applied sciences

MDPI

Review

Blockchain-Based Multimedia Content Protection: Review and Open Challenges

Amna Qureshi * and David Megías Jiménez

Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya (UOC), CYBERCAT-Center for Cybersecurity Research of Catalonia, Castelldefels (Barcelona), 08860 Catalonia, Spain; dmegias@uoc.edu
* Correspondence: aqureshi@uoc.edu

Abstract: In this paper, we provide a holistic survey of multimedia content protection applications in which blockchain technology is being used. A taxonomy is developed to classify these applications with reference to the technical aspects of blockchain technology, content protection techniques, namely, encryption, digital rights management, digital watermarking and fingerprinting (or transaction tracking), and performance criteria. The study of the literature reveals that there is currently no complete and systematic taxonomy dedicated to blockchain-based copyright protection applications. Moreover, the number of successfully developed blockchain-based content protection systems is very low. This points towards a research gap. To fill this gap, we propose a taxonomy that integrates technical aspects and application knowledge and can guide the researchers towards the development of blockchain-based multimedia copyright protection systems. Furthermore, the paper discusses some technical challenges and outlines future research directions.

Keywords: blockchain; digital watermarking; digital rights management; digital fingerprinting; cryptography

Citation: Qureshi, A.; Megías, D. Blockchain-Based Multimedia Content Protection: Review and Open Challenges. *Appl. Sci.* **2021**, *11*, 1. https://dx.doi.org/10.3390/app11010001

Received: 28 November 2020
Accepted: 17 December 2020
Published: 22 December 2020

1. Introduction

Content distribution is a process of digital distribution or delivery of multimedia content such as audio, text, animation and video. Traditionally, multimedia content was distributed through physical exchange of papers, compact discs, or DVDs. With the technological evolution and growth of the Internet, multimedia content in the form of digital formats can be published online through digital distribution channels, such as the Internet-based delivery platforms [1] or peer-to-peer (P2P) file distribution and sharing systems [2], among others. These online distribution platforms have become the de facto standards for content delivery ensuring great performance, wide availability, and cost efficiency. According to the 2019 Global Internet Phenomena Report [3], media streaming applications, and on-demand video [1,4] and audio [5] delivery platforms, constitute a large portion of Internet traffic. However, with the widespread use of these delivery platforms, the safety of the multimedia content, the preservation of copyright, the traceability of copyright violators, and the secure distribution of content have become increasingly ubiquitous problems for content owners, multimedia producers and distributors.

To prevent data from being illegally downloaded and shared, and to track and punish copyright violators, it is important that the multimedia content owners can prove their copyrights over the contents upon copyright infringement. Many traditional content protection technologies, such as encryption [6], Digital Rights Management (DRM) [7], watermarking [8,9], and forensic watermarking (digital fingerprinting) [10–14] have been designed to protect data copyright or content ownership. Though a few of the distribution systems [6–14] address the problems of copyright protection, traceability, and secure content distribution, there are several open issues to be addressed: (1) there does not exist an effective proof-of-delivery mechanism; (2) a deposit is required to place an order for the content before its delivery, which involves a certain risk that the customer may receive

tampered data; (3) the specific information of copyright and transaction is not public to the clients; (4) clients' identities need to be verified through multiple interactions; and (5) often these systems are dependent on centralized trusted third parties for payment, management of the licenses and keys, and generation and verification of the watermark or fingerprint. These trusted third parties are vulnerable to single point failures, compromise and hacking attacks.

The blockchain technology, which is widely known as a mechanism to provide transaction verification, can be used to design a decentralized and transparent multimedia distribution system. The blockchain [15] is a distributed digital ledger of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (i.e., creating resistance against tampering).

In recent years, the blockchain technology has become a source of new hope with its broad spectrum of applications, e.g., finance, health care, supply-chain management or intrusion detection, to name a few. Recently, its footprint can be observed in intellectual property or copyright protection applications. The main attributes of the blockchain technology—i.e., transparency, decentralization, reliable database, collective maintenance, trackability, security and credibility, digital cryptocurrency, and programmable contracts—provide innovative ideas for protecting digital intellectual property and ensuring traceability. In recent years, a rapid development of decentralized applications based on blockchain technology has been observed, but the combination of content protection and blockchain technologies has not received much attention from researchers. Apart from a few commercially available blockchain-based copyright protection platforms [16,17], one can find only a handful of blockchain-based copyright protection schemes in the literature. Recently, the authors in [18] investigated the use of blockchain technology in diverse online multimedia applications, such as music and advertising industries, healthcare, social media, and content delivery networks. Though the descriptive study analyzes the characteristics (target market, underlying platform technologies, consensus protocols and reward system) of the existing blockchain-based online media platforms, the research direction is not focused on addressing the problems related to integration of copyright protection mechanisms with the blockchain technology. Through this research work, we attempt to investigate how copyright infringement-related problems can be resolved using the blockchain technology.

The key contribution of this paper is to provide a holistic survey of multimedia content protection applications that use the blockchain technology. A taxonomy is developed to classify these applications based on technical blockchain characteristics, content protection mechanisms, and performance criteria. To the best of our knowledge, no systematic taxonomy has been defined in the literature to characterize the state-of-the-art of blockchain-based copyright protection schemes. The proposed taxonomy integrates technical aspects and application knowledge to address the challenges with feasible solutions and identify the possible research gaps in blockchain-based copyright protection applications. We believe that the current moment is opportune to present this survey due to recent emergence of copyright protection systems based on blockchain.

The rest of the paper is organized as follows. Section 2 presents the taxonomy of blockchain-based multimedia content protection applications. Section 3 surveys recent work on copyright protection schemes based on the blockchain technology. Additionally, we compared the schemes w.r.t. the attributes defined in the taxonomy. Section 4 provides an overall discussion and reveals a number of insights into the field of research. In addition, the future research directions are outlined. Finally, we present the conclusions of this research work in Section 5.

2. Taxonomy of Blockchain-Based Multimedia Content Protection Systems

This section presents the proposed taxonomy that allows the decomposition and comparison of blockchain-based multimedia content applications in the literature in a systematic manner. This taxonomy identifies the common dimensions and requirements of blockchain-based copyright protection systems. The proposed taxonomy defines seven categories that are further divided into sub-categories. A comprehensive and in-depth classification of the defined categories is graphically represented in Figure 1.

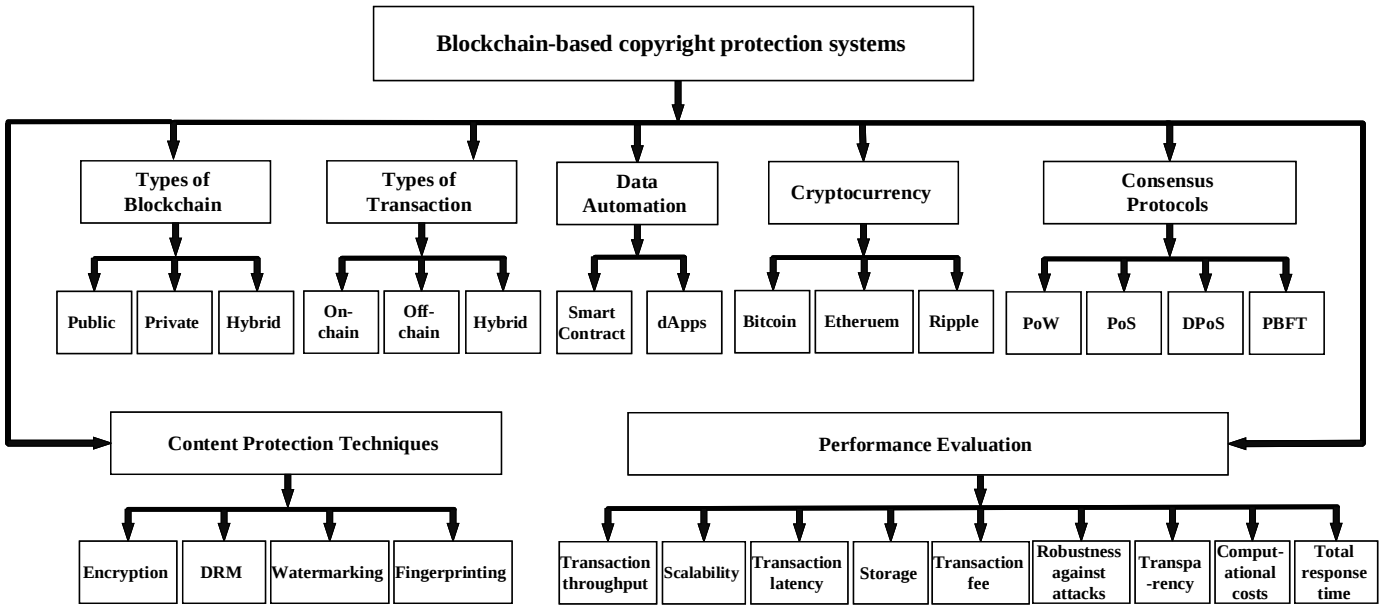

Figure 1. Taxonomy of Blockchain-based Copyright Protection Systems.

2.1. Types of Blockchain

The three possible types of blockchain are listed below:

- Public (permissionless) blockchain: A decentralized blockchain in which any node can join the network with read and write access permissions. It establishes trust through a consensus mechanism that makes the transaction immutable, once it is stored on the network. Since all nodes need to participate in the consensus process, the transaction speed is anomalously slow. Examples of a public blockchain are Bitcoin and Ethereum.
- Private (permissioned) blockchain: A partially decentralized blockchain in which only permissioned nodes can participate in the consensus, accounting and building blocks. It is managed by a trusted party and the encrypted database is commonly shared among the permissioned nodes. An example of this type is MultiChain.
- Hybrid (consortium) blockchain: A type of blockchain that combines “low-trust" offered by public blockchains and the “single highly-trusted entity" model of private blockchains. It has a multi-party consensus mechanism in which all operations are verified by special pre-approved nodes. A few examples include Quorum, Hyperledger, and Corda.

2.2. Types of Transaction

A transaction implies a state transition that changes data in the blockchain from one value to another. A blockchain transaction can involve cryptocurrency, smart contract, record, or data storage. The three different types of transactions on the blockchain are listed below:

- On-chain transactions: These are available on the distributed ledger and are visible to all participants on the network. Different details of this transaction are recorded

on the block and distributed to the entire blockchain, thus making the transaction irreversible as it cannot be altered. For the transaction to be complete, there has to be an agreed number of confirmations by miners. Moreover, the completion depends on network congestion. Consequently, sometimes transactions are delayed in case of a large volume of transactions waiting to be confirmed.

- Off-chain transactions: These occur outside of a main blockchain and are not published on the network. The involved parties can choose to have an agreement outside of the blockchain. In addition, it may involve a guarantor, who is responsible for confirming the completion of the transaction and certifying that the agreement has been honored. Upon agreement by the involved entities outside the blockchain, the actual transaction is then executed on the blockchain. These transactions can be carried out using different methods, e.g., multi-signature technologies, credit-based solutions, among others. Off-chain transactions are executed instantly as compared to on-chain transactions.
- Hybrid transactions: These transactions combine certain aspects of both on-chain and off-chain transactions. The separation of operations into on- and off-chain is based on different criteria, such as cost, decentralization, storage, privacy, etc.

2.3. Data Automation

A self-automated code, also known as a smart contract, consists of a program code, a storage file and an account balance. It is executed by miners that use consensus protocols to agree upon the sequence of actions resulting from the contract's code. Any user can create a contract by posting a transaction to the blockchain. The program code of a contract is fixed when the contract is created and cannot be changed, thus providing immutability. A contract's storage file is stored on the public blockchain. A smart contract can be invoked by entities within (other smart contracts) and outside (external data sources) the blockchain. While executing its code, the contract may read from or write to its storage file. Moreover, it can receive money into its account balance, and send money to other contracts or users. A smart contract is identified by a hash of 160 bits (a hexadecimal address used by many cryptocurrencies, e.g., Ethereum or LiteCoin, among others), and is operated within the environment that supports the use of a public-key cryptography. Smart contracts are widely used in most of the currently existing cryptocurrency networks and are the prominent features of Ethereum. A smart contract can be used to perform one type of transaction, while a distributed application (dApp) can bundle a set of smart contracts together to perform complex transactions. This dApp is a user-friendly interface (similar to a traditional website) that allows users to interact with the smart contracts stored on the blockchain.

Smart contracts could offer a number of benefits, such as accuracy (less prone to manual error), lower execution risk (automatic execution by the network), fewer intermediaries (reduced reliance on third-party intermediaries), lower cost (less human intervention and fewer intermediaries), speed and real-time updates (automated tasks), and new business models (from DRM and watermarking/fingerprinting of multimedia content to automated access to storage units).

2.4. Cryptocurrency

A cryptocurrency is a digital currency that uses cryptography to secure and verify transactions as well as to control the creation of new units of a particular cryptocurrency. The most attractive characteristic of cryptocurrency is its organic nature as it is not issued by any centralized authority (e.g., bank or financial intermediary). The main benefit of using cryptocurrency is that the funds are transferred more easily between any two parties in the transaction. All these transactions are facilitated through the use of public and private keys for security purposes, and are carried out with minimal processing costs. Bitcoin and Ethereum have been the two most popular cryptocurrencies since the emergence of the cryptocurrency phenomenon. Recently, Ripple has emerged as the third

largest cryptocurrency in the trading market [19]. These three cryptocurrencies have a high market cap and a liquidity rate [20], and are the most traded cryptocurrencies on the mainstream trading platforms such as Plus500 [21]. A brief overview of top three cryptocurrencies is presented below:

- Bitcoin is the first P2P payment network of electronic cash based on the blockchain technology. The Bitcoin network adopts a hash-based proof-of-work (PoW) distributed consensus protocol. Bitcoin is pseudonymous, i.e., the funds are delivered to the Bitcoin addresses instead of the real-world identities. The average block creation time is 10 min, and the block size is limited to 1 MB [22], which constrains the network throughput. Moreover, the scalability is limited to 3–7 transactions/second [23]. Moreover, it is vulnerable to hacking attacks and theft, while being completely encrypted.
- Ethereum is an open-source, public, blockchain-based distributed computing platform that uses a proof-of-stake (PoS) consensus mechanism and allows programming of various types of smart contracts within the system. The transferable amount in Ethereum is ether. Any action in Ethereum requires gas, which is used as a fee instead of ether for ease of computations. The average block creation time is 17 s [24], and blocks are limited by a 6.7 million gas [25]. A simple Ethereum transaction can cost around 21,000 units of gas. However, a complicated smart contract can cost a lot more. The scalability of Ethereum is limited to 15–20 transactions/second [26]. Moreover, it is susceptible to security violations due to Solidity Language, causing compromise of stored data.
- Ripple is a for-profit technology platform that allows banks, payment providers, and digital asset exchanges to provide faster payment settlements and offers lower currency exchange costs. XRP is the cryptocurrency used by the Ripple payment network to make cross-border payments. Unlike blockchain mining, the Ripple network uses a unique distributed consensus protocol to validate transactions. This enables faster transactions without any centralized authority. The transactions in the Ripple network are confirmed instantly by the XRP gateways and take roughly 4 s. The Ripple network can process 1500 transactions/second [27]. Since Ripple is pre-mined, there exist little or no incentive for common nodes to work in the network, which subsequently leaves the corporations to provide the validator nodes.

2.5. Consensus Protocols

A consensus mechanism comprises protocols and algorithms, which establish the rules that the nodes (devices on the blockchain that maintain the blockchain and sometimes process transactions) must follow to validate the blocks. This mechanism solves data synchronization between the nodes that do not trust each other in a distributed system. The consensus protocol is a fault-tolerant mechanism that is used to achieve the necessary agreement on a single data value or a single state of the network. It consists of the following objectives: reaching an agreement, collaboration, cooperation, equal rights to every node, and mandatory participation of each node. Most blockchains use one of the following commonly used consensus protocols:

- PoW: The nodes (miners) involved in this process compete with each other to solve a complex mathematical puzzle. The first node to find a solution obtains the right to validate the block to create a new block that implements a transaction. Bitcoin and Ethereum 1.0 use the PoW [28]. However, PoW requires a lot of energy and computer power to reach a consensus, and therefore, it is a very expensive option.
- PoS: The miners in this process are required to prove the ownership of a certain amount of currency tokens to establish their stake. Hence, the more tokens a node has, the more likely it will validate the block, and thus, will determine the authenticity of the block. Dash and Neo use PoS [29]. Ethereum 2.0, an upgrade to the Ethereum blockchain, has switched to PoS [28] from PoW, in order to provide increased scalability and throughput. One of the major drawbacks of PoS is that it promotes “crypto-coin saving", rather than spending.

- Delegated proof-of-stake (dPoS): As a variation of the PoS, dPoS requires all token owners to select a group of delegates, who they trust to participate in the validation process. The nodes with the highest votes then authenticate the transactions. Lisk and BitShares use dPoS [30]. Though dPoS does not require much computing power, it is vulnerable to centralization as the number of witnesses is strictly limited.
- Practical Byzantine Fault Tolerance (PBFT): Byzantine fault tolerance (BFT) refers to reaching a consensus between two nodes communicating safely across a distributed network in the presence of malicious nodes. One of the examples of BFT, PBFT, is designed to be a high performance consensus algorithm that can rely on a set of trusted nodes in the network. PBFT can only tolerate faulty or malicious nodes until the number of such nodes is less than one-third of all the nodes. Since greater number of honest nodes will agree on a correct decision than a faulty or malicious nodes agreeing on an incorrect decision, false information will be rejected by the majority. This mechanism is currently being leveraged by Hyperledger Fabric and Zilliqa [31].

2.6. Multimedia Content Protection Techniques

Generally, a content protection technique can be defined as a measure to protect multimedia data against the threats arising from an unauthorized access to a user or a group of users. The protected properties generally include copy protection, traceability, authentication of content source and receivers, usage control, digital rights associated with the content, and secure distribution of content and access keys. According to Arnold et al. [32], any end-to-end content protection method should address all these basic security properties. Thus, an end-to-end copyright protection system is expected to provide security before and after transmission of the content, i.e., it ensures an authorized access of content, and controls the usage of the content once it is in the user's possession. In the following section, a brief overview of the most effective approaches for multimedia content protection is presented.

2.6.1. Multimedia Encryption

The process of encoding plaintext messages into ciphertext messages is called encryption, and the reverse process of transforming ciphertext back to plaintext is called decryption. This technique is expected to provide one or more of the following properties:

- Confidentiality: It refers to limiting data access or disclosure to authorized users and preventing access or disclosure to unauthorized ones.
- Integrity: It refers to protecting data against modification, or alteration, whether by accident or deliberately.
- Authenticity: It refers to enabling the receiver of data to ascertain its origin.

In the naïve approach, the entire multimedia content is encrypted using standard encryption methods such as symmetric (e.g., Advanced Encryption Standard (AES), Rivest Cipher (RC5), etc.) and asymmetric (Rivest–Shamir–Adleman (RSA), Digital Signature Algorithm (DSA), etc.) cryptographic algorithms. Since the multimedia content such as audio or video data is typically very large in size, the naïve approach becomes computationally demanding. Nowadays, many new encryption algorithms for audio and video have been proposed to avoid the naïve approach and gain better efficiency. These new algorithms can be divided into various categories: full encryption, selective encryption, joint compression and encryption, syntax-compliant encryption, scalable encryption and multi-access encryption.

Another important form of public-key cryptography is the homomorphic cryptosystem, which allows certain types of operations (addition/multiplication (partially homomorphic), or both (fully homomorphic) to be carried out over encrypted data while yielding the same encrypted results as if the operations were run on plaintext. Homomorphic cryptosystems are useful for copyright protection applications as they allow content owners to make computations directly to the ciphertext without exposing the keys. This property prevents the buyers' privacy-sensitive information from being exposed.

2.6.2. Digital Rights Management (DRM)

DRM systems have been developed to provide the secure delivery of digital content to an authorized receiver with restrictions (e.g., copying, printing or editing) on the usage of the content after delivery. A typical DRM system provides means for protecting content, creating and enforcing rights, identifying users, and monitoring of the content usage. A generic DRM architecture consists of three entities: content provider (responsible for generating the multimedia content, its metadata, and the corresponding content encryption keys, and encrypting the content), license provider (responsible for creating licenses and managing the content encryption keys), and a user (who has rights to access the content downloaded via a local software, called a DRM agent). DRM can be implemented as both software (Apple's FairPlay) and/or hardware (smart cards) solutions.

A DRM system is designed to satisfy the following security requirements:

- Unauthorized copying: It ensures that the digital asset is packaged in a secure manner so as to prevent unauthorized usage. This secure packaging is achieved by encryption.
- Secure distribution: It must securely distribute the digital asset to the authorized user.
- Conditional access: It must obtain the access conditions (licenses) specified by the owners of the protected content. The license consists of rights expression language, metadata or watermark, and a security mechanism to prevent users from circumventing DRM by modifying the access conditions.
- Tampering resistance: It must provide an effective tamper-resistant mechanism to process protected data and enforce content usage rights.

The core technologies used by DRM to fight piracy include encryption, passwords, watermarking, digital signature and payment systems. Encryption and password technologies are used to control who has access to the content and how it is used. Watermarks and digital signatures are used to protect the authenticity and integrity of the content, the copyright holders, and the users. Digital watermarking complements DRM to ensure that the digital rights of the copyright holders are not violated. Unlike traditional DRM schemes that compress and encrypt single multimedia content into multiple copies with each copy targeted at a specific application, and provide single access-control, modern DRM systems have been proposed to support encryption of scalable code streams with multiple keys to allow multiple accesses. Since a watermark can be used to identify the original content owner, it discourages a user from misrepresenting the content as if it was his/her own as well as unauthorized distribution or sharing it illegally with unauthorized parties.

2.6.3. Digital Watermarking

Unlike multimedia encryption, digital watermarking provides posterior protection when the multimedia content is decrypted by the authorized users. It imperceptibly alters the original content (host signal) by hiding the identification information (watermark) in it. This information can later prove ownership, and verify the authenticity of the carrier signal. A digital watermarking system generally includes two stages: watermark embedding and extracting. In the embedding algorithm, a watermark is embedded into the host signal to produce a watermarked signal, while in the extraction algorithm, the watermark is extracted from the manipulated/modified signal. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. The watermark detection can only verify ownership, whereas watermark extraction can prove ownership. A secret key is used during the embedding and the extraction processes in order to prevent illegal access to the watermark.

Each of these following properties must be taken into consideration when applying a certain watermarking technique [33]:

- Imperceptibility: The perceptual similarity between the original and the watermarked versions of the digital content. The embedded watermark must not introduce distortion, which can cause quality degradation.

- Robustness: The ability to detect the watermark after common signal processing operations (such as cropping, compression or additive noise). A watermark must be robust enough to withstand all kinds of signal processing operations (at least below some distortion threshold). Depending on the robustness against attacks, digital watermarking can be categorized as robust, fragile and semi-fragile.
- Capacity: The number of bits a watermark encodes within a unit of time (or space in the case of still images).
- Security: The ability to resist intentional and/or malicious attacks. A watermarking algorithm must be secure in the sense that an attacker must not be able to detect the existence of embedded data or extract/remove it. Watermark information should only be accessible to the authorized parties.

Digital watermarking has been widely and successfully applied across a wide range of applications, such as copyright protection, transaction tracking, content authentication, broadcast monitoring, copy control, device control and legacy enhancement. The majority of the watermarking schemes proposed in recent years across the above mentioned range of applications focuses on producing image and video watermarked data, and very few focus on audio content.

2.6.4. Multimedia Fingerprinting

Unlike digital watermarking, which is incapable of tracing back the source of piracy, multimedia fingerprinting (also called transaction tracking) can trace back the identities of the pirates (colluders) upon finding an illegal copy. This traceability is achieved by embedding a unique user-specific information, known as a fingerprint, into different copies of the same content. A multimedia fingerprinting algorithm is a protocol between the content owner and the customer that involves three processes: fingerprint generation, embedding operation, and traceability of pirates from pirated/colluded copies.

A multimedia fingerprinting scheme is expected to address the following constraints [34]:

- Robustness: A fingerprint's robustness against signal processing operations is determined by the adopted watermark embedding method. Thus, a robust watermarking algorithm must be adopted so that the fingerprinting scheme can trace an illegal re-distributor after the digital content has been manipulated by common signal processing attacks.
- Collusion resistance: While digital fingerprinting may be effective at identifying a single adversary, multiple malicious buyers may collaborate to launch powerful collusion attacks against the fingerprinting system. By comparing their different versions, the colluders can attempt to identify the locations containing the fingerprint signal, remove the information from these locations and thereby create a copy that cannot be traced back to any of them. Thus, a fingerprinting scheme must be designed to withstand such collusion attacks.
- Quality tolerance: Fingerprinted content should have good visual quality and perceptual similarity to the original content.
- Embedding capacity: The capacity determines the length of fingerprint allocated to each user. The fingerprint is a binary string that can be long. Therefore, a digital fingerprint system should have a large enough embedding capacity to accommodate a full fingerprint.

From the customer's point of view, a traditional fingerprinting protocol between him/her and the content owner is unattractive, because during the embedding procedure, the content owner obtains the identity information of the customer. This enables a malicious content owner to embed the identity information of the customer into any content without the customer's consent, and subsequently, accuse him/her of illegal re-distribution. To eliminate this threat, anonymous fingerprinting protocols were developed based on cryptographic tools (such as homomorphic encryption, secure multiparty computation or zero-knowledge proof protocols). A complete and sound anonymous fingerprinting protocol [35] is expected to provide buyer frameproofness, traceability, collusion resistance,

anonymity, non-repudiation, dispute resolution and unlinkability. Recently, a growing number of anonymous and collusion-resistant fingerprinting techniques have been proposed for multimedia content.

2.7. Performance Requirements

To evaluate the performance of blockchain-based copyright protection applications, several metrics should be taken into consideration. These are defined as follows:

- Transaction throughput: Throughput can be defined as the number of transactions/second in each block, whereas transaction throughput can be defined as the rate at which valid transactions are committed by the blockchain in a defined time period.
- Scalability: The size and frequency of the blocks along with the number of transactions that the system can process to cope with the increased workload.
- Transaction latency: The amount of time required to add a block of transactions in the blockchain. This includes the propagation time and any settling time due to the consensus mechanism in place.
- Storage: On-chain storage of users' data (such as personal information, copyright information or keys) or off-chain mechanism (such as InterPlanetary File System (IPFS) or data lake) to store large amount of copyrighted data.
- Transaction fee: In Ethereum, an execution fee is used to compensate miners for the computational resources required to perform different smart contract functions (e.g., content registration or delivery). The gas price is measured in terms of ether. Hence, the total transaction fee is the gas consumed multiplied by the gas price. In Bitcoin, the transaction fee is the cost that a user incurs when he/she sends coins from one bitcoin wallet into another. This fee is based on the size (in bytes) of the transaction and the age of its inputs. The miners responsible for mining the block that includes the transaction are being paid with the transaction fee in BTC.
- Robustness of content protection schemes against different types of attacks: The copyright protection schemes (based on encryption, DRM, watermarking or fingerprinting) must be resistant against all possible threats, such as security, privacy, signal processing, tampering, communication and collusion attacks, among others. These threats are discussed in Section 2.6.
- Transparency of copyrighted multimedia content: In the copyright protection schemes based on watermarking/fingerprinting, the embedded watermark/fingerprint must be transparent and should not introduce distortion, which can cause quality degradation.
- Computational costs in generation of copyright content: These are on- or off-chain costs associated with the process of generating copyrighted content (encrypted with access control, watermarked or fingerprinted).
- Total response time: It includes the time taken by the content owner in registering the copyrighted content on the blockchain so as to make it available for the clients, and the time taken in delivering the content to the client upon final payment settlement.

3. State-of-The-Art of Blockchain-Based Content Protection Systems

Recently, both industry and academia have started to consider preservation of intellectual property rights using blockchain technologies. In the existing research, blockchain is considered to be a transparent and reliable ledger, which is used to solve the problems of copyright protection faced by the content owners and producers, e.g., the rights attribution certificate, data integrity, authenticity, piracy tracing and transparency, among others. In the remainder of this section, a brief overview of existing blockchain-based content protection systems is provided w.r.t. their main attributes and implementation details.

In Reference [36], the authors propose a blockchain-based framework that guarantees copyright compliance of multimedia objects by means of smart contracts. The proposed system uses an off-chain centralized storage solution, data lake, to store the transaction details of all the data added on the blockchain. The information stored on the data lake is

encrypted and digitally signed to ensure the privacy and authenticity of the information. The stored data can only be accessed by the authorized users after verification of their digital signatures and access rights by the consent of the majority nodes. Although the decentralized data management framework ensures user data privacy and control, it is a proof-of-concept that has not been implemented and evaluated in the real world.

Peng et al. [37] propose an Ethereum-based digital copyright management system that enables content owners and customers to deal directly without the need of a centralized authority. In the proposed system, digital watermarking, the ElGamal cryptosystem, a perceptual hash function, the smart contract, and IPFS are used. However, the scheme incurs high overhead (memory and CPU time) due to use of ElGamal encryption for encrypting the whole multimedia content.

Chi et al. [38] introduce a secure and reliable blockchain-based real time eBook market system that allows users to publish themselves and receive direct payments from readers without any trusted party involvement. The proposed trading platform uses blockchain for protecting copyright of paid content and securely managing direct payments. It provides eBook ownership verification, data protection and confidentiality, permission to read the purchased ebook, authentication of a legitimate purchaser, non-forgeability and verifiability of both eBook contents and direct payment transactions, and prevention of eBook piracy and illegal distribution. The published encrypted (using Elliptic Curve Cryptography) eBook contents along with the book key are stored in a book repository.

Kishigami et al. [39] proposed a high-definition video copyright management system based on a decentralized blockchain to assist the content creators' demand for an efficient way to manage DRM. In the proposed scheme, the right holders themselves can control the system, which is based on the PoW mechanism. In this technique, the headers of ultra-high resolution video content (i.e., 4K or 8K) are encrypted and decrypted to balance the cryptographic costs associated with encryption/decryption operations. However, the system does not have an incentive mechanism for mining computation power. In addition, it does not provide cross-platform rendering and access policy control of the media file.

Zhao and O'Mahoney [40] proposed BMCProtector, a prototype implementation based on an Ethereum blockchain and smart contract technologies, for effective protection of music copyright and rights of copyright owners. BMCProtector uses the AES algorithm to encrypt the audio file, vector quantization (a watermarking technique) to track ownership of the music file off-chain, and an off-chain access control mechanism (DRM) to control the copyright of music during its distribution and usage. The deployed smart contract is responsible for sharing the copyright parameters of the music owners and automatic royalty payments distribution to the wallet addresses of the different copyright owners. However, BMCProtector provides the proof-of-concept design for a copyright management of audio files only. Moreover, it cannot redprovide copyright redprotection of music files in other formats, e.g., an audio file recorded during playing and then uploaded illegally.

In Reference [41], the Blockchain as a Service (BaaS) model is proposed for building a DRM platform that provides high-level credit and security to the content provider, the service provider, and the customers. The DRM platform provides core content rights information storage in the blockchain for tamper-resistant protection to prevent copyright from being violated or misused. The content consumers can use blockchain-based digital currency for content consumption payment. A cryptocurrency digital rights coin based on multi-signatures is proposed as a payment mechanism on the platform. Dynamic key agreement and session data encryption are used to ensure secure communications and data transfer. This scheme uses many modulo operations that significantly limit the cost-effectiveness of the generating a temporary shared key. Moreover, the scheme is based on the alliance chain, and thus has a centralized authority that prevents direct transactions between the content owner and the customer.

Ma et al. [42] proposed a Ethereum-based scheme, DRMChain, which ensures the correct usage of digital content by the authenticated users, and provides flexible external storage of decentralized digital content using IPFS. DRMchain employs two isolated

blockchain application interfaces (BAI): BAI plain interface that stores the original content with its cipher summary, and BAI cipher interface, which stores the DRM-protected content service, such as content watermark, encryption, license and redviolation tracing, among others. DRMChain provides efficient and secure authentication, privacy protection, multi signature-based conditional traceability, and trusted and high-level credible content protection. However, DRMchain does not prevent the offline spread of the divulged copies. Moreover, the system lacks the diversified copyright management functions, such as copyright transaction. In addition, it lacks an effective punishment and reward mechanism.

Reference [43] proposed a blockchain-based DRM scheme for copyright protection of design works. The proposed system is categorized into two methods: copyright protection and trading. The copyright protection method performs copyright registration, information query and correlation verification, while the trading process encompasses design content protection and a proof-of-delivery method to guarantee fair trade. The enrolled buyer can purchase registered works from the content providers (sellers) through smart contracts. During the content delivery, the content is encrypted with the buyer's public key, and it is then delivered to the buyer through the application. Before receiving the content, the buyer needs to input his/her secret key to the application first, that performs decryption and makes it available to the buyer. However, the proposed scheme does not guarantee the security of the user's secret key submitted to the blockchain application for signing for the delivered content and the content decryption.

In Reference [44], a watermarking-based tamper-proof multimedia blockchain framework is proposed that provides security and integrity to the distributed image. The proposed blockchain model is based on a compressed sensing (CS)-based self-embedding watermarking algorithm in which the unique watermark information consists of a cryptographic hash and an image hash. The cryptographic hash comprises of transaction histories for retrieving the metadata of multimedia content from the multimedia blockchain, while the image hash is used for preserving retrievable original multimedia content.

The cryptographic hash can be used to retrieve the information of multimedia content (e.g., ownership and modification history) that is stored on the multimedia blockchain, and the image hash can be used to identify the tampered regions. The CS samples can be utilized for reconstructing the original image and locating the tampered regions. In the blockchain, a transaction is composed of the transaction information of the image containing transaction ID and the information of CS samples. Upon approval of the transaction by the validating nodes, the image is distributed and is then stored on a media database server. Though storing image verification information on the blockchain is a good strategy, the image is still stored in centralized manner or kept by the owner, which affects the availability of image management.

In Reference [45], an automated penalization of breach (APB) contract is proposed that consists of four main components: a claim-or-refund smart contract, a robust watermarking scheme, an oblivious-transfer scheme and a non-interactive zero knowledge (NIZK) proof for mutually distrusting parties. In this scheme, the sender and the receiver create a claim-or-refund transaction on Bitcoin, where an amount is deposited that can be spent at any time with a jointly signed transaction or spent after a period of time by a sender-only signed transaction. At the receiver's end, the received document consists of the receiver's secret key, which is embedded into it with a robust binary watermarking scheme. A two-party computation protocol is jointly performed by the parties to embed and ensure that the receiver's embedded key is retrievable for the sender in case of a content leakage.

Reference [46] proposes a blockchain-based data hiding method for digital video protection, which improves the integrity authentication of confidential data and videos. The proposed method consists of the following three parts: (1) on-chain data protection method that focuses on the integrity check and the security of the video by registering the signature of the video content on the blockchain; (2) off-chain data protection based on a data hiding algorithm that can achieve a good balance between visual distortion, embedding capacity and robustness; and (3) data protection management agreement based

on a smart contract that consists of registration, inquiry and transfer contract models. However, in the proposed scheme, the users need to request data extraction from data hiding servers so as to enable multimedia playback.

In [47], the blockchain technology is used to store the watermark securely and to provide timestamp authentication for multiple watermarks. The proposed system uses the perceptual hash function for calculating a hash value of an image, the blockchain technology for recording metadata related to the copyright information, the QR code for generating a watermark, the digital watermarking algorithm for embedding the copyright information, the cryptographic hash function for calculating the hash values of both original and watermarked images, and the IPFS network for saving, managing and distributing the watermarked image and its related copyright information. The proposed scheme, however, provides the proof-of-concept design for copyright management of digital images only. Moreover, it can be observed that the perceptual hash values of modified/edited images (such as rotated or cropped) considerably differ from those of the original and the original image hash values recorded on the blockchain.

In [48], Fei proposes BDRM, a blockchain-based DRM system with the property of a fine-grained usage control. BDRM utilizes a smart contract to achieve copyright management related operations, such as copyright registration and copyright transactions. Moreover, a novel authorization tree is designed in the blockchain. Each time a user conducts a rights transaction, a usable digital watermark is embedded, and digital content distribution is performed under the encryption domain. The authorization tree is then updated and the transaction is recorded on the blockchain. The content is encrypted with the secret key of the content owner and is stored in the distributed file system (IPFS). However, BDRM is only applicable to copyright registration of a single content owner.

Reference [49] presents Y-DWMS, a digital watermark management system, based on a public smart contract platform to prevent digital rights infringement. The proposed system adopts non-repudiation of smart contracts and non-tampering of blockchain to implement a DRM mechanism that prevents users from sharing encryption keys or their accounts. The smart contract is designed to perform verification of watermarks in the disclosed copy, authentication of the informer's report, traceability of infringement, an act of rewarding informers and punishing infringers, and recovery of losses suffered by the copyright holders. However, Y-DWMS is still in an early stage of development and suffers from some security issues, such as account security and privacy.

Wu et al. [50] proposed a blockchain and smart contract-based data trading system with data tracking and illegal behavior detecting functions. It enables two trading scenarios with privacy protection against any unauthorized party, including the trading platform. An effective fingerprint method is designed to detect the manipulated image, thus protecting data copyright. A data fingerprint generator is designed to generate a fingerprint by concatenating multiple feature vectors extracted from the data. Upon finding an illegally distributed copy, the data fingerprint generator extracts an identifiable vector, which is then compared with the fingerprints recorded in all existing contracts. The generated fingerprint is resistant to minor data modifications, such as cropping, adding noise and changing brightness. However, the system does not satisfy the privacy and security properties of an anonymous fingerprinting protocol in a decentralized environment.

In Reference [51], the authors propose a P2P content distribution system based on the blockchain technology. The proposed system uses collusion-resistant fingerprinting (to provide collusion resistance), homomorphic and symmetric encryption schemes (to ensure content protection and data confidentiality), a perceptual hash function (to provide content authentication), an Ethereum-based smart contract (to execute atomic payment and provide proof-of-delivery) and the IPFS network (to store multimedia content). While the privacy and security properties of an anonymous fingerprinting protocol in a distributed environment are addressed by the proposed system, it is a proof-of-concept that has not been implemented and evaluated in the real world.

In Reference [52], Li proposes a blockchain-based novel fingerprint-related chaotic image encryption scheme that provides authentication, traceability, and resistance against security attacks (e.g., chosen plaintext attack or tampering). In this scheme, the content distributors' fingerprints embedded in the encrypted images are encoded with Tardos's collusion-resistant codes to record multiple fingerprints with fixed length of data and to provide traceability. Before content distribution, the original image is embedded with the signature of the sender and the fingerprints of all system distributors using a reversible watermarking scheme and a chaotic map. This fingerprinted image is then encrypted using Fridrich's structure, which consists of substitution, permutation and diffusion. The fingerprint, the data hiding key, and the encryption key are recorded on the blockchain. At the receiver's end, upon decryption, the fingerprinted image is obtained, and it contains the signature of the sender and all the fingerprints of the superior distributors (merged fingerprint), which can be extracted individually, and then compared with the recorded information on the blockchain for verification. Though the system provides collusion resistance, data integrity, and copyright protection, it does not satisfy all the privacy and security properties of an anonymous fingerprinting protocol in a decentralized environment.

Reference [53] presents a robust blockchain-based copyright protection system (RobustCPS) for audio content. RobustCPS consists of the following three parts: (1) the audio content is segmented into blocks; (2) content-based fingerprint is generated by applying the singular value decomposition (SVD) on each block; and (3) similarity detection is performed through an execution of a smart contract, which determines whether a similar fingerprint exists on the Ethereum blockchain. If a similar fingerprint is found on the blockchain, RobustCPS sends a warning to the copyright shareholder of the corresponding fingerprint so as to prevent copyright violation. In case a similar fingerprint is not found, the generated content-based fingerprint will be recorded on the blockchain. The content-based fingerprint is resistant to common signal processing attacks and de-synchronization attacks. Though the system is able to protect copyright across multiple online platforms, it does not provide security against collusion attacks. Additionally, it is a proof-of-concept that has not been implemented on the blockchain.

3.1. Comparative Analysis

This section presents a comparison and a fine-grained analysis of blockchain-based multimedia content protection schemes presented in Section 3 w.r.t. the attributes defined in the taxonomy (Section 2). The analysis is presented in the form of Tables 1 and 2, Figure 2, and an in-depth discussion on the systems' properties. The tables also allow a side-by-side comparison of the systems presented in Section 3.

Table 1 presents the comparison of the schemes w.r.t. types of blockchain, transaction types, data automation, cryptocurrency, consensus protocols, and content protection techniques, while Table 2 compares the performance of these scheme w.r.t. the performance evaluation metrics mentioned in Section 2.7. In Tables 1 and 2, a cell contains "–" when the corresponding attribute is not addressed by the scheme.

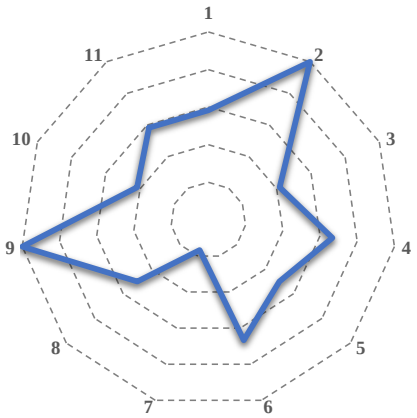

Figure 2. Analysis of security objectives of multimedia content protection techniques achieved by the analyzed systems.

Table 1. Comparison of blockchain-based copyright protection schemes with reference to the taxonomy.

References	Types of Content	Types of Blockchain	Types of Transaction	Data Automation	Crypto-currency	Consensus Protocols	Content Protection Techniques
Kishigami et al. (2015) [39]	HD video	Permissioned	On-chain	–	Bitcoin	PoW	DRM
Bhowmik & Feng (2017) [44]	Image	–	On-chain	Smart contract	Ethereum	–	Watermarking
Vishwa & Hussain (2018) [36]	–	Permissioned	Hybrid	dApp	Ethereum	–	Encryption
Zhao & Mahony (2018) [40]	Audio	Permissionless	Hybrid	dApp	Ethereum	PoW	Watermarking-based DRM
Ma et al. (2018) [41]	Video	Consortium	On-chain	dApp	Ethereum Token	PoW/PoS/ PBFT	DRM
Ma et al. (2018) [42]	Video	Permissioned	Hybrid	dApp	Ethereum	PoW/PoS/ PBFT	Watermarking-based DRM
Zhao et al. (2018) [46]	Video	Permissioned	Hybrid	Smart contract	Bitcoin	–	Watermarking
Meng et al. (2018) [47]	Image	Permissionless	Hybrid	–	–	–	Watermarking
Peng et al. (2019) [37]	Image	Permissioned	Hybrid	dApp	Ethereum	–	Encryption+ Watermarking
Lu et al. (2019) [43]	Image	Consortium	On-chain	dApp	–	–	DRM
Mangipudi et al. (2019) [45]	Document	–	Hybrid	Smart contract	Bitcoin	–	Watermarking
Fei (2019) [48]	–	Consortium	Hybrid	Smart contract	Ethereum	Proof-of-Authority	Watermarking-based DRM
Zhao et al. (2019) [49]	–	Permissioned	On-chain	dApp	Ethereum	PBFT	Watermarking-based DRM
Wu et al. (2019) [50]	Image	–	Hybrid	dApp	–	–	Fingerprinting
Qureshi & Megías (2019) [51]	Image, Audio, Video	Permissioned	Hybrid	Smart contract	Ethereum	–	Fingerprinting
Chi et al. (2020) [38]	Document	Self-developed	Hybrid	–	Customized coin	PoW	ECC-based encryption
Li (2020) [52]	Image	–	On-chain	–	–	–	Encryption+ Fingerprinting
Zhao (2020) [53]	Audio	Permissionless	On-chain	Smart contract	–	–	Content-based Fingerprinting

Table 2. Comparison of the blockchain-based multimedia content protection schemes with reference to the performance evaluation.

References	Performance Evaluation											
	Transaction throughput	Scalability	Transaction Latency	Storage	Transaction Fee	Robustness against Attacks				Transparency	Computational Costs	Total Response Time
						Signal Processing	Communication	Collusion	Security			
Kishigami et al. (2015) [39]	3–7 tps	–	10 min	On-chain	0.0001 BTC	–	–	–	Tampering resistance + Conditional access	–	–	–
Bhowmik & Feng (2017) [44]	15–20 tps	–	17 s	On-chain	0.00042 Ether	–	–	–	Tampering resistance	–	–	–
Vishwa & Hussain (2018) [36]	15–20 tps	–	17 s	On-chain+ Data lake	–	–	–	–	Data confidentiality	–	–	–
Zhao & Mahony (2018) [40]	123k tps per day	–	17 s	On-chain+ IPFS	–	Yes	Yes	–	Conditional access + Data confidentiality	–	–	–
Ma et al. (2018) [41]	– (HyperLedger fabric) 15–20 tps (Ethereum)	Yes (multi-sig)	– (HyperLedger fabric) 17 s (Ethereum)	On-chain	0.00042 Ether	–	Yes	–	Tampering resistance + Conditional access	–	1074 ms	987 ms
Ma et al. (2018) [42]	15–20 tps	Yes (multi-sig)	17 s	On-chain+ IPFS	0.00042 Ether	Yes	Yes	–	Tampering resistance + Conditional access + Traceability	38.96 dB	12,000 ms	45,000 ms
Zhao et al. (2018) [46]	3–7 tps	–	10 min	On-chain + Server	0.0001 BTC	Yes	Yes	–	Data integrity Tampering resistance	35.50 db	–	–
Meng et al. (2018) [47]	–	–	–	On-chain+ IPFS	–	–	–	–	Data integrity Tampering resistance	–	–	–
Peng et al. (2019) [37]	15–20 tps	–	17 s	On-chain + IPFS	0.00042 Ether	–	Yes	–	Data integrity Access control	–	–	–
Lu et al. (2019) [43]	–	–	–	On-chain + Personal equipment	–	–	Yes	–	Data confidentiality Proof-of-delivery Traceability	–	–	–
Mangipudi et al. (2019) [45]	3–7 tps	Yes (multi-sig)	10 min	On-chain + Server	–	Yes	Yes	Yes	Data integrity Fairness	–	–	–
Fei (2019) [48]	–	–	–	On-chain + IPFS	–	–	–	Yes	Conditional access Fine-grained usage control	–	–	97.077 ms
Zhao et al. (2019) [49]	–	Computationally intensive contract	–	On-chain	–	–	Yes	Yes	Traceability Rewards & Punishments Screen Record Prevention	–	–	–
Wu et al. (2019) [50]	–	–	–	On-chain + Server	–	Yes	Yes	–	Tamper proofness Traceability Frameproofness Non repudiation	–	–	–

Table 2. *Cont.*

References	Performance Evaluation											
	Transaction throughput	Scalability	Transaction Latency	Storage	Transaction Fee	Robustness against Attacks				Transparency	Computational Costs	Total Response Time
						Signal Processing	Communication	Collusion	Security			
Qureshi & Megías (2019) [51]	15–20 tps	–	17 s	On-chain+ IPFS	–	Yes	Yes	Yes	Proof-of-delivery Traceability Frameproofness Unlinkability	–	–	–
Chi et al. (2020) [38]	–	–	2.80 – 3.30 s	On-chain+ Server	–	–	Yes	–	Data confidentiality Non forgeability Verifiability	–	425.60ms (10 MB file)	11,386 ms (10 MB file)
Li (2020) [52]	–	–	–	On-chain	–	–	Yes	Yes	Data integrity Traceability	–	–	–
Zhao (2020) [52]	15–20 tps	–	17 s	On-chain	–	Yes	No	No	Authenticity	–	–	–

From Tables 1 and 2, we can make the following observations w.r.t. the attributes defined in the taxonomy:

- Most of the selected schemes [36,37,39,42,45,46,49,51] use a permissioned (private) blockchain, which implies a control layer on top of the blockchain that is governed by a trusted authority, who is responsible for permitting actions to be performed by the allowed system entities. Several other schemes [41,43,48] use consortium blockchain as a distributed ledger to retain control and privacy, while cutting down costs and increasing transaction speeds.
- The majority of the schemes [36–38,40,42,46–49,51,52] utilize hybrid transactions, which imply on-chain recording of data in a private or publicly accessible blockchain service, such as the content's metadata, copyright owners' or users' information, watermark or fingerprint of the user (in an encrypted form), DRM license and content obligation, among others, and off-chain mechanisms, such as generation and storage of copyrighted content, extraction of copyright information from the content or traceability protocol. The on-chain transactions are performed to achieve transparency, security, immutability and auditability, and are considered best for cryptocurrency transfers in a completely decentralized manner. The off-chain mechanisms allow the authorities to save on-chain costs as these do not have a transaction fee. In addition, these mechanisms are quite fast since these are not bound by the transactional speed limitations linked to on-chain transactions.
- In many schemes [36,37,40–43,49,50], multiple smart contracts are bundled together to create a blockchain-enabled dApp to automate the desired functionality between the copyright owner and the buyers. These contracts include a series of functions, such as data processing, value transfer, copyright protection, content distribution, and traceability. In other systems [44–46,48,51,53], a single smart contract is proposed to facilitate the purchase of the copyrighted content between the copyright owner and the clients (buyers).
- In the majority of the schemes [36,37,40,42,44,46,48,49,51,53], Ethereum, which is the second largest cryptocurrency platform by market capitalization behind Bitcoin, is used as a cryptocurrency for transactions. The Ethereum crypto token (Ether) transactions tend to be confirmed faster by the blockchain, and are much cheaper than most transactions on Bitcoin. Moreover, Ethereum not only allows Ether transfers between people, but can be used to create all types of other cryptocurrencies, such as in [41].
- Many schemes [38–42] use the most prominent consensus protocol, i.e., PoW, to confirm transactions and produce new blocks in the chain. PoW is the dominant choice in existing digital currencies due to its security features, which use cryptography that deters denial-of-service (DoS) and sybil attacks.
- The majority of the schemes guarantee content protection by using digital watermarking either as a standalone mechanism [44–47] or in combination with DRM [40,42,48,49] or encryption [37]. Only three schemes [50–53] used digital fingerprinting to provide copyright protection, while only two schemes, proposed in [39,41], used DRM techniques to ensure conditional access.
- From Table 2, we can make the following observations w.r.t. to the performance of the systems:
  - Since the majority of the schemes have utilized either Bitcoin or Ethereum for development or testing purposes, the average transaction throughput (3–7 tps for Bitcoin and 15–20 tps for Ethereum) and latency rates (10 min for Bitcoin and 17 s for Ethereum) have been considered. However, only a few schemes [37,39,41,42,44,46] consider the transaction fees per block per day.
  - Only a few schemes [41,42,45] address scalability by using the Schnorr's multi-signature technology, which also improves the privacy of the system and prevents spam attacks to a higher degree. In [49], a quite small number of miners

are pseudo-randomly selected to execute off-chain computationally intensive smart contracts.

– The majority of the schemes use IPFS or data servers for storing and distributing the copyrighted content to the buyers upon a successful purchase.
– All schemes are based on different content protection mechanisms and satisfy the basic security requirements described in Section 2.6. Figure 2 illustrates the 11 identified individual security properties (excluding the common security properties) of four multimedia content protection techniques (encryption, DRM, watermarking and fingerprinting), and the analyzed systems (18) that satisfy each of these objectives.
  It can be observed that the majority of the systems provide data integrity (12 systems) and protection against communication attacks (12 systems). In terms of tamperproofness, we can observe that many systems guarantee tampering resistance (8 systems). This is to be expected since this property is provided by the blockchain technology. It can be observed that fewer schemes address data confidentiality (7 systems), traceability (7 systems), authenticity (6 systems), and conditional access (6 systems). In terms of security against attacks, only a few schemes are robust against common signal processing (7 systems) and collusion/coalition (5 systems) attacks. Considering the quality tolerance objective, we observe that transparency of the copyrighted (watermarked/fingerprinted) content is evaluated by many fewer schemes (2 systems).
– Most of the schemes presented in Table 2 are proof-of-concepts and have not been evaluated in a real-world scenario. In only three schemes [38,41,42], the total response time or the computational overhead in generating the copyrighted content is evaluated.

4. Limitations, Open Challenges and Future Research Directions

This section presents the limitations and research challenges that must often be faced when designing blockchain-based multimedia copyright protection applications. In addition, possible research directions are pointed out to be considered in future works.

4.1. Limitations and Research Challenges of Content Protection Techniques

The limitations and research challenges of the multimedia content protection techniques presented in Section 2.6 are discussed below:

- Encrypted content is only as secure as the key used for encrypting it. Thus, cryptographic keys must be carefully managed (e.g., transmission, storage or updating) to ensure data remains protected, yet accessible when needed among multiple users of a system.
- Encryption techniques cannot prevent a user from unauthorized usage and illegal distribution of the content upon decryption of the received content.
- Most of the research work involving DRM is non-interoperable, which does not constitute an efficient option for clients. For this reason, consumers may seek alternative options to obtain the content, such as P2P file-sharing applications. However, to make DRM systems interoperable, the content providers or vendors of multimedia players would need to know the sensitive information related to the DRM protection scheme, thus increasing the risk of leakage. In such a case, a single leakage (or "hack") has the potential to compromise not only one of several distribution channels, but the distribution of all interoperably DRMed content.
- DRM systems may give rise to a number of legal issues if not used correctly, e.g., the use of monitoring tools, either intentionally or unintentionally, to report and collect data pertaining to their consumers' habits and preferences (such as the type of content they enjoy, when they enjoy it and even where, by accessing users location details, among others). This may result in serious privacy implications, such as using these data for purposes unrelated to the platform or selling it to third parties.

- At the embedder's end in a digital watermarking scheme, maintaining an appropriate balance between robustness, capacity and imperceptibility properties is a challenging task, since these properties contradict one another, i.e., if one is increased, the other decreases.
- Security and complexity features have been given less priority in the development of the watermarking schemes. The more complex the watermarking scheme is, the higher the costs associated with the embedding and detection processes. The costs associated with the watermark embedding and detection should be minimal in order to meet the real-time requirements.
- In digital fingerprinting schemes based on collusion-resistant codes, there exists a trade-off among the size of a user base N, the collusion resilience c_0, and the codeword length m. With an increase in N or c_0, the length of m increases and vice versa. This trade-off may make the traceable code impractical because many applications require a large user base and collusion resistance. However, these requirements will result in long traceable codes.
- Most of the research work involving anonymous fingerprinting protocols assume the presence of a trusted third party that is responsible for generating the fingerprint and tracing the copyright violators. This trust implies a belief by the user that the trusted entity will behave in an expected manner in order to ensure security and anonymity. In a few other schemes that have avoided the use of such a party, the computational and communicational overheads are quite high due to the use of at least one of the following highly demanding technologies: homomorphic encryption, bit-commitment or secure multi-party computation.
- All types of attacks—internal and external—should be taken into consideration to evaluate the security and robustness of novel or existing watermarking and fingerprinting schemes.

4.2. Limitations and Research Challenges of the Blockchain Technology

In this section, we discuss the limitations and research challenges of the blockchain technology:

- The blockchain suffers from a scalability problem due to the limited block size, e.g., Bitcoin can reach 7 transactions per second due to the Bitcoin protocol restricting block sizes to 1 MB. A possible solution to this problem is to increase the block size, but it creates a strain on the security due to the fact that an increase in the probability of orphaned blocks would distinctly affect the bandwidth and validation costs. The higher the block size limit, the larger the transaction load, blockchain congestion, and transaction delays. Consequently, a decrease in the transaction fee would result in less security. Thus, a trade-off between security, scalability and decentralization is a challenge in the development of a blockchain.
- Permissionless blockchains establish that the recorded data is accessible, and thus, enable its public access to all participants. However, this may compromise data privacy. Furthermore, in the case that a sensitive or confidential data is uploaded mistakenly to the public blockchain, there is no way to rectify the damage.
- The codes of smart contracts are susceptible to the inclusion of bugs due to human error or incomplete information. Moreover, the self-executing nature of smart contracts implies reduced flexibility to give effect to the actual intentions of the parties.
- A programming language to implement smart contracts is an ongoing research field. Currently, the most used object-oriented and high-level language to implement complex smart contracts in Ethereum is Solidity (Turing-complete language), which is still evolving and has a number of limitations, such as lack of general purpose libraries, type checking and multi-threading support, among others. Other popular programming languages (Python, C++, Java) are also used to code smart contracts. However, making programs readable (human readable code and human readable execution) in each form remains a challenge. In the case of Bitcoin, the scripting language to write a

simple code is not Turing complete and does not support all possible programming structures, specifically loops.

- Blockchain could suffer from 51% attacks, where some nodes may attain the majority in a network and abuse it, e.g., they may reverse transactions to perform double spending and prevent other miners from confirming blocks.
- User's privacy can be breached within the blockchain, e.g., user's real IP address can be traced, transaction history can be linked to reveal his/her true identity or linkability through his/her connected set of nodes.
- Blockchain lacks interoperability due to the lack of universal standards. Existing blockchain networks have their own parameters, such as consensus models, transaction schemes, cryptocurrency, and smart contract functionality. Moreover, the uncertainty and speculative nature of cryptocurrency still prevent its widespread adoption.

4.3. Future Research Directions

In this section, we describe possible research directions that are identified during the fine-grained analysis of the 18 blockchain-based multimedia content protection systems. Future research works should address these research potentials to tackle the challenges identified in Sections 4.2 and 4.3, and to enhance the usability of the blockchain technology in copyright protection applications.

4.3.1. Designing an Efficient Blockchain-Based Framework to Satisfy the System Requirements of Copyright Protection Applications

- Scalability: Off-chain mechanisms such as Lightning Network (LN) for Bitcoin [54] and Plasma for Ethereum [55], or on-chain schemes like SegWit for Bitcoin [56] and Sharding [57] for Ethereum, can solve the blockchain's scalability problem. However, for LN, the main challenges are security and transparency per-transaction basis and centralization (presence of hubs), while in Plasma, long waiting periods (7–14 days) for withdrawal of funds and security risks are the open challenges. Similarly, the main challenges of SegWit are complexity, increased storage space and network bandwidth, while communication and security are the main issues in Sharding. The studies on addressing security, complexity, decentralization, performance, and communication strategies are expected to achieve significant research interest in the future.
- Validation of a framework: Many of the blockchain-based copyright protection applications solely focus on the technology's benefits, while leaving aside the details of their implementation. Therefore, it is important to design a practical blockchain-based framework that should address both technical and implementation details, e.g., assessing the advantages and disadvantages of permissioned and permissionless systems before opting for one of these solutions, the selection of the appropriate consensus mechanism depending on the requirements (e.g., transaction throughput, latency, minimum transaction fee, centralization/decentralization and security, among others), and the evaluation of the performance by implementing the proof-of-concepts to calculate computational overheads and the total response time.
- Standardization: The recognized technological standards establish specifications and procedures that are beneficial in terms of ensuring efficiency, reliability, and enhanced security. Through our fine-grained analysis, it can be deduced that there is a need of a universal standard that the multimedia content providers, producers and involved companies could follow to share new blockchain-based copyright protection solutions as well as to integrate these with the existing systems. Similarly, this standard should allow automatic conversion between different cryptocurrencies to enhance user experience.
- Privacy-aware design: Future research studies need to investigate possible privacy-aware solutions that could protect the privacy of the entities (content owner, buyer, and so on) involved in the transactions of the blockchain-based content protection applications. The privacy and security requirements should be defined at the initial stage of these schemes due to the fact that the data (e.g., information related to

the content owner, the public keys of the participants, pseudonyms and copyright information, among others) is visible to everyone on the network.

- Unlinkability: The privacy leakage issue in the blockchain needs to be addressed in order to prevent linkability and possible identification. Future research works could study the feasibility of incorporating anonymity mechanisms, such as CoinShuffle [58] (shuffle addresses), Zerocash [59] (hides the payment's origin, destination, and transferred amount) or differential privacy into the applications to meet the anonymity requirements.
- Smart contract security: All possible security and privacy attacks (e.g., eavesdropping, DDoS attack or impersonation) on the smart contract should be analyzed through formal security analysis. Moreover, smart contract transactions must be designed to be technically reversible in order to prove their long-term effectiveness. Furthermore, in order to modify or reverse a smart contract, the triggering event for the modification and its termination/extension should be anticipated by the code. Therefore, the problem of addressing security and privacy attacks on a smart contract needs further investigation.
- Dispute resolution: The immutability property of blockchain can act as a double-edged sword, since it removes the possibility of modifying/updating the content or the copyright information stored on it. Moreover, in the existence of immutability, the problem of resolving disputes over the copyright can be an interesting research topic.

4.3.2. Designing Multimedia Content Protection Systems to Support the Blockchain Technology

- Design improvements: The fine-grained analysis of the evaluated state-of-the-art systems sheds light on the need to improve traditional content protection mechanisms (encryption, DRM, watermarking/fingerprinting) so as to enable amicable integration with the blockchain technology. For example, key management, concurrent key acquisition and protection of keys can be explored in future studies for implementing blockchain-based multimedia encryption systems. Similarly, transfer of access rights to the consumers without a trusted third party, smooth execution of the transaction between the copyright provider and the client, and privacy-aware fine-grained usage control in blockchain-based DRM systems need further investigations. Likewise, in blockchain-based watermarking and fingerprinting schemes, low embedding and computational complexity, high robustness against possible security attacks, and acceptable transparency are a few mentionable open research challenges that the future research should tackle to enable widespread use of the blockchain-based copyright protection applications.
- Trustless systems: Fully decentralized content protection mechanisms had existed before the advent of blockchain. A key advantage that blockchain offers in addition to decentralization is trustlesness. The analyzed blockchain-based content protection systems are based on hybrid trust models that include presence of trusted third party or trusted users. Thus, there is a need to exploit the blockchain technology to its full potential and build truly trustless copyright protection systems.
- Security issues: The integration of the blockchain technology with an access control mechanism for off-chain sources needs to be investigated to ensure that only authorized parties can access the sensitive information. In addition, there is a need to address how to make the off-chain sources fault tolerant and prevent them becoming bottlenecks or single points of failure.
- Promoting adoption of blockchain in copyright applications: Most studies have yet to address the costs and limitations in deploying the content protection mechanisms on blockchain at the commercial level, and it would take considerable time to evolve, and require further technological advancements and security guarantees to be accepted by all the involved parties (such as copyright owners, multimedia producers, buyers, and others).

5. Conclusions

This study is aimed to present an overview of blockchain-based content protection applications. In this work, we have defined a taxonomy to classify the state-of-the-art blockchain-based copyright protection schemes w.r.t. technical characteristics of the blockchain technology, the most commonly used content protection mechanisms, and performance criteria. The discussion begins with some background knowledge of the blockchain technology and four commonly used content protection techniques. Then, a detailed review of blockchain-based copyright protection applications is presented. Moreover, these schemes are compared w.r.t. the defined taxonomy. In addition, some significant research challenges of content protection schemes and the blockchain technology are discussed. Finally, several future research directions are outlined.

For researchers, blockchain has an excellent potential to be broadly applied in copyright protection and management applications. The blockchain-based copyright protection applications allow copyright owners and consumers to interact without costly intermediaries. These applications allow the content owners to upload copyrighted content, control licensing/copyright options, manage distribution, trace sources of piracy, and receive payments upon content usage. However, there are still many open issues that need to be further researched and analyzed in order to create workable copyright protection applications that can fully benefit from the use of the blockchain technology. The success of such applications is however dependent on different factors related to the blockchain technology, such as scalability, reliability or market adoption, that are difficult to foresee. Researchers must consider all these aspects while designing and implementing a new blockchain-based content protection scheme. We hope that this survey will be considered a primary reference that can facilitate the process of finding the most relevant information w.r.t. integration between the content protection mechanisms and the blockchain technology.

Author Contributions: A.Q. and D.M.J. commonly finished the manuscript. Both authors have read and approved the final manuscript. Original draft preparation: both authors; Writing—review & editing: both authors. All authors have read and agreed to the published version of the manuscript.

Funding: The authors acknowledge the financial support received from the Spanish Government through grant RTI2018-095094-B-C22 "CONSENT".

Acknowledgments: The authors thank Alice Keefer Riva for proofreading the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Valley, S. Netflix. 2007. Available online: http://www.netflix.com/ (accessed on 21 December 2020).
2. Cohen, B. BitTorrent. 2005. Available online: https://www.utorrent.com/ (accessed on 21 December 2020).
3. SANDVINE. 2019 Global Internet Phenomena Report. 2019. Available online: https://www.sandvine.com/global-internet-phenomena-report-2019 (accessed on 21 December 2020).
4. Amazon.com, Inc. Amazon Prime Video. 2006. Available online: https://www.primevideo.com/ (accessed on 21 December 2020).
5. Van Dijk, W. Streamit. 2003. Available online: https://www.streamit.eu/audio-distribution-platform/ (accessed on 21 December 2020).
6. Hamidouche, W.; Farajallah, M.; Sidaty, N.; Assad, S.E.; Deforges, O. Real-time selective video encryption based on the chaos system in scalable HEVC extension. *Signal Process. Image Commun.* **2017**, *58*, 73–86. [CrossRef]
7. Chen, Y.Y.; Jan, J.K.; Chi, Y.Y.; Tsai, M.L. A Feasible DRM Mechanism for BT-Like P2P System. In Proceedings of the International Symposium on Information Engineering and Electronic Commerce, Ternopil, Ukraine, 16–17 May 2009; pp. 323–327.
8. Pizzolante, R.; Castiglione, A.; Carpentieri, B.; Santis, A.D.; Castiglione, A. Reversible Copyright Protection for DNA Microarray Images. In Proceedings of the 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Krakow, Poland, 4–6 November 2015; pp. 707–712. [CrossRef]
9. Qiu, Y.; Gu, H.; Sun, J. Reversible watermarking algorithm of vector maps based on ECC. *Multimed. Tools Appl.* **2018**, *77*, 23651–23672. [CrossRef]
10. Qureshi, A.; Megías, D.; Rifà-Pous, H. Secure and Anonymous Multimedia Content Distribution in Peer-to-Peer Networks. In Proceedings of the 6th International Conference on Advances in Multimedia, Nice, France, 23–27 February 2014; pp. 91–96.
11. Megías, D. Improved Privacy-Preserving P2P Multimedia Distribution Based on Recombined Fingerprints. *IEEE Trans. Dependable Secur. Comput.* **2014**, *12*, 179–189. [CrossRef]

12. Qureshi, A.; Megías, D.; Rifà-Pous, H. PSUM: Peer-to-Peer Multimedia Content Distribution using Collusion-Resistant Fingerprinting. *J. Netw. Comput. Appl.* **2016**, *66*, 180–197. [CrossRef]
13. Megías, D.; Qureshi, A. Collusion-resistant and privacy-preserving P2P multimedia distribution based on recombined fingerprinting. *Expert Syst. Appl.* **2017**, *71*, 147–172. [CrossRef]
14. Kuribayashi, M.; Funabiki, N. Decentralized tracing protocol for fingerprinting system. *APSIPA Trans. Signal Inf. Process.* **2019**, *8*, 1–8. [CrossRef]
15. Nakamoto, S. Bitcoin: A Peer-To-Peer Electronic Cash System. 2008. Available online: http://www.bitcoin.org/bitcoin.pdf (accessed on 21 December 2020).
16. Michalko, M.; Kwan, W. DECENT, 2015. Available online: https://decent.ch/ (accessed on 21 December 2020).
17. Spotify USA, Inc. Mediachain, 2016. Available online: http://www.mediachain.io/ (accessed on 21 December 2020).
18. Shrestha, B.; Halgamuge, M.N.; Treiblmaier, H. Using Blockchain for Online Multimedia Management: Characteristics of Existing Platforms. In *Blockchain and Distributed Ledger Technology Use Cases: Applications and Lessons Learned*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 289–303. [CrossRef]
19. Bambrough, B. Ripple's XRP Has More Than Doubled In Price This Week, Far Outpacing Bitcoin and Ethereum—Here's Why. 2020. Available online: https://www.forbes.com/sites/billybambrough/2020/11/24/ripples-xrp-has-more-than-doubled-in-price-this-week-far-outpacing-bitcoin-and-ethereum-heres-why/?sh=71901a8512e5 (accessed on 21 December 2020).
20. Statista. Distribution of Leading Cryptocurrencies from 2015 to 2020, by Market Capitalization. 2020. Available online: https://www-statista-com.biblioteca-uoc.idm.oclc.org/statistics/730782/cryptocurrencies-market-capitalization/ (accessed on 21 December 2020).
21. Machine, P.W.T. What Are the Most Traded Cryptocurrencies? 2020. Available online: https://www.plus500.com/Trading/CryptoCurrencies/What-are-the-Most-Traded-Cryptocurrencies~2 (accessed on 21 December 2020).
22. Kawase, Y.; Kasahara, S. Transaction-Confirmation Time for Bitcoin: A Queueing Analytical Approach to Blockchain Mechanism. In *Queueing Theory and Network Applications*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 75–88.
23. Shahriar Hazari, S.; Mahmoud, Q. Improving Transaction Speed and Scalability of Blockchain Systems via Parallel Proof of Work. *Future Internet* **2020**, *12*, 125. [CrossRef]
24. Siriwardena, P. The Mystery Behind Block Time. 2017. Available online: https://medium.facilelogin.com/the-mystery-behind-block-time-63351e35603a (accessed on 21 December 2020).
25. Mitra, R. Bitcoin VS Ethereum: [The Ultimate Step-by-Step Comparison Guide]. 2020. Available online: https://blockgeeks.com/guides/bitcoin-vs-ethereum-ultimate-comparison-guide/ (accessed on 21 December 2020).
26. Terry, L. What Should We Expect From The Upcoming Release of Ethereum 2.0? 2020. Available online: https://hackernoon.com/what-should-we-expect-from-the-upcoming-release-of-ethereum-20-gc5m38hs (accessed on 21 December 2020).
27. Prut, A. Ripple (XRP)—Quick Introduction. 2019. Available online: https://medium.com/the-capital/ripple-xrp-quick-introduction-60b682375609 (accessed on 21 December 2020).
28. Won, D. Ethereum Proof of Stake Date: Date + What You Need to Know. 2020. Available online: https://www.exodus.io/blog/ethereum-proof-of-stake-date (accessed on 21 December 2020).
29. Won, D. Best Proof of Stake Coins 2020 for Easy Passive Income. 2020. Available online: https://www.exodus.io/blog/best-proof-of-stake-coins (accessed on 21 December 2020).
30. Staff, K. List Of DPOS Coins | DPOS Cryptocurrencies. 2018. Available online: https://kryptomoney.com/dpos-coins (accessed on 21 December 2020).
31. Fan, C.; Ghaemi, S.; Khazaei, H.; Musilek, P. Performance Evaluation of Blockchain Systems: A Systematic Survey. *IEEE Access* **2020**, *8*, 126927–126950. [CrossRef]
32. Arnold, M.; Schmucker, M.; Wolthusen, S.D. *Techniques and Applications of Digital Watermarking and Content Protection*, 2nd ed.; Artech House Publishers, Inc.: Norwood, MA, USA, 2003.
33. Cox, I.; Miller, M.; Bloom, J.; Fridrich, J.; Kalker, T. *Digital Watermarking and Steganography*, 2nd ed.; Morgan Kaufmann Publishers Inc.: San Francisco, CA, USA, 2007.
34. Katzenbeisser, S.; Petitcolas, F.A. *Information Hiding Techniques for Steganography and Digital Watermarking*, 1st ed.; Artech House, Inc.: Norwood, MA, USA, 2000.
35. Qureshi, A.; Megías, D.; Rifà-Pous, H. Framework for Preserving Security and Privacy in Peer-to-Peer Content Distribution Systems. *Expert Syst. Appl.* **2015**, *42*, 1391–1408. [CrossRef]
36. Vishwa, A.; Hussain, F.K. A Blockchain based approach for multimedia privacy protection and provenance. In Proceedings of the IEEE Symposium Series on Computational Intelligence, Bangalore, India, 18–21 November 2018; pp. 1941–1945, [CrossRef]
37. Peng, W.; Yi, L.; Fang, L.; XinHua, D.; Ping, C. Secure and Traceable Copyright Management System Based on Blockchain. In Proceedings of the IEEE 5th International Conference on Computer and Communications, Chengdu, China, 6–9 December 2019; pp. 1243–1247. [CrossRef]
38. Chi, J.; Lee, J.; Kim, N.; Choi, J.; Park, S. Secure and reliable blockchain-based eBook transaction system for self-published eBook trading. *PLoS ONE* **2020**, *15*, e0228418. [CrossRef] [PubMed]
39. Kishigami, J.; Fujimura, S.; Watanabe, H.; Nakadaira, A.; Akutsu, A. The Blockchain-Based Digital Content Distribution System. In Proceedings of the IEEE 5th International Conference on Big Data and Cloud Computing, Dalian, China, 26–28 August 2015; pp. 187–190. [CrossRef]

40. Zhao, S.; O'Mahony, D. BMCProtector: A Blockchain and Smart Contract Based Application for Music Copyright Protection. In Proceedings of the International Conference on Blockchain Technology and Application, Xi'an, China, 10–12 December 2018; pp. 1–5. [CrossRef]
41. Ma, Z.; Huang, W.; Gao, H. Secure DRM Scheme Based on Blockchain with High Credibility. *Chin. J. Electron.* **2018**, *27*, 1025–1036. [CrossRef]
42. Ma, Z.; Jiang, M.; Gao, H.; Wang, Z. Blockchain for digital rights management. *Future Gener. Comput. Syst.* **2018**, *89*, 746–764. [CrossRef]
43. Lu, Z.; Shi, Y.; Tao, R.; Zhang, Z. Blockchain for Digital Rights Management of Design Works. In Proceedings of the IEEE 10th International Conference on Software Engineering and Service Science, Beijing, China, 18–20 October 2019; pp. 596–603. [CrossRef]
44. Bhowmik, D.; Feng, T. The Multimedia Blockchain: A distributed and tamper-proof media transaction framework. In Proceedings of the 22nd International Conference on Digital Signal Processing (DSP), London, UK, 23–25 August 2017; pp. 1–5. [CrossRef]
45. Mangipudi, E.V.; Rao, K.; Clark, J.; Kate, A. Towards Automatically Penalizing Multimedia Breaches (Extended Abstract). In Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS PW), Stockholm, Sweden, 17–19 June 2019; pp. 340–346. [CrossRef]
46. Zhao, H.; Liu, Y.; Wang, Y.; Wang, X.; Li, J. A Blockchain-Based Data Hiding Method for Data Protection in Digital Video. In *Smart Blockchain*; Springer International Publishing: Berlin/Heidelberg, Germany, 2018; pp. 99–110. [CrossRef]
47. Meng, Z.; Morizumi, T.; Miyata, S.; Kinoshita, H. Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain. In Proceedings of the IEEE 42nd Annual Computer Software and Applications Conference, Tokyo, Japan, 23–27 July 2018; Volume 2, pp. 359–364. [CrossRef]
48. Fei, X. BDRM: A Blockchain-based Digital Rights Management Platform with Fine-grained Usage Control. *Int. J. Sci.* **2019**, *6*, 54–63.
49. Zhao, B.; Fang, L.; Zhang, H.; Ge, C.; Meng, W.; Liu, L.; Su, C. Y-DWMS—A digital watermark management system based on smart contracts. *Sensors* **2019**, *19*, 3091. [CrossRef] [PubMed]
50. Wu, Z.; Zheng, H.; Zhang, L.; Li, X. Privacy-friendly Blockchain Based Data Trading and Tracking. In Proceedings of the 5th International Conference on Big Data Computing and Communications, QingDao, China, 9–11 August 2019; pp. 240–244. [CrossRef]
51. Qureshi, A.; Megías, D. Blockchain-based P2P multimedia content distribution using collusion-resistant fingerprinting. In Proceedings of the 11th Asia-Pacific Signal and Information Processing Association (APSIPA) Annual Summit and Conference, Lanzhou, China, 18–21 November 2019; pp. 1606–1615. [CrossRef]
52. Li, R. Fingerprint-related chaotic image encryption scheme based on blockchain framework. *Multimed. Tools Appl.* **2020**, 1–21. [CrossRef]
53. Zhao, J.; Zong, T.; Xiang, Y.; Gao, L.; Beliakov, G. Robust Blockchain-Based Cross-Platform Audio Copyright Protection System Using Content-Based Fingerprint. In *Web Information Systems Engineering*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 201–212. [CrossRef]
54. Poon, J.; Dryja, T. The bitcoin lightning network: Scalable off-chain instant payments. *Draft Version 0.5* **2016**, *9*, 14.
55. Poon, J.; Lee, J.H. Plasma: Scalable autonomous smart contracts. *Work. Draft* **2017**, *9*, 1–14.
56. Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2794–2830. [CrossRef]
57. Kokoris-Kogias, E.; Jovanovic, P.; Gasser, L.; Gailly, N.; Syta, E.; Ford, B. OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–24 May 2018; pp. 583–598. [CrossRef]
58. Ruffing, T.; Moreno-Sanchez, P.; Kate, A. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. In *Computer Security—ESORICS 2014*; Kutylowski, M., Vaidya, J., Eds.; Springer International Publishing: Berlin/Heidelberg, Germany, 2014; pp. 345–364. [CrossRef]
59. Sasson, E.B.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M. Zerocash: Decentralized Anonymous Payments from Bitcoin. In Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA, USA, 18–21 May 2014; pp. 459–474. [CrossRef]