Forensic Science International: Digital Investigation 35 (2020) 301017

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

A blockchain based solution for the custody of digital files in forensic medicine

Monia Lusetti [a, *], Luca Salsi [b], Andrea Dallatana [c]

[a] Azienda Unità Sanitaria Locale – IRCCS di Reggio Emilia, Via Amendola 2, 42122, Reggio Emilia, Italy
[b] Independent Researcher, 19 Rue Saint Philippe, 06000, Nice, France
[c] Independent Researcher, Fraz. Ghiara Sabbioni 117 Fontanellato, 43012, Parma, Italy

ARTICLE INFO

Article history:
Received 5 June 2019
Received in revised form
16 June 2020
Accepted 17 June 2020
Available online xxx

Keywords:
Forensic science
Digital file integrity
Secure evidence storage
Blockchain
Cryptography

ABSTRACT

Despite the benefits that digital forensic medical evidence offers, the custody and sharing of such information remains an ongoing problem. While waiting for an optimal solution, both professionals and institutions must evaluate their options and choose the least disadvantageous among them. This paper proposes resolving the problem through an operational hybrid platform that uses a consensus mechanism to record a transparent history of access and prevent unauthorised users from modifying it. The digital evidence is encrypted and saved in an online file storage system, while the file properties are stored on a private implementation of the Hyperledger Fabric™ blockchain. The blockchain nodes allow access to the data through a dynamic consensus mechanism, and all operations (like uploads, views, or deletions) are continuously and permanently recorded on the blockchain. The network is safe and accessible through a dedicated application. All information is agreed upon and shared between the blockchain nodes to avoid single points of failure, and secure access to digital evidence is assured by combining cryptography and the blockchain consensus mechanism.

The result is a secure and complete framework with which to upload, store and share digital forensic medical evidence.

Despite some limitations, this proposal offers an implementable solution for the custody of digital evidence in forensic medicine that has been identified through existing and innovative technologies, the implementation of a proof of principle prototype, and benchmarks.

1. Introduction

When a potential crime is being investigated, health practitioners play an important role in documenting injuries, health conditions, or negative findings. For example, photo-documentation by health practitioners can benefit patients, the justice system, and third parties, enhancing and reinforcing written descriptions and hand-drawn body diagrams (Office of the United Nations High Commissioner for Human Rights, 2004; World Health Organization Geneva, 2003; Faculty of Forensic and Legal Medicine PICS Working Group, 2017; The Royal College of Pathologists of Australasia, 2018; Office of Criminal Justice Planning, 2001). However, despite the adoption and evolution of technology in mainstream society, many practitioners still hesitate to use digital files for documentation purposes. Such reluctance derives mainly from the concerns, frustrations, and worries related to less-standardised aspects of digital evidence application and management (Witzke and Robinson, 2016; Robinson and Robinson, 2016a).

For the purposes of this document, the terms 'digital evidence' and 'electronic evidence' refer to any information of probative value that is stored or transmitted in binary form and that is produced during a medical examination. For example, digital images of one person's body, including the genitalia, anus, and breasts, can be collected with suitable recommended technology.

Frequently, the creation of digital evidence requires uncommon skills within the medical community like the mastery of a digital single-lens reflex (SLR) camera (Faculty of Forensic and Legal Medicine PICS Working Group, 2017; The Royal College of Pathologists of Australasia, 2018; Anderson and Moore, 2018a) or training in specific software. Then, assuming that professionals

* Corresponding author.
E-mail addresses: lusetti.mo@gmail.com (M. Lusetti), salsi.luca@gmail.com (L. Salsi), an.dallata@gmail.com (A. Dallatana).

https://doi.org/10.1016/j.fsidi.2020.301017
2666-2817/

possess enough of a technical background, digital files containing sensitive or private data storage, access, retention, and retrieval can be managed by choosing the less-disadvantageous option among a wide range of possibilities, none of which, are considered totally secure at the moment (Faculty of Forensic and Legal Medicine PICS Working Group, 2017; Anderson and Moore, 2018b). Moreover, digital file submissions involve consultation and coordination with different agencies like police forces, courts, the patient, social services, insurance companies, the prosecution, the defence, other health professionals or other medico-legal services (Anderson and Moore, 2018c). In particular, when different parties must share data, the level of complexity increases, and often professionals struggle with ethical issues, legal duties, and technical problems.

In this paper, we propose a practical solution to the problem of uploading, storing, submitting, and sharing digital evidence amongst health professionals and other agencies, starting from a theoretical level and considering issues like the chain of evidence and data protection.

Mostly, healthcare professionals collect electronic evidence during their clinical practice; investigations into alleged or suspected ill-treatment, physical abuse, domestic violence, and sexual assault; work in police custody; or their activity as pathologists (Office of the United Nations High Commissioner for Human Rights, 2004; World Health Organization Geneva, 2003).

Such digital files can eventually be offered as an item of evidence in court; then, their identification or authentication must be provided (Office of the United Nations High Commissioner for Human Rights, 2004; World Health Organization Geneva, 2003; Robinson and Robinson, 2016b). In other words, a witness must give evidence of their accuracy through chronological documentation that records the sequence of custody, control, transfer, analysis, and disposition of electronic evidence. Thus, the chain of custody ensures the identity and integrity of evidence, while it excludes its tampering or alteration. Through this process, evidence becomes acceptable for courts and other agencies and is defensible; moreover, misidentification and adulteration risks are eliminated. At the same time, based on a well-documented chain of custody, the party against whom the evidence is provided will be able to object to it when first disclosed, or to withdraw from other objections.

The international forensic medical community has not yet reached a consensus regarding digital evidence custody and sharing (Office of the United Nations High Commissioner for Human Rights, 2004; Faculty of Forensic and Legal Medicine PICS Working Group, 2017; The Royal College of Pathologists of Australasia, 2018; Robinson and Robinson, 2016a; Kelly and Regan, 2003; Scientific Working Group on Digital Evidence, 2017; New South Wales Health, 2015; Scientific Working Group Imaging Technology, 2012a; den Otter et al., 2013). As an alternative to traditional hard copies, some of the more detailed current medical guidelines (Faculty of Forensic and Legal Medicine PICS Working Group, 2017; The Royal College of Pathologists of Australasia, 2018; New South Wales Health, 2015) recommend downloading images from a hard drive onto a ‘secure’ system, which implies using appropriate security safeguards such as encryption technology, passwords, and PIN codes. At this stage, the initial file is considered the ‘best evidence’ or the ‘Master Copy’ since it is the closest to the original. Subsequently, a ‘Working Copy’ is usually made, either from the original or from the best evidence, for professional use (Faculty of Forensic and Legal Medicine PICS Working Group, 2017; Anderson and Moore, 2018a). However, every time the best evidence has to be released to other parties such as a court, the chain of custody form must be updated, or a new one must be attached to the top of the stack. In the end, the evidence, a stack of log forms, and a witness who can authenticate them are the basic requirements for a correct prosecution worldwide.

To ensure the integrity of the files, a more sophisticated method exists, and it consists of generating and storing a file hash as soon as the digital file is uploaded (Scientific Working Group on Digital Evidence, 2017; Scientific Working Group Imaging Technology, 2012a). Thus, every user can verify that the file has not been altered since the hash was computed. Despite its benefits, the file-hashing technique is more common within police forces than in healthcare services, and some outstanding issues of tampering and substitution could still persist as the file hash needs to be stored in a database which is vulnerable to different types of attacks (Cerrudo and Fayo, 2007).

Additional challenges around electronic evidence include holding it longer than necessary, which is considered unsafe with regard to confidentiality (Official Journal of the European Union, 2016a; Official Journal of the European Union, 2016b; Department of Health, 1996; Federal Trade Commission, 2013; Australian Government Fed, 2014; California Civil Code, 2018) and a waste of resources (Faculty of Forensic and Legal Medicine PICS Working Group, 2017; The Royal College of Pathologists of Australasia, 2018; New South Wales Health, 2015). Yet file deletions are a time-consuming and demanding process for the professionals or the institutions involved.

All the above-mentioned problems lead to a significant discrepancy in what patients (Page et al., 2011), decision-makers (Scientific Working Group Imaging Technology, 2012b; Nagosky, 2005), and the public (Robinson and Robinson, 2016a) expect from digital forensic medical evidence, what current leading guidance explicitly establishes (Faculty of Forensic and Legal Medicine PICS Working Group, 2017; The Royal College of Pathologists of Australasia, 2018; New South Wales Health, 2015; Department of Justic, 2013), and what health professionals concretely put into practice (Anderson and Moore, 2018a, 2018b, 2018c). As modern technology evolves quickly, digital evidence has to meet strict legal requirements and unrealistic social expectations, but current recommendations for health practitioners vary widely and lack specificity, encouraging the use of cryptography at the most (New South Wales Health, 2015).

Due to the complexity of the framework and significant variables like a tight schedule, an unsuitable setting, the patient's level of cooperation, budget limitations, technical issues, and law constraints, health professionals can feel overwhelmed when presenting evidence in court (Faculty of Forensic and Legal Medicine PICS Working Group, 2017; Robinson and Robinson, 2016a). Furthermore, they worry that the success of criminal prosecution in high-profile cases or when international cooperation is needed could be compromised by less ordinary issues regarding the chain of evidence (Faculty of Forensic and Legal Medicine PICS Working Group, 2017; Anderson and Moore, 2018a; Anderson and Moore, 2018b; Anderson and Moore, 2018c).

To our knowledge, modern technology has narrowed the gap between expectations and reality in this field but has not yet gained its full potential.

In our opinion, the keystone to meeting expectations for transparent and safe evidence management among agencies within the respect of current legal requirements are blockchain technologies. We define blockchain technology as an open, distributed ledger that can record transactions between two parties in an efficient, verifiable, and permanent way (Iansiti and Karim, 2017). In particular, distributed-ledger technologies are digital systems for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time. Unlike traditional databases, distributed ledgers have no central data store or administrative functionality. Here, each node processes and verifies all data generating a record and creating a consensus of its veracity. A distributed ledger is optimal to record data and allow

dynamic transactions. It is a significant revolution in record-keeping, changing the gathering and dissemination of information (Nakamoto, 2009).

Instead of the traditional trust-based paper trail or a digital system employing a username/password combination, a user authentication system based on cryptographic proof and stored on physical devices is used. As a result, the proof of identity is more robust and secure.

In this paper, we propose a solution to the problem of preserving 'best evidence' while safeguarding confidentiality, through a hybrid platform that stores the encrypted digital evidence in a redundant online file storage and interacts with a private implementation of the Hyperledger Fabric™ blockchain.

2. Solution description

The proposed solution is a digital platform, called Custody Chain (CC), which aims to facilitate the coordinated work of healthcare professionals and law enforcement agencies, creating a full framework where digital evidence is securely uploaded, stored and shared by several applications included into the platform. The purpose is to create an efficient chain of evidence for electronic evidence that meets confidentiality duties and justice administration requirements.

As a precondition, current best practices require an uncompromised computer equipped with a secure operating system (Scientific Working Group on Digital Evidence, 2018; Home Office Scientific Development Branch, 2007), and it has to have the CC platform installed.

For exposition purposes, the process applicable to digital photographs of a forensic medical case is described below. After appropriate changes in the acquisition process, the following solution applies to other types of digital medical imaging.

Digital evidence consists of a file with the data structure shown in Table 1.

2.1. Encryption, USB device and file hash

To upload the original file into the platform, previously authorised professionals shoot images through a camera, or other recording device, equipped with a commercially available Secure Digital (SD) card memory, which is inserted in a card reader.

Once transferred to the computer, images are encrypted automatically by the CC platform with a symmetric key cryptography (Advanced Encryption Standard (AES) with 256 bits key) (Department of Commer, 2001). Symmetric cryptography is most suitable to encrypt large files like high-resolution images or videos, and AES has been recognised as a secure and efficient algorithm for symmetric cryptography (Department of Commer, 2001; Hofheinz and Kiltz, 2007). To distribute the symmetric key to the authorised users safely, it is encrypted with their 2048 bits Rivest–Shamir–Adleman (RSA) asymmetric public key (Rivest et al., 1978).

The user's asymmetric private key is stored in a small portable device that each user receives once registered to the CC platform. The device contains the personal cryptographic data of the user, and it is connected to the computer through a Universal Serial Bus (USB) connection. The USB device, as represented in Fig. 1, stores the user private key in an internal tamper-resistant Hardware Secure Module (HSM), secured against both computer viruses and hardware attacks.

Moreover, the USB device is protected with a 6-digit Personal Identification Number (PIN). The device is personal, and it is blocked after three wrong PIN insertions. Several commercial products that would fit the requirements are already available.

The USB device is used as authentication method as well to access to the platform, removing the usage of username and password.

Only authorised users equipped with their USB device including the private key can decrypt and access files. This solution adopts an hybrid cryptosystem combining an AES 256 bits symmetric key cryptography, to encode/decode the file, with a 2048 bits RSA asymmetric key cryptography to distribute the symmetric key.

Then, the platform deletes the content from the SD card and performs a wipe process to delete all the data present on the SD card permanently. The wipe process follows the National Institute of Standards and Technology Special Publication (NIST SP) 800-88 standard (Kissel et al., 2014). Next, the encrypted file is saved on the online file storage; thus, all the following online phases involve encrypted images.

The file's hash is immediately generated and stored on the blockchain among file properties like name, time stamp and metadata. Several hash algorithms like Message-Digest 5 (MD5) or Secure Hash Algorithms (SHA) are already in use in the field of computer forensics (Netherlands Forensic Institute Ministry of Justice and Security, 2018). For the platform we chose a 256 bits SHA3 algorithm as state of the art in the industry (National Institute of Standards and Technology, 2015).

2.2. Platform workflow

The operational steps of the platform are the following:

1. Files are transferred by the professional from the camera SD to the computer with the CC platform installed.
2. As soon as transferred, files are encrypted by the platform, and stored automatically in a redundant online file storage.
3. After the storage, the file on the camera SD is deleted automatically and permanently by the platform.
4. The user creates a case on the platform grouping together multiple files.
5. The platform generates a univocal identification code (ID) for each file, and a univocal ID code (Case ID) to identify a specific set of files. The responsibility to authenticate the Case ID remains on the uploader.
6. User's notes are saved in the file properties and stored automatically on the blockchain with the files' metadata.
7. A pointer to the file and the file's hash are stored on the blockchain, to ensure the integrity of the file and the preservation of its metadata, if present.
8. Administrative rights are assigned to the logged in professional (i.e. the doctor), who is temporarily in charge of the case. Then, the administrator (Admin) can authorise viewing rights to users who registered before (i.e. other professionals).
9. Users are classified continuously based on their registration data (i.e. position and rank), so administrative rights are transferred automatically to the higher in rank. Previous users keep the viewer's rights as far as they are authorised by the current Admin.
10. Registered professionals, like judges and lawyers, will be able to view the files only when assigned to the corresponding viewing rights by the Admin. Each information access like date, time and user's data is traceable since recorded and stored onto the blockchain.
11. As the case evolves, users and the official in charge may change. So, administrative rights are transferred, and viewing rights can be added or revoked within the platform.

Two types of Admins are necessary within the platform, the Platform Admin and the Case Admin.

Table 1
Summary of the data structure.

Type of data	Where to be saved	List of data
File properties	On the blockchain	- File ID (6 alphanumeric characters); - file hash (256 bits); - file metadata (specific to the type of file, for example file name, file type, date, time, device, size, dimensions, shutter speed, aperture, ISO, flash, exposure, focal length, white balance, location); - uploader ID; - upload timestamp; - eventually, description (string with useful information associated with the image); - eventually, keywords; - Case ID; - User ID authorised to view the file (list); - symmetric key encrypted with the authorised users public keys (list); - report of authorised accesses (timestamp, UserID, operation type); - report of unauthorised access attempts (timestamp, UserID).
File properties	On a Hardware Security Module	- Symmetric key needed to encrypt/decrypt the file.
User properties	On the blockchain	- User ID (technical alphanumeric string); - RSA 2048 bits public key; - description; - uploader (Y/N); - administrator rank; - list of Case IDs for which the user is Case Admin; - list of Case IDs for which the user has access to; - list of File IDs for which the user has access individually; - list of accesses (timestamp, File ID, operation type).
User properties	On the USB device	- RSA 2048 bits private key; - RSA 2048 bits public key; - user ID (technical alphanumeric string).
Case properties	On the blockchain	- Case ID (6 alphanumeric characters); - eventually, description (string with useful information associated with the case); - list of File IDs; - Case Admin ID; - list of users authorised to upload files to the case; - list of users authorised to view the files of the case.

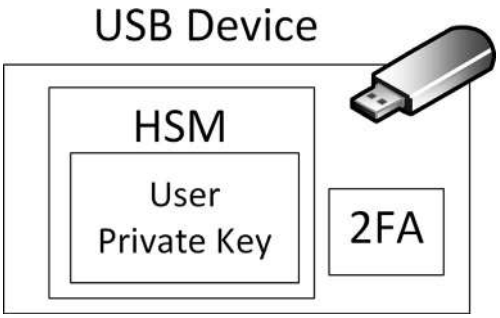

Fig. 1. Representation of the USB device's functional components.

Platform Admins are the Information Technology (IT) professionals in charge of the correct platform's operational functioning and of the users' management. They administer the creation of new profiles and the physical distribution of USB devices, but they cannot assign viewing rights. In exceptional cases, they can add or remove Case Admins or files following a precise procedure. They redistribute lost credentials like passwords or USB devices. Also, they offer general support to the users, handling occurrences and organising training sessions when required.

Case Admins consist of different registered users, depending on the jurisdiction; they include healthcare professionals, prosecution officers, judges, lawyers, or other authorised professionals. According to their rank, they are allowed to edit the list of users who access the specific set of files, adding or revoking viewing rights. Since the platform allows one Case Admin per case, the uploader is appointed as first Case Admin. As the case evolves, administrator rights are transferred automatically when viewing rights are assigned to a higher-in-rank user by the Case Admin. The current Case Admin can manually transfer the case ownership to a user with equal or superior administrator rank, using a dedicated platform functionality. By default, former Case Admins can keep the viewing rights on the set of files unless they are revoked by the new Case Admin.

The platform interacts with a private implementation of the Hyperledger Fabric™ blockchain, and information is synchronised continuously among all nodes to guarantee data integrity. Meanwhile, unauthorised access is avoided through a consensus mechanism in real time. Furthermore, stored files are not modifiable, and the file's hash is stored on the blockchain to guarantee integrity.

The functional diagram of the platform is shown in Fig. 2.

When a user displays a file, the platform records the access with the useful information; this information is stored and synchronised on the blockchain in chronological order.

2.3. System storage and blockchain synchronisation

The online file storage is redundant and its compliance with current predominant data protection laws (Official Journal of the European Union, 2016a; Official Journal of the European Union, 2016b; Department of Health, 1996; Federal Trade Commission, 2013; Australian Government Fed, 2014) derives from the attribution of the univocal Case ID. As illustrated in point 5 of paragraph 2.2 'Platform workflow', for each file and set of files the platform provides to the user a univocal code to assign to the patient, and to report in the medical records; thus, within the platform, patients' pictures will not be attributable to their personal data. Moreover, files are stored using commercial services already compliant with data protection laws.

When required, the online file storage can be located in the proper national domain.

Due to confidentiality issues and the users involved, the adopted

blockchain technology has to be private, permissioned, and it has to support smart contracts. To this end, public blockchains like Ethereum (Buterin, 2013) do not fit the case. At the same time, Hyperledger Fabric™ (Hyperledger Fabric, 2017) hosted by The Linux Foundation® does fit the case. It is private, permissioned and allows a smart contract logic. In other words, public blockchains are open systems that allow anyone to take part in the network. Instead, the peers of a Hyperledger Fabric™ network are agreed through a Membership Service Provider (MSP). Hyperledger Fabric™ provides a membership identity service defined within their Endorsement policies; it manages user IDs and authenticates the participants on the network. Furthermore, the new blocks in the Hyperledger Fabric™ blockchain are agreed through a consensus mechanism, instead of using protocols like Proof of Work or Proof of Stake, ensuring faster performance and less energy consumption. Fabric achieves end-to-end throughput of more than 3500 transactions per second in certain popular deployment configurations, with sub-second latency, scaling well to over 100 peers (Androulakiet al., 2018). Hyperledger Fabric™ is licensed under a Creative Commons Attribution 4.0 International License.

The blockchain peers host the ledger and the smart contracts and they are in charge of validating all the network transactions (Hyperledger Fabric, 2017). They are built in health facilities, courts, police stations and other subsidiaries, as shown in Fig. 3.

Peers with access to integrated HSMs can be designated as authority nodes and they provide an additional level of security to all encryption operations of evidence files by ensuring that their symmetric keys are never exposed to potentially insecure systems.

An authority node operates as a server-side automated runtime process; it also acts as an authorised user for all cases in its jurisdiction since it stores the file symmetric key.

Platform Admins can interact with authority nodes to perform authorisation related activities within the blockchain consensus logic.

2.4. Platform operations

2.4.1. General access to the platform

Each user accesses the platform only with its PIN-protected USB device without the need of username and password. Once the CC desktop application has been opened, it accesses the personal USB device to sign an authorisation transaction with the embedded private key.

The user is prompted to input the 6-digit PIN and, on the positive confirmation, he is finally able to perform all authorised operations.

2.4.2. Case creation

If authorised to do so, a platform user can create a new case, by activating the corresponding operation and by providing all case properties as shown in Table 1.

A new Case ID is created automatically, and the user becomes the Case Admin.

The new case is added on the blockchain with the corresponding properties.

2.4.3. File upload

A platform user with upload rights and access to the case wants to add a new file to an existing case. After the file is read from the SD card, the file hash is generated and stored on the blockchain with all its properties. The platform generates a new File ID, and the file is added to the case chosen by the user.

The file is encrypted by the application with a newly generated symmetric key, which is encrypted with the public key of all authorised users and stored on the blockchain among the file properties, as shown in Table 1.

Then, the encrypted file is uploaded to the online storage, and the file on the SD card is wiped permanently.

The functional diagram of this operation is shown in Fig. 4.

2.4.4. View file

A user with the corresponding view rights wants to see a file. The platform retrieves the file's private key encrypted with the user's public key from the blockchain and the encrypted file from the online storage. The application decrypts the symmetric key with the user's private key taken from the USB device. The file is decrypted; its hash is calculated and verified with the one stored on the blockchain.

The functional diagram of this operation is shown in Fig. 5.

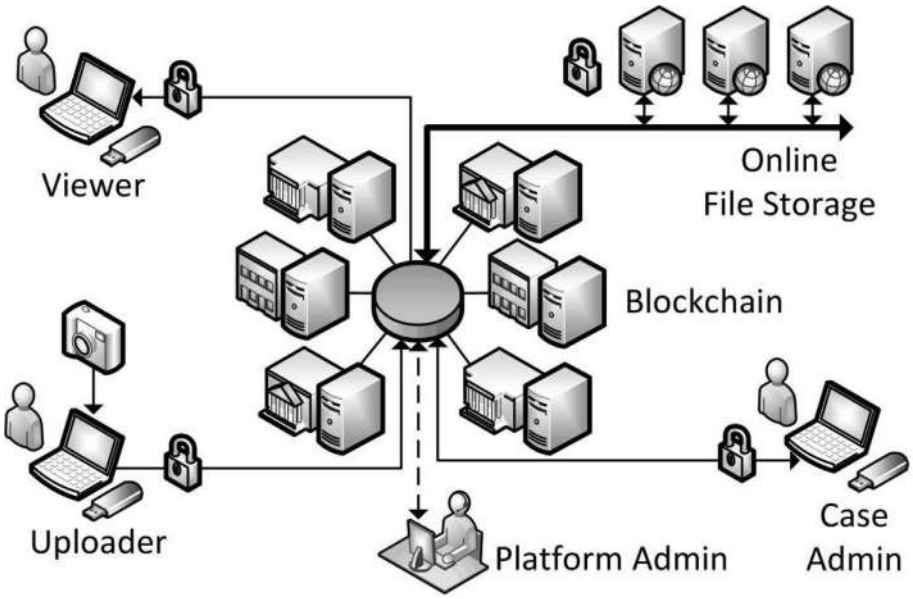

Fig. 2. Functional diagram of the platform.

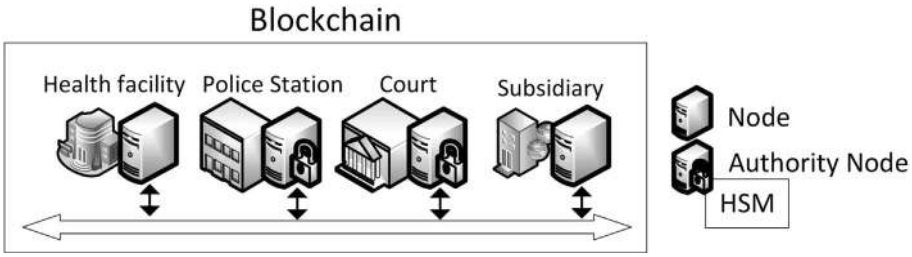

Fig. 3. Blockchain nodes types.

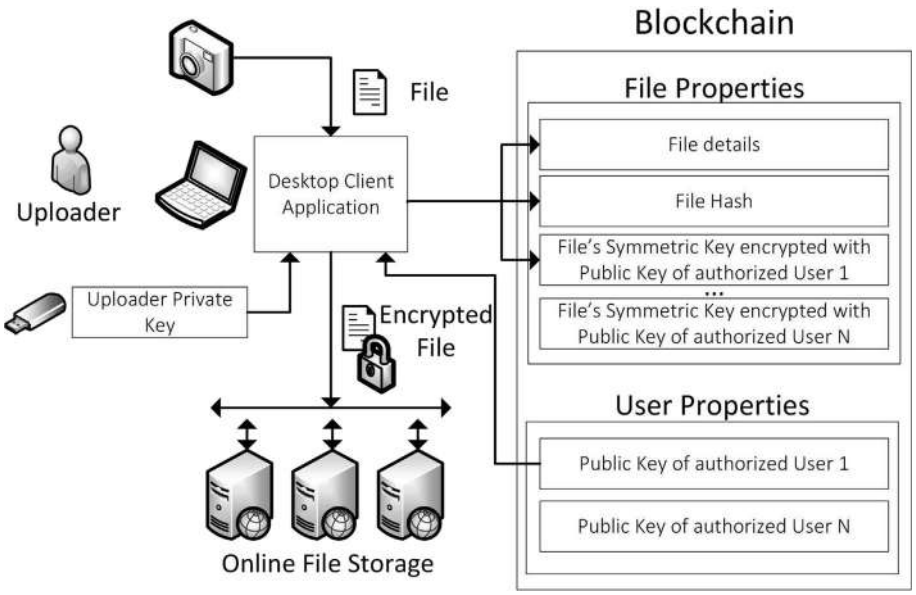

Fig. 4. Functional diagram of the file upload operation.

2.4.5. View right management

The Case Admin wants to add view rights to a user. An authority node retrieves the newly authorised user's public key, which is used to encrypt the file's symmetric key. Then, the encrypted key is added on the blockchain in the file's properties.

2.4.6. View right removal

The Case Admin wants to remove the view rights from a user. Since the user may still have the file's symmetric key, it is necessary to encrypt it with a new symmetric key.

An authority node retrieves the encrypted file, then decrypts it with its private key; then the file is encrypted again with a new symmetric key. The newly encrypted file is stored in the online storage.

Finally, the new symmetric key is encrypted with all the remaining authorised user's public keys.

The functional diagram of this operation is shown in Fig. 6.

2.4.7. User creation

The operation to create a new user is performed by Platform Admins and requires the recording of all user properties, as shown in Table 1, on the blockchain in association with a new identity.

The user's public key is retrieved from a generated RSA 2048 bits asymmetric key pair stored on a newly assigned USB device.

Then, the user is assigned rights based on the role on the platform.

2.4.8. Logs access

All platform operations are logged in the blockchain, and authorised users can access them at any time. Logs consist of operation type, performing user and timestamp.

2.4.9. Case/file deletion

Depending on local policies and legal framework, users with authorisation can request cases or files to be archived or permanently removed from both the blockchain and online file storage.

2.5. Desktop application

The system platform is accessed with a dedicated desktop application developed with the open-source framework Electron (2016) which graphical interface allows the user to perform all the operations.

The application interacts with the blockchain through dedicated restful web services, built using a REST API where HTTP methods are available to retrieve, add, modify or delete resources.

Also, the application interacts with the USB device to authenticate the user, and to perform encryption operations. Moreover, it allows essential features like zoom, crop, light adjustment, contrast enhancement, and it provides a dedicated template for report writing.

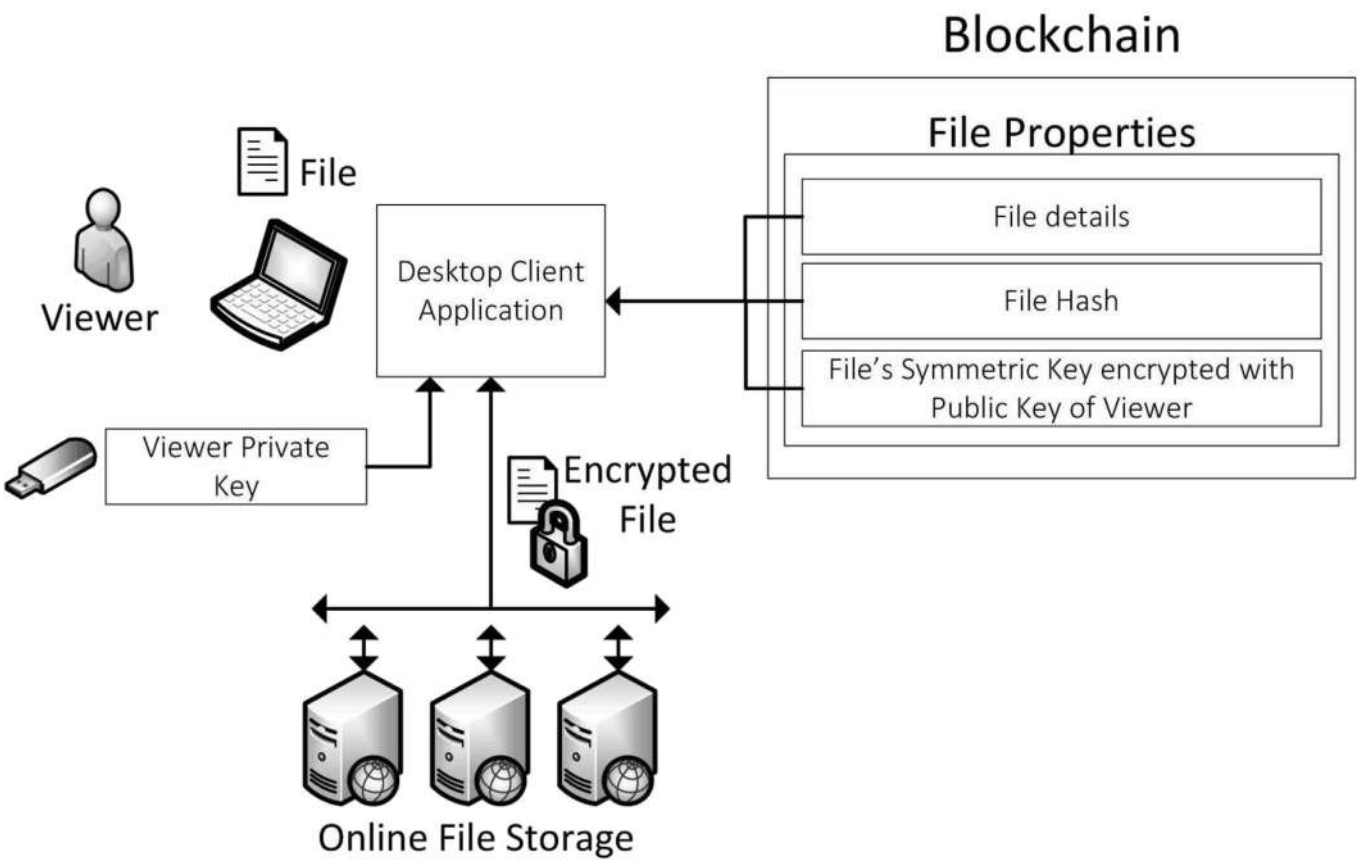

Fig. 5. Functional diagram of the view file operation.

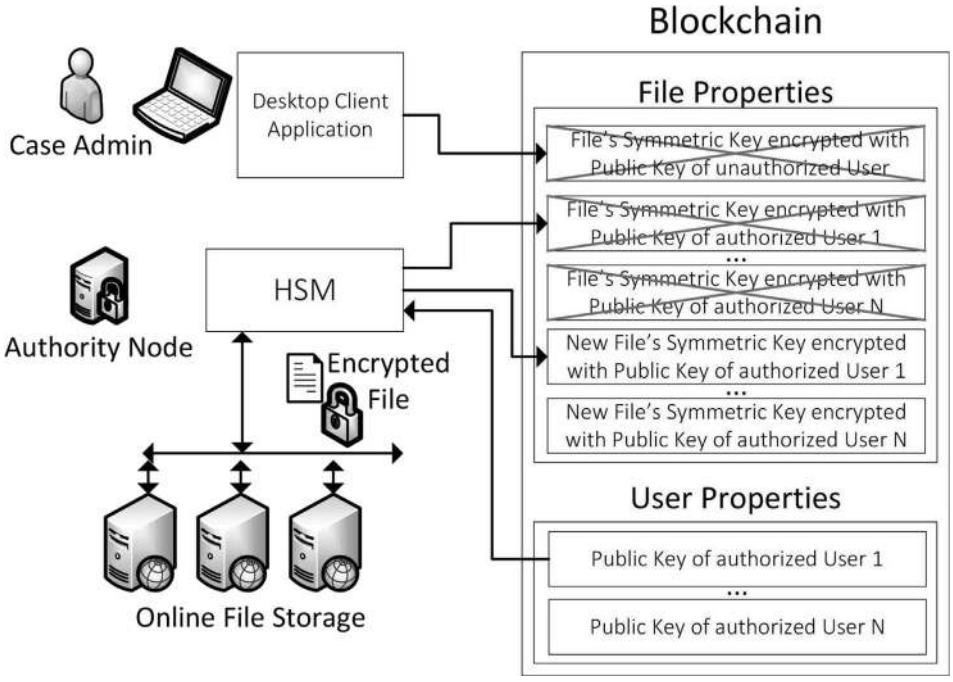

Fig. 6. Functional diagram of view rights removal operation.

2.6. Deployment considerations

The CC platform scope is to facilitate the work of the organisations involved in the custody of digital evidence (health facilities, courts, police stations and other subsidiaries).

About the deployment considerations of the proposed solution, dedicated hardware, software and human resources must be involved.

As an example, an independent dedicated team is in charge of the application development, maintenance and upgrade. Depending on the users' needs and feedback, updates of the platform are released periodically.

To deploy the platform, some of the requirements that each of the involved organisations must apply are the following:

- deployment of an uncompromised computer, with a secure operating system and the CC application installed, for each platform user. Alternatively, virtual solutions can be adopted to adapt to existing infrastructure.
- Set-up and maintenance of the online file storage by a specific organisation; several commercial solutions are available at a reasonable rate.
- Provision of at least one HSM module for each authority node; several commercial solutions are available at a moderate cost.
- Supply of a personal USB device for each user; several commercial solutions are available at a low cost.
- Employment of a Platform Admin, for each organisation, for the USB devices' management and general support provision to other users.

2.7. Prototype benchmarks

To verify all the key aspects of the intended design, a proof-of-principle prototype has been built and tested.

Performance has been evaluated for the two primary platform operations: File upload (2.4.3) and View file (2.4.4).

The machine used for the benchmarks has the following specifications:

- Cpu: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80 GHz.
- RAM: 16 GB.
- Hard Disk: SSD with a Transfer Speed of 540 MB/s.
- OS: Ubuntu 16.04
- Internet connection for the communication with the Online File Storage: 50 MB/s Download, 5 MB/s Upload.

Configuration of the Fabric blockchain network deployed: 2-Organizations, 2-Peers.

File upload:

For this test, we considered all the operations required by the CC application to upload a single file to the platform.

File specifics: JPG Image of 7 MB with a resolution of 6000 $\times$ 4000 pixels.

The steps involved in the operation with the relative times of execution are the following:

1. Hash of the file (SHA3, 256 bits): 3971.66 ms.
2. Symmetric encryption of the file (AES 256): 59.77 ms, the resulting encrypted file has a size of 14 MB.
3. Asymmetric encryption of the 256 bits key (RSA 2048 bits): 2.36 ms.
4. Upload of the encrypted file to the online file storage: 7023.18 ms.
5. Blockchain interaction: the transaction is approved by the blockchain in 2132.33 ms.

To summarise, the total time of the operation necessary to upload a 7 MB image to the platform is ~13 s. The upload of the encrypted file to the online file storage is the most time-consuming operation and can be improved with better connection speeds.

Also, the blockchain operation's performance was evaluated using Hyperledger Caliper with the following results:

- Send Rate: 121.8 Transactions Per Second;
- Average Latency: 0.16 s;
- Throughput: 120.5 Transactions Per Second.

View file:

For this test, we considered all the operations required by the CC application to retrieve a single file from the platform.

File specifics: JPG Image of 7 MB with a resolution of 6000 $\times$ 4000 pixels, the same considered in the previous test.

The steps involved in the operation with the relative times of execution are the following:

1. Retrieval of the file's private key, address and file info from the blockchain: 240.42 ms
2. Download of the encrypted file from the online file storage: 280.45 ms
3. Decryption of the private key (RSA 2048): 2.76 ms
4. Decryption of the file (AES 256): 164.91 ms
5. Hash calculation and validation: 4098.60 ms

To summarise, the total time of the operation necessary to download and view a 7 MB image from the platform is ~5 s.

Also, the blockchain operation's performance was evaluated using Hyperledger Caliper with the following results:

- Send Rate: 429.5 Transactions Per Second;
- Average Latency: 0.04 s;
- Throughput: 429.4 Transactions Per Second.

Considering the results of the benchmarks, the overhead introduced by the use of the platform to simple upload and download operations can be considered acceptable given the added security benefits.

3. Related work

There are several other related research works that have attempted to improve the security of digital evidence acquisition, storage, and access.

The work presented by Saleem and Popov in 2011 (Saleem et al., 2011) tackles the problem of secure identity verification by storing the private keys of the forensic examiners on smart cards, ensuring that their signing information is protected and not tampered with.

In 2017, Shah et al. (2017) kept the use of smart cards and presented a solution that employs a chain of rings keeping the necessary information to ensure that all the stored evidence's integrity is verified. The chain starts when the first ring is added by extracting the evidence; then, every time the evidence is handed over, a new ring is added to the chain.

In 2019, Lone and Mir (2019) introduced a solution that uses a private permissioned blockchain to store and share the information related to the chain of evidence, improving the integrity, transparency, authenticity, security, and auditability of the system.

Furthermore, since 2017, several commercial ventures have proposed to store and share electronic medical records among

different organisations within a network, using a distributed ledger and smart contracts. A private blockchain is used to store and share data, and a digital token is issued on the Ethereum public blockchain to transfer value among the participants of the network.

The solution proposed in this paper stems from the practical issues related to the digital forensic medical evidence acquisition, storage, and sharing given the relevant literature in the field of forensic computer science, legal medicine and jurisprudence. Among the strengths of the proposed approach is that it must be considered that a private permissioned blockchain like Hyperledger Fabric dynamically validates all the transactions sharing sensible data between all the nodes and permanently recording all the operations. Moreover, the PIN-protected USB device storing each user's private key in a tamper-resistant internal HSM constitutes a safer approach to identify the users and to sign all the transactions digitally. As a step further, we present a hybrid cryptography system that combines asymmetric and symmetric cryptography to maximise security.

4. Discussion

Numerous challenges characterise digital evidence storage and sharing (Office of the United Nations High Commissioner for Human Rights, 2004; World Health Organization Geneva, 2003; Faculty of Forensic and Legal Medicine PICS Working Group, 2017; The Royal College of Pathologists of Australasia, 2018; Anderson and Moore, 2018a; Anderson and Moore, 2018b; Anderson and Moore, 2018c; Robinson and Robinson, 2016b; Page et al., 2011). Such issues are not entirely addressed by current leading guidances (Faculty of Forensic and Legal Medicine PICS Working Group, 2017; The Royal College of Pathologists of Australasia, 2018; New South Wales Health, 2015), and less standardised aspects of electronic evidence management still constitute a weakness (Office of the United Nations High Commissioner for Human Rights, 2004; Faculty of Forensic and Legal Medicine PICS Working Group, 2017; The Royal College of Pathologists of Australasia, 2018; Witzke and Robinson, 2016; Robinson and Robinson, 2016a; Kelly and Regan, 2003; Scientific Working Group on Digital Evidence, 2017; New South Wales Health, 2015; Scientific Working Group Imaging Technology, 2012a; den Otter et al., 2013; Official Journal of the European Union, 2016a; Official Journal of the European Union, 2016b; Department of Health, 1996; Federal Trade Commission, 2013; Australian Government Fed, 2014; California Civil Code, 2018; Department of Justic, 2013). Additionally, the expectations of patients, decision-makers, and society at large (Robinson and Robinson, 2016a; Page et al., 2011; Scientific Working Group Imaging Technology, 2012b; Nagosky, 2005), as well as other variables (Faculty of Forensic and Legal Medicine PICS Working Group, 2017; Robinson and Robinson, 2016a), increase the insiders' sense of burden.

In our opinion, the actual need for efficiency, transparency, and reliability is met through the development of the presented hybrid platform that stores the encrypted digital evidence in a redundant online file storage and entrusts all file properties and security with a private implementation of the blockchain Hyperledger Fabric (Hyperledger Fabric, 2017).

Starting with a broad range of advantages and covering the limitations that the proposed solution offers to the involved parties, we present and discuss several aspects to consider, including reflections for further research.

Regarding the benefits, from the patients' perspective, the described blockchain-based permissioned system constitutes a disincentive for illegitimate attempts to access the files since access is validated by all peers, like health facilities and government infrastructure (Fig. 3), through a consensus algorithm. Moreover, this solution ensures privacy safeguarding (Office of the United Nations High Commissioner for Human Rights, 2004; World Health Organization Geneva, 2003; Official Journal of the European Union, 2016a; Official Journal of the European Union, 2016b; Department of Health, 1996; Federal Trade Commission, 2013; Australian Government Fed, 2014) as long as it avoids the input of patients personal data into the platform. In addition, when required by law (Official Journal of the European Union, 2016a; California Civil Code, 2018), individual rights like the right to erase personal data or withdraw consent for storing pictures can be exercised by authorised parties as described in paragraphs 2.4.6. and 2.4.9.

From the health professionals' standpoint, the proposed solution transfers the burden of correct storage and evidence handling (Office of the United Nations High Commissioner for Human Rights, 2004; World Health Organization Geneva, 2003; Faculty of Forensic and Legal Medicine PICS Working Group, 2017; The Royal College of Pathologists of Australasia, 2018; Witzke and Robinson, 2016; Robinson and Robinson, 2016a; Anderson and Moore, 2018b; Anderson and Moore, 2018c; New South Wales Health, 2015; den Otter et al., 2013; Department of Justic, 2013) from the professional, or the institution, to the CC platform; the files are stored and encrypted within its systems, where access is granted only to authorised users. Additionally, the system's authentication method reduces the risk of username and password oversight or theft (Faculty of Forensic and Legal Medicine PICS Working Group, 2017) because a USB device and PIN procedure is utilised as described in paragraphs 2.1 and 2.4.1 (Fig. 1). Further, information sharing becomes safer and more transparent for peer review and second-opinion purposes through the use of a single blockchain-based platform where all the actions performed are permanently recorded, as shown in Table 1. Notably, the platform promotes independent judgment among authorised reviewers (Office of the United Nations High Commissioner for Human Rights, 2004; World Health Organization Geneva, 2003; Faculty of Forensic and Legal Medicine PICS Working Group, 2017; The Royal College of Pathologists of Australasia, 2018; Office of Criminal Justice Planning, 2001; New South Wales Health, 2015; Department of Justic, 2013), who are able to access the 'best evidence' (Faculty of Forensic and Legal Medicine PICS Working Group, 2017; Anderson and Moore, 2018a), eventually adding their reports to the system. Again, as described in chapter 2.1, the developed hybrid cryptographic system (Hofheinz and Kiltz, 2007) combines symmetric and asymmetric encryption (Department of Commer, 2001; Rivest et al., 1978), allowing secured access from sites outside the workplace, such as home or the forensic site.

Moreover, health professionals who work in hostile conditions can upload files in a lawful and censorship-resistant network for future consultation. Further, the digital rights management system described in chapters 2.2, 2.4.5 and 2.4.6 allows immediate access to the file by the authorised users; consequently, paperwork decreases, and authorisations can be managed more efficiently than in the case of a traditional paper based system. An additional advantage is the recovery of lost access caused by a misplaced USB device or lost credentials, thanks to the recovery procedures performed by the Platform Admin as explained in chapter 2.2. Moreover, the online file storage solution with data redundancy avoids the files being stored on one single hardware that could be damaged or confiscated at any time (Figs. 2 and 4).

Pertaining to the forensic challenges, the proposed solution conforms to the accepted standards and the applicable rules of evidence, since it meets the current criteria for the correct acquisition, storage and sharing of digital evidence (Scientific Working Group Imaging Technology, 2012a; Scientific Working Group on Digital Evidence, 2018; Kissel et al., 2014). The usage of

blockchain technologies in conjunction with cryptography guarantees the chain of evidence allowing traceable access to files.

Additionally, the secure, shared storage of the files hash further reduces the risk of tampering. Blockchain technologies record all attempts to access data in an immutable register (Hyperledger Fabric, 2017), enabling the detection of illicit activities.

For research and teaching purposes, files can be classified and searched adding keywords and descriptions to their metadata that are stored automatically.

Despite the advantages, open points still remain, and they are outlined and considered here. First, the computer used to upload the files to the platform must be uncompromised; otherwise, unauthorised access to the files could happen, and a remote access trojan installed on the operator's computer could take screenshots or videos to share without authorisation. To avoid such illegitimate data leakage, users must follow security recommendations (Scientific Working Group on Digital Evidence, 2018; Home Office Scientific Development Branch, 2007) using a security-oriented operating system for both the uploading and the viewing of the files. However, authorised users are not prevented from taking a picture or screenshot of the displayed evidence and spread it.

Furthermore, safe operating procedures must be put in place to replace Case Admins as well as Platform Admins, who hold a crucial position within the entire system.

Concerning the pairing between the client's identity and the Case ID, the responsibility remains on the uploader, as a different approach could compromise confidentiality. For instance, inserting the patient's name in the file's properties means that such data would remain unencrypted. Also, it must be considered that every image depicting the client's personal data, such as ID shots (Faculty of Forensic and Legal Medicine PICS Working Group, 2017) or pictures of the consent form, constitutes a risk for privacy safeguarding.

Another limitation of general order is that all patient data is part of their medical record; but their presence on a different software could undermine the efficacy of the entire system.

Unsurprisingly, the platform must be adapted to the different legal frameworks of the various countries, and the rapid evolution of innovative technologies like blockchain must be taken into account. Again, further developments of quantum technologies may require the update of cryptography standards. The cited limitations may compromise confidentiality and data protection, allowing unauthorised usage of data.

In this paper, we propose a blockchain-based solution for the custody of digital files in forensic medicine as a theoretical model with the development of a proof-of-principle prototype. The next step is the development of a pilot prototype, which will require further testing and in-field application, and may involve some adaptations of the current solution.

5. Conclusions

A solution for the custody and sharing of digital files in forensic medicine without relying on a centralised network is proposed here. At first, we focused on the major issues under the patient's perspective, the professionals' views and the legal requirements, analysing the current, predominant guidances. However, with reference to confidentiality safeguarding, health professionals responsibilities, and computer forensics issues, they all appear weak at some point. As a solution, we propose a hybrid platform using a consensus mechanism to record a transparent history of access and to avoid data modification by unauthorised users. The network is safe and accessible through a dedicated application. All information is agreed and shared between the blockchain nodes to avoid single points of failure, and secure access to files is assured by combining cryptography and the blockchain consensus mechanism. Despite some limitations, an implementable solution for the custody of digital files in forensic medicine has been identified.

Further possible improvements consist of creating and storing copies of digital files containing sensitive or private data at different resolutions to distribute low definition versions to private users, while only health practitioners and the court are enabled to access the original file. Besides, it could be implemented a specifically developed programmable camera with a dedicated firmware, that encrypts the file automatically as soon as shot.

Further applications include all the circumstances in which the file format of a document, a picture, or a video has legal implications, like consent forms, advanced healthcare directives, living wills, or images shot by health professionals while on duty.

Declarations of competing interestCOI

None.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

CRediT authorship contribution statement

Monia Lusetti: Conceptualization, Resources, Writing - original draft, Visualization, Supervision, Project administration. **Luca Salsi:** Conceptualization, Software, Investigation, Resources, Writing - original draft. **Andrea Dallatana:** Conceptualization, Methodology, Software, Validation, Investigation, Resources, Data curation, Visualization, Supervision.

Acknowledgements

We are immensely grateful to Dr Maria Nittis, Head of Department Forensic Medical Unit WSLHD/NBMLHD, and Dr Will Anderson, Lead Forensic Medical Examiner Hampshire and BTP, for their comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of these esteemed persons.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.fsidi.2020.301017.

References

Dr Will Anderson, Søren Moore. Oral Communication at 'Patient Focused! Training Clinicians How to Photograph Patients Professionally, Ethically, and Legally' Course 2018; Types of camera/How a Digital Camera Works, Day 1, Tuesday 06th March 2018.

Anderson, Dr Will, Moore, Søren, 2018b. Oral Communication at 'Patient Focused! Training Clinicians How to Photograph Patients Professionally, Ethically, and Legally' Course. Storage of images, Day 3, Thursday 08th March 2018.

Anderson, Dr Will, Moore, Søren, 2018c. Oral Communication at 'Patient Focused! Training Clinicians How to Photograph Patients Professionally, Ethically, and Legally' Course. Submission of images, Day 3, Thursday 08th March 2018.

Androulaki, E., et al., 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains. https://arxiv.org/pdf/1801.10228.pdf. (Accessed 26 May 2019).

Australian government federal register of legislation, privacy act 1988. https://www.legislation.gov.au/Details/C2014C00076, 2014—. (Accessed 5 May 2019).

Buterin, V., 2013. A next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper. (Accessed 26 May 2019).

California Civil Code, 2018. Assembly bill n. 375. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. (Accessed 5 May 2019).

Cerrudo, C., Fayo, E.M., 2007. Hacking databases for owning your data. https://www.

blackhat.com/presentations/bh-europe-07/Cerrudo/Whitepaper/bh-eu-07-cerrudo-WP-up.pdf. (Accessed 26 May 2019).
den Otter, J.J., Smit, Y., dela Cruz, L.B., Özkalipci, Ö., Resmiye, O., 2013. Documentation of torture and cruel, inhuman or degrading treatment of children: a review of existing guidelines and tools. Forensic Sci. Int. 224, 27–32. https://doi:10.1016/j.forsciint.2012.11.003.
U.S. Department of commerce national Institute of standards and technology, announcing the advanced encryption standard (AES). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf, 2001–. (Accessed 26 May 2019).
U.S. Department of health and human services, health insurance portability and accountability act of 1996 (HIPAA). https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996, 1996–. (Accessed 5 May 2019).
U.S. Department of justice Office on violence against women, A national protocol for sexual assault medical forensic examinations. https://cdn.ymaws.com/www.safeta.org/resource/resmgr/Protocol_documents/SAFE_PROTOCOL_2012-508.pdf, 2013–. (Accessed 26 May 2019).
Electron, 2016. An open source library developed by GitHub for building cross-platform desktop applications. https://www.electronjs.org. (Accessed 26 May 2019).
Faculty of Forensic and Legal Medicine PICS Working Group, 2017. Guidelines on photography. https://fflm.ac.uk/wp-content/uploads/2018/01/PICS-Working-Group-Guidelines-on-Photography-Dr-Will-Anderson-May-2017.pdf. (Accessed 26 May 2019).
Federal Trade Commission, 2013. Children's online privacy protection rule. https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5. (Accessed 26 May 2019).
Hofheinz, D., Kiltz, E., 2007. Secure hybrid encryption from weakened key encapsulation. https://link.springer.com/content/pdf/10.1007%2F978-3-540-74143-5_31.pdf. (Accessed 26 May 2019).
Home Office Scientific Development Branch, 2007. Digital imaging procedure. Version 2.1. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/378451/DIP_2.1_16-Apr-08_v2.3__Web_2835.pdf. (Accessed 1 May 2019).
Hyperledger Fabric, 2017. A blockchain platform for the enterprise. https://hyperledger-fabric.readthedocs.io/. (Accessed 26 May 2019).
Iansiti, M., Karim, R.L., 2017. The truth about blockchain. Harv. Bus. Rev. 95, 118–127.
Kelly, L., Regan, L., 2003. Good Practice in Medical Responses to Recently Reported Rape, Especially Forensic Examinations. Child and Woman Abuse Studies Unit, London.
Kissel, R., Regenscheid, A., Scholl, M., Stine, K., 2014. Guidelines for media sanitization. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf. (Accessed 26 May 2019).
Lone, A.H., Mir, R.N., 2019. Forensic-chain: blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digit. Invest. 28, 44–55.
Nagosky, D.P., 2005. The admissibility of digital photographs in criminal cases. https://www.crime-scene-investigator.net/admissibilityofdigitalphotographs-leb.pdf. (Accessed 26 May 2019).
Nakamoto, S., 2009. Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. (Accessed 26 May 2019).
National Institute of Standards and Technology, 2015. SHA-3 standard: permutation-based hash and extendable-output functions. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf. (Accessed 26 May 2019).
Netherlands Forensic Institute Ministry of Justice and Security, 2018. Technical supplement: forensic use of hash values and associated hash algorithms. https://www.forensischinstituut.nl/binaries/nfi/documenten/publicaties/2018/02/13/vakbijlage-forensisch-gebruik-van-bestandskenmerken-en-bijbehorende-hashalgoritmen/Supplement-hashes-v2018_01a_English.pdf. (Accessed 26 May 2019).
New South Wales Health, 2015. Photo and video imaging in cases of suspected child sexual abuse, physical abuse and neglect. https://www1.health.nsw.gov.au/pds/ActivePDSDocuments/PD2015_047.pdf. (Accessed 26 May 2019).
Office of Criminal Justice Planning, 2001. California medical protocol for examination of sexual assault and child sexual abuse victims. https://www.caloes.ca.gov/grantsmanagementsite/documents/2-923%20to%202-950%20protocol.pdf. (Accessed 28 April 2019).
Office of the United Nations High Commissioner for Human Rights, 2004. Istanbul protocol. Manual on the effective investigation and documentation of torture and other cruel, inhuman or degrading treatment or punishment. https://www.ohchr.org/Documents/Publications/training8Rev1en.pdf. (Accessed 28 April 2019).
Official Journal of the European Union, 2016a. Regulation (EU) 2016/679 of the European parliament and of the council. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN. (Accessed 5 May 2019).
Official Journal of the European Union, 2016b. Directive (EU) 2016/680 of the European parliament and of the council. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&qid=1557062454536&from=EN. (Accessed 5 May 2019).
Page, J., Fernie, C.G.M., 2011. Fundamental principles. In: Stark, M.M. (Ed.), Clinical Forensic Medicine: A Physician's Guide. Springer Science+Business Media, New York, pp. 45–69.
Rivest, R.L., Shamir, A., Adleman, L., 1978. A method for obtaining digital signatures and public-key cryptosystems. http://people.csail.mit.edu/rivest/Rsapaper.pdf. (Accessed 26 May 2019).
Robinson, E.M., 2016a. Legal issues related to photographs and digital images. In: Robinson, E.M. (Ed.), Crime Scene Photography. Elsevier Inc., London, pp. 695–735.
Robinson, E.M., 2016b. Crime scene photography. In: Robinson, E.M. (Ed.), Crime Scene Photography. Elsevier Inc., London, pp. 61–123.
Saleem, S., Popov, O., 2011. Protecting digital evidence integrity by using smart cards. In: Baggili, I. (Ed.), Digital Forensics and Cyber Crime. ICDF2C 2010. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer, Berlin, Heidelberg, pp. 110–119.
Scientific Working Group Imaging Technology, 2012a. Best practices for maintaining the integrity of digital images and digital video. https://www.swgit.org/pdf/Section%2013%20Best%20Practices%20for%20Maintaining%20the%20Integrity%20of%20Digital%20Images%20and%20Digital%20Video?docID=54. (Accessed 26 May 2019).
Scientific Working Group Imaging Technology, 2012b. Digital imaging technology issues for the courts. https://www.swgit.org/pdf/Section%2017%20Digital%20Imaging%20Technology%20Issues%20for%20the%20Courts?docID=56. (Accessed 26 May 2019).
Scientific Working Group on Digital Evidence, 2017. SWGDE best practices for maintaining the integrity of imagery. https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Maintaining%20the%20Integrity%20of%20Imagery. (Accessed 26 May 2019).
Scientific Working Group on Digital Evidence, 2018. Best practices for computer forensic examination. https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensic%20Examination. (Accessed 26 May 2019).
Shah, M.S.M.B., Saleem, S., Zulqarnain, R., 2017. Protecting digital evidence integrity and preserving chain of custody. JDFSL 12, 122–130.
The Royal College of Pathologists of Australasia, 2018. Photography for clinical forensic medicine. https://www.rcpa.edu.au/getattachment/bda8bae6-1df5-449e-85a6-073eeb8e2fce/Photography-for-Clinical-Forensic-Medicine.aspx. (Accessed 26 May 2019).
Witzke, D., 2016. Digital imaging technologies. In: Robinson, E.M. (Ed.), Crime Scene Photography. Elsevier Inc., London, pp. 586–625.
World Health Organization Geneva, 2003. Guidelines for medico-legal care for victims of sexual violence. https://www.who.int/violence_injury_prevention/publications/violence/med_leg_guidelines/en/. (Accessed 28 April 2019).