Marzo 2019

Distributed Ledger Technology e Smart Contract: finalmente è Legge. Prime riflessioni su una rivoluzione tecnologico-giuridica.

Avv. Fabrizio Cascinelli e Avv. Cristina Bernasconi, PwC TLS Avvocati e Commercialisti; Dott. Marco Monaco, PwC Technology - Blockchain Competence Center Lead

In data 12 febbraio 2019 è stato pubblicato in Gazzetta Ufficiale 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" (il "Decreto Semplificazioni" o, semplicemente "Decreto").

Tra le altre novità, il Decreto ha previsto all'art. 8-ter rubricato "Tecnologie basate su registri distribuiti e smart contract" le seguenti definizioni:

(i) "**Tecnologie basate su registri distribuiti**", quali le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili;

(ii) "**Smart contract**", quali un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse.

Le tecnologie basate su registri distribuiti

Le tecnologie basate su registri distribuiti sono le tecnologie che la Bank for International Settlements (BIS) ha definito come "*processes and related technologies that enable nodes in a network (or arrangement) to securely propose, validate and record state changes (or updates) to a synchronised ledger that is distributed across the network's nodes*"[1], evidenziando come la natura di tali tecnologie sia insita nell'utilizzo

[1] BIS, Committee on Payments and Market Infrastructures, Distributed ledger technology in payment, clearing and settlement, February 2017.

delle c.d. reti di nodi, che collegati gli uni agli altri rendono possibile lo scambio di dati tra un utente ed un altro.

Il termine 'DLT', o Distributed Ledger Technologies (tecnologie a registri distribuiti), indica infatti un insieme di protocolli che permettono ad una rete composta da nodi di attori di pari entità (*peer nodes*) di gestire un registro, o ledger, sincronizzato tra i partecipanti grazie all'utilizzo della crittografia e senza necessità di un unico nodo centrale che si occupi della gestione e del controllo del registro.

Le DLT abilitano la possibilità di gestire un registro in cui le evoluzioni dei dati custoditi siano condivise e controllate da più attori contemporaneamente. Un sottoinsieme di tali protocolli, indicato con il termine di Blockchain, individua quei particolari protocolli nel quale l'evoluzione dei dati del registro è governata attraverso strutture a blocchi crittograficamente concatenati l'uno all'altro. La principale caratteristica delle Blockchain, rispetto alle DLT, è proprio che ciascun nodo della rete detiene una copia completa del registro contenente tutte le transazioni effettuate da tutti gli attori. Le DLT che non rientrano in questa definizione di Blockchain, invece, non sono basate su una struttura a blocchi e permettono quindi di creare sottogruppi di *data disclosure* dove ciascun nodo detiene solo una parte del registro delle transazioni, ovvero quelle in cui il nodo stesso è originatore o ricevente, per garantire maggiore privacy tra i partecipanti.

Si può quindi affermare che nelle DLT, diversamente dai registri centralizzati (i classici *Database*), il controllo dell'evoluzione dei dati è condiviso tra alcuni partecipanti della rete. Nelle Blockchain, che sono un sottoinsieme delle DLT, il controllo dell'evoluzione dei dati tracciati nel registro è condiviso tra tutti i partecipanti della rete.

Una transazione è l'elemento chiave di una Blockchain: è il modo con cui un generico attore (nodo) può richiedere una modifica al registro andandone ad alterare il contenuto. Il registro non sarà altro che il risultato di tutte le transazioni fatte da tutti i nodi dal momento esatto in cui è nata la Blockchain fino al momento attuale in cui la si osserva.

In una Blockchain, infatti, ciascun nodo ha una propria copia completa del registro delle transazioni. Il protocollo, che altro non è che un insieme di regole che implementa una specifica Blockchain, prevede che solo 1 nodo della rete per volta (e mai lo stesso) possa aggregare tutte le transazioni fatte dai nodi in un intervallo di tempo definito (a seconda della rete) in una struttura dati chiamata blocco. Questo blocco viene legato crittograficamente al blocco precedente, includendo al suo interno l'impronta digitale (*hash*) dell'ultimo blocco disponibile sulla rete e successivamente viene inviato a tutti i partecipanti.

Ciascun nodo (o partecipante) andrà ad aggiornare il proprio registro locale sulla base delle transazioni presenti nel blocco ricevuto. In questo modo si ha la ragionevole certezza che tutti i nodi della rete abbiano, in locale, un registro perfettamente identico agli altri partecipanti.

Questa tecnologia ha dei risvolti interessanti: volendo cambiare un'informazione inclusa nel registro attraverso una transazione passata, non esiste una copia centrale da alterare. Un ipotetico nodo malevolo dovrebbe cambiare tutti i registri di tutti i nodi della rete. Inoltre, cambiare l'informazione equivale a modificare il blocco passato, ma questa operazione ne cambia anche la sua impronta digitale, richiedendo la modifica (o il ricalcolo) anche del blocco successivo e di tutti gli altri blocchi della catena fino a quello attuale.

Questa riscrittura dell'intera catena può avvenire solo in alcuni tipi di Blockchain e solo se tutti i nodi (o almeno la maggioranza) sono concordi nell'effettuarla. In alcuni casi questa operazione è improbabile: ad esempio nelle Blockchain c.d. *permissionless* (sia per lo pseudonimato dei partecipanti, che per i disincentivi dovuti al *Proof-Of-Work*) la probabilità di riuscire a riscrivere i blocchi è prossima allo zero. In alcune Blockchain c.d. *permissioned*, invece, gli attori sono tutti noti, ma se il numero è sufficientemente elevato e la governance della rete tiene conto di alcuni aspetti, anche in questo caso la probabilità di effettuare una riscrittura potrebbe in teoria essere ridotta al minimo.

Per questo motivo alcune Blockchain, ma non tutte, hanno una caratteristica molto interessante: le informazioni al loro interno sono immutabili e riconducibili ad un particolare istante nel tempo.

Ovviamente, ciò non comporta obbligatoriamente che le informazioni custodite in una Blockchain siano automaticamente certificate: la semantica del dato non può essere verificata da questa tecnologia e dipenderà sempre dagli attori che inseriscono le informazioni e dai processi di controllo esterni alla Blockchain e necessari a certificare il dato. Quello che però previene automaticamente la Blockchain è la possibilità di modificare i dati a posteriori, permettendo (ed obbligando) all'attore che li fornisce di poterne reclamare la proprietà, ovvero certificando che quel particolare attore ha effettuato quella particolare transazione in quell'istante di tempo.

Se il più noto utilizzo di tale tecnologia è stato legato alla registrazione e scambio di criptovalute, ed in particolare di Bitcoin, ormai i trend attuali sostengono che tale non può considerarsi il solo e unico utilizzo.

Il mercato ha iniziato ad interrogarsi sui possibili utilizzi di tecnologie DLT oltre le criptovalute, spaziando, dalla gestione delle filiere produttive per tracciare ogni singolo oggetto in un registro decentralizzato e condiviso, alla gestione decentralizzata delle identità, alle più recenti applicazioni nel settore bancario e finanziario basate sui pagamenti, sulle registrazioni post-trading e sui sistemi di *clearing* e *settlement* di operazioni. L'attenzione si è dunque spostata sulla possibilità di sfruttare tali tecnologie quali mezzo di registrazione e conservazione di dati, garantendone integrità e certezza di data e tempo.

Il background della norma italiana - gli interventi del Parlamento Europeo

La possibilità di utilizzare un metodo che permetta di garantire in tempo immediato certezza delle informazioni trasmesse, essendo registrate in una catena di blocchi non sovra-trascrivibili, è stata accolta con interesse dal mercato, tanto che in Europa il Legislatore ha riconosciuto l'attualità del tema ed ha inteso dedicare ampio spazio allo studio degli sviluppi di tali tecnologie.

A tal riguardo, il Parlamento Europeo ha pubblicato nel febbraio 2017 il paper "*Come la tecnologia blockchain può cambiarci la vita*"[2], riconoscendo che "*le blockchain rappresentano una modalità particolarmente trasparente e decentralizzata per la registrazione di elenchi di transazioni*" ed analizzando quali possano essere gli utilizzi concreti oltre la registrazione di criptovalute (*e.g.* brevetti, gestione dei diritti dei contenuti digitali, voto elettronico, smart contract).

Il Parlamento Europeo ha analizzato altresì i potenziali benefici e rischi che l'utilizzo di tali tecnologie potrebbero comportare, nonché le difficoltà che ancora sussistono prima di una capillare diffusione sul mercato. Riconoscendo che "*le blockchain sottraggono alle élite centrali parte del controllo sulle interazioni quotidiane con la tecnologia, ridistribuendolo tra gli utenti*", il Parlamento europeo ha sottolineato come, a fronte di crescenti aspettative sociali in termini di responsabilità da parte delle istituzioni, anche finanziarie, "*la popolarità della tecnologia blockchain potrebbe anche riflettere una tendenza sociale emergente a privilegiare la trasparenza all'anonimato*".

A tal riguardo, con una risoluzione del 3 ottobre 2018, il Parlamento Europeo ha espressamente sottolineato che "*la DLT può introdurre, attraverso i necessari meccanismi di cifratura e controllo, un paradigma informatico che può democratizzare i dati e rafforzare la fiducia e la trasparenza, fornendo un percorso sicuro ed efficace per l'esecuzione delle transazioni*"[3].

La capacità delle tecnologie DLT di creare una base di azione comune, all'interno della propria rete tra gli utenti coinvolti, che sia in grado di garantire certezza temporale degli accadimenti registrati sulla rete stessa potrebbe rappresentare la chiave di volta dell'implementazione di determinate operatività.

Sulla base di tale contesto, l'Autorità legislativa europea ha riconosciuto la necessità di introdurre un *framework* normativo ed un piano di azione a livello europeo, chiedendo a tal fine l'intervento della Commissione Europea e del Consiglio.

[2] EPRS – Servizio Ricerca del Parlamento europeo, Philip Boucher, Analisi approfondita, Febbraio 2017.
[3] Parlamento Europeo, Risoluzione del 3 ottobre 2018 sulle tecnologie di registro distribuito e Blockchain: creare fiducia attraverso la disintermediazione, 2017/2772.

Le molteplici applicazioni a valere sulle tecnologie basate su registri distribuiti: gli Smart Contract

Nel novero degli ambiti di applicazione delle DLT, anche sulla scorta di quanto riconosciuto dal Financial Stability Board[4], lo stesso Parlamento Europeo ha in più occasioni evidenziato come uno degli ambiti di maggior impatto dell'utilizzo delle tecnologie DLT possa essere rappresentato dai c.d. "Contratti intelligenti" o "smart contract" (gli "Smart Contract"). Sia nel *paper* del febbraio 2017 sia nella risoluzione del 3 ottobre 2018, il Parlamento Europeo ha riconosciuto che "*i contratti intelligenti sono un elemento importante abilitato dalle DLT e possono fungere da fattori chiave delle applicazioni decentralizzate*".

Gli Smart Contract, già nel 1994, erano definiti come "protocollo di transazione computerizzato che esegue i termini di un contratto". Ciò vale tanto più oggi in un contesto di diffusione di tecnologia DLT, e di *blockchain* in particolare, dal momento che i termini dell'accordo sarebbero programmati nella forma di codici e di istruzioni, memorizzati in una *blockchain*, gli uni interdipendenti dagli altri.

In questo modo, uno Smart Contract richiamato da una transazione fatta da un generico attore ne può certificare non solo la sottoscrizione da parte dello stesso, ma anche la valutazione dei termini codificati al suo interno per la valutazione dell'esito.

Infatti, un generico attore (nodo) ha la possibilità di codificare determinate azioni in uno Smart Contract da pubblicare su una Blockchain. Un generico firmatario, può sottoscrivere il contratto attraverso una transazione e fornire, contestualmente alla firma, dei parametri di *input*. Lo Smart Contract non fa altro che eseguire le operazioni codificate al suo interno sulla base degli *input* forniti e produrre uno specifico risultato il cui fine è quello di alterare le informazioni presenti nel registro distribuito in modo che tutti i nodi della rete possano quindi osservarne lo stato aggiornato.

Le operazioni dello Smart Contract, infatti, sono avviate dalla transazione del firmatario che è inclusa in un blocco ed inviata a tutti i nodi della rete. Ciascuno di loro eseguirà la transazione che invoca lo Smart Contract e produce lo stesso output degli altri in modo da permettere di avere la stessa copia del registro aggiornato su tutti i nodi.

Il framework normativo auspicato in materia di DLT e Smart Contract

Il Parlamento Europeo ha individuato due macro ambiti di interesse che richiederebbero ulteriori approfondimenti e una definizione certa del quadro giuridico, al fine di garantire la certezza necessaria agli operatori per poter applicare quanto ipotizzato:

(i) l'inquadramento degli Smart Contract nell'ambito degli ordinamenti giuridici nazionali, superando il contrasto che si verrebbe a creare tra una tecnologia

[4] e.g. FSB, Financial Stability Implications from FinTech, *Supervisory and Regulatory Issues that merit Authorities' attention*, 27 June 2017.

fondata sulla immutabilità di termini e condizioni e ordinamenti giuridici fondati, almeno in parte, sull'autonomia delle parti che potrebbero decidere di modificare determinate condizioni in corso di validità del contratto;

(ii) il riconoscimento della validità di una firma digitale crittografata, anche attraverso l'elaborazione di norme tecniche da parte delle organizzazioni internazionali competenti.

A tal fine, il Parlamento Europeo ha espressamente incaricato la Commissione Europea di promuovere l'introduzione di tali tecniche, nonché il superamento di potenziali ostacoli all'utilizzo di tali contratti nel mercato digitale unico.

La Commissione Europea, in tale contesto, è stata particolarmente attiva negli scorsi anni a sostenere lo sviluppo di osservatori, partnership e forum che potessero implementare il c.d. *Digital Single Market*. È stato assunto, fra gli altri, l'impegno congiuntamente con la European Blockchain Partnership (EBP) di sviluppare la European Blockchain Services Infrastructure (EBSI) introducendo il primo set di servizi pubblici digitali cross-border.

Con particolare riferimento alla definizione di un background normativo per gli Smart Contract, la Commissione Europea ha avviato il 5 dicembre 2018 una "*call for tenders*", conclusasi lo scorso 17 gennaio 2019, "*Study on Blockchains: Legal, Governance and Interoperability Aspects",* volta ad approfondire gli aspetti legali e regolamentari relativi alle tecnologie DLT e alla relativa applicazione ed impatti, nonché a costituire le basi del futuro framework normativo in materia.

L'intervento legislativo italiano. Una definizione incompleta in attesa delle Linee guida dell'AGID

Nel contesto delineato finora, il legislatore italiano, primo tra tutti gli stati membri della EU, ha inteso introdurre nell'ordinamento giuridico nazionale le definizioni di tecnologie basate su registri distribuiti nonché di Smart Contract, dando evidenza altresì di alcune conseguenze nel contesto giuridico del nostro ordinamento derivanti da caratteristiche tecnologiche di entrambi, tecnologie DLT e Smart Contract.

Il Decreto precisa quanto segue:

a) la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica, ai sensi dell'articolo 41 del Regolamento UE n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno;

b) gli smart contract soddisfano il requisito della forma scritta esclusivamente previa identificazione informatica delle parti interessate.

Anche il legislatore italiano, evidentemente, ha inteso dare atto dell'importanza che le tecnologie DLT e gli Smart Contract possano garantire integrità allo scambio di dati, riconoscendo valenza giuridica a tale certificazione.

Le definizioni di cui al Decreto non possono, tuttavia, ritenersi conclusive dell'*iter* legislativo in tal senso né possono dirsi direttamente applicabili nella prassi.

È espressamente richiesto l'intervento dell'Agenzia per l'Italia digitale al fine di emanare linee guida da adottare entro 90 giorni dalla data di entrata in vigore della Legge di conversione del Decreto (*i.e.* il 13 febbraio 2019). Le linee guida dovranno specificare:

a) gli standard tecnici che debbono possedere le tecnologie basate su registri distribuiti affinchè possano produrre gli effetti giuridici della validazione temporale elettronica;

b) i requisiti per l'identificazione informatica delle parti vincolate da uno smart contract.

Esclusivamente a seguito di tale intervento, potranno avere un reale significato le previsioni del Decreto in materia di riconoscimento della forma scritta degli smart contract nonché di validazione temporale elettronica della memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti.

Il lavoro di AGID è fondamentale per rendere effettivamente applicabile (anche in sede giurisdizionale) la nuova norma. Limitandosi, infatti, alla lettura testuale delle nuove definizioni sorgono diversi dubbi. Ad esempio, stando alla definizione, un registro distribuito erogato da un singolo attore utilizzando tre *server* di un servizio *cloud* dovrebbe poter beneficiare degli effetti giuridici della validazione temporale elettronica. Purtroppo, però, in questo caso specifico un qualsiasi esperto (ad esempio in caso di contestazione della validità di tale tecnologia in sede giurisdizionale) potrebbe dimostrate la semplice alterabilità del contenuto da parte dell'attore e quindi farne decadere gli effetti giuridici.

È importante, dunque, identificare e definire i requisiti tecnici entro i quali ricade un registro distribuito o una Blockchain per poter essere considerata immutabile e conseguentemente beneficiare degli effetti giuridici definiti dalla normativa.

Allo stesso modo, è fondamentale definire tecnicamente i concetti di 'distribuito, condiviso e replicabile' in quanto alcune Blockchain prevedono una copia completa del registro su tutti i nodi della rete, ma alcune tecnologie di registri distribuiti innovative prevedono una distribuzione, condivisione e replicazione dei dati '*on a need to know basis*' (ovvero solo tra i nodi interessati alla transazione). È importante, quindi, porre attenzione alla definizione per evitare di lasciare questo tipo di registri distribuiti al di fuori del perimetro di applicazione della normativa.

La stessa definizione di Smart Contract necessita di un approfondimento importante da parte di AGID.

Diversamente da quanto indicato dal nome, infatti, uno Smart Contract non è altro che una logica di *business* applicata ad una transazione effettuata su un registro distribuito e quindi è solo lontanamente riconducibile al classico concetto di "contratto". Il punto più delicato è proprio dovuto al fatto che il vero vantaggio di uno Smart Contract rispetto ad un generico software è la possibilità di poter automaticamente fare *enforcing* delle logiche codificate rispetto ad *asset* tracciati sul registro distribuito. Per meglio chiarire questo concetto con un esempio, ipotizziamo un registro distribuito che traccia *asset* puramente digitali e quindi esistenti unicamente sullo stesso registro (es. voti, euro, Bitcoin o altre Cryptocurrencies). In questo caso, uno Smart Contract è in grado, da solo, di fare *enforcing* di regole di business in esso cablate: "permetti l'assegnazione di un voto solo se il chiamante non ha già effettuato altre transazioni in passato". Lo Smart Contract è autonomo nel decidere se la transazione è lecita o meno e non necessita di intervento da parte di soggetti esterni.

Le potenzialità degli Smart Contract al di fuori dell'*enforcement* automatico di regole di business codificate sono molto marginali: l'identificazione certa, la non ripudiabilità, la codifica informatizzata, ecc, sono caratteristiche offerte da molte tecnologie pre-esistenti come la crittografia PKI, la *digital identity* o le funzioni di *hashing*.

Questo vantaggio, però, lo si può sfruttare solo in contesti in cui lo Smart Contract agisce su *asset* tracciati dal registro distribuito: nel caso in cui l'*asset* sia presente nel mondo reale, ma solo rappresentato in formato digitale su una Blockchain, allora lo Smart Contract ha bisogno di aiuto dal mondo esterno. Ad esempio, un registro distribuito che traccia proprietà fisiche (es. beni immobili o auto), avrà al suo interno *asset* univoci che fanno riferimento al mondo reale. In questi casi, tuttavia, uno Smart Contract non è in grado di effettuare *enforcing* delle logiche di business: è possibile verificare attraverso uno Smart Contract il passaggio da un *owner* (es. lo scrivente) ad un altro (es. il lettore), tuttavia quello sarà solo un passaggio della rappresentazione digitale. Nel mondo reale lo scrivente potrebbe rifiutarsi di cedere la proprietà dell'oggetto al lettore.

Qui entra in gioco la regolamentazione e, dunque, le specifiche tecniche dell'Agid: definire come e quando è possibile creare una relazione tra ciò che appartiene al mondo fisico/reale ed il relativo *digital twin* tracciato nel registro distribuito, in modo che uno scambio effettuato sul registro (*on-chain*) da uno Smart Contract sia legale (ed *enforceable*) anche per il suo corrispondente nel mondo reale.

Inoltre, sia per quanto riguarda il caso di *asset* puramente digitale che quello di *digital twin*, il lavoro di Agid è enormemente delicato: dando piena efficacia a uno Smart Contract, si entra nell'ambito di quello che è stato definito *code-is-law*. La storia (cfr. TheDAO) ha già insegnato che gli Smart Contract possono essere soggetti a malfunzionamenti e bug che possono essere sfruttati da attori malevoli per far eseguire

allo Smart Contract istruzioni non espressamente volute dall'*owner* o autore. In questi casi, la linea di demarcazione non è per nulla nitida: se vale la logica del *code-is-law* allora anche le azioni non volute (potenzialmente fraudolente) saranno considerabili come 'legali' e quindi *enforceable*. Diversamente se si deve valutare caso per caso allora l'intera normativa del DL Semplificazioni perde di efficacia.

Un possibile accorgimento da adottare da un punto di vista tecnico potrebbe essere quello di prevedere la necessità per ciascuno Smart Contract di includere l'*hash* di un contratto tradizionale che descriva a parole quello che è stato codificato nello Smart Contract. Alcune tecnologie (cfr. Corda) hanno introdotto questo concetto di *Legal Prose*: se un attore malevolo dovesse sfruttare un *bug* del codice per eseguire delle operazioni non previste dalla *Legal Prose*, allora la transazione potrebbe essere ritenuta invalida e l'attore malevolo sarebbe costretto ad effettuare la transazione contraria (nel caso di *asset* reali l'*enforcing* potrebbe essere annullato).

Ad ogni modo, sarà necessario uno studio molto attento dei possibili risvolti dovuti alle specifiche proposte da Agid e sarebbe auspicabile l'avvio di un processo efficace di consultazione pubblica.

Considerazioni conclusive

Un tassello significativo del quadro regolamentare in materia di tecnologie DLT e Smart Contract è stato introdotto: le previsioni incluse nell'articolo 8-ter del Decreto rappresentano senz'altro un punto fermo nel percorso di innovazione al quale si sono avviate anche le autorità europee, nell'ambito di un più ampio scenario di digitalizzazione dei servizi di interesse pubblico.

Ciò, tuttavia, non può dirsi sufficiente né definitivo a fronte di esigenze sempre maggiormente insistenti sul fronte pratico-operativo.

Il contenuto e il livello di dettaglio delle definizioni previste, infatti, possono dirsi l'emblema della difficoltà di introdurre una volta per tutte una definizione chiara ed esaustiva che stabilisca a livello normativo i limiti necessari per operare.

La definizione *in itinere* delle procedure e delle specifiche tecniche potrebbe rappresentare un ostacolo per i prestatori di servizi e gli *stakeholders* interessati all'utilizzo di tali tecnologie innovative. La potenziale ampiezza di tali chiarimenti operativi potrebbe, altresì, richiedere un *effort* significativo, al fine di implementare correttamente e tempestivamente le misure che saranno previste in materia. Non vi è dubbio che l'iniziativa legislativa italiana, pioniera in ambito UE, sia lodevole. Siamo probabilmente di fronte all'avvio di un lungo percorso per rendere efficace questa rivoluzione tecnologico-giuridica.