Digital evidence e tutele processuali: potenzialità della tecnologia blockchain

Brighi , R.; Ferrari, V.

DOI
10.1415/91542
Publication date
2018
Document Version
Final published version
Published in
Ragion pratica

Raffaella Brighi, Valeria Ferrari

Digital evidence e tutele processuali: potenzialita768; della tecnologia blockchain

(doi: 10.1415/91542)

Ragion pratica (ISSN 1720-2396)
Fascicolo 2, dicembre 2018

Raffaella Brighi, Valeria Ferrari

Digital evidence e tutele processuali: potenzialità della tecnologia *blockchain*

Digital evidence and procedural protections: potential of blockchain technology

Datafication of society and proliferation of cybercrime determine the unique importance of digital evidence in today's criminal proceedings. The integrity of data is crucial for their usability as evidence before the court; the traceability and *ex-post* verifiability of their lifecycle is necessary for the cross-examination on their validity as evidence. In digital forensics, the term *chain of custody* refers to a set of tools and practices aimed at guaranteeing the proper treatment of digital evidence and the accurate documentation of all the activities concerning its identification, collection, storage and analysis. The need to verify the correctness of digital evidence's treatment is made more urgent by the diffusion of highly intrusive detection instruments such as trojan horses, and by the increasingly transitional dimension of digital investigations. Therefore, the development of proper recording tools is crucial. The present work discusses how blockchain technologies could be deployed to maintain a transparent and tamperproof register of forensics activities shared among all private and public actors which participate to the digital evidence lifecycle. This instrument would facilitate national and international cooperation in digital investigations, guaranteeing both the integrity of data and the transparency of meta-information concerning their treatment. Ultimately, this would allow to better protect defendants' rights in relation to digital evidence.

Keyword: Digital evidence – defendants' rights – blockchain – chain of custody – cooperation.

1. Il vaglio della prova digitale: imprescindibilità degli standard tecnico-normativi

Nell'ottobre 2015 conquista la copertina dell'«Economist» un articolo dal titolo *The trust machine*. L'oggetto del testo è una tecnologia, quella sottostante il *bit-*

Raffaella Brighi, CIRSFID, Università di Bologna, Via Galliera 3, 40121 Bologna. Email: raffaella.brighi@unibo.it

Valeria Ferrari, IViR, University of Amsterdam, Nieuwe Achtergracht 166, 1018 WV Amsterdam. Email: v.ferrari@uva.nl

Il saggio è frutto di un lavoro di ricerca congiunto che impegna entrambe le autrici. Ai fini di questo studio, R. Brighi si è occupata dei §§. 1, 4; V. Ferrari è autrice dei §§ 2, 3, 5.

coin, che «permette a persone che non hanno particolare fiducia l'una nell'altra di collaborare tra di esse, senza dover ricorrere ad un'autorità centrale e neutrale»[1]. Questa tecnologia è la c.d. *blockchain*: un registro pubblico condiviso da una rete distribuita di computer in cui le informazioni — validate dall'intero network — sono impresse irreversibilmente senza possibilità di modifica da parte dei singoli nodi, ma in ogni momento verificabili dai soggetti legittimati[2]. Fondandosi sulla crittografia forte[3], la *blockchain* mantiene le informazioni segrete e, al tempo stesso, presuppone un consenso distribuito sulla loro validità e integrità. Grazie ad una singolare capacità di combinare trasparenza, sicurezza e riservatezza, essa consente un controllo individuale su informazioni e dati, promettendo di trasformare non solo il modo in cui le persone scambiano valore *online*, ma più in generale il ruolo delle istituzioni e dei tradizionali intermediari.

Allo stato attuale del dibattito sulle possibili implementazioni e implicazioni, sembrano particolarmente vantaggiose le proposte di utilizzare la *blockchain* per assicurare integrità, riservatezza e autenticità dei dati informatici, soprattutto in contesti in cui diversi attori vantino, in relazione ad essi, interessi contrapposti[4].

La capacità della *blockchain* di rendere visibile e verificabile ogni evento o azione fin dall'origine senza la necessità di un'autorità *trusted* centralizzata, suggerisce di indagare se e come questa «macchina della fiducia» possa essere efficacemente sfruttata nell'ambito della *digital forensics*[5] per garantire i requisiti di integrità e autenticità della prova informatica, la verificabilità delle procedure poste in essere e la riproducibilità delle operazioni compiute sui reperti (*accountability*), a salvaguardia dei diritti di tutte le parti coinvolte nel procedimento giudiziario[6].

Con l'avvento della società dell'informazione e il proliferare dei *digital device* che sempre di più mediano l'interazione tra persone — e tra queste e gli oggetti che le circondano — la prova digitale ha assunto un ruolo chiave nella ricostruzione della realtà processuale a supporto del percorso decisionale

[1] *The trust machine: The technology behind bitcoin could transform how the economy works*, «The Economist», 31 ottobre 2015.

[2] Si rimanda al §3 per la descrizione della tecnologia *blockchain*.

[3] La crittografia si dice «forte» o «debole» a seconda del tempo e delle risorse computazionali necessarie per ricavare il messaggio originale da quello cifrato. La "forza" di un sistema crittografico dipende da due parametri: l'algoritmo crittografico e la lunghezza della chiave (espressa in numero di bit).

[4] Si veda, ad esempio, il progetto MyHealthMyData (MHMD-H2020-ICT-2016), relativo alla gestione dei dati in ambito sanitario; o il progetto di Walmart e IBM (2018) per la tracciabilità della catena produttiva nel settore alimentare.

[5] Per un inquadramento dei principi e metodi della disciplina si rimanda a C. Maioli, *Introduzione all'informatica forense*, in P. Pozzi (a cura di), *La sicurezza preventiva dell'informazione e della comunicazione*, FrancoAngeli, Milano, 2004.

[6] Sono questi i requisiti sottolineati dalla Convenzione sul Crimine informatico del Consiglio D'Europa (CETS n. 185) del 2001.

del giudice penale e, in maniera crescente, in tutti gli altri ambiti processuali. A ciò, tuttavia, non si è affiancata una sistematizzazione tecnico-giuridica delle procedure di trattamento dei dati digitali a uso processuale tale da smorzarne le fragilità intrinseche.

La struttura peculiare del dato informatico ingenera nella prassi processuale l'illusione dell'oggettività della rappresentazione digitale e del significato ad essa attribuibile[7] e quindi una fiducia acritica nell'idoneità del reperto a supportare il ragionamento logico-probatorio del giudice[8]. Al contrario, volatilità dei dati, immaterialità dei bit e possibilità di occulta alterazione delle tracce digitali impongono particolari cautele sia procedurali che valutative. Riproponendo questioni tipiche della prova scientifica, il frequente ricorso alla *digitale evidence* richiede di definire anche per l'informatica forense una cornice epistemologica di riferimento per il *contesto* processuale[9].

Per determinare il valore probatorio di una prova scientifica è chiesta al giudice, *peritus peritorum*, la capacità di verificare sia la validità scientifica del metodo impiegato dall'esperto sia l'applicazione corretta del metodo nel caso concreto[10]. Di qui, emerge come il principio dell'autonomia del giudice nella valutazione e interpretazione della prova scientifica debba essere accompagnato, da un lato, da specifiche cornici normative che disciplinino precisi criteri di valutazione del sapere scientifico e regole attinenti l'ammissibilità, l'assunzione e l'utilizzo della prova scientifica; dall'altro, preceduto dalla predisposizione di standard tecnici e protocolli operativi che valgano per la singola area di ricerca e a cui fare riferimento nella valutazione[11].

Tali necessità assumono un carattere pregnante nell'ambito dell'informatica forense e si riflettono nell'armonizzazione – a livello non solo Europeo, ma

[7] Sui metodi formali con cui nella scienza dell'informazione i dati binari si trasformano in informazioni e, successivamente, le informazioni in conoscenza sia consentito il rimando a R. Brighi, *Il ruolo dei dati informatici nella costruzione della realtà*, Aracne, Roma, 2016.
[8] F. Cajani, *Il vaglio dibattimentale della digital evidence*, «Archivio Penale» LXV(3), 2013, 837-852.
[9] Così S. Jasanoff, *La scienza davanti ai giudici*, Giuffrè, Milano, 2001.
[10] M. Taruffo, *La prova scientifca. Cenni generali*, «Ragion pratica», 2, 2016, 335-354. È, in particolare, a partire dalla famosa sentenza *Daubert* del 1993 che si riconosce la necessità di lasciare al giudice il primato decisionale anche di fronte a evidenze provenienti da fonti esperte. Cfr. Daubert v. Merrel Dow Pharmaceuticals, 509 U.S. 579 (1993). La bibliografia sulla sentenza è vastissima. Per tutti si veda O. Dominioni, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, 2015. Va rilevato che il modello derivato da tale sentenza non convince dal momento che finisce con l'attribuire al giudice il compito di stabilire quale sia la scienza valida fino, in qualche modo, a contribuire a definire il sapere scientifico. Cfr. C.M. Tallacchini, *Scienza e diritto. Verso una nuova disciplina*, in S. Jasanoff, *La scienza davanti ai giudici*, cit.
[11] Come sottolineato da Susan Haack, una corretta delineazione del rapporto tra scienza e diritto deve puntare sul connubio tra enunciati teorici ed enunciati osservativi, ed impone di valutare la fase anteriore al processo per evitare l'ingresso in giudizio di risultati scientifici ma di dubbia efficacia probatoria. S. Haack, *Legalizzare l'epistemologia*, Egea, 2015.

anche internazionale – della normativa di contrasto al crimine informatico[12], nel rafforzamento della collaborazione investigativa[13], nonché nella predisposizione di procedure operative e standard tecnici funzionali ad una corretta espletazione degli accertamenti informatici e della loro documentazione[14]. L'apporto dell'informatica forense a tutte le fasi del processo sembra oggi in via di consolidamento[15], tuttavia in un campo così delicato come quello dell'indagine penale non è facile trovare soluzioni di equilibrio che consentano una collaborazione efficace tra le forze dell'ordine e preservino, allo stesso tempo, prerogative e istanze della sovranità statale.

Il presente lavoro esplora come sfruttare le proprietà tecniche della *blockchain* per dare risposta alle esigenze di integrità, trasparenza e immutabilità della *digital evidence* in un'ottica di standardizzazione. In particolare, si intende proporre una implementazione su tecnologia *blockchain* del paradigma della catena di custodia – strumento importante per la garanzia del contradditorio nella formazione della prova – con l'intento di definire un registro condiviso tra gli attori (processuali e privati) che interagiscono a vario titolo con la prova digitale, agevolando la cooperazione e garantendo sia l'integrità del dato sia la trasparenza e la verificabilità delle procedure.

2. La catena di custodia della prova digitale

La possibilità di ricorso al dato digitale come fonte di prova inconfutabile è spesso inficiata dai caratteri di ambiguità e fragilità che sono attribuibili sia al reperto in sé, sia alle varie attività volte a portare quest'ultimo al vaglio del giudice. Abbiamo a che fare, infatti, con elementi informativi che, prescindendo dal supporto fisico che li contiene, possono subire alterazioni o essere eliminati con estrema facilità, anche per semplici sviste o in conseguenza di processi automatici. Non solo il dato è per sua natura estremamente volatile, ma risulta anche difficile, persino

[12] Si veda in particolare la Convenzione di Budapest del Consiglio di Europa del 23 novembre 2001, ratificata in Italia con la Legge n. 48 del 18 marzo 2008, principale strumento normativo internazionale vincolante riguardante il crimine informatico e le relative indagini.

[13] L'obiettivo della cooperazione internazionale nel contrasto al crimine informatico è sottolineato da vari strumenti legislativi comunitari tra cui la citata Convenzione di Budapest e la Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio (Direttiva NIS) e si riflette nella creazione di enti di coordinamento sovranazionali come Europol, Eurojust ed ENISA, posti a guida dell'operato degli Stati Membri dell'UE.

[14] Rilevano, in modo particolare, gli standard ISO/IEC 27037:2012 (e successivi) che delineano i modelli operativi dell'informatica forense.

[15] S. Black, N. Daied, *Time to think differently: catalysing a paradigm shift in forensic science*, Philosophical Transactions Royal Society London, Biol Sci., 2015. Sul punto anche R. Brighi, C. Maioli, *Un cambio di paradigma nelle scienze forensi. Dall'armonizzazione tecnico-giuridica a una nuova cornice epistemologia*, «Informatica e diritto», XXIV (1-2), 2015, 217-234.

ad un occhio esperto, identificare eventuali manipolazioni o deterioramenti dello stesso. Pertanto, quando un reperto digitale viene addotto in processo come elemento di prova, fondamentale sarà la verifica della sua integrità e genuinità, e, quindi, del rigore del suo trattamento dal momento della sua identificazione a quello della sua introduzione in dibattimento.

Ciò è riconosciuto e ribadito dal legislatore nel dettato degli artt. 244, 247 e 354 c.p.p., come modificati dalla L. 18 marzo 2008, n. 48[16], i quali disciplinano i casi di ispezione, perquisizione e accertamento urgente aventi ad oggetto «dati», «informazioni», «programmi informatici» o «sistemi informatici o telematici». Nonostante l'apprezzabile intento sottostante queste disposizioni, tuttavia, la ratifica della convenzione di Budapest lascia aperti importanti quesiti: (1) da un lato, quello affrontato a più riprese da giurisprudenza e dottrina relativo alle conseguenze della mancata adozione delle misure prescritte dalle norme in esame; (2) dall'altro, l'assenza di indicazioni di standard operativi e requisiti metodologici su cui poter misurare l'adeguatezza di un elemento di prova digitale.

Per quanto concerne il primo quesito, gli interpreti sono mossi dalla preoccupazione di evitare che al vaglio del giudice siano ammesse prove che, data la mancata adozione delle appropriate cautele in fase di acquisizione e custodia, non siano idonee all'accertamento del fatto. Tuttavia, si è osservato che, anche a voler ammettere un intervento del giudice in sede di ammissione della prova, altro non si avrebbe che una valutazione – del tutto simile all'istruttoria dibattimentale – delle modalità di acquisizione della *digital evidence*, la quale si presenta, comunque e inevitabilmente, come prova precostituita rispetto al contraddittorio. Pertanto, l'orientamento maggioritario è pacifico nell'ammettere che, nei (frequenti) casi in cui l'instaurazione del contraddittorio per la formazione della prova digitale risulti impraticabile, l'esercizio del diritto di difesa dell'imputato viene rimandato ad un contraddittorio dibattimentale «postumo», di mera critica «sulla prova» già formata in sede di accertamenti istruttori[17].

In quest'ottica, l'accurata documentazione delle attività degli investigatori forensi risulta elemento imprescindibile ai fini dell'esercizio del diritto di difesa. Infatti, per poter contestare le possibili irregolarità di metodo e quindi l'affidabilità del reperto addotto a prova del fatto, la difesa deve essere messa in grado di conoscere e scrutinare nel dettaglio le varie attività compiute dalla polizia giudiziaria o dai consulenti tecnici che hanno portato al risultato probatorio in esame.

[16] Gli articoli in esame, che costituiscono un riferimento fondamentale circa l'ammissibilità della prova digitale in processo, impongono l'utilizzo di misure idonee ad «assicurare la conservazione dei dati originali e ad impedirne l'alterazione» (artt. 244 e 247), nonché, nel caso di accertamento urgente, la «immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità».
[17] P. Tonini, *Il documento informatico: problematiche civilistiche e penalistiche a confronto,* «Corr. Giur.», 2012, 3, 432-439.

A tale necessità di documentazione le migliori prassi danno risposta con l'istituto di matrice nordamericana, già utilizzato per particolari tipi di beni fisici, della «catena di custodia» (*chain of custody*). Con tale termine si allude, nel nostro ordinamento, ad un complesso di norme processuali e regole tecniche che – al fine ultimo di garantire genuinità e integrità dei reperti e ripercorribiltà delle operazioni – impongono la meticolosa documentazione di ogni passaggio compiuto dai dati digitali dal momento dell'acquisizione al loro ingresso in processo[18].

Da qui il secondo quesito: sancendo l'obbligo di adottare adeguate cautele volte alla protezione del dato e della sua genuinità, le norme mutuate dalla Convenzione di Budapest lasciano all'operatore la scelta delle specifiche procedure e degli strumenti tecnologici necessari. D'altronde, una valutazione aprioristica del legislatore avrebbe rischiato di irrigidire la disciplina in modo inappropriato. A ragione, tuttavia, alcuni critici hanno sottolineato come la mancata indicazione di metodo rischi di vanificare la dichiarazione di scopo. Seppur in vigenza di *best practice* internazionalmente riconosciute, infatti, trascuratezza, imperizia e metodologie inappropriate nel mantenimento della catena di custodia minacciano di veicolare all'attenzione del giudice reperti digitali erroneamente identificati, acquisiti o custoditi, e impediscono l'esperimento delle opportune perizie e valutazioni[19].

La definizione e l'adozione di standard metodologici e strumenti tecnici idonei a garantire certezza e trasparenza alle procedure dell'informatica forense è pertanto funzionale a un corretto espletamento dell'attività valutativa del giudice e all'esercizio del diritto di difesa sull'elemento di prova informatico. Inoltre, la crescente complessità dei servizi del settore ICT[20] e l'internazionalizzazione delle indagini ad oggetto digitale[21] aumentano ulteriormente il rischio di violazioni, intensificando l'esigenza di armonizzazione rigorosa tracciabilità delle procedure.

[18] Sul tema cfr. L. Bartoli, C. Maioli, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, «Informatica e diritto», XXIV (1-2), 2015, 139-151.

[19] Appartengono a un passato recente casi di cattive pratiche, quali la richiesta di ammissibilità come prova di *log* di *server* inviati via fax dal *provider*, stampe di *home page* o di e-mail, supporti di memorizzazione ispezionati dagli accertatori prima di apporre i sigilli. Cfr. A. Monti, *Attendibilità dei sistemi di computer forensic*, «ICT-Security», 9, 2003; G. Vaciago, *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli, 2012. Il tema della rilevanza giudiziaria delle cattive pratiche è stato affrontato da alcune decisioni tra cui rilevano quelle relative al c.d. caso Vierika del Tribunale (21 luglio-22 dicembre 2005 n. 1823) e dalla Corte d'Appello di Bologna (30 gennaio-27 marzo 2008 n. 369), e la decisione del c.d. caso Garslasco (Trib. Vigevano, sent. 17 dicembre 2009).

[20] Ad esempio particolari problematiche emergono nel contesto delle indagini sul *cloud*. Cfr. C. Federici, *Nuovi orizzonti per l'acquisizione remota di Personal Cloud Storage*, in C. Maioli (a cura di) *Questioni di Informatica forense*, Aracne, Roma, 2015, 113.

[21] È frequente che la *digital evidence* sia ricercata, acquisita, conservata e quindi trasmessa e gestita da un numero svariato di attori appartenenti a paesi diversi, tra cui soggetti privati quali fornitori di servizi di informazione e telecomunicazione di vario genere. La necessità

3. Le proprietà della *blockchain* al servizio dell'informatica forense

La *blockchain* emerge nel panorama degli strumenti tecnologici oggi a disposizione per favorire lo scambio sicuro e riservato di informazioni digitali[22]. Conosciuta come la tecnologia sottostante le c.d. monete virtuali – prime tra tutte il *bitcoin* – la *blockchain* combina tecniche di crittografia asimmetrica[23], funzioni di *hash*[24] e le proprietà dei sistemi distribuiti[25] per garantire uno scambio di informazioni *peer-to-peer* trasparente e affidabile, senza la necessità di ricorrere a terzi intermediari per garantire paternità e integrità dei dati in un ambiente virtuale *trustless*.

Nel sistema *blockchain*, le informazioni sono registrate in modo indelebile in «blocchi di dati», validati[26] e condivisi da tutti i nodi (computer) facenti

di ritenere utilizzabili in un paese elementi di prova digitale assunti in un paese diverso e l'esigenza di fare affidamento sull'operato di attori esterni alle forze dell'ordine presuppongono un clima di reciproca fiducia e collaborazione tra soggetti che sono portatori, talvolta, di prerogative e obiettivi divergenti. Cfr. D. Mezzana, *Prove elettroniche: attori, ostacoli e fattori di facilitazione*, in *Informatica e diritto*, XXIV, 2015, n. 1-2, pp. 121-138.

[22] Cfr. N. Kshetri, *Blockchain's roles in strengthening cybersecurity and protecting privacy*, «Telecommunications Policy», 41, 2017, 1027-1038; G. Zyskind *et al*., *Decentralizing Privacy: Using Blockchain to Protect Personal Data*, 2015 IEEE CS Security and Privacy Workshops, 2015; F. Dai *et al*., *From Bitcoin to Cybersecurity: a Comparative Study of Blockchain Application and Security Issues*, ICSAI, 2017.

[23] Come è noto, la crittografia asimmetrica prevede l'utilizzo di una coppia di chiavi complementari: quanto viene cifrato con una chiave può essere decifrato esclusivamente con l'altra chiave della coppia ma non è possibile risalire da una all'altra. Ciò consente di realizzare i sistemi a chiave pubblica, nei quali ciascuno dei soggetti che si scambiano informazioni ha la titolarità di una diversa coppia di chiavi. Una chiave della coppia, la chiave privata, rimane segreta, conosciuta solo al titolare, l'altra chiave della coppia, la chiave pubblica è resa conoscibile a tutti coloro che intendano comunicare con il titolare. Questi sistemi consentono di garantire tanto la riservatezza delle comunicazioni, quanto l'autenticità e l'integrità dei messaggi.

[24] La funzione di *hash* è una funzione unidirezionale, ovvero impossibile da invertire, che genera, a partire da una sequenza di dati di dimensione arbitraria, una stringa binaria di lunghezza costante (*digest* o impronta) e ne garantisce l'unicità. Qualsiasi modifica al messaggio, anche minima, porterà alla generazione di un diverso valore di *hash*, con una conseguente verifica della compromissione del dato. La funzione di *hash* trova ampio utilizzo negli ambiti della sicurezza informatica, quali firme digitali e altre forme di autenticazione nonché nell'ambito dell'informatica forense per garantire l'integrità dei dati acquisiti.

[25] In informatica un sistema distribuito è un insieme di calcolatori indipendenti che appare agli utenti e alle applicazioni come un singolo sistema coerente. Nei sistemi *blockchain* non esiste più nessun centro ma la governance è distribuita secondo una architettura di rete peer-to-peer, in cui i nodi non sono gerarchizzati ma possono fungere al contempo da client e server verso gli altri nodi terminali (host) della rete. Mediante questa configurazione, qualsiasi nodo è in grado di avviare o completare una transazione.

[26] Il processo di validazione dei pacchetti di dati immessi in una *blockchain* è delegato all'intero network, così che nessun nodo ha la facoltà di inserire, modificare o rimuovere una informazione in modo autonomo. Tale processo di validazione collettiva è generalmente detto consenso distribuito e, nei protocolli tradizionali tra cui quello di *Bitcoin*, si basa sulla risoluzione di un problema crittografico (*proof of work*). A causa della eccessiva quantità di

parte del network. Questi blocchi di dati, concatenati tra essi in un *merkle tree*[27], sono da un lato trasparenti ad ogni membro del network, dall'altro protetti tramite crittografia. Ciò garantisce (a) un consenso distribuito su tutto ciò che viene immesso nella catena informativa; (b) inalterabilità delle informazioni da parte di attori malevoli, siano essi esterni o interni al network; e (c) privatezza delle informazioni registrate, accessibili solo attraverso appropriate chiavi private. Inoltre, ciascun blocco di dati, nel momento in cui è registrato sulla *blockchain*, può essere automaticamente contrassegnato da una sequenza numerica che identifichi in modo certo e univoco la data e l'ora contestuali: questa è la funzione del *timestamp*, attraverso cui la *blockchain* permette di annotare e opporre a terzi la precisa collocazione temporale degli eventi da essa censiti.

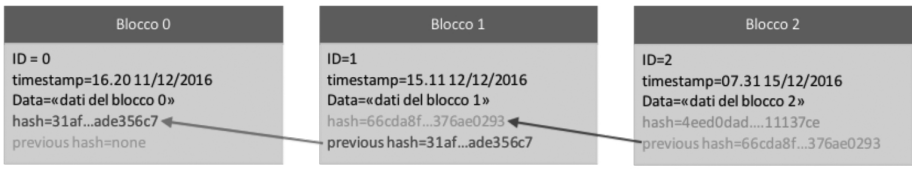

Fig.1. La blockchain del Bitcoin.

Grazie a queste caratteristiche, la *blockchain* si presta a rispondere a quelle esigenze di integrità, trasparenza e autenticità che sono pregnanti nel contesto dell'informatica forense, e in particolare per il mantenimento della catena di custodia della prova digitale, strumento strategico per la garanzia del contraddittorio nella formazione della prova[28].

energia computazionale richiesta da tale meccanismo, alcuni protocolli più recenti si basano su sistemi alternativi quali il *proof of stake* o il *proof of activity*, per i quali si rimanda a A. Castor, *A (Short) Guide to Blockchain Consensus Protocols*, su https://www.coindesk.com/.

[27] Un *merkle tree* è una struttura dati ramificata basata su *hash*. I pacchetti di dati sono accoppiati a due a due creando un *hash* per ogni coppia; ogni *hash* viene poi accoppiato con un altro *hash* e così via finché non si arriva a un unico *hash (root)*. Questo procedimento può essere rappresentato come un albero dove le foglie sono i pacchetti di dati originari, i rami gli hash intermedi e la radice l'hash finale. La struttura a albero permette di verificare solo un particolare ramo che collega una foglia alla *root* piuttosto che dover verificare gli *hash* di tutto il blocco.

[28] In argomento alcune prime proposte, presentate tra il 2015 e il 2018, vengono da: J. Fisher, M.H. Sanchez, *Authentication and verification of digital data utilizing blockchain technology* (brevetto US 20160283920 A), 2016; D. Salgado, *Blockchain of Evidence*, Report for the UK Ministry of Justice; J. Hack Park *et al.*, *Block chain based data logging and integrity management system for cloud forensics*, «Computer Science & Information Technology», 2017; C. Kamhoua *et al.*, *ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability*, CCGRID 2017; J. Lee, *Beyond Bitcoin: Leveraging blockchain for forensic applications*, Grant Thornton, 2017; C. Liu, *How the Blockchain Could Transform the Process of Documenting Electronic Chain of Custody*, Ventura, 2017; K. Zatyko, *Improving Cyber Forensics & Cybersecurity through Block Chain*

Sfruttando la tecnologia *blockchain* si possono progettare archivi decentralizzati di informazioni e meta-informazioni relative ai reperti digitali, a cui i vari attori vengono selettivamente legittimati ad accedere tramite un sistema di crittografia asimmetrica, che realizzano pienamente il paradigma della catena di custodia. Si hanno, così, *repository* di informazioni la cui certezza, integrità e trasparenza è affidata al controllo distribuito dell'intero network.

Per ogni elemento digitale presente sulla catena di custodia è possibile impostare requisiti di accesso specifici, legittimando ciascun nodo a visualizzare alcune informazioni piuttosto che altre, in attuazione delle esigenze di protezione dei dati. Inoltre, il medium tecnologico stesso è garanzia di immutabilità e tiene traccia di ogni accesso o modifica, rendendo nota all'intero network ogni eventuale tentativo di manipolazione.

Infine, la *blockchain* distribuita, condivisa tra vari attori, si presta come mezzo istantaneo, sicuro e dotato di un sistema di certificazione *built-in* per la trasmissione delle richieste di informazioni e di elementi di prova digitale tra autorità di diversi paesi e tra queste e i *service providers* privati[29].

4. Un modello di catena di custodia basato sulla tecnologia *blockchain*

Si presenta dunque la modellazione di uno strumento che, sfruttando le proprietà della tecnologia *blockchain*, svolge le funzioni tipicamente attribuite all'istituto della catena di custodia dei dati digitali: un database decentralizzato, interoperabile e sicuro, capace di risponde al contempo alle esigenze di standardizzazione delle procedure, tracciabilità e trasparenza delle operazioni forensi come sopra illustrate, al fine di favorire la collaborazione tra gli attori nazionali e internazionali che sono a vario titolo coinvolti nelle indagini ad oggetto digitale.

Secondo la prassi attuale, la catena di custodia ha inizio con il verbale relativo al sopralluogo e al sequestro, il quale contiene informazioni quali il numero del caso, il reparto investigativo a cui esso è assegnato, il nome dell'investigatore incaricato, una breve descrizione del caso, il luogo di rinvenimento del supporto e così via. Tale «blocco» di informazioni funge, nel sistema qui proposto, da anello iniziale di una *chain* specificatamente creata per il caso in esame. Tale catena sarà mano a mano costruita attraverso l'inscrizione delle informazioni, raggruppate in successivi blocchi, relative ai vari reperti, operazioni di analisi, accessi eseguiti e

Technology with Truth Based Systems, International Symposium on Forensic Science Error Management, 2015; A.H. Lone, R.N. Mir, *Forensic-chain: Ethereum blockchain based digital forensics chain of custody*, «Scientific & practical cyber security journal», 2, 2017.

[29] Sul punto si vedano in particolare gli esiti del progetto *Evidence* (FP7, 2014-2016). È ormai matura la convinzione che sia necessario realizzare un quadro comune europeo in materia di trattamento e scambio della prova digitale.

software utilizzati nell'ambito delle indagini attinenti al caso, secondo le diverse fasi metodologiche in cui si articolano le attività informatico-forensi[30].

Nell'ambito del sopralluogo si procede frequentemente con la copia forense[31] del supporto analizzato. In tal caso la *blockchain* assolverà la funzione di certificare la corrispondenza tra copia e originale attraverso l'inscrizione degli *hash* rispettivamente risultanti dall'insieme dei dati costituente il supporto originario e dalla copia forense di quest'ultimo[32]. In tal modo, sarà possibile in ogni momento verificare genuinità e integrità delle copie sottoposte ad attività di analisi attraverso il confronto dei risultati delle funzioni di *hash* memorizzati sulla catena di custodia.

Raccolti i dati e registrato l'*hash* di ogni potenziale elemento di prova, quindi, saranno effettuate le opportune analisi per estrapolare il materiale informativo utile ai fini dell'istruttoria. In tale fase il corretto utilizzo dello strumento proposto richiederebbe l'accurata registrazione di un ulteriore *hash:* quello del codice sorgente di ogni software utilizzato per le analisi. Si rende così possibile verificare a posteriori la versione e dunque il funzionamento del programma eseguito per l'analisi - verifica che, assieme al controllo della coincidenza tra copia analizzata e dati originali, è indispensabile per la validazione dei risultati probatori ottenuti.

In una *blockchain* ogni soggetto – o nodo del network – è abilitato ad interagire con il database distribuito per inserire o visualizzare informazioni tramite una coppia di chiavi crittografiche, di cui una pubblica e una privata: ogni dato è dunque firmato con la chiave pubblica identificativa del soggetto che la immette; in questo modo, il sistema stesso può verificare la legittimità dell'inserimento e di chi lo compie. Viceversa, ad un dato impresso sulla *blockchain* si potrà avere accesso solo tramite l'apposita chiave privata.

Nel modello di *blockchain* qui proposto per la catena di custodia forense, quindi, ad ogni soggetto di volta in volta legittimato deve essere concessa la chiave privata idonea a rivelare l'informazione necessaria. Tale sistema garantisce, da un lato, la piena confidenzialità e sicurezza di quanto immesso sulla *blockchain*: si tratta di un tipo di crittografia non facile da aggirare, che rende l'accesso ai

[30] Lo standard ISO/IEC 27037:2012 suddivide il processo di gestione della prova digitale nelle fasi di: identificazione, raccolta, acquisizione e conservazione. Sono queste le fasi iniziali del ciclo di vita della prova. Le migliori pratiche e i documenti ISO successivi definiscono anche attività ulteriori, quali: analisi, valutazione e presentazione.

[31] Una copia forense (o *bit stream image*) è la copia bit per bit dei dati digitali presenti in un dispositivo di memorizzazione di dati digitali verso un altro dispositivo di memorizzazione. È una esatta clonazione, senza perdita di dati nella destinazione e senza alterazione della sorgente; consente di copiare anche dati dello spazio cancellato e di preservare le date originarie dei file. Lo scopo è quello di compiere le fasi successive su una copia dei dati e non sugli originali.

[32] Si osserva che la *blockchain* non è adatta alla memorizzazione di grandi quantità di dati. Pertanto, il risultato della copiatura dovrà essere memorizzato su un database esterno, rispetto al quale la *blockchain* può essere deputata alla gestione degli accessi.

dati impossibile ad ogni utente non autorizzato; dall'altro, permette di gestire e memorizzare le interazioni dei vari soggetti parte del network con flessibilità, istantaneità e massima certezza. Inoltre, grazie alla funzione del *timestamp* sopra descritta, ciascuna operazione compiuta nell'ambito delle investigazioni e i successivi accessi alle prove saranno registrati con automatica annotazione della data e dell'ora contestuali, in modo tale da certificare la corretta sequenza temporale degli eventi rilevanti per la catena di custodia degli elementi di prova digitale.

Le singole operazioni compiute nell'ambito del processo forense sono quindi registrate dal sistema in modo automatico, immutabile e cronologicamente ordinato, così che i soggetti di volta in volta interessati potranno in ogni momento ricostruire il ciclo di vita dei reperti digitali e la successione degli eventi ad essi relativi. Infine, si può predisporre il requisito tecnico per cui ad ogni accesso o presa visione di un reperto sia registrata, contestualmente, non solo la chiave pubblica corrispondente al nodo del network e il *timestamp*, ma anche l'identità personale dell'operatore incaricato, lo scopo e la durata dell'intervento (Figura 2).

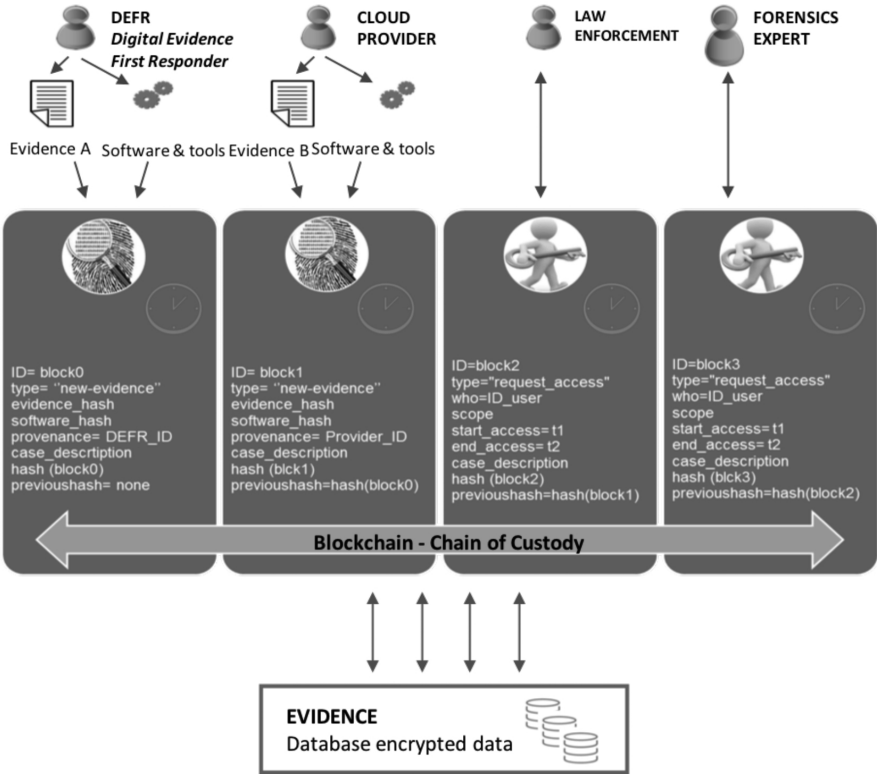

Fig. 2. Catena di custodia degli elementi di prova digitale tramite blockchain.

Per rispondere ad esigenze di celerità e trasparenza nella collaborazione internazionale in materia di indagini digitali lo strumento in esame può essere utilizzato per veicolare lo scambio di richieste e l'attribuzione di accesso a informazioni tra forze dell'ordine di diverse giurisdizioni, attori giudiziari internazionali e prestatori di servizi coinvolti nelle indagini. Anche a questo scopo, il database distribuito e crittografato, usato quale mezzo tecnologico di invio e ricezione di richieste e informazioni, si presterebbe quale registro – sottratto al controllo esclusivo di ciascuna delle parti – degli atti ufficiali compiuti dai vari soggetti. Una funzione in senso lato «notarile», che, assolta dalla tecnologia in esame in posizione *super partes*, è di estrema utilità in un ambito in cui la delicatezza degli interessi perseguiti richiede la massima celerità e certezza delle procedure[33].

5. Conclusioni

La prova digitale va assumendo un ruolo centrale nelle indagini penali, e sempre più frequentemente incide in modo decisivo sul percorso logico-probatorio del giudice. La sua idoneità a tale scopo, tuttavia, rischia di essere sopravvalutata se non si tiene conto della estrema volatilità e fragilità dei *bit* che costituiscono l'informazione digitale e della differenza epistemologica tra risultanza scientifica e prova giudiziale. Con riferimento all'informatica forense, quindi, il reinquadramento del rapporto tra scienza e processo è uno sforzo propedeutico alla definizione, da un lato, di standard normativi che guidino il giudice nella valutazione della prova digitale; dall'altro, di protocolli operativi e strumenti tecnici funzionali a un corretto espletamento delle attività di indagine e alla loro critica in sede processuale.

Il presente lavoro partito dalla disamina delle problematicità che caratterizzano attualmente la prassi forense e delle loro ricadute in ambito processuale ha proposto una soluzione che sia capace di garantire trasparenza, efficienza e certezza delle procedure e dei risultati probatori, nonché tracciabilità delle attività inerenti le indagini informatiche.

L'accurata documentazione di ogni atto compiuto nell'ambito delle indagini è, infatti, presupposto fondamentale per l'esercizio del diritto di difesa sulla formazione della prova digitale. Pertanto, lo strumento descritto e analizzato sfrutta la tecnologia *blockchain* nella sua funzione documentale per tenere traccia, come vuole l'istituto della catena di custodia, di ogni attività compiuta sul reperto digitale – dalla sua identificazione al suo ingresso in processo – con il fine ultimo di assicurare la piena tracciabilità del ciclo di vita del reperto informatico,

[33] Si veda il progetto *NotarChain* presentato nel 2017 dal Notariato e IBM (http://www.notariato.it/sites/default/files/cs_notarchain_13102017.pdf).

testimoniare genuinità e integrità dei dati e coadiuvare la collaborazione tra i vari attori coinvolti nelle indagini forensi.

La proposta qui elaborata trova giustificazione nella sempre maggiore incidenza nella giustizia penale di problemi tecnici ed organizzativi inerenti al trattamento e allo scambio della prova informatica e risponde a specifici requisiti emergenti dalla prassi della *digital forensics* che si acutizzano ulteriormente a fronte dell'impiego di strumenti di acquisizione dei dati altamente intrusivi e occulti quali, tra i più recentemente dibattuti, i captatori informatici[34].

[34] I captatori sono programmi installati in modo occulto nel dispositivo dell'utilizzatore per ottenere dati utili direttamente dal dispositivo del sospettato. La Legge 23 giugno 2017, n.103 (la c.d. Riforma Orlando) riforma la disciplina delle intercettazioni di comunicazioni, regolamentando (per la prima volta in Italia) l'uso dei cosiddetti «captatori informatici». In argomento si vedano, tra tutti, M. Torre, *Il captatore informatico*, Giuffrè, Milano, 2017 e G. Giostra, R. Orlandi (a cura di), *Nuove norme in tema di intercettazioni*, Giappicchelli, 2018.