

CopyrightChain: Permissioned Blockchain-based Collaboration and Design Right using Hyperledger Composer and IPFS

Nursena Baygin
Computer Engineering Department, Kafkas
University, Kars/Turkey

Mehmet Karakose
Computer Engineering Department, Firat University,
Elazig/Turkey

ABSTRACT

Information technologies, which have developed in every field in recent years, bring various problems in digital environments. The increase in digital records has increased the importance given to digital identity information in terms of data security and data source. With digital identity, information such as where and when data is shared can be obtained. Data that can be easily reproduced in digital environment puts copyright holders in a difficult situation. This article outlines how copyrights can be secured digitally and executed in a transparent manner. For this purpose, the furniture sector, which is one of the sectors where personalized products increase, has been examined as an example. Reaching customer demands in customized production and ensuring manufacturer-customer integration can be achieved by overcoming various difficulties. For this purpose, blockchain-based in this article proposed to bring together the actors in the manufacturing sector and the customer. In addition, it was emphasized how to secure the copyright of products designed by the customer or other actors. It is known that the data obtained during the protection of copyrights becomes cumbersome over time. For this purpose, it is aimed to increase the speed by using an external database. A distributed database, IPFS, was used for this.

Keywords

Blockchain, Smart Contract, Copyright, IPFS, Mass Customization.

1. INTRODUCTION

Access to digital content has become easier with the widespread technological developments. However, the easy access to digital content causes uncontrolled distribution and the security of the original data is endangered with various information changes. In addition, there are variations and uncontrolled distributions beyond the control of the original data owner. Today, data control systems are centralized. This is an indication that the control of the original data takes place from a single center. In such a structure, manipulating, changing or deleting data is seen as a big problem. The management, monitoring and document release issues of digital content are critical. Erroneous transactions arising from document changes in existing data platforms and with increasing consumption are also increasing. Therefore, decentralized reliable databases are needed [1].

Blockchain refers to ledgers shared between all users on the consensus network. Without the need for a third party, the platform is reliably managed with a decentralized structure. It is impossible to change the data on this platform, where each transaction is stored in a timestamped and cryptographic manner [2].

Blockchain attracts great attention thanks to the advantages it offers today. However, blockchain has an issue associated with inefficiency and cost when storing large files such as design data. Storing hash values on the blockchain instead of the original data itself produces much more reliable and effective results. For this purpose, keeping the original data on different platforms and storing the hash values obtained from the original data on the block chain will give very effective results. The Inter-Planetary File System (IPFS) is the most preferred open source and distributed file system that provides peer-to-peer sharing among these platforms [3]– [6]. When a data is loaded into IPFS, it creates hash values and access to data is provided with this hash value. In this study, these hash values are stored in smart contracts and access is provided in line with the content owner request. Smart contracts are code that enables transactions to be carried out in accordance with predefined terms and conditions. When designing a platform, the necessary conditions are determined, the rights of the users are secured and the rules are determined.

Copyright owners cannot effectively control the use of their data on the internet. It costs close to zero to copy this data and access the copied data. In addition, it can be very difficult to pay license fees to data rights holders in case of data usage. In order to receive the payment, there must be a contract between the user and the beneficiary, and this creates serious costs for both parties. Another problem is that the database companies where the data are stored and the right holders have to share their data revenues.

The motivation and contributions of this study can be summarized as follows:

- A blockchain-based proposal has been introduced for the control of digital content by creating a smart contract. With this proposed method, it provides a decentralized platform and enables transactions to be made without the approval of third parties.
- It highlights the requirements of copyright protection and investigates the suitability of the blockchain in protecting these rights.
- A proposal is made for fast, secure and cost-effective protection of the copyrights of data shared over the network using computer technologies. In addition, an answer to the question of how to encourage copyright holders to obtain copyright over the network was sought. It has been suggested that the data should be shared in a more secure environment with the copyright.
- A blockchain model has been proposed showing how to use IPFS technology to reduce the data load stored in the blockchain.

The rest of this paper is organized as follows. In Section 2, information about the studies in the literature is given. In

Section 3, the theoretical background for the related study is presented. Section 4 seeks an answer to the question of why copyright protection in digital media is necessary. In Section 5, the proposed method is presented. Section 6, results of the proposed method are explained Section 7, information was given about future works.

2. RELATED WORK

Bitcoin is a blockchain-based technology that enables cryptocurrency exchange that doesn't need a centralized structure. It is an important study in terms of proving the applicability of blockchain [7]– [9]. Blockchain demonstrates its success in finance in other areas. With this aspect, it is followed with great interest both in the private sector and in the academic community. Blockchain is seen as an important way of dealing with critical problems in copyright issues [10], [11]. Nikolaos et. al. carried out a blockchain-based study to distribute and protect the copyrights in the music industry to all stakeholders. It is aimed to eliminate conflicts about music rights, to update data and to define copyright [12].

Yi et. al. basically designed a two-layer system for copyright management. As seen in the figure, the first layer is a layer that provides interaction with users, while the second layer is for data storage. In copyright protection, it is an important question whether digital data will be stored in the blockchain or in an external database [13]. Storage of data on an external platform brings along an important problem in terms of data security. For this purpose, Wang et al. conducted a study for the security of data stored in IPFS to protect copyrights. The data are encrypted and secured with the ELGamal encryption algorithm [3].

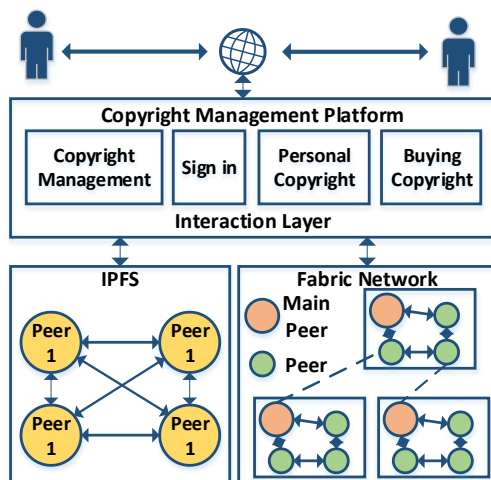


Fig 1: System structure [13]

The content of data stored in an external database must be protected before it is made available to the public. For this purpose, content encryption was made and watermarks embedded in digital content were used in the study conducted by Zhaofeng et al. [14]. The copy of every data protected in the digital environment is the same. The block chain increases the security of these copies by providing them with personalization. It performs this process with time stamp and cryptographic algorithms, hash value functions. It can provide the establishment of license terms with blockchain copyright management. Assigning open source licenses by determining the limits of internet access [15]. Blockchain cryptographic algorithms offer a traceable structure by combining the hash structure and consensus mechanism. Based on this, Ruzhi et al. proposed a smart contract based plan for digital rights

management that enables real-time transactions based on consensus [16].

Digital intellectual property protection technologies produce inefficient results in terms of authority management, traceability, reliability and scalability. In a study proposed by Lijun et. al. as a solution to this problem, copyright information is transformed into identity string using quadratic matrix transformation. Traceable identity information is obtained in this blockchain-based study. This system, which ensures that copyright information is secured, improves the ability against attack situations [17]. Due to the increasing cloud services central structures in recent years, concerns regarding privacy, security and traceability have increased. Technologies with distributed databases such as IPFS and blockchain produce efficient results to solve such problems.

Table 1. Related studies in the literature

Reference	Year	Contribution	Technology
Zhini [18]	2020	Increase the efficiency of digital music copyright protection	Blockchain-based system
Wei et al. [19]	2020	Cooperation and secure copyrights in e-government and financial transactions	Ethereum
Rishabh et al. [20]	2019	Securing copyright on stock photo websites	IPFS + Ethereum
Shishir et al. [21]	2019	Reliably managing to business networking	Hyperledger Composer
Jin Tao et al. [22]	2018	Data trace for food safety	IPFS + Ethereum
Randhir et al. [5]	2020	Preventing unauthorized access to patient data	IPFS + Consortium blockchain
Ali and Najim [23]	2020	Safeguarding the copyrights of digital images	IPFS + Blockchain
Pongnumkul et al. [24]	2017	Ethereum lower latency and Hyperledger Fabric has a higher throughput	Hyperledger Fabric + Ethereum
Katarzyna and Marek [25]	2020	Ensuring the security the digital pages and storing the data images in the blocks	Imagechain

Many companies conduct various researches to increase their purchasing potential. In today's technology, meeting customer demands significantly affects the sales potential. This pushes manufacturers to learn about user requests. In the furniture industry, user requests are obtained and analyzed with statistical data such as surveys and feedback. One of the

biggest problems encountered in this sector, which is directed towards user demands, is product replication and imitation. The images presented in the internet environment are imitated by other companies and released to the market. In the proposed system, it is aimed to produce products in cooperation with the designer, engineer, researcher and manufacturer in line with the user's requests. A product that the customer and its collaborators are entitled to emerges. At this point, obtaining the copyrights of the product will prevent counterfeit structures and uncontrolled duplication. The proposed system focuses on how to secure the copyright of the product designed by any of the members.

3. THEORETICAL BACKGROUND

3.1 Blockchain

Blockchain refers to the distributed and immutable database of a decentralized network Bitcoin, the blockchain application, has increased its popularity with the first cryptocurrency feature. It can show its success announced in the financial field in other areas. It provides user security and data consistency with asymmetric cryptography and distributed consensus algorithms [26]. When a node in the network wants to initiate a transaction, it records and broadcasts data on the network. Nodes in the network receiving the broadcast data query the accuracy of the data and perform the verification process. According to the consensus algorithm used in the network, the data is stored in the blockchain as a block. With its distributed structure, approved data is copied in all nodes. Thus, a distributed ledger structure is obtained [27].

3.1.1. Characteristic of Blockchain

Reliability: Each transaction in the blockchain is followed by all users and followed by validators. All transactions are monitored by users and protected by cryptographic algorithms against network attacks.

Persistence: Transactions on the blockchain are stored as blocks, and each block is encrypted and stored. Insecure blocks are overridden by miners.

Auditability: Every transaction in the blockchain is recorded in blocks with a timestamp. Thus, each transaction performed can be monitored and verified. In addition, after each transaction is approved by the signing method, it is added to the block chain permanently.

Decentralization: In the blockchain, every user on the network has the right to access. The data are not stored in a central database, so there is no data loss that occurs in central databases [28], [29].

3.1.2. Taxonomy of Blockchain Systems

Blockchain is basically divided into three groups according to usage permissions and network participation conditions. Blockchain types are as follows:

Public blockchain: Open networks refer to the type of blockchain that all users not managed by any authority can access data. There are no restrictions in creating a consensus. Each transaction can be monitored transparently. Networks such as Ethereum, Bitcoin, Litecoin, Monero are examples of open networks.

Private blockchain: Private blockchains are types that depend on authority permission. Although it is seen as contrary to the blockchain logic, the transparent monitoring and protected execution of all transactions reveals the difference. Such blockchains are subject to permission to join the network. Monax and multichain are examples of private blockchains.

Consortium blockchain: This type of network is a combination of open networks and private networks. Only the selected group participates in the consensus process. It refers to groups that come together for certain purposes. The network is closed and job descriptions are clear. Transactions are progressing faster than other types of blockchain. Hyperledger, Corda, Quorum consortium are examples of blockchain [30], [31].

3.2 Smart Contract

Traditional contracts have problems such as asymmetric knowledge between parties, passive agreements, ineffective rules and high costs. Smart contracts, invented by Nick Szabo in 1990, emerged as protocols that are automatically executed, have information storage feature and allow various calculations to be made [32]. The smart contract consists of codes that aim to secure relationships in public networks. The interaction between the participants is ensured by creating contracts with the rules that have been decided in advance by the participants. Ethereum and Hyperledger are public platforms that enable smart contract creation. Contracts created on these platforms are stored on the blockchain and tasks can be run by any participant at any time [33]. Smart contracts are usually written in Solidity language and only byte code of the written code is stored in the blockchain. People who process transactions performed in smart contracts are called miners. Miners execute codes through the Ethereum Virtual Machine (EVM) [34].

3.3 Mass Customization

In today's markets, customer demands are among the important factors affecting competitive power. In order for producers to get the share they want from the market, a customer-oriented production model should also be adopted in addition to mass production. At this point, mass customization refers to the ability to produce customized products at mass production cost, quality and delivery speed. This production model has four main components: high volume, cost effectiveness, customer sensitivity and consistent quality. In addition to the successful applications of MC in the literature, there is limited information about its common and problem-free results [35].

MC is capable of meeting the customer's needs of manufacturers quickly and in a wide variety of products. Increases customer satisfaction as it is a customer-oriented production model [36]. It is interesting by many companies with its advantages. However, it is very important that the infrastructure is suitable to switch to this production model. In addition, factors such as quality management, supply chain, company capacity have critical value for production. The products produced with MC technology are created by choosing and combining many options. For this type of production, it is possible with customer request information and creating a mathematical simulation model. The designer needs cooperation between manufacturers, customers and suppliers and trust between parties. It is possible to meet these needs with blockchain. For this purpose, it is thought that companies using blockchain and MC infrastructure will get more effective results [37].

3.4 The Inter-Planetary File System (IPFS)

Nowadays, with the increase in data size, the need for reliable storage areas increases. IPFS provides an ideal environment for storing files with its decentralized structure. It allows users to access and store data by storing them with hash values [38]. It is sufficient to know the hash value to reach the data. However, this situation causes various security vulnerabilities.

Therefore, encryption methods should be used to store data with IPFS security [4], [39]. In this proposed study, the data is secured with asymmetric encryption method. With asymmetric encryption, the encryption process is performed by adding the public key of the recipient to the data. Thus, access to data is made possible only with the recipient's public key.

3.5 Hyperledger Composer

Hyperledger Composer is a project from the tools of Hyperledger Fabric and supported by The Linux Foundation. Hyperledger Composer aims to simplify modeling to implement business network and transaction logic. It is a collaboration tool that accelerates smart contracts development and distributed ledger structure [40], [41]. With this tool, collaboration networks can be modeled and integrated into systems. Hyperledger basically has two storage areas, distributed ledgers and a state database. It is an immutable structure that stores file-based serial blocks that define the distributed ledger blockchain. Each block contains one or more transactions. In the status database, every transaction is recorded after the approval of the parties. The state database can be rebuilt in contrast to the distributed ledger. There are two options, LevelDB embedded in Hyperledger Fabric and external CouchDB [42]. Hyperledger composer is a web-based tool used to run applications from development, packaging, and testing. Many Business Network Archives (.bna) can be created together in this application environment. .bna s basically consists of four main files: Model (.cto), Command (.js), Query (.qry), and access control (.acl). and the access control file refers to the sections where access controls are defined [39].

4. DIGITAL PROTECTION REQUIREMENT AND BLOCKCHAIN COMPLIANCE

4.1 Digital Rights Protection Security Requirements

In traditional cases, copyrights are obtained when it comes to any new design. However, it is not possible to obtain the copyright of a product designed in a digital environment and to secure the rights of the person. A reliable paradigm has been proposed for user-generated copyrights of user-generated products. The new requirements are as follows:

Product design information verifiability: Product design information must be auditable and verifiable by the design platform before being uploaded to the blockchain environment. It should be investigated whether any design product is applicable and has royalty value.

Identity management and ensuring confidentiality: An effective system should be capable of storing and protecting the identity information of its users. However, it is very important to store information about who produced the design product.

Protection of product ingredient information: It is among the platform requirements to prevent leakage of content information before the product design process ends. Protection against the dissemination of design information should be ensured, and access to content information through the approval process should be adopted. It should contain restrictions and conditions and usage rules.

Copyright Apply: The user must have the copyright application right after accepting the design verification process.

Monitoring violations of rights: When the product design information is created, if the content is used for infringement,

the platform manager is able to track the identity of the person who committed the violation.

Copyright transparency: Copyright should not be found in databases that act independently. A platform should be developed that will not allow product copyright infringement and distribution on the internet.

4.2 Blockchain Suitability for Digital Rights Protection

Blockchain known as distributed ledger although there are several shortcomings, it has enough potential in the copyright industry for how to distribute and execute digital content. With blockchain technology, it is aimed to protect various property rights and to spread automated platforms through self-managing "Smart Contracts". In addition, information about copyright ownership and distribution can be analyzed with the method called "Time Stamp" [16]. With time stamp, the date and time of each transaction performed on the internet are recorded. Thus, it is ensured that each transaction is carried out in a traceable time. The process of creating and modifying digital content is very important. Digital fingerprints are created by taking the "hash" values of the data with the summary function, which is another feature of the block chain [42]. In addition, various protocols are added to these hash values to create unique codes. Today, the cumbersome structure of copyrights obtained with written protocols can be made more effective with blockchain. With its decentralized structure, it can eliminate the costs paid to blockchain copyright database companies, which removes the authorities. Thus, sharing the income of copyright holders can be prevented.

5. IMPLEMENTING BLOCKCHAIN FOR COPYRIGHT

In this section, a comprehensive description of the functioning of the proposed method, participants and components is given.

5.1 Platform Architecture and Technical Features of Components

In this section, it is aimed to give information about the architecture and technical integration of the system. The architecture of the proposed platform is shown in Figure 2. It provides interaction with users with Angular 4 and processes user requests to Hyperledger network via REST API. Smart contracts are created and the blockchain network is modeled with Hyperledger Composer. Hyperledger fabric is intended to enable users to validate copyright documents and provide distributed ledger technology. IPFS is used to securely store data that needs to be kept off the chain. Registration creation, access, modification, update and approval processes take place on the proposed platform. Each transaction is stored with hash values.

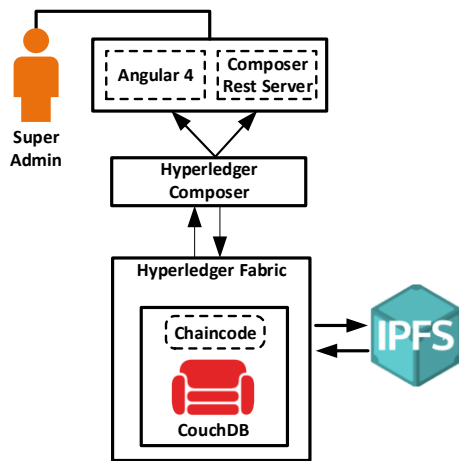


Fig 2: Proposed system structure

5.2 Components of Platform Framework

In this section, it is aimed to give detailed information about the proposed platform compounds.

Participants: Participants are divided into three groups as Super Administrator, Administrator and Users in this proposed platform. While the super manager is the person who established the system, the managers are the actors in the production sector. Users are people who want to buy or design furniture. Figure 3 shows all the actors in the system.

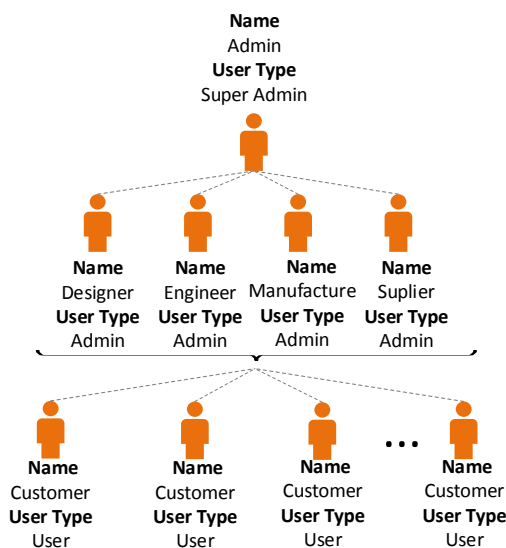


Fig 3: Actors of the proposed method

Participants in the system are customer (user), designer (admin), engineer (admin), supplier (admin) and manufacturer (admin). It refers to the actors that increase the speed and reliability of the system by cooperating with each other in the proposed system. It is important that copyright is stored securely. Therefore, it is aimed to secure the copyrights of the designed product information. The copyright of the product designed by the customer, designer or engineer is secured with the contributions of other participants. With the approval of the super managers, new participants are included in the system. Also, super administrators can monitor user activities. Users can add, delete and update product copyrights. Users who have copyright on the product design are presented with a smart contract. Time, region and copyright type are reported by the system.

Front-End: The front end of the system has been developed with the help of the composer-rest-server and Angular framework provided with Hyperledger Composer. REST API is created with Composer-rest-server. The skeleton structure of the system is created with the Angular framework. Angular user interaction is made and user requests are processed into Hyperledger composer through the REST API.

Blockchain Database (onchain): Couch DB refers to the database it hosts within Hyperledger Fabric. By establishing a peer-to-peer connection with this database, it is ensured that every transaction performed is recorded.

Assets: Assets in the blockchain are related to tangible or intangible goods and services in the network. Concrete concepts such as fruits, cars, houses or abstract concepts such as intellectual property rights refer to assets. In the proposed system, assets refer to copyright information.

IPFS (offchain): Blockchain produces inefficient results in systems where large data is recorded. For this purpose, storing the data in a different database and storing the hash values of data on the block chain will produce more rational solutions. In the system proposed for this purpose, copyright information of the products is stored in the IPFS database.

Transactions: It refers to the asset actions that take place between the participants. In the proposed system, the transactions can be divided into participant and copyright transactions. Adding, deleting, viewing participants refers to the first group. Transactions such as creating, deleting, viewing, approving copyright refer to the second group.

5.3 Creating Skeletal Structure of Platform

In this section, information is given about how the skeleton structure of the proposed platform was created with Hyperledger Composer. The Hyperledger composer main component is defined on the proposed platform as shown in the Figure 4. Hyperledger composer is a programming model with APIs that allows the business network and participants to send transactions that exchange assets. Each business network file contains Model file (.cto), function file (.js), query file (.qry) and access control file (.acl). In the proposed method, it has been defined that the .cto and js files of the business network are explained in the previous sections. In the Access control section, the restrictions of the users are taken into consideration and the delegation of authority is defined. For example, authority has been given to admins and super admins to approve a designed product for production. In the Query File section, queries are defined. Simple queries were used and it was aimed for the users to query the information they deemed necessary.

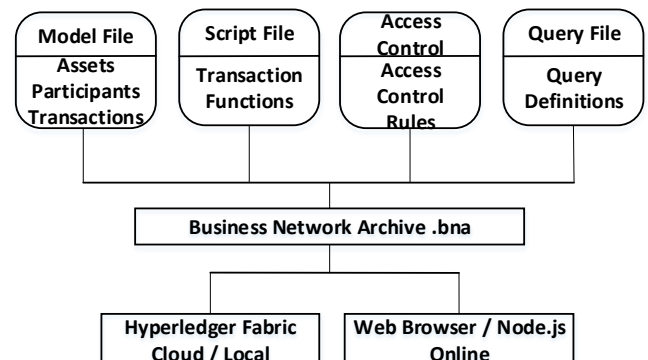


Fig 4: Hyperledger Composer

5.4 Copyright Encryption of Product and Owner Information

Blockchain offers a cumbersome structure in systems with large data size. Various external databases are used for this purpose. In the proposed study, the IPFS database is used. In addition to providing a reliable system, IPFS has shortcomings in accessing data. For this purpose, data privacy with the public key cryptography method is recommended for reliable recording and access of data. As can be seen in the figure 5, admin requests permission to access the user's information. If the user approves the permission, composite data is created on the system side and the session key is created. Thus, a new password is created each time permission is requested. The encrypted data created is sent to the admin and the user. The admin decrypts and uploads it back to IPFS by performing the operations on the data.

5.5 Copyright Structure and Transaction Process

In this part of the study, the algorithms of proposed method are included. In Algorithm 1, it offers users the ability to create a copyright. A unique copyright is created by comparing it with existing copyrights based on the information provided. Copyright variables are added to the copyright creator information and added to the blockchain along with the creation date. The copyright created with algorithm 2 is deleted. Copyright-protected information is requested and if the creator of that copy is copyrighted, the copyright is allowed to be deleted. Only the creator can delete the copyright. Algorithm 3 allows viewing of copyright information. The user can view any copyrighted information by entering the copyrighted information. Algorithm 4 provides confirmation of copyright. Only Super admin and administrators can perform this operation. All administrators and super administrators in the system must approve the copyright. In the proposed system, it is assumed that there is only one designer, engineer, manufacturer and supplier.

Algorithm 1 Copyright Creation

Input: copyrightId
Output: Creates the copyright with appropriate value in CopyrightChain

```

1: if copyright exists then
2:   return
3: else
4:   set the copyright attributes
5:   set participants (who invoke this function) address as creator
6:   push the address to CopyrightChain
7:   push the current time to creationDate

```

Algorithm 2 Copyright Delete

Input: copyrightId
Output: Removes the copyright from CopyrightChain

```

8: if copyright exists && owner then
9:   remove the copyright from CopyrightChain
10: else
11:   return

```

Algorithm 3 Copyright Display

Input: copyrightId
Output: Displays the appropriate copyright instance from CopyrightChain

```

12: if copyright exists then
13:   return the copyright view from CopyrightChain
14: else
15:   return

```

Algorithm 4 Copyright Confirmation

Input: copyrightId
Output: Confirmation the appropriate copyright instance from CopyrightChain

```

16: if copyright exists then
17:   return
18: else
19:   confirm

```

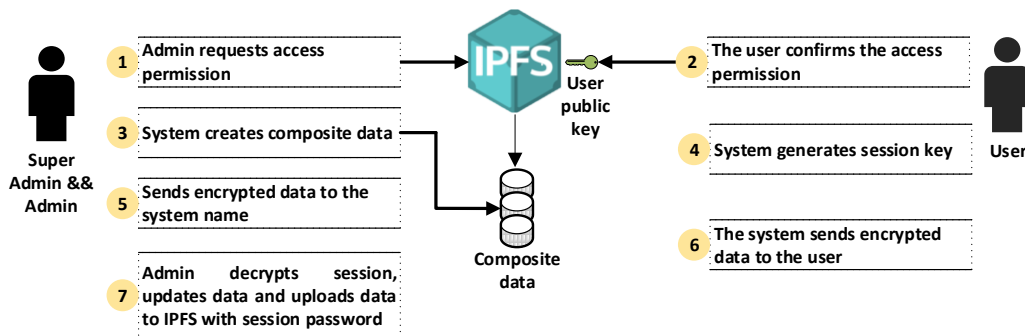


Fig 5: IPFS public key cryptography

6. DISCUSSION

In this study, Hyperledger Composer business network based on the Hyperledger Fabric has been evaluated. The server runs on a local personal computer with Ubuntu 18.04 with 16 GB, 256 SSD an Intel core i7. Docker v17.03 and Docker-compose v1.13.0 are used as the essential toolsets. Response times to created assets were compared. Assets from 100 up to 800 were created as shown in the Figure 5. Also, Figure 6 shows the average response time. It is seen that as the number of assets increases, the average response time is fixed.

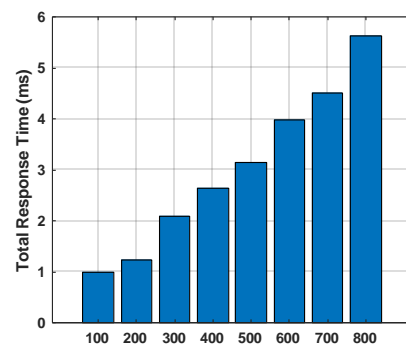


Fig 6: Hyperledger Composer response time

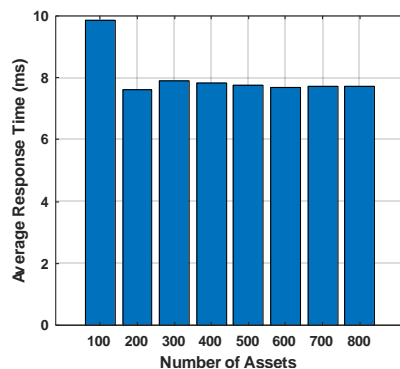


Fig 7: Hyperledger Composer Average response time

7. CONCLUSION

In this study proposed on how to securely store copyright in digital environment using Hyperledger Composer. For this purpose, a prototype was presented by showing the furniture industry as an example. In the furniture industry, design copyrights are not guaranteed digitally. In addition, since the actors of the furniture industry do not exist together, uncertainties are encountered regarding supply and demand. Manufacturers who obtain customer requests through surveys face various challenges. In this proposed study, it is aimed to gather the players on a single platform by ensuring cooperation. In addition, the roles of the actors in the system in creating copyright are emphasized and necessary permissions are defined. In this study, which emphasizes the importance of cooperation and data security, the emergence of new products and the protection of copyright are emphasized. While blockchain offers important advantages in terms of security, it does not provide sufficient efficiency in terms of big data storage. As the data size increases, the system begins to slow down and not get the required efficiency. In this system proposed for this purpose, an external database, IPFS, is used for data storage. With IPFS, copyright information is stored and transactions are recorded in the block chain. In addition, for data security, IPFS can be secured with cryptographic algorithms. For this purpose, the public key cryptography method, which is a two-stage security for data security, is proposed in this study. With the blockchain, which is transparent, reliable, traceable and decentralized, the difficulties of copyright in the digital environment are overcome.

8. FUTURE WORK

As an extension of our proposed system, we focus on regulating the permissions required for copyright approval of many actors in the system (if there is more than one designer, manufacturer, supplier, engineer). We are also investigating the existence of other solutions to increase the speed of the system and storage space without using IPFS. Another issue we focus on is the determination of specific standards and steps to be taken in case of violation of rights in sample design documents.

9. REFERENCES

[1] N. Nizamuddin, K. Salah, M. Ajmal Azad, J. Arshad, and M. H. Rehman, "Decentralized document version control using ethereum blockchain and IPFS," *Computers & Electrical Engineering*, vol. 76, pp. 183–197, 2019.

[2] M. Li, C. Lal, M. Conti, and D. Hu, "LEChain: A blockchain-based lawful evidence management scheme for digital forensics," *Future Generation Computer Systems*, vol. 115, pp. 406–420, 2021.

[3] W. Peng, L. Yi, L. Fang, D. Xinhua, and C. Ping. 2019 Secure and Traceable Copyright Management System Based on Blockchain. *IEEE 5th Int. Conf. Comput. Commun. ICC3* 2019

[4] Y. Chen, H. Li, K. Li, and J. Zhang. 2017 An improved P2P file system scheme based on IPFS and Blockchain. *IEEE Int. Conf. Big Data, Big Data 2017*, vol. 2018-Janua, pp. 2652–2657.

[5] R. Kumar, N. Marchang, and R. Tripathi. 2020 Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain. *Int. Conf. Commun. Syst. NETWORKS, COMSNETS*

[6] H. R. Hasan and K. Salah, "Combating Deepfake Videos Using Blockchain and Smart Contracts," *IEEE Access*, vol. 7, pp. 41596–41606, 2019.

[7] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A Survey on Blockchain Interoperability: Past, Present, and Future Trends," 2020, [Online]. Available: <http://arxiv.org/abs/2005.14282>.

[8] M. Dabbagh, K. K. R. Choo, A. Beheshti, M. Tahir, and N. S. Safa, "A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities," *Computers&Security*, vol. 100, p. 102078, 2021.

[9] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain Meets Cloud Computing: A Survey," *IEEE Communications Surveys Tutorials*, no. c, pp. 1–22, 2020.

[10] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou. 2016 Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. *IEEE Symp. Secur. Privacy, SP 2016*, pp. 839–858,

[11] Z. Meng, T. Morizumi, S. Miyata, and H. Kinoshita. 2018 Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain. *Int. Comput. Softw. Appl. Conf.*, vol. 2, pp. 359–364

[12] N. Kapsoulis et al., "Consortium blockchain smart contracts for musical rights governance in a collective management organizations (CMOs) use case," *Future. Internet*, vol. 12, no. 8, 2020.

[13] Y. Ouyang, X. Zheng, X. Lu, L. Xiaowei, and S. Zhang. 2019 Copyright protection application based on blockchain technology. *IEEE Intl Conf Parallel Distrib. Process. with Appl. Big Data Cloud Comput. Sustain. Comput. Commun. Soc. Comput. Networking, ISPA/BDCLOUD/SustainCom/SocialCom 2019*, pp. 1271–1274

[14] Z. Ma, M. Jiang, H. Gao, and Z. Wang, "Blockchain for digital rights management," *Future Generation Computer Systems*, vol. 89, pp. 746–764, 2018.

[15] A. Savelyev, "Copyright in the blockchain era: Promises and challenges," *Computer Law Security Review.*, vol. 34, no. 3, pp. 550–561, 2018.

[16] R. Xu, L. Zhang, H. Zhao, and Y. Peng. 2017 Design of Network Media's Digital Rights Management Scheme Based on Blockchain Technology. *IEEE 13th Int. Symp. Auton. Decentralized Syst. ISADS 2017*, pp. 128–133

[17] L. Xiao, W. Huang, Y. Xie, W. Xiao, and K. C. Li, "A Blockchain-Based Traceable IP Copyright Protection

- Algorithm,” *IEEE Access*, vol. 8, pp. 49532–49542, 2020.
- [18] Z. Cai, “Usage of Deep Learning and Blockchain in Compilation and Copyright Protection of Digital Music,” *IEEE Access*, vol. 8, pp. 164144–164154, 2020.
- [19] W. Liang, D. Zhang, X. Lei, M. Tang, K. C. Li, and A. Zomaya, “Circuit Copyright Blockchain: Blockchain-based Homomorphic Encryption for IP Circuit Protection,” *IEEE Transactions on Emerging Topics in Computing*, vol. 6750, no. c, pp. 1–11, 2020.
- [20] R. Mehta, N. Kapoor, S. Sourav, and R. Shorey. 2019 Decentralised Image Sharing and Copyright Protection using Blockchain and Perceptual Hashes. 11th Int. Conf. Commun. Syst. Networks, COMSNETS 2019, vol. 2061
- [21] S. Ranjan, A. Negi, H. Jain, B. Pal, and H. Agrawal. 2019 Network System Design using Hyperledger Fabric: Permissioned Blockchain Framework. 12th Int. Conf. Contemp. Comput. IC3 2019, pp. 3–8
- [22] J. T. Hao, Y. Sun, and H. Luo, “A safe and efficient storage scheme based on blockchain and IPFS for agricultural products tracking,” *J. Comput.*, vol. 29, no. 6, pp. 158–167, 2018.
- [23] A. Muwafaq and S. N. Alsaad, “Design scheme for copyright management system using Blockchain and IPFS,” *International Journal of Computing and Digital Systems*, pp. 1–6, 2021.
- [24] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong. 2017 Performance analysis of private blockchain platforms in varying workloads. 26th Int. Conf. Comput. Commun. Networks, ICCCN 2017
- [25] K. Koptyra and M. R. Ogiela, “Imagechain—Application of Blockchain Technology for Images,” *Sensors*, vol. 21, no. 1, p. 82, 2020.
- [26] J. Zarrin, P. H. Wen, L. B. Saheer, and B. Zarrin, “Blockchain for Decentralization of Internet: Prospects, Trends, and Challenges,” pp. 1–23, 2020, [Online]. Available: <http://arxiv.org/abs/2011.01096>.
- [27] Y. Liu et al., “Blockchain-Based Identity Management Systems: A,” *Journal Network and Computer Applications*, p. 102731, 2020.
- [28] P. De Filippi, M. Mannan, and W. Reijers, “Blockchain as a confidence machine: The problem of trust & challenges of governance,” *Technology in Society*, vol. 62, p. 101284, 2020.
- [29] P. Tasca and C. J. Tessone, “A Taxonomy of Blockchain Technologies: Principles of Identification and Classification,” *Ledger*, vol. 4, 2019.
- [30] B. Bhushan, P. Sinha, K. M. Sagayam, and A. J., “Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions,” *Computers Electrical Engineering*, no. July 2019, p. 106897, 2020.
- [31] N. Zahed Benisi, M. Aminian, and B. Javadi, “Blockchain-based decentralized storage networks: A survey,” *Journal of Network and Computer Applications*, vol. 162, p. 102656, 2020.
- [32] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, “Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools, Techniques and Challenges,” *IEEE Access*, vol. 8, pp. 24746–24772, 2020.
- [33] Y. Issaoui, A. Khiat, A. Bahnasse, and H. Ouajji, “Smart Logistics: Blockchain trends and applications,” *J. Ubiquitous Syst. Pervasive Networks*, vol. 12, no. 2, pp. 09–15, 2020.
- [34] A. A. Zarir, G. Oliva, Z. Jiang, and A. Hassan, “Developing Cost-Effective Blockchain-Powered Applications: A Case Study of the Gas Usage of Smart Contracts Transactions in the Ethereum Blockchain Platform,” *CEUR Workshop Proc.*, vol. 2657, no. October, pp. 1–9, 2020.
- [35] H. Sheng, T. Feng, L. Chen, D. Chu, and W. Zhang, “Motives and performance outcomes of mass customization capability: evidence from Chinese manufacturers,” *Journal of Manufacturing Technology Management*, 2020.
- [36] P. J. Jost and T. Süsler, “Company-customer interaction in mass customization,” *International journal of production economics.*, vol. 220, no. May 2019, p. 107454, 2020.
- [37] X. Zhu, J. Shi, S. Huang, and B. Zhang, “Consensus-oriented cloud manufacturing based on blockchain technology: An exploratory study,” *An exploratory study. Pervasive and Mobile Computing*, vol. 62, p. 101113, 2020.
- [38] A. Tenorio-Fornés, S. Hassan, and J. Pavón. 2018 Open peer-to-peer systems over blockchain and IPFS: An agent oriented framework. CRYBLOCK 2018 - Proc. 1st Work. Cryptocurrencies Blockchains Distrib. Syst. Part MobiSys 2018, pp. 19–24
- [39] S. Chentharra, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology, vol. 15, no. 12 December. 2020.
- [40] A. H. Lone and R. N. Mir, “Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer,” *Digital Investigation.*, vol. 28, pp. 44–55, 2019.
- [41] R. Wutthikarn and Y. G. Hui. 2018 Prototype of blockchain in dental care service application based on hyperledger composer in hyperledger fabric framework. 22nd Int. Comput. Sci. Eng. Conf. ICSEC 2018, pp. 2–5
- [42] S. Aggarwal and N. Kumar, “Hyperledger,” *Adv. Comput.*, 2020.
- [43] Baygin, N., Baygin, M., & Karaköse, M. 2020 Blockchain Application in Mass Customization: A Furniture Sector Example. In 2020 International Conference on Data Analytics for Business and Industry: Way Towards a Sustainable Economy (ICDABI) (pp. 1–5). IEEE.
- [44] Baygin, N., Baygin, M., & Karaköse, M. 2019 Blockchain Technology: Applications, Benefits and Challenges. In 2019 1st International Informatics and Software Engineering Conference (UBMYK) (pp. 1–5). IEEE.