2022 3rd International Conference for Emerging Technology (INCET)
Belgaum, India. May 27-29, 2022

Blockchain-based Intellectual Property Management Using Smart Contracts

CS Wanigasooriya
Department of Computer Science, General Sir John Kotelawala Defence University
Rathmalana, Sri Lanka
36-se-0004@kdu.ac.lk

ADAI Gunasekara
Department of Computer Science, General Sir John Kotelawala Defence University
Rathmalana, Sri Lanka
asela@kdu.ac.lk

KGKG Kottegoda
Department of Computational Mathematics, General Sir John Kotelawala Defence University
Rathmalana, Sri Lanka
kapilak@kdu.ac.lk

2022 3rd International Conference for Emerging Technology (INCET) | 978-1-6654-9499-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/INCET54531.2022.9824855

***Abstract* — Smart contracts are an attractive aspect of blockchain technology. A smart contract is a piece of executable code that runs on top of the blockchain and is used to facilitate, execute, and enforce agreements between untrustworthy parties without the need for a third party. This paper offers a review of the literature on smart contract applications in intellectual property management. The goal is to look at technology advancements and smart contract deployment in this area. The theoretical foundation of many papers published in recent years is used as a source of theoretical and implementation research for this purpose. According to the literature review we conducted, smart contracts function automatically, control, or document legally significant events and activities in line with the contract agreement's terms. This is a relatively new technology that is projected to deliver solutions for trust, security, and transparency across a variety of areas. An exploratory strategy was used to perform this literature review.**

Keywords— intellectual property, blockchain, smart contracts

I. INTRODUCTION

A blockchain is a continuously expanding list of data blocks that are cryptographically connected to one another. The previous block, a timestamp, and any necessary transaction data are normally included in the blocks that make up the chain. The most well-known association of blockchain is with Bitcoin [1]. It serves as the Bitcoin network's backbone and allows its fundamental functions. However, despite this connection, blockchain technology is more widely applicable. Its primary features are particularly appealing in sectors that demand precise and secure record-keeping and administration. For this reason, banks have found a lot of success. The use of blockchains to record transaction details is a natural use of the technology. Blockchains are resistant to retroactive modifications due to their mathematical properties.[2] The immutability of blockchain data is critical for ensuring security and giving credibility to the legitimacy of the data contained inside. The majority of blockchain ledgers are also open to the public. They are maintained and seen by the public. This is also necessary to maintain the blockchain's security. In general, blockchain has evolved into a novel solution to solve traditional computer challenges from a unique outlook. The issue of intellectual property management is one such challenge that we hope to solve. The use of blockchain technology to implement intellectual property can eliminate third-party registration agencies, notarize all intellectual property rights so that they can't be tampered with, greatly improving the efficiency of intellectual property rights protection, and solving the tedious and complex problems of intellectual property services.

Furthermore, due to the popularity of blockchains, smart contracts have received significant attention in recent years. Nick Szabo originally described a smart contract in 1997 [3], which is a computerized transaction system that implements the terms of a contract. A smart contract is a piece of business logic that runs on a blockchain to enable multi-party agreements easier to negotiate, verify, execute, and implement. Smart contracts basically automate contract execution by including the parties' obligations, as well as limitations, validation criteria, and business logic for completing the transaction. Smart contracts further improve data transparency and strengthen the legitimacy and validity of business processes regulating transactions inside the blockchain network by validating, verifying, and adding restrictions. Smart contract security, on the other hand, is a systematic engineering problem that must be investigated from a global viewpoint, and a complete research of smart contract security concerns is urgently needed. The objective of this review is to analyze the applicability and feasibility of mechanisms such as smart contracts and address the fundamental aspects of blockchain that might pose security concerns in smart contracts within the field of intellectual property.

II. METHODOLOGY

A literature review technique was used to conduct this literature exploration study [4]. The foundation for tracing the evolution of blockchain technology, especially for increasing domains in smart contract implementation, is a literature evaluation on smart contract applications. There are four steps to the literature review in this study [4]. The first stage is to go through the study goals and methods. The second stage entails doing a literature review and practical screening of materials on smart contract concerns. The third stage evaluates the papers' quality and data extraction. Finally, the findings are analyzed in the fourth stage.

A. Planning Phase

The examination of objectives and protocols is an important part of the literature study that must be completed [6]. The purpose of the literature review, the creation of the literature procedure and criteria, data extraction techniques, data analysis, and presentation of the review results are all covered in this stage.

B. Selection Phase

The scientific publications assessed in the second stage of the study were gathered from research papers in the Google Scholar, IEEEXplore, ScienceDirect, arXiv, SSRN, etc. Scientific papers relevant to the review topic, notably blockchain and smart contracts, are used as review material. Because this is a new technology, the time frame for searching this paper was determined. Publications of various categories, such as journal papers, conference papers, and white papers, are explored. Following the retrieval of the results, the filtering procedure is carried out to ensure that the papers received are the correct ones. This screening procedure removes papers that aren't related to the issue, as well as research on smart contracts, duplicates, and publications for which we can't get the entire text.

C. Exclusion and inclusion criteria

This step eliminates papers that aren't relevant or appropriate for the study topic, papers that aren't full, and publications that can't be downloaded or accessed. Then, at this step, any papers that aren't relevant to blockchain technology or smart contracts are removed. Following the exclusion phase, the next stage is to choose inclusion criteria, which include journal papers, peer-reviewed conference papers and publications that meet the inclusion requirements for smart contract applications.

D. Synthesis

The last stage of this review is to collect data or information from publications to serve as material for studying, analyzing, and identifying smart contract application implementation in intellectual property management. The extraction is carried out utilizing qualitative procedures at this point.

III. BLOCKCHAIN BASED INTELLECTUAL MANAGEMENT SYSTEMS

A. Types of blockchain

1) Blockchain that is open to the public (permissionless): Any user might access permissionless blockchains. Each member has the ability to play any position in the system, including node, full node, and miner [7]. Because of the characteristics listed above, these blockchains are frequently referred to as public blockchains [8]

2) Blockchain for private (permissioned) use: Each user in a permissioned blockchain system has a certain set of available roles. Miners could be a small group of users who have been pre-selected and identified [9]. Other users may be free to take on the roles of nodes and full nodes in general, or the entire system may be invitation-only.

3) Hybrid blockchain (consortium): Users can control who has access to the information held on the blockchain in this type of decentralized network. Aside from that, a piece of blockchain information or documents may be made public while the remainder of the information in the private network is kept as private as possible. The blockchain hybrid network is adaptable, allowing users to access a private blockchain alongside a variety of public blockchains [10].

B. Transactions

A transaction is a state transition in the blockchain that moves data from one value to another. A bitcoin transaction, a smart contract, a record, or data storage can all be part of a blockchain transaction. The three different types of blockchain transactions [11] are listed below:

1) On-chain: Happen on the distributed ledger and are visible to everyone in the network. The numerous details of the transaction are recorded on the block and distributed to the entire blockchain, making it irrevocable because it cannot be modified. For a transaction to be complete, miners must agree on a certain number of confirmations. Furthermore, network congestion affects completion. As a result, when there is a significant volume of transactions awaiting confirmation, transactions may be delayed.

2) Off-chain: Take place outside of a main blockchain and aren't visible to the rest of the network. The parties concerned have the option of reaching an agreement outside of the blockchain. It may also include a guarantor, who is in charge of validating the transaction's completion and declaring that the agreement has been followed. The real transaction is then completed on the blockchain after the involved entities outside the network agree. These transactions can be carried out in a variety of ways, including multi-signature technology and credit-based systems. In comparison to on-chain transactions, off-chain transactions are completed instantly.

3) Hybrid: Incorporate characteristics of both on-chain and off-chain transactions into a single transaction. Different factors, including as cost, decentralization, storage, privacy, and so on, are used to divide operations into on-chain and off-chain categories.

IV. EXISTING SYSTEMS

A. Conventional Legal Paperwork

Currently, intellectual property, including digital assets, is controlled through traditional legal agreements [12], [13]. For a variety of reasons, this obsolete and outdated strategy has perpetuated the status quo. When considering the different advantages and disadvantages listed, the disadvantages significantly outnumber the advantages. The existing system identifies and binds the transfer of intellectual property using traditional legal documents. Due to the nature of the assets being analyzed, this strategy is both outdated and difficult to implement. Due to the very fluid and adaptable nature of digital items, it is absurd to believe that such contracts can even be enforced. Identifying the assets that are being considered is quite tough. The paperwork's confusing and opaque language makes it easy to mislead someone. A legal mediator, such as an attorney or a judge, is required for this process. To acknowledge the contractual commitments, a centralized authority is required. Regional and country-specific differences in laws may cause complications. Finally, both sides will incur significant financial costs because of this process.

B. Multimedia Content Protection Techniques

In general, a content protection approach can be characterized as a method of safeguarding multi-media material from hazards posed by unlawful access by a single user or a group of users. All these essential security

properties should be addressed by any end-to-end content protection mechanism. As a result, an end-to-end copyright protection system is intended to guarantee security both before and after content transmission, i.e., it ensures permitted content access and limits content usage while it is in the user's possession. [14]. Some of the multimedia protection approaches such as encryption, watermarking, digital rights management, and fingerprinting are discussed in the following section.

1) Encryption for Multimedia

Standard encryption methods, such as symmetric cryptographic algorithms, are used to encrypt the full multimedia. Many new audio and video encryption technologies have recently been proposed to avoid the simplistic approach and improve efficiency. Full encryption, combined compression and encryption, scalable encryption, and other unique techniques are among them. Confidentiality, integrity, and authenticity are all provided by this method.

2) Digital Rights Management (DRM)

Digital rights management (DRM) is a broad word that refers to a set of regulations, strategies, and tools that govern how digital content is used [15]. Simply defined, a DRM system controls how content is used. This system's main features are numerous. They include facilitating the packaging of raw content into an appropriate form for easy distribution and tracking, protecting the content for tamper-proof transmission, protecting the content from unauthorized use, and enabling the specification of appropriate rights, which define the modes of content consumption.

3) Digital Watermarking

The process of embedding the given watermark information (such as possessory name, symbol, signature, etc.) into the protective information (such as picture, sound, video) and picking the given watermark information from the protective information, which is not perceived by the human perceptual system, is referred to as digital watermarking technique.[16]

4) Fingerprinting Multimedia

Multimedia fingerprinting can trace back the identity when an unlawful copy is discovered. This is accomplished by embedding a unique user-specific fingerprint in several copies of the same information. A multimedia fingerprinting algorithm consists of three steps: fingerprint generation, embedding, and pirate traceability from illegal copies.

V. RELATED WORK

Industry and academia have recently begun to examine the use of blockchain technologies to preserve intellectual property rights. According to current research, blockchain is a transparent and dependable ledger that is used to tackle copyright protection issues encountered by content owners and creators, such as rights attribution certificates, data integrity, authenticity, piracy tracing, and transparency.

The authors of reference [17] propose a blockchain-based system that uses smart contracts to ensure copyright compliance of multimedia items. To record the transaction details of all the data contributed to the blockchain, the suggested system employs a data lake, an off-chain centralized storage option. To secure the privacy and validity of the data kept in the data lake, it is encrypted and digitally signed. The stored data can only be accessed by authorized users if the majority nodes have agreed to verify their digital signatures and access privileges.

Peng et al. [18] propose a system that simulates the entire system and uses the public chain to create a secure digital copyright management system. This method eliminates the need for a centralized organization and allows copyright owners and users to trade directly. Use digital watermarking, the improved Blockchain, perceptual hash function, smart contract, ElGamal encryption algorithm, and IPFS in this system to provide a new option for digital copyright protection in the fast-growing Internet era.

To aid content providers' demand for an effective approach to manage digital rights management, Kishigami et al. [19] introduced a decentralized blockchain-based high-definition video copyright management system. For digital content delivery, the blockchain technology promotes the optimum decentralized design. Mining technology and a nonce are used to add transaction information to the blockchain. The proof-of-work system ensures the blockchain's security.

Chi et al. [20] present a blockchain-based eBook transaction system that allows writers and readers to buy books directly from one other without the need for intermediaries. Any user can be an author or a buyer of eBook material in the proposed system. Although there are no intermediate fees because the transaction is direct, the security of eBook contents and eBook purchase transactions cannot be guaranteed. In the absence of trust parties, they suggested a secure and reliable eBook direct transaction mechanism that solves all security issues.

Based on the blockchain model, the Bhowmik et al. [21] proposes a new distributed and tamperproof media transaction framework. The proposed Multimedia Blockchain system is based on a self-embedding watermarking technique that use compressed sensing to detect tampering and restore original information.

For effective protection of music copyright and copyright owners' rights, Zhao and O'Mahoney [22] presented BMCProtector, a prototype solution based on an Ethereum blockchain and smart contract technology. BMCProtector encrypts the audio file with the AES algorithm, tracks ownership of the music file off-chain with vector quantization (a watermarking approach) and controls the copyright of music during distribution and usage with an off-chain access control mechanism (DRM).

Fei presents BDRM, a blockchain-based DRM solution that allows for fine-grained usage management, in [23]. Copyright management functions, such as copyright registration and copyright transactions, are handled by BDRM using a smart contract. In addition, the blockchain has a revolutionary authorization tree. When a user performs a rights transaction, a useful digital watermark is implanted, and digital content distribution is done in the encryption domain. The transaction is subsequently recorded on the blockchain, and the authorization tree is updated. The content is encrypted using the content owner's secret key and stored in a distributed file system (IPFS).

VI. RESULTS

This section compares and analyzes the various blockchain-based Intellectual property management strategies discussed in related works section. *TABLE I.* breaks down the identified technologies in the selected papers.

TABLE I. COMPARISION OF RELATED WORK

Reference	*Data automation*	*Blockchain*	*Content*	*Protection*
Vishwa & Hussain(2018) [17]	dApp	Permissioned	-	Encryption
Peng et al.(2019) [18]	dApp	Permissioned	Image	Encryption + Watermarking
Kishigami et al.(2015) [19]	-	Permissioned	Video	DRM
Chi et al.(2020) [20]	-	Self-developed	Document	ECC Encryption
Bhowmik & Feng(2017) [21]	Smart Contract	-	Image	Watermarking
Zhao (2020) [22]	Smart Contract	Permissionless	Audio	Content Fingerprinting
Fei(2019) [23]	Smart Contract	Consortium	-	Watermarking

All the related work are based on various content protection approaches and meet the minimum standards. In numerous publications, smart contracts are bundled together to establish a blockchain-enabled dApp to automate the needed functionality between the copyright owner and the customers. Most of the papers that were chosen, employ a permissioned blockchain, which means that there is a control layer on top of the blockchain that is managed by a trusted authority that oversees allowing actions to be conducted by the authorized system entities. Many of the papers are proof-of-concepts that have not been tested in a real-world setting.

VII. DISCUSSIONS

Most of the blockchain based systems analyzed only focus on the technological benefits, leaving aside the actual implementation. Designing a practical blockchain based framework that focuses on the technical and implementation details is crucial to evaluate the performance by analyzing the computational overheads and the total response time. Moreover, smart contracts transactions should be designed to prove the long-term effectiveness by conducting a security analysis. Therefore, the problems of security and privacy regarding smart contracts must be investigated. Studies should be carried out to further address the cost and limitation of deploying such system.

VIII. CONCLUSION

Blockchain has the potential to be widely used in copy-right protection and intellectual property management applications, according to academics. Copyright owners and consumers can engage without the need for costly intermediaries thanks to blockchain-based copyright protection systems. Content owners can use these applications to upload copyrighted content, control licensing and copyright options, manage distribution, track pirate sources, and get fees for content usage.

However, there are still several unresolved issues that need to be explored and analyzed further to develop usable intellectual property management applications that can fully benefit from blockchain technology. However, the success of such applications is contingent on a variety of aspects connected to blockchain technology, including as scalability, dependability, and market adoption, which are difficult to predict. When building and implementing a new blockchain-based content protection mechanism, researchers must examine all these factors.

ACKNOWLEDGMENT

I would like to extend my gratitude to Dr. ADAI Gunasekara and Dr. KGKG Kottegoda for their kind cooperation and support.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.” [Online]. Available: www.bitcoin.org

[2] 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, doi: 10.1109/ACCESS.2020.2969990.

[3] N Szabo, “The Idea of Smart Contracts,” 1997.

[4] C. Okoli and K. Schabram, “A guide to conducting a systematic literature review of information systems research,” 2010.

[5] J. Webster and R. T. Watson, “Analyzing the past to prepare for the future: Writing a literature review,” MIS quarterly, pp. xiii–xxiii, 2002.

[6] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, “Lessons from applying the systematic literature review process within the software engineering domain,” Journal of systems and software, vol. 80, no. 4, pp. 571–583, 2007.

[7] I.-C. Lin and T.-C. Liao, “A Survey of Blockchain Security Issues and Challenges,” Int. J. Netw. Secur., vol. 19, pp. 653–659, 2017.

[8] M. Salimitari, M. Chatterjee, M. Yuksel, and E. Pasiliao, “Profit Maximization for Bitcoin Pool Mining: A Prospect Theoretic Approach,” in Proceedings - 2017 IEEE 3rd International Conference on Collaboration and Internet Computing, CIC 2017, Dec. 2017, vol. 2017-January, pp. 267–274. doi: 10.1109/CIC.2017.00043.

[9] X. Wang et al., “Survey on blockchain for Internet of Things,” Computer Communications, vol. 136, pp. 10–29, 2019, doi: https://doi.org/10.1016/j.comcom.2019.01.006.

[10] M. Zarour et al., “Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records,” IEEE Access, vol. 8, pp. 157959–157973, 2020, doi: 10.1109/ACCESS.2020.3019829.

[11] F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” Telematics and Informatics, vol. 36. Elsevier Ltd, pp. 55–81, Mar. 01, 2019. doi: 10.1016/j.tele.2018.11.006.

[12] “United States SEC, ‘Intellectual property transfer agreement,’” https://www.sec.gov/Archives/edgar/data/1383312/000119312507072385/dex104.html.

[13] “PARLIAMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA Printed on the Order of Government.”

[14] Z. Ma, “Digital rights management: Model, technology and application,” China Communications, vol. 14, no. 6, pp. 156–167, 2017, doi: 10.1109/CC.2017.7961371.

[15] S. R. Subramanya and B. K. Yi, “Digital rights management,” IEEE Potentials, vol. 25, no. 2. pp. 31–34, 2006. doi: 10.1109/MP.2006.1649008.

[16] L. Robert and T. Shanmugapriya, "A study on digital watermarking techniques," International journal of Recent trends in Engineering, vol. 1, no. 2, p. 223, 2009.

[17] A. Vishwa and F. K. Hussain, "A Blockchain based approach for multimedia privacy protection and provenance," in 2018 IEEE Symposium Series on Computational Intelligence (SSCI), 2018, pp. 1941–1945. doi: 10.1109/SSCI.2018.8628636.

[18] W. Peng, L. Yi, L. Fang, D. XinHua, and C. Ping, "Secure and Traceable Copyright Management System Based on Blockchain," in 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Dec. 2019, pp. 1243–1247. doi: 10.1109/ICCC47050.2019.9064101.

[19] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu, "The Blockchain-Based Digital Content Distribution System," in 2015 IEEE Fifth International Conference on Big Data and Cloud Computing, Aug. 2015, pp. 187–190. doi: 10.1109/BDCloud.2015.60.

[20] J. Chi, J. Lee, N. Kim, J. Choi, and S. Park, "Secure and reliable blockchain-based eBook transaction system for self-published eBook trading," PLoS ONE, vol. 15, no. 2, Feb. 2020, doi: 10.1371/journal.pone.0228418.

[21] D. Bhowmik and T. Feng, "The multimedia blockchain: A distributed and tamper-proof media transaction framework," in 2017 22nd International Conference on Digital Signal Processing (DSP), Aug. 2017, pp. 1–5. doi: 10.1109/ICDSP.2017.8096051.

[22] S. Zhao and D. O'Mahony, "BMCProtector: A Blockchain and Smart Contract Based Application for Music Copyright Protection," in Proceedings of the 2018 International Conference on Blockchain Technology and Application, 2018, pp. 1–5. doi: 10.1145/3301403.3301404.

[23] X. Fei, "BDRM : A Blockchain-based Digital Rights Management Platform with Fine-grained Usage Control," 2019.