Blockchain e Pubblica Amministrazione: verso un futuro decentralizzato

AWARE

AUTRICI

Sofia Brunelli

Luisa Gaburova

CURATRICI E CURATORE

Alice Grieco

Alessia Baccani

Edoardo Crivellaro

SI RINGRAZIANO

Alessia Sementilli

Svetlana Falconi

MAGGIO 2021

INDICE

ABSTRACT

Gli autori del seguente paper si pongono l'obiettivo di analizzare e proporre una soluzione di implementazione e utilizzo della tecnologia *Blockchain* nel settore della Pubblica Amministrazione italiana. Particolare attenzione viene rivolta al quadro normativo nazionale di riferimento circa l'utilizzo di sistemi Blockchain e *Smart contracts* e alla questione della mancanza di linee guida specifiche in materia. Un'approfondita ricerca riguardo le diverse tipologie di Blockchain, ad oggi esistenti, porta alla luce una scarsa comprensione generale delle sue potenzialità e dei suoi benefici, nonché una necessità di standardizzazione dei processi di migrazione dai tradizionali sistemi di raccolta dati centralizzati e frammentati a un sistema pubblico decentralizzato, che garantisce alti standard di vigilanza e trasparenza sull'utilizzo dei dati appartenenti alle organizzazioni governative e ai cittadini.

La prima parte del paper è costituita da un capitolo nozionistico in cui vengono illustrate le principali caratteristiche della tecnologia Blockchain, illustrando le differenze tra pubbliche, private e ibride. La seconda parte è dedicata alla legislazione in materia di Blockchain e smart contract a livello italiano, seguita da un paragrafo sulla compatibilità di tale tecnologia con il Regolamento generale Europeo per la protezione dei dati personali (GDPR). Il secondo capitolo si conclude con un approfondimento sul tema dell'identità digitale applicata a Blockchain e il nuovo paradigma della *Self Sovereign Identity* (SSI). In conclusione, vi è un quadro generale di opportunità e limiti applicativi di questa tecnologia nel settore pubblico, citando il caso studio estone.

Infine, gli autori del paper presentano un set di proposte di policy con l'obiettivo di rendere più chiara la legislazione italiana relativa a Blockchain e Smart Contract, con particolare riferimento al processo di identificazione digitale e all' individuare un tipo di Blockchain adatto al contesto della Pubblica Amministrazione. La difficoltà di quest'ultima proposta risiede nella complessa conciliazione dell'approccio tipicamente decentralizzato della tecnologia Blockchain con quello centralizzato degli organi pubblici.

INTRODUZIONE

Uno dei principali motori della trasformazione digitale è sicuramente la tecnologia Blockchain. Questa possiede tutte le caratteristiche di una *disruptive technology*: la sua implementazione di fatto altera il modo in cui operano industrie, governi e consumatori. Sebbene inizialmente il suo utilizzo fosse relegato al campo delle criptovalute, negli ultimi anni è stata esplorata la sua pervasività sia in ambito pubblico che privato.

Il nuovo paradigma imposto dalla tecnologia blockchain è basato sulla disintermediazione e sull'elevato grado di trasparenza di ciò che avviene in essa. La natura decentralizzata delle reti basate su Blockchain stride con l'approccio centralizzato usato dagli enti governativi. L'adozione di un'infrastruttura di rete pubblica basata sulla tecnologia Blockchain segnerebbe il passaggio da un modello accentrato a uno decentrato di gestione delle informazioni e delle transazioni. Inoltre, un database pubblico decentralizzato potrebbe favorire lo sviluppo di nuove modalità di governo delle relazioni e di gestione delle transazioni sia tra gli organi della Pubblica Amministrazione sia tra cittadini e organizzazioni terze. Tra i potenziali benefici perseguibili attraverso l'implementazione e l'utilizzo della Blockchain ricordiamo: trasparenza, sistemi automatizzati di rilevamento di frodi e manipolazione dei dati e ostacolo alla corruzione. Infatti, una rete Blockchain pubblica permette l'accesso ai dati a tutti i membri che vi partecipano e offre una panoramica completa e dettagliata di tutte le transazioni effettuate. L'archiviazione dei dati in registri distribuiti dà la possibilità di verificare la cronologia delle transazioni, rappresentando un deterrente ai comportamenti scorretti o fraudolenti. L'accesso e la verificabilità dei dati consentono ai diversi attori un maggiore controllo su tutti i processi e l'aumento di fiducia nelle relazioni, ma anche una migliore capacità predittiva circa rischi o eventi futuri. L'adozione della Blockchain consente di ridurre molti costi e l'incidenza dell'errore umano grazie all'automatizzazione dei processi. Infine, una rete Blockchain pubblica si caratterizza per i suoi alti livelli di resilienza e sicurezza informatica, integrità e qualità dei dati. La presenza di copie di un set di informazioni su molti nodi anziché in un unico database centrale permette di ridurre la perdita o la manipolazione di dati e informazioni derivanti da attacchi hacker o tentativi di modifica o manomissione dei dati da parte di un partecipante della rete.

Tuttavia, tale tecnologia, applicata nell'ambito della pubblica amministrazione, presenta una serie di criticità, derivanti da fattori organizzativi interni, e una scarsa comprensione generale dei benefici apportati dalla Blockchain. Quest'ultima rappresenta un'opportunità anche per il settore pubblico, numerosi governi hanno avviato progetti pilota a supporto di processi governativi e amministrativi di varia natura. Il paper si propone di analizzare lo stato dell'arte delle applicazioni della tecnologia Blockchain a livello pubblico e con particolare riferimento al quadro normativo italiano, allo scopo di delineare un set di proposte programmatiche finalizzate ad accelerare e standardizzare l'adozione di una rete blockchain nazionale.

1. BLOCKCHAIN E REGISTRI DISTRIBUITI

Blockchain è stata concepita nel 2008 da Satoshi Nakamoto e può essere definita come un database decentralizzato, una rete *peer-to peer* che memorizza un registro delle transazioni. La principale differenza con i sistemi centralizzati è che, invece di utilizzare un'istituzione intermediaria, come le banche per coordinare le transazioni, Blockchain consente a qualsiasi individuo di accedere a un registro delle attività registrate[1]e delle transazioni. Nelle reti decentralizzate, come Blockchain, i dati non vengono raccolti in un unico posto, ma in singoli "nodi" e ognuno di essi è una copia di un singolo set di dati. Una volta raggiunto un certo numero di transazioni approvate, viene formato un nuovo "blocco". Successivamente i blocchi vengono concatenati e bloccati crittograficamente insieme formando una storia cronologica degli eventi, ciò significa che la stessa storia degli eventi vive su ogni nodo del sistema. Chiunque può diventare un "nodo" e partecipare alla Blockchain installandola sul proprio server e avere libero accesso alla rete, in modo da verificare esattamente cosa è successo. Le caratteristiche più interessanti e dirompenti di tale tecnologia (basata sulla decentralizzazione) sono la trasparenza, la sicurezza e l'immutabilità dei dati. Le transazioni di dati che avvengono tra i blocchi della catena possono essere di qualsiasi tipo, ma le più note riguardano le criptovalute come *Bitcoin*, motivo per cui molte persone credono che Blockchain e Bitcoin siano sinonimi. In realtà, il campo finanziario è solo una delle possibili applicazioni di questo sistema innovativo e apparentemente democratico: chiunque potrebbe infatti partecipare a una Blockchain e avere accesso a una copia di essa. Tutti possono gestire più nodi (o solo uno) e chiunque può finire per scrivere il blocco successivo. In questo tipo di rete peer-to-peer l'idea di fiducia è legata al sistema piuttosto che a un singolo individuo o istituzione, poiché si fa affidamento su tutti i partecipanti alla rete che verificano costantemente i dati. In effetti, la resilienza del sistema si basa sul fatto che così tante persone lo stanno assicurando in un dato momento.

Questa tecnologia si fonda sul concetto di fiducia e trasparenza poiché Blockchain consente di tracciare ogni transazione fino a quando non viene convalidata e aggiunta a un blocco, gli utenti sono in grado di vedere se si è verificato un errore e dove si è verificato nel processo.

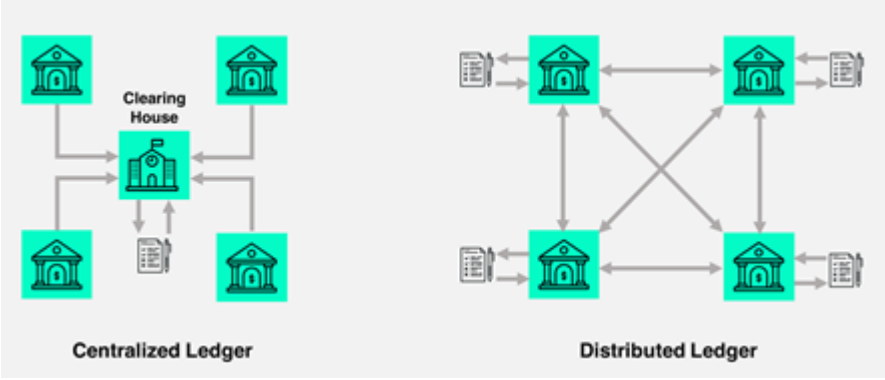

Immagine 1 - Transactions on a Blockchain. Source: *Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH*.

[1] Il termine *asset* può essere inteso in molti modi: non solo come denaro, ma anche come proprietà, custodia, contratti, beni e persino informazioni di identificazione personale.

1.1 BLOCKCHAIN PUBBLICHE

Le Blockchain pubbliche (*Public Permissionless Blockchains*) sono accessibili a tutti senza restrizioni. Tutti hanno la possibilità di leggere ed effettuare transazioni o partecipare al meccanismo di consenso. Quelle pubbliche hanno natura globale e rappresentano il modello di Blockchain originario. La rivoluzione introdotta da questa tecnologia è data dal suo potere di disintermediazione e dalla scarsità delle risorse. La Blockchain permette di fare transazioni finanziarie o di asset digitali senza il ricorso a un ente centrale, che funge da intermediario con funzioni di controllo e garanzia. Nei tradizionali sistemi di pagamento elettronico, il controllo centralizzato delle transazioni permette di evitare fenomeni di *double spending*[2] o contraffazione; la Blockchain pubblica consente, invece, di raggiungere questo risultato in un sistema completamente decentralizzato. Prendendo come riferimento la Blockchain pubblica per eccellenza, Bitcoin, tra i suoi membri partecipanti ci sono anche i cosiddetti *miners*, i quali dietro compenso si impegnano a risolvere algoritmi matematici per poter validare le transazioni secondo un meccanismo chiamato *Proof of Work*. Quando viene comunicata la soluzione dal primo miners che riesce a risolvere l'algoritmo, gli altri nodi del network verificano la soluzione in base ad un meccanismo "democratico": il 51% deve concordare sulla sua correttezza. Quando il consenso è raggiunto, le transazioni convalidate e verificate vengono inserite come unico "blocco" nel registro distribuito, aggiungendosi ai blocchi creati in precedenza. Non vi è dunque alcun ente o istituzione centrale che controlli la correttezza delle transazioni, poiché questa funzione viene svolta dagli utenti stessi. Si realizza così una "decentralizzazione delle funzioni amministrative e di supervisione". Il registro sfruttato da una Blockchain pubblica è caratterizzato dal fatto che lo stesso set di informazioni è presente in tutti i nodi: ciascun partecipante ne detiene una copia aggiornata e autentica, con il risultato che non esiste una versione centrale o ufficiale del registro, ma migliaia di copie egualmente valide ed "ufficiali" poiché può essere consultato nella sua interezza e in ogni momento da chiunque, compresi soggetti non partecipanti alla Blockchain. Infine, poiché i blocchi sono crittograficamente collegati l'uno all'altro, ogni eventuale modifica di un qualsiasi blocco si riverbererebbe su tutti gli altri, rendendola immediatamente nota ai partecipanti, quindi anche la cancellazione o la modifica delle informazioni immesse è pressoché irrealizzabile. In una Blockchain pubblica, l'immutabilità dei dati registrati è una proprietà insita nell'architettura stessa della tecnologia, avente carattere non assoluto, ma relativo: il livello di immutabilità cresce all'aumentare del numero di partecipanti al network. Una Blockchain pubblica di grandi dimensioni (attualmente le più importanti sono Bitcoin ed *Ethereum*) basa la propria sicurezza sia sugli aspetti tecnici sia su meccanismi di incentivazione dei partecipanti: come nella teoria dei giochi, ogni utente è costretto ad agire correttamente. I miners, che permettono la gestione decentralizzata della piattaforma Blockchain, vengono retribuiti in criptovalute. Qualora uno di essi dovesse tentare di modificare il registro a proprio vantaggio, sarebbe immediatamente noto al resto dei partecipanti,

[2] La doppia spesa in economia è una truffa che consiste nello spendere lo stesso titolo valutario due o più volte. Nell'economia tradizionale sono stati gli istituti finanziari centralizzati a fornire un controllo che evitasse la doppia spesa mentre è un potenziale problema in uno schema di cassa digitale, in cui uno stesso singolo token digitale potrebbe essere speso più di una volta presso venditori diversi (in mancanza di un organo o di un sistema certificatore) perché esso è costituito da un file che può essere duplicato o falsificato. Fonte: Wikipedia

scatenando la perdita di fiducia nella Blockchain e l' immediata svalutazione della criptovaluta ad essa collegata. La Blockchain pubblica risulta essere una tecnologia estremamente innovativa, che ha introdotto un nuovo paradigma di organizzazione sociale e di gestione dei dati. Una struttura simile, tuttavia, ha un costo energetico notevole: il funzionamento della Proof of Work impone il costante utilizzo, da parte dei nodi miners, di molta energia elettrica. Altro limite è basato sull'aspetto normativo: imputare la responsabilità a un individuo che ha commesso un atto illecito su una rete decentralizzata è pressoché impossibile in quanto le Blockchain pubbliche non prevedono l'identificazione personale degli utenti, poiché questi effettuano le transazioni attraverso chiavi crittografiche[3], che permettono di operare in anonimato. Le autorità pubbliche non potrebbero dunque intervenire unilateralmente in una rete decentralizzata per assicurare il rispetto delle norme giuridiche, sempre che esista una legge territorialmente applicabile.

1.2 LE BLOCKCHAIN IBRIDE E PRIVATE

Le Blockchain ibride (conosciute anche come *Public Permissioned Blockchains*) sono Blockchain in cui esistono non c'è parità in termini di potere operativo. Ci sono i nodi gestori del sistema e quelli partecipanti, che possono solo consultare i dati presenti nel registro. Esistono varie soluzioni per la validazione dei blocchi, ad esempio il voto di maggioranza dell'insieme dei membri che ne costituiscono i nodi. Una Blockchain ibrida può essere pubblica per la lettura delle informazioni, ma limitata ai partecipanti quando si tratta di eseguire transazioni sulla rete. In sintesi, i nodi non sono posti sullo stesso piano rispetto alle operazioni che possono compiere nel sistema.

Si pensi, ad esempio, a registri pubblici in cui gli enti della Pubblica Amministrazione partecipano nell'inserire (o validare) informazioni, che però sono destinate per natura alla pubblicità per un obbligo di trasparenza nei confronti dei cittadini. Su una Blockchain Ibrida il registro è replicato su tutti i nodi ed è liberamente accessibile e consultabile, vale a dire che qualsiasi modifica sarebbe immediatamente nota ai partecipanti, al pari di quanto avviene nelle Blockchain pubbliche.

Infine, le Blockchain private (*Private Permissionless Blockchains*) che non sono accessibili al pubblico. Solo i membri che ne fanno parte sono autorizzati a leggere ed eseguire operazioni. Una tipologia di Blockchain piuttosto antitetica rispetto al significato intrinseco del termine che prelude trasparenza, immutabilità e apertura al pubblico globale.

In una Blockchain privata esiste un'autorità che gestisce il registro e che può dunque ripristinare e modificare le transazioni senza difficoltà: questo comporta certamente una serie di vantaggi, ma rende davvero minima la differenza con un comune database gestito secondo una logica centralizzata. Le Blockchain ibride e private hanno, quindi, natura centralizzata e la maggioranza dei partecipanti ha un ruolo passivo perché non prendono parte alla gestione del database. In una Blockchain Ibrida questi ultimi avranno comunque la possibilità di consultare il registro nella sua

[3] Tra i metodi di sicurezza della blockchain c'è anche la crittografia a chiave pubblica. La chiave pubblica è un indirizzo sulla blockchain. I token di valore inviati nella rete vengono registrati come appartenenti a questo indirizzo. Invece la chiave privata è come una password che permette al suo proprietario di accedere alle sue risorse digitali oppure di interagire con le varie funzionalità della blockchain. Fonte: Wikipedia.

interezza in qualsiasi momento e quindi di esercitare una forma di vigilanza sulla sua gestione dei dati da parte dei nodi gestori, senza poter prendere parte al meccanismo di validazione e verifica delle informazioni registrate. La sicurezza di Blockchain ibride e private può essere garantita solo attraverso i meccanismi tradizionali o l'integrazione di sistemi IoT che registrano dati in tempo reale e li inviano alla rete Blockchain. Sia nelle Blockchain ibride che in quelle private la caratteristica della decentralizzazione viene a mancare e la sicurezza del network è direttamente proporzionale alla sicurezza dei sistemi sui quali si appoggiano i nodi validatori. Entrambe queste tipologie di blockchain non si possono definire immutabili poiché non c'è un'effettiva impossibilità di apporre modifiche al registro, tuttavia esiste l' impossibilità di operare modifiche al registro senza che ciò venga a conoscenza dei partecipanti.

1.3 L'EFFICACIA LEGALE DEGLI SMART CONTRACTS

Ethereum è una delle blockchain più famose e utilizzate nel mondo reale per gli scambi economici, ma anche per scambiare asset digitali e offrire servizi di storage di dati sicuri e decentralizzati[4]. Questa rete funziona attraverso l'uso della sua potenza di calcolo che viene pagata in Ether, che funge quindi sia da criptovaluta che da carburante. L'aspetto innovativo di questa blockchain è la programmabilità. Gli sviluppatori hanno la possibilità di creare applicazioni web decentralizzate chiamate *Dapps*[5], cioè applicazioni che non sono controllate da persone, aziende o istituzioni, e dove i dati degli utenti sono tenuti al sicuro. Quindi la principale differenza con la rete Bitcoin è che Ethereum consente di eseguire non solo transazioni finanziarie ma anche la costruzione di applicazioni e l'esecuzione di contratti intelligenti, noti come *Smart Contracts*.

In uno Smart Contract le clausole del contratto vengono elaborate da un software e sintetizzate in un codice appropriato. Quando le condizioni del contratto vengono soddisfatte, si esegue automaticamente senza la necessità di un intervento umano. Nick Szabo negli anni '90 coniò per la prima volta il termine Smart Contract[6]: "protocollo di transazione informatizzato che esegue i termini di un contratto in modo automatico" che può essere registrato su Blockchain e avvalersi dunque di caratteristiche specifiche quali immutabilità, autosufficienza e verificabilità. Uno Smart Contract non corrisponde al contratto scritto di natura giuridica, ma al software (o protocollo informativo) sviluppato per l'esecuzione dello stesso. Per chiarire, uno Smart Contract è un software per automatizzare l'esecuzione di obbligazioni contrattuali. In sostanza sono automatismi informatici e inizialmente non vi erano legami con la tecnologia blockchain. Con l'avvento di Ethereum, blockchain con la quale nasce la possibilità di sviluppare ed eseguire smart contract

[4] Ethereum è la seconda più grande piattaforma di criptovaluta per capitalizzazione di mercato, dietro a Bitcoin. È una blockchain open source decentralizzata e che permette la costruzione di applicazioni e l'implementazione degli Smart Contracts. Ether (ETH) è la criptovaluta generata dai minatori di Ethereum come ricompensa per i calcoli eseguiti per proteggere e aggiungere blocchi alla blockchain. Fonte: Wikipedia.

[5] Le Dapp su Ethereum sono applicazioni web supportate da contratti intelligenti di Ethereum. Invece di utilizzare un server o un database centralizzato, queste applicazioni si basano sulla blockchain come *back-end* per la logica e l'archiviazione del programma. Ciò porta ad applicazioni potenzialmente inarrestabili: chiunque può distribuire una copia del *front-end* e collegarla liberamente alla rete pubblica Ethereum. Fonte: Wikipedia.

[6] I. Bashir,Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2nd Edition, Packt, ISBN978-1788839044, 2018.

decentralizzati, questi ultimi si sono inevitabilmente legati alla tecnologia inventata da Satoshi Nakamoto. Tali applicativi basati su blockchain sono progettati per eseguire e mantenere il sistema trasparente, sicuro e affidabile, eliminando così la necessità di coinvolgere una terza parte che funge da oracolo o validatore di una determinata transazione. Obiettivi economici correlati all'utilizzo degli Smart Contracts includono la riduzione dei costi giudiziali, danni da frode e arbitrati. Inoltre, uno smart contract è un software le quali funzioni replicano gli obblighi di natura contrattuale tra due o più parti, come la restituzione di un prestito; vengono eseguiti in automatico, indipendentemente dal volere delle parti. Dunque, esprimono a pieno il principio *code is law*, ovvero il codice è legge. L'efficacia legale dei contratti digitali, ad oggi è un tema molto dibattuto e controverso nonostante vi sia una normativa italiana che fornisce una cornice regolatoria per favorire l'adozione di questo innovativo strumento da parte di enti pubblici e privati. Restano attualmente solo alcune criticità come l'assenza di Linee Guida dell'Agenzia per l'Italia Digitale, tuttavia rimane lecito e legale adottare gli Smart Contracts nella propria attività di impresa.

2. NORMATIVA ITALIANA

Le molteplici applicazioni della tecnologia blockchain e la loro pervasività hanno messo in rilievo la necessità di un impellente intervento normativo in materia. Una simile tecnologia ha posto ardue sfide nei confronti dell'ordinamento giuridico mettendo in discussione, in particolare, principi quali la certezza del diritto.

Il quadro giuridico italiano relativo a Blockchain e Smart Contracts non è ben definito. Tuttavia, una tale incompletezza del dettato normativo è cosa comune a livello internazionale, ad eccezione di qualche stato federale americano, e per di più risulta essere in linea con le prescrizioni europee in materia come si vedrà più avanti.

Le difficoltà che i legislatori incontrano sono duplici. Da un lato si rischia che un quadro giuridico altamente dettagliato limiti le potenzialità di queste tecnologie dette *disruptive*; dall'altro alcune caratteristiche intrinseche di Blockchain e Smart Contracts possono incontrare limiti tecnico-giuridici nella legislazione nazionale, in particolare in materia di diritto contrattuale o di protezione dei dati personali. In un tale contesto, il ruolo del diritto risulta essere di vitale importanza: esso ha il compito di smorzare l'impatto socio-economico di blockchain e smart contract e allo stesso tempo favorire l'innovazione tecnologica affinché le potenzialità di questi strumenti possano essere dispiegate appieno.

Per orientarsi al meglio all'interno di un quadro normativo incerto è bene citare le tre fonti del diritto italiano ed europeo che concernono blockchain e smart contract:

1. Il Decreto Legislativo n. 82 del 7 marzo 2005, o "Codice dell'Amministrazione Digitale" (CAD);
2. Il Decreto-legge 14 dicembre 2018, n. 135, coordinato con la legge di conversione 11 febbraio 2019, n. 12, recante «Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione.», o Decreto Semplificazioni;
3. Infine, il Decreto Semplificazioni rimanda al regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014 o regolamento "electronic IDentification Authentication and Signature" (eIDAS).

È importante ricordare che nel diritto civile italiano, affinché un atto possa vincolare due soggetti, è richiesta la forma scritta ai sensi dell'articolo 2702 del Codice Civile. A tal fine, il Codice dell'Amministrazione Digitale delinea processi idonei a dare validità ai documenti informatici al fine di assicurare la medesima efficacia probatoria della scrittura privata. In particolare, l'art. 20, comma 1-bis considera un documento elettronico in forma scritta quando il firmatario utilizza non solo una firma elettronica qualificata, ma anche una elettronica avanzata. La prima è definita ai sensi dell'art. 1, comma 1, lettera q-bis, come l'*insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.* La seconda, ai sensi dell'art. 1, comma 1, lettera r è definita come *un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.* Un esempio di firma digitale elettronica avanzata è la firma grafometrica apposta sui tablet con una penna elettronica, mentre uno di firma digitale qualificata è una card con chip che contiene alcuni dati anagrafici e il codice fiscale, come la Tessera Sanitaria.

Inoltre, lo stesso articolo 20 del CAD stabilisce che il medesimo valore è riconosciuto alla firma digitale e a un documento formato secondo i requisiti stabiliti dall'Agenzia per l'Italia Digitale (AGID), previa identificazione informatica del suo autore, in modo tale da garantire la sua sicurezza, integrità e immodificabilità e, in maniera manifesta e inequivoca, la riconducibilità all'autore.

Infine, l'art. 20, comma 1-bis, del CAD stabilisce che *l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità.* Perciò crittografia asimmetrica, hash e decentralizzazione del database potrebbero essere elementi sufficienti a garantire l'integrità e l'immutabilità del documento in esame e dunque la sua idoneità a soddisfare il requisito della forma scritta.

Per estendere l'analisi alla legislazione più recente, la Legge di conversione 11 febbraio 2019, n. 12, del Decreto Legge 14 dicembre 2018, n. 35 (il c.d. Decreto Semplificazioni), all'art. 8-ter, comma 2, dopo aver fornito una prima definizione di Smart Contract stabilisce che gli stessi *soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'AGID con linee guida*.

Gli smart contract, pur richiamando la nozione di contratto, sono programmi per computer e la loro efficacia probatoria, dunque il loro valore scritto, sono subordinati alla preventiva identificazione informatica delle parti interessate, attraverso alcuni requisiti che devono essere indicati dall'AGID. Tuttavia tali linee guida, che avrebbero dovuto essere pubblicate poco dopo l'approvazione del decreto legge, non sono ancora state rilasciate, rendendo gli sforzi definitori del legislatore un esercizio puramente teorico.

Più nello specifico, l'articolo 8-ter riporta una definizione di tecnologie basate su registri distribuiti, precisando che la memorizzazione di un documento informatico via DLT *produce gli effetti giuridici*

della validazione temporale elettronica come stabilito dell'articolo 41 del Regolamento Ue 910/2014 sull'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel mercato interno (c.d. regolamento eIDAS). Per fare chiarezza è bene ricordare che la validazione temporale elettronica, anche detta *timestamp*, secondo la definizione dell'art. 3, paragrafo 33, del regolamento eIDAS, consente di combinare la data e l'ora con dati in forma elettronica insieme ad altri dati in forma elettronica, al fine di dimostrare l'esistenza degli stessi in quel momento specifico.

L'articolo 8-ter relega dunque la tecnologia blockchain a un ruolo di semplice "validazione temporale" nell'ordinamento italiano, limitandone la portata euristica e il suo carattere innovativo. Si tratta di un riconoscimento normativo che, sebbene vada accolto con favore, era già insito nella natura dei registri distribuiti, creati proprio per dare garanzia dell'avvenimento di un dato fatto in una determinata data.

A livello comunitario, il già citato regolamento eIDAS disciplina l'uso di firme elettroniche, identità digitale e contenuti elettronici per armonizzarne l'utilizzo attraverso le frontiere nel mercato unico. Il regolamento risulta essere rilevante per il quadro normativo blockchain per i seguenti motivi:

1. Il contenuto della blockchain è un documento elettronico formato da hash e dati. Secondo il regolamento eIDAS, i dati presenti su Blockchain, memorizzati in blocchi, sono un "documento elettronico", poiché questo è definito dall'art. 35 del regolamento stesso come qualsiasi contenuto memorizzato in forma elettronica;
2. eIDAS stabilisce che non può essere negato valore legale a un documento solo perché esso è in forma elettronica. La situazione è più complessa quando si parla di firme elettroniche e sigilli elettronici in quanto eIDAS riconosce tre diversi livelli di firma elettronica: semplice, avanzata e qualificata. Blockchain sembrerebbe soddisfare i criteri tecnici per i primi due, ma per essere legalmente vincolante la firma deve rivestire criteri legali più elevati quali l'utilizzo dei servizi di un Trust Service Provider (TSP). Per questo motivo, da una prospettiva europea, le transazioni effettuate su una rete blockchain non hanno di per sé valore legale.

Sebbene, dunque, un simile quadro legislativo possa sembrare vago e indefinito, la posizione del legislatore italiano risulta essere in linea con la strategia europea. Infatti, se da un lato l'UE ha manifestato una chiara volontà di regolare le criptovalute e le loro implicazioni in termini di tassazione e antiriciclaggio, dall'altro ha mostrato un approccio normativo antitetico rispetto ad altri usi della tecnologia. A tal proposito, la risoluzione del Parlamento Europeo del 3 ottobre 2018 "Distributed Ledger Technologies e Blockchains: Building Trust with Disintermediation" ha sancito la volontà di non regolamentare le DLT e la Blockchain e ha specificato che gli Stati membri non devono disciplinare queste tecnologie e devono rimuovere gli ostacoli alla loro adozione, armonizzando così gli approcci normativi evitando una frammentazione che nuocerebbe ai potenziali risvolti di tale tecnologia[7]. Un simile invito lascia intendere che gli Stati membri non devono arrancare dietro al dinamico sviluppo delle reti Blockchain cercando di contenerle in un

[7]Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione (2017/2772(RSP))

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52018IP0373&from=IT

futile apparato normativo, bensì devono adattare la legislazione esistente ai problemi che possono sorgere e sostenerla con incentivi e finanziamenti.

Le transazioni che avvengono all'interno di queste reti, come nel caso degli Smart Contracts, è chiaro che possono avere implicazioni legali, per esempio in termini di obbligazioni, ma queste relazioni possono già essere inquadrate nell'attuale sistema normativo con i necessari adattamenti legali per rendere il mondo fisico compatibile con quello digitale[8]. Ciò nonostante, è bene che il legislatore italiano adotti una posizione chiara nei confronti della valenza giuridica delle transazioni che avvengono su blockchain senza però doverne limitare le potenzialità che derivano dal suo libero sviluppo.

In definitiva, i criteri che una blockchain deve possedere per avere valore legale devono essere dettati dall'AGID, alla quale la legge ha affidato il compito di definire le relative linee guida sulle caratteristiche tecnologiche. In particolare, all'AGID è stato affidato il compito di emanare linee guida per individuare i requisiti che il processo di conclusione di uno smart contract deve avere per soddisfare la forma scritta e, allo stesso tempo, di emanare linee guida per individuare gli standard tecnici che le tecnologie basate su registri distribuiti devono possedere per produrre gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento eIDAS.

In questo elaborato ci si soffermerà più avanti su una possibile modalità di identificazione sicura delle parti coinvolte in una blockchain e, di conseguenza, negli smart contracts.

2.1 COMPATIBILITÀ DELLA BLOCKCHAIN CON IL GDPR

Un altro tipo di preoccupazione a livello normativo riguarda la conformità tra blockchain e Regolamento europeo sulla protezione dei dati personali (GDPR) e la conseguente potenziale esposizione alla responsabilità legale.

La caratteristica che più stride con il Regolamento europeo è quella della decentralizzazione, la quale molto spesso porta con sé un elevato grado di anonimato degli utenti. Di fatto, il titolare del trattamento dati non è sempre riconducibile ad una persona fisica o giuridica, inficiando così l'allocazione di responsabilità soprattutto nel caso di una blockchain pubblica.

Una seconda complicazione riguarda la possibilità di modificare o cancellare i dati (c.d. diritto all'oblio) e come si è già visto tale flessibilità viene meno a causa della forte decentralizzazione del sistema su cui si basa la tecnologia blockchain. Di particolare rilevanza in questo caso sono gli articoli 16 e 17 i quali stabiliscono rispettivamente diritto alla rettifica e alla cancellazione dei dati.

Relativamente al primo articolo, il problema risulta particolarmente oneroso nel caso di Blockchain pubbliche, le quali, a causa dell'elevato numero di nodi coinvolti, rendono più difficile l'operazione di rettifica delle informazioni sigillate nella catena.

Per quanto riguarda il secondo articolo, è stata sottolineata la difficoltà di applicare il diritto alla cancellazione alle Blockchain. Di fatto, cancellare i dati dalle Blockchain è oneroso, poiché queste reti sono spesso progettate appositamente per rendere difficile la modifica unilaterale dei dati, che

[8]Laura Cappello, Italy: Regulatory approach to blockchain technologies, OneTrust DataGuidance, 2020 https://www.dataguidance.com/opinion/italy-regulatory-approach-blockchain-technologies

a sua volta dovrebbe generare fiducia nella rete garantendo l'integrità dei dati. La difficoltà di rispettare l'articolo 17 del GDPR[9] è quindi gravata da fattori tecnici, ma anche da motivi di governance. Infatti, anche se ci fosse un modo per garantire la conformità da una prospettiva tecnica, potrebbe essere difficile far sì che tutti i nodi implementino le relative modifiche sulla propria copia del database (in particolare nelle blockchain pubbliche/permissionless)[10].

Per quanto riguarda il caso degli smart contract è importante far riferimento all'articolo 22 del GDPR, il quale riguarda l'elaborazione di dati esclusivamente automatizzata. *L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*. Una decisione è basata esclusivamente sul trattamento automatizzato quando non vi è alcun coinvolgimento umano nel processo decisionale. L'articolo 22 del GDPR, tuttavia, riguarda solo le "decisioni" prese attraverso un trattamento dei dati esclusivamente automatizzato, mentre il considerando 71 del GDPR parla anche di una *decisione, che può includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani*. Uno smart contract in esecuzione su blockchain può qualificarsi come una decisione che rientra nell'articolo 22 GDPR quando produce effetti legali.

A questo punto è importante stabilire i limiti e i casi in cui è necessario avere il consenso del soggetto interessato:

1. Secondo l'articolo 22 GDPR, l'esecuzione automatizzata è tollerata quando è necessaria per stipula o per l'esecuzione di un contratto tra l'interessato e il responsabile del trattamento. Il requisito, affinché il contratto in questione sia concluso tra il responsabile del trattamento e l'interessato soggetto, sottolinea ancora una volta l'importanza di essere in grado di identificare chiaramente il responsabile del trattamento dei dati in relazione alle blockchain.
2. L'articolo 22(2)(b) GDPR autorizza, inoltre, gli Stati membri o l'UE a creare esenzioni al divieto di trattamento automatizzato a condizione che diritti e interessi delle persone coinvolte siano salvaguardati. In questa fase, nessuna legislazione è stata approvata a livello di UE o di Stato membro per consentire esplicitamente solo il trattamento automatizzato dei dati in relazione ai contratti intelligenti.
3. L'articolo 22(2)(c) GDPR consente il trattamento automatizzato dei dati quando è basato sul consenso esplicito dell'interessato.

[9]Cfr. Judgment of the Court (Grand Chamber), 13 May 2014. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.

[10]European Parliament, Blockchain and the General Data Protection Regulation Can distributed ledgers be squared with European data protection law?
https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

Inoltre, ciò che è richiesto non è solo il consenso, ma il “consenso esplicito”, che però non è definito nel Regolamento. Sembrerebbe, dunque, che il secondo comma dell’articolo 22 del GDPR preveda una serie di casi in cui è possibile operare legalmente gli smart contract[11].

Dopo aver analizzato la compatibilità della tecnologia blockchain con il Regolamento europeo sulla protezione dei dati personali si può invertire l’analisi e domandarsi come si possono raggiungere gli obiettivi preposti dal GDPR attraverso la Blockchain. Di fatto, è possibile pensare a una struttura in cui il titolare del trattamento dati può consentire, rifiutare e ritirare l'accesso dei propri dati, come nel caso della cosiddetta *Self Sovereign Identity* (SSI), che verrà analizzata in seguito. Le parti interessate potrebbero decidere attraverso uno Smart Contract secondo quali modalità i loro dati possono essere utilizzati, da chi e su quali basi. La blockchain sarebbe un ottimo mezzo per consentire ai soggetti di gestire direttamente i propri dati. In questo sistema, i contratti intelligenti potrebbero essere utilizzati per fornire l'accesso ai dati a una terza parte quando richiesto.

2.2 IDENTITÀ DIGITALE

I dati che compongono la nostra identità sono molteplici: nome e cognome, data di nascita, nazionalità, forme di identificatore nazionale come il numero di passaporto, la patente di guida, ecc. Questi dati sono emessi da entità centralizzate, in particolare autorità statali e sono memorizzati in database centralizzati. Sebbene il controllo di tali dati nel mondo fisico passi attraverso il nostro esplicito consenso e ciò avviene in modo manifesto, lo stesso non si può dire dell’universo digitale. In effetti, i cittadini continuano a non avere la completa proprietà e il pieno controllo delle loro identità digitali e devono interfacciarsi con processi di identificazione online frammentati, perdendo inconsapevolmente il valore che i loro dati generano. Nel mondo dell'identità digitale, le informazioni collegate all'identità di un individuo vengono chiamate "attributi identificativi” e vi è un numero potenzialmente illimitato di tali attributi. In queste circostanze il rischio di violazione dei dati personali è direttamente proporzionale al grado di centralizzazione dei dati stessi.

In quest’ottica si colloca la necessità e la tendenza di togliere il controllo sull'identità digitale alle istituzioni governative e attori corporativi per restituirla agli individui. Tutto ciò potrebbe essere reso possibile dalla tecnologia Blockchain, la quale permette una gestione e una memorizzazione più sicura delle identità digitali, fornendo un'infrastruttura unificata e interoperabile[12].

Allo stato attuale, esistono diversi modelli di identità digitale.

Il modello centralizzato è quello attualmente dominante. Centralizzato non significa che c'è una sola fonte centrale per le identità digitali, bensì che le identità digitali sono quasi sempre fornite da qualche autorità terza (spesso una società privata) per uno scopo specifico, come l’accesso ai propri servizi. Le informazioni sull'identità sono "centralizzate" all'interno di quell'entità. Risulta essere anche il modello più frammentato per l’elevato numero di player nell’universo digitale.

[11]European Commission, EU Blockchain Observatory and Forum - e-Identity Workshop Report - November 7, 2018
https://www.eublockchainforum.eu/sites/default/files/reports/workshop_5_report_-_e-identity.pdf
[12]European Commission, EU Blockchain Observatory and Forum - Blockchain and digital identity
https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

Il modello federato invece vede la presenza di diversi *identity provider* pubblici e privati che si accordano sul rilascio di credenziali uniche per l'accesso ai propri servizi, come avviene nel caso del servizio pubblico di identità digitale (SPID). Quest'ultimo certifica l'identità tramite un'entità terza (Poste Italiane) e consente l'accesso a determinati servizi online della Pubblica Amministrazione[13].

2.3 DECENTRALIZZAZIONE E SELF SOVEREIGN IDENTITY

Un'evoluzione, relativamente recente, nella gestione dell'identità digitale è costituita dal modello decentralizzato. Il paradigma dell'identità decentralizzata, basato sui registri distribuiti e le tecnologie Blockchain, si fonda sull'idea di mettere l'utente al centro della struttura e quindi di rimuovere la necessità di terze parti che intervengano nel processo identificativo. In questo mondo, l'utente "crea" la propria identità digitale associando credenziali verificabili da autorità riconosciute, per esempio i governi, gli utenti possono in effetti creare gli equivalenti digitali delle credenziali del mondo fisico, come le carte d'identità nazionali e le patenti di guida che rimangono sotto il loro controllo.

In particolare, la creazione di identità decentralizzate inizia con la costituzione di un identificatore decentralizzato (DID) al quale si allegano attributi. Una volta fatto questo, l'utente può raccogliere credenziali da autorità fidate e gestirle in modo autonomo secondo le circostanze.

Nel momento in cui l'individuo deve fare una rivendicazione, per esempio dimostrare che ha il diritto di votare in un'elezione o è abbastanza grande per acquistare alcolici, l'utente può semplicemente presentare la credenziale appropriata per quella specifica circostanza.

Grazie a varie tecniche crittografiche, come la firma digitale, è possibile ottenere una prova che la credenziale è autentica (cioè, che sia effettivamente rilasciata dall'autorità e non sia manomessa) e che l'utente che la presenta è effettivamente la persona a cui ci si riferisce, come illustrato nello schema che segue.

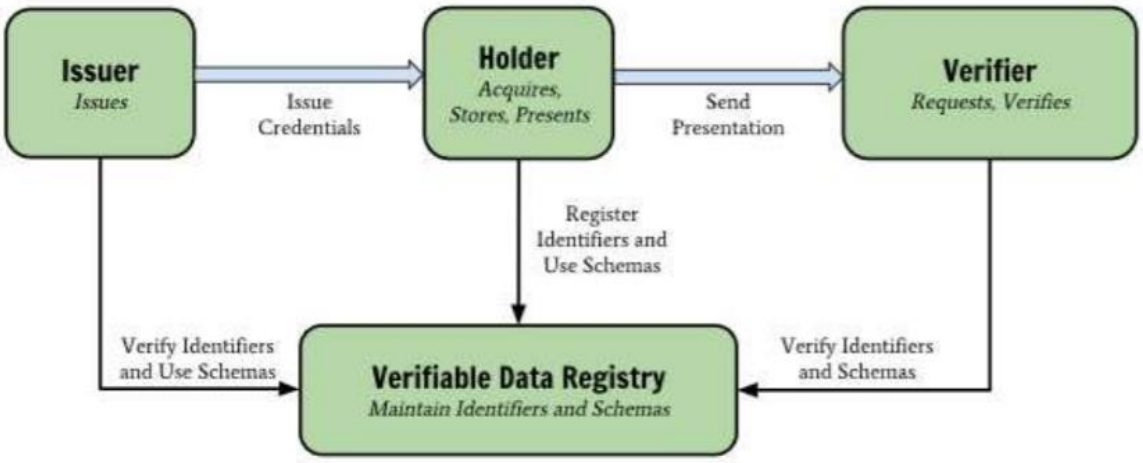

Immagine 2 - Flow of information of the verifiable claims generation. Source: *eIDAS supported SSI.*

[13]Annalisa Casali, Self Sovereign Identity: norme, applicazioni, benefici e sviluppi futuri, 31 marzo 2021 https://www.blockchain4innovation.it/tecnologie/self-sovereign-identity-norme-applicazioni-benefici-e-sviluppi-futuri/

La cosiddetta *Self Sovereign Identity* (SSI) è un tipo di identità digitale decentralizzata che dà agli utenti il controllo non solo dei loro DID, ma anche dei dati associati ad essi. In un sistema basato su SSI, gli utenti hanno un controllo molto più accurato su quanti dati condividono e con chi.

In questo contesto, la blockchain può costituire una soluzione per diversi aspetti relativi all'identificazione decentralizzata perché di fatto, fornisce un'infrastruttura per gestire i dati in modo decentralizzato e allo stesso tempo affidabile.

Si possono immaginare diversi potenziali usi per blockchain in un contesto di SSI, tra cui:

- Creazione di DID: gli indirizzi blockchain sono ottimi DID poiché sono unici, generati dall'utente stesso e sfruttano già la crittografia a chiave pubblica/privata.

- Usare la blockchain come registro DID: le blockchain potrebbero anche essere usate come registri DID, ovvero database dove memorizzare informazioni su chi è collegato a specifiche identità digitali.

- Credenziali notarili mettendo gli *hash* sulla Blockchain, si possono "autenticare" le credenziali. Questo non significa, però, memorizzare le credenziali sulla rete, il che è generalmente sconsigliato e in contrasto con il GDPR. In questo caso, la Blockchain agirebbe come un *timestamp* che fornisce sia la prova di quando la credenziale è stata creata sia "sigilla" quella credenziale rendendo qualsiasi manomissione evidente agli osservatori esterni. Per esempio, un'università potrebbe inviare l'hash di un diploma per registrarlo sulla Blockchain al momento della laurea. Questo fornisce allo studente un timestamp di quando il diploma è stato rilasciato e un modo di provare in qualsiasi momento in futuro che il diploma che viene presentato è quello che era registrato in quel momento[14].

Nonostante questo paradigma rivendichi una maggiore decentralizzazione rispetto agli altri, anche in questo caso un utente rimarrebbe vincolato da terze parti come i certificatori di identità. Tuttavia, per avere tante identità digitali quante quelle fisiche, un modello di certificazione centralizzato sembrerebbe essere l'unica strada percorribile. Basti pensare, inoltre, alle molteplici identità che una persona può crearsi sul web per capire la necessità di un ente centralizzato che certifichi l'identità nell'universo digitale.

3. LA BLOCKCHAIN NEL CONTESTO DELLA PUBBLICA AMMINISTRAZIONE

L'indice DESI (*Digital Economy and Society Index*) è un indice composito che prende in considerazione fattori quali l'integrazione delle tecnologie digitali o la connettività per indicare il grado di digitalizzazione di un paese. Ogni anno viene pubblicato un report dalla Commissione Europea per tracciare l'andamento in ogni paese. In particolare, l'Italia nel 2020 è risultata 25esima su 28 paesi, davanti solo a Romania, Grecia e Bulgaria, ben sotto la media europea[15]. Nello specifico,

[14]European Commission, EU Blockchain Observatory and Forum - Blockchain and digital identity https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf
[15]European Commission, The Digital Economy and Society Index (DESI), DESI 2020 https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi

per l'indice "servizi pubblici digitali" che tiene in considerazione il grado di digitalizzazione dei servizi pubblici e la loro qualità, l'Italia si è posizionata 19esima, sempre sotto la media europea.

Un altro indice della Commissione Europea, più specifico e pertinente nel nostro caso, è l'*e-government Benchmark*. Questo computa il grado di utilizzo delle tecnologie digitali ICT per ottimizzare i processi interni e le interazioni dell'amministrazione pubblica verso i cittadini, le imprese e altre amministrazioni[16]. In questo caso, sempre nel 2020, l'Italia è risultata ultima nell'utilizzo dei servizi di eGovernment.

Questi indici riflettono una situazione drammatica in quanto a integrazione tra pubblica amministrazione (PA) e tecnologie ICT. Sebbene il processo sia lento e vada attuato lungo varie linee strategiche quali la dematerializzazione dei dati, l'implementazione di infrastrutture adeguate e l'interoperabilità dei sistemi; in molti sostengono i benefici dell'applicazione di DLT e blockchain ai servizi della PA. Oltre a una maggiore efficienza in termini di semplificazione e tempestività, l'impiego di tali tecnologie aumenterebbe il grado di trasparenza dei processi e limiterebbe la possibilità di errore umano.

A tal proposito, è bene citare la nascita di due progetti: EBSI (European Blockchain Services Infrastructure), nato nel febbraio 2019, e IBSI (Italian Blockchain Services Infrastructure). Il primo mira a diventare un'infrastruttura digitale *gold standard* per sostenere il lancio e il funzionamento di servizi pubblici transfrontalieri in tutta l'UE sfruttando la tecnologia blockchain.

EBSI mira, invece, a stabilirsi virtualmente in ogni settore pubblico che potrebbe beneficiare della tecnologia blockchain ed è costituito da una rete di nodi distribuiti in tutta Europa, attualmente una trentina[17]. Inoltre, ESSIF (European self-sovereign identity framework) è parte di EBSI integrando così il modello di identità autonoma che permette agli utenti di creare e controllare la propria identità attraverso i confini, senza fare affidamento su autorità centralizzate.

Infine, uno dei principi guida su cui si fonda EBSI è quello circa la natura della rete Blockchain che si vuole implementare, vale a dire sul modello *public-permissioned* (Blockchain Ibrida). Tale principio mira alla creazione di una blockchain che incorpori alcune caratteristiche architetturali della blockchain pubblica e altre di quella privata, garantendo un'identità nota a tutti i partecipanti aggirando così il problema dell'anonimato, tipico di blockchain pubbliche. In questo modo, i nodi verrebbero gestiti dalla Commissione europea e dagli Stati membri che amministrano le autorizzazioni di scrittura e di partecipazione al network[18]. La partecipazione ad EBSI è perciò basata sull'autorizzazione e ammissione secondo una politica di controllo centralizzata e non tutti i nodi sono autorizzati a eseguire azioni sulla rete, ma tutti possono verificare le azioni che vengono eseguite sulla stessa.

IBSI, invece, è un progetto sperimentale promosso a livello nazionale da vari enti tra cui l'AgID nell'ambito del European Blockchain Partnership alla luce della Strategia Blockchain promossa dalla

[16]Commissione europea, eGovernment per la pubblica amministrazione https://ec.europa.eu/info/business-economy-euro/egovernment_it

[17]Cfr. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

[18]D. Alessi, S. Buescema, D. Marchese, M. Nicotra, Progetto IBSI, verso la blockchain per i servizi pubblici in Italia, 31 marzo 2021
https://www.agendadigitale.eu/documenti/progetto-ibsi-verso-la-blockchain-per-i-servizi-pubblici-in-italia/

Commissione europea. La sua applicazione alla PA è volta ad "incrementare la semplificazione, la trasparenza, la sicurezza e l'efficacia delle interlocuzioni e dei servizi resi, nel rispetto del principio del *Once Only Principle*, ovvero di consentire a cittadini e imprese di fornire dati solo una volta quando interagiscono con le Pubbliche Amministrazioni[19]".

Modelli simili, perciò, ben si adattano alla PA in cui è necessario un controllo centralizzato delle transazioni e che allo stesso tempo garantiscano la presenza di identità verificate. Come suggerisce il Dottor Alessandro Sannini, CEO di Twin Advisors, uno dei settori che più beneficerebbe da un'infrastruttura Blockchain, sempre nell'ambito della PA, sarebbe quello degli appalti pubblici. Questa applicazione, sottolinea Sannini, va vista in un'ottica di lotta alla corruzione, riduzione delle asimmetrie informative e semplificazione dei processi amministrativi.

Per quanto riguarda il meccanismo di consenso, quello implementato è chiamato Proof of Authority (PoA), il più adatto per servizi di interesse pubblico sebbene non rifletta appieno il principio della decentralizzazione. Esso si basa, in breve, sulla possibilità di alcuni nodi, detti validatori, di autorizzare la transazioni grazie al fatto che la loro identità è conosciuta.

3.1 IL CASO ESTONE

Tra i paesi europei, che hanno identificato la tecnologia blockchain come un valido supporto nella digitalizzazione della pubblica amministrazione, si distingue in particolare l'Estonia, che ha investito fortemente nella digitalizzazione e in particolare nell'adozione dei registri distribuiti sin dal 2012 con il «registro delle successioni» tenuto dal Ministero della Giustizia. Il governo estone ha adottato un sistema denominato KSI (*Keyless Signature Infrastructure*)[20], si configura come una particolare forma di registro distribuito che garantisce una struttura di rete in grado di assicurare la costante disponibilità dei dati e il rilevamento in tempo reale di tentativi di frode e modifiche non autorizzate, il tutto grazie al sistema di rilevamento autonomo delle anomalie basate su un processo di verifica immediato e automatizzato dell'originalità di un file o un dato immesso nel database.

Il valore innovativo del modello KSI è stato progressivamente valorizzato e adottato per un numero sempre maggiore di servizi, tra cui si annoverano, in particolare, il registro delle proprietà, il registro delle imprese e il registro sanitario. Quest'ultima innovazione si pone come la riforma di maggior rilievo e interesse dell'e-Government, specialmente in un periodo di pandemia globale; la qualità e la quantità dei dati correlati al sistema sanitario, infatti, impone di assicurare standard di sicurezza ed integrità molto elevati. Il sistema garantisce interoperabilità tra i database delle strutture sanitarie nazionali, nonché la loro accessibilità in qualsiasi sede del sistema sanitario nazionale, aiutando ad abbattere i costi e i tempi della burocrazia e anche ad aumentare l'efficacia delle cure.

La natura distribuita del sistema di e-Government Estone ha semplificato la condivisione dei dati tra i soggetti autorizzati, ha ridotto i costi complessivi delle cure mediche e delle richieste assicurative.

[19]AgID, Blockchain: AgID promotrice dell'infrastruttura italiana IBSI https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2021/03/02/blockchain-agid-promotrice-dellinfrastruttura-italiana-ibsi

[20] Fonte: https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/

Tale sistema, virtuoso in grado di autoalimentarsi, inoltre, ha portato alla teorizzazione di un sistema di remunerazione dei suoi partecipanti, ad esempio: nel caso del registro sanitario nazionale, sono previste ricompense per l'attività di registrazione di dati anonimizzati prestata dagli operatori sanitari, che potranno essere utilizzati per finalità di studio ed analisi, coniugando la digitalizzazione dell'amministrazione con l'investimento nella ricerca scientifica. Nei fatti, quindi, anche il settore della ricerca scientifica trae benefici da tale sistema, la quale ha a propria disposizione un consistente quantitativo di dati, seguono anche minori costi di gestione del protocollo a carico dell'amministrazione.

Alla luce di questa analisi, bisogna far chiarezza su due questioni fondamentali. Nonostante il caso estone sia conosciuto come il più efficace ed efficiente sotto il punto di vista tecnologico e organizzativo, in quanto il modello KSI ha decisamente rivoluzionato e migliorato la pubblica amministrazione sotto una moltitudine di punti di vista, non si può parlare di adozione da parte di una vera e propria blockchain di natura decentralizzata. Si tratta di un modello di blockchain privata o meglio ancora di un registro distribuito che si avvale dei vantaggi della funzione di time-stamping per certificare l'esistenza e l'originalità di un dato. Tuttavia resta un sistema chiuso, non di natura 'pubblica', come si potrebbe erroneamente supporre, in cui solo gli enti della pubblica amministrazione hanno accesso e autorità di operare, ma a differenza dei database tradizionali, ogni modifica e tentativo di frode o utilizzo illecito dei dati è immediatamente segnalato a tutti i membri parte del sistema.

Inoltre, il caso estone ci insegna quanto sia fondamentale l'avanzamento di un'opera di digitalizzazione, di investimenti infrastrutturali per garantire la connessione internet sull'intero territorio nazionale, nonché uno sforzo verso la riduzione del digital divide generazionale, per evitare problemi di implementazione di tecnologie come blockchain.

È auspicabile che, nel prossimo futuro, i vari governi nazionali europei si coordinino per promuovere una sana cooperazione su questi temi.

4. PROPOSTE DI POLICY

Alla luce di quanto detto finora, è evidente che la strada da percorrere in materia di Blockchain e Smart contracts a livello italiano sia ancora lunga. Le proposte di policy che seguono, da un lato si prefiggono l'obiettivo di rendere più chiaro e definito un quadro giuridico caratterizzato da definizioni che limitano la portata euristica della tecnologie che tentano di normare e dall'altro, indirizzare la strategia italiana nell'ambito della digitalizzazione della Pubblica Amministrazione.

4.1 PROCESSO DI IDENTIFICAZIONE INFORMATICA DELLE PARTI

Come già detto precedentemente, l'art. 8-ter, comma 2, del Decreto Semplificazioni del 2019 stabilisce che gli smart contract *soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall' AGID con linee guida*.

Con la Determinazione n. 116/2019 del maggio 2019, l'AGID ha istituito un gruppo di lavoro per emanare le linee guida previste dal Decreto Semplificazioni, ma, ad oggi, tali linee non sono ancora state pubblicate. In attesa della loro pubblicazione, è evidente che in Italia manchi ancora una normativa che disciplini i requisiti affinché l'identità possa essere considerata certificata e certa, in conformità con il Regolamento eIDAS. Quest'ultimo è quello che ha reso possibile la creazione negli Stati Membri della Carta d'Identità Elettronica (CIE) e l'accesso, attraverso la stessa, ai servizi di tutte le pubbliche amministrazioni degli stati europei per assicurare una maggiore standardizzazione.

Una possibile strada da intraprendere, per assicurare la "previa identificazione informatica delle parti interessate", potrebbe essere quella di legare il sistema di identificazione elettronica (eID) conforme al Regolamento eIDAS con il sistema DID/SSI.

Nell'ambito eIDAS, i fornitori di servizi online possono autenticare i propri utenti mediante il loro eID; per fare ciò, devono essere collegati a un nodo eIDAS che trasferisca la loro richiesta di autenticazione al nodo eIDAS del paese che emette eID. Nella risposta di autenticazione, insieme al risultato dell'autenticazione stessa, i fornitori di servizi possono ricevere una serie di dati che identificano in modo univoco l'utente, l'eIDAS Minimum Data Set. Tale processo è possibile sia per persone fisiche che giuridiche. Il collegamento del DID con l'eIDAS Minimum Data Set può essere effettuato consentendo all'utente, che gestisce il DID, di eseguire un'autenticazione eIDAS, agendo come fornitore di servizi. Questa autenticazione può essere eseguita al momento della creazione del DID, ma anche successivamente[21].

Tecnicamente, questo riconoscimento reciproco è garantito dal quadro di interoperabilità eIDAS, basato sull'utilizzo di nodi nazionali eIDAS che gestiscono lo scambio transfrontaliero di informazioni. Tale modello, sebbene da rifinire in termini tecnici, garantirebbe al tempo stesso certezza, standardizzazione e compliance.

Proposta programmatica:

- Creare un processo di identificazione informatica unico e sicuro in modo da riconoscere validità giuridica alle transazioni che avvengono su Blockchain e che implicano gli utenti con identità verificata;
- Sfruttare infrastrutture preesistenti, come i nodi eIDAS, per implementare una strategia di identificazione informatica degli individui e integrarle in un sistema DID/SSI al fine di avere identità certe e verificate;
- Standardizzare il processo non solo a livello italiano, ma anche comunitario sfruttando un'infrastruttura europea per incentivare le transazioni transfrontaliere.

[21]Carlos Gomez Muñoz, SSI and eIDAS: a vision on how they are connected, eIDAS Observatory, 2019 https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf

4.2 IMPLEMENTAZIONE DI UN SISTEMA DI E-GOVERNANCE BASATO SU RETE BLOCKCHAIN IBRIDA (PUBLIC PERMISSIONED)

È ragionevole considerare, quindi, l'introduzione della tecnologia blockchain nei sistemi della pubblica amministrazione come uno strumento in grado di garantire maggiore trasparenza nel rapporto tra cittadini e Stato, in grado di automatizzare e velocizzare lenti e macchinosi processi burocratici, di ridurre drasticamente l'errore umano e di migliorare l'interoperabilità tra gli attori della PA[22].

Willian Nonnis, Full-Stack e Blockchain Developer presso il Ministero della Difesa, rivela in sede di intervista, i principali problemi connessi alla difficoltà di implementare una rete basata su Blockchain sul piano nazionale: mancanza di infrastrutture adeguate e frammentazione della PA. Infatti, nonostante gli evidenti vantaggi di tale tecnologia, l'implementazione della stessa nei sistemi delle organizzazioni pubbliche presenta diverse criticità e difficoltà applicative. La migrazione da un sistema centralizzato a uno decentralizzato richiede l'avvio di un processo di trasformazione che non tutti sono inclini ad accettare, specie negli enti pubblici dove i lavoratori sono poco propensi a cambiamenti e innovazioni che richiedono una formazione specifica e il passaggio a un *modus operandi* diverso dal tradizionale.

Bisognerebbe, dunque, adeguare l'organizzazione alla nuova tecnologia implementata. Altra criticità è rappresentata dal basso e spesso frammentato numero di iniziative per l'adozione di nuove tecnologie, specialmente da parte di organi governativi. La velocità di sviluppo della tecnologia e il basso numero di evidenze nel settore pubblico non possono che accrescere l'incertezza dei manager nelle scelte di adozione della Blockchain. Inoltre, ad oggi, risulta piuttosto evidente la difficoltà di distinzione tra i modelli di Blockchain esistenti. Una Blockchain Pubblica (Permissionless) è completamente diversa a livello strutturale e funzionale da una Blockchain Ibrida (Public Permissioned) e una Blockchain Privata (Permissioned); tanto che spesso si parla scorrettamente di sistemi basati su tecnologia Blockchain, che sono, invece, registri distribuiti ma non necessariamente decentralizzati e dunque non definibili come Blockchain nella sua accezione originaria. Una possibile risposta a tali criticità è la sperimentazione su piccola scala delle iniziative che si vuole intraprendere al fine di comprendere quali sono e come possono interagire in armonia gli aspetti tecnologici e i fabbisogni organizzativi specifici dei processi di e-government. Successivamente occorre anche considerare che il passaggio a una sperimentazione su larga scala spesso richiede un certo livello di standardizzazione che non sempre è perseguibile con tecnologie non mature, che devono rispondere alle esigenze di integrazione dei processi amministrativi di diversi enti pubblici.

Ad oggi, la tipologia di Blockchain più ampiamente autorizzata è il modello *Permissioned,* che prevede la presenza di un gestore della piattaforma e consente (o nega) l'accesso ai registri, alle transazioni nonché l'adesione di nuovi membri ad un numero ristretto di attori. Viene meno, dunque, la caratteristica della centralizzazione e dell'immutabilità e di conseguenza tutti i benefici

[22] Agenda Digitale, *Blockchain per la PA, progetti e settori di impiego*, 2019: https://www.agendadigitale.eu/documenti/blockchain-per-la-pa-progetti-e-settori-di-impiego/

derivanti dalle stesse. L'implementazione di una rete Blockchain comporta dunque una scelta di progettazione che, indifferentemente dagli ambiti applicativi, è dettata dalle esigenze dei promotori dell'iniziativa e dai diversi fabbisogni degli utenti. Nel settore pubblico, le iniziative basate su tecnologia Blockchain sono spesso di tipo private-autorizzate, come abbiamo visto per il caso estone, dove resta presente un ordine gerarchico, poiché l'accesso ai registri e la possibilità di creare dei blocchi è consentito a un numero ristretto di operatori pubblici. Ci si interroga dunque, se sia opportuno adottare tale tipologia di Blockchain, in particolare nell'ambito dei rapporti e relazioni tra cittadino e la Pubblica Amministrazione. Secondo gli autori del paper, gli scenari in cui sviluppare direttrici di innovazione in questo contesto debbano prevedere l'adozione di Blockchain ibride, in modo tale da non eliminare gli accessi autorizzati agli operatori della Pubblica Amministrazione, ma allo stesso tempo dare la possibilità ai cittadini di poter consultare le operazioni effettuate. La blockchain ibrida rappresenta il modello che tenta di utilizzare la parte migliore delle soluzioni blockchain private e pubbliche. Idealmente, implementare una blockchain ibrida significherà accesso controllato e libertà allo stesso tempo.

In questo modo, si arriverebbe a un buon compromesso tra un sistema di governance centralizzata e distribuzione dei controlli, nel quale la fiducia è riposta in chiunque dimostri matematicamente di esserne in grado (risolvendo un complicato enigma crittografico) e un sistema di governance centralizzata e controlli distribuiti.

L'Unione Europea sta lavorando su progetti, come ad esempio *"Blockchain per il bene sociale"*, che prevedono l'uso e lo sviluppo di piattaforme in cui la collettività gestisca autonomamente, tramite l'uso della tecnologia blockchain, i propri dati. Anche L'UE, ha individuato nella Blockchain Ibrida, lo strumento tecnologico per poter facilitare l'interoperabilità tra gli organi della Pubblica Amministrazione e migliorare la vita ai propri cittadini. Tali progetti dovranno garantire la tracciabilità dei processi produttivi e migliorare la trasparenza nella spesa pubblica e pubblica amministrazione. Inoltre, dovranno consentire la gestione dei dati ed essere adottabili da ampie comunità, senza mettere a rischio la salvaguardia della privacy e della trasparenza.

Proposta Programmatica

- Implementare una rete Blockchain per la Pubblica Amministrazione di natura ibrida, in linea con il modello progettato dall'UE, per armonizzare e standardizzare i processi di adozione della tecnologia Blockchain a livello nazionale e comunitario.

4.3 STANDARDIZZAZIONE DEI PROCESSI DI ADOZIONE DEI SISTEMI BLOCKCHAIN NELLA PUBBLICA AMMINISTRAZIONE

Per evitare problemi, quali la frammentazione e la duplicazione delle diverse iniziative basate su tecnologia Blockchain intraprese nel settore pubblico, occorre introdurre una standardizzazione dei processi. Si ritiene, infatti, che lo sviluppo di una piattaforma condivisa basata su Blockchain Ibrida

per l'esecuzione delle diverse iniziative nell'e-Government possa consentire la standardizzazione dei processi e la replicabilità delle iniziative. Tuttavia, stabilire chi dovrà controllare la piattaforma, in che modalità e se la Blockchain sarà capace di adeguarsi alle diverse legislazioni esistenti in vari Paesi rappresenta dei limiti alla scalabilità e, dunque, delle questioni aperte. Sebbene ci siano dei benefici legati all'utilizzo di un sistema Blockchain nel settore pubblico, esistono, tuttavia, diverse criticità che occorre prendere in considerazione. In particolare, dal punto di vista tecnologico, l'implementazione della Blockchain richiede un adeguamento delle tecnologie per l'informazione e la comunicazione presenti all'interno delle organizzazioni, il cui costo potrebbe essere più o meno rilevante. Dal punto di vista organizzativo, invece, l'implementazione della Blockchain richiede uno sforzo progettuale sia nei rapporti tra le organizzazioni, sia all'interno delle singole aziende coinvolte. L'implementazione della Blockchain richiede la definizione e la formalizzazione dei rapporti tra i diversi partner che costituiscono una rete, inoltre la rivisitazione dei modelli di organizzazione del lavoro e dei meccanismi che regolano i rapporti tra i lavoratori e le attività esistenti all'interno delle singole organizzazioni. Il successo dell'implementazione di una Blockchain dipende molto dalla capacità di introdurre innovazioni tecnologiche e organizzative, che siano coerenti con i modelli culturali preesistenti nelle organizzazioni coinvolte.

Proposta programmatica:

- Elaborazione di una standardizzazione riguardante l'adattamento di una Blockchain nel settore pubblico.

CONCLUSIONE

L'Italia sta muovendo i primi passi verso l'implementazione di un'infrastruttura nazionale, basata su Blockchain, per comprenderne a fondo le caratteristiche principali e le potenzialità al fine di semplificare l'apparato burocratico, velocizzare processi e scambi di informazioni e garantire così una maggiore efficienza dei servizi offerti dalla Pubblica Amministrazione. L'affermazione della Blockchain, in un contesto tale, avverrà in modo lento e graduale affinchè tutto l'ecosistema familiarizzi con il suo utilizzo. Questo dovrà avvenire sia per coloro che offrono servizi basati su Blockchain (impiegati della Pubblica Amministrazione) sia per coloro che ne usufruiscono (cittadini di tutte le età) per agevolare l'interazione con la comunità.

È importante sottolineare la necessità di chiarezza terminologica in un campo in cui si può cascare facilmente nell'errore. Se è vero che non è tutto oro quel che luccica, ugualmente si può dire che non è tutto Blockchain quel che si basa sui DLTs. L'esasperazione del termine Blockchain ha creato confusione sull'interpretazione dei reali benefici di una vera Blockchain pubblica, dunque di natura decentralizzata, e quelli di una tecnologia basata su registri distribuiti, dove esiste comunque un ordine gerarchico e vi è pochissima differenza con i tradizionali database centralizzati.

La proposta di implementare una Blockchain ibrida nell'ambito della Pubblica Amministrazione, non solo è in linea con la strategia europea, ma ha il fine ultimo di prendere il meglio di una Blockchain

pubblica e di una privata per adeguare le loro potenzialità a un contesto macchinoso come quello burocratico-amministrativo.

Infine, dato il dinamico avanzamento tecnologico di alcuni attori sulla scena internazionale nonché la sperimentazione della tecnologia Blockchain da parte di organi pubblici, è necessario ridefinire le priorità strategiche nazionali in ambito digitale al fine di cavalcare l'onda dell'innovazione e non esserne travolti passivamente. Da un lato sono, perciò, necessarie una serie di azioni infrastrutturali trasversali per modernizzare il paese con la creazione di piattaforme abilitanti e programmi di accelerazione; dall'altro il legislatore deve favorire tale processo in modo che avvenga in pieno rispetto della legge. Questo arduo compito consiste nel trovare il giusto equilibrio tra la promozione della tecnologia Blockchain senza imbrigliarla in una apparato normativo limitante e nella necessità di non lasciare vuoti normativi che generino zone grigie incerte in cui operare.

BIBLIOGRAFIA

Private, Public, and Consortium Blockchains - What's the Difference?, https://www.binance.vision/blockchain/private-public-and-consortium-blockchains-whats-the-difference.

I. Bashir,Mastering Blockchain: Distributed ledger technology, decen-tralization, and smart contracts explained, 2nd Edition, Packt, ISBN978-1788839044, 2018.

AgID, 2021. Blockchain: AgID promotrice dell'infrastruttura italiana IBSI; https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2021/03/02/blockchain-agid-promotrice-dellinfrastruttura-italiana-ibsi

Alessi D., Buescema S., Marchese D., Nicotra M., 2021. Progetto IBSI, verso la blockchain per i servizi pubblici in Italia; https://www.agendadigitale.eu/documenti/progetto-ibsi-verso-la-blockchain-per-i-servizi-pubblici-in-italia/

Algerio S., 2020. Blockchain: compatibilità con il GDPR dell'aggiornamento dei dati e del diritto all'oblio; https://www.blockchain4innovation.it/esperti/blockchain-compatibilita-con-il-gdpr-dellaggiornamento-dei-dati-e-del-diritto-alloblio/

Artzt M., 2019. EU: Is blockchain compatible with the GDPR? Part 1, OneTrust DataGuidance; https://www.dataguidance.com/opinion/eu-blockchain-compatible-gdpr-part-1

Casali A., 2021. Self Sovereign Identity: norme, applicazioni, benefici e sviluppi futuri; https://www.blockchain4innovation.it/tecnologie/self-sovereign-identity-norme-applicazioni-benefici-e-sviluppi-futuri/

Cappello L., 2020. Italy: Regulatory approach to blockchain technologies, OneTrust DataGuidance; https://www.dataguidance.com/opinion/italy-regulatory-approach-blockchain-technologies

Gomez Muñoz C., 2019. SSI and eIDAS: a vision on how they are connected, eIDAS Observatory. https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf

Commissione europea, 2020. eGovernment per la pubblica amministrazione; https://ec.europa.eu/info/business-economy-euro/egovernment_it

European Commission, 2018. EU Blockchain Observatory and Forum - e-Identity Workshop Report; https://www.eublockchainforum.eu/sites/default/files/reports/workshop_5_report_-_e-identity.pdf

European Commission, 2019. EU Blockchain Observatory and Forum - Blockchain and digital identity. https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

European Commission, 2020. The Digital Economy and Society Index (DESI). https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi

European Parliament, 2019. Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law? https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

Morelli C., 2019. Blockchain e GDPR: le tre strade per garantire compatibilità; https://www.altalex.com/documents/news/2019/09/03/blockchain-gdpr-tre-strade-per-garantire-compatibilita

Nuzzo A. (a cura di), 2021. Blockchain e autonomia privata, fondamenti giuridici, LUISS University Press;

Zwitter Andrej J., Gstrein Oskar J., Yap E., 2020. Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual, Frontiers in Blockchain. https://doi.org/10.3389/fbloc.2020.00026

Agenda Digitale, *Blockchain per la PA, progetti e settori di impiego*, 2019: https://www.agendadigitale.eu/documenti/blockchain-per-la-pa-progetti-e-settori-di-impiego/

AWARE

www.awarethinktank.it
info@awarethinktank.it