [10]. Further research is needed on the copyright and content protection methods for structure design blueprints and specification/working sheets.

B. Blockchain

Blockchain is a ledger technology that uses chain structure and cryptographic algorithms for distributed data storage [11]. Records in blockchain are difficult to tamper with, but easy to trace.

The smart contract was proposed by N. Szabo in 2008 [12]. It is now an important part of the blockchain technology system, which can automatically perform the preset operations ignoring any human intervention [13]. The application and research of blockchain in various fields have received much attention [14-15].

1) Copyright Protection for Digital Content

Z. Ma et al. proposed a DRM method based on blockchain [16-17]. They also studied the trace method of illegal content and the generation method of image digital watermark. Z. Meng et al. proposed to store the digital watermark of an image in blockchain to implement copyright registration [18]. J. Zeng et al. studied the implementation framework for image copyright registration using consortium chain [19]. PIC-CHAIN, which developed by Baidu, synchronizes the image copyright information in blockchain with Beijing Internet Court so that legal effect can be achieved [20].

Most of these studies are aimed at digital content with a single functional composition. They may not be fully suitable for the protection of digital design works.

2) Trading Methods for Digital Content

D. Roman and K. Vu studied the use of smart contracts for data market [21]. In this method, the buyer needs to prepay the price to a smart contract first, and actively trigger the smart contract to issue the payment to the seller. In such methods, since the buyer is a stakeholder, he is likely to lose the objectivity and enthusiasm for triggering the smart contract. There is room for further optimization.

H. R. Hasan and K. Salah proposed a PoD (Proof of Delivery) method based on blockchain [22]. The method uses a method of joint deposit payment to ensure the credibility of the trading process. This paper will eliminate the need for a deposit and implement PoD for digital design works from a new perspective.

III. OVERVIEW OF THE SCHEME

A. Roles of The Participants

According to the requirements of the participants in DRM of digital design works. The following three types of roles are summarized in this paper:

- **Blockchain Application:** The implementer of the blockchain-based solution, which provides DRM services for other participants.
- **Designer:** The original owner of a digital design work. By using the application, a designer can register works for copyright protection, verify of the copyright information and sell the registered works.
- **Buyer:** A buyer can use the application to conduct copyright inspection and purchase for digital design works that have been registered.

Designers and buyers need to get registration and real-name authentication through the application before they can perform any DRM related operations. A set of public/private key pairs will be generated for each user during the registration.

B. The Framework

According to the needs and resolution logic of DRM for digital design works, it can be divided into two major problems: copyright protection and trading of the works. They can also be further refined into a series of sub-problems. An overview of the functional goals and the techniques used is as follows:

1) Copyright Protection

a) **Copyright Registration:** The designer registers the copyright of his work through blockchain. The credibility, validity, and security of copyright registration can be guaranteed by the tamper-proof nature of blockchain, timestamp, and the anti-collision and unidirectionality of hash algorithms.

b) **Copyright Information Query:** Any user can query the copyright information of a registered work in blockchain. This provides credible reference to potential buyers and relevant regulatory authorities. Due to the traceability of blockchain, users can also view the copyright change history of a specific work. Thus, the legitimacy of the copyright acquisition path can be verified.

c) **Correlation Verification:** A user may submit a work to the application to verify whether it is associated with the work registered in blockchain. This verification will be implemented by verifying the hash of the work.

2) Trading of The Works

a) **Transfer of Ownership:** A Buyer can purchase a digital design work from the designer. Smart contracts are used to monitor buyers' payment and designers' delivery. The contract also acts as an intermediary, who is responsible to receive/issue advance payments and transfer the ownership. Relevant invoices are automatically recorded during the process.

b) *Design Content Protection*: During the delivery, it is necessary to protect the content of works in case of the interception by others. For this, the paper uses public key cryptography to encrypt and protect digital design works.

c) *PoD (Proof of Delivery)*: It is used to prove that the buyer has successfully received the transaction. If verification of PoD is passed, a smart contract will be triggered to issue the payment to the designer. The PoD is implemented by using public key cryptography and the proposed correlation verification method to ensure the fairness of trade.

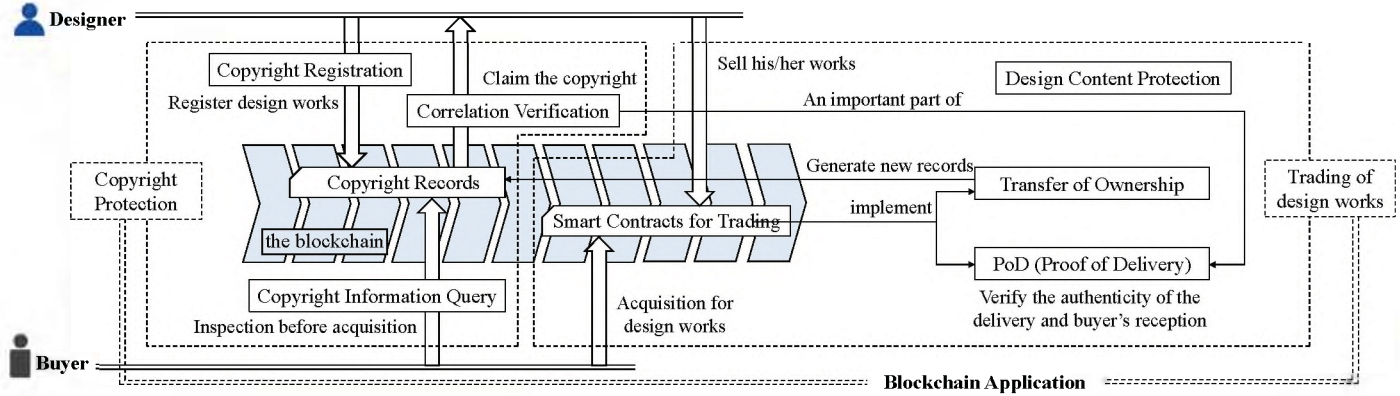


Figure 1. The overview of the proposed scheme

IV. A COPYRIGHT PROTECTION METHOD FOR DIGITAL DESIGN WORKS USING BLOCKCHAIN

This section illustrates the method for copyright protection of digital design works.

A. The Structure of Copyright Records

Based on the requirements of the Copyright Law, the confidentiality of production details and the needs of trading, this paper divides the copyright information into the following five parts. Together, a copyright record can be formed. The record is stored in blockchain.

- 1) *Work ID*: A unique ID assigned for each registered work.
- 2) *Overview*: Information that can be publicly displayed in a design work, including the identity of the designer, the effect design drawing, and the brief introduction, such as the fabric and accessories needed for production.
- 3) *Hash of The Details*: Technical details that need to be kept confidential in the design, including the hash of the structure design blueprint and the hash of the specification/working sheet.
- 4) *Owner*: The identity of the current owner. This identity should have been authenticated by the blockchain application.
- 5) *Invoice for Ownership Authorization*: If the owner is authorized by registration, it is the designer's digital signature for a record that should be stored. The record includes the *Overview*, *Hash of The Details*, *Work ID*, *Owner*. While, if by trading, it is the relevant evidence, such as the ID of the trading contract.

Digital design works can be regarded as special digital assets that require copyright protection. The realization of copyright protection is the premise of trading. For digital design works that are not registered in blockchain, the trading method is beyond the scope of this paper. After the transfer of ownership, query method for the transfer history will return back in the scope of copyright protection.

An overview of the relationship among the three participants, the relationship between the various sub-methods and the functional goals are shown in Fig. 1.

If multiple copyright registrations are performed using the same work, the hash of the details and the effect design drawing in overview will be exactly the same. However, the work ID assigned each time is unique.

Transfer of the ownership will result in a new copyright record. This record is the same with its previous version, expect *Owner* and *Invoice for Ownership Authorization*.

B. Copyright Registration

Copyright records for all digital design works are originally registered by their designers. The workflow is as follows:

- 1) *Generate Hash Digests*: The designer calculates the hash digests of the structure design blueprint and the specification/working sheet by using the application. Then, they are uploaded and recorded as *Hash of The Details*. While the actual files are not uploaded.
- 2) *Upload Copyright Information*: The designer uploads the *Overview* of the work through the application. The designer's identity is used as the initial *Owner* as default.
- 3) *Generate Work ID*: The application assigns a unique ID for each registered work.
- 4) *Sign The Record*: The designer uses his/her private key to generate a digital signature for *Work ID*, *Overview*, and *Hash of The Details*. Then, the signature is stored as *Invoice for Ownership Authorization*.
- 5) *Generate a Copyright Record*: The application puts all the data obtained in the above steps into one record and release it to the blockchain.

The workflow is as shown in Fig. 2.

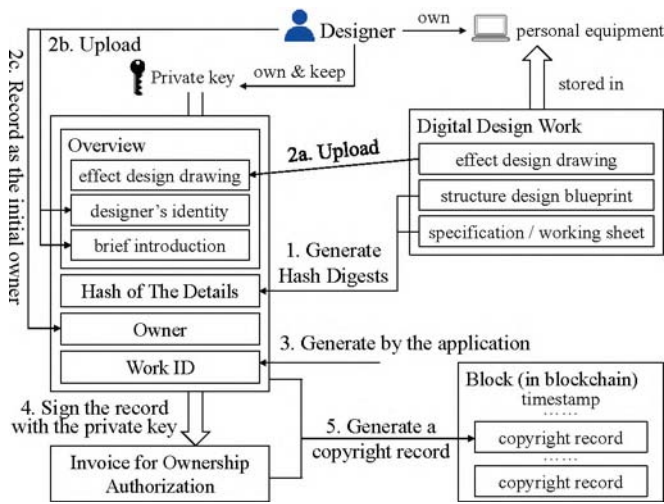


Figure 2. The workflow of copyright registration for a digital design work

C. Query and Verification of Copyright Records

Any user can query for copyright records by work ID. What's more, by tracking all copyright records in blockchain with the same work ID, a path of ownership transfer history can be gained. If the source of the path is consistent with the original registration record, the legitimacy of the acquisition channel can be proved.

Since the detailed design is only stored in the designer's personal device, the reverse calculation is not possible to be done only with the *Hash of The Details* in the blockchain. To deal with copyright verification request from others, like regulatory authorities, the owner can just submit the original files of the work with the *Work ID* in blockchain. By ID, the verifier can query the relevant copyright record in blockchain. After verifying the owner's identity in the record, the verifier can recalculate the hash digests of the submitted files and compare them with the *Hash of The Details* in the record. If the hash digests match, the authenticity of both the files of the design work from the owner and the copyright record in the blockchain can be proved.

The whole process of the authenticity verification for a digital design work is as shown in Fig.3.

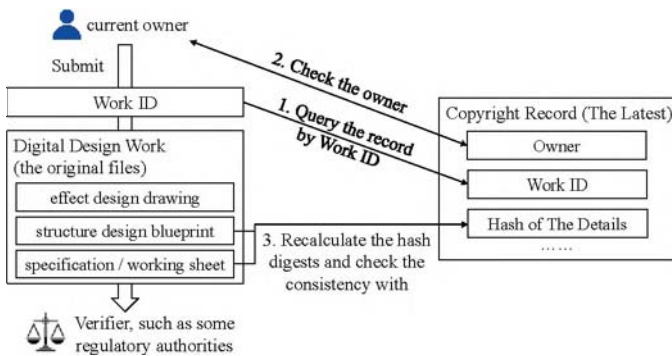


Figure 3. The authenticity verification for a digital design work

V. A METHOD FOR THE TRADING OF DIGITAL DESIGN WORKS USING SMART CONTRACTS

A buyer can purchase registered works from their current owners through smart contracts. The purchase will lead to the delivery of work files and the transfer of ownership.

A. The Workflow

The workflow is as follows:

1) *Reach an Agreement*: The buyer and the seller negotiate about the trading details, such as the work ID, the price, the deadline for seller's delivery, the deadline for buyer's payment and the deadline for buyer's signing for the delivery. These details will be developed into smart contracts for automatic execution. A digital contract with unique contract ID will also be generated.

2) *Payment from The Buyer*: The buyer pays the agreed price to the smart contract.

3) *Notification for Delivery*: After the smart contract receives the buyer's payment, it will automatically record related bank statement as a piece of evidence. Then, the application will notify the seller to deliver the work.

4) *Delivery*: The seller sends the work files to the buyer via the application before the deadline. If the seller fails to meet the deadline, a breach of the contract will occur. This may cause the punishment to the seller.

5) *Notification for Reception*: The application records the hash digest of the delivery into blockchain as evidence. Then, it notifies the buyer to receive the delivery.

6) *Reception*: The buyer starts to get the delivery by submitted his private key to the application. Same with the delivery from the seller, a deadline should be met.

7) *Proof of Delivery*: The buyer's operation to start the reception will trigger the PoD method. Through this method, the buyer's reception and the authenticity of the received files are verified. Buyer's digital signature for the delivery will also be automatically generated and recorded.

8) *Payment Issuing*: If the verification of PoD is passed, the smart contract will be triggered to issue the payment to the seller. Otherwise, the smart contract will turn to operations for violation.

9) *Transfer of The Ownership*: The smart contract releases a new copyright record into blockchain. In this record, the *Owner* will be updated to the buyer, the contract ID will be recorded in *Invoice for Ownership Authorization*, and the rest will remain unchanged.

B. Proof of Delivery with Content Protection

During the delivery process, the seller first encrypts the files for delivery using the buyer's public key. Then, the encrypted files will be sent to the buyer via the application. When the buyer is going to get the delivery, he has to submit his private key to the application first. The files are then decrypted by the application and available for the buyer. At the same time, the application will automatically generate two digital signatures (denoted as *Signature_{on-struct}* and *Signature_{on-}*

tech respectively) for the structure design blueprint and the specification/working sheet in the files using buyer's private key. These two digital signatures will be recorded on the blockchain as an evidence for the reception.

After the operations above, the smart contract uses the buyer's public key to decrypt the signatures so that two hash digests will be obtained. By checking the consistency of the hash digests with Hash of The Details in the copyright record, the authenticity of the delivery can be verified.

According to public key cryptography, the content of the delivery can only be obtained by decrypting it using the buyer's private key [23]. Combined with the principle of digital signature, if the consistency check has been passed, it proves that the buyer has obtained the effective content of the work, that is, the implementation of proof of delivery.

Using the application as an agent to do operations with the buyer's private key can also reduce the using difficulty for non-professional users to a certain extent, just like Libra [24-25].

The proof of delivery method can be implemented by smart contracts, which can be described by the pseudo-code of $PoD()$, as shown in Algorithm 1.

Algorithm 1 Pseudo-code of $PoD()$

Proof of delivery verification based on smart contracts

Input: the work ID of design (ID_{work}),
the buyer's identity (ID_{buyer}),

Algorithm 1 Pseudo-code of $PoD()$

Proof of delivery verification based on smart contracts

buyer's digital signature for the structure design blueprint in the decrypted file ($S_{on-struct}$),
buyer's digital signature for the specification/working sheet in the decrypted file (S_{on-sw})

Output: the subsequent trading operation (O_{PoD}),

- 1: $record_{work} \leftarrow$ query the latest copyright record in blockchain by ID_{work}
- 2: $hash_{struct0} \leftarrow$ the hash digest of the structure design blueprint in recordwork
- 3: $hash_{sw0} \leftarrow$ the hash digest of the specification/working sheet in recordwork
- 4: $PK_{buyer} \leftarrow$ get buyer's public key by ID_{buyer}
- 5: $hash_{struct1} \leftarrow$ decrypt $S_{on-struct}$ by using PK_{buyer}
- 6: $hash_{sw1} \leftarrow$ decrypt S_{on-sw} by using PK_{buyer}
- 7: **if** $hash_{sw0} == hash_{struct1}$ **and** $hash_{sw0} == hash_{sw1}$ **then**
- 8: $O_{PoD} \leftarrow$ issue the advance payment to the seller
- 9: **else**
- 10: $O_{PoD} \leftarrow$ the operation for violation
- 11: **end if**
- 12: **return** O_{PoD}

The whole process of the trading using smart contracts is shown in Fig. 4.

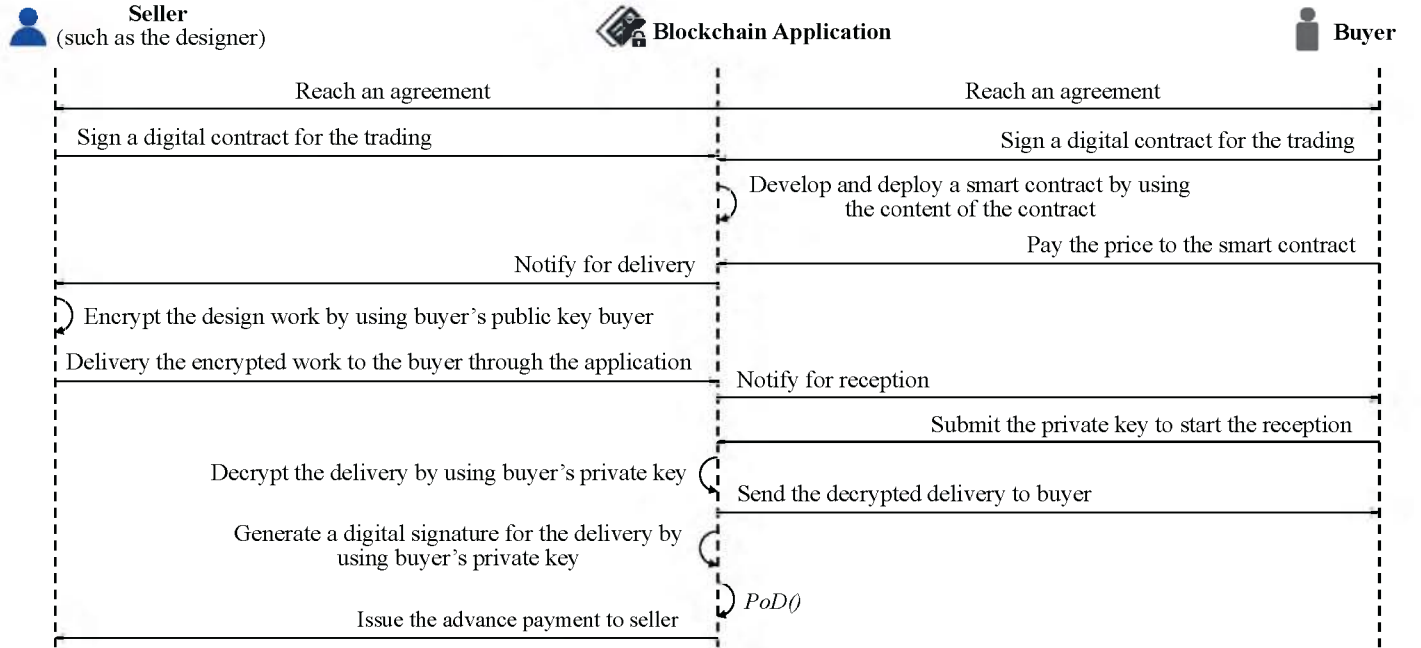


Figure 4. The detailed workflow of the trading method for digital design

VI. ANALYSIS AND EVALUATION

A. The Effect of The Copyright Protection Method

1) *Traceability*: All users can use the unique work ID to query copyright records in blockchain. By collecting copyright

records with the same work ID, a path of ownership transfer history can be gained. That may also help to guarantee the legitimacy of the acquisition channel.

2) *Displayability*: The effect design drawing in the copyright record can provide intuitive effect reference for the potential buyer and relevant supervision department.

3) *Confidentiality*: The Structure design blueprint and specification/working sheet, which contain production details, are only stored in the owner's personal equipment. According to cryptography, the actual content of these two files cannot be gained using only the hash digest in the copyright record. Therefore, the content of the detailed design can be protected.

4) *High Efficiency*: The notarization of the copyright record is achieved by the consensus algorithm of the blockchain. According to the statistics of the National Copyright Administration of the Republic of China, the total number of copyright registrations in China in 2017 was 200,1966 [28]. The 24-hour transaction speed of bitcoin on August 13, 2019, GMT+8 is 3.91 TPS [29]. That means even with the processing speed of bitcoin network, which has relatively a low efficiency, it takes only 5.93 days to complete all the copyright registrations in that whole year. This time is much shorter than the current time needed (about 30 working days) for the copyright registration of a design work through the Copyright Office.

B. Security and Fairness of The Trading Method

The paper demonstrates the security and fairness of the proposed scheme by using the following scenarios.

1) Fake Design Work Delivered

If the digital design work delivered by the seller does not match the copyright record in blockchain, the PoD verification cannot be passed. Thus, the seller cannot gain the payment from the smart contract.

If the seller registers fake information at the time of copyright registration in order to cheat in the verification of PoD, evidence of fraud will be left due to the tamper-proof nature of blockchain. In this case, the buyer can resort to the relevant regulatory authorities with the fake work they have got, the fraudulent record in blockchain, and the seller's digital signature for that fraudulent record. Sellers will be punished for this.

What's more, even if the seller registers a fake design work, real effect design drawing must be used in the registration to achieve the purpose of the sales. The effect design drawing itself has condensed the designer's inspiration and has a certain value. Fake copyright registration records are not protected. This will cost the seller the opportunity to protect his inspiration. Therefore, the combination of the proposed method can guarantee the fairness of the trading. The authenticity of copyright registration can also be encouraged to a certain extent.

2) Repeated Copyright Registration

Registering the same digital design work multiple times will generate different design IDs. Even if the seller repeatedly registers the same design work multiple times, he can never steal the ownership of the work that has been sold. On the contrary, this repeated registration and trading behavior will leave digital evidence of piracy in blockchain.

3) Default in Reception

The buyer needs to submit his private key to the application to get the delivery and decrypt it. Therefore, if the buyer has not agreed to receive the delivery, the real content of the digital design work can never be obtained. Therefore, the security of the work can be ensured. Besides, a deadline for the buyer to sign for the delivery is also set in the smart contract. If the deadline is not met, the default process will get started.

C. Comparison with Other Existing Schemes

In the issue of DRM of digital design works, the comparison among the proposed scheme, the legal protection measures [1-3], traditional DRM schemes [30-31] and blockchain-based schemes for single-functional content [16-20] is shown in Table 1. Traditional DRM methods cannot balance the confidentiality of the details and the displayability.

It can be seen in Table 1 that the proposed scheme has merits in comprehensive performance. In addition, the detailed design work is only stored in the owner's personal device in the scheme, which is more in line with the traditional psychology of secrecy. Therefore, for users who are not familiar with blockchain technology, the proposed scheme may be more acceptable.

TABLE I. THE COMPARISON WITH OTHER EXISTING SCHEMES IN THE PERFORMANCE OF DRM FOR DESIGN WORKS

Scheme to Be Used	The Performance in DRM for Design Works					
	Decentralization	Time consuming	Confidentiality	displayability	Storage of the detailed content	Guarantee of the fairness of the trade
The proposed scheme	High	Low	High	High	Only in personal equipment	The proposed PoD method
Legal protection measures only	/	High	Low	High	Free access to the public	/
Traditional DRM schemes	Low	Low	Low / High	High / Low	Servers of the service provider	Service provider's reputation
Blockchain-based schemes for single-functional content	High	Low	Low	High	Distributed file system, like IPFS	/

VII. IMPLEMENTATION

Since the real-name authentication is a must, according to the research of K. Wüst and A. Gervais, the proposed scheme is more suitable to be implemented on the base of consortium blockchain [26].

Take garment design as an example, this paper carried out a proof-of-concept experiment by using Hyperledger Fabric 1.3 [27]. The results are as shown in Fig. 5 and Fig. 6.


In Fig. 5, the copyright record of a digital garment design work is shown. In the record, the style design drawing is

publicly displayed. While, only the hash digests of the structure design blueprint and specification/working sheet are recorded, not the real files. Meanwhile, the ownership transfer history is also recorded.

In Fig. 6, a part of the log of the trade is shown. This log is recorded in blockchain. It includes the hash of the encrypted

delivery, buyer's digital signature for the decrypted files of the delivery, the payment issuing transaction, and the transfer of the ownership. Each transaction hash in blockchain for all the details above is also shown. These are all important evidence generated when using the trading smart contract and the proposed PoD method.

Copyright Related Information

Work ID	gw731ff1f737f2e04516d1a4c44f1	Category	shirt
Design Work Name	Casual Shirt for Ladies	Fabric	cotton 100%
Registration Time	Tue Sep 10 2019 16:31:09 GMT+0800	Accessory	zipper (resin)
Designer	Tony Wang (310110198810011234)	Current Owner	Tony Wang (310110198810011234)
Style Design		Structure Design	b14c38906cd99bd6a58c6b0ea16ccf7bfaf03aa2881d25552b0d61727154dbc1
		Specification / Working Sheet	635e5d223bcc2aa29e647a46b7cdc932e1c81ce6e93c426b8a01d05a7f6211f8

Ownership Proofs / Transfer History (The Trace)

Time	From	To	Gain Ownership Through
Tx Hash in Blockchain		Designer's Digital Signature / Trading Contract ID	
Tue Sep 10 2019 16:31:09 GMT+0800	----- (-----)	Tony Wang (310110198810011234)	Copyright Registration (With Digital Signature Available)
2d3f27b0795d09141fa85676b1f6e0f54c8d009a6bd6d0e010d93ab997d63913		MEUCIQCH4LtzjBPT0nlfcdWODrqYYQjptZvX8ZrTgTYQPQ9GAlgDXXQsC1gKf9P4RWD6Clw7FWuouS5KCzfvU9uHoAlw3M=	

Figure 5. A copyright record of a digital garment design work

Hash of Encoded Structure Design: cbf0e1de588ac117fb556cb5f80c084212152d693050001c1cc5e6354cb5374a	Prepayment Token: pye9b42c88a037c8b42382f2767d4e1c4a
e6dde3a6b65188581bd589d75f7da66e8681b3741af83758bbe6786012c2b9ea	Statement Tx Hash: 3ab9b8f2daac759ac5dc32caae1bf94abd0a98bf542739f6b29aff2532d4ebca
Hash of Encoded Specification / Working Sheet: 20812bfd154aed623e034c8f3b1bc86d8ca43a0f2fd77dfd16950ff0daf1fdd	3e6d70fd5320db8e2e8e245d798079becc7e8eb5a98ec7c9697e0d2f0eede9
b4d548a264d13073c0cabcc01eb2ad4a2ee54f49459fb48905253845f803d980b	Work ID: gw731ff1f737f2e04516d1a4c44f1
Digital Signature on Structure Design: MEQCIFB1asab29zwm/z1gYCxYaCqwrKt4CNnoCb fPGhx2TiFAiBhW3uqukaQVr0yuPG3iGLKnNAPBp8vhAT324ziIaHS9w==	9f4b296de0d15d7fa0b4a1d27e4b048d09267960c8188c241a050416d1f3cd09
Digital Signature on Specification / Working Sheet: MEUCIQDsqrOhX+fWBNU6mCNlIB h6p8WEN/waoyLZD7dAtqs9DQlgrO5KXYldIRB1xny+W2jMylXm5FU6QR1P9Qi3PXEh3rs =	
f9870757952eaf57264492d62691f2788231e6ace8031375ebc3911c14af2641	

Figure 6. A log of the trading process of a design work using a smart contract and the proposed PoD method

VIII. CONCLUSION AND FUTURE WORKS

This paper proposes a scheme for DRM of design works using blockchain, and elaborates on garment design as an example. Two methods of copyright protection and the trading

are described, which complements each other. In the method for copyright protection, this paper demonstrates the structure of copyright records and sub-methods of the registration, query, and verification of copyright. The analysis shows the method has the characteristics of traceability, displayability,

confidentiality and efficiency. In the method for trading, this paper proposes to use smart contracts to automate the trading process. A PoD method is also proposed by using public key cryptography. After analysis in multiple scenarios, the results show that the method has certain security and fairness.

In addition, a proof-of-concept experiment is carried out. In this experiment, the key points of the proposed scheme are shown in an intuitive way. Through comparison with other schemes, the result shows that the proposed scheme has merits in comprehensive performance and may better satisfy the psychology of secrecy.

In the proposed PoD method, the user needs to submit his/her private key to the application for signing for the delivery and the decryption. Therefore, as the controversy over Libra, which keeps the private keys for its users, the protection of the user's private key should be further studied.

REFERENCES

- [1] L. Wang, "The Status and Improvement of Intellectual Property Protection of China's Fashion Design," *Legal System and Society*, vol. 26, no. 32, pp. 220-221, Nov. 2017.
- [2] J. Long, "Research on Legal Issues Related to Garment Design Copyright," *Market Modernization*, vol. 60, no. 1, pp. 12-13, Jan. 2018.
- [3] L. Zhang, "Innovative Conception of Research on Intellectual Property Protection of Chinese Fashion Design," *Journal of Donghua University (Social Science)*, vol. 15, no. 1, pp. 1-7, Mar. 2015.
- [4] R. Xu, L. Zhang, H. Zhao and Y. Peng, "Design of Network Media's Digital Rights Management Scheme Based on Blockchain Technology," 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), Bangkok, 2017, pp. 128-133.
- [5] L. Guo and X. Meng, "Digital content provision and optimal copyright protection," *Management Science*, vol. 61, no. 5, pp. 1183-1196, May, 2015.
- [6] P. Bellini, M. Mesiti, P. Nesi and P. Perlasca, "Protection and composition of crossmedia content in collaborative environments," *Multimedia Tools and Applications*, vol. 77, no. 2, pp. 2083-2114, Jan. 2018.
- [7] Z. Zhang and L. Zhao, "A Design of Digital Rights Management Mechanism Based on Blockchain Technology," *International Conference on Blockchain (ICBC)*, Seattle, WA, USA, 2018, pp. 32-46.
- [8] M. Su, H. Zhang, M.Z.A. Bhuiyan, X. Du, P. Zhang, "An effective copyright-protected content delivery scheme for p2p file sharing networks," *International Journal of Communication Systems*, vol. 31, no. 16, pp. e3476, 2018.
- [9] B. Bodó, D. Gervais, and J. P. Quintais, "Blockchain and smart contracts: the missing link in copyright licensing?," *International Journal of Law and Information Technology*, vol. 26, no. 4, pp. 311-336, 2018.
- [10] Y. Chen and L. Peng, "Research on the Copyright Protection Technology of Digital Clothing Effect Diagram," *International Conference of Pioneering Computer Scientists, Engineers and Educators (ICPCSEE)*, Singapore, 2017, pp. 741-750.
- [11] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, [online] Available: <https://bitcoin.org/bitcoin.pdf>.
- [12] N. Szabo, Smart Contracts, 1994, [online] Available: <http://szabo.best.vwh.net/smart.contracts.html>.
- [13] V. Buterin, A next-generation smart contract and decentralized application platform, 2014, [online] Available: https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.
- [14] J. Al-Jaroodi and N. Mohamed, "Blockchain in Industries: A Survey," in *IEEE Access*, vol. 7, pp. 36500-36515, 2019.
- [15] J. Abou Jaoude and R. George Saade, "Blockchain Applications – Usage in Different Domains," in *IEEE Access*, vol. 7, pp. 45360-45381, 2019.
- [16] Z. Ma, M. Jiang, H. Gao, Z. Wang, "Blockchain for digital rights management", *Futur. Gener. Comput. Syst.*, vol. 89, pp. 746-764, 2018.
- [17] Z. Ma, W. Huang and H. Gao, "A new blockchain-based trusted DRM scheme for built-in content protection," *EURASIP Journal on Image and Video Processing*, 2018.
- [18] Z. Meng, T. Morizumi, S. Miyata and H. Kinoshita, "Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain," 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, 2018, pp. 359-364.
- [19] J. Zeng, C. Zuo, F. Zhang, C. Li and L. Zheng, "A Solution to Digital Image Copyright Registration Based on Consortium Blockchain," *Chinese Conference on Image and Graphics Technologies (IGTA)*, Beijing, China, 2018, pp. 228-237.
- [20] PIC-CHAIN, 2018, [online] Available: <http://c-chain.baidu.com/#/>.
- [21] D. Roman, K. Vu, "Enabling Data Markets Using Smart Contracts and Multi-party Computation," in 2018 International Conference on Business Information Systems, Berlin, Germany, 2018, pp. 258-263.
- [22] H. R. Hasan and K. Salah, "Proof of Delivery of Digital Assets Using Blockchain and Smart Contracts," in *IEEE Access*, vol. 6, pp. 65439-65448, 2018.
- [23] W. Diffie and M. Hellman, "New directions in cryptography," in *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, November 1976.
- [24] Libra, 2019, [online] Available: <https://libra.org/zh-CN/white-paper/>.
- [25] Calibra, 2019, [online] Available: <https://calibra.com>.
- [26] K. Wüst and A. Gervais, "Do you Need a Blockchain?," 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, 2018, pp. 45-54.
- [27] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukoli, S. W. Cocco, J. Yellick, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains", *Proceedings of the Thirteenth EuroSys Conference on EuroSys '18*, pp. 1-15, 2018.
- [28] National Copyright Administration of The People's Republic of China, "Statistics on The Copyright Registration in China in 2017," Oct. 2018, [online] Available: <http://www.ncac.gov.cn/chinacopyright/contents/11228/386868.html>.
- [29] BTC.com, Aug. 2018, [online] Available: <https://btc.com/>.
- [30] F. Frattolillo, "Digital copyright protection: Focus on some relevant solutions," *International Journal of Communication Networks and Information Security*, vol. 9, no. 2, pp. 282-293, Aug. 2017.
- [31] S. Lee, K. Kim, J. Kang and H. Kim, "Bypassing DRM protection in e-book applications on Android," 2018 International Conference on Information Networking (ICOIN), Chiang Mai, 2018, pp. 194-198.