UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Tesi di Laurea Triennale

Analisi di compatibilità fra GDPR e Distributed Ledgers Technology

Orso De Vero

12 Novembre 2024

Università degli Studi di Padova
Facoltà di Ingegneria
Dipartimento di Ingegneria dell'Informazione (DEI)
Corso triennale in Ingegneria dell'Informazione

Presidente
Prof. Marco Santagiustina

Relatore
Prof. Mauro Migliardi

Laureando
Orso De Vero

Data
12 Novembre 2024

Per aspera ad astra. (Et lauream.)

Indice

Abstract

Il GDPR è il regolamento in materia di protezione dei dati personali in Europa. Per studiarlo, sono di particolare interesse i Diritti e i Pilastri del GDPR. I sistemi *Distributed Ledger Technology (DLT)* permettono di distribuire l'informazione tramite la cooperazione fra i partecipanti in una rete *peer-to-peer*, mediante l'uso di algoritmi di consenso, senza quindi l'ausilio di una base di dati centralizzata. Tra i più comuni esempi di tali sistemi troviamo le blockchain.

Ci chiediamo se questa tecnologia sia compatibile con le leggi GDPR e procediamo ad analizzare le interazioni fra GDPR e algoritmi di consenso nei sistemi DLT.

Il contesto delle blockchain è particolarmente interessante perché presenta alcune caratteristiche tecnologiche in contrasto con le leggi GDPR; e, nonostante ciò, è una tecnologia che ha goduto di un'enorme applicazione dal 2008, anno di rilascio del Bitcoin, la prima criptovaluta basata su DLT.

Dall'analisi delle interazioni fra GDPR, in forma di Diritti e Pilastri da un lato, e DLT, in forma di algoritmi di consenso e configurazioni di partecipazione alla rete dall'altro, si delinea uno stato dell'arte in cui la compatibilità non è completa, ma esiste una direzione in cui procedere, quella delle configurazioni a consorzio, o federate.

Di questo tipo di configurazioni ne esistono alcuni esempi pratici, come le iniziative a livello europeo, quali *EBSI (European Blockchain Services Infrastructure),* utilizzata dai diversi *use case* del progetto *Trace4EU*.

Parte I.

Introduzione e motivazione

1. Motivazione

Il *General Data Protection Regulation (GDPR)* è in tensione con i sistemi *Distributed Ledgers Technology (DLT - in italiano, Tecnologia di Registri Distribuiti)*, in particolare le blockchain, perché non è chiara l'attribuzione di responsabilità della gestione dei dati, né del rispetto dei diritti previsti dal GDPR.

Questo tema è di particolare interesse per poter capire i limiti e le strade da percorrere per poter sfruttare le potenzialità dei sistemi DLT nel futuro, specialmente in ambiti nei quali sia necessario garantire un corretto trattamento di dati sensibili; oltre che a garantire la legalità delle operazioni, ipotesi fondamentale nella nostra società.

La questione si fa ulteriormente interessante dal momento che le criptovalute hanno goduto di un'enorme espansione dal 2008, anno di pubblicazione del Bitcoin; espansione che, dal 2016, anno di entrata in vigore delle leggi GDPR, è potenzialmente non conforme alle leggi di protezione dei dati in ambito Europeo.

Per questo motivo, analizziamo le possibili interazioni fra GDPR, da un lato, studiato in forma di Pilastri e Diritti, e DLT, dall'altro, in forma di configurazioni di rete e algoritmi di consenso disponibili. Nel corso dell'analisi, porremo in luce sia i punti di contrasto osservati, che i punti in cui un sistema DLT risulti compatibile con il GDPR. Delineeremo così una direzione che questa tecnologia può intraprendere, riepilogando nelle conclusioni tutto ciò che abbiamo scoperto, dai punti di attenzione ai punti di forza, portando anche alcuni esempi pratici che testimoniano l'evoluzione di questa tecnologia.

1.1. Elementi di base di un sistema *Distributed Ledger Technology (DLT)*

Un sistema DLT può essere catalogato secondo quattro componenti: la struttura dati, il protocollo di consenso, i permessi di accesso alla rete e l'esistenza o meno di un processo di mining di valute, piuttosto che l'utilizzo di una valuta preesistente.

In questa esposizione, studieremo alcuni protocolli di consenso e i permessi di accesso alla rete.

1.2. Cos'è e come funziona una blockchain

La *blockchain* è l'esempio più comune di DLT. In essa, la struttura dati che forma il *ledger* è una catena lineare di blocchi.

I protocolli di consenso più comuni che verranno analizzati sono il *Proof of Work (PoW)* e il *Proof of Stake (PoS)*. In questa tesina ne analizzeremo alcuni altri, come il *Delegated Proof of Stake (DPoS)*, variante del PoS; il *Proof of Burn (PoB)*; e infine il *Proof of Authority (PoA)*.

Per quanto riguarda i permessi di accesso alla rete, questi possono essere divisi in due categorie:

- *permissionless*: l'accesso è libero, chiunque può partecipare, validando nuovi blocchi della catena e recuperando lo storico completo delle transazioni;

- *permissioned*: l'accesso è ristretto, sottoposto ad una fase di autenticazione.

Nella categoria *permissioned*, troviamo due ulteriori modalità: *consortium* (blockchain a consorzio, o federata, in italiano) e blockchain privata.

Nel modello *consortium*, i nodi che validano i nuovi blocchi della catena sono limitati in numero e identificati, quindi esiste un sistema di registrazione e autenticazione dei nodi; mentre l'accesso in lettura allo storico del ledger può ancora essere aperto al pubblico.

Nel modello privato, invece, anche l'accesso in lettura è ristretto ai soli partecipanti, previa autenticazione.

Infine, per quanto riguarda i processi di *mining* delle valute, questi sono utilizzati solo nel protocollo PoW, mentre il protocollo PoS si appoggia a valute già oggetto di *mining*. Esempio più famoso di *mining* è quello dei Bitcoin, la prima criptovaluta pubblica e *permitionless*, che utilizza il consenso di tipo *Proof of Work*. Fra i due, il PoW è, quindi, quello più energivoro, tanto da aver dato vita al fenomeno delle cosiddette *mining farm*.

Nei protocolli di consenso è previsto un meccanismo che incentiva la corretta collaborazione fra i nodi al momento di validare nuovi blocchi della catena. Questo incentivo è il cosiddetto *golden nonce*.[1] A questo corrisponde una quantità di criptovaluta che viene accreditata al proprietario del nodo che ha validato il nuovo blocco della catena. Nel caso del PoW, ciò avviene quando questi risolve il *puzzle* computazionale e aggiunge un nuovo blocco alla catena. In altri termini, è una commissione che viene incassata dai nodi validatori, come ricompensa per aver generato un nuovo blocco.

[1] Il termine deriva dall'espressione *"**n**umber used only **once**."*

Origine dei protocolli di verifica decentralizzati

L'idea di un sistema basato su blocchi che vengono firmati mediante la crittografia asimmetrica viene fatta risalire a [Cha79], un *whitepaper* scritto da D. L. Chaum nel 1979. Egli teorizza e illustra il funzionamento dei *vault* crittografici, precursori delle attuali criptovalute. Utilizza la parola *"chain"* (per la precisione, *"chained"*) 1 sola volta e la parola *"block"* ben 18 volte, in un documento di 11 pagine.

1.2.1. Algoritmi di consenso

Di grande interesse per la nostra analisi sono i protocolli di consenso. Focalizziamo la nostra attenzione su di essi nei seguenti paragrafi.

1.2.1.1. *Proof of Work* (PoW)

L'idea alla base del *Proof of Work* è quella di richiedere una prova computazionale di cospicua complessità all'utilizzatore del servizio. Trova radici in applicazioni *anti-spam* e *anti-Denial of Service (anti-DoS)* ed è nota anche sotto altri nomi: *CPU cost function*, *client puzzle*, *computational puzzle*, *CPU pricing function*.

Questo meccanismo funge da bilanciatore per la blockchain stessa.

Il modello *Proof of Work* è necessario solo nelle blockchain pubbliche e *permissionless*, in quanto è l'unico modo per rendere possibile la partecipazione di utenti senza una registrazione previa [SV17].

1.2.1.2. *Proof of Stake* (PoS)

Nel modello *Proof of Stake*, invece di richiedere la risoluzione di una prova computazionale, viene chiesta la dimostrazione di possedere una quantità di un certo *asset*. Questo tipo di consenso si appoggia quindi su altre valute, anziché includere un processo di *mining*. L'ammontare di valuta in possesso dell'utente è il suo "*stake*", ovvero la sua "*posta in gioco*". Quanto maggiore è la posta che si decide di utilizzare, tanto maggiore è la probabilità che il nodo sia selezionato alla validazione del blocco successivo della catena.[2] Per fissare le idee, riportiamo un esempio quantitativo dalla bibliografia: in una blockchain a consenso PoS che si appoggi sul Bitcoin come valuta della posta in gioco, un utente in possesso dell'1% dei Bitcoin ha l'1% di probabilità di essere selezionato per generare il blocco successivo, incassando così la commissione legata alla transazione, il *golden nonce* [SV17].

[2] *"The next block writer on the blockchain is selected at random, with higher odds being assigned to nodes with larger stake positions."*, in [Inv].

1.2.1.3. *Delegated Proof of Stake* (DPoS)

Nel modello di consenso DPoS, la selezione del vincitore del *golden nonce* diventa un processo a due fasi.

Viene eletta una commissione di delegati o "testimoni" per mezzo di una votazione, in cui i voti hanno valore proporzionale alla posta in gioco in possesso a ciascuno dei votanti. Una volta che la commissione è eletta, è questa che provvede a selezionare i blocchi successivi e a votare a favore o contro l'inclusione degli stessi nella catena.

Il sistema con il quale vengono selezionati i vincitori del *golden nonce* si basa quindi su una votazione e sulla posta in gioco dei partecipanti alla votazione [SV17].

1.2.1.4. Proof of Burn (PoB)

Anche il modello PoB si appoggia su criptovalute precedentemente oggetto di *mining*, in particolare secondo il modello PoW.

Nel PoB, il meccanismo di validazione di nuovi blocchi prevede che i nodi validatori dimostrino di aver "bruciato" una certa quantità di criptovaluta in loro possesso. Per fare ciò, è necessario che effettuino una transazione verso un *wallet* (portafogli) destinatario dal quale non è più possibile recuperare gli importi inviati [SV17]. Tale portafogli è certificato come inutilizzabile.

1.2.1.5. Proof of Authority (PoA)

Infine, il modello PoA sottopone la validazione di nuovi blocchi ad un sistema di autenticazione a chiavi private. Per poter generare un nuovo blocco della catena, è necessario e sufficiente possedere una chiave privata abilitata o riconosciuta.[3] Inoltre, non è possibile, per uno stesso nodo validatore, scrivere più blocchi consecutivamente sulla catena.

Per queste caratteristiche, il modello PoA può essere paragonato ad un sistema di scambio di informazioni dietro autenticazione come può essere quello usato in un server email, ma in un contesto in cui è utilizzabile in modo automatico da elaboratori per scambiare informazioni, in modo ordinato, in forma di transazioni, permettendo l'esecuzione dei cosiddetti *smart contract*.

È di cruciale importanza che l'identità degli attori non venga compromessa, al fine di poter esercitare correttamente il privilegio di creare nuovi blocchi in questo modello di consenso.

[3] Le prime chiavi private riconosciute sono impostate nella fase iniziale di configurazione (*bootstrapping*) di un sistema DLT che impieghi il modello PoA.

Brevissimo cenno sulla sicurezza dei modelli di consenso

Il consenso distribuito, sostituendo quello centralizzato, risolve alcune problematiche ad esso legato, ma non è esso stesso esente da problemi.

Mentre il consenso centralizzato introduce un *single-point-of-failure* nel sistema, quello distribuito è soggetto al problema noto come *Byzantine fault*. Si tratta del problema decisionale di come arrivare ad un consenso quando le parti possono compiere ognuna una scelta indipendente e diversa dalla strategia di azione concordata in precedenza.

Non espandiamo ulteriormente questo aspetto, ma citiamo solamente alcuni riferimenti per gli interessati: *51% attack* (PoW), *nothing-at-stake attack* (PoS), *bribery attack* (PoS) [SV17].

1.3. Le leggi GDPR

Che cos'è il GDPR

Il GDPR è il regolamento europeo in materia di protezione dei dati. Vengono stabiliti e chiariti limiti e responsabilità degli attori coinvolti nel trattamento dei dati delle persone fisiche nei sistemi informatici. Inoltre, stabilisce alcuni diritti fondamentali delle persone fisiche, tra i quali anticipiamo: l'accesso ai propri dati da parte dell'utente; la conoscenza delle modalità di utilizzo dei dati; la possibilità di decidere se e come i propri dati vengano elaborati; e la rimozione dei propri dati.

L'entità che decide quali dati raccogliere, il come e il perché raccoglierli è denominata *Data Controller*. L'entità che si occupa di elaborarli è chiamata *Data Processor*. Il *Data Processor* può non coincidere con il *Data Controller*, come spesso è il caso [Com]. L'utente del quale vengono raccolti e trattati i dati è indicato con il termine *Data Subject*.

Procediamo con l'elencare Pilastri e Diritti del GDPR, fissando così le basi dell'analisi che andremo a svolgere nella seconda parte di questa tesina, in cui confronteremo GDPR e DLT [Sev].

1.3.1. Pilastri del GDPR

1.3.1.1. Legalità

Il primo Pilastro del GDPR è quello della legalità (art. 5 e 6). Prima di tutto, la richiesta di raccolta dati deve avere fondamento legale. Inoltre, lo scopo per cui i dati vengono raccolti non può essere illegale né poco chiaro.

1.3.1.2. Limitazione di scopo

Il secondo Pilastro stabilisce che lo scopo per il quale i dati vengono richiesti deve essere dichiarato, consentendo all'utente di scegliere di esserne a favore o contro (art. 5). Portiamo un esempio dalla bibliografia per mostrare il limite fra ciò che è permesso o meno: un viaggiatore chiede informazioni ad un'agenzia di viaggi per andare in vacanza in California; con questa informazione, l'operatore dell'agenzia può suggerire offerte di viaggio in sconto verso mete limitrofe; ciò che non può fare, invece, è utilizzare l'informazione per offrire al viaggiatore altri tipi di servizi.

1.3.1.3. Minimalità dei dati

Il terzo Pilastro implica che il *Data Controller* può fare richiesta solo della minima quantità di dati sufficiente a permetterne l'elaborazione, da parte del *Data Processor*, per gli scopi dischiarati (art. 5). Proseguendo l'esempio del viaggiatore, l'agenzia di viaggi potrebbe chiedere delle informazioni aggiuntive circa i gusti del cliente, in modo da poter restringere il campo di ricerca a stabilimenti balneari o di montagna. Non sarebbe invece possibile chiedere al cliente il suo orientamento politico o dove ha trascorso le vacanze negli ultimi anni, in quanto informazioni sensibili, o non necessarie.

1.3.1.4. Esattezza dei dati

Il quarto Pilastro indica che i dati devono essere raccolti in modo corretto e, su richiesta del *Data Subject*, possano essere corretti anche successivamente, tramite apposite procedure di correzione (art. 5).

1.3.1.5. Limitazione di conservazione

Il quinto Pilastro, sulla limitazione di conservazione, stabilisce che i dati possono essere conservati solo per una durata prestabilita, affine allo scopo dichiarato (art. 5). Esistono delle eccezioni, che riguardano le finalità di interesse pubblico, storico-scientifiche, o statistiche.

1.3.1.6. Confidenzialità e integrità

Il sesto Pilastro rappresenta la sicurezza dei dati (art. 5). Il *Data Processor* deve disporre di tutte le misure necessarie a prevenire le brecce informatiche di dati, così come gli accessi fisici non autorizzati. I dati devono quindi essere protetti contro accessi, modifiche o rimozioni non autorizzate. Inoltre, il *Data Processor* deve disporre di processi di recupero dati nel malaugurato caso in cui tali brecce avvengano.

1.3.1.7. Responsabilità

Infine, in accordo con il settimo Pilastro, deve essere possibile individuare *Data Controller* e *Data Processor*, come responsabili del rispetto delle norme GDPR (art. 5). Ogni entità dovrà disporre di mezzi per dimostrare l'ottemperanza oggettiva al GDPR.

1.3.2. Diritti del GDPR

Procediamo ora con i Diritti previsti dalle leggi GDPR.

1.3.2.1. Diritto di Informazione

Il *Diritto di Informazione* (art. 13 e 14) stabilisce che, al momento della raccolta dei dati e non dopo, l'utente debba essere messo a conoscenza dei dettagli riguardanti i dati che vengono raccolti dal *Data Controller*, i criteri utilizzati per raccoglierli e quali sono gli scopi finali. Tale diritto si applica anche nel caso in cui i dati non siano raccolti direttamente dall'utente, ma indirettamente, ovvero attraverso terze parti in contatto con il *Data Controller*.

1.3.2.2. Diritto di Accesso

Il *Diritto di Accesso* (art. 15) conferisce all'utente la possibilità di richiedere accesso ai propri dati personali oggetto del trattamento da parte dei *Data Controller* e *Data Processor*, così come di richiedere tutti i dettagli relativi alla raccolta dei dati: scopi, finalità, metodi, profilazioni automatiche.

1.3.2.3. Diritto di Rettifica

Il *Diritto di Rettifica* (art. 16) è duale al quarto Pilastro di Esattezza dei dati: l'utente può richiedere che vengano corrette le informazioni conservate da *Data Controller* e *Data Processor*, come ad esempio può avvenire nell'aggiornamento dei dati anagrafici di una persona.

1.3.2.4. Diritto di Cancellazione, o Diritto all'Oblio

Il *Diritto di Cancellazione* (art. 17), conosciuto anche come *Right To Be Forgotten (RTBF)* in inglese o come *Diritto all'Oblio* in italiano, permette all'utente di richiedere la completa rimozione dei propri dati personali oggetti di trattamento da parte di *Data Controller* e *Data Processor*. In generale, viene applicato nel momento in cui si conclude un contratto fra cliente e *Data Controller*. Inoltre, la sua

applicazione è subordinata alla necessità di trattenere copia dei dati, come è possibile per altre leggi in ambito giudiziario. Altre condizioni che possono presentarsi in concomitanza con una richiesta di cancellazione sono: la raccolta di dati non autorizzata, la revoca del consenso prestato al trattamento dei dati, o l'opposizione ai criteri di raccolta dati.

1.3.2.5. Diritto di Limitazione del trattamento

Il *Diritto di Limitazione del trattamento* (art. 18) stabilisce che l'utente può chiedere, anziché la rimozione, la sospensione temporanea del trattamento dei dati. Il *Data Controller* è soggetto a procedere nel momento in cui sia contestata l'esattezza dei dati, oppure la legalità della raccolta dei dati, o, ancora, siano questi utilizzati all'interno di dispute legali. Prima di poter tornare a processare i dati, inoltre, il *Data Controller* deve informare l'utente.

1.3.2.6. Diritto di Portabilità

Il *Diritto di Portabilità* (art. 20) indica che l'utente può richiedere che vengano loro restituiti i propri dati personali oggetto di trattamento o che questi vengano trasferiti ad un altro *Data Controller*, con eventuale passaggio anche di *Data Processor*. Tale trasferimento deve essere eseguibile in un formato elettronico leggibile da elaboratore.

1.3.2.7. Diritto di Opposizione

Per il *Diritto di Opposizione* (art. 21), l'utente può chiedere revoca del consenso prestato o dichiararsi contrario al trattamento dei suoi dati personali da parte dei *Data Controller* e *Data Processor*, a patto che non esistano ulteriori vincoli legali superiori ai diritti della persona fisica per i quali sia necessario trattenere copia dei dati personali.

1.3.2.8. Diritto di Opporsi al Trattamento Automatizzato

Con il *Diritto di Opporsi al Trattamento Automatizzato* (art. 22), l'utente può opporsi a decisioni prese da algoritmi automatizzati che analizzano i dati oggetto del trattamento, come ad esempio avviene nelle profilazioni delle basi cliente. L'utente può quindi chiedere che tale decisione automatica venga riesaminata manualmente. Fanno eccezione i casi in cui il soggetto abbia prestato consenso esplicito, oppure il *Data Controller* sia autorizzato dall'Unione Europea, oppure tali algoritmi sono necessari alla stipulazione di un contratto.

Parte II.

Analisi

Una volta stabilite le fondamenta, procediamo con l'analisi delle interazioni fra Diritti e Pilastri GDPR, da un lato, e permessi di accesso e protocolli di consenso dei sistemi DLT dall'altro.

In [BSALL23], troviamo una revisione sistematica di letteratura che analizza ben 114 fonti, evidenziando tre problemi di incompatibilità, che riassumiamo di seguito:

- diritto all'oblio da un lato (GDPR); e immutabilità dall'altro (blockchain);

- chiarezza e trasparenza sui ruoli di *Data Controller* e *Data Processor* e relative responsabilità (GDPR); e ambiguità e genericità di operazione dei nodi in una rete *peer-to-peer (P2P)* pubblica (*permissionless blockchain*);

- difficoltà di applicazione delle leggi GDPR al contesto distribuito della rete di nodi che opera la blockchain.

Nella nostra analisi, applicheremo le seguenti convenzioni, eccetto dove diversamente specificato:

- individuiamo il *Data Controller* e il *Data Processor* nei nodi in grado di creare e pubblicare nuovi blocchi sulla blockchain;

- individuiamo i *Data Subject* negli utenti utilizzatori del *ledger*, cioè in grado di emettere le transazioni che verranno poi pubblicate sulla blockchain dai nodi validatori.

2. Confronto e analisi fra GDPR e blockchain

Sviluppiamo la nostra analisi partendo dai tipi di permessi di accesso alla rete di una blockchain e proseguendo con gli algoritmi di consenso utilizzati. Dopodiché, affronteremo la valutazione dei Pilastri e infine quella dei Diritti delle leggi GDPR.

2.1. Analisi a partire dalla blockchain

2.1.1. Analisi per permessi di rete

2.1.1.1. *Public permissionless*

La rete *P2P* nel caso *public permitionless* non ha confini geografici: chiunque può partecipare alla blockchain.

Ne consegue che un operatore di un nodo al di fuori dell'Unione Europea possa scegliere di non rispettare nessuno dei Diritti e dei Pilastri, perché l'utilizzo di una blockchain pubblica non prevede né il monitoraggio delle attività degli utenti presso l'UE, né la fornitura di un servizio agli stessi (art. 3). Allo stesso tempo, per la natura *permitionless* della blockchain, non è possibile discriminare la partecipazione degli utenti su base geografica.

Pertanto, ricaviamo una prima incompatibilità, fra reti *P2P* globali (utilizzate in DLT *public permitionless*) e leggi che hanno valenza e applicabilità su base geografica (regolamentando l'operato di *Data Controller* e *Data Processor*, nel caso del GDPR).

Inoltre, poiché nella configurazione *permitionless* è necessario il metodo di consenso PoW, si anticipa che la stessa conclusione verrà ritrovata nell'analisi dell'interazione fra algoritmo PoW e GDPR.

2.1.1.2. *Consortium*

Nel caso della rete a consorzio, detta anche blockchain federata (*federated blockchain*), la validazione di nuovi blocchi sulla blockchain avviene da parte di un gruppo di nodi selezionati, identificati e limitati in numero.

A differenza del caso precedente, in cui qualsiasi partecipante alla rete può contribuire alla creazione di nuovi blocchi della catena, la partecipazione alle blockchain federate è limitata e, perciò, ad esempio, è possibile effettuare una selezione su base geografica. La registrazione dei nodi può essere subordinata ad un contratto, come spesso è il caso, ed è possibile iniziare a stabilire, in modo più verosimile, il ruolo di *Data Controller* e di *Data Processor* di chi opera un nodo della rete.

Questo è dunque il primo risultato importante: il primo passo affinché una blockchain, o in generale i DLT, siano conformi alle leggi GDPR è la possibilità di sfruttare la configurazione a consorzio.

2.1.1.3. *Private* (*permissioned*)

Nelle blockchain private, la rete è interamente incapsulata all'interno di un'entità. Si tratta di un caso particolare della blockchain federata trattata precedentemente. Pertanto, è immediato identificare *Data Controller* e *Data Processor* nell'entità che gestisce la blockchain privata in maniera centralizzata.

2.1.2. Analisi per algoritmo di consenso

Volgiamo ora la nostra attenzione agli algoritmi di consenso.

2.1.2.1. *Proof of Work* (PoW)

L'algoritmo di consenso *Proof of Work* fa riferimento all'omonimo concetto, nel quale viene richiesto all'utente che voglia utilizzare un determinato servizio di dimostrare di aver svolto un certo quantitativo di lavoro, prima di poter usufruire del servizio. Tale concetto nasce dal contesto dei filtri *anti-spam* e *anti-Denial of Service* e trova applicazione anche nelle blockchain pubbliche. In questo caso, l'operazione che richiede di risolvere un problema di una certa complessità computazionale è l'aggiunta di un nuovo blocco alla catena. Ricordiamo innanzitutto che la conseguenza di tale aggiunta è la riscossione del *golden nonce* da parte del nodo che ha validato il blocco. Inoltre, il concetto di *Proof of Work* rappresenta un primo meccanismo di protezione dal rischio di *double spending* nelle blockchain pubbliche. Nel caso dei Bitcoin, risolvere il puzzle computazionale consiste nel trovare una stringa s, che rappresenterà l'intestazione del blocco successivo e include l'hash del precedente blocco, l'hash del nodo radice dell'albero di Merkle della blockchain e il *golden nonce*, fra le altre informazioni, tale che l'hash SHA-256 di s inizi con n caratteri "0". Il numero n è noto e incrementa ogni 4 anni, dimezzando il valore del *golden nonce*.

La scelta di utilizzare l'algoritmo PoW è strettamente necessaria solamente nelle configurazioni *public permitionless*, per le quali abbiamo già visto emergere una

prima incompatibilità. Muovendo verso blockchain private o federate, possiamo considerare obsoleto il modello di consenso PoW a favore di modelli PoS più efficienti, dal momento che l'accesso alle risorse della blockchain è regolato.

2.1.2.2. Proof of Stake (PoS)

Nel modello *Proof of Stake*, i *miners* di blocchi vengono selezionati in modo probabilistico. La probabilità di essere selezionati è proporzionale alla quantità della valuta di appoggio in proprio possesso. Questa quantità è ciò che rappresenta lo *"stake"*, o *"posta in gioco"*.

Dal punto di vista della configurazione della blockchain, restringiamo il campo alle blockchain private o federate. In entrambi questi casi, è possibile, in fase di registrazione, rilevare la quantità iniziale di valuta per ciascun partecipante. Tuttavia, senza ulteriori vincoli, né di configurazione della rete di nodi, né di algoritmo di consenso, qualsiasi nodo della rete ottiene l'informazione (sensibile) della quantità di valuta in possesso a ciascun altro nodo, dal momento che ogni nodo è in grado di creare nuovi blocchi e determinare l'evoluzione della catena.

Dal punto di vista della protezione dei dati, questo vuol dire che la validità di ogni blocco nella blockchain basata su Proof of Stake è potenzialmente legata in modo indelebile ad un'informazione sensibile dei *Data Subject*, per tutta la durata di vita della blockchain, senza possibilità di limitarne la distribuzione presso i nodi. Uno dei Diritti fondamentali, quello di Cancellazione, suggerisce che in questi casi si possano riscontrare delle incompatibilità fra le leggi GDPR e i sistemi DLT.

2.1.2.3. Delegated Proof of Stake (DPoS)

Gli effetti indesiderati appena analizzati per il modello PoS affliggono tutti gli schemi di consenso basati su PoS. Tuttavia, è interessante osservare come il modello *Delegated Proof of Stake* affronti il problema del consenso distribuito e quali conseguenze comporti per la nostra analisi di compatibilità con il GDPR.

In questo modello di consenso, viene eletta una commissione di nodi validatori delegati, noti anche come "testimoni", da parte dell'intera comunità di nodi che partecipano alla blockchain; stavolta, è questa votazione ad essere proporzionale alla posta in gioco dei nodi partecipanti. L'informazione viene dunque registrata non più all'interno di un *ledger*, in modo immutabile, bensì si riflette in una maggior capacità di voto in fase di registrazione, con conseguente maggiore possibilità di selezione dei delegati. Per riflesso, si ottiene un risultato finale simile, se non equivalente, a quello della selezione probabilistica proporzionale alla posta in gioco impiegato nel modello PoS, senza l'effetto indesiderato di registrare dati sensibili dei *Data Subject* nella blockchain.

Proseguendo l'analisi del funzionamento di questo algoritmo di consenso, i "testimoni" si alternano nella selezione del prossimo blocco candidato ad essere il successivo nella catena ed effettuano una votazione per giungere al consenso. Il processo non è più globale all'intera rete ma è delegato alla commissione di delegati, eletta dalla rete stessa. La commissione rappresenta l'intera rete, incapsulando l'informazione sensibile della posta in gioco di ciascuno degli utenti.

Possiamo nuovamente affermare di essere giunti a delle nuove conclusioni per la nostra analisi: la strategia adottata nel concetto di delega è tale da incapsulare un dato sensibile (ammontare di valuta in possesso ai singoli *Data Subject*) in uno astratto, pseudonimo (il livello di reputazione, ovvero il privilegio di selezionare il delegato desiderato, facendo uso del proprio voto, di valore proporzionale alla propria posta in gioco). Come è noto, la pseudonimizzazione non è anonimità. Tuttavia, il valore pseudonimo non è necessariamente pubblico in questo sottocaso (rete a consorzio, consenso DPoS); può essere riservato, trasmesso in fase di registrazione al consorzio e mai più. Viene utilizzato solo la prima volta per stabilire il valore della votazione iniziale, così come un *seed* casuale viene utilizzato per generare una sequenza casuale di numeri.

Inoltre, è possibile individuare i *Data Controller* e *Data Processor* nei nodi delegati, il ché è un ulteriore passo avanti per chiarire l'applicabilità del GDPR al contesto dei sistemi DLT.

Un'ulteriore osservazione che si può fare e che tornerà utile nell'analisi è il fatto che il sistema di reputazione basato sulla posta in gioco di ciascun utente può essere paragonato ad un sistema di profilazione automatico dell'utente. Come è noto, questo aspetto è in sovrapposizione al Diritto di opporsi al trattamento decisionale automatizzato, pertanto deve essere possibile ispezionare manualmente il risultato della conversione da posta in gioco a reputazione, in caso di necessità.

2.1.2.4. Proof of Burn (PoB)

Nel modello di consenso *Proof of Burn*, il sistema di selezione casuale è ancora presente, ma stavolta viene basato sulla quantità di valuta di appoggio che i *miners* dimostrano di aver "bruciato"; per fare ciò, essi emettono transazioni verso un portafogli (o *wallet*) dal quale non è possibile recuperare la valuta.

Dal punto di vista della protezione dei dati, la selezione dei successivi blocchi della catena viene di nuovo fatta risalire all'intera rete di partecipanti. Come abbiamo visto, questo comporta l'individuazione di *Data Controller* e *Data Processor* in tutti i nodi partecipanti alla blockchain. Inoltre, come nel caso del PoS, parte del processo è permanentemente registrato sulla blockchain per tutta la durata di vita della stessa, a differenza del DPoS, in cui la parte sensibile è incapsulata in modo pseudonimo e può essere mantenuta riservata tramite la registrazione al consorzio.

Per questi motivi, il modello PoB sembra ugualmente incompatibile con il GDPR, quanto lo è il modello PoS.

2.1.2.5. Proof of Authority (PoA)

Nel modello di consenso *Proof of Authority*, gli attori in possesso di specifiche chiavi private sono in grado di scrivere nuovi blocchi della catena. Da un lato, le chiavi private dei partecipanti vengono registrate in fase di configurazione e primo avvio del sistema DLT, potendo anche essere aggiunte o modificate in un secondo momento. Dall'altro, il meccanismo di autenticazione è familiare ai sistemi informatici da ben prima dell'avvento dei *ledger* distribuiti.

Ai fini della nostra analisi di compatibilità con le leggi GDPR, notiamo come la precisa autenticazione dei partecipanti conferisca maggior chiarezza e trasparenza nel momento di voler individuare gli attori principali responsabili della protezione dei dati trattati. Sono infatti facilmente individuati sia i *Data Controller* che i *Data Processor*, grazie alle chiavi private unicamente assegnate ad essi.

Proseguiamo notando come i nodi validatori nel modello PoA possano provvedere alla validazione delle transazioni emesse da qualsiasi partecipante. Ciò ne fa emergere un ruolo con delle caratteristiche molto simili a quelle desiderabili già osservate per i nodi delegati o "testimoni" nel caso del consenso DPoS. In particolare, osserviamo dei vantaggi in più rispetto ai modelli derivati del *Proof of Stake*.

Un primo vantaggio consta nel fatto che la scrittura dei nuovi blocchi non può avvenire consecutivamente per opera dello stesso validatore. Un altro vantaggio, più o meno desiderabile a seconda del contesto, è che la selezione del blocco successivo non sia più legata alla quantità di valuta, alla "*posta in gioco*", in possesso al nodo validatore. Quest'ultimo può essere un fattore interessante quando si vogliano coordinare i partecipanti al *ledger* distribuito con un meccanismo basato su reputazione e integrità, piuttosto che su risorse controllate. Quest'ultima caratteristica può essere reintrodotta nel modello DPoS, sostituendo il sistema basato sulla quantità di valuta con uno puramente basato sulla reputazione. Tuttavia, rimarrebbe presente la componente probabilistica di selezione del blocco successivo.

Terminiamo l'analisi osservando almeno due punti critici.

Un primo punto è se il sistema di autenticazione che venga utilizzato automaticamente per adempiere a degli *smart contract*, ad esempio, possa essere equiparato ad un processo di trattamento automatizzato dei dati, ovvero della chiave privata. Poniamo il caso in cui un nodo validatore veda la propria identità compromessa: sarà possibile esercitare il Diritto di Opposizione al trattamento automatizzato del dato, la chiave privata, in un tale scenario? Comporterà la revoca definitiva della chiave privata in questione?

Un secondo punto di attenzione è quello più familiare, legato all'immutabilità del *ledger*. Anche in questo caso, infatti, la principale causa di incompatibilità fra sistemi DLT e leggi GDPR rimane la necessità di poter eseguire operazioni di modifica, rettifica e cancellazione.

In conclusione, notiamo che il modello PoA è adatto alla configurazione di sistemi DLT sia pubblici, sia privati e anche a consorzio.

2.2. Analisi a partire dal GDPR

2.2.1. Analisi per Pilastro GDPR

2.2.1.1. Legalità

Procediamo ora con l'analisi del primo Pilastro, che abbraccia i concetti di legalità, integrità e trasparenza.

Per quanto riguarda la legalità e dell'integrità, è possibile conoscere i requisiti esatti delle informazioni utilizzate da una blockchain indagando il tipo di accesso alla rete ed il modello di consenso utilizzato. Essendo questi fattori noti a priori, l'unica variabile è l'effettiva implementazione della blockchain di ogni caso specifco.

Osserviamo un caso peculiare nel modello PoB: è noto che bruciare valute (i.e. banconote) è un atto illegale; tuttavia, questo è lo stesso atto di cui il modello PoB fa uso nel proprio algoritmo.

Per quanto concerne la trasparenza, osserviamo che le configurazioni *public permitionless* e *consortium* godono della miglior trasparenza, quando è pubblico l'accesso in lettura. Non può dirsi lo stesso delle blockchain private. Dalle precedenti analisi, siamo interessati ad approfondire l'analisi delle blockchain federate.

Analizzando i modelli di consenso dal punto di vista della trasparenza, osserviamo che nell'algoritmo DPoS è presente un rischio. Nell'analisi del DPoS, infatti, era stata assunta la possibilità di mascherare un dato sensibile (la posta in gioco dei partecipanti) con uno pseudonimo (un punteggio di reputazione). Questa conversione poteva essere mantenuta privata in fase di registrazione al consorzio, proteggendo così i dati dei *Data Subject*. Tuttavia, ora ci troviamo di fronte ad un nuovo problema. Nelle altre configurazioni, ad esempio PoW e PoS, la trasparenza del sistema è tale da garantire di poter verificare che tutto funzioni come dichiarato nell'algoritmo di consenso. D'altro canto, se nel DPoS non è possibile verificare la corretta conversione fra posta in gioco e reputazione iniziale, esiste il rischio di operare una blockchain con punteggi deviati, creando effetti negativi per l'economia, come l'inflazione, la deflazione e la doppia spesa.

Dunque, sembra di primaria importanza la messa in atto di un processo di verifica trasparente dell'implementazione nelle blockchain che usano modelli con delegati, come per il DPoS.

2.2.1.2. Limitazione di scopo

Essendo noti a priori i dati necessari dalla configurazione di accesso alla rete e dall'algoritmo di consenso, dovrebbe essere possibile conoscere gli scopi per cui ciascuna informazione viene raccolta e trattata dai *Data Controller* e *Data Processor*.

Pertanto, in linea teorica, ogni combinazione di queste configurazioni dovrebbe risultare conforme al GDPR. Vanno dunque valutati i casi specifici sulla base dell'effettiva implementazione dei sistemi DLT in uso.

Nel caso di nostro maggior interesse, accesso a consorzio e consenso DPoS, vengono registrate le transazioni presenti nel *ledger* per tutta la durata di vita della blockchain; in più, in maniera riservata, ma di trasparente verifica, le poste in gioco iniziali di tutti i partecipanti al momento della registrazione.

Esiste un rischio nella possibilità di effettuare più volte la votazione proporzionale per eleggere la commissione di delegati; al cambiare di ruolo in delegato o ex-delegato, cambiano le responsabilità dell'attore in questione.

2.2.1.3. Minimalità dei dati

Per il terzo Pilastro, la minimalità è garantita, in linea teorica, dall'algoritmo di consenso e, in quella pratica, dalla sua implementazione; poiché la minimalità ha anche interesse di carattere tecnico, osserviamo che è più verosimile che venga rispettata affinché le computazioni di un sistema così complesso come una rete distribuita *P2P* sia efficiente e meno ridondante possibile.

Nel tema della ridondanza troviamo un aspetto di una certa rilevanza, in quanto i nodi validatori posseggono ciascuno una copia dello stato più aggiornato della blockchain. Se possono esistere dei rischi circa la minimalità, potrebbero trovarsi proprio in questo aspetto. Torniamo comunque a sottolineare l'interesse di carattere tecnico di questo fattore, che suggerisce che questo problema possa essere affrontato nel progetto dell'algoritmo di consenso, potendo così essere comprovato a priori in linea teorica. Tuttavia, al momento, non può essere garantita a priori e rappresenta un possibile primo rischio concreto di incompatibilità fra Pilastri e sistemi DLT. Vedremo che questo stesso problema si ripresenta nell'analisi di altri Pilastri successivi.

2.2.1.4. Esattezza dei dati

Per il quarto Pilastro, ritroviamo due degli aspetti precedentemente analizzati per il caso consorzio con modello DPoS.

Da un lato, l'esattezza della conversione da posta in gioco a reputazione. Dall'altro, l'esattezza di ciascuna copia dello stato del *ledger*, esistente in ciascuno dei nodi validatori.

Può essere utile prevedere l'aggiunta di una stima di tempo necessario entro il quale è verosimile che tutti i nodi abbiano concordato lo stesso stato del *ledger*, fino ad un certo numero di *record* (cioè esclusi al più un ristretto numero di *record* più recenti in corso di conferma consensuale).

Infine, è da considerare anche l'ipotesi di poter applicare delle correzioni alle transazioni. Ciò potrebbe non essere possibile, per via della natura immutabile del *ledger*.

2.2.1.5. Limitazione di conservazione

Per il quinto Pilastro, esiste un caso, raro ma possibile, in cui la ripetuta mancanza di consenso nella votazione per il successivo blocco della catena (DPoS) porti al fenomeno del raddoppio della dimensione del seguente blocco da sottoporre a votazione. Si tratta comunque di un caso limite e facilmente rilevabile; tuttavia, rappresenta un rischio da non sottovalutare: se la votazione per il blocco successivo è bloccata, allora vuol dire che i delegati (eletti dall'intera rete di partecipanti) sono in disaccordo; poiché essi rappresentano la volontà dei singoli partecipanti, una nuova ronda di elezioni di delegati (rappresentanti la stessa identica demografica che ha portato alla situazione bloccante iniziale) potrebbe rimanere nuovamente irrisolta, portando allo stallo.

Poniamo questo aspetto a confronto con il quinto Pilastro poiché, in caso di stallo, è prevedibile un aumento temporaneo della quantità dei dati raccolti, che deve essere risolto entro un tempo sufficiente a permettere di continuare ad operare la blockchain con regolarità ed entro le politiche di protezione dei dati. Questo aumento di dati raccolti da parte dei *Data Controller* e *Data Processor* ha conseguenze anche nei precedenti Pilastri di Minimalità e di Esattezza dei dati. Infine, le norme GDPR sono molto stringenti sul tema della conservazione dei dati: è infatti necessario indicare una politica di ritenzione esplicita dei dati trattati.

Un altro aspetto interessante per l'interazione con il quinto Pilastro è il tema dell'immutabilità del *ledger*. Una volta che una transazione entra a far parte dello stato aggiornato di una blockchain, vi resta per tutta la durata di vita della stessa. Questo può rappresentare un altro rischio per la Limitazione di onservazione, se dovesse essere necessario la rimozione di informazioni registrate nei blocchi. D'altro canto, ogni blocco è necessario al suo successivo, quindi sussiste una legittimità nel conservare tutti i blocchi inalterati. Questo rimane un punto aperto nella nostra analisi finora. Bisogna stabilire se è necessario inserire dati sensibili all'interno dei blocchi, o se è possibile farne a meno.

2.2.1.6. Confidenzialità e integrità

Il sesto Pilastro è relativo alla sicurezza dei dati.

Nel caso di maggiore interesse, DPoS in una blockchain a consorzio, il maggior rischio di confidenzialità sussiste in fase di registrazione, con la trasmissione del valore della posta in gioco di ciascun partecipante.

Non rileviamo osservazioni particolari al caso delle blockchain: la trasmissione sicura di dati è un tema ben noto, che esula dall'ambito della nostra analisi.

2.2.1.7. Responsabilità

Infine, per il settimo Pilastro, nella configurazione consorzio e consenso DPoS, è quantomeno possibile individuare sia i *Data Controller* che i *Data Processor* nel gruppo di nodi delegati investiti dal ruolo di processare i dati di tutta la blockchain.

Qualora un *Data Subject* ritenesse opportuno far pervenire un reclamo, potrebbe rivolgersi ad uno o più nodi validatori. È interessante osservare che, mentre è facilmente individuato il destinatario del reclamo, non è altrettanto semplice capire come agire sulla base del reclamo stesso. Se, infatti, i dati presenti nel *ledger* derivano da un consenso distribuito, come può un individuo, in quanto *Data Subject*, chiederne una rettifica? Inoltre: come può il singolo rettificare una decisione fondata sul consenso di una moltitudine (peraltro, una moltitudine che rappresenta l'insieme di tutti gli utenti partecipanti)?

Questo rappresenta un rischio nella pratica, anche per le soluzioni a consorzio con DPoS. Senza chiare conseguenze di responsabilità, non è possibile stabilire come dare seguito ad eventuali reclami per far valere i Diritti di ciascun singolo *Data Subject*.

2.2.2. Analisi per Diritto GDPR

2.2.2.1. Diritto di Informazione

In accordo con il primo Diritto, vanno comunicate ai *Data Subject* tutta una serie di coordinate (informazioni esplicite riguardanti i Diritti, i dati di contatto, presenza o meno di sistemi decisionali automatizzati, etc.). Fra queste, osserviamo quelle che risultano maggiormente rischiose nel caso di maggiore interesse, quello del consorzio a consenso DPoS.

Identità e dati di contatto di *Data Controller*, *Data Processor* e *Data Protection Officer*: queste identità corrispondono a quelle dei nodi validatori eletti a delegati dall'intera rete; tuttavia, a seguito di successive votazioni, i *Data Controller* potrebbero variare nel tempo. Notando che tale cambiamento avviene solo per mezzo di votazioni alle quali ciascun *Data Subject* partecipa, dovrebbe essere semplice implementare in piena trasparenza degli aggiornamenti di identità dei *Data Controller*, qualora fossero necessari.

Politica di ritenzione: come visto in precedenza, la politica di ritenzione espone un rischio nel modello DPoS quando si verifica uno stallo. Ad aggravare la situazione, vi è il fatto che questa politica va resa nota nel momento iniziale della partecipazione del *Data Subject* alla blockchain, non dopo.

Spiegazione esplicita dei Diritti seguenti (rettifica, oblio, limitazione del trattamento, portabilità, opposizione, reclamo alle autorità competenti): come appena visto per la politica di ritenzione, deve essere possibile stabilire a priori ed esplicitamente che cosa avviene e come applicare ciascuno dei Diritti GDPR dei *Data Subject* al contesto delle blockchain.

Questi tre punti vanno risolti anche per via teorica, a priori, in modo da permetterne l'inclusione fra le informazioni esplicite necessarie al soddisfacimento del primo Diritto.

2.2.2.2. Diritto di Accesso

Per il secondo Diritto, i *Data Subject* possono richiedere conferma delle informazioni in possesso a *Data Controller* e *Data Processor*. Le richieste di accesso vertono sulle stesse identiche coordinate che vengono illustrate nel primo Diritto. Pertanto, manteniamo le stesse conclusioni del punto precedente.

Una peculiarità che osserviamo è la possibilità di creare un processo dedicato per l'accesso; tale processo può essere implementato al livello dei nodi validatori delegati, nel caso di una blockchain a consenso DPoS, e può essere un *"nice-to-have"* per velocizzare l'adesione alle leggi GDPR.

Notiamo inoltre, che nel caso di blockchain pubbliche, l'accesso è un'immediata conseguenza della trasparenza totale di questa configurazione. Tuttavia, abbiamo già constatato come le blockchain pubbliche soffrano di alcune incompatibilità con il GDPR, che le rendono impraticabili a questo scopo.

2.2.2.3. Diritto di Rettifica

Il terzo Diritto, ricollegabile al Pilastro dell'esattezza dei dati, può dare vita ad incompatibilità nel momento in cui consideriamo la possibilità di commettere errori umani da parte degli utenti. Ad esempio, un utente potrebbe effettuare una transazione con il wallet sbagliato e potrebbe voler correggere l'errore. Tuttavia, il *ledger* di una blockchain è immutabile.

Un caso del genere potrebbe essere tenuto in considerazione per sviluppi futuri riguardanti le blockchain in linea con il GDPR.

La stessa situazione si ripresenta per il Diritto all'Oblio e per quello di Opposizione.

Siamo dunque giunti ad un'ulteriore conclusione per la nostra analisi: il funzionamento delle blockchain va esteso per permettere l'applicazione dei Diritti di rettifica e all'oblio.

2.2.2.4. Diritto di Cancellazione, o Diritto all'Oblio

Uno dei Diritti più importanti nel GDPR è il cosiddetto *Right To Be Forgotten*, o Diritto all'Oblio.

Continuiamo l'analisi iniziata per il Diritto di rettifica con la seguente domanda: una volta che le transazioni entrano nel *ledger*, a chi appartengono?

Se al *Data Subject*, allora dovrebbe essere possibile eliminarle completamente una volta che viene richiesto di far valere il Diritto all'Oblio unitamente a quello di Opposizione.

D'altro canto, i blocchi presenti nel *ledger*, che raggruppano delle transazioni, entrano a far parte dello stato del *ledger* in modo immutabile e sono necessari per la validità della catena. Deve in qualche modo essere possibile eliminare solo le transazioni dai blocchi ma non i blocchi dalla catena, senza invalidare la blockchain.

Procediamo a restringere il campo alla configurazione di blockchain a consorzio con algoritmo di consenso DPoS e vedere cosa succede in fase di registrazione.

Abbiamo osservato come tale configurazione permetta di evitare che le informazioni più sensibili vengano scritte permanentemente nelle blockchain. Resta ora da analizzare il caso in cui un utente eserciti il Diritto all'Oblio e questo comporti uno sbilanciamento dei poteri di voto, quindi decisionali, dei nodi validatori delegati, o "testimoni". Infatti, ogni utente contribuisce a stabilire la commissione di nodi delegati tramite il proprio voto, direttamente proporzionale alla propria posta in gioco iniziale; come abbiamo visto, è necessaria la possibilità di verificare, in modo trasparente, la corretta assegnazione dei risultati.

Pertanto, potrebbe essere necessario mantenere il punteggio di reputazione degli utenti anche quando essi abbiano esercitato il proprio Diritto all'Oblio; oppure, è sempre possibile reindire la votazione o il ricalcolo dei voti.

2.2.2.5. Diritto di Limitazione del trattamento

Per il Diritto di Limitazione del trattamento, un *Data Subject* può contestare e richiedere l'interruzione dell'elaborazione dei propri dati da parte dei *Data Controller* e *Data Processor*.

Un tale Diritto può avere delle conseguenze in una blockchain: non sarà più possibile effettuare nuove transazioni che contengano dati del *Data Subject* in questione; e gli eventuali blocchi ancora in corso di essere validati dovranno essere scartati.

Ciò equivale ad un congelamento dell'attività del *Data Subject* sulla blockchain, per la durata della limitazione richiesta.

Da notare che in presenza di molteplici *Data Controller* e *Data Processor*, la richiesta deve in qualche modo pervenire a tutti i nodi validatori. In una blockchain a consorzio con un numero limitato di partecipanti ci si può ragionevolmente aspettare che la richiesta venga automaticamente estesa a tutti i *Data Controller* e *Data Processor*, a meno che il *Data Subject* non abbia specificato di voler limitare il trattamento da parte di solo uno di essi.

In quest'ultimo caso, va considerata la possibilità che una larga parte degli utenti potrebbe fare una simile richiesta, con il risultato di sbilanciare la distribuzione del lavoro nella rete *peer-to-peer*.

A parte queste osservazioni, il quinto Diritto è rilassato rispetto ai precedenti Diritti di rettifica e di oblio. Per tale motivo, l'immutabilità del *ledger* non riveste un ruolo problematico al soddisfacimento di questo Diritto.

2.2.2.6. Diritto di Portabilità

Per il Diritto di Portabilità, l'utente può richiedere il trasferimento dei propri dati da un *Data Controller* ad un altro. Il trasferimento deve avvenire in maniera automatizzata, in un formato elettronico leggibile da una macchina.

Abbiamo già visto, per i Diritti di rettifica e di oblio, come l'immutabilità del *ledger* ponga dei netti limiti a ciò che è consentito fare a posteriori in una blockchain.

Anche nel caso della portabilità ci troviamo in questa situazione: nel caso in cui la portabilità dovesse, per qualche motivo, essere applicata a singole transazioni presenti all'interno di un blocco della catena, allora dovrebbe essere messo in atto lo stesso meccanismo di modifica descritto in precedenza.

2.2.2.7. Diritto di Opposizione

Per il Diritto di Opposizione, un *Data Subject* può richiedere che il trattamento dei suoi dati venga interrotto. Generalmente, si tratta di un Diritto legato a quello di cancellazione o oblio.

Pertanto, vanno ripetute le stesse considerazioni viste nei diritti di rettifica, oblio e portabilità.

2.2.2.8. Diritto di Opporsi al Trattamento Automatizzato

Nell'ultimo Diritto, non troviamo particolari difficoltà di applicazione. Nelle blockchain non è sempre presente un meccanismo di profilazione automatico. Nel caso di maggior interesse delle blockchain federate e consenso DPoS, la profilazione avviene nella fase di registrazione e corrisponde alla conversione da posta in gioco iniziale del *Data Subject* a punteggio di reputazione, o potere di voto.

Al fine di permettere l'opposizione alla profilazione automatica, sarà sufficiente effettuare, o verificare, manualmente la conversione, il ché dovrebbe essere sempre possibile.

Parte III.

Conclusioni

3. Considerazioni finali

Dal confronto fra alcune specifiche dei sistemi DLT (algoritmi di consenso e tipo di accesso) e delle leggi GDPR (in forma di Diritti e Pilastri), sono emerse delle considerazioni che riassumiamo in questa sezione finale.

Da un lato, troviamo dei punti di attenzione, ovvero le potenziali incompatibilità fra la tecnologia in questione e le leggi di protezione dei dati. Dall'altro, sono emerse alcune osservazioni utili a tracciare un possibile percorso futuro di armonia fra DLT e GDPR.

3.1. Traccia delle incompatibilità odierne fra GDPR e DLT

Dalla nostra analisi, sono risultati i seguenti punti di attenzione.

Non sono garantiti a priori i Pilastri di (3) Minimalità, (4) Esattezza e (5) Limitazione di conservazione e i Diritti di (3) Rettifica, (4) Oblío, (6) Portabilità e (7) Opposizione

L'analisi ha evidenziato che non sono garantiti a priori:

- i Pilastri di (3) Minimalità, (4) Esattezza e (5) Limitazione di conservazione;

- i Diritti di (3) Rettifica, (4) Oblío, (6) Portabilità e (7) Opposizione.

I tre Pilastri sono in contrasto con la natura immutabile del *ledger* in un sistema DLT, in quanto in esso vengono archiviate tutte le transazioni per una quantità indefinita di tempo, ovvero per l'intero ciclo di vita del sistema DLT, non conosciuto a priori; e non è possibile modificare una transazione una volta che essa faccia parte della catena di blocchi, a meno di estendere le operazioni concesse sul *ledger* e dal sistema DLT.

Lo stesso si riflette nei quattro Diritti sopracitati, poiché anch'essi vertono sulla capacità di alterare i dati trattati, che in questo contesto sono contenuti in un *ledger* immutabile.

Inoltre, per il (1) Diritto di Informazione, nelle leggi GDPR è previsto che l'utente finale sia messo al corrente di tutti i propri Diritti e di come vengano trattati i

propri dati, prima che il trattamento abbia inizio. Per queste incompatibilità, può essere utile la predisposizione di un sistema che, a priori, fornisca delle garanzie di *eventuale conformità* con i Pilastri e i Diritti critici che abbiamo evidenziato. Un'altra opzione è di caratterizzare la conservazione dei dati trattati tramite delle condizioni esplicite, anziché degli intervalli di tempo prestabiliti. Si tratta, tuttavia, di soluzioni ancora parziali e di approcci che richiedono una certa flessibilità da parte delle applicazioni basate su sistemi DLT.

Infine, dal momento che è richiesta una garanzia a priori per il primo Diritto, questi punti di attenzione possono essere studiati in fase di progetto degli algoritmi di consenso e della configurazione di rete da utilizzare.

3.2. Osservazioni utili per il futuro

Dall'analisi effettuata, possiamo delineare i seguenti quattro passaggi come punto di partenza per rendere i sistemi DLT compatibili con il GDPR.

In primo luogo, indichiamo la possibilità di sfruttare la configurazione a consorzio (detta anche federata) nei sistemi DLT.

In secondo luogo, è emerso come sia utile adottare un modello di consenso diverso dal PoW; ciò è sempre possibile nelle blockchain di tipo *permissioned*, di cui la configurazione a consorzio fa parte.

In terzo luogo, vi è la possibilità di utilizzare un algoritmo di consenso derivato dal PoS, che incapsuli le informazioni sensibili in informazioni pseudonimizzate in fase di registrazione alla blockchain federata; l'esempio analizzato è il DPoS; o, in alternativa, altrettanto valida o migliore in base al contesto, la possibilità di sfruttare il consenso PoA o una sua variante, per un sistema di selezione slegato dalla quantità di valuta in possesso ai partecipanti.

Infine, come quarto punto,

- per i modelli basati su DPoS: la riservatezza delle informazioni pseudonimizzate in fase di registrazione e, allo stesso tempo, la possibilità di effettuare verifiche trasparenti del processo di conversione da dato sensibile a dato pseudonimo;

- per i modelli basati su PoA o suoi derivati: la protezione delle chiavi private e la possibilità di derivare una variante nella quale i nodi validatori abbiano una funzione del tutto simile a quella dei nodi "delegati" del modello DPoS.

Risolvere i punti aperti corrisponde al soddisfacimento del (1) Diritto di Informazione, in quanto diventerà possibile informare i *Data Subject* circa l'intera operatività in materia di protezione dei dati al momento della registrazione degli stessi alla blockchain *permissioned*.

A titolo d'esempio, citiamo i seguenti due progetti europei.

Trace4EU

Si tratta di un consorzio attualmente composto da 30 partner dislocati in 14 paesi. [Tra]

Gli obiettivi del progetto sono di migliorare la coesione sociale ed economica dei Paesi in Europa, sfruttando i sistemi DLT per la trasformazione digitale. Per conseguire ciò, il gruppo si prefigge di migliorare le operazioni digitali in termini di inclusività, trasparenza e sicurezza. L'uso delle blockchain in questo contesto contribuisce positivamente alla tracciabilità di beni e merci, inclusi documenti e dati, e alla trasparenza dei flussi di beni, che i cittadini possono verificare in autonomia.

European Blockchain Services Infrastructure (EBSI)

EBSI è l'infrastruttura europea per i servizi basati su blockchain. [EBS]

Fondata nel 2018 con il contributo di 29 paesi (i paesi dell'Unione, il Liechtenstein e la Norvegia) e della Commissione Europea, dando origine alla *European Blockchain Partnership (EBP).*

L'obiettivo di questa partnership è di sfruttare le blockchain per fornire servizi di interesse pubblico e privato ai cittadini di tutte le nazioni coinvolte, creando un ecosistema internazionale e affidabile per i cittadini europei.

Ringraziamenti

In primo luogo, un vivo ringraziamento va alle Professoresse e ai Professori, dei quali sentirò la mancanza, che mi hanno fornito i più utili consigli durante questo percorso di Università.

In secondo luogo, un ringraziamento di cuore va alle persone che ho conosciuto all'Università, studenti e non.

Spero di trovarmi presto, di nuovo, in un contesto dove si condivida un senso di piacere della scoperta e di curiosità per la tecnologia come quello che ho respirato negli anni in cui ero in sede.

Bibliografia

[BSALL23] Rahime Belen-Saglam, Enes Altuncu, Yang Lu, and Shujun Li. A systematic literature review of the tension between the gdpr and public blockchain systems. *Blockchain: Research and Applications*, 4(2): 100129, 2023, https://www.sciencedirect.com/science/article/pii/S2096720923000040.

[Cha79] Computer systems established, maintained, and trusted by mutually suspicious groups, ELECTRONICS RESEARCH LABORATORY, College of Engineering, University of California, Berkeley, 94720. https://chaum.com/wp-content/uploads/2022/02/techrep.pdf.

[Com] What is a data controller or a data processor?, European Commission, European Commission. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_en.

[EBS] EBSI, EBSI. https://hub.ebsi.eu/.

[Inv] Proof of stake, Investopedia, Investopedia. https://www.investopedia.com/terms/p/proof-stake-pos.asp.

[Sev] What are the 7 main principles of gdpr?, GDPR EU, GDPR EU. https://www.gdpreu.org/7-main-data-protection-principles-under-gdpr/.

[SV17] Blockchain technology handbook, BlockchainHub, BlockchainHub. https://www.studocu.com/row/document/tribhuvan-vishwavidalaya/computer-science-information-technology/blockchaintechnologyhandbook/65121443.

[Tra] Trace4eu, Trace4EU, Trace4EU. https://trace4eu.eu/.