Towards Designing a Blockchain-Based Model for E-Book Publishing

Maznun Arifa Mohammadan Makhtar[1], Novia Admodisastro[2], Suleymenova Laura Askarbekkyzy[3]
Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Selangor, Malaysia[1,2]
South Kazakhstan Pedagogical University, Shymkent, Kazakhstan[3]

***Abstract*—This paper examines the application of blockchain technology in e-book publishing by analyzing previous research and identifying current limitations. The study investigates how smart contracts and cryptographic algorithms can facilitate agreements between publishers and authors. While blockchain has been widely adopted in digital publishing domains, such as image, video, music, and scientific journals, research on its application to e-books remains limited. Existing solutions typically address individual challenges such as transaction transparency, authenticity, or copyright protection, but rarely integrate them into a single framework. To provide a systematic synthesis of prior works, this paper develops a taxonomy of blockchain-based e-book publishing models across six dimensions: platform, storage, smart contract usage, cryptographic algorithm, tokenization, and actors. This paper reviews seven (7) blockchain-based models in e-book publishing and identifies their limitations. Based on these insights, a conceptual blockchain-based smart contract model for e-book publishing was proposed using Ethereum platform, incorporating InterPlanetary File System (IPFS) storage and cryptographic algorithms. The proposed model has the potential to significantly enhance the security and rights protection for authors and publishers, thereby fostering a more secure and equitable e-book publishing landscape.**

Keywords*—*e-book publishing; Ethereum; blockchain technology; smart contract

I. Introduction

The book publishing industry has been a central component in the creation and dissemination of knowledge through books, magazines, journals, articles, dictionaries, and other reading materials. As technology evolves, many people read and distribute digital content online. However, digital publishing is vulnerable to illegal downloads, copying, content sharing, and piracy. Some issues regarding copyright law in the digital environment are a lack of transparency about the legal status of copyrighted works, piracy, and difficulties in getting compensated fairly [1]. This scenario also occurs in the publishing industry, where publishers need to ensure the e-book is secure while protecting the author's and publisher's rights.

An electronic book, also known as an e-book, is a digital version of traditional reading materials. The term "e-book" has been changing depending on the way it is presented and the evolution of technology [2]. Recent research in e-book publishing shows that non-transparent transactions, unfair royalty distribution, unprotected copyright, and unauthenticity of published materials are the main problems for digital content creators in this era. E-book publishing has created a trustless environment, as nobody is responsible for the security, validity, and ownership of the purchased e-book [3]. The authors do not have complete control over their e-books after publication. Non-transparent transactions may deny the actual sales reports to the authors [4]. The e-book's sales history is difficult to track and not tamper-proof, leaving it vulnerable to illegitimate alteration and unauthorized distribution. Unprotected copyright protection may lead to unfair royalty payments because the authors were unable to track each sales transaction [5]. In addition, published e-books lack authenticity because their content can be replicated, reproduced, and redistributed unethically. Unauthenticated e-books may affect total sales and the royalty paid to the authors [6].

Blockchain has significantly contributed to digital publishing, including image, video, music, scientific journals, and e-book publishing. The concept of blockchain was initially proposed by Satoshi Nakamoto in 2008. Nakamoto introduced Bitcoin, a cryptocurrency that allows a peer-to-peer electronic cash system [7]. Blockchain is a data structure that operates in a decentralized, peer-to-peer network consisting of a chain of blocks. Each block contains transactions and also a hash value from the previous block, which makes it immutable and tamper-proof [8]. Distributed ledger technology (DLT) is the main characteristic that enables all transactions to be stored in a blockchain [9]. DLT allows data exchange between the network participants without intermediaries [10]. Blockchain works on a consensus algorithm, a mechanism used among the participants (nodes) to agree on the transactions [11]. Blockchain creates an audit trail of transactions between participants. Therefore, payment can be made directly without the intervention of a third party, such as a financial institution, because blockchain can act as a mediator for data transformation or calculation [12]. When blockchain is combined with smart contracts and cryptography, it can help solve problems of trust, authenticity, and copyright protection in e-book publishing [6].

This paper examines prior work to gain a deeper understanding of the design, methods, algorithms, limitations, and weaknesses. A blockchain-based conceptual model for e-book publishing using the Ethereum platform was proposed to address all those challenges. The model incorporates the InterPlanetary File System (IPFS) and a smart contract to provide three key benefits: transparent transactions, e-book authenticity, and copyright protection to the authors through fair royalty distribution.

Unlike the previous study, which focuses on a single or two aspects such as transparency of transactions, authenticity, or copyright protection, this study integrates all three elements into a single conceptual model. The combination of IPFS,

cryptographic mechanisms, Ethereum smart contract, and multi-actor involvement reflects the structure of the real e-book publishing ecosystem. This holistic approach constitutes the core novelty of this work and directly addresses the identified research gap, thus adding value to the current body of knowledge.

The rest of this paper is structured as follows: Section II presents the research contribution; Section III presents the background information; Section IV reviews related works; Section V introduces the taxonomy of blockchain-based e-book publishing, and Section VI explains the proposed conceptual model; Section VII presents the discussion, and finally, Section VIII concludes with future work.

II. Research Contribution

This study contributes to the domain of blockchain-based e-book publishing by addressing the specific challenges of e-book distribution. While prior work has proposed solutions focusing on isolated aspects, such as transparency, authenticity, or copyright protection, these solutions rarely integrate these elements into a unified framework. The contributions of this paper are:

- Conceptual model for e-book publishing: The proposed model integrates Ethereum smart contracts with InterPlanetary File System (IPFS) storage and cryptographic algorithms to ensure transparent transactions, authenticity verification, and copyright protection.
- Multi-actor involvement: unlike previous work that primarily emphasizes author-customer interactivity or self-publishing, this model incorporates the publisher and the author as key participants alongside the customer. This reflects the practical realities in the e-book publishing industry.
- Comparative analysis and gap identification: Through a comparative review of seven (7) related blockchain-based models, this study identifies key limitations in existing approaches. The proposed model explicitly addresses these gaps by combining transaction transparency, e-book authenticity, and automated royalty payment within a single conceptual framework.
- Development of a taxonomy: This paper develops a taxonomy that classifies blockchain-based e-book publishing models across six dimensions: platform, storage, smart contract usage, cryptographic algorithms, tokenization, and actors. The taxonomy provides a structured framework for comparing prior works and identifying research gaps, thereby establishing a theoretical reference for future studies.

III. Background

A. Electronic Book (E-Book) Publishing

The first e-book development started in the 1970s by Project Gutenberg and the Oxford Text Archive. Project Gutenberg was initiated by Michael Hart in 1971 at the University of Illinois, and the first e-book published was "Declaration of Independence," followed by "Bill of Rights" in 1971 [13]. These publications led to Hart's other big idea: to create the world's first e-book library. In 1976, the Oxford Text Archive focused on providing electronic academic resources to scholars. From the 1980s to the 1990s, the development of e-books expanded to several formats and media. The publishers gain more confidence in publishing e-books for academic areas and linking with libraries as a niche market. In 1989, e-books were published on Compact Disc Read-Only Memory (CD-ROM) and could be accessed using computers [14]. Since then, several discussions about digital copyright have started.

E-book publishing experienced massive growth alongside technological development. E-books can be accessed on multiple devices, such as PDAs, Pocket PCs, e-book readers, and mobile phones [15]. A new horizon of e-books started when Amazon introduced the Kindle in 2007. Kindle changes the reader's reading behavior because it provides readability flexibility [16]. Other e-book readers, such as Barnes & Noble Nook and Kobo, also entered the market due to their convenience and cost-effectiveness.

The potential and benefits of adopting blockchain technology into publishing, specifically intellectual property and monetary rights, have been addressed. The most important highlight is self-publishing 3.0, which means a direct transaction between the authors and readers without intervention from any third party [17]. Instead of self-publishing, some authors may need to publish their books through a publisher. In the e-book publishing process, the process can be classified into three (3) elements: content providers, service platforms, and reading devices [16]. The end-user is the customer who accesses the e-book by downloading it onto their reading devices. Generally, e-book publishing is the same as physical books, but with additional parties involved in digitization. The entire process of e-book publishing is illustrated in Fig. 1.

Fig. 1. E-book publishing process.

The parties involved in e-book publishing are as follows: 1) author: the person who writes a manuscript to be published by the publisher and owns the copyright of their respective work; 2) publisher: the organization or company that processes the author's manuscript to be published in digital format, manage copyright, receive sales payment and pay royalty to the author and 3) customer(s)/subscriber(s): the potential buyer of the e-book.

The publishing process begins when the author(s) write and send a manuscript to the publisher. The manuscript will be evaluated before approval for publication. The publisher will decide on the e-book format with the consent of the author(s). Then, the process of developing an e-book begins with editing and proofreading. Some of the e-books might need illustration and design. The programming part will be done to integrate the

multimedia elements and the system used. The final e-book product format varies, typically PDF or EPUB. The e-book will be published on various websites and mobile platforms, including the App Store, Google Play, and the Huawei App. The customer(s) or subscriber(s) will purchase the e-book from the selling platform and access it on their devices.

Previous related works [4], [5] have suggested that blockchain is a better solution for e-book publishing due to its characteristics, which can provide transparency, integrity, and immutability. The following section will discuss the explanations of blockchain, decentralized repository systems, and smart contract.

B. Blockchain

In recent years, blockchain technology has expanded far beyond cryptocurrencies. Blockchain has been applied in various industries, including healthcare, automotive, insurance, agriculture, advertising, and education [18]. Blockchain's decentralized peer-to-peer networks and distributed ledger technology features benefit businesses by providing transparency, immutability, security, and tamper-resistance. Blockchain will mitigate all risks of a "principal-agent" problem, which then shapes the blockchain character as "trustless" or "trust-free" [19].

Blockchain is a chain of blocks linked together using cryptographic algorithms that permanently record transactions in a large, distributed ledger. Each block stores the hash of the previous block, and a new block is created when the sender submits a transaction. This security feature in blockchain makes it extremely difficult to manipulate the data. The latest block will undergo mining before being added to the chain. Mining is a data validation process that involves solving a specific algorithm. Miners will validate and verify the transactions using various consensus protocol mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS). This protocol ensures that peers have the same data in the blockchain [8]. Every transaction in the blockchain is timestamped, and once added, it cannot be changed.

Depending on its objectives, each organization may choose the type of blockchain that best meets its requirements. Each type of blockchain has different characteristics and functionalities. There are three (3) main types of blockchain: public (permissionless) blockchain, private (permissioned) blockchain, and consortium/federated blockchain [20].

- A public blockchain is open-access, decentralized, and allows any node to enter the network. The nodes read, write, and validate the data through a consensus mechanism. No individual or organization owns the public blockchain, which is self-governing. Examples of public blockchains are Bitcoin, Ethereum, and Litecoin.
- A private blockchain is a centralized blockchain managed by an organization or authority. It is usually applied to small businesses and has limited use within private entities. Only authorized users can view the data and transactions within the network. Corda and Ripple are examples of private blockchains.
- Consortium or Federated blockchain is a combination of public and private blockchain in which a part of the blockchain is partially centralized. Only selected nodes can choose the services they intend to participate in, and the remaining nodes can only access transactions, not the consensus process. Hyperledger Fabric is an example of a Consortium blockchain.

Shukla [21] provided an overview of blockchain research and outlined a future agenda, highlighting how blockchain applications are expanding beyond cryptocurrency into domains such as copyright protection and publishing. This perspective reinforces the timeliness of applying blockchain in e-book publishing.

The following section will discuss the Ethereum blockchain and its components: the repository system, smart contracts, and cryptographic algorithms.

1) Ethereum blockchain: The Ethereum Blockchain is an open-source, public (permissionless) blockchain platform with smart contract functionality that can verify a predetermined set of rules. Any node can join the Ethereum network if the user has an Ethereum client account [12]. Fig. 2 illustrates the deployment of the e-book publishing model in the Ethereum blockchain by executing a smart contract on the Ethereum Virtual Machine. This decentralized machine can execute smart contract code in Ethereum nodes. A dApp is a decentralized application that acts as a web interface to connect users with a smart contract.

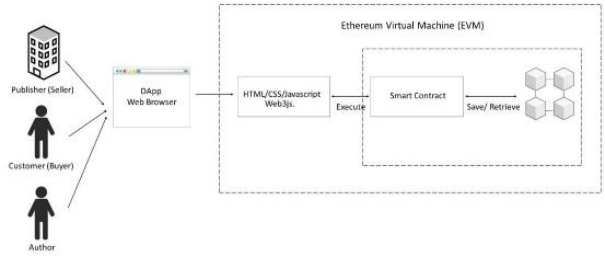

Fig. 2. Decentralized blockchain-based e-book publishing architecture (Nurgaida Yutia et al., 2022) adapted with permission.

In e-book publishing, a public (permissionless) blockchain is better suited for adaptation because the system requires involvement from both internal and external parties, such as publishers, authors, and customers. Furthermore, the system aims to facilitate a safe, secure trading environment for all stakeholders. Public blockchains provide high transparency, enabling authors and publishers to access sales and royalty records. Ethereum is an example of a public blockchain that offers functionality beyond cryptocurrency and has been widely used to develop decentralized applications (dApps) to support business management processes.

2) Smart contract: A smart contract is one of the main components of the Ethereum blockchain. A smart contract refers to a programmable agreement embedded in the blockchain that automatically enforces predefined rules between stakeholders. It works as a contract between two (2) or more parties that has been electronically transformed. A smart

contract allows code to specify how the process should be managed, and it provides a distributed, unchangeable record of all events that have occurred [18]. The key elements of smart contracts are the elimination of trusted third parties, forger assistance, transparency, autonomous execution, accuracy, and paperless motivation [14].

In e-book publishing, a smart contract is an agreement between the author(s) and the publisher. A smart contract can automate royalty payments without intermediaries. Publishing rights, such as the author's copyright and the publisher's ownership, can be securely recorded on the blockchain, making them verifiable and legitimate. Smart contract programmed using Solidity Programming Language on a web-based Integrated Development Environment (IDE), Remix. Smart contracts do not involve any third party to create an agreement between the author(s) and the publisher.

3) Repository system: Blockchain architecture is designed around a consensus mechanism, and decentralization requires full participation by nodes. The expansion in transaction volume will increase data storage in parallel with the involvement of nodes to maintain its stability [22]. Therefore, there is a need for an alternative way to store large amounts of data in decentralized storage systems such as InterPlanetary File System (IPFS), PFS, Storj, SWARM, Filecoin, and Sia.

IPFS is a globally distributed system widely used in the Ethereum Blockchain environment. While blockchain can provide high security, storing data on it would be very expensive. Currently, the Ethereum chain size is around 500GB – 1TB, and every node should be able to store the data. If the block expands, it would not be feasible for the blockchain to perform the transactions [23]. IPFS can store large files, and the data links or hashes are stored on the blockchain. A cryptographic algorithm in IPFS made it immutable. IPFS uses a content-addressing technique to store files. The distributed storage system architecture in IPFS guarantees the accessibility of the data on the network because all the peers have exact copies of the data [24]. If the data has been modified, IPFS will compute a new hash and update it across peers.

For example, Pubchain, a solution for academic resource publications in the Ethereum blockchain, uses IPFS for publication storage, was proposed by [25]. Authors will upload their articles to the system, and the articles will be time-stamped. The articles will be registered in the blockchain as permanent records and stored in IPFS, with metadata created accordingly. The smart contract will write the metadata into the blockchain.

4) Cryptographic algorithm: Cryptographic algorithms are the backbone of blockchain. Blockchain and smart contracts use various cryptographic algorithms to ensure the authenticity, integrity, and privacy of data. These algorithms are vital in securing transactions, ensuring immutability, and enabling blockchain functionality. Some algorithms that are commonly used are:

a) Hash functions: Cryptographic hash functions formed from the Merkle-Damgard method need one input: the message to be hashed [26]. A hash function is a one-way function that is not reversible. One input produces a single, fixed-length output, called a hash value. A hash function can ensure the integrity and authenticity of a message. Message Digest (MD) and Secure Hash Algorithms (SHA) are examples of hash functions.

b) Public-key cryptography: Encryption and decryption of a message using a pair of keys assigned to the corresponding receiver. The readable message will be encrypted with the receiver's public key and decrypted with the receiver's private key. Only the receiver can encrypt the message, thus providing confidentiality and authenticity. Public-key cryptography is the technology behind digital wallets in the blockchain [27]. Examples of public-key cryptography are Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC).

c) Digital signatures: Mathematical techniques for verification and authentication of a digital message by assigning a pair of keys, private-public keys, with the involvement of a signer and verifier [28]. A digital document will be signed using the sender's private key, and the verifier will verify the originator by decrypting it with the sender's public key. Digital signatures are often used with hash functions to verify the authenticity and integrity of a message.

C. Blockchain in Digital Publishing

Studies from 2020 to 2023 show that the work of blockchain models for digital publishing has mainly been developed for other assets, such as image publishing [29], music streaming [30], scientific publications [31], video publishing [32] and the student's academic record [33]. Nevertheless, the implementation of blockchain in e-book publishing has not been extensively explored. The existing work is unsuitable for e-books because its process flow and architectural design differ from those of e-books.

Therefore, this study will focus on implementing blockchain technology in e-book publishing to provide transparency, authenticity, and copyright protection. Blockchain can enable secure transactions and potentially create a new business model. Trusted distributed ledger technology is the primary reason blockchain should be used in the publishing industry. Every e-book published has its respective copyright owner. The publisher must retain the transaction records and reasonably manage the author's royalties.

In the blockchain e-book publishing scenario, there are five (5) practical use cases.

- Track of history records: Blockchain can record every transaction. The records are transparent and can be viewed by everyone; therefore, the origins of the transactions are traceable.
- Royalty payment systems: The Ethereum blockchain can give authors a fair royalty distribution by constructing a smart contract with pre-determined rules. The author must verify the smart contract before the e-book is up for sale. Royalty will be delivered automatically without the intervention of a third party, such as a financial institution or publisher. The author will receive the royalty after every successful customer purchase.

- Piracy prevention: e-Book publishing is easily exposed to various kinds of piracy, such as copying, illegal downloading, reprinting, and redistribution. Blockchain, using cryptographic algorithms, can mitigate the risks of any fraud.
- Copyright protection: A smart contract in blockchain enables fixed copyright registration and allows creative rights.
- Cost-effective for large data storage: e-Book size varies depending on the content. Some publishers use a large, centralized storage system, which is both costly and complex. Others might use the cloud, but costs will increase as data grows. However, blockchain and peer-to-peer storage systems, such as IPFS, can provide decentralized, secure storage at minimal cost.

IV. Related Works

This section describes seven (7) related works on e-book publishing using the blockchain model found in the literature. These works serve different objectives, involve various entities, utilize different platforms, employ distinct processes, and employ diverse methods.

IPFS-Blockchain-Based Authenticity of Online Publications proposed by [6] aim to provide authenticity and integrity of published digital content in different versions of original e-books (languages). The proposed model is demonstrated in a system that uses the Ethereum blockchain and smart contracts to ensure the authenticity and integrity of the e-book. The system utilized IPFS to store the data, as it is more cost-effective than blockchain storage. E-book hash data will be generated in IPFS and stored in the blockchain. The hash will be retrieved when the transaction matches it with the database. If the hash has been altered, the original content has been modified. By using this method, only authentic, original e-books will be sold to customers.

Another blockchain model proposed by study [5] protects the author's copyright and transparency in transactions by providing a transparent sales ledger that could be accessed by the publisher, author, and customers. The model shown in Fig. 3 was built on the Ethereum blockchain, using a smart contract to track e-book sales. Every transaction will be verified by consensus and digitally signed using Elliptic Curve Cryptography (ECC) before being stored in the blockchain. Both the author and the publisher must deposit twice the actual book price for double verification. After the authorization process, half of the deposit will be refunded to the authors, and the publisher will get a full refund and the sales percentage. The royalty payment will be made immediately to the author upon completion of the transaction, thereby eliminating the need for third-party involvement and ensuring high reliability, integrity, and security.

An intellectual property trading system, named JS Digital Asset Trading System, was developed for e-book trading [34]. Only authorized persons can access the e-book in this system; only authentic books can be sold to customers. The system used Asymmetric Key Encryption (AKE), in which the author uses his public key to encrypt the e-book before uploading it into the system. Then, when the customer purchases the e-book, the author will decrypt it with his private key. The e-book will be encrypted again using the customer's public key and sent to the customer. The customer needs to decrypt the e-book using their private key. This approach ensures the security and authenticity of the trading process. However, the study did not discuss any solutions for royalty distribution among publishers and authors.

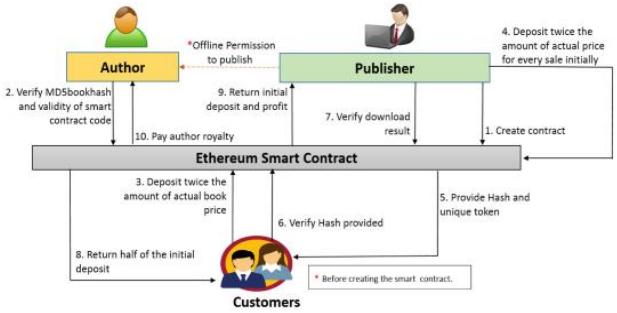

Fig. 3. Blockchain-based protection for author royalty of digital asset system architecture.

Another blockchain-based trading system scheme has been proposed by [35]. The JSP Digital Asset Trading System was developed to provide transparency, as the digital asset owner can view the transactions and receive payment immediately after the transaction (refer to Fig. 4). The "Random-Checker Proof of Stake" consensus mechanism was used to reduce transaction time, while AKE is used for verification. The proposed system uses a smart contract to allocate the share percentage between the authors. However, the proposed system does not involve the publisher.

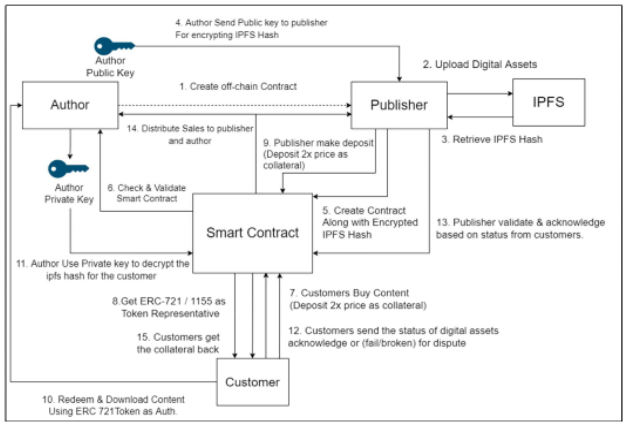

Fig. 4. Blockchain-based protection of author royalty of digital asset system overview.

A blockchain-based eBook market system proposed by [3] could facilitate self-publishing by enabling transparent transactions. The authors will receive direct payments from the system without intermediaries. In this system, a book can be sold by the chapter or as a whole. The proposed system uses a smart contract to ensure reliability, copyright protection, and the security of e-book transactions.

A Non-Fungible Token (NFT) is a unique identifier for digital assets that allows users to purchase ownership rights to those assets. NFTs are typically applied to collectible items, such as games, music, and art. A blockchain-based NFT model

was proposed by [36] for e-book publishing, it allows the author to sell individual chapters and the entire e-book. This model utilizes IPFS as an external storage system to reduce costs and energy consumption. An NFT e-book is linked with a smart contract to ensure security and preserve the owner's copyright. However, NFT item procurement uses a bidding system, meaning the potential buyer must bid on the e-book's price within a limited timeframe. The successful buyer will have ownership of the e-book if the author accepts the offer. Furthermore, NFT items are typically sold in limited quantities to preserve their uniqueness. Therefore, the publisher must create a unique e-book, for example, by offering an e-book with additional audio of the authors reading several chapters.

The last related work is by study [4] which enhances the earlier work of [5]. They proposed adding security features to the data links of smart contract digital assets using Elliptic Curve Cryptography (ECC). In earlier work, the data link for digital assets in smart contracts is in plain text, making it vulnerable to attack. Therefore, ECC is used to encrypt data links, thereby strengthening data integrity and authenticity. Smart contracts are also used for sales, payments, and royalty distribution between author and publisher. In addition, IPFS is used for data storage, and ERC-721 is used as a standard for token-based authorization. ERC-721 is a standard for non-fungible tokens on Ethereum, meaning each asset is unique.

A. Discussion of Related Works

Table I summarizes the comparison of the existing related work in blockchain-based e-book publishing. In conclusion, although they are in the same domain, each related work has its own primary objectives and is developed based on its specific needs and requirements. However, every work has its limitations and boundaries. Both [4], [5] proposed the same three (3) objectives: to provide transparency, to preserve copyright, and to ensure e-book authenticity. Although [6] and [34] proposed solutions for authenticity, their solution differs in their system architectures. The work by [6] involved authors, the main publisher, secondary publishers, and customers, whereas the work by [34] involved only authors and customers. Other work with the involvement of two (2) parties is by [35] and [3]. Both works suggested a service application for the author to self-publish their e-books. No publisher is involved in this process; thus, the purchasing transaction will be made only between the authors and customers. Another solution by [36] suggested non-fungible tokens (NFTs), a token representing a unique digital asset that could allow an individual to have ownership of the author's work. This model also involves the author and the customers. The variation in actor involvement highlights a critical distinction across existing models. Some approaches reflect a broader publishing ecosystem, while the solution involves direct interaction between customers and authors. Models that exclude publishers may be practical for independent distribution. Still, they do not capture the realities of e-book publishing, where publishers play a key role in validation, e-book management, and royalty distribution. The differences observed in actor participation further justify the need for structured classification. Therefore, to synthesize these variations and to better position the proposed conceptual model, this study introduces a taxonomy of blockchain-based e-book publishing models. The detail of the taxonomy is presented in Section V.

While the analysis in Table I highlights the comparison of the objectives, actor involvement, and limitations across existing works, revealing different publishing workflows and priorities, Table II complement by focusing on the technical implementation of these models, specifically the choice of blockchain platform, storage mechanisms, and cryptographic algorithms. Together, these tables offer a complete picture of both functional and technical perspectives of existing solutions.

Referring to Table II, four (4) works were built on the Ethereum blockchain platform [4], [5], [6], [34]. Publishers need a public environment and visibility to market e-books to potential buyers. Hence, Ethereum is the most suitable choice for publishers to trade their products. In [3], [36], the authors did not specifically mention which platform was used in their work, as the proposed solution generally works across any blockchain platform. [35] developed their blockchain platform and utilized their own cryptocurrency, JSP Coin.

However, six (6) out of seven (7) models use smart contract despite three (3) works not being built in Ethereum [3], [35], [36]. This is because the smart contract can also be deployed to other blockchain platforms. For example, a smart contract can be applied to Hyperledger Fabric using a "chaincode" package [37].

Regarding storage systems, four (4) works utilize IPFS, and three (3) works use other storage, such as local storage and blockchain storage. E-book files could be large, especially for books with illustrations and graphics. Storing e-books on the blockchain would be very costly; therefore, a better option would be a decentralized storage system, such as IPFS, Storj, or SWARM. Work by [5] applied cloud-based storage, but it could also be extended into other decentralized storage systems.

Related work shows that various cryptographic algorithms have strengthened the system's security. A hash function is the standard algorithm used because the hash is part of an element in the blockchain. If the e-book files are stored in IPFS, the IPFS hashes will be stored on the blockchain. The hash function is crucial to ensure the e-book is not modified during the transaction. Apart from that, [5] specifically mentioned the use of MD5Hash and IPFS hash in their solutions.

Digital signatures are also an essential feature of blockchain. A digital signature ensures the authenticity of the data transmission on the blockchain network. Various types of digital signatures were used in the study, including Elliptic Curve Cryptography (ECC), Elliptic Curve Digital Signature Algorithm (ECDSA), and Asymmetric Key Encryption (AKE). From the study, every solution used at least one digital signature method. The work by [3] is more comprehensive, which explains why a greater number of methods were employed in their solutions. A study by [36] explores the possibility of adapting non-fungible tokens (NFTs) to e-book publishing; specifically, the ERC-721 standard enables authors to create crypto assets. In e-book publishing, digital signatures are crucial to ensure that a real publisher uploads the authentic e-book. The customer will verify the e-book signature by decrypting it using the publisher's public key.

TABLE I. COMPARISON OF PREVIOUS RELATED WORKS OF BLOCKCHAIN IN E-BOOK PUBLISHING

No.	Authors	Proposed Work	Objectives	Actors	Limitations
1.	[6]	IPFS-Blockchain-Based Authenticity of Online Publications	Authenticity, Integrity	Author, publisher, customer	• Author creates smart contract, publisher validates it • No discussion on payment/royalty
2.	[5]	Blockchain-based Framework for Protecting Author Royalty of Digital Assets	Transparency, Copyright, Authenticity	Author, publisher, customer	• Both publisher and buyer must deposit 2× book price • May affect usability
3.	[34]	JS Digital Asset Trading System	Transparency, Authenticity	Author, customer	• 4× encrypt–decrypt process • 3× e-book transfers over network • Author must always be active to decrypt
4.	[35]	JSP Digital Asset Trading System	Transparency, Copyright	Author, customer	• Only author & buyer involved • Developed own blockchain platform • Uses its own cryptocurrency (JSP Coin) • Marketplace style, no publisher role
5.	[3]	Blockchain-based eBook Market System for Self-Publishing	Transparency, Copyright, Authenticity, Confidentiality, Validity, Integrity	Author, customer	• Designed for self-publishing only • Relies on third-party service application
6.	[36]	Non-Fungible Tokens (NFTs) for Publishing	Copyright	Author, customer	• NFT better for special/collectible editions • Buyer must bid in limited timeframe • Ownership can be resold
7.	[4]	Blockchain-based Protection of Author Royalty of Digital Assets	Transparency, Copyright, Authenticity	Author, customer	• Publisher & buyer must deposit 2× book price • Similar limitations to Nizamuddin et al. (2019)

TABLE II. SUMMARY OF STORAGE, PLATFORM, AND ALGORITHM USED IN BLOCKCHAIN-BASED E-BOOK PUBLISHING

No.	Authors	Smart Contract	Storage	Platform	Cryptographic Algorithm				Token / NFT
					Symmetric Encryption	Asymmetric Encryption	Digital Signature	Hashing / Integrity	
1.	[5]	✓	IPFSa	Ethereum	Not applicable	Not applicable	✓ (Not specified)	✓ (Not specified)	✓ (conceptual token – CID)
2.	[6]	✓	IPFS	Ethereum	Not applicable	✓ (ECCc)	✓ (ECCc)	✓ (MD5b)	✓ (digital token – unspecified)
3.	[34]	N/A	Not specified	Own platform	Not applicable	✓ (RSAf)	Not applicable	Not applicable	Not applicable
4.	[35]	✓	Not specified	Own platform	✓ (AESd)	✓ (public/private key)	✓ (Tx signature)	Not applicable	Not applicable
5.	[3]	✓	Not specified	Ethereum	✓ (AES)	Not applicable	✓ (ECC)	✓ (MACe)	Not applicable
6.	[36]	N/A	Not stated	Not stated	Not applicable	Not applicable	Not applicable	Not applicable	✓ (NFTs – conceptual)
7.	[4]	✓	IPFS (implied)	Ethereum	Not applicable	✓ (ECC)	✓ (ECC)	Not applicable	✓ (NFTs – implied)

[a]IPFS – InterPlanetary File System, [b]MD5 – Message-Digest Algorithm, [c]ECC – Elliptic Curve Cryptography, [d]AES – Advanced Encryption Standard, [e]MAC – Message Authentication Code, [f]RSA – Rivest-Shamir Adleman

V. TAXONOMY OF BLOCKCHAIN-BASED E-BOOK PUBLISHING MODELS

To systematically evaluate the diversity of blockchain applications in e-book publishing, this study develops a taxonomy framework that classifies prior works across six dimensions: platform, storage, smart contract usage, cryptographic algorithm, tokenization, and actors involved. This taxonomy serves two (2) purposes: first, to consolidate scattered findings into a structured framework; and second, to highlight the positioning of the proposed conceptual model within the broader research landscape.

As summarized in Table III, most models rely on the Ethereum blockchain, while some use custom-built or other blockchain platforms. Storage mechanisms vary from centralized cloud storage to decentralized solutions such as IPFS. For instance, [38] proposed a cross-chain copyright protection scheme in which storage and verification are distributed across multiple blockchains, supported by arbitration and supervision entities. This approach demonstrates how storage mechanisms can be extended beyond single-chain IPFS or cloud solutions. Smart contracts are primarily used in these solutions. The cryptographic algorithm implemented includes symmetric encryption (e.g., AES), asymmetric encryption (e.g., RSA, ECC), digital signatures (e.g., EDCSA, transaction-based signatures), and hashing (e.g., MD5, SHA). Similarly, the SecureRights framework by [39] enhances authenticity and digital rights management (DRM) by combining a blockchain smart contract with cryptographic watermarking, fingerprinting, and IPFS. This demonstrates how cryptographic techniques can be extended beyond conventional encryption and hashing to support end-to-end protection of digital content. Tokenization ranges from none to fungible tokens to NFTs used to represent ownership or incorporate publishers as intermediaries in the distribution process.

TABLE III. TAXONOMY OF BLOCKCHAIN-BASED E-BOOK PUBLISHING MODELS

Dimension	Categories / Options	Examples in Literature
Platform	Ethereum, Own Blockchain, Other (e.g., Hyperledger)	[4], [5], [6], [35]
Storage	On-chain, Cloud-based, IPFS / Decentralized	[6] – IPFS; [35] – NFT + external storage
Smart Contract	Royalty automation, Authenticity verification, Marketplace	[5] – Royalty automation; [3] – Marketplace
Cryptographic Algorithm	AES, RSA, ECC, Hashing (MD5, Keccak256, SHA)	[34] – RSA; [3] – AES + MAC
Tokenization	None, Fungible Token (ERC-20), Non-Fungible Token (ERC-721)	[36] and [4] – NFT;
Actors Involved	Author + Customer, Author + Publisher + Customer	Most self-publishing models involve Author + Customer; the Proposed model includes the publisher.

The taxonomy framework is illustrated in Fig. 5, which visualizes the classification across six dimensions. The diagram highlights how blockchain-based models can be categorized based on their technical implementation and functional scope. Together, Table III and Fig. 5 provide a comprehensive reference structure for analyzing similarities and differences among blockchain-based approaches to e-book publishing.

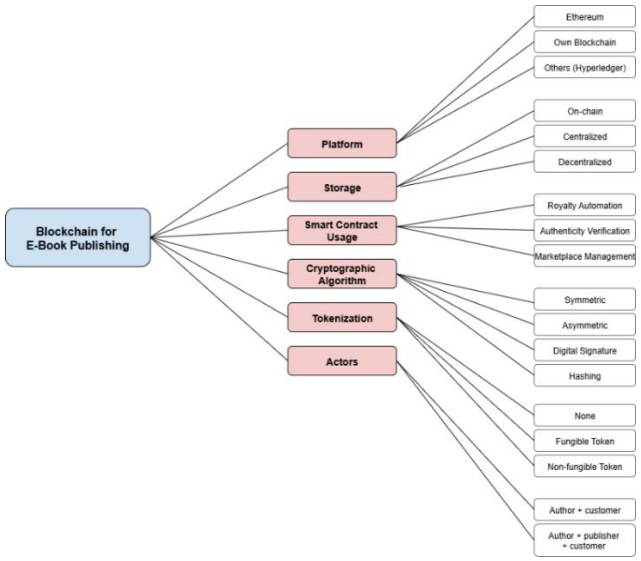

Fig. 5. Taxonomy of blockchain-based e-book publishing models.

A key insight from this taxonomy is that existing works are often fragmented, with most solutions addressing only one or two dimensions at a time. For example, [6] focus primarily on authenticity and storage (IPFS), while [36] highlight copyright protection via NFTs, but overlook encryption and publisher involvement. Similarly, [34] implements asymmetric cryptography but lacks integration with decentralized storage. Few models integrate multi-actor involvement, hybrid cryptography, and automated royalty payments within the same framework. This observation underlines the distinctiveness of the proposed conceptual model, which consolidates these features into a unified approach designed for practical application in e-book publishing.

VI. PROPOSED SOLUTIONS

This section presents a proposed conceptual model of blockchain-based e-book publishing using a smart contract on the Ethereum blockchain. The model aims to provide transparent transactions, verify the authenticity of e-books, and protect authors' copyright by delivering fair royalties and payments to publishers. Fig. 6 provides a general overview of the Blockchain-based E-Book Publishing conceptual model and the interactions among the parties involved with a smart contract on the Ethereum blockchain. This proposed model cannot be applied to self-publishing authors and the marketplace, as there is no direct participation of the publisher and customer. It involves four (4) main actors: the author(s), the publisher, the customer, and the smart contract.

The proposed model applies to a single publisher, which could facilitate e-book marketing and distribution through the publisher's sales platform. The business procedures and internal system processes will take place as follows:

- The publisher will upload an encrypted, signed e-book to the external storage IPFS.
- The details of the e-book, such as the title, price, author(s), and book category, will be added to the system. The contract will be initiated, but it is noted that it is not yet official.
- Hash code generated from IPFS will be stored in the blockchain.
- The author will be notified about the new contract and receive a request for e-book hash verification.
- The author will verify the new contract and the hash code to validate the authenticity of the e-book uploaded into the system. After the author's verification, the new contract will be officially created. The e-book will now be visible for sale.
- Customers will request an e-book by sending a purchase request to the system.
- The request will be notified and reviewed. Upon acceptance, the smart contract will generate the payment request function. The customer will be authorized first to ensure that they are a legitimate buyer.
- The customer should deposit the payment.
- The payment will be validated. The transaction will be aborted if the customer fails to pay within the allocated time.
- Upon successful payment, the smart contract will request the user to verify the e-book hash value for authentication.
- The hash verification by the customer. This ensures the authenticity of the e-book and that the person verifying the hash is the actual purchaser.

- A download link will be provided if the hash verification is successful.
- The customer will download or may access the e-book from IPFS.
- Successful download/access notifications will be sent to the smart contract.
- After a successful download, the smart contract will notify the author and publisher of the sales.
- Royalty payment to the author(s) and sales payment to the publisher will be delivered according to the pre-determined rules set up at the beginning of the smart contract's creation.
- Alternatively, the author(s) and publisher can also request the sales statement from the system.

To further illustrate how the proposed model can be applied in the e-book publishing environment, consider a real e-book purchase by a customer. When the customer initiates the purchase, the smart contract triggers an authenticity verification by comparing the e-book's IPFS hash with the metadata hash stored on the blockchain. If the values match, the system grants access to the encrypted file and automatically releases royalty payments to the author and publisher in accordance with predefined rules. This IPFS-anchored hash verification pattern has been widely adopted in blockchain-based digital publishing applications, indicating its practical feasibility [6], [40], [41], [42].

The following section discusses the theoretical and practical implications of this study, situates the model within the existing body of knowledge, and highlights its potential relevance to stakeholders in the e-book publishing industry.

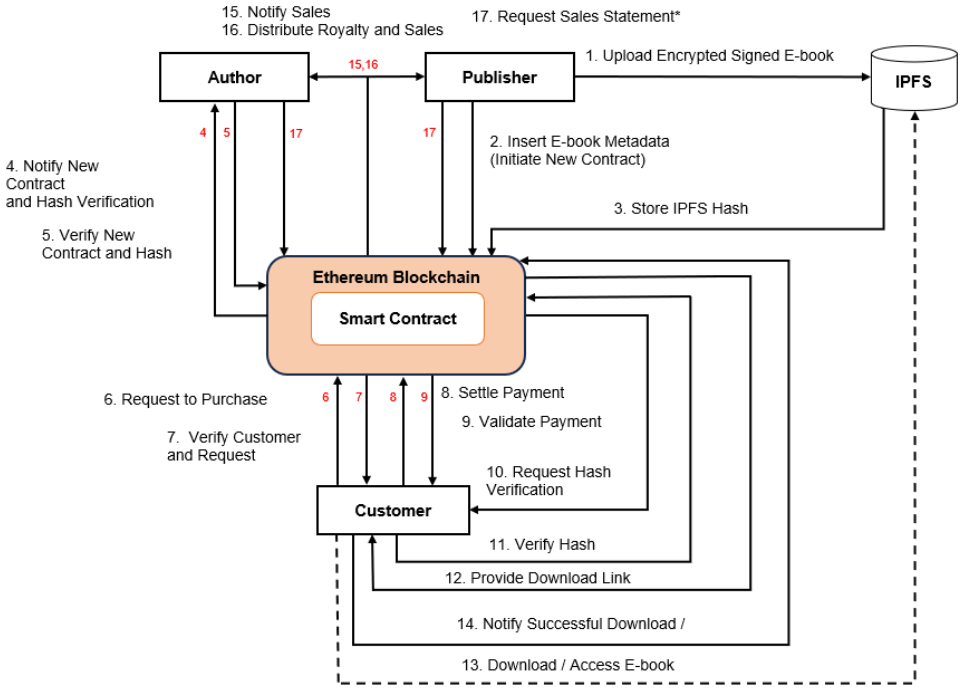

Fig. 6. The conceptual model of blockchain-based e-book publishing.

VII. Discussion

The proposed conceptual model addresses the limitations observed in prior work on the blockchain-based e-book publishing approach. Tables I and II, together with the proposed taxonomy, give a clear overview of how the proposed model is different from previous blockchain-based e-book publishing solutions. While past studies mostly focused on one or two specific functions, such as transaction transparency or authenticity, this study combines multiple essential elements, including storage, cryptographic methods, and actor involvement, into one complete and realistic workflow.

Beyond outlining the model, it is necessary to consider the broader implications for theory and practice, as well as the limitations that will shape future work.

A. Research Implications

This study contributes to the theoretical and practical insights into the domain of blockchain-based e-book publishing, as described below:

1) Theoretical implications: The paper advances blockchain research by locating e-book publishing as a distinct case within digital content publication, where interaction between the authors, publisher, and customers is more complex compared to music and image publishing. By integrating an Ethereum smart contract, IPFS, and a cryptographic algorithm, this model demonstrates how multi-actor relationships can be supported transparently and securely. This study develops a taxonomy for a blockchain-based model of e-book publishing,

classifying it across six dimensions. This taxonomy provides a structured framework for synthesizing prior works and systematically identifying research gaps, thereby serving as a reference for future studies. This aligns with broader blockchain research by [21], which emphasizes the importance of structured frameworks and systematic taxonomies in advancing the blockchain research agenda. The comparative review of seven (7) models further strengthens theoretical understanding by highlighting persistent issues around transparent transactions, e-book authenticity, and copyright protection.

2) Practical implications: For publishers, this model offers a pathway to improve the copyright protection for authors by enforcing automated royalty distribution, thus reducing disputes and building trust in e-book publishing transactions. The model enhances copyright protection through two mechanisms: 1) each e-book will be authorized by the author using hash verification, and 2) royalty payments are executed automatically through smart contracts, ensuring transparency and reducing the sales record manipulation. Author benefit from enhanced visibility and control over sales records, addressing their long-standing concern about the transparency of the royalties. Customers gain assurance that the purchased e-books are authentic and verified. For policymakers, the model demonstrates how blockchain can be applied beyond cryptocurrency to support intellectual property protection. The taxonomy also has practical implications for decision-makers, enabling stakeholders to evaluate existing blockchain solutions based on platform, storage, smart contract usage, cryptographic algorithm, tokenization, and the actors involved. Unlike the previous blockchain model for the digital content that focused on a single function, such as authenticity or transparency, the proposed model's significance lies in its ability to integrate multiple critical e-book publishing functions into a unified and automated workflow.

B. Research Limitations

Although this study contributes to a conceptual blockchain-based model for e-book publishing, several limitations must be acknowledged. First, the research is still conceptual in nature and has not yet been validated through a prototype implementation or testing. In addition, the model is currently limited to a single-publisher scenario. Thus, the model does not apply to a self-publishing and marketplace developed by a third party.

While blockchain offers transparency, e-book authenticity, and robust copyright protection in e-book publishing, its implementation in the real world faces several key challenges. One of the main issues is scalability. Transaction processing time and gas fees can increase significantly when transaction volume is high, potentially delaying e-book verification and payment confirmation. Another key limitation is user adoption. Publisher, author, and customer may not be familiar with blockchain operations, which could slow adoption, especially when the transaction process involves additional steps such as e-wallet creation or gas fee payments. Finally, the integration with existing e-book publishing infrastructure requires the publisher to adjust its internal operations and administrative organization, which can increase the operational costs and complexity. These factors need to be considered to ensure the system's effectiveness, cost efficiency, and usability in practical development.

VIII. Conclusion and Future Works

This paper examined existing blockchain-based approaches to e-book publishing. Through a comparative analysis of seven (7) related works, the persistent gaps in ensuring transparent transactions, e-book authenticity, and copyright protection for the authors are identified. To address these gaps, a conceptual blockchain-based model was proposed that leverages Ethereum smart contract, IPFS, and cryptographic algorithms to provide transparency, authenticity verification, and fair royalty distribution.

The study makes four (4) key contributions: 1) a conceptual model that integrates transparency, authenticity, and copyright protection in a unified model, 2) explicit inclusion of multi-actor involvement – author, publisher, and customer, reflecting real-world e-book publishing process, 3) comparative analysis of prior models to identify limitations and position of the proposed solution, and 4) the development of the taxonomy that establishes a theoretical reference for future study. Together, these contributions provide both theoretical value by advancing blockchain research in e-book publishing and practical significance by offering a foundation for the publishers and authors to adopt with secure e-book distribution mechanisms.

While no prototype or simulation was conducted at this stage, it sets the groundwork for future development. Planned work includes implementing a prototype in Solidity and Ethereum with IPFS storage, evaluating its feasibility with experts, and conducting experimental performance validation in a real e-book publishing scenario. Expanding the model to multi-author environments and integration with tokenization mechanisms, such as NFTs, is also part of the future directions.

From a feasibility perspective, implementing this model on the Ethereum network needs to take into consideration gas fees and scalability constraints. Transaction costs can increase during peak network usage, affecting the user experience. However, using a second layer (Layer-2) solution such as Polygon or Arbitrum can help reduce costs and speed up transactions [43]. Future studies could explore these combinations to improve system performance. By pursuing these next steps, the proposed model can evolve into a validated solution that enhances trust, fairness, and security in the e-book publishing ecosystem.

References

[1] A. Savelyev, "Copyright in the blockchain era: Promises and challenges," Computer Law and Security Review, vol. 34, no. 3, pp. 550–561, Jun. 2018, doi: 10.1016/j.clsr.2017.11.008.

[2] L. Manley and R. P. Holley, "History of the Ebook: The Changing Face of Books," Technical Services Quarterly, vol. 29, no. 4, pp. 292–311, Oct. 2012, doi: 10.1080/07317131.2012.705731.

[3] 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.

[4] M. I. S. Ayasy and A. M. Barmawi, "Protecting Author Royalty of Digital Assets Using Blockchain and Elliptic Curve Cryptography," Institute of

Electrical and Electronics Engineers (IEEE), Jan. 2022, pp. 86–92. doi: 10.1109/gecost55694.2022.10010412.

[5] N. Nizamuddin, H. Hasan, K. Salah, and R. Iqbal, "Blockchain-Based Framework for Protecting Author Royalty of Digital Assets," Arab J Sci Eng, vol. 44, no. 4, pp. 3849–3866, Apr. 2019, doi: 10.1007/s13369-018-03715-4.

[6] N. Nizamuddin, H. R. Hasan, and K. Salah, "IPFS-blockchain-based authenticity of online publications," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer Verlag, 2018, pp. 199–212. doi: 10.1007/978-3-319-94478-4_14.

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

[8] P. Zheng, Z. Jiang, J. Wu, and Z. Zheng, "Blockchain-Based Decentralized Application: A Survey," IEEE Open Journal of the Computer Society, vol. 4, pp. 121–133, 2023, doi: 10.1109/OJCS.2023.3251854.

[9] C. Tuteja, N. Saxena, P. Johri, and V. R. Vadi, "Blockchain Technology: A case study of its Decentralized Use," in 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing, COM-IT-CON 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 771–775. doi: 10.1109/COM-IT-CON54601.2022.9850511.

[10] A. H. Mohammed, A. A. Abdulateef, and I. A. Abdulateef, "Hyperledger, Ethereum and Blockchain Technology: A Short Overview," in HORA 2021 - 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings, Institute of Electrical and Electronics Engineers Inc., Jun. 2021. doi: 10.1109/HORA52670.2021.9461294.

[11] N. Six, N. Herbaut, and C. Salinesi, "Blockchain Software Patterns for the Design of Decentralized Applications: A Systematic Literature Review," Blockchain: Research and Applications, vol. 3, no. 2, Jun. 2022, doi: 10.1016/j.bcra.2022.100061.

[12] T. Ali Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations," IEEE Access, vol. 7, pp. 176838–176869, 2019, doi: 10.1109/ACCESS.2019.2957660.

[13] C. Armstrong, "Books in a virtual world: The evolution of the e-book and its lexicon," Sep. 2008. doi: 10.1177/0961000608092554.

[14] T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on blockchain based smart contracts: Applications, opportunities and challenges," Mar. 01, 2021, Academic Press. doi: 10.1016/j.jnca.2020.102857.

[15] M. Vassiliou and J. Rowley, "Progressing the definition of 'e-book,'" Library Hi Tech, vol. 26, no. 3, pp. 355–368, 2008, doi: 10.1108/07378830810903292.

[16] C. C. Lin, W. C. Chiou, and S. S. Huang, "The challenges facing e-book publishing industry in Taiwan," in Procedia Computer Science, Elsevier B.V., 2013, pp. 282–289. doi: 10.1016/j.procs.2013.05.037.

[17] An Alliance of Independent Authors, "Authors and the Blockchain Towards a Creator Centered Business Model," London. Accessed: Oct. 17, 2024. [Online]. Available: https://www.allianceindependentauthors.org/wordpress/wp-content/uploads/2017/07/Authors-and-the-Blockchain_Towards-a-Creator-Centered-Business-Model.pdf

[18] H. Guo and X. Yu, "A survey on blockchain technology and its security," Blockchain: Research and Applications, vol. 3, no. 2, Jun. 2022, doi: 10.1016/j.bcra.2022.100067.

[19] P. De Filippi, M. Mannan, and W. Reijers, "Blockchain as a confidence machine: The problem of trust & challenges of governance," Technol Soc, vol. 62, Aug. 2020, doi: 10.1016/j.techsoc.2020.101284.

[20] C. H. V. N. U. Bharathi Murthy, M. L. Shri, S. Kadry, and S. Lim, "Blockchain based cloud computing: Architecture and research challenges," IEEE Access, vol. 8, pp. 205190–205205, 2020, doi: 10.1109/ACCESS.2020.3036812.

[21] A. Shukla, P. Jirli, A. Mishra, and A. K. Singh, "An overview of blockchain research and future agenda: Insights from structural topic modeling," Journal of Innovation and Knowledge, vol. 9, no. 4, Oct. 2024, doi: 10.1016/j.jik.2024.100605.

[22] M. Kassab, "Exploring Non-Functional Requirements for Blockchain-Oriented Systems," in Proceedings of the IEEE International Conference on Requirements Engineering, IEEE Computer Society, Sep. 2021, pp. 216–219. doi: 10.1109/REW53955.2021.00040.

[23] "Decentralized Storage | ethereum.org." Accessed: Oct. 17, 2024. [Online]. Available: https://ethereum.org/en/developers/docs/storage/

[24] P. A. Lobo and V. Sarasvathi, "Distributed File Storage Model using IPFS and Blockchain," in 2021 2nd Global Conference for Advancement in Technology, GCAT 2021, Institute of Electrical and Electronics Engineers Inc., Oct. 2021. doi: 10.1109/GCAT52182.2021.9587537.

[25] T. Wang, S. Chang Liew, and S. Zhang, "PubChain: A decentralized open-access publication platform with participants incentivized by blockchain technology," in 2020 International Symposium on Networks, Computers and Communications, ISNCC 2020, Institute of Electrical and Electronics Engineers Inc., Oct. 2020. doi: 10.1109/ISNCC49221.2020.9297213.

[26] D. Sharma and M. Saxena, "Different Cryptographic Hash Functions for Security in the Blockchain," in 2023 International Conference on Data Science and Network Security, ICDSNS 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICDSNS58469.2023.10245326.

[27] S. Ahmad, S. K. Arya, S. Gupta, P. Singh, and S. K. Dwivedi, "Study of Cryptographic Techniques Adopted in Blockchain," in 4th International Conference on Intelligent Engineering and Management, ICIEM 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICIEM59379.2023.10166591.

[28] K. Saini, S. Sharma, and U. Sarkar, "Blockchain and Cryptography," in Proceedings - 2022 4th International Conference on Advances in Computing, Communication Control and Networking, ICAC3N 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1863–1868. doi: 10.1109/ICAC3N56670.2022.10074345.

[29] R. Sharma, S. Pawar, S. Gurav, and P. Bhavathankar, "A unique approach towards image publication and provenance using blockchain," in Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology, ICSSIT 2020, Institute of Electrical and Electronics Engineers Inc., Aug. 2020, pp. 311–314. doi: 10.1109/ICSSIT48917.2020.9214203.

[30] Y. Jiang and J. Zhou, "Digital Music Copyright Protection System Based on Blockchain," in 2022 4th International Academic Exchange Conference on Science and Technology Innovation, IAECST 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 962–966. doi: 10.1109/IAECST57965.2022.10062214.

[31] E. B. E. Correa, V. De B. Nascimento, and A. J. G. Abelem, "DASP: Distributed and Autonomic Scientific Publisher Proposal for Editorial Process Management on Permissioned Blockchain," in 2021 3rd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2021, Institute of Electrical and Electronics Engineers Inc., Sep. 2021, pp. 25–26. doi: 10.1109/BRAINS52497.2021.9569805.

[32] J. Zheng, S. Teng, P. Li, W. Ou, D. Zhou, and J. Ye, "A Novel Video Copyright Protection Scheme Based on Blockchain and Double Watermarking," Security and Communication Networks, vol. 2021, 2021, doi: 10.1155/2021/6493306.

[33] M. Maheswari, S. Prasath, R. Rajesh, and D. Ramalakshmi, "Blockchain-based Access Control Model for Student Academic Record with Authentication," in Proceedings of the 7th International Conference on Intelligent Computing and Control Systems, ICICCS 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 1411–1414. doi: 10.1109/ICICCS56967.2023.10142704.

[34] J. Putsorn, S. Nontree, and T. Chomsiri, "JS Digital Assets Trading System," in 2019 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT-NCON), IEEE, 2019. Accessed: Oct. 18, 2022.[Online]. Available: https://ieeexplore.ieee.org/document/8692301

[35] T. Chomsiri and D. Pansa, "JSP Digital Asset Trading System," in 2019 23rd International Computer Science and Engineering Conference (ICSEC), 2019. doi: 10.1109/ICSEC47112.2019.8974847.

[36] M. Rahrouh, W. Alayash, and M. Ghanem, "The Potential Application Of NFT in the Publishing Industry; Opportunities and Challenges," in 2022 International Arab Conference on Information Technology (ACIT), IEEE, Nov. 2022, pp. 1–5. doi: 10.1109/ACIT57182.2022.9994159.

[37] "Deploying a smart contract to a channel — Hyperledger Fabric Docs main documentation." Accessed: Oct. 17, 2024. [Online]. Available: https://hyperledgerfabric.readthedocs.io/en/latest/deploy_chaincode.html

[38] R. Xie and M. Tang, "A digital resource copyright protection scheme based on blockchain cross-chain technology," Heliyon, vol. 10, no. 17, Sep. 2024, doi: 10.1016/j.heliyon.2024.e36830.

[39] T. Madushanka, D. S. Kumara, and A. A. Rathnaweera, "SecureRights: A Blockchain-Powered Trusted DRM Framework for Robust Protection and Asserting Digital Rights," 2024.

[40] J. Anthal, S. Choudhary, and R. Shettiyar, "Decentralizing File Sharing: The Potential of Blockchain and IPFS," in 2023 International Conference on Advancement in Computation and Computer Technologies, InCACCT 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 773–777. doi: 10.1109/InCACCT57535.2023.10141817. [41]M. M. Arer, P. M. Dhulavvagol, and S. G. Totad, "Efficient Big Data Storage and Retrieval in Distributed Architecture using Blockchain and IPFS," in 2022 IEEE 7th International conference for Convergence in Technology, I2CT 2022, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/I2CT54291.2022.9824566.

[41] H. S. Huang, T. S. Chang, and J. Y. Wu, "A secure file sharing system based on IPFS and blockchain," in ACM International Conference Proceeding Series, Association for Computing Machinery, Jul. 2020, pp. 96–100. doi: 10.1145/3409934.3409948.

[42] M. Mandal, M. S. Chishti, and A. Banerjee, "Investigating Layer-2 Scalability Solutions for Blockchain Applications," in Proceedings - 2023 IEEE International Conference on High Performance Computing and Communications, Data Science and Systems, Smart City and Dependability in Sensor, Cloud and Big Data Systems and Application, HPCC/DSS/SmartCity/DependSys 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 710–717. doi: 10.1109/HPCC-DSS-SmartCity-DependSys60770.2023.00101.