applied sciences

MDPI

Article

A Watermarking Protocol Based on Blockchain

Franco Frattolillo

Department of Engineering, University of Sannio, Corso Garibaldi 107, 82100 Benevento, Italy; frattolillo@unisannio.it

Received: 27 September 2020; Accepted: 30 October 2020; Published: 2 November 2020

Abstract: Digital watermarking can be used to implement mechanisms aimed at protecting the copyright of digital content distributed on the Internet. Such mechanisms support copyright identification and content tracking by enabling content providers to embed perceptually invisible watermarks into the distributed copies of content. They are employed in conjunction with watermarking protocols, which define the schemes of the web transactions by which buyers can securely purchase protected digital content distributed by content providers. In this regard, the "buyer friendly" and "mediated" watermarking protocols can ensure both a correct content protection and an easy participation of buyers in the transactions by which to purchase the distributed content. They represent a valid alternative to the classic "buyer and seller" watermarking protocols documented in the literature. However, their protection schemes could be further improved and simplified. This paper presents a new watermarking protocol able to combine the "buyer friendly" and "mediated" design approach with the blockchain technology. The result is a secure protocol that can support a limited and balanced participation of both buyers and content providers in the purchase transactions of protected digital content. Moreover, the protocol can avoid the direct involvement of trusted third parties in the purchase transactions. This can reduce the actual risk that buyers or sellers can violate the protocol by illicitly interacting with trusted third parties. In fact, such peculiarities make the proposed protocol suited for the current web context.

Keywords: watermarking protocols; digital copyright protection; blockchain

1. Introduction

Social networks and user-generated content platforms have turned common web users into actual producers of multimedia digital content. Such content can be easily duplicated without reducing their perceptual quality. They can be also maliciously modified and/or re-distributed, thus damaging the reputation of their legitimate owners, or revealing their private information, or causing economic loss. In addition, current mechanisms implemented to protect the copyright of multimedia digital content cannot adequately meet the protection requirements needed to solve piracy problems on the Internet.

One of the technologies proposed to protect the users' copyrights on their multimedia digital content is "digital watermarking" [1,2] used in conjunction with "watermarking protocols" [3–5].

Digital watermarking makes it possible to insert hidden information, such as, for example, a "fingerprint" [6–8], within any copy of content that has to be protected. Such information, called a "watermark", can be used to identify the user who possesses the content, and makes the copy of the content unique and personalized.

However, to combat the unauthorized sharing of multimedia digital content on the Internet, it is necessary to distribute the watermarked content according to specific interaction schemes defined by watermarking protocols. Thus, whenever a copy of watermarked content is found in a suspicious location, such as in file repositories shared by peer-to-peer applications, the embedded watermark can be used as a proof of ownership to establish who has initially obtained the copy and then illegally shared it on the Internet.

The most relevant watermarking protocols documented in the literature enable the implementation of mechanisms for copyright protection based on content tracking by fingerprinting [3–5,8,9]. They mainly involve two parties: the "buyer" and the "seller". The former wishes to get content from a web content provider, whereas the latter wishes to release it in a digitally protected form obtained by inserting a watermark. In particular, the early experiences also involve specific trusted third parties (TTPs), called "watermark certification authorities" (WCAs), whose main function is to guarantee the correct execution of the protocols [4,10–15]. However, the introduction of WCAs can reduce the security level of the protocols, since TTPs can give rise to potential collusive behaviors with buyers or sellers [2,16]. As a consequence, a number of watermarking protocols are based on "simplified" interaction schemes that do not exploit WCAs [17–21]. Such approaches appear to be more secure, but they turn out to be impracticable in the current web context, since they are characterized by interaction schemes that force buyers to perform complex security actions to complete content purchase transactions [22].

The watermarking protocols described in [22–24] attempt to overcome the drawbacks affecting previous solutions existing in the literature by proposing a new "buyer friendly" and "mediated" design approach. Such an approach reintroduces the TTP, but its role is carefully limited to a restricted part of the protocol, so as to enable a simplified participation of buyers in the content purchase transactions without reducing the security level of the protocol.

Although such experiences represent a good balance between security and easy participation of buyers in the protocol, further efforts are needed to simplify the interaction schemes of such watermarking protocols, so as to make them best suited to the current web context that does not like the presence of TTPs. In this regard, it is worth noting that blockchain technology has begun to be employed in the area of digital copyright protection [25–29]. In fact, blockchain belongs to the category of distributed ledger technologies that enable commercial or network transaction data to be recorded in cryptographic chained blocks by employing several security technologies, such as cryptographic hash, digital signature, and distributed consensus mechanism. When they are appended to a chain, blocks are timestamped and linked in a way that makes them resilient to modifications. Therefore, they are considered to be trusted for transactions among web entities, and can be verified in a decentralized way by exploiting multiple web nodes to form a consensus on whether a transaction is valid or not. In addition, blockchain supports the so-called "smart contracts", which represent a way to automatically execute the terms of an agreement reached between distinct web entities. More precisely, a smart contract encapsulates a number of preset rules in the form of code, and sets corresponding trigger events under specific conditions: when the conditions are met, the terms of the agreement are automatically executed without control from a central authority [26–31].

This paper presents a new watermarking protocol based on blockchain technology. The protocol is built on the experiences previously conducted with the protocols documented in [22–24], and follows the buyer friendly and mediated design approach. The main aim is to simplify the interaction scheme of the protocol by exploiting the blockchain technology, which makes it possible to better control the involvement of the TTP in the protocol. In fact, such an involvement has been further restricted in order to reduce the possibility of collusive actions from the TTP, making the developed protocol more secure and suited to the current web context.

The paper is organized as follows. Section 2 reports on related work. Section 3 introduces the main challenges faced in developing the proposed protocol. Section 4 reports the basics of the proposed protocol, whereas Section 5 describes the protocol in detail. Section 6 analyzes the proposed protocol. Section 7 focuses on the main implementation aspects of the watermarking protocol. The final remarks are in Section 8.

2. Related Work

Most of the watermarking protocols documented in the literature do not exploit blockchain technology, but they are based on the well-known "buyer and seller" protection schemes and their variants characterized by the absence of TTPs. They are widely described and discussed

in [5,22–24]. Some of them also inspire the so-called DRM (digital rights management) systems, which are complex web platforms that adopt specific technologies and interaction schemes to enable the copyright protection of digital content on the Internet [32,33]. More precisely, DRM systems do not actually define watermarking protocols, but they still implement mechanisms by which to prevent the unauthorized use of protected digital content without payment. To achieve such a goal, DRM systems use technologies based on encryption and key management [34]. However, such technologies cannot inhibit legitimate users from illegally sharing their purchased content on the Internet.

To overcome the drawbacks reported above, a number of DRM systems implement protection schemes based on "trusted computing". They prevent the sharing of illegal keys and protected content by enabling the access to such content on the basis of the web users' biometric features [35,36]. In fact, such systems appear to be very promising, but they lack flexibility, since they need particular hardware, such as "trusted platform modules" (TPMs) or fingerprint recognizers, and cannot defend against specific attacks, such as screen recording or I/O monitoring.

The blockchain technology, in conjunction with digital watermarking, is employed in a number of DRM systems to provide some copyright management services, such as to keep track of possible and required content modifications, copyright transfers or other transaction trails related to the managed digital content [37–39]. In particular, digital watermarking is mainly used to provide content tracking by fingerprinting. However, such DRM systems do not implement protection schemes able to address the peculiar problems that affect watermarking protocols, such as the "customer's right problem" or the "unbinding problem" [4,11,22]. As a consequence, once content is downloaded and tampered, there is no legal way to prove the ownership of the content and to trace who should be responsible for copyright infringement. In fact, such considerations motivate the design of innovative watermarking protocols able to exploit the blockchain technology to overcome the limitations described above.

3. Main Challenges

One of the main challenges in designing watermarking protocols consists of accurately defining the role played by TTPs in the purchase transactions, since TTPs could collude with the other parties involved in the protocols [17,20,40] so as to impair them. In this regard, the best solution would be to totally eliminate TTPs from protocols. However, such a solution is not always possible, since protocols often need TTPs to validate specific data, or some phases of the protocol, or, for example, the plug-ins that have to be downloaded and installed in the buyers' web browsers to complete the purchase transactions [22,23]. Furthermore, when TTPs play a limited role in the protocols, buyers end up being forced to perform complex security actions to complete the purchase transactions, and this makes the protocols impractical for the web context [17–21,40–44].

The watermarking protocols presented in [22–24] do not completely eliminate the TTP, but they carefully exploit it without assigning it a central role in order to simplify the buyer participation in the protocols. In particular, the TTP participates only in the initial phase of the protocols and restricts its role to the generation of a number of tokens needed to unambiguously bind the chosen content to the buyer, the seller and the ongoing purchase transaction.

Although the role of the TTP is rather restricted in the protocols described in [22–24], it has to be further limited if the main goal is to develop an innovative watermarking protocol suited for the current web context. In this regard, blockchain technology represents a challenge to achieve such a goal. In fact, it can be exploited in the proposed protocol with the aim of securely tracking the purchase transactions in a public ledger that can be updated by automatically executing smart contracts without resorting to the control of a TTP [26–29]. Thus, the TTP involved in the proposed protocol can act as a simple and trusted web distributor of secure tokens needed to complete the purchase transactions of protected digital content. In fact, it is not a WCA, even though it has to behave as a TTP in the sense of a common certification authority (CA) [45–47].

The adoption of blockchain technology to strongly restrict the role of TTP makes it necessary to accurately design and code the smart contract that controls the execution of the proposed watermarking

protocol and validates each purchase transaction. In fact, this represents a relevant practical challenge well documented in the literature, since the code that implements the contract, once it has been released, can no longer be modified or updated. Therefore, if the code of the contract is incorrect or gives rise to a problem during use, it ends up impairing the entire protocol [48].

4. Basics of the Protocol

The proposed watermarking protocol is based on a limited set of well-known security facilities: public key infrastructure (PKI), homomorphic cryptosystem [49], encrypted and signed tokens [4,5,22], and blind and readable watermarking scheme [1]. Furthermore, it exploits the public key and secure communication support implemented by the SSL/TLS protocol for all the messages exchanged among the web entities involved in the protocol [46].

In more detail, if a piece of content and a watermark can be described according to a block-wise representation in the form of $X = \{x_1, x_2, \dots x_l\}$ and $W = \{w_1, w_2, \dots w_l\}$ respectively, the watermark insertion adopted by the proposed protocol, denoted as $\oplus$, results in the following expression:

$$X \oplus W = \{x_1 \oplus w_1, x_2 \oplus w_2, \dots x_l \oplus w_l\} = \bar{X}$$

since such an insertion is assumed to be based on linear watermarks [1,10,17,50]. Furthermore, if $X = \{x_1, x_2 \dots x_l\}$ is a digital content, its encryption by means of the function $\mathbb{E}$ results in the following expression:

$$\mathbb{E}_{pk}(X) = \mathbb{E}_{pk}(x_1, x_2 \dots x_l) = (\mathbb{E}_{pk}(x_1), \mathbb{E}_{pk}(x_2) \dots \mathbb{E}_{pk}(x_l))$$

since $\mathbb{E}$ is assumed to be a block-wise function [10,50].

Finally, the encryption function $\mathbb{E}$ is assumed to be "homomorphic" with respect to the watermark insertion. This means that any linear watermark can be embedded directly into the encrypted domain according to the following expression [10,50]:

$$\mathbb{E}_{pk}(X \oplus W) = \mathbb{E}_{pk}(X) \oplus \mathbb{E}_{pk}(W) = \mathbb{E}_{pk}(\bar{X})$$

In fact, a cryptosystem $\mathbb{E}$ is homomorphic with respect to an operation $\odot$ if

$$\mathbb{E}_{pk}(m_1 \odot m_2) = \mathbb{E}_{pk}(m_1) \odot \mathbb{E}_{pk}(m_2)$$

for any two plain messages m_1 and m_2 [49]. As a consequence, homomorphic encryption makes it possible to perform operations by directly working on encrypted data.

5. Watermarking Protocol

The proposed watermarking protocol is an enhancement of the buyer friendly and mediated protocols presented in [22–24]. It has been designed and developed according to what is reported in Section 3. Therefore, it exploits the blockchain technology to avoid the participation of a TTP in the core of the protection phase so as to simplify and secure the basic interaction scheme characterizing the protocols described in [22–24]. The result is an innovative watermarking protocol in which the blockchain is employed to lock in a public ledger the main tokens characterizing purchase transactions. In fact, such tokens are collected and controlled by executing a specific smart contract: if they turn out to be correct, the ongoing purchase transaction is automatically validated and completed without the direct intervention of a TTP.

Even though the proposed protocol can run without a centralized control, it still needs a TTP acting as a trusted web distributor of security tokens, such as one-time public and private key pairs and encrypted "nonces" [51], needed to complete the purchase transactions of protected digital content according to the original buyer friendly and mediated approach [22]. Moreover, the proposed protocol

needs a further TTP, called "judge". It does not participate in the phase of the protocol that applies the protection to the digital content distributed on the Internet. It only participates in the subsequent "identification and arbitration phase" needed to determine the identity of an illegal distributor of a copy of a protected digital content [22–24]. In fact, the TTP and the judge could even coincide, but conventional certification authorities do not usually implement the service performed by the judge [17,22].

More precisely, the proposed watermarking protocol is characterized by a protection scheme in which: (1) the seller or content provider $\mathcal{CP}$ releases content in an encrypted and watermarked form; (2) the buyer $\mathcal{B}$ can obtain the protected content by simply decrypting it; (3) the purchase transaction of a protected digital content occurring between the buyer and the content provider is validated by automatically executing a smart contract within a blockchain $\mathcal{BC}$, which takes charge of controlling all the tokens generated by the transaction; (4) buyer and content provider take part in transactions that employ security tokens guaranteed by a "registration authority" $\mathcal{RA}$ [22–24]; (5) a judge $\mathcal{J}$ guarantees the dispute resolution protocol and determines if a buyer is guilty of having released pirated copies [22–24].

The protocol consists of two subprotocols: the *protection protocol* and the *identification and arbitration protocol*. The meanings of the symbols used to describe the protocol are reported in Table 1.

Table 1. Meanings of the symbols used to describe the proposed protocol.

Symbol	Meaning
$\mathcal{B}$	buyer
$\mathcal{CP}$	content provider or seller
$\mathcal{RA}$	registration authority
$\mathcal{BC}$	blockchain
$\mathcal{J}$	judge
X	digital content purchased by $\mathcal{B}$
X_d	information used by $\mathcal{CP}$ to unambiguously identify X
T_X	timestamp referred to the transaction by which $\mathcal{B}$ buys X
B_{id}	information used to identify $\mathcal{B}$
B_{ad}	destination address provides by $\mathcal{B}$
N	nonce used to mark the watermarking transaction
W	watermark
$W_{Ent.}$	part of the watermark W generated by the entity Ent.
$\bar{X}$	watermarked X
$pk_{Ent.}$	public key of the entity Ent.
$sk_{Ent.}$	secret key of the entity Ent.
$pk^X_{Ent.}$	one time public key generated by the entity Ent. in the transaction to watermark X
$sk^X_{Ent.}$	one time secret key generated by the entity Ent. in the transaction to watermark X
$E_{key}(\dots)$	token encrypted using the key key and a public key cryptosystem
$\mathbb{S}_{key}(\dots)$	token digitally signed using the secret key key and the SHA-1 secure hash algorithm
$\mathbb{E}_{key}(\dots)$	token encrypted using the key key and a cryptosystem that is privacy homomorphic with respect to the watermark insertion
$\mathbb{D}_{key}(\dots)$	decryption function corresponding to the encryption function $\mathbb{E}_{key}(\dots)$

5.1. Protection Protocol

The protocol, whose scheme is reported in Table 2, starts when $\mathcal{B}$ visits the $\mathcal{CP}$'s web site, chooses the content X, and sends the purchase request to $\mathcal{CP}$ in the message m_1.

Table 2. Protection protocol.

$\mathcal{B}$	:	visits the $\mathcal{CP}$'s web site and chooses the content X
$\mathcal{B} \rightarrow \mathcal{CP}$	:	$m_1 = \{\text{request for } X\}$
$\mathcal{CP} \rightarrow \mathcal{RA}$	:	$m_2 = \{\text{request for security tokens}\}$
$\mathcal{RA} \rightarrow \mathcal{CP}$	:	$m_3 = \{pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N), \mathbb{S}_{RA}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))\}$
$\mathcal{CP} \rightarrow \mathcal{B}$	:	$m_4 = \{X_d, T_X, pk^X_{\mathcal{RA}}, \mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N)), \mathbb{S}_{\mathcal{CP}}(X_d, T_X, pk^X_{\mathcal{RA}}, \mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N)))\}$
$\mathcal{CP}$	:	generates $W_{\mathcal{CP}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(W_{\mathcal{CP}}), \mathbb{E}_{pk^X_{\mathcal{RA}}}(X)$
$\mathcal{CP}$	:	generates $\mathbb{E}_{pk^X_{\mathcal{RA}}}(W) = \mathbb{E}_{pk^X_{\mathcal{RA}}}(W_{\mathcal{CP}}) \| \mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$
$\mathcal{CP}$	:	generates $\overline{\mathbb{E}_{pk^X_{\mathcal{RA}}}(X)} = \mathbb{E}_{pk^X_{\mathcal{RA}}}(X) \oplus \mathbb{E}_{pk^X_{\mathcal{RA}}}(W)$
$\mathcal{CP} \rightarrow \mathcal{B}$	:	$m_5 = \{\overline{\mathbb{E}_{pk^X_{\mathcal{RA}}}(X)}\}$
$\mathcal{CP} \rightarrow \mathcal{BC}$	:	$m_6 = \{X_d, T_X, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N), \mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N)), \mathbb{S}_{\mathcal{CP}}(X_d, T_X, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N), \mathbb{S}_{RA}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N)))\}$
$\mathcal{B} \rightarrow \mathcal{BC}$	:	$m_7 = \{X_d, T_X, pk^X_{\mathcal{RA}}, \mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N)), B_{id}, B_{ad}\}$
$\mathcal{BC}$	:	activates the smart contract
$\mathcal{BC}$	:	compares the tokens and verifies the signatures included in m_6 and m_7
$\mathcal{BC}$	:	generates a node in the blockchain by which to publish X_d, T_X, $pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N), \mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N)), \mathbb{S}_{\mathcal{CP}}(X_d, T_X, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N), \mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N)))$
$\mathcal{BC}$	:	implements the payment phase
$\mathcal{BC} \rightarrow \mathcal{RA}$	:	$m_8 = \{B_{ad}, pk^X_{\mathcal{RA}}\}$
$\mathcal{BC}$	:	$E_{pk_{\mathcal{RA}}}(B_{id}, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$
$\mathcal{BC} \rightarrow \mathcal{CP}$	:	$m_9 = \{E_{pk_{\mathcal{RA}}}(B_{id}, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))\}$
$\mathcal{CP}$	:	saves a new entry in its databases composed of X_d, T_X, $pk^X_{\mathcal{RA}}$, $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$, $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$, and $E_{pk_{\mathcal{RA}}}(B_{id}, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$ whose search key is $W_{\mathcal{CP}}$
$\mathcal{RA} \rightarrow \mathcal{B}$	:	$m_{10} = \{sk^X_{\mathcal{RA}}\}$
$\mathcal{B}$	:	$\bar{X} = \mathbb{D}_{sk^X_{\mathcal{RA}}}(\overline{\mathbb{E}_{pk^X_{\mathcal{RA}}}(X)})$

Upon receiving the purchase request, $\mathcal{CP}$ contacts $\mathcal{RA}$, by sending the message m_2, in order to obtain the security tokens to complete the purchase transaction. In fact, $\mathcal{RA}$ is a TTP that publishes a list of pairs, each including a public key $pk^X_{\mathcal{RA}}$ and an encrypted token $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$. In particular, $pk^X_{\mathcal{RA}}$ corresponds to the secret key $sk^X_{\mathcal{RA}}$. They represent a one-time key pair that can be used only in the current transaction [52]. N is a "nonce" represented by a binary string. It is encrypted by employing the public key $pk^X_{\mathcal{RA}}$ and a cryptosystem that is "privacy homomorphic" [49] with respect to the subsequent watermark insertion. In fact, the resulting token $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$ will be then used to generate the watermark to be inserted into the content X.

The chosen pair $(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$ is returned by $\mathcal{RA}$ in the message m_3 together with the signature $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$.

Upon receiving m_3, $\mathcal{CP}$ can confirm the purchase request made by $\mathcal{B}$. In fact, $\mathcal{CP}$ generates two tokens, X_d and T_X. The former is a string that identifies the requested content X. It includes the name of the content and further data that can unambiguously describe it. The latter is

a timestamp that is referred to the ongoing transaction. Then, $\mathcal{CP}$ generates the signature $\mathbb{S}_{\mathcal{CP}}(X_d, T_X, pk^X_{\mathcal{RA}}, \mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N)))$ and sends the message m_4 to $\mathcal{B}$, which includes X_d, T_X, $pk^X_{\mathcal{RA}}$, $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$, and $\mathbb{S}_{\mathcal{CP}}(X_d, T_X, pk^X_{\mathcal{RA}}, \mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N)))$.

After having confirmed the purchase request, $\mathcal{CP}$ can apply the protection to X. Therefore, $\mathcal{CP}$ generates its part of watermark, denoted by $W_{\mathcal{CP}}$, which is a fingerprinting binary code obtained as an anti-collusion code [6,7,16] concatenated with an error correcting code used to address the problems of bit errors that can arise during the watermark verification process. Then, $\mathcal{CP}$ encrypts $W_{\mathcal{CP}}$ and X using the public key $pk^X_{\mathcal{RA}}$ and the same homomorphic cryptosystem used by $\mathcal{RA}$ to encrypt N, thus generating $\mathbb{E}_{pk^X_{\mathcal{RA}}}(W_{\mathcal{CP}})$ and $\mathbb{E}_{pk^X_{\mathcal{RA}}}(X)$.

Then, according to the basics reported in Section 4, $\mathcal{CP}$ concatenates $\mathbb{E}_{pk^X_{\mathcal{RA}}}(W_{\mathcal{CP}})$ and $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$ to generate the encrypted watermark $\mathbb{E}_{pk^X_{\mathcal{RA}}}(W)$ according the following expression:

$$\mathbb{E}_{pk^X_{\mathcal{RA}}}(W) = \mathbb{E}_{pk^X_{\mathcal{RA}}}(W_{\mathcal{CP}}) \| \mathbb{E}_{pk^X_{\mathcal{RA}}}(N) = \mathbb{E}_{pk^X_{\mathcal{RA}}}(W_{\mathcal{CP}} \| N) \quad (1)$$

Moreover, $\mathcal{CP}$ can embed the encrypted watermark $\mathbb{E}_{pk^X_{\mathcal{RA}}}(W)$ directly into the encrypted content $\mathbb{E}_{pk^X_{\mathcal{RA}}}(X)$ according to the following expression:

$$\overline{\mathbb{E}_{pk^X_{\mathcal{RA}}}(X)} = \mathbb{E}_{pk^X_{\mathcal{RA}}}(\bar{X}) = \mathbb{E}_{pk^X_{\mathcal{RA}}}(X \oplus W) = \mathbb{E}_{pk^X_{\mathcal{RA}}}(X) \oplus \mathbb{E}_{pk^X_{\mathcal{RA}}}(W) \quad (2)$$

since encryption is homomorphic with respect to watermark insertion [10,49,50]. The encrypted and watermarked content $\overline{\mathbb{E}_{pk^X_{\mathcal{RA}}}(X)}$ can be thus sent by $\mathcal{CP}$ to $\mathcal{B}$ in the message m_5.

At this point, $\mathcal{CP}$ and $\mathcal{B}$ can activate the smart contract in the blockchain $\mathcal{BC}$ by sending the messages m_6 and m_7, respectively.

In particular, the message m_6 is sent by $\mathcal{CP}$ to $\mathcal{BC}$, and contains X_d, T_X, $pk^X_{\mathcal{RA}}$, $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$, $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$, and the signature $\mathbb{S}_{\mathcal{CP}}(X_d, T_X, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N), \mathbb{S}_{RA}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N)))$.

The message m_7 is sent by $\mathcal{B}$ to $\mathcal{BC}$, and includes X_d, T_X, $pk^X_{\mathcal{RA}}$, and $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$. In addition, $\mathcal{B}$ also sends B_{id} and B_{ad} to $\mathcal{BC}$ in the message m_7: the former is a token that unambiguously identifies $\mathcal{B}$, whereas the latter represents his/her destination address. In particular,

- B_{id} is generated depending on the specific "negotiation mechanism" chosen by $\mathcal{B}$ among those ones supported by $\mathcal{BC}$ [4,5]. In this regard, in the proposed protocol $\mathcal{BC}$ is assumed to provide multiple negotiation mechanisms, which enable $\mathcal{B}$ to be identified, for example, using an anonymous digital certificate or a personal digital certificate or a credit card [4,5]. In fact, the last two mechanisms enable $\mathcal{B}$ to be directly identified. However, they are assumed to be implemented according to the concept of "multilateral security" applied to web transactions [53,54].
- B_{ad} is the $\mathcal{B}$'s shipping address that will enable him/her to receive the secret key $sk^X_{\mathcal{RA}}$ corresponding to the public key $pk^X_{\mathcal{RA}}$.

When the messages m_6 and m_7 are received by $\mathcal{BC}$, the code associated to a specific smart contract is automatically executed. The code of the contract mainly compares the tokens, verifies the signatures contained in the two received messages, and checks whether the tokens $pk^X_{\mathcal{RA}}$ and $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$, generated by $\mathcal{RA}$, have been already used in a previous purchase transaction or not. In fact, this means to check whether $pk^X_{\mathcal{RA}}$ and $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$ have been already published in a node of the blockchain or not. If all data turn out to be correct, match, and the tokens generated by $\mathcal{RA}$ have not been used in previous transactions, the code enables the generation of a new node in $\mathcal{BC}$, which makes some of the tokens identifying the ongoing transactions, such as X_d, T_X, $pk^X_{\mathcal{RA}}$, $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$, $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$, and $\mathbb{S}_{\mathcal{CP}}(X_d, T_X, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N), \mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N)))$, public. Moreover, the execution of the smart contract within $\mathcal{BC}$ takes also charge of implementing the payment phase. It ends by sending two messages, m_8 and m_9, to $\mathcal{RA}$ and $\mathcal{CP}$, respectively.

The message m_8 includes B_{ad} and $pk^X_{\mathcal{RA}}$, and enables $\mathcal{RA}$ to send the secret key $sk^X_{\mathcal{RA}}$ to $\mathcal{B}$ in the message m_{10}. $\mathcal{B}$ can thus decrypt $\overline{\mathbb{E}_{pk^X_{\mathcal{RA}}}(X)}$ and obtain the final protected content according to the following equalities:

$$\overline{\mathbb{E}_{pk^X_{\mathcal{RA}}}(X)} = \mathbb{E}_{pk^X_{\mathcal{RA}}}(\bar{X}), \qquad \bar{X} = \mathbb{D}_{sk^X_{\mathcal{RA}}}(\overline{\mathbb{E}_{pk^X_{\mathcal{RA}}}(X)}) \tag{3}$$

The message m_9 contains the security token $E_{pk_{\mathcal{RA}}}(B_{id}, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$. It is stored by $\mathcal{CP}$ in a new entry in its databases, whose search key is the watermark $W_{\mathcal{CP}}$. The entry also includes the following tokens: X_d, T_X, $pk^X_{\mathcal{RA}}$, $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$, and $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$. Such tokens are needed to prove that $\mathcal{B}$ is the legitimate owner of the protected content $\bar{X}$ sold by $\mathcal{CP}$ through a transaction registered by a node published in the blockchain $\mathcal{BC}$.

5.2. Identification and Arbitration Protocol

The protocol is run by $\mathcal{CP}$ to identify the responsible distributor of a pirated copy of $\bar{X}$, who was the legitimate copyright owner of $\bar{X}$, with undeniable evidence [4,5].

As shown in Table 3, the first step of the protocol consists of extracting the watermark W' from the pirated copy of $\bar{X}$, denoted as X'. After the extraction of $W' = W'_{\mathcal{CP}} \| N'$, $\mathcal{CP}$ can access its databases and use $W'_{\mathcal{CP}}$ to search them for a match. If a possible match is found [11], $\mathcal{CP}$ can retrieve the tokens saved during the purchase transaction of $\bar{X}$, which are X_d, T_X, $pk^X_{\mathcal{RA}}$, $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$, $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$, and $E_{pk_{\mathcal{RA}}}(B_{id}, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$. Then, $\mathcal{CP}$ can send the tokens, together with W', to $\mathcal{J}$ in the message m_1.

Table 3. Identification and arbitration protocol.

$\mathcal{CP}$	:	finds X' in the market and extracts $W' = W'_{\mathcal{CP}} \| N'$
$\mathcal{CP}$	:	searches its databases for a possible match on $W'_{\mathcal{CP}}$
$\mathcal{CP} \rightarrow \mathcal{J}$	:	$m_1 = \{W', X_d, T_X, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N), \mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N)), E_{pk_{\mathcal{RA}}}(B_{id}, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))\}$
$\mathcal{J}$	:	searches $\mathcal{BC}$ for a node including $pk^X_{\mathcal{RA}}$ and $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$
$\mathcal{J}$	:	retrieves the tokens published in the node of $\mathcal{BC}$, which are X_d, T_X, $pk^X_{\mathcal{RA}}$, $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$, $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$, $\mathbb{S}_{\mathcal{CP}}(X_d, T_X, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N), \mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N)))$
$\mathcal{J}$	:	verifies if the tokens retrieved from $\mathcal{BC}$ match those ones received from $\mathcal{CP}$
$\mathcal{J} \rightarrow \mathcal{RA}$	:	$m_2 = \{pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N), E_{pk_{\mathcal{RA}}}(B_{id}, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))\}$
$\mathcal{RA}$	:	decrypts $E_{pk_{\mathcal{RA}}}(B_{id}, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$
$\mathcal{RA} \rightarrow \mathcal{J}$	:	$m_3 = \{B_{id}, N\}$
$\mathcal{J}$	:	compares N' with N and adjudicates

$\mathcal{J}$ receives m_1 and verifies the signature $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$. Then, it searches the blockchain $\mathcal{BC}$ for a node using $pk^X_{\mathcal{RA}}$ and $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$ as search keys. If a node is found, $\mathcal{J}$ can access the tokens published by the node, which are reported in Table 2, and compare them with those one received by $\mathcal{CP}$. If all the tokens match, $\mathcal{J}$ can send $pk^X_{\mathcal{RA}}$, $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$, and $E_{pk_{\mathcal{RA}}}(B_{id}, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$ to $\mathcal{RA}$ in the message m_2.

$\mathcal{RA}$ decrypts $E_{pk_{\mathcal{RA}}}(B_{id}, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$ and verifies the received tokens. If all data are correct, $\mathcal{RA}$ decrypts $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$ and sends B_{id} and N to $\mathcal{J}$ in the message m_3.

Upon receiving m_3, $\mathcal{J}$ compares N' and N. If $N' = N$, the identity of the buyer B_{id} is revealed, and $\mathcal{J}$ can adjudicate him/her to be a traitor, thus closing the case. Otherwise, the protocol ends without exposing any identity.

6. Protocol Analysis

In the conducted analysis, the ideal behavior of the proposed watermarking protocol can be modeled as follows: a content provider $\mathcal{CP}$ sells the digital content X to a buyer $\mathcal{B}$; $\mathcal{B}$ obtains the protected digital content $\bar{X}$ from $\mathcal{CP}$; a blockchain $\mathcal{BC}$ is a ledger that publishes the tokens that identify each purchase transaction of digital content distributed on the web; a registration authority $\mathcal{RA}$ generates some specific data that have to be used by $\mathcal{CP}$ to protect X; a judge $\mathcal{J}$ decides whether $\mathcal{B}$ is guilty of releasing pirated copies.

The ideal behavior is modeled under the following assumptions:

- $\mathcal{J}$ and $\mathcal{RA}$ cannot be corrupted.
- $\mathcal{CP}$ and $\mathcal{B}$ can be only corrupted "statically", i.e., the set of the corrupt entities is decided at the beginning of the protocol execution and cannot be modified throughout the execution [55].
- $\mathcal{BC}$ is assumed to be characterized by an "honest-but-curious" behavior [55]. As a consequence, $\mathcal{BC}$ is obliged to follow the rules of the protocol, even though it can try its best to get information from the executed actions. This means that $\mathcal{BC}$ cannot collude with $\mathcal{B}$ or $\mathcal{CP}$, and this is a reasonable assumption, since $\mathcal{BC}$ is assumed to limit its action to automatically executing a smart contract whose code is approved and accepted in advance and cannot be modified during the life of the blockchain [26–30].
- Uncorrupt buyers and content providers are assumed to never release pirated copies.

The assumptions reported above ensure that, if $\mathcal{CP}$ and $\mathcal{B}$ are uncorrupt, $\mathcal{B}$ receives a unique and personalised protected content $\bar{X}$ during the purchase transaction. Therefore, if a pirated copy of $\bar{X}$ is found on the web, it can be always traced back to $\mathcal{B}$ and to the purchase transaction. On the contrary, if $\mathcal{CP}$ is corrupt, $\mathcal{B}$ receives a protected content $\bar{X}$ that cannot be correctly tied to any buyer. As a consequence, nobody can be adjudicated to be a traitor, and the corruption of $\mathcal{CP}$ ends up being useless and pernicious just for $\mathcal{CP}$. Likewise, if $\mathcal{B}$ is corrupt, $\mathcal{CP}$ can abort the purchase transaction without releasing any content.

6.1. Assumptions

The proposed protocol assumes that the watermark insertion technique employed to protect a digital content is robust against the most common and nonmalevolent manipulations, and survives the most relevant and intentional attacks, such as signal processing based attacks, geometric attacks, or collusion attacks [6,7,56–60]. In fact, such an assumption is realistic since there is a vast literature on watermark insertion techniques that documents the existence of increasingly robust and secure watermarking algorithms [1,20,21,61–65] together with a promising and increasing research activity in the development of new techniques and algorithms.

The protocol also assumes that the digital encryption applied within the context of a PKI is characterized by indistinguishability under chosen plaintext attack (IND-CPA). As a consequence, an adversary cannot get any knowledge about a plaintext message m from the corresponding ciphertext c.

Finally, the protocol assumes that the adopted cryptosystem is privacy homomorphic with respect to watermark insertion according to what is specified in Section 4 [49].

6.2. Analysis

The security analysis follows the scheme adopted in [22–24], and examines the behavior of the proposed watermarking protocol when corrupt entities make their strongest attacks [46,47,66,67]. Therefore, the analysis is restricted to two main attacks, which represent the two worst cases for security: (1) when $\mathcal{CP}$ is corrupt and tries to cheat $\mathcal{B}$; (2) when $\mathcal{B}$ is corrupt and attempts to cheat $\mathcal{CP}$. In both cases, according to what is reported in Sections 3 and 5, the analysis is conducted by assuming the presence of an honest-but-curious $\mathcal{BC}$ [55,68] and of a TTP $\mathcal{RA}$.

6.2.1. $\mathcal{CP}$ is Corrupt

Consider the execution of the proposed protocol when a corrupt party $\mathcal{CP}^c$ and an honest $\mathcal{B}$ are involved.

$\mathcal{B}$ chooses the content X and communicates the wish to buy it to $\mathcal{CP}^c$. $\mathcal{CP}^c$ interacts with $\mathcal{RA}$ and obtains $pk^X_{\mathcal{RA}}$ and $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$. During this preliminary phase, no corrupting actions may occur.

Lemma 1 (Basic Lemma)**.** *Under the basic assumptions reported in Section 6.1, if $\mathcal{CP}^c$ tries to embed a corrupt watermark W^c into X in order to accuse an innocent buyer of illegal content distribution, such a corruption is disclosed by running the identification and arbitration protocol.*

Proof. Since the watermark W is composed of N and $W_{\mathcal{CP}}$ (see Expression (1)) , $\mathcal{CP}^c$ can embed a corrupt watermark into X only if it can corrupt the part N of W. Therefore, consider the case in which $\mathcal{CP}^c$ wants to embed a corrupt N^c into the content X purchased by $\mathcal{B}$. To achieve such a goal, $\mathcal{CP}^c$ has to be able to:

1. embedd the watermark $W^c = W_{\mathcal{CP}}||N^c$ into the content X directly in the encrypted domain, according to the Expressions (1) and (2);
2. obtain the generation of a node in the blockchain $\mathcal{BC}$, which occurs only if $\mathcal{BC}$ can certify consistency between the security tokens sent in the messages m_6 and m_7 by $\mathcal{CP}^c$ and $\mathcal{B}$ respectively (see Table 2).

The former condition is needed because $\mathcal{B}$ obtains the final and protected version of the purchased content $\bar{X}$ by decrypting the content $\overline{\mathbb{E}_{pk^X_{\mathcal{RA}}}(X)}$ with the secret key received by $\mathcal{RA}$ in the message m_{10} (see Table 2), according to the Expression (3). This also means that, if $\mathcal{CP}^c$ wants to use a corrupt key $pk^{X^c}_{\mathcal{RA}}$ to encrypt the nonce N^c, it has also to control the corresponding secret key sent by $\mathcal{RA}$ to $\mathcal{B}$ in the message m_{10}, which has to necessarily become $sk^{X^c}_{\mathcal{RA}}$.

The latter condition implies that $\mathcal{CP}^c$ can obtain or generate a valid and verifiable signature $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N^c))$ on the corrupt token $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N^c)$. Furthermore, if $\mathcal{CP}^c$ decides to also employ a corrupt key $pk^{X^c}_{\mathcal{RA}}$ to encrypt N^c, then the corrupt signature to obtain or generate becomes $\mathbb{S}_{\mathcal{RA}}(pk^{X^c}_{\mathcal{RA}}, \mathbb{E}_{pk^{X^c}_{\mathcal{RA}}}(N^c))$.

In this regard, it is worth noting that, under the assumptions reported in Section 6.1, $\mathcal{CP}^c$ cannot generate a valid signature $\mathbb{S}_{\mathcal{RA}}(\ldots)$ on corrupt tokens. This means that $\mathcal{CP}^c$ cannot choose an arbitrary nonce N^c or key pair $(pk^{X^c}_{\mathcal{RA}}, sk^{X^c}_{\mathcal{RA}})$ to conduct a purchase transaction, but it could only attempt to reuse tokens generated by $\mathcal{RA}$ in previous purchase transactions. However, the following considerations have to be taken into account:

1. When a key pair $(pk^X_{\mathcal{RA}}, sk^X_{\mathcal{RA}})$ and an encrypted nonce $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$ are employed in a valid purchase transaction, they are included and published in a node of $\mathcal{BC}$, and can no longer be re-used, as reported in Section 5.1.
2. Once the public key $pk^X_{\mathcal{RA}}$ has been chosen and sent to $\mathcal{B}$ in the message m_4, it can no longer be corrupted by $\mathcal{CP}^c$, since it has to correspond to the secret key $sk^X_{\mathcal{RA}}$ released by $\mathcal{RA}$ in the message m_{10}. Therefore, if $\mathcal{CP}^c$ encrypts the watermark to be inserted into X using the corrupt key $pk^{X^c}_{\mathcal{RA}}$, it ends up generating the content $\overline{\mathbb{E}_{pk^{X^c}_{\mathcal{RA}}}(X)})$. However, $\mathcal{B}$ will employ the secret key $sk^X_{\mathcal{RA}}$ to decrypt the received content $\overline{\mathbb{E}_{pk^{X^c}_{\mathcal{RA}}}(X)})$ according to the Expression (3), thus generating a protected content containing an unknown and unpredictable watermark. In fact, this just damages $\mathcal{CP}^c$, which ends up releasing a piece of content including a watermark that cannot be linked to any buyer.
3. If $\mathcal{CP}^c$ receives the key $pk^X_{\mathcal{RA}}$ from $\mathcal{RA}$ in the message m_3 and forwards the corrupt key $pk^{X^c}_{\mathcal{RA}}$ to $\mathcal{B}$ in the message m_4, the key exchange is always disclosed by $\mathcal{BC}$ unless $\mathcal{CP}^c$ generates a valid signature $\mathbb{S}_{\mathcal{RA}}(pk^{X^c}_{\mathcal{RA}}, \ldots)$, which, as reported above, is impossible. This is because $\mathcal{BC}$ compares

the tokens received in the messages m_6 and m_7, and generates a new node in the blockchain only if the tokens turn out to be consistent.

4. For the same reason reported at the previous point, if $\mathcal{CP}^c$ receives the encrypted nonce $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$ from $\mathcal{RA}$ in the message m_3 and forwards the corrupt nonce $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N^c)$ to $\mathcal{BC}$ in the message m_6, the nonce exchange is always disclosed by $\mathcal{BC}$ unless $\mathcal{CP}^c$ generates a valid signature $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N^c))$, which, as reported above, is impossible.

Therefore, suppose that $\mathcal{B}$ starts a purchase transaction and that $\mathcal{CP}^c$ receives the message m_3 containing $pk^X_{\mathcal{RA}}$, $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$, and $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$ (see Table 2). Suppose also that $\mathcal{CP}^c$ inserts a corrupt watermark $W^c = W_{\mathcal{CP}}||N^c$ into the content X, thus creating the protected copy $\bar{X}^c$, and suppose that $\bar{X}^c$ is found in the market. $\mathcal{CP}^c$ starts the identification and arbitration protocol by extracting the watermark W^c from $\bar{X}^c$ and by sending to $\mathcal{J}$ all the tokens existing in its databases and associated to W^c, according to what is reported in Section 5.2.

Suppose that $\mathcal{CP}^c$ wants to cheat $\mathcal{J}$ in order to accuse a buyer of illegal content distribution. To achieve such a goal, $\mathcal{CP}^c$ has to send, among the others, the following corrupt tokens $pk^X_{\mathcal{RA}}$, $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N^c)$, $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N^c))$, $E_{pk_{\mathcal{RA}}}(B_{id}, pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N^c))$ to $\mathcal{J}$ (see Table 3), which have to be all coherent with N^c. However, according to what is reported above and under the assumptions of Section 6.1, the following constraints have to be considered:

- $\mathcal{CP}^c$ cannot generate a valid signature $\mathbb{S}_{\mathcal{RA}}(\ldots)$ on arbitrary security tokens;
- the security tokens that can be employed in a valid purchase transaction have to be among those ones generated by $\mathcal{RA}$;
- $\mathcal{CP}^c$ cannot reuse security tokens employed in previous purchase transactions and already published in the nodes of $\mathcal{BC}$;

As a consequence, if $\mathcal{CP}^c$ attempts to accuse an innocent buyer of illegal content distribution by generating corrupt tokens coherent with the corrupt watermark $W^c = W_{\mathcal{CP}}||N^c$ embedded into the content X^c found in the market, the attempt ends up being revealed by the execution of the identification and arbitration protocol, and this prevents the protocol from adjudicating anybody to be a traitor. □

Lemma 2. *Under the assumptions reported in Section 6.1, if $\mathcal{CP}^c$ tries to alter the tokens that are managed during the protection phase in order to accuse an innocent buyer of illegal content distribution, such a corruption is disclosed by the identification and arbitration protocol.*

Proof. The basic lemma proves that the security tokens, such as $pk^X_{\mathcal{RA}}$, $\mathbb{E}_{pk^X_{\mathcal{RA}}}(N)$, and $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$, generated by $\mathcal{RA}$ and associated to a valid purchase transaction registered by a node of $\mathcal{BC}$, cannot be coherently corrupted by $\mathcal{CP}^c$ to insert an arbitrary watermark into the content purchased by $\mathcal{B}$ without such a corruption being disclosed by running the identification and arbitration protocol. More precisely, the impossibility of corrupting the security tokens has been proved be the basic lemma independently of the corruption of the watermark to be inserted into X. In fact, the proof is mainly based on the general incapacity of $\mathcal{CP}^c$ to alter or regenerate or reuse the tokens generated by $\mathcal{RA}$ for a given purchase transaction [22–24]. Therefore, the attempts of $\mathcal{CP}^c$ to alter the tokens generated by $\mathcal{RA}$ can be always disclosed by running the identification and arbitration protocol, since such tokens either have been generated and employed during previous, valid purchase transactions by $\mathcal{RA}$ or are directly generated by $\mathcal{CP}^c$ and so they cannot be registered in a node of $\mathcal{BC}$. □

The lemmas reported above prove that $\mathcal{CP}^c$ cannot frame an innocent buyer, because every attempt to corrupt the security tokens that have to be registered in the nodes of $\mathcal{BC}$ is disclosed by the identification and arbitration protocol, and this prevents the watermarking protocol from adjudicating anybody to be a traitor.

6.2.2. $\mathcal{B}$ is Corrupt

Consider the execution of the proposed protocol when the involved parties are a corrupt buyer $\mathcal{B}^c$ and an honest $\mathcal{CP}$.

Suppose that $\mathcal{B}^c$ contacts $\mathcal{CP}$ in order to buy the content X. $\mathcal{B}^c$ receives the confirmation message m_4 from $\mathcal{CP}$, which contains the following tokens: X_d, T_X, $pk^X_{\mathcal{RA}}$, $\mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N))$, $\mathbb{S}_{\mathcal{CP}}(X_d, T_X, pk^X_{\mathcal{RA}}, \mathbb{S}_{\mathcal{RA}}(pk^X_{\mathcal{RA}}, \mathbb{E}_{pk^X_{\mathcal{RA}}}(N)))$ (see Table 2).

Lemma 3 (Basic Lemma)**.** *Under the basic assumptions reported in Section 6.1, if $\mathcal{B}^c$ tries to complete the purchase transaction by employing a corrupt content identifier X^c_d in order to impair the piracy tracing mechanism implemented by $\mathcal{CP}$, such a corruption is disclosed and the purchase transaction is aborted.*

Proof. Suppose that $\mathcal{B}^c$ wants to use a corrupt identifier X^c_d to conduct the purchase transaction. Under the assumptions reported in Section 6.1, such a goal can be achieved only if $\mathcal{B}^c$ can obtain the generation of a node in the blockchain $\mathcal{BC}$ which contains X^c_d. This occurs only when $\mathcal{BC}$ can certify consistency between the security tokens sent by $\mathcal{CP}$ and $\mathcal{B}^c$ in the messages m_6 and m_7 respectively (see Table 2). This also means that, if $\mathcal{B}^c$ wishes to include the corrupt identifier X^c_d in the message m_7, the buyer must ensure that the corresponding signature $\mathbb{S}_{\mathcal{CP}}(X_d, \ldots)$ is included in the message m_6. However, it is worth noting that, under the assumptions reported in Section 6.1:

1. $\mathcal{B}^c$ cannot autonomously generate a valid and verifiable signature $\mathbb{S}_{\mathcal{CP}}(\ldots)$ on corrupt tokens.
2. X_d is generated by $\mathcal{CP}$ to unambiguously identify the content X requested by the buyer. Therefore, $\mathcal{CP}$ uniquely accepts the content identifiers that it has generated during the initial phase of the protection protocol. No other identifiers can be accepted.
3. X_d is always sent by $\mathcal{CP}$ to $\mathcal{BC}$ in the message m_6, together with the corresponding signature $\mathbb{S}_{\mathcal{CP}}(\ldots)$. Therefore, if the content identifiers included in the messages m_6 and m_7 do not coincide or do not match with the signature $\mathbb{S}_{\mathcal{CP}}(\ldots)$, $\mathcal{BC}$ does not complete the purchase transaction.

As a consequence, $\mathcal{B}^c$ cannot employ arbitrary content identifiers in the protection protocol, but he/she can, at the most, exploit pairs $(X_d, \mathbb{S}_{\mathcal{CP}}(X_d, \ldots))$ generated by $\mathcal{CP}$ in other previous, incomplete purchase transactions. In fact, such pairs must not be already included in nodes of the blockchain.

Suppose that $\mathcal{B}^c$ can get two distinct content identifiers Y_d and Z_d, together with the corresponding signatures $\mathbb{S}_{\mathcal{CP}}(Y_d, \ldots)$ and $\mathbb{S}_{\mathcal{CP}}(Z_d, \ldots)$, from $\mathcal{CP}$. The two identifiers refer to the content Y and Z distributed by $\mathcal{CP}$.

Suppose that $\mathcal{B}^c$ starts a transaction with $\mathcal{CP}$ to purchase X. $\mathcal{B}^c$ receives X_d and $\mathbb{S}_{\mathcal{CP}}(X_d, \ldots)$ from $\mathcal{CP}$ in the message m_4. This also means that $\mathcal{BC}$ will receive X_d and $\mathbb{S}_{\mathcal{CP}}(X_d, \ldots)$ from $\mathcal{CP}$ in the subsequent message m_6, and this will prevent $\mathcal{B}^c$ from using any other pair of content identifier and signature in the message m_7. In fact, if this happens, $\mathcal{BC}$ can always disclose the mismatch between the tokens included in the message m_6 and those ones included in the message m_7, according to what is reported above. As a consequence, every attempt of $\mathcal{B}^c$ to conduct a purchase transaction by employing corrupt content identifiers causes the purchase transaction to abort. □

Lemma 4. *Under the assumptions reported in Section 6.1, if $\mathcal{B}^c$ tries to corrupt the tokens needed to run the protection protocol in order to impair the piracy tracing mechanism implemented by the watermarking protocol, such a corruption is directly disclosed by $\mathcal{BC}$ and the purchase transaction is aborted.*

Proof. This lemma is an extension of the basic lemma, which has proved that $\mathcal{B}^c$ cannot deceive $\mathcal{BC}$ by proposing arbitrary content identifiers or identifiers that are incoherent with the corresponding signatures. The trivial reason is that $\mathcal{BC}$ accepts the tokens sent by $\mathcal{B}^c$ in the message m_7 only if they are consistent with those ones sent by $\mathcal{CP}$ in the message m_6. Therefore, every attempt of $\mathcal{B}^c$ to corrupt

the tokens generated by $\mathcal{CP}$ during a purchase transaction causes the protection protocol to abort without releasing any protected content. □

The lemmas reported above prove that the corrupt entity $\mathcal{B}^c$ cannot cheat $\mathcal{CP}$ in order to release a piece of content not tied to any buyer, because every attempt to corrupt the tokens managed by the protection protocol is always disclosed by $\mathcal{BC}$, which can thus abort the purchase transaction.

7. Implementation

The first prototype implementation of the proposed protocol is mainly based on the experiences documented in [22,24]. It consists of two parts.

The former comprises the same set of C++ separate programs that implement $\mathcal{B}$, $\mathcal{CP}$, $\mathcal{RA}$, and $\mathcal{J}$ in [22,24]. The programs run on Linux operating system and communicate via TCP implemented by standard socket library. They implement the encryption/decryption and watermark insertion algorithms by exploiting the NTL library and the GNU Multi Precision Arithmetic library. In particular, watermark insertion is based on the "Quantization Index Modulation" algorithm [61] extended to the homomorphic cryptosystem proposed by Paillier [69] according to the main ideas reported in [9,63]. It follows the indications reported in [42], which successfully address a number of problems that tend to make watermark insertion directly into the encrypted domain inefficient. In this regard, in order to reduce both the number of encryptions and the operations performed on encrypted values, watermark insertion is carried out in the encrypted domain by exploiting the specific technique of the "composite signal representation" described in [42], also called "efficient composite embedding" [50].

The latter implements the blockchain $\mathcal{BC}$ according to the Figure 1. In particular, the blockchain can be classified as "public", with a fully decentralized architecture, and based on the classic "proof of work" consensus algorithm [27]. Furthermore, the nodes of the blockchain are implemented in Ethereum [70], whereas the smart contract employed by the proposed protocol is written in Solidity [71].

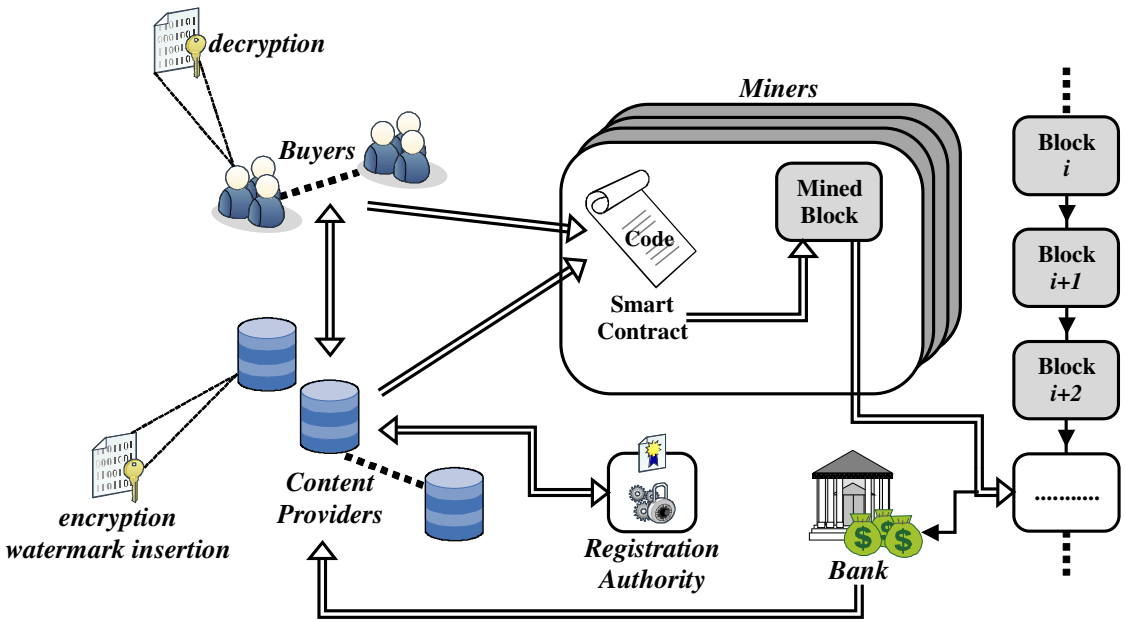

Figure 1. The blockchain within the proposed watermarking protocol.

The performance of the proposed prototype implementation mainly depends on both the basic operations characterizing watermarking protocols and the overhead induced by the blockchain management. In fact, the former are the classic encryption/decryption and watermark insertion operations. Their performances are omitted because, as reported above, they are well documented

by the results published in [22,24]. On the contrary, the latter depends on a number of factors, such as, for example, the Ethereum node implementation, the adopted consensus algorithm, and the number of nodes averagely involved in the blockchain, which are essentially independent of proposed watermarking protocol [28,29]. In this regard, it is worth noting that an Ethereum, public and decentralized blockchain, based on the "proof of work" consensus algorithm, is characterized by undoubted advantages, such as decentralization, lack of trusted third parties, and immutability [27–29], but it is also affected by low performance and efficiency levels caused by the time needed for propagating, processing, and validating the purchase transactions [72]. In fact, the higher the number of nodes participating in the blockchain is, the more limiting power consumption and block generation rate become. However, the main goals of the proposed protocols are to achieve high levels of robustness and security without reducing simplicity of the protection scheme. After all, it is not wrong to think that the proposed watermarking protocol will be able to take advantage of the next generation blockchains, which promise to achieve higher performance and efficiency levels, particularly in terms of power consumption, due the development of new consensus algorithms. Nevertheless, such performance aspects have not been investigated because they are out of the scope of this paper.

8. Conclusions

The main goal in developing the proposed protocol has been to simplify the basic interaction scheme that characterizes the previous protocols that adopt a "buyer friendly" and "mediated" design approach without compromising on their relevant achievements [22–24]. The solution has been found in the smart contracts to be exploited within the blockchain technology. In fact, a smart contract has been employed to simply validate the security tokens generated during purchase transactions and then published as immutable purchase information in the blocks maintained by the blockchain [27–29,31]. It has made it possible to avoid the direct involvement of a TTP in the protection scheme without forcing buyers to carry out complex actions to participate in the purchase transactions. In this way, the interaction scheme turns out to be simple while, at the same time, it strongly reduces the possibility of collusion actions among the parties participating in the protocol, thus making the protocol secure and suited to the current web context.

The proposed protocol also confirms the security achievements characterizing the previous similar protocols [22–24]: (1) $\mathcal{CP}$ keeps control on the content that it distributes on the Internet, since it never releases them in unprotected forms; (2) $\mathcal{B}$ is the only entity that gets access to the final watermarked content $\bar{X}$, and this makes it possible to trace back pirated copies of $\bar{X}$ to $\mathcal{B}$; (3) X is never released in a partially protected form, thus solving the specific problem arisen in the watermarking protocol proposed in [11] and discussed in [22,23]; (4) a suspected buyer is not required to cooperate in the "identification and arbitration protocol" to make appropriate adjudications.

Finally, it is worth noting that the adoption of blockchain technology represents a relevant step in the direction of secure and simplified buyer friendly and mediated watermarking protocols. Moreover, the performance achieved by the prototype implementation of the proposed protocol is overall good, even though it is penalised by the adopted consensus algorithm. However, this cannot be considered an actual problem, since next generations of blockchains will be able to implement improved algorithms and to provide better and better performances [73,74].

Funding: This research received no external funding.

Acknowledgments: The author wishes to thank Domenico Di Pietro for his good advice.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Cox, I.; Miller, M.; Bloom, J.; Fridrich, J.; Kalker, T. *Digital Watermarking and Steganography*; Morgan Kaufmann: Burlington, MA, USA, 2007.
2. Barni, M.; Bartolini, F. Data Hiding for Fighting Piracy. *IEEE Signal Process. Mag.* **2004**, *21*, 28–39. [CrossRef]
3. Gopalakrishnan, K.; Memon, N.; Vora, P.L. Protocols for watermark verification. *IEEE Multimed.* **2001**, *8*, 66–70. [CrossRef]
4. Frattolillo, F. Watermarking protocol for web context. *IEEE Trans. Inf. Forensics Secur.* **2007**, *2*, 350–363. [CrossRef]
5. Frattolillo, F. Watermarking Protocols: Problems, Challenges and a Possible Solution. *Comput. J.* **2015**, *58*, 944–960. [CrossRef]
6. Trappe, W.; Wu, M.; Wang, Z.J.; Liu, K.J.R. Anti-collusion fingerprinting for multimedia. *IEEE Trans. Signal Process.* **2003**, *41*, 1069–1087. [CrossRef]
7. Liu, K.J.R.; Trappe, W.; Wang, Z.J.; Wu, M.; Zhao, H. *Multimedia Fingerprinting Forensics for Traitor Tracing*; Hindawi Publishing Corporation: New York, NY, USA, 2005.
8. Pehlivanoglu, S. An Asymmetric Fingerprinting Code for Collusion-resistant Buyer-seller Watermarking. In Proceedings of the 1st ACM Workshop on Information Hiding and Multimedia Security, Montpellier, France, 17–19 June 2013; ACM: New York, NY, USA, 2013; pp. 35–44.
9. Kuribayashy, M.; Tanaka, H. Fingerprinting Protocol for Images Based on Additive Homomorphic Property. *IEEE Trans. Image Process.* **2005**, *14*, 2129–2139. [CrossRef] [PubMed]
10. Memon, N.; Wong, P.W. A buyer-seller watermarking protocol. *IEEE Trans. Image Process.* **2001**, *10*, 643–649. [CrossRef]
11. Lei, C.L.; Yu, P.L.; Tsai, P.L.; Chan, M.H. An Efficient and Anonymous Buyer-Seller Watermarking Protocol. *IEEE Trans. Image Process.* **2004**, *13*, 1618–1626. [CrossRef] [PubMed]
12. Fan, C.I.; Chen, M.T.; Sun, W.Z. Buyer-Seller Watermarking Protocols with Off-line Trusted Parties. In Proceedings of the IEEE Int. Conf. on Multimedia and Ubiquitous Engineering, Seul, Korea, 26–28 April 2007; IEEE Computer Society: Washington, DC, USA, 2007; pp. 1035–1040.
13. Das, V.V. Buyer-Seller Watermarking Protocol for an Anonymous Network Transaction. In Proceedings of the 1st Int. Conf. on Emerging Trends in Engineering and Technology, Nagpur, India, 16–18 July 2008; IEEE Computer Society: Washington, DC, USA, 2008; pp. 807–812.
14. Laxmi, V.; Khan, M.N.; Kumar, S.S.; Gaur, M.S. Buyer seller watermarking protocol for digital rights management. In Proceedings of the 2nd Int. Conf. on Security of information and networks, Famagusta, North Cyprus, 6–10 October 2009; ACM: New York, NY, USA, 2009; pp. 298–301.
15. Hu, D.; Li, Q. A secure and practical buyer-seller watermarking protocol. In Proceedings of the Int. Conf. on Multimedia Information Networking and Security, Hubei, China, 18–20 November 2009; IEEE Computer Society: Washington, DC, USA, 2009; pp. 105–108.
16. Zhao, H.V.; Liu, K.J.R. Traitor-within-Traitor Behavior Forensics: Strategy and Risk Minimization. *IEEE Trans. Inf. Forensics Secur.* **2006**, *1*, 440–456. [CrossRef]
17. Rial, A.; Deng, M.; Bianchi, T.; Piva, A.; Preneel, B. A Provably Secure Anonymous Buyer–Seller Watermarking Protocol. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 920–931. [CrossRef]
18. Rial, A.; Balasch, J.; Preneel, B. A Privacy-Preserving Buyer–Seller Watermarking Protocol Based on Priced Oblivious Transfer. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 202–212. [CrossRef]
19. Xu, Z.; Li, L.; Gao, H. Bandwidth Efficient Buyer-seller Watermarking Protocol. *Int. J. Inf. Comput. Secur.* **2012**, *5*, 1–10. [CrossRef]
20. Bianchi, T.; Piva, A. TTP-free asymmetric fingerprinting based on client side embedding. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 1557–1568. [CrossRef]
21. Bianchi, T.; Piva, A.; Shullani, D. Anticollusion solutions for asymmetric fingerprinting protocols based on client side embedding. *Eurasip J. Inf. Secur.* **2015**, *2015*, [CrossRef]
22. Frattolillo, F. A Buyer–Friendly and Mediated Watermarking Protocol for Web Context. *ACM Trans. Web.* **2016**, *10*, 1–8. [CrossRef]
23. Frattolillo, F. Watermarking protocols: An excursus to motivate a new approach. *Int. J. Inf. Secur.* **2018**, *17*, 587–601. [CrossRef]

24. Frattolillo, F. A multiparty watermarking protocol for cloud environments. *J. Inf. Secur. Appl.* **2019**, *47*, 246–257. [CrossRef]
25. Tapscott, D.; Tapscott, A. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*; Portfolio-Penguin: New York, NY, USA, 2016.
26. Mougayar, W. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*; Wiley: Hoboken, NJ, USA, 2016.
27. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
28. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
29. Aggarwal, S.; Chaudhary, R.; Aujla, G.S.; Kumar, N.; Choo, K.K.R.; Zomaya, A.Y. Blockchain for smart communities: Applications, challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *144*, 13–48. [CrossRef]
30. Tresise, A.; Goldenfein, J.; Hunter, D. What Blockchain Can and Can't Do for Copyright. *Aust. Intellect. Prop. J.* **2018**, *28*, 144–157.
31. Macrinici, D.; Cartofeanu, C.; Gao, S. Smart contract applications within blockchain technology: A systematic mapping study. *Telemat. Inform.* **2018**, *35*, 2337–2354. [CrossRef]
32. Ku, W.; Chi, C.H. Survey on the Technological Aspects of Digital Rights Management. In Proceedings of the 7th Int. Information Security Conference, Lecture Notes in Computer Science, Palo Alto, CA, USA, 27–29 September 2004; Zhang, K., Zheng, Y., Eds.; Springer: Berlin, Germany, 2004; Volume 3225, pp. 391–403.
33. Zhang, Z.; Pei, Q.; Ma, J.; Yang, L. Security and Trust in Digital Rights Management: A Survey. *Int. J. Netw. Secur.* **2009**, *9*, 247–263.
34. Abdalla, H.; Hu, X.; Wahaballa, A.; Abdalla, A.; Ramadan, M.; Zhiguang, Q. Integrating the Functional Encryption and Proxy Re-cryptography to Secure DRM Scheme. *Int. J. Netw. Secur.* **2017**, *19*, 27–38.
35. Barbareschi, M.; Cilardo, A.; Mazzeo, A. A partial FPGA bitstream encryption enabling hardware DRM in mobile environment. In Proceedings of the ACM Int. Conf. on Computing Frontiers, Como, Italy, 16–18 May 2016; ACM: New York, NY, USA, 2016; pp. 443–448.
36. Lee, C.C.; Li, C.T.; Chen, Z.W.; Lai, Y.M.; Shieh, J.C. An improved E-DRM scheme for mobile environments. *J. Inf. Secur. Appl.* **2018**, *39*, 19–30. [CrossRef]
37. Bhowmik, D.; Feng, T. The multimedia blockchain: A distributed and tamper-proof media transaction framework. In Proceedings of the 22nd Int. Conf. on Digital Signal Processing, London, UK, 23–25 August 2017; IEEE Computer Society: Washington, DC, USA, 2017; pp. 1–5.
38. 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; IEEE Computer Society: Washington, DC, USA, 2018; pp. 359–364.
39. Zhaofeng, M.; Weihua, H.; Hongmin, G. A new blockchain-based trusted DRM scheme for built-in content protection. *Eurasip J. Image Video Process.* **2018**, *2018*, 91. [CrossRef]
40. Deng, M.; Preneel, B. Attacks On Two Buyer-Seller Watermarking Protocols and An Improvement for Revocable Anonymity. In Proceedings of the IEEE Int. Symp. on Electronic Commerce and Security, Guangzhou, China, 3–5 August 2008; IEEE Computer Society: Washington, DC, USA, 2008; pp. 923–929.
41. Deng, M.; Preneel, B. On secure and anonymous buyer-seller watermarking protocol. In Proceedings of the 3rd Int. Conf. on Internet and Web Applications and Services, Athens, Greece, 8–13 June 2008; IEEE Computer Society: Washington, DC, USA, 2008; pp. 524–529.
42. Deng, M.; Bianchi, T.; Piva, A.; Preneel, B. An efficient buyer-seller watermarking protocol based on composite signal representation. In Proceedings of the 11th ACM Workshop on Multimedia and Security, Princeton, NJ, USA, 7–8 September 2009; ACM: New York, NY, USA, 2009; pp. 9–18.
43. Wen, Q.; Wang, Y. Improvement of the Digital Watermarking Protocol based on the Zero-Watermark Method. In Proceedings of the 3rd Annual Summit and Conf. of Asia Pacific Signal and Information Processing Association, Xi'an, China, 18–21 October 2011; APSIPA Publisher: Xi'an, China, 2011.
44. Terelius, B. Towards transferable watermarks in buyer-seller watermarking protocols. In Proceedings of the IEEE Int. Work. on Information Forensics and Security, Guangzhou, China, 18–21 November 2013; IEEE Computer Society: Washington, DC, USA, 2013; pp. 197–202.

45. Qiao, L.; Nahrstedt, K. Watermarking schemes and protocols for protecting rightful ownership and customer's rights. *J. Vis. Commun. Image Represent.* **1998**, *9*, 194–210. [CrossRef]
46. Poh, G.S.; Martin, K.M. Classification Framework for Fair Content Tracing Protocols. In Proceedings of the 8th Int. Workshop on Digital Watermarking, Guildford, UK, 24–26 August 2009; Ho, A.T.S., Shi, Y.Q., Kim, H.J., Barni, M., Eds.; Lecture Notes in Computer Science; Springer: Berlin, Germany, 2009; Volume 5703, pp. 252–267.
47. Poh, G.S. Design and Analysis of Fair Content Tracing Protocols. Ph.D. Thesis, Department of Mathematics, Royal Holloway, University of London, Egham, Surrey, UK, 2009.
48. Cong, L.W.; He, Z. Blockchain Disruption and Smart Contracts. *Rev. Financ. Stud.* **2019**, *32*, 1754–1797. [CrossRef]
49. Fontaine, C.; Galand, F. A Survey of Homomorphic Encryption for Nonspecialists. *Eurasip J. Inf. Secur.* **2007**, *2007*. [CrossRef]
50. Bianchi, T.; Piva, A. Secure Watermarking for Multimedia Content Protection: A Review of its Benefits and Open Issues. *IEEE Signal Process. Mag.* **2013**, *30*, 87–96. [CrossRef]
51. Ellison, C.; Frantz, B.; Lampson, B.; Rivest, R.; Thomas, B.; Ylonen, T. *SPKI Certificate Theory*; RFC 2693; RFC Editor: Marina del Rey, CA, USA, 1999.
52. Williams, D.M.; Treharne, H.; Ho, A.T.S. On the Importance of One-time Key Pairs in Buyer-seller Watermarking Protocols. In Proceedings of the Int. Conf. on Security and Cryptography, Athens, Greece, 26–28 July 2010; IEEE Computer Society: Washington, DC, USA, 2010; pp. 441–446.
53. Rannenberg, K. Multilateral Security. A Concept and Examples for Balanced Security. In Proceedings of the 9th ACM Workshop on New Security Paradigms, Ballycotton, County Cork, Ireland, 18–21 February 2001; ACM: New York, NY, USA, 2001; pp. 151–162.
54. Rannenberg, K.; Royer, D.; Deuker, A. *The Future of Identity in the Information Society—Challenges and Opportunities*; Springer: Berlin, Germany, 2009.
55. Canetti, R. Security and Composition of Cryptographic Protocols: A Tutorial. *ACM SIGACT News.* **2006**, *37*, 67–92. [CrossRef]
56. Hartung, F.; Su, J.K.; Girod, B. Spread Spectrum Watermarking: Malicious Attacks and Counterattacks. In Proceedings of the SPIE Security and Watermarking of Multimedia Contents, San Jose, CA, USA, 23–27 January 1999; Delp, E.J., Wong, P.W., Eds.; SPIE: Bellingham, WA, USA, 1999; Volume 3657, pp. 147–158.
57. Katzenbeisser, S.; Veith, H. Securing Symmetric Watermarking Schemes Against Protocol Attacks. In Proceedings of the SPIE Security and Watermarking of Multimedia Contents IV, San Jose, CA, USA, 19 January 2002; Delp, E.J., Wong, P.W., Eds.; SPIE: Bellingham, WA, USA, 2002; Volume 4675, pp. 260–268.
58. Petitcolas, F.A.P. Watermarking schemes evaluation. *IEEE Signal Process. Mag.* **2000**, *17*, 58–64. [CrossRef]
59. Petitcolas, F.A.P.; Steinebach, M.; Raynal, F.; Dittmann, J.; Fontaine, C.; Fates, N. A public automated web-based evaluation service for watermarking schemes: StirMark Benchmark. In Proceedings of the SPIE Electronic Imaging 2001, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, 22–25 January 2001; Wong, P.W., Delp, E.J., Eds.; SPIE: Bellingham, WA, USA, 2001; Volume 4314, pp. 575–584.
60. Barni, M.; Bartolini, F. *Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications*; CRC Press: Boca Raton, FL, USA, 2004.
61. Chen, B.; Wornell, G. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Trans. Inf. Theory* **2001**, *47*, 1423–1443. [CrossRef]
62. Malvar, H.S.; Florêncio, D.A.F. Improved Spread Spectrum: A New Modulation Technique for Robust Watermarking. *IEEE Trans. Signal Process.* **2003**, *51*, 898–905. [CrossRef]
63. Prins, J.P.; Erkin, Z.; Lagendijk, R.L. Anonymous fingerprinting with robust QIM watermarking techniques. *Eurasip J. Inf. Secur.* **2007**, *2007*, [CrossRef]
64. Zebbiche, K.; Khelifi, F.; Loukhaoukha, K. Robust additive watermarking in the DTCWT domain based on perceptual masking. *Multimed. Tools Appl.* **2018**, *77*, 21281–21304. [CrossRef]
65. Begum, M.; Uddin, M.S. Analysis of Digital Image Watermarking Techniques through Hybrid Methods. *Adv. Multimed.* **2020**, *2020*, [CrossRef]
66. Bellare, M.; Rogaway, P. The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs. In Proceedings of the 25th Int. Cryptology Conference, Saint Petersburg, Russia, 28 May–1 June 2006; Vaudenay, S., Ed.; Lecture Notes in Computer Science; Springer: Berlin, Germany, 2006; Volume 4004, pp. 409–426.

67. Williams, D.M.; Treharne, H.; Ho, A.T.S.; Waller, A. Formal Analysis of Two Buyer-Seller Watermarking Protocols. In Proceedings of the 7th Int. Workshop on Digital Watermarking, Lecture Notes in Computer Science, Busan, Korea, 10–12 November 2008; Kim, H.J., Katzenbeisser, S., Ho, A.T.S., Eds.; Springer: Berlin, Germany, 2008; Volume 5450, pp. 278–292.
68. Canetti, R. Universally Composable Security: A New Paradigm for Cryptographic Protocols. In Proceedings of the 42nd IEEE Int. Symp. on Foundations of Computer Science, Newport Beach, CA, USA, 8–11 October 2001; IEEE Computer Society: Washington, DC, USA, 2001; pp. 136–145.
69. Paillier, P. Public-key Cryptosystems Based on Composite Degree Residuosity Classes. In Proceedings of the Eurocrypt '99, Lecture Notes in Computer Science, Prague, Czech Republic, 2–6 May 1999; Springer: Berlin, Germany, 1999; Volume 1592, pp. 223–238.
70. Ethereum. Available online: https://ethereum.org (accessed on 1 November 2020).
71. Solidity. Available online: https://solidity.readthedocs.io (accessed on 1 November 2020).
72. Bamakan, S.M.H.; Motavali, A.; Bondarti, A.B. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Syst. Appl.* **2020**, *154*, 113385. [CrossRef]
73. Fernandez-Carames, T.M.; Fraga-Lamas, P. A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories. *IEEE Access* **2019**, *7*, 45201–45218. [CrossRef]
74. Palacios, R.C.; Gordon, M.S.; Aranda, D.A. A critical review on blockchain assessment initiatives: A technology evolution viewpoint. *J. Softw. Evol. Process.* **2020**, *2020*, [CrossRef]