



**Focus on**

***LA PRIVACY IN AMBIENTE  
BLOCKCHAIN:  
GDPR E TECNOLOGIA  
BLOCKCHAIN SONO  
COMPATIBILI?***

**Ottobre 2018**

[www.lascalaw.com](http://www.lascalaw.com)

[www.iusletter.com](http://www.iusletter.com)

Milano | Roma | Torino | Bologna | Firenze | Venezia | Vicenza | Padova | Ancona

[redazione@iusletter.com](mailto:redazione@iusletter.com)



## 1. Premessa

*Privacy* e *blockchain* sono due argomenti che in questi ultimi mesi hanno avuto molta eco mediatica. Da un lato per via del rialzo delle quotazioni del *bitcoin* lo scorso autunno e dall'altro per via dell'entrata in vigore a maggio di quest'anno del **GDPR** (il Regolamento (UE) 2016/679 sul trattamento dei dati personali) che ha rivitalizzato l'attenzione del pubblico sul tema del trattamento dei dati personali.

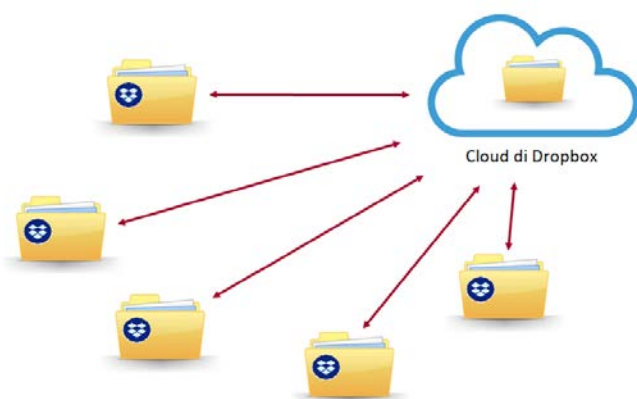
È giunto quindi il momento di chiedersi se legge e tecnologia possono andare a braccetto o se la prima ostacola lo sviluppo della seconda. Da più parti, infatti, si sostiene che la blockchain non è compatibile con il GDPR rinvigorendo ancora di più le posizioni criptoanarchiche "antisistema" e scoraggiando gli entusiasti *technologist* e *geek*.

In questo breve lavoro, sosterrò al contrario della corrente *mainstream* che GDPR e *blockchain* sono compatibili e che in particolare è possibile costruire un'architettura *peer to peer* utilizzando le soluzioni criptografiche di una **DLT** (*Distributed Ledger Technology*) in modo da essere GDPR *compliant*.

## 2. Cosa è la *blockchain*

Iniziamo con chiarendo cos'è la *blockchain*. A tal fine è utile fare un'analogia con un servizio assai noto: **Dropbox**.

Si tratta di un servizio fornito dalla Dropbox Inc. che consente di avere una copia di *file*, per



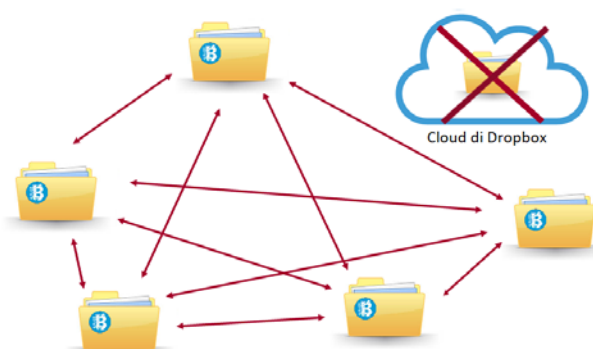
esempio un *.docx*, su un *server* su *cloud* (situato in UE, Irlanda). Chiunque voglia questo servizio (gratuito in versione base), altro non deve fare che andare sul sito [dropbox.com](https://www.dropbox.com) e scaricare il *software client*. Fatto ciò, gli comparirà sul suo PC in locale (C:) una cartella un po' particolare, poiché qualsiasi file inserito in essa viene



automaticamente replicato su una uguale cartella sul *server* in *cloud* di Dropbox. In pratica, la cartella sul mio PC è costantemente sincronizzata con la cartella nel *cloud*. La comodità di questo servizio è che lavorando su un PC in casa e uno sul luogo di lavoro, per esempio, si può avere replicata su ciascuno di essi la medesima cartella dropbox e quindi lavorare indistintamente su uno di essi modificando vecchi *file* o creandone di nuovi e poi trovare tali modifiche anche sugli altri PC dove la cartella dropbox è stata caricata. Allo stesso modo, se si perde un PC o se viene rubato, è sufficiente comprarne uno nuovo, caricare il *client* dropbox e scaricare tutto il contenuto della cartella dropbox originaria senza che nessun *file* vada perso.

Con il servizio dropbox posso anche creare dei *file* condivisi, cioè dei *file* sui quali possono lavorare in simultanea altri utenti. Per farlo, il primo utente fornisce a Dropbox l'indirizzo *e.mail* dei partecipanti al network che quindi ricevono un invito a partecipare. Coloro che accettano, entrano a far parte di una rete privata di utenti nella cui cartella dropbox compare il *file* condiviso; a questo punto tutti possono partecipare alle modifiche e vedere quelle fatte dagli altri partecipanti. Infatti, quando viene modificato un file condiviso, la modifica viene replicata sul *file* in *cloud* che poi si sincronizza con tutti i *file* caricati nelle cartelle dropbox di ciascuno dei partecipanti al *network* che quindi hanno sempre accesso all'ultima versione del *file*.

La *blockchain* funziona più meno nello stesso modo, solo che non esiste un Dropbox Inc. con il *cloud* al vertice che controlla, protegge e sincronizza i dati del *file* condiviso. Tale *file* è invece solo caricato in copia sui PC dei partecipanti al *network* in un mutuo e reciproco scambio di informazioni dove tutti controllano tutti e insieme sostituiscono assai efficacemente Dropbox Inc.



Anche con una *blockchain* gli utenti devono scaricare sul loro PC un *software client* e con esso il *file* condiviso. Il *client* contiene anche le regole per la modifica del *file* (il c.d. protocollo) per cui chiunque può modificare il *file* condiviso, e tali modifiche viaggiano direttamente da un PC all'altro (detti nodi) senza necessità di un *server* centrale. Se tali modifiche rispettano il



protocollo (per esempio, rimanendo nell'analogia del file .docx, l'uso solo di un certo *font*, o altre regole redazionali), i nodi le accettano e quando il consenso raggiunge il 50%+1 dei nodi, il *file* è aggiornato in modo definitivo, è sedimentato potremmo dire, e si passa ad analizzare le successive proposte di modifica provenienti da altri nodi.

### 3. Impostazione centralistica della legge e impostazione distribuita dalla *blockchain*

Se quindi una *blockchain* lavora sostanzialmente senza una testa, e cioè senza un nodo che sia dotato di privilegi particolari e che governa le operazioni di allineamento e aggiornamento del *file* condiviso, è difficile dire chi abbia la responsabilità degli eventuali illeciti commessi in *blockchain*. Si potrebbe ipotizzare che l'abbia chi ha impostato il protocollo o di chi lo applica, ma proprio la natura distribuita di un *network blockchain* rende in linea di massima impossibile individuare con certezza un soggetto responsabile, sia da un punto di vista tecnologico sia da un punto di vista prettamente legislativo senza contare che per la responsabilità aquiliana occorre anche considerare l'elemento soggettivo dell'illecito (colpa o *dolo*).

Questo non deve sorprendere poiché la tecnologia *blockchain* è nata proprio sul solco di idee anarchiche, cioè con lo scopo dichiarato di aggirare il controllo governativo e rendere gli uomini liberi da regole e vincoli imposti dall'alto.

Qualsiasi legge, per sua propria natura, si rivolge ad un soggetto. La struttura della norma, come si studia al primo anno di giurisprudenza, è formata da precetto e sanzione, entrambi tali elementi fanno riferimento al soggetto obbligato e/o responsabile. Una norma quindi prevede sempre l'individuazione di un soggetto da cui attendersi una condotta e a cui imputare una responsabilità.

Nel caso della *blockchain* tale soggetto semplicemente non esiste, è sfumato; ma se anche lo individuassimo, si tratterebbe di una sorta di *fictio iuris* o al peggio di una individuazione in astratto, per categoria, rimanendo in concreto assai difficile se non impossibile applicare alcuna sanzione. Rimanendo nell'analogia del *file* dropbox condiviso di cui al paragrafo precedente: quando tale *file* è aggiornato come è possibile sapere chi lo ha modificato, come si può



distinguere la responsabilità di chi lo ha aggiornato da quella di chi lo ha approvato raggiungendo il consenso della maggioranza? Pertanto, è forse vero che ontologicamente una *blockchain* è incompatibile con il GDPR che invece prevede un soggetto, il titolare, che decide e governa le operazioni di trattamento di dati personali, e uno o più soggetti che lo coadiuvano in tali trattamenti, i responsabili.

Questo vale soprattutto nel caso delle *blockchain* pubbliche (*permissionless*), cioè quelle realizzate con *software open source*, dove tutti i nodi hanno uguale ruolo e non servono autorizzazioni di alcuno di essi per partecipare al *network*. Ma ciò potrebbe valere anche per le *blockchain* private (*permissioned*) o miste pubbliche e private, dove alcuni nodi assumono un ruolo particolare, per cui potrebbero esporsi ad una responsabilità teorica e pratica per violazione di legge.

A questo punto dobbiamo quindi chiederci se il GDPR si applica alla *blockchain*, e in particolare se si applica alla *blockchain* pubblica, cioè se è inevitabile che una *blockchain* pubblica (quindi quella più soggetta a difetto di controllo e di *enforcement* da parte di autorità) tratti dati personali e, soprattutto se i nodi debbano o meno considerarsi titolari o responsabili del trattamento. Se infatti ricorresse questa inevitabilità, ci troveremmo di fronte ad un problema concreto, ovvero l'impossibilità di costruire una *blockchain* pubblica, o misto privata pubblica, senza esporci alla violazione di legge o alla sua pratica impossibilità di *enforcement*.

#### 4. Il GDPR raggiungerà presto il suo limite elastico con le DAO

Voglio sottolineare questo aspetto, perché se è vero che le *Decentralized Autonomous Organizations* (DAO) prenderanno piede ci troveremo presto in situazioni di insanabile frizione tra dettato normativo e tecnologia e dovremo essere costretti a pensare al concetto di imputabilità in termini completamente nuovi. Portata alle sue estreme e futuribili conseguenze, la tecnologia *blockchain* consente l'assunzione di decisioni giuridicamente rilevanti da parte di un *network* che non è scomponibile nella volontà o nella condotta dei singoli nodi, ma che è sintesi di quella. Sconfiniamo qui in un campo che trascende il diritto e approda nell'intelligenza



artificiale (AI) e in organismi superindividuali, ma poiché tutto ciò che accade nel mondo fisico ha poi riflessi nel mondo del diritto, sono certo che prima o poi una meditazione sulla responsabilità e soggettività delle DAO si imporrà.

## 5. Le comuni soluzioni criptografiche adottati in una *blockchain*

Sono quindi le *blockchain* compatibili con il GDPR? Ebbene, lo sono nella misura in cui le soluzioni criptografiche che sono impiegate in esse sono esenti dalla qualifica di dato personale: se sostanzialmente le chiavi asimmetriche e le impronte *hash* non sono dati personali, allora è possibile costruire una *blockchain* o più in generale una DLT senza preoccuparci troppo di *privacy*, se invece tali funzioni ricadono nella definizione di dato personale, costruire una *blockchain* pubblica, o pubblico-privata, sarà impossibile senza violare la legge o senza imporre oneri eccessivi ai nodi.

## 6. Definizione di dato personale

La definizione di dato personale fornita dall'art. 4 del GDPR, non dissimile da quella dell'art. 2 della direttiva 95/46/CE, recita:

*“dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale”.*

A leggere questa definizione, verrebbe da dire che tutto è un dato personale. E in effetti c'è chi ha sottolineato la possibilità di leggere la definizione in termini così ampi e ha qualificato la legge europea sulla *privacy* come la legge del tutto. Se infatti il dato personale è una qualsiasi informazione che può in qualche modo, attuale o potenziale, condurre all'identificazione di una



persona fisica, non riusciamo a darci un confine. Qualsiasi informazione, prima o poi, può essere utile per l'identificazione di una persona fisica. In altri termini, se si parte dall'assunto che tutto è informazione (e pare proprio che sia così, compresi gli oggetti fisici) e se si seguono certi ragionamenti per cui l'uomo, in quanto essere senziente, dà forma ed addirittura esistenza all'Universo, dobbiamo inevitabilmente concludere, senza fare troppa filosofia, che tutto è dato personale. E l'analisi *Big Data* sembra sempre più suggerire tale conclusione.

## 7. Lettura dell'art. 2 della Direttiva (95/46/CE) da parte del WP nel 2007 (WP136): contenuto, scopo e risultato

Per circoscrivere la nozione di dato personale, viene in aiuto il Gruppo di Lavoro ex art. 29, oggi Comitato europeo per la protezione dei dati, che con il parere WP136 del 2007 (recentemente confermato nella sua validità e attualità) ha fornito utili elementi per l'interprete volti a scongiurare, o quantomeno limitare, il rischio di una definizione di dato personale omnicomprendente.

Adottando un approccio analitico sulla definizione di dato personale fornita dalla legge (*“qualsiasi informazione riguardante una persona fisica identificata o identificabile”*), il Gruppo ha individuato le tre parole che forniscono la sua chiave di lettura: *“informazione”*, *“riguardante”* e *“identificabile”*.

Quanto al concetto di *informazione*, essa è di poco aiuto per circoscrivere la portata della definizione. Come visto sopra tutto è informazione: qualsiasi ente che viene percepito, sia esso materiale (un oggetto fisico, un fenomeno atmosferico) o immateriale (un'emozione, un diritto), è per ciò solo un'informazione. Peraltro, un'informazione può essere considerata dato personale indipendentemente dalla sua natura (oggettiva o soggettiva), dalla forma (scritta, sonora, visiva, ecc.) o dal supporto (cartaceo, elettronico, magnetico, meccanico, ecc.).

Quanto al concetto di *riguardante* si può aggiungere qualcosa. Va notato innanzi tutto che nella versione in inglese è scritto *«related to»* che non è proprio *«riguardante»*, ma un concetto più



ampio. Nella traduzione della direttiva del 1995, era addirittura scritto “*concernente*” (art. 4 del Codice), il che sembrava più far riferimento ad un attributo della persona fisica. Con “*riguardante*”, quindi, si è fatto un passo in avanti, ma “*related to*” è comunque un qualcosa in più; vuol dire che l’informazione è *connessa* in qualche modo ad una persona fisica. Concetto quindi molto ampio che potrebbe essere appunto tradotto con “*connessa a*”, sicché il Gruppo ha fornito un *test* di verifica del nesso tra informazione e persona fisica basato su una triplice analisi: un dato è “personale” se, oltre agli altri elementi che pure devono ricorrere, è per *contenuto* o per *scopo* o per *risultato* riconducibile all’identificazione attuale o potenziale di una persona fisica.

Per il contenuto, vale l’esempio di una cartella clinica il cui contenuto è chiaramente riferibile ad una persona fisica;

per lo scopo vale l’esempio dell’indirizzo IP di un PC. Esso non è immediatamente percepibile come dato personale, come accade per il contenuto di una cartella clinica, ma se è utilizzato per rintracciare una persona fisica (per esempio chi commette un illecito penale o civile mettendo in rete o fruendo abusivamente di materiale coperto da *copyright*, per cui dall’IP, incrociando i dati con l’ISP, si risale al titolare del contratto e per presunzione all’identità del colpevole) allora è anch’esso considerato dato personale, ancorché identifichi direttamente solo una macchina;

per il risultato, vale l’esempio dei dati di navigazione dei taxi utilizzati solo per ottimizzare lo smistamento delle chiamate. Manca qui il contenuto e lo scopo e tuttavia il trattamento si risolve di fatto in un monitoraggio dei percorsi dei tassisti, loro abitudini e *performance*. Dati quindi riferibili a persone fisiche.

## 8. Caso Alba-Cooper

L’esempio dei taxi appena visto è utile per comprendere come la definizione di dato personale del GDPR può essere inclusiva anche di trattamenti che hanno ad oggetto informazioni che non possono considerarsi dati personali al momento del loro primo trattamento, ma che diventano





tali per via del successivo incrocio con altri dati. Il concetto di dato personale, pertanto, è mutevole, dinamico, soggetto cioè a una serie di circostanze a contorno, esogene, che ne decretano la sua qualificazione giuridica in un senso o nell'altro.

Come accennato, i dati di navigazione dei taxi sono dati personali in quanto non superano il test del WP136 per la parte riferibile a “risultato”. Per tale ragione, un simile trattamento può essere effettuato dalle compagnie di taxi solo dietro accordo con i tassisti, ovvero ottenendo dalle loro rappresentanze sindacali un consenso informato. Nessun trattamento, invece, è effettuato sui dati dei passeggeri, ai quali infatti non deve essere chiesto alcun consenso. Tuttavia, ciò si è rilevato non sempre vero e i dati del traffico dei veicoli hanno finito per diventare dati personali dei passeggeri. Nel 2013 un cittadino statunitense facendo leva sul **FOIL - Freedom Of Information Act** dello Stato di New York ha chiesto e ottenuto dalla *New York City Taxi and*



Figura 1. Il caso Cooper-Alba. Incrociando i dati di corsa dei taxi con le foto dei paparazzi si può ricavare la destinazione dei vip e la loro propensione a pagare mance.

*Limousine Commission* copia dei dati di navigazione di tutti taxi newyorchesi e ha pubblicato tali dati su Internet, peraltro mettendo a disposizione degli utenti un *software* di ricerca in modo da facilitare il rintraccio delle singole corse. Il risultato è stato emblematico. I dati in questione erano ovviamente anonimi, cioè contenevano solo le corse, la targa del taxi e l'importo di corsa con eventuale mancia del passeggero. È tuttavia accaduto che gli utenti hanno iniziato ad utilizzare tali dati incrociandoli con quelli presi da *tabloid* specializzati in *gossip* di *star* della TV e del cinema. Nello specifico, tra le tante celebrità, Jessica Alba e Bradley Cooper furono paparazzati in circostanze diverse mentre prendevano un taxi fuori dall'albergo in cui



alloggiavano. Nelle foto erano visibili anche le targhe dei taxi e fu facile quindi utilizzare quel dato per vedere, utilizzando il *software* in rete, dove gli attori si erano recati e se avevano o meno lasciato la mancia. Ecco allora che, sebbene la pubblicazione dei dati della *New York City Taxi and Limousine Commission* di per sé non potesse considerarsi pubblicazione di dati personali riferibili ai passeggeri, lo divennero nel momento in cui tali dati furono incrociati con le foto dei paparazzi.

Ciò dimostra non solo che tutto può essere potenzialmente considerato come dato personale, ma anche che ciò che oggi non lo è, lo può diventare domani.

## 9. Persone identificate o identificabili (considerando 26 Direttiva e GDPR)

Come visto, la seconda parte della definizione di dato personale contenuta nell'art. 4 del GDPR fa riferimento a "*persona fisica identificata o identificabile*". Sono quindi dati personali, le informazioni che restano impigliate nelle maglie del *test* che abbiamo visto sopra (contenuto, scopo e risultato) e che, al tempo stesso, consentono l'identificazione di una persona fisica.

Il requisito dell'identificabilità introduce nella definizione un elemento di concretezza: per essere "personale" un dato deve essere in concreto soggetto ad un'operazione, attuale o potenziale, di identificazione di un soggetto persona fisica.

Il considerando 26 del GDPR (conforme al considerando 26 della precedente direttiva) così recita:

*“per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime vale a dire informazioni che non si riferiscono a una persona fisica*



*identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato".*

**WP136**  
Opinion n. 4  
del 20 giugno  
2007

“relating to”:

1. contenuto
2. scopo
3. risultato

“identificata o identificabile”:

In relazione alle circostanze concrete, ovvero tenendo conto della possibilità:

1. legale
2. tecnologica
3. di fatto

Come si legge, il concetto di identificabilità passa per una verifica concreta dei mezzi e delle risorse che colui che compie il trattamento può effettivamente (*rectius*: ragionevolmente) impiegare. Questa specificazione rende l'identificabilità un concetto relativo che si declina come sussistente o meno a seconda del soggetto

che tratta i dati. In tale prospettiva, un medesimo dato, è considerato personale se lo tratta colui che ha i ragionevoli mezzi per risalire all'identità del soggetto interessato a cui il dato si riferisce, e non è considerato personale se colui che lo tratta non ha ragionevolmente accesso a mezzi e risorse tali per risalire all'identità del soggetto interessato a cui si riferisce.

Nel caso Alba-Cooper visto prima, gli attori non erano identificabili in origine, non era cioè associabile a loro un particolare percorso di un taxi, ma lo sono diventati successivamente, sono cioè stati identificati come coloro a cui particolari percorsi di taxi erano riconducibili. I percorsi in questione – o meglio le informazioni relative a percorso, numero di taxi, importo della corsa e della mancia – sono diventati quindi dati personali solo in un momento successivo, quando cioè è stato agevolmente consentito agli utenti di incrociare le foto con il *data base* riferendoli a persona fisica identificata (i VIP).

## 10. Cosa sono e come funzionano le chiavi asimmetriche in BC

Tra i primi commentatori che hanno studiato le implicazioni della tecnologia *blockchain* in una prospettiva *privacy* e GDPR c'è chi sostiene che le chiavi pubbliche siano senza eccezioni dati pseudonimi, se non addirittura dati personali.



Tuttavia, alla luce dei ragionamenti appena svolti, sappiamo che non tutto è dato personale, ma che tale nozione è *dinamica* e *relativa*. Dinamica in quanto la natura di un'informazione può mutare dal momento della sua raccolta diventando dato personale solo in successivamente. Relativa in quanto un dato personale può essere tale solo per un determinato soggetto in legittimo possesso di (o che può legittimamente o ragionevolmente accedere a) una *lista di corrispondenza*, ovvero ad una lista che associa in modo univoco ciascun codice (*keycoded data*) ad una determinata identità.

Vediamo quindi se questa nozione di dato personale è adattabile alle soluzioni criptografiche impiegate in un protocollo blockchain, e in particolare alle *chiavi asimmetriche*.

Le chiavi asimmetriche sono comunemente utilizzate per le firme digitali. Si tratta di chiavi criptografiche accoppiate in modo tale che un testo cifrato con una di esse può essere decifrato solo con l'altra, così consentendo di verificare la paternità dei messaggi.

Il funzionamento può essere sintetizzato come segue.

Un certificatore genera una coppia di chiavi asimmetriche e consegna una di esse (chiamiamola chiave privata) ad una persona identificata in modo certo e rende disponibile su un registro pubblico l'altra chiave della coppia (chiamiamola chiave pubblica). Ebbene, per fornire la prova della provenienza di un messaggio, il titolare della chiave privata deve cifrarlo con questa e, poiché il destinatario potrà decifrarlo solo utilizzando la corrispondente chiave pubblica, quest'ultimo con ciò sarà in grado di verificare l'identità del mittente consultando il registro delle chiavi pubbliche.

## 11. Il WP136 test applicato alle chiavi asimmetriche

Le chiavi asimmetriche utilizzate in un sistema di firma digitale, quindi, sono univocamente associate all'identità di una persona; sono anzi utilizzate proprio per consentire tale identificazione. In una *blockchain*, invece, le chiavi asimmetriche sono solo utilizzate per consentire la spendita di un credito espresso in criptovaluta o, più in generale, l'esecuzione di una transazione senza incorrere nel *problema della doppia spesa*, ovvero il problema l'abusivo



uso multiplo di un medesimo file in ambiente digitale, dove notoriamente non esiste distinzione tra originale e copia.

Tale differenza non è secondaria: le chiavi in firma digitale sono senz'altro dati personali per *scopo* e *risultato*, nonché per il fatto che esiste una lista di corrispondenza addirittura pubblica, e quindi facilmente accessibile a chiunque. In una *blockchain*, invece, non esiste alcuna lista di corrispondenza, né c'è associazione tra chiavi e identità. Le prime, inoltre, non sono impiegate affatto per risalire all'identità dell'utilizzatore della chiave privata, né è facile che ciò accada, se non ricorrendo a sofisticate tecniche di *digital forensic*. Tali circostanze non consentono alle chiavi asimmetriche, come impiegate in una *blockchain*, di superare il *test* del WP136, né più né meno di come non lo supera il numero di serie stampato sulle banconote.

## 12. Cos'è e come funziona l'impronta hash in BC

L'impronta *hash*, detta in termini tecnici anche *digest*, è l'*output* di una funzione *hash*, ovvero una particolare funzione (classe di funzioni) che trasforma un certo valore (testo) in una stringa alfanumerica di lunghezza fissa.

La particolarità di un *digest* è che non consente in nessun modo di risalire al testo originale cifrato in quanto non c'è corrispondenza univoca tra *input* e *output*. Inoltre, poiché le possibili permutazioni dei simboli che compongono l'*output* è enorme (due elevato a potenza di 256 nella funzione *hash* utilizzata nel protocollo *bitcoin*), possiamo con ragionevole



approssimazione dire che il *digest* di un testo equivale ad una sua “impronta”, così come quella

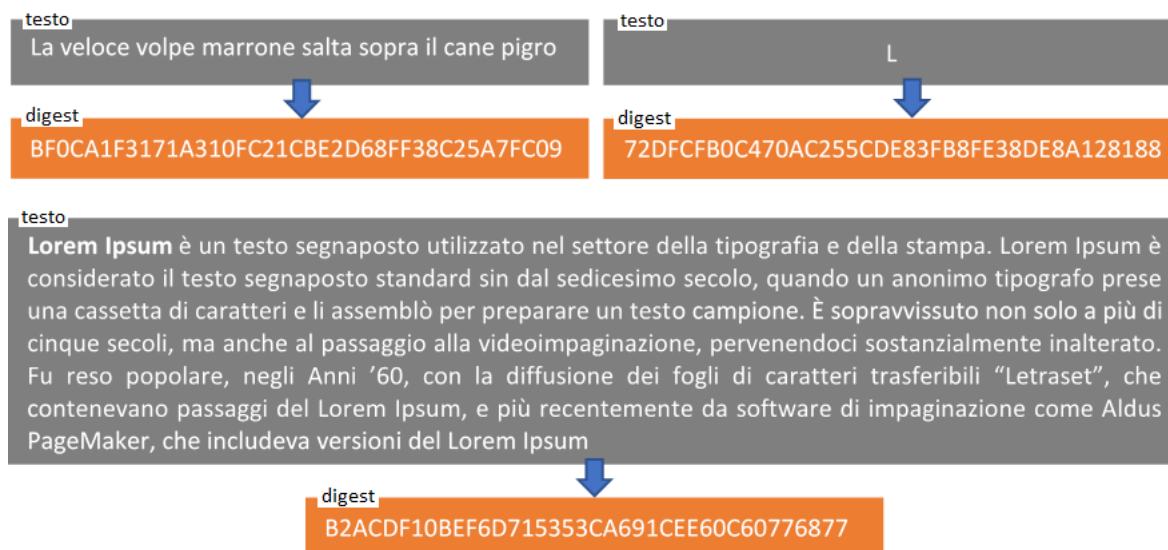


Figura 2. Il *digest* ha sempre lunghezza uguale, qualunque sia la lunghezza del testo (una piccola modifica del testo, genera una grande differenza del *digest*).

digitale a cui siamo abituati identifica con ragionevole certezza una determinata persona.

Le impronte *hash* sono ampiamente utilizzate in *blockchain* per formare e gestire la catena dei blocchi e quindi per garantire l’inalterabilità dei dati e la corretta validazione delle transazioni effettuate dai nodi del *network*.

### 13. Opinione del WP136 sulle funzioni unidirezionali (in generale, dato anonimo)

Le funzioni di *hash* hanno la proprietà di anonimizzare i dati, cioè di consentire il loro trattamento... senza trattarli. Un *digest*, infatti, può essere oggetto di trattamento senza che da esso si possa risalire in alcun modo, neanche teorico, ai dati personali che rappresenta. In altri termini, o si sa a prescindere che un certo *digest* è stato ottenuto da un determinato *set* di dati personali, disposti in una specifica sequenza e codifica, oppure esso è del tutto dissociato e non riconducibile ai dati che lo hanno generato.

Tale *unidirezionalità* delle funzioni *hash* ha addirittura portato il Gruppo dei Garanti Europei a sostenere quanto segue nel parere WP136: “è inoltre possibile mascherare l’identità rendendo



*impossibile la reidentificazione, per esempio con la crittografia unidirezionale che crea in genere dati anonimi”.*

Secondo gli esperti, quindi, le funzioni *hash* rendono impossibile la reidentificazione creando, in genere, dati anonimi. Da notare che con l’inciso “in genere”, il Gruppo fa riferimento evidentemente alla possibilità di associare i *digest* a liste di corrispondenza il che ovviamente, al ricorrere degli altri elementi del *test* WP136 (ad esempio, il rendere facilmente disponibili tali liste), rende vano l’impiego di funzioni *hash* nel processo di anonimizzazione).

Ciò nonostante, è interessante notare che gli stessi Garanti, in linea di principio, ritengono l’applicazione di una funzione unidirezionale circostanza sufficiente per anonimizzare i dati e quindi per procedere al trattamento in modo sicuro.

Anche a proposito della funzione *hash*, quindi, deve concludersi che essa non implica un trattamento di dati personali, a condizione ovviamente, come per le chiavi asimmetriche, che ricorrano (o non ricorrano) certi elementi a contorno che costituiscono sufficiente garanzia di protezione dei dati.

#### 14. Casascius

La dimostrazione pratica che una *blockchain* non implica necessariamente un trattamento di dati personali è fornita dalla circolazione (invero assai limitata) di supporti fisici che rappresentano unità di valore espresse in criptovaluta.

L’esempio più noto è la moneta Casascius. Si tratta apparentemente di una comune moneta metallica sulla quale è stampata una chiave privata che sblocca un credito di 1 *bitcoin* (ma ci sono di diverso taglio) e in parte celata da un adesivo particolare che, una volta rimosso, non può essere applicato nuovamente. Tale soluzione, consente alla moneta in questione di passare di mano in mano né più né meno di una comune moneta di corso legale consentendo pagamenti in *bitcoin* tanto



Figura 3. Casascius.



anonimi quanto lo sono i pagamenti in contanti. Pertanto, a meno di non considerare i numeri di serie sulle banconote dati personali, l'esempio del Casascius dimostra che in *blockchain* i dati circolano in forma anonima.

## 15. Parere del notariato

Lo scorso marzo il Consiglio Nazionale del Notariato ha preso posizione in tema di pagamenti in *bitcoin* rispondendo al quesito di un professionista (Quesito Antiriciclaggio n. 3-2018/B) che si domanda se *“il pagamento del prezzo della vendita di un bene immobile in bitcoin – o altra criptovaluta – violi le norme in materia di limitazione all’uso del denaro contante (art. 49 del D.Lgs. n. 231/2007, come modificato dal D.Lgs. n. 90/2017) nonché quelle in materia di indicazione analitica dei mezzi di pagamento (art. 35, comma 22 del D.L. n. 223/2006, convertito con modificazioni in L. n. 248/2006)”*.

Dopo una lunga dissertazione sulla natura e sul funzionamento dei *bitcoin* il CNN non ha ritenuto applicabile ai pagamenti in tale valuta la disposizione che impone l’obbligo di indicazione analitica delle modalità di pagamento del corrispettivo sottolineando la differenza con i pagamenti in contanti dove il pubblico ufficiale rogante assiste al, e testimonia il, passaggio materiale di contanti o assegno circolare, cosa che non avverrebbe nell’utilizzo di criptovalute. Ecco il passaggio:

*“...mentre in talune transazioni effettuate in contanti il pubblico ufficiale può essere testimone di una traditio che avviene in sua presenza, con ciò rendendo in qualche modo tracciato almeno un singolo segmento del flusso anonimo del contante, l’operazione in bitcoin costituisce una transazione che potrebbe essere definita apparente; essa proviene, infatti, da un “conto”, che l’acquirente dichiara essere proprio, ad un altro conto del quale, parimenti, il venditore asserisce la titolarità, ma il tutto senza che possa esservi il benché minimo riscontro della veridicità di tali dichiarazioni”*.





In questa opinione è trascurato un fatto fondamentale, ovvero che i *bitcoin* sono contante virtuale e che l'identificazione dell'ordinante e del beneficiario del pagamento è senz'altro possibile senza eccezioni anche se effettuato con criptovalute.

A tal fine è sufficiente che l'ufficiale rogante si faccia parte attiva nella *traditio*, cioè nel trasferimento materiale di valore, e crei, in presenza delle parti, due coppie di chiavi asimmetriche (operazione assai semplice che è possibile fare con innumerevoli *tool*/a disposizione anche in rete), chiamiamole coppia C, come compratore, formata dalla chiave privata **Cpr** e dalla chiave pubblica **Cpu**, e coppia V, come venditore, formata dalla chiave privata **Vpr** e dalla chiave pubblica **Vpu**. Successivamente l'ufficiale assegnerà le chiavi alle parti, e quindi la coppia C al compratore e la coppia V al venditore (è irrilevante in questa fase che le chiavi private Cpr e Vpr siano visibili a tutti) e chiederà al primo di effettuare il pagamento dell'importo di compravendita al suo nuovo indirizzo Cpu. Il compratore, quindi, utilizzerà i *bitcoin* in suo possesso accedendo ad un proprio "conto" di cui possiede la chiave privata ed effettuerà l'accredito sul nuovo indirizzo identificato con la chiave Cpu. Verificata la transazione (ovvero aggiunto in *blockchain* il blocco contenente la transazione e atteso un ragionevole tempo di convalidazione – circa sei blocchi), il notaio chiederà al compratore di utilizzare la sua chiave privata Cpr per trasferire il credito esistente su Vpu. Il venditore, a questo punto, potrà utilizzare a sua discrezione la chiave Vpr per trasferire il prezzo su un proprio "conto" sicuro, oppure potrà tenere i *bitcoin* su Vpu confidando che né il notaio né controparte siano tentati di appropriarsene utilizzando Vpr (a loro nota).

Con questi passaggi, apparentemente complicati, ma in realtà assai semplici (in sintesi, si creano due coppie di chiavi e si chiede al compratore di fare una doppia transazione), il notaio è in grado di testimoniare a tutti gli effetti la *traditio*, ovvero che il compratore e il venditore da lui identificati siano rispettivamente il *tradens* e l'*accipiens* dell'operazione di pagamento.

A questo punto vale la pena fare una riflessione: se anche il Consiglio Nazionale del Notariato confonde, mi si lasci dire, un po' grossolanamente, la disposizione delle chiavi asimmetriche in *blockchain* con la disposizione di credenziali di accesso ad un conto corrente bancario, significa



che la strada da fare nel nostro Paese per colmare un ritardo cognitivo a livello istituzionale su questa tecnologia è piuttosto lunga.

## 16. Dati personali inseriti in chiaro in blockchain

Sebbene, come visto, le soluzioni criptografiche che caratterizzano una *blockchain* non comportino necessariamente un tema di protezione di dati personali, va detto che è tuttavia possibile inserire deliberatamente in *blockchain* dati personali in chiaro in modo che siano accessibili a chiunque da tutto il mondo senza possibilità di rimozione se non impiegando uno sforzo in termini di consenso ed energia impraticabile.

Nella *blockchain* dei *bitcoin*, per esempio, esiste un apposito spazio nell'intestazione dei blocchi chiamato *coinbase* a disposizione degli utenti per inserire messaggi di qualunque genere che, via via che nuovi blocchi “sedimentano”, cioè si aggiungono nella sequenza della catena, sono impossibili da rimuovere. Altre *blockchain*, poi, potrebbero essere appositamente progettate in modo tale da non rispettare le disposizioni del GDPR ricorrendo, per esempio, all'impiego di chiavi pubbliche di firme digitali proprio allo scopo di identificare i soggetti interessati cui i dati in *blockchain* si riferiscono.

In questi casi non è chiaro, secondo l'impostazione del Regolamento (e invero, come accennato all'inizio di questo lavoro, secondo una qualsiasi impostazione di legge), come potrebbe l'interessato pretendere il *diritto all'oblio* con la cancellazione dei suoi dati, né a chi dovrebbe rivolgere tale richiesta. Si presenterebbe infatti un insuperabile problema di *enforcement*, ovvero proprio il tipo di impedimento voluto dal movimento criptoanarchico che ha fatto germogliare e ha sviluppato la tecnologia *blockchain*.

## 17. Il titolare del trattamento in una blockchain

Se la chiave pubblica e l'impronta *hash* non sono dati personali, vien da sé che i nodi, fintanto che si limitano a svolgere le loro funzioni di *mining* e fintanto che il protocollo del *network* sia



realizzato con un'architettura rispettosa del diritto alla protezione dei dati personali, non sono titolari del trattamento e non devono rispettare le disposizioni del GDPR. Caricare su un *server* tutto o parte del *database* della *blockchain* al fine di validare i blocchi non costituisce di per sé un'operazione volta all'identificazione dei titolari delle chiavi pubbliche, né l'identificazione di questi è un effetto secondario ed immediato delle operazioni di *mining* o di *routing* del traffico. In tale prospettiva, nello spirito criptoanarchico che ha dato origine a questa rivoluzione tecnologica, chiunque può partecipare alla costruzione e rafforzamento di un *network* pubblico *blockchain* senza dover provvedere agli adempimenti previsti dal GDPR e senza dover adottare particolari misure di sicurezza.

Diverso è naturalmente il caso dei *wallet* e degli *exchange*, ovvero di tutti quegli ISP che raccolgono le opportunità di *business* offerte da una *blockchain* pubblica e in rete offrono servizi accessori agli utenti del *network* che vanno dalla gestione delle chiavi, allo scambio di criptovalute, e in futuro chissà cos'altro. Nel farlo trattano i dati personali dei propri clienti e quindi, come qualsiasi altro fornitore di servizi della società dell'informazione, debbono considerarsi a tutti gli effetti titolari del trattamento.

## 18. Conclusioni

Nel prossimo futuro, l'ecosistema digitale si popolerà di reti *peer-to-peer* con protocollo *blockchain*. Alcune saranno di tipo pubblico, altre private e altre ancora miste pubblico-private. In tutti i casi i servizi veicolati saranno forniti secondo un modello di *business* che sfrutta l'orizzontalità del *network* decentralizzato e remunera i nodi con *token* o criptovalute di nuovo conio.

Alcuni nodi tratteranno chiavi e impronte *hash* per fini identificativi più o meno diretti disponendo di liste di corrispondenza con l'identità dei soggetti interessati ad esse associati. Altri tratteranno le stesse chiavi e impronte al solo fine di consentire il funzionamento del *network* contando sulla remunerazione loro spettante per l'attività di *mining* e non avranno accesso ad alcuna lista di corrispondenza, né sarà previsto che lo abbiano. I dati da loro trattati,



quindi, non saranno personali nel senso inteso dal WP136 e dalla CGUE, non essendo dati “*relating to a natural person*”, difettando contenuto, scopo e risultato, e non essendo i soggetti interessati “*identificabili*”, mancando la ragionevole possibilità per loro di disporre di risorse e informazioni atte all’identificazione.

Il GDPR e la tecnologia *blockchain* non sono quindi ontologicamente incompatibili. Progettare un protocollo *blockchain* in modo tale che le soluzioni criptografiche impiegate non debbano considerarsi dati personali, e addirittura non debbano neanche considerarsi dati pseudonimi, è possibile, ed è anzi la regola.

Credo che in futuro la *blockchain*, anziché rappresentare un rischio per i diritti e le libertà fondamentali dell’individuo in termini di *privacy*, sarà lo strumento che metterà definitivamente nelle mani dei soggetti interessati la disponibilità esclusiva e il controllo dei loro dati.

*Francesco Rampone*

*Of Counsel*

*Team IP/IT*

*f.rampone@lascalaw.com*

