A Blockchain-based Application to Protect Minor Artworks

Clara Bacciu, Angelica Lo Duca and Andrea Marchetti
IIT-CNR - Via G. Moruzzi 1, 56124 Pisa, Italy

Keywords: Blockchain, Ethereum, Recordkeeping, IPFS, Cultural Heritage, Minor Artwork.

Abstract: A new emerging trend concerns the implementation of services and distributed applications through the blockchain technology. A blockchain is an append-only database, which guarantees security, transparency and immutability of records. Blockchains can be used in the field of Cultural Heritage to protect minor artworks, i.e. artistic relevant works not as famous as masterpieces. Minor artworks are subjected to counterfeiting, thefts and natural disasters because they are not well protected as famous artworks. This paper describes a blockchain-based application, called MApp (Minor Artworks application), which lets authenticated users (private people or organizations), store the information about their artworks in a secure way. The use of blockchain produces three main advantages. Firstly, artworks cannot be deleted from the register thus preventing thieves to remove records associated stolen objects. Secondly, artworks can be added and updated only by authorized users, thus preventing counterfeiting in objects descriptions. Finally, records can be used to keep artworks memory in case of destruction caused by a natural disaster.

1 INTRODUCTION

Minor artworks are works that are artistically relevant but not as well-known as famous masterpieces, or belonging to the so-called minor arts, such as books and manuscripts, pottery, lacquerware, furniture, jewellery, or textiles. Examples of such works could be those kept in some small libraries or churches, or even in private households. In general, since it is often not well protected, a minor artwork may be more subject to counterfeiting, theft, and natural disaster. In Italy, trafficking in works of art is the third most lucrative illegal activity, and globally the trend is the same. Minor artworks having a medium/high value are easy to smuggle and sell for organised crime, since controls on the origin of the good and on subsequent transactions are often limited, even in famous museums (Chiodi and Fedeli, 2018). This is true despite the existence of International treaties on protection of cultural heritage, like the UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects (Rome, 1955). As for this treaty, buyers have the obligation to check if the artwork has been stolen or illegally exported. Some databases exist that can be used to perform those checks, like the Interpol database of stolen artwork[1], but are not always up-to-date or easily accessible. To complicate things, in the last decades, Italy (as many other places in the world) has suffered a series of catastrophic events that largely affected cultural heritage: earthquakes, landslides, floods, collapses in important archaeological sites such as Pompei. Such events may have affected not only the works themselves, but even their catalogues. Finally, often, although minor artworks are registered in local databases, they can be easily erased from these catalogues, thus they can be completely forgotten in case of theft. These motivations stress the need for new practices to protect cultural heritage. Blockchain technology can prove to be effective in keeping digital archives of works of art secure and up-to-date, providing an aid for protection against natural and environmental disasters, war damages, organised crime.

In this paper we would like to demonstrate that the blockchain technology can be used to protect minor artworks and then we present a practical application (MApp) as a proof of the validity of this position. MApp combines the benefits of the blockchain technology and the Interplanetary File System (IPFS)[2] for the management of minor artworks archives. MApp provides users, either private people or organizations, a public repository for minor artworks storage. Thanks to some specific advantages of blockchain, MApp is a secure application, which prevents thieves

[1] https://www.interpol.int/How-we-work/Databases/Stolen-Works-of-Art-Database Access Date: 2019-07-29

[2] https://ipfs.io/ Access Date: 2019-07-29

Bacciu, C., Lo Duca, A. and Marchetti, A.
A Blockchain-based Application to Protect Minor Artworks.
DOI: 10.5220/0008347903190325
In *Proceedings of the 15th International Conference on Web Information Systems and Technologies (WEBIST 2019)*, pages 319-325
ISBN: 978-989-758-386-5

from removing records from the repository, prevents counterfeiters with tampering with objects descriptions, and helps users preserving artworks memory in case of destruction of the physical object. Compared to standard databases, the blockchain register guarantees integrity, transparency and authenticity of records.

The remainder of the paper is organized as follows: in Section 2 we give an overview of the blockchain and IPFS technologies and in Section 3 we illustrate the related work. Section 4 describes the problem setting and Sections 5 and 6 the MApp application and its implementation. Finally, in Section 7 we give conclusions and future work.

2 BACKGROUND

In this section we give an overview of the technologies exploited by MApp: blockchain and IPFS.

2.1 Blockchain

A blockchain is a particular implementation of a Distributed Ledger (DL) (Zheng et al., 2016). A DL is essentially a database, which is shared among different nodes of a network. In practice, all the nodes of the network share the same copy of the database and any change made on a node is replicated to all the other nodes in few minutes and, in some cases, even in few seconds. The updates to the repository (called *transactions*) are cryptographically signed by the node that sent them, and are communicated between participants in a peer-to-peer fashion. DLs can be *permissioned* (as opposite of *permissionless*) if a new record can be added to the ledger only by some trusted actor (e.g. government, departments and so on), and *private* (as opposite of *public*) if only trusted nodes can read the content of the ledger. The protocol for the first functioning blockchain was introduced in 2008 to support the Bitcoin digital currency (Nakamoto, 2008), and implements the ledger as a chain of blocks. Each block contains a payload and a header. The payload contains a series of transactions, while the header contains a timestamp, a cryptographic signature of the payload (usually a hash of the entire content), and a link to the previous block of the chain (i. e., the cryptographic hash of the previous block). This way, the integrity of the information stored in the blockchain is protected through a security system based on cryptography, since each block becomes dependent from the content of all the previous blocks, making it impossible to modify the data contained in old blocks without rewriting also the new ones. With respect to a standard database, a blockchain is an append-only register. This means that information can only be added, but it cannot be removed. Modifications to the stored data can be done by re-uploading a new version of it. A distributed consensus algorithm is used to decide which transactions are to be considered valid. New participants that want to start collaborating to the maintenance of the repository must follow this algorithm. There is no need of a central authority or trust between nodes; the consensus algorithm and cryptography grant the correctness of data even in presence of some malicious nodes. Signatures and timestamping guarantee non-repudiation and are a valid tool to perform audits. Summarizing, the big advantages of a blockchain as repository of data are that it is distributed, with no need of a central authority a no single point of failure, immutable, and secure. The main issues with blockchain implementation of distributed ledgers are scalability and efficiency: often, consensus algorithms that are used to grant consistency are expensive in terms of time and resources. But in some cases trust assumptions can be relaxed, so that simpler consensus algorithms can be used. The most important blockchain protocols are: the above mentioned Bitcoin, Ethereum (Wood, 2014), Hyperledger (Cachin, 2016).

2.2 IPFS

IPFS is a peer-to-peer distributed filesystem which permits the storage and the search of files, applications, websites and data. The substantial difference between IPFS and the classical HTTP transmission protocol, which regulates the current version of the Web, consists in the transition from a client-server architecture to a peer-to-peer architecture. The client-server architecture is characterized by a location based addressing, while the peer-to-peer one is defined by a content based addressing. This means that IPFS assigns each content an immutable address, which does not change even in case of network failure. Such an immutable address is built by applying a hash function to every content. All the hash functions are stored into a Distributed Hash Table (DHT), which is used to access contents in the IPFS.

The use of IPFS produces the following benefits: a) *availability*, which implies that a resource (e.g. web site, file and so on) is always available; b) *anti-censorship*, which implies that it is difficult for authorities to censor resources; *fast information retrieval*, which gives the possibility to access resources even in case of a slow network.

3 LITERATURE REVIEW

The problem of managing records through a blockchain has been largely investigated during the last few years. In her paper, Lemieux proposes a classification of blockchain applications (Lemieux, 2017), based on which information is stored in the blockchain: a) *mirror type*, b) *digital record type*, c) *tokenized type*.

In the mirror type, the blockchain serves as a mirror, which stores only records fingerprints. The complete information of a record is stored into an external repository and the blockchain is used only to verify records integrity. In (García-Barriocanal et al., 2017) the authors describe a first implementation of a decentralized metadata database, based on the combination of the blockchain and IPFS technologies. In their paper Liang et. al. describe ProvChain (Liang et al., 2017), a system which guarantees data provenance in cloud environments. Vishwa et. al. (Vishwa and Hussain, 2018) illustrate a blockchain-based framework, which guarantees copyright compliance of multimedia objects by means of smart contracts.

In the digital record type, the blockchain is used to store all the records in the form of smart contracts. In (Bhowmik and Feng, 2017) the authors illustrate a distributed and tamper-proof framework for media. Each media is represented by a watermark, which is firstly compressed and then stored into a blockchain. Approved modifications to media are stored in the blockchain thus preventing tampering. In (Galiev et al., 2018) the authors describe Archain, a blockchain-based archive system, which stores small-sized records. Multiple roles are defined in the system, thus allowing records creation, approval and removal.

In the tokenized type, records are stored in the blockchain and they are linked to a cryptocurrency. Adding, updating or removing a record has a cost. This constitutes an innovative case, where the literature is not consolidated yet. An example of this type of blockchain is represented by the Ubitquity Project[3], which records land transactions on behalf of companies and government agencies.

4 PROBLEM SETTING

The problem of storing minor artworks' data into an archive can be considered as a particular case of *recordkeeping*, which consists in creating, managing, preserving, and defining access conditions about records stored into an archive. ARMA International[4]'s Generally Accepted Recordkeeping Principles (ARMA International, 2017) define a global standard that identifies the criticalities and a high-level framework of good practices for information governance. They are a common set of principles that describe the conditions under which business records and related information should be maintained. They are: *Accountability*: there should be a person that is responsible and accountable for all the process; *Transparency*: all the information should be documented in an open and verifiable manner; *Integrity*: the information assets should be as authentic and reliable as possible; *Protection*: no unauthorized parties should be able to access private information; *Compliance*: laws and policies should be kept into consideration; *Availability*: information should be efficiently and accurately retrieved; *Retention*: information should remain accessible for a period of time depending on legal, regulatory, fiscal, operational, and historical requirements; *Disposition*: it should be possible to erase all the information that is no longer needed.

The following functional requirements are essential for recordkeeping (García-Barriocanal et al., 2017): a) resource discovery/information retrieval; b) resource management; c) resource use by appropriate audiences; d) security; e) linking with related resources; f) software and hardware needs.

Resource discovery and information retrieval should include an easy and fast way to search artworks and their related information. Results of searches should depend on the type of audiences: every artwork's owner should decide which information can be accessed by others. An appropriate ontology, such as the Dublin Core Ontology (Weibel, 1997), should be defined to represent artworks and permit an appropriate search by properties.

Resource management should guarantee the acquisition of news about each minor artwork, such as a temporary movement to an exhibit or a theft. Every artwork movement should be traceable and documented. In addition, only authorized users, such as the artwork's owner, should be able to register an artwork movement.

Resource use by appropriate audiences should define access control policies on artworks. Access control on information about artworks should guarantee the following aspects: 1) only its owner should add an artwork, 2) the artwork's owner should be aware of who can access and update his/her artwork, 3) only

[3]http://www.ubitquity.io/brazil_ubitquity_llc_pilot.html Access Date: 2019-07-29

[4]ARMA International is a not-for-profit professional association and a global authority on governing information as a strategic asset

authorized users could access an artwork, 4) a group of supervisor users should manage artworks in terms of approvals/rejects.

Security of minor artworks should concern the following aspects: privacy, authenticity and integrity. Privacy is a security property which allows only authorized users to access data. Authenticity is the property of attributing records to their legitimate authors. Integrity refers to the property of guaranteeing that a record has not been modified by anyone. Integrity should be provided through a tamper-proof environment, where every artwork is not modified by unauthorized users.

Linking is one of the most interesting aspects that a system for recordkeeping should provide. Linking should concern both relations among artworks of the same archive (internal linking) and among artworks of different archives (external linking). In general, linking is not a simple task, because it cannot be made completely automatic. Human operators, in fact, must check that links among resources are correct, in order to guarantee the quality of links.

Software and hardware needs refer to digital preservation of artworks thus making them available over time. Recordkeeping should take care of storage media instability and deterioration, which could lead to data loss, and technology obsolescence and incompatibility, which may happen both at the hardware and software level.

Moreover, we took into consideration the the ISO Standard 15489-1:2016 *Information and documentation Records management*(ISO, 2016), that defines concepts and principles for the creation, acquisition and management of records. Section 7.2 Characteristics of a record lists the following: *Authenticity*: records must be created and maintained in such a way that creators are authorized and identified, and that records are protected against unauthorized addition, deletion, alteration, use and concealment; *Reliability*: the content of a record should be accurate, and its creator should be worth of trust; *Integrity*: a record should be complete and protected against unauthorized alteration. Every alteration should be documented and traceable; *Usability*: a usable record is one that can be located, retrieved, presented and interpreted.

All the described functional requirements are considered in this paper, but linking, which is deferred as future work and investigation.

5 MAPP

In order to satisfy almost all the requirements of recordkeeping, we propose MApp, a system which combines and exploits the benefits of blockchain and IPFS. The use of blockchain for recordkeeping is able to satisfy some of the requirements described in Section 4. In particular, a blockchain satisfies resource management and resource use by appropriate audiences indirectly, resource discovery/information retrieval, security directly (García-Barriocanal et al., 2017). The use of IPFS for recordkeeping can guarantee digital preservation of minor artworks. Linking with related resources cannot be guaranteed neither by a blockchain nor by an IPFS, because it requires an additional logic, based for example on mechanisms defined by Semantic Web (Berners-Lee et al., 2001) and Linked Data (Bizer et al., 2011). Currently, this aspect is out the scope of this paper. We defer this kind of research to future work.

5.1 Users

Users of the system may play one of the following roles: *generic user*, *publisher*, *verifier*. A generic user can *search* for an approved artwork in the system. The search can be done by artwork author or title. A publisher user can *publish* or *update* an artwork in the system. When a new artwork is published, its status is set to *pending*. This means that the artwork is not approved yet thus cannot be accessed by third parties neither can be updated by its author. A verifier is an expert in the field to which the artwork belongs, and can *vote* for the approval of the artwork description. If an artwork reaches a certain number of votes (a parameter that can be set in the system), its status becomes *approved*, thus it can be searched by generic users and updated by its publisher. This mechanism based on votes constitutes a basic algorithm for compliance with the principle of reliability of a record. More complex strategies can be defined and we defer this kind of study to future work.

5.2 Artwork Description

Every minor artwork is described through some properties defined through vocabularies. Although there are many more or less formal standards for the description of artworks, in our system we exploit two vocabularies: Dublin Core[5] and extended Dublin

[5]http://www.dublincore.org/specifications/dublin-core/dces/ Access Date: 2019-07-29

Table 1: Properties defined in Dublin Core and the Extended Dublin Core.

Property	DC	Extended DC
Abstract	✗	✓
Access Rights	✗	✓
Accrual Periodicity	✗	✓
Alternative Title	✗	✓
Contributor	✓	✓
Coverage	✓	✓
Creator	✓	✓
Date	✓	✗
Date Available	✗	✓
Date Created	✗	✓
Date Modified	✗	✓
Description	✓	✓
Format	✓	✓
Identifier	✓	✓
Language	✓	✓
License	✗	✓
Member Of	✗	✓
Publisher	✓	✓
Relation	✓	✓
Rights	✓	✓
Spatial Coverage	✗	✓
Source	✓	✓
Subject	✓	✓
Temporal Coverage	✗	✓
Title	✓	✓
Type	✓	✓
Version	✗	✓

Core[6]. Dublin Core provides 15 basic properties to describe artworks. Extended Dublin Core allows a more detailed description of an artwork, through the use of qualifiers (or subclasses) that allow a refinement of the scheme with the addition of more precise meanings on the basic terms. Each Dublin Core element is optional and may be repeated. Table 1 shows which properties are present in the two sets.

The choice of these metadata elements was made by taking into account two factors. First of all, we tried to choose vocabularies able to represent the vast set of typologies of minor artworks. Secondly, we chose a compromise between the complexity of the description, the ease of use for a non-expert user and the degree of precision of the system used. For this reason, a user can choose one of the two sets to represent their artworks. Dublin Core provides a meta information scheme designed to assign reasonably broad properties to any digital material. It is a flexible, simple and extensible scheme that is suitable for most of the foreseen use cases.

[6]http://dublincore.org/specifications/dublin-core/dcmi-terms/ Access Date: 2019-07-29

5.3 Operations

As already said, a publisher can perform two operations: *publish* and *update* an artwork.

Algorithm 1: Publish(artwork).

```
f ← artwork.facsimiles
m ← artwork.metadata
s ← subset(m)
binary1 ← transform(f)
if binary1 then
  hash1 ← upload_to_ipfs(binary1)
  if hash1 then
    m* ← artwork.metadata + hash1
    binary2 ← transform(m*)
    if binary2 then
      hash2 ← upload_to_ipfs(binary2)
      if hash2 then
        result ← add_to_blockchain(hash2, s)
        return result
      end if
    end if
  end if
end if
return FALSE
```

Algorithm 1 shows the pseudocode of the publish operation. Every artwork is composed of one or more facsimiles and some metadata, done through one of the previously described vocabularies. The facsimiles are converted in binary data (through the *transform* function) and then uploaded to the IPFS (through the *upload_to_ipfs* function). The upload returns an hash for each facsimile, and the hashes are included in the artwork metadata. The metadata undergoe the previous two steps (*transform* and *upload_to_ipfs*). The returned hash of the metadata is then saved in the blockchain, together with a small subset of the artwork metadata, used for the search operation.

The function for update is similar to that for publication: it receives the artwork and its new metadata as input; if the status is *approved*, the new metadata are transformed to binary and then updated in the IPFS. If this last operation is successful, the new metadata are added to the blockchain.

Algorithm 2 shows the search function, which receives a *metadata* as input. The metadata can be either an author or an artwork name. The function searches for the metadata in the blockchain and returns the list of matching artworks pointers. For each retrieved artwork pointer, the complete artwork information (metadata and facsimiles) is taken from IPFS and added to the result.

Algorithm 2: Search(metadata).

```
artwork_list ← get_by_tag_blockchain(metadata)
result ← 0
if artwork_list then
  for artwork_pointer in artwork_list do
    hash ← artwork_pointer.hash
    artwork ← get_ipfs(hash)
    result.append(artwork)
  end for
end if
return result
```

6 IMPLEMENTATION

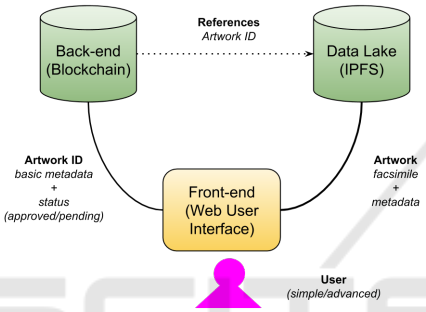

Figure 1: The system architecture.

Figure 1 illustrates the MApp architecture, which is composed of three elements: a) the *front-end* (Web User Interface), b) the *back-end* (blockchain), c) the *data lake* (IPFS). The front-end provides the users with all the operations to manage artworks. The back-end contains the transactions concerning every artwork. The data lake contains all the artworks (facsimiles and metadata), which can be accessed through the description hash contained in the blockchain. As back-end the Ethereum blockchain[7] was used. For the Data Lake, MApp exploits IPFS. In order to establish the connection between the back-end and the front-end, javascript and web3.js[8] were used, while for the connection between the back-end and the data lake, Infura[9] was exploited. The source code of MApp can be downloaded from GitHub[10]. There is also a live version of MApp[11] (available only in Italian).

[7]https://www.ethereum.org/ Access Date: 2019-07-29
[8]https://web3js.readthedocs.io/en/v1.2.0/ Access Date: 2019-07-29
[9]https://infura.io/ Access Date: 2019-07-29
[10]https://github.com/lukasd2/Digital-Archives-dApp Access Date: 2019-07-29
[11]https://lukasd2.github.io/Digital-Archives-dApp/src/artworks.html Access Date: 2019-07-29

6.1 The Web User Interface

On the left side of the Web Interface (Footnote 11) it is possible to activate the module for inserting an object and to consult the main information relating to the active user (the user address, the token balance and the permissions). The central section contains the list of all the artworks recorded on the blockchain and the main information about each object. It also allows you to filter objects based on their approval status and search by title. The part on the right shows the complete description and the facsimiles of a selected artwork, extracted from the Data Lake.

6.2 The Blockchain

As already said, MApp exploits the Ethereum blockchain to manage artworks. All the artworks are stored into an Archive, which is represented by the following smart contract, written in Solidity[12]:

```
contract Archive{
 mapping (uint => Artwork) public artworks;
 uint artworkCounter;

 function publishArtwork(...){...}
 function updateArtwork(...){...}
 function searchArtwork(...){...}
 function approveArtwork(...){...}
}
```

The `artworks` variable contains all the artworks, both approved and not approved yet, `artworkCounter` contains the current number of artworks contained in the archive. The functions define all the operations that can be done on the archive: `publish`, `update`, `search` and `approve` an artwork.

Every artwork is defined by a structure containing: the Artwork ID, the address of the author of the description, the artwork name or title, the hash of the complete description of the artwork on IPFS, the hash of the representative image associated to the artwork on IPFS, the approval status (true if approved or false if not approved yet), the number of positive votes for approval.

Users management is implemented through three well-known contracts (`Whitelist.sol`, `RBAC.sol` and `Roles.sol`), taken from the OpenZeppelin library[13]. These contracts are used to add users to the list of advanced users, which can vote for artworks approvals.

[12]https://solidity.readthedocs.io/en/v0.5.5/ Access Date: 2019-07-29
[13]https://openzeppelin.org/ Access Date: 2019-07-29

6.3 The Data Lake

As already said, the Data Lake is implemented through IPFS. When a user publishes a new artwork, this is added to the Data Lake, where it is identified through a unique description hash that guarantees that information is not changed without a corresponding update transaction. The same description hash is also stored in the blockchain, together with some basic information (such as the artwork author) and its status.

7 CONCLUSIONS AND FUTURE WORK

In this paper we have described MApp, a blockchain-based application, aimed to be an aid for the protection of minor artworks. We have described numerous advantages of the use of blockchain to protect Cultural Heritage. First of all, a blockchain is intrinsically distributed, in the sense that data are not hosted by a single central authority, thus all the information it stores is replicated on all the nodes of the network. This means that there is no single point of failure, so the archive is protected against accidental data loss or malicious attempts to erase information during a theft. In addition, in case of artworks destruction, caused for example by a natural disaster, the blockchain may contribute to keep the artworks memory for an indefinite period of time. Secondly, only authorized users can add/update artworks, thus preventing counterfeiting of the descriptions, and all the changes to the artwork description are documented and remain traceable in case of audits. It is worth mentioning, though, that identity authentication is performed by checking if a transaction is signed with a correct private key. That is, identity is associated with key ownership, with no guarantees over the real identity of the owner of that key. As future work, we would like to validate the implemented solution through experiments, and test it in a real use-case, i.e. to store objects contained in local and small museums. In addition, we would like to test the benefits of implementing the system using another type of blockchain, such as Hyperledger[14].

ACKNOWLEDGEMENTS

We would like to thank Lukasz Szczygiel for his thesis work in the implementation of MApp.

[14]https://www.hyperledger.org/ Access Date: 2019-07-29

REFERENCES

ARMA International (2017). *Generally Accepted Record-keeping Principles*.

Berners-Lee, T., Hendler, J., Lassila, O., et al. (2001). The semantic web. *Scientific american*, 284(5):28–37.

Bhowmik, D. and Feng, T. (2017). The multimedia blockchain: A distributed and tamper-proof media transaction framework. In *2017 22nd International Conference on Digital Signal Processing (DSP)*, pages 1–5.

Bizer, C., Heath, T., and Berners-Lee, T. (2011). Linked data: The story so far. In *Semantic services, interoperability and web applications: emerging concepts*, pages 205–227. IGI Global.

Cachin, C. (2016). Architecture of the hyperledger blockchain fabric. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*.

Chiodi, S. and Fedeli, G. C. (2018). Beni culturali e conflitti armati, catastrofi naturali e disastri ambientali: le sfide ei progetti tra guerra, terrorismo, genocidi, criminalità organizzata.

Galiev, A., Prokopyev, N., Ishmukhametov, S., Stolov, E., Latypov, R., and Vlasov, I. (2018). Archain: a novel blockchain based archival system. In *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, pages 84–89.

García-Barriocanal, E., Sánchez-Alonso, S., and Sicilia, M.-A. (2017). Deploying metadata on blockchain technologies. In *Research Conference on Metadata and Semantics Research*, pages 38–49. Springer.

ISO (2016). *ISO 15489-1/2: 2016-Information and documentation - Records management*.

Lemieux, V. L. (2017). A typology of blockchain record-keeping solutions and some reflections on their implications for the future of archival preservation. In *2017 IEEE International Conference on Big Data (Big Data)*, pages 2271–2278.

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., and Njilla, L. (2017). Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, pages 468–477.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Vishwa, A. and Hussain, F. K. (2018). A blockchain based approach for multimedia privacy protection and provenance. In *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 1941–1945.

Weibel, S. (1997). The dublin core: a simple content description model for electronic resources. *Bulletin of the American Society for Information Science and Technology*, 24(1):9–11.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 151:1–32.

Zheng, Z., Xie, S., Dai, H.-N., and Wang, H. (2016). Blockchain challenges and opportunities: A survey. *Work Pap.–2016*.