Clusit
Associazione Italiana per la Sicurezza Informatica

Blockchain & Distributed Ledger:

aspetti di governance, security e compliance

In collaborazione con

POLITECNICO MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET digital innovation

Sommario

SOMMARIO 1

INTRODUZIONE DELL'OSSERVATORIO BLOCKCHAIN & DISTRIBUTED LEDGER DEL POLITECNICO DI MILANO 3

INTRODUZIONE DI GABRIELE FAGGIOLI, PRESIDENTE DEL CLUSIT 5

La Blockchain: considerazioni di base 8

Consenso distribuito 8

Classificazione delle Blockchain 9

Permissionless 11

Permissioned 12

Blockchain Pubblica 13

Blockchain Privata o Federata 14

Tokenizzazione 14

Sperimentazione, PoC, annunci e casi: la mappa della Blockchain nel mondo 17

L'impatto della Blockchain sui modelli di governance 21

Modelli di governance 21

Governance, fiducia, consenso 21

L'influenza delle Blockchain sui modelli di governance 22

Impatti sulla governance del cambiamento tecnologico 23

Impatti sulla corporate governance 24

Regulatory Environment 26

Alcuni aspetti legali e contrattuali degli Smart Contracts 27

Una possibile chiave di lettura: l'analisi sociologica del diritto 27

Definizione e caratteristiche principali degli Smart Contracts 28

"Code is Law" e la "Net-neutrality" 29

Il rapporto tra diritto e informatica: problemi di "trasposizione" 30

Proprietà giuridico/legali di uno Smart Contract e liabilities connesse 32

Gli Smart Contract e il diritto dei contratti 32

Altri profili giuridici di rilievo: legge applicabile e foro competente 34

La situazione italiana attuale 35

Blockchain e Privacy **37**
GDPR e Blockchain 37
Quale trattamento di dati personali nella Blockchain permissioned? 38
La difficile individuazione dei ruoli privacy 40
Il trasferimento dei dati 41
L'esercizio dei diritti degli interessati 41
Le attività di standardizzazione **42**
Perché standard su Blockchain 42
I lavori in ambito ISO 43
I lavori in ambito CEN/CENELEC e nazionale 44
Conclusioni 44
Cyber attacchi **46**
La Governance della security nei progetti DLT **50**
L'impatto della Blockchain sull'Information Security 51
Garantire la qualità e la sicurezza del codice 53
Perché è importante? 53
Garantire la qualità e la sicurezza del codice: l'infrastruttura 54
Garantire la qualità e la sicurezza del codice: il backend 54
Garantire la qualità e la sicurezza del codice: il front end 56
Garantire la qualità e la sicurezza del codice: gli Smart Contracts 57
Garanzie a contorno del funzionamento del "codice" dello Smart Contract 58
Blockchain come opportunità per strumenti a supporto dell'information & cyber security **60**
Log Management 60
Identity and Access Management (IAM) 61
Certification Authority 61
DNS 61
Tracciamento attività audit 62
AUTORI E LICENZA D'USO 63

Introduzione dell'Osservatorio Blockchain & Distributed Ledger del Politecnico di Milano

Quando si pensa agli esordi della Blockchain e alla sua diffusione si pensa immediatamente alla possibilità di dare vita a una alternativa ai sistemi "transazionali" centralizzati. Non per caso il primo pensiero va alla Blockchain come alternativa al mondo bancario come lo abbiamo sempre conosciuto. Solo più recentemente, l'immagine della Blockchain si è arricchita di nuovi contenuti e si configura come alternativa ai sistemi centralizzati di tanti altri settori.

La prospettiva "titanica" di "attaccare" o mettere in discussione il mondo delle banche e le organizzazioni "centralizzate" ha fatto passare sottotraccia un aspetto della Blockchain che potrebbe essere anche più radicale della contrapposizione tra modelli centralizzati e distribuiti: ovvero la rivisitazione del paradigma della sicurezza e della privacy.

Quasi come un benefico effetto secondario che si scopre a valle di un progetto che aveva altri obiettivi, la Blockchain invita a ripensare l'approccio alle logiche di security delle transazioni, di privacy dati e di accesso. Già nella fase più buia della "rete dei blocchi", con i media concentrati a criminalizzarne l'utilizzo da parte di soggetti che sfruttavano le prime criptocurrency per transazioni illegali, è apparso chiaro a molti che quelle criticità potevano benissimo rappresentare una opportunità. Ovvero, permettevano di passare da una sicurezza basata sul concetto di "cassaforte centralizzata e blindata", ad una sicurezza basata sul concetto di una comune responsabilità sul valore del dato, di un coinvolgimento di tutti i partecipanti grazie a un approccio distribuito. In altre parole, da un unico grande "caveau" iperprotetto a tante "casseforti" distribuite ovunque, presso tutti i server di tutti i partecipanti, tutte, paradossalmente aperte per quanto attiene l'accesso, ma blindatissime per quanto concerne la possibilità di "appropriarsi" dei dati, ovvero di utilizzarli o modificarli per altri scopi.

E il passaggio da un "tutto al centro", ad un "tutto distribuito" conta su una leva ancora una volta innovativa rispetto ai modelli tradizionali: la condivisione della responsabilità e la distribuzione della fiducia.

Appare così evidente che il paradigma dell'Internet of Value ha tutte le caratteristiche per cambiare anche l'approccio alla sicurezza. Tuttavia, non si deve correre il rischio di interpretare la Blockchain come una soluzione per "la sicurezza", quanto di un importante "effetto secondario" che permette di passare ad un ambiente che non è necessariamente più sicuro, ma che stabilisce regole e comportamenti che possono contribuire e ridurre i fattori di rischio. Non è in definitiva corretto pensare alla Blockchain come ad una soluzione per garantire maggiore sicurezza, ma come a una soluzione che permette di affrontare in modo nuovo (anche) la sicurezza e pone temi nuovi rispetto ai requirements del "mondo centralizzato".

E questo primo punto è tanto più vero se si pensa che con la Blockchain sono arrivate anche tante nuove minacce e l'industria della sicurezza non ha certo perso l'occasione per mettere a disposizione strumenti e strategie per ridurre anche questi nuovi fattori di rischio.

Se poi si guarda ai Registri Distribuiti dal punto di vista della loro stessa sicurezza, il cambio di paradigma impone una rilettura del senso stesso di "minaccia digitale", non più indirizzata "al singolo" inteso come soggetto fisico o come azienda, ma alla "comunità" e l'individuazione di nuove forme di protezione passa a sua volta dalla collaborazione di più soggetti.

L'immagine di Blockchain come luogo sicuro in assoluto è una immagine "insicura", al contrario occorre guardare alla fotografia della Blockchain come a un ambiente che permette di disegnare nuove "architetture" che permettono di ridurre e governare i fattori di rischio e di minimizzare l'esposizione delle imprese alle nuove minacce. La Trasparenza e l'Immutabilità della Blockchain sono un deterrente nei confronti della diffusione di cattive pratiche e sono allo stesso tempo un acceleratore nella identificazione di punti di debolezza. La crittografia offre garanzie che unite alle diverse forme di Consenso, permette di predisporre dei modelli comportamentali che rispettano le logiche "Secure by design" e che se non riducono in assoluto i fattori di rischio, offrono maggiori possibilità per gestirli.

È significativo ricordare che proprio nei primi mesi di quest'anno uno dei maggiori exchange del mondo cripto, l'americana Coinbase, ha acquisito la startup italiana Neutrino specializzata nell'analisi, nella ricerca e nell'identificazione di frodi, minacce e transazioni illegali sulle Blockchain. Un fatto significativo rispetto alla necessità di affrontare il tema della sicurezza puntando sempre di più sull'intelligenza e sullo studio di comportamenti e dei flussi. La Blockchain permette di lavorare sulla conoscenza e di accelerare l'individuazione e la sperimentazione di soluzioni e un altro esempio lo si può trovare anche nel fenomeno delle "SideChain", nella possibilità cioè di "spostare fuori dalla Blockchain" quelle transazioni e quei dati che rischiano di non adattarsi ai criteri e alle logiche di apertura delle Blockchain pubbliche e che possono trovare "maggiore protezione" su canali esterni, in forma di compromesso tra permissionless e permissioned Blockchain, a testimonianza che la presunta "inflessibilità" della Blockchain si può superare per dare risposte più efficaci anche sulla security.

Resta poi da evidenziare, oggi più mai, il tema del rapporto tra la protezione e la privacy dei dati personali e le tante possibili "declinazioni" nel mondo Blockchain. Si tratta di un ambito che rivela come il rapporto tra dati, sicurezza, privacy e Blockchain sia da affrontare in chiave multidisciplinare a partire dall'assunto che "Code is Law". Perché se è vero che la prima fonte di "insicurezza" arriva dai comportamenti è altrettanto vero che, i buoni comportamenti trovano sempre di più la loro attuazione proprio grazie all'evoluzione di un codice che, sfruttando la programmabilità della Blockchain, possa "programmare" le buone pratiche.

Introduzione di Gabriele Faggioli, Presidente del Clusit

In questi mesi la Blockchain e la distributed ledger technology (DLT), stanno raggiungendo il punto di massima attenzione ed entusiasmo: sono innumerevoli le iniziative pubbliche e private in cui se ne discute e gli articoli dove se ne scrive. Si cominciano anche, finalmente, a vedere le prime applicazioni pratiche.

Anche la politica considera questa tecnologia come potenzialmente in grado di impattare profondamente sulla società: si intravedono possibili utilizzi che potrebbero in pochi anni rivoluzionare la vita dei cittadini, delle imprese e della pubblica amministrazione.

Si dice che con la Blockchain si potrebbe battere nuova moneta, si potrebbero rivoluzionare le modalità di voto in sede elettorale, si potrebbe garantire la provenienza delle merci nella logistica, si potrebbe certificare l'autenticità degli atti notarili, sarebbe possibile pagare automaticamente i premi assicurativi, si potrebbero snellire le procedure di acquisizione e verifica dei certificati medici da parte delle società sportive e così via.

Tutte ipotesi di lavoro estremamente interessanti e potenzialmente utilissime, ma dove la sicurezza gioca un ruolo essenziale. Riteniamo, quindi, parte fondamentale della mission del Clusit mettere in guardia l'industria e l'amministrazione pubblica dai rischi dovuti ad un uso superficiale della Blockchain ed in generale di qualunque tecnologia.

Il nostro obiettivo non è quello di sconsigliare l'uso e la sperimentazione della Blockchain, anzi! Il Clusit, al contrario, sostiene da sempre l'innovazione tecnologica e la sperimentazione. Ma ogni nuova tecnologia rappresenta oltre a una opportunità anche un rischio, non sempre conosciuto, compreso e affrontato adeguatamente. Anche la Blockchain, quindi, deve essere affrontata considerando gli angoli "bui", analizzandone i pregi e i rischi, le opportunità e i pericoli.

Il mondo deve evolversi, ma l'evoluzione deve essere sicura. Non è più possibile buttare il cuore oltre all'ostacolo. Occorre, come in altri contesti come l'intelligenza artificiale, muoversi con grande attenzione, studio e analisi prima di mettere sul mercato prodotti che potrebbero trasformarsi in armi contro il singolo e la collettività.

Lasciamo ad altri l'analisi precisa di cosa si possa fare con la Blockchain e con la DLT: per questo abbiamo chiesto la collaborazione dell'Osservatorio Blockchain & Distributed Ledger del Politecnico di Milano.

Continuando la lettura di questo Position paper, il lettore troverà alcune domande da fare ai propri team che stanno valutando o implementando la tecnologia per motivi di business, come per esempio:

- Che impatto ha sull'organizzazione aziendale e la governance?
- Come si può controllare la qualità e la sicurezza del software che usiamo? Che garanzie ci dà il vendor o il consorzio che ce lo fornisce?

- Chi è responsabile di un malfunzionamento del software degli Smart Contract che viene sviluppato?
- Come ci si garantisce dalle frodi di interfaccia tra la Blockchain e il sistema informativo tradizionale?
- Che leggi ci sono o presumibilmente ci saranno che possono vanificare i nostri investimenti o, al contrario, portarli a (maggior) valore?
- Se la Blockchain è pubblica i dati sono esportabili all'estero?
- La Blockchain è compatibile con il GDPR? Come si può risolvere il problema del diritto all'oblio se ciò che va sulla Blockchain non è cancellabile?

Alcune note finali.

Abbiamo fatto uno sforzo per censire i problemi di sicurezza che potrebbero derivare dalla tecnologia Blockchain e ciò per identificare i vantaggi che potrebbero avere eventuali insider, attaccanti esterni o cyber criminali. (si veda il capitolo Cyber attacchi).

Nel Position paper abbiamo soprattutto fatto riferimento al contesto delle Blockchain private, permissioned, ed evitato di approfondire le cryptovalute. Intravediamo, infatti, nelle Blockchain private un maggior uso potenziale in scenari aziendali, anche se il tema è ancora da esplorare compiutamente.

In questo Position paper vi sono alcune solo alcune indicazioni relative al funzionamento della tecnologia rimandando per approfondimenti alle molte pubblicazioni specializzate di altri autorevoli autori (a parte i numerosi libri sull'argomento, tra cui uno in italiano scritto da uno dei nostri contributori[1], un buon compendio lo abbiamo trovato qui: https://www.Blockchain4innovation.it/esperti/Blockchain-perche-e-cosi-importante/).

Nel momento in cui consolidiamo questo documento, una parte del nostro team sta redigendo uno schema di intervista da somministrare ad aziende e amministrazioni che già sperimentano l'uso della Blockchain e del DLT. Contiamo di poter raffinare il nostro contributo con il loro aiuto in un secondo tempo.

Consideriamo questo Position paper come un primo passo ed è nostra intenzione continuare nel 2019 con altre pubblicazioni da mettere a disposizione delle aziende e della collettività.

Un mio particolare ringraziamento va agli autori di questo Position paper: è stata una bellissima esperienza lavorare con loro, tutti grandi professionisti preparatissimi su questi temi. I loro nomi li trovate in calce.

[1] Roberto Garavaglia, Tutto su blockchain, Hoepli, aprile 2018 https://www.hoepli.it/libro/tutto-su-blockchain/9788820383145.html

Una copia elettronica di questo documento è disponibile sul sito internet del Clusit: https://www.clusit.it. La licenza d'uso è Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) https://creativecommons.org/licenses/by-nc-sa/4.0/

Gabriele Faggioli Presidente CLUSIT

La Blockchain: considerazioni di base

Una soluzione basata su Blockchain prevede generalmente lo sfruttamento di una piattaforma in cui i partecipanti possono svolgere determinate funzioni che risultano nella scrittura o lettura di un dato su un **sistema di registri distribuiti**, il cui governo e controllo possono essere decentralizzati, acceduto da una pluralità di enti connessi ad una rete peer-to-peer.

Il meccanismo, in termini molto semplificati, ma utili alla nostra analisi, prevede che quando un ente richiede di effettuare una transazione, la richiesta sia propagata sulla rete che ne **verifica la legittimità**, inserendola in un "**blocco di informazioni**" in attesa di validazione.

Tale processo, che per le Blockchain pubbliche come quelle dei Bitcoin è chiamato "**processo di verifica indipendente**", precede quello di validazione effettiva che si avrà con il mining del blocco ed è eseguito da ciascun singolo nodo, senza ancora preoccuparsi di cosa stiano facendo, nello stesso istante (e magari sulle medesime transazioni), gli altri. In questa fase ciascun nodo non si preoccupa di raggiungere quel consenso distribuito che avverrà successivamente con la validazione del blocco nel quale sono inserite le transazioni verificate.

I partecipanti alla Blockchain **aggiorneranno la propria copia di registro solo con il nuovo blocco validato** da un soggetto (il c.d. "nodo validatore") che ottiene la fiducia di tutti, sotto forma di **consenso distribuito** raggiunto mediante **l'adozione di regole comuni** e grazie a un **sistema di incentivi** o di **regole di governance** accettate da ciascun ente.

Sulle Blockchain pubbliche come quella dei Bitcoin ciascun nodo che si accinge a validare un blocco di transazioni opera "in concorrenza" con gli altri, cercando di risolvere per primo un problema matematico complicato; un'attività, questa, molto costosa in termini di risorse necessarie che è altresì nota con il nome di "**mining**" (nell'analogia con il processo di estrazione dell'oro, richiedente molti sforzi a una collettività di individui - i minatori - che lavorano gli uni in competizione con gli altri su una risorsa naturale "scarsa").

Ciascun blocco, allorquando validato, sarà "**collegato crittograficamente**" al nodo precedente mediante un sistema di **marcature temporali** (o "timestamp"), formando in questo modo una catena di blocchi (una "Blockchain" appunto) validati.

In definitiva, i blocchi così strutturati conterranno una sequenza ordinata di transazioni verificate e validate, la cui verità è stata accettata dall'insieme di partecipanti che ha adottato le stesse regole del protocollo di consenso distribuito.

Consenso distribuito

Proof of Work e Proof of Stake sono due esempi di protocolli per il consenso distribuito.

Il primo (altresì noto come "**PoW**") si basa sulla risoluzione di una complicata serie di operazioni crittografiche (possiamo definirlo un "cripto-puzzle") che ciascun nodo validatore deve compiere in competizione con gli altri. Solo il nodo che per primo riuscirà a risolvere il

cripto-puzzle avrà diritto a "imporre" la propria "**verità storica**" (ossia la sequenza delle transazioni verificate da ciascun singolo nodo) e **verrà remunerato** tramite **l'attribuzione di una ricompensa** espressa in criptoasset tipici della Blockchain su cui opera la validazione dei blocchi, nonché mediante l'incasso degli **incentivi associati a ciascuna transazione presente nel blocco.**

Una tipologia di protocollo per il consenso distribuito alternativa alla PoW è la **Proof-of-Stake** (PoS). Mentre la PoW si basa solo sulla capacità di calcolo dei nodi validatori, la PoS considera **la quota effettiva di criptoasset nella disponibilità del nodo intenzionato a validare**. Quindi, in un sistema PoS, più quote di criptoasset si hanno nella rete, più si possono validare i blocchi. Per esempio, se un miner detiene una quota del 5% del totale della criptovaluta in circolazione, tale miner può validare solo il 5% dei blocchi.

I due meccanismi descritti sono normalmente impiegati nelle Blockchain cosiddette "**pubbliche**".

Come vedremo in seguito, però, esistono anche altre tipologie di Blockchain definite "**private**" o "**ibride**" che impiegano sistemi diversi per raggiungere il consenso distribuito, generalmente basati su BFT (Byzantine Fault Tolerance) ispirato alla metafora dei generali bizantini.

La metafora dei generali bizantini è utilizzata nei sistemi informatici distribuiti ogni volta che si ha la necessità di determinare una votazione il cui risultato può essere o vero o falso e quando si rende necessario efficientare il più possibile il lavoro di determinazione del voto stesso. Questo scenario può rappresentare il problema tipico del consenso distribuito su una Blockchain, dove si cerca di individuare un protocollo alternativo alla Proof-of-Work e alla Proof-of-Stake al fine di risparmiare energia, avendo comunque la certezza di raggiungere un'unica versione di verità verso la quale converge una maggioranza di consensi.

Il problema: ci sono alcuni generali (in numero dispari) dell'Impero Bizantino che stanno accerchiando la città di Roma, ognuno con il proprio esercito. Per espugnare la città i generali devono decidere se attaccare o ritirarsi. La situazione a contorno impone che i generali possano comunicare solo tramite messaggeri e che sia impedito loro di riunirsi; inoltre si è a conoscenza dell'esistenza di alcuni traditori infiltratisi nel gruppo, ma non se ne conosce l'identità e neppure il numero. L'assedio avrà successo se i generali leali riescono a trovare un accordo sulla loro strategia.

Fuor di metafora, il consenso sulla Blockchain viene raggiunto quando vi è un rapporto tra miner "buoni" e miner "disonesti" predeterminato, la cui validazione è risolta dall'algoritmo di derivazione BFT, ossia Byzantine Fault Tolerance.

Classificazione delle Blockchain

Le Blockchain si basano, come detto, su **tecnologie a registri distribuiti o DLT (Distributed Ledger Technology)** con la caratteristica organizzazione dei dati raggruppati in blocchi di transazioni, l'un l'altro legati secondo una sequenza temporale.

Esistono altre architetture dati che possiamo considerare DLT, ma non Blockchain, come Tangle o Hashgraph che presentano un'architettura dati nota come DAG: Directed Acyclic Graph.

Per poter adeguatamente classificare questa tecnologia è utile separare le caratteristiche che sono comuni a tutte le Blockchain, definendole tali di fatto, e quali invece possono variare generando dei sottoinsiemi con vantaggi propri e distinti.

Caratteristiche che accomunano le Blockchain:

- **Sistema distribuito:** una Blockchain è un sistema distribuito su un'ampia rete di nodi i cui dati registrati sono protetti da attacchi in quanto le stesse informazioni sono replicate, verificate e validate mediante l'adozione di diversi protocolli (o regole) comunemente accettati da ciascun ente;

- **Immutabilità delle informazioni trascritte**: in una Blockchain i dati registrati e validati non possono essere modificati perché ogni nuova informazione è indissolubilmente legata allo storico delle transazioni precedenti, eventuali manipolazioni di dati, quindi, sarebbero immediatamente evidenziate non consentendo la successiva validazione.

Caratteristiche che differenziano le Blockchain:

- **Permessi di partecipazione alla rete e governance**: permissioned vs permissionless;

- **Poteri di lettura e scrittura associati ai vari utenti**: quali utenti hanno diritto di scrivere nuove transazioni? quali possono solo consultare il registro? a che condizioni?

- **Fiducia tra i partecipanti alla rete**: esiste un ente del quale tutti si fidano che orchestra le attività sulla piattaforma oppure non è necessario in quanto il meccanismo di fiducia è cablato nel protocollo?

- **Meccanismo di validazione delle operazioni**: quale protocollo di consenso distribuito adottare?

Ai fini del presente documento riteniamo utile classificare la Blockchain secondo due direttrici: Permessi e Governance (legata alla proprietà della piattaforma).

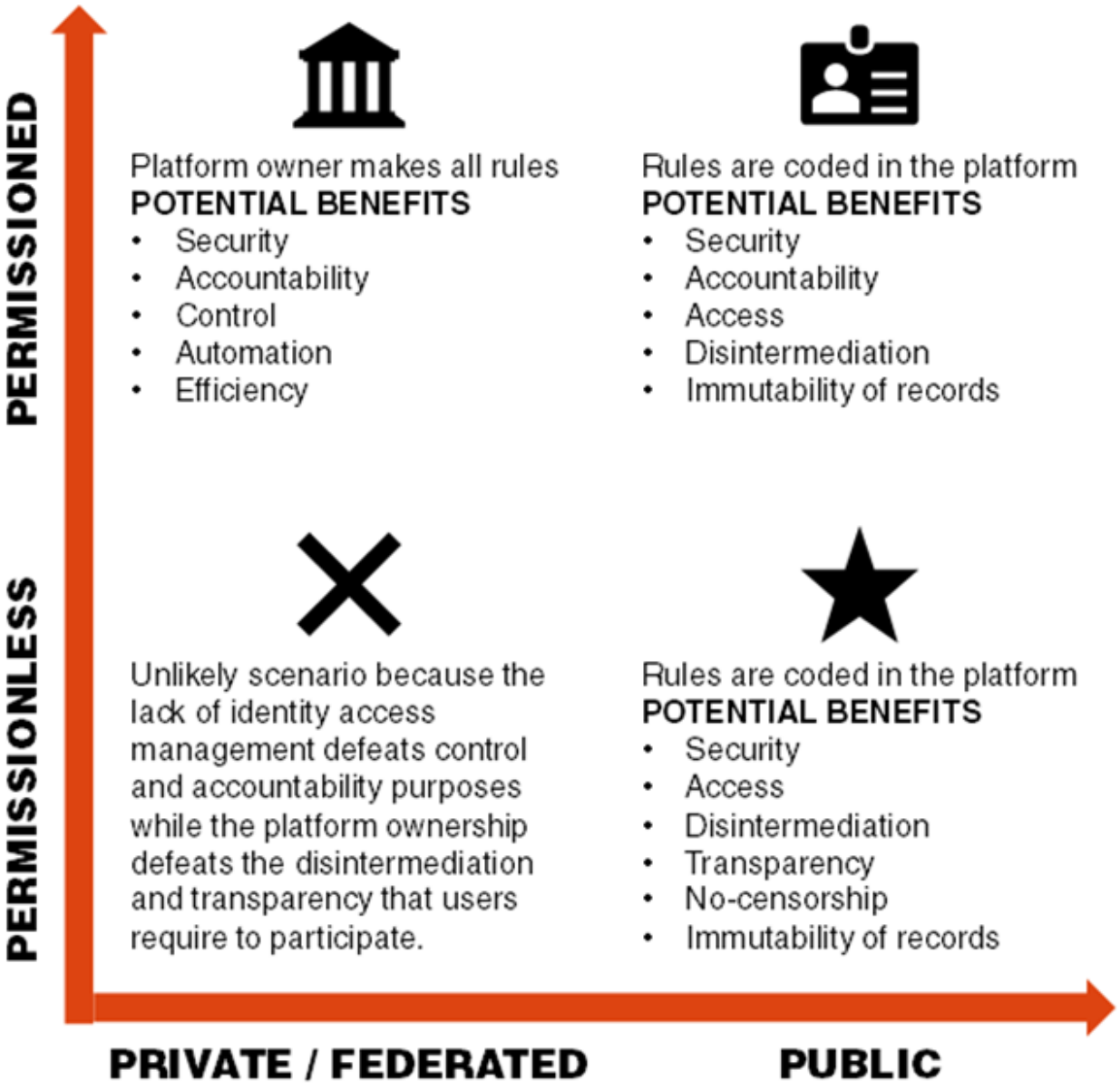


Figura 1: Una possibile classificazione della Blockchain

Permissionless

Una piattaforma Blockchain "**permissionless**" è aperta al pubblico che può scaricare il relativo software, vedere ogni transazione riportata sul registro, effettuare operazioni e candidarsi, a sua volta, ad effettuarne la validazione.

La Blockchain permissionless per l'eccellenza è quella del Bitcoin e si dice tale (ossia priva di permessi) perché non serve alcuna autorizzazione per fruire della piattaforma, che, tuttavia, grazie alle sue caratteristiche tecniche è al riparo da attacchi atti a minarne l'efficacia.

Gli attori che operano sulla piattaforma sono inoltre pseudonimizzati rendendo così le transazioni

non direttamente riconducibili a persone fisiche. Infatti, è assolutamente certo l'indirizzo (o lo pseudonimo, o wallet) che ha originato la transazione, ma non è identificabile in modo diretto e certo la persona fisica che possiede la chiave privata che controlla quell'indirizzo.

La seguente figura illustra le caratteristiche principali delle piattaforme permissionless (in rosso sono evidenziati gli aspetti che connotano tali Blockchain, favorendo il lettore nella comprensione di ciò che le contraddistingue rispetto alle Blockchain "permissioned" di cui si vedrà in seguito).

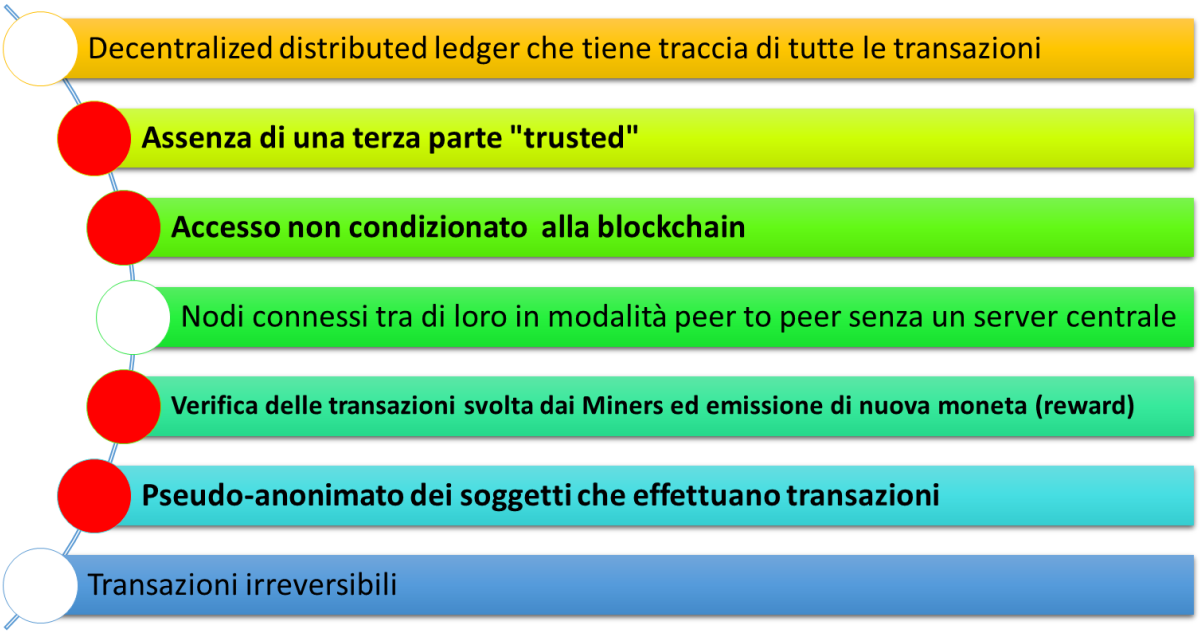


Figura 2: Principali caratteristiche delle Blockchain permissionless

Permissioned

La Blockchain "**permissioned**" (o anche "permission") invece prevede una qualche forma di regolamentazione degli accessi e dei poteri che ciascun utente ha sulla piattaforma. In questa categoria rientrano, ad esempio, Blockchain come Corda, Hyperledger e Ripple.

È attualmente presente un vivace dibattito sull'utilità di tali sistemi in ragione del fatto che i medesimi mettono in discussione una delle caratteristiche più rivoluzionarie della Blockchain "pura", ossia la possibilità di pervenire alla **disintermediazione di un ente centrale (o terzo)** datore di fiducia, negli scambi di valore.

Questi ultimi, invece, nelle Blockchain permissioned sarebbero in qualche modo influenzati (o influenzabili) da chi definisce le regole di accesso e fruizione della piattaforma.

Di là della precedente considerazione, le Blockchain "permissioned" restano uno strumento importante per le organizzazioni che possono trovare in queste soluzioni il giusto compromesso nello sfruttare alcune caratteristiche della Blockchain, come l'**immutabilità** delle informazioni trascritte e la **distribuzione** dei dati su più nodi, operando comunque in un perimetro nel quale è

possibile esercitare il livello di controllo necessario per essere conformi alle normative che impattano sulle medesime.

La seguente figura illustra le caratteristiche principali delle piattaforme “permissioned” (in verde sono evidenziati gli aspetti che connotano tali Blockchain, favorendo il lettore nella comprensione di ciò che le contraddistingue rispetto alle Blockchain “permissionless” di cui si è detto in precedenza).

Figura 3: Principali caratteristiche delle Blockchain permissioned

Blockchain Pubblica

Una Blockchain pubblica non è controllata da nessuna autorità centrale, né da un gruppo di autorità, ma dalla comunità intera che esercita tale controllo per proteggere i propri interessi.

Quella dei Bitcoin è un classico esempio di Blockchain pubblica: le transazioni sono validate dai nodi cosiddetti “minatori” (o “miners”) e chiunque può essere un miner che compete con gli altri per ottenere una ricompensa in bitcoin. Tale appannaggio gli consentirà di essere remunerato per aver svolto diligentemente la sua funzione, ossia validare i blocchi di transazioni verificate.

Questo tipo di piattaforma rappresenta una grande innovazione rispetto al passato, in quanto, prima dell’avvento del Bitcoin, qualsiasi piattaforma tecnologica aveva un proprietario che ne moderava l’attività ed era responsabile della correttezza dei dati transazionali su di essa registrati. Queste funzioni, nella Blockchain pubblica, sono invece svolte dal protocollo stesso e dall’accettazione comune del medesimo.

Ma questo modello presenta anche delle criticità (su cui la comunità di esperti sta lavorando) la più importante delle quali è relativa alla **scalabilità**. Per meglio spiegare questo problema è sufficiente fare riferimento alla capacità della Blockchain del Bitcoin di processare solamente circa sette

transazioni al secondo; è evidente come ciò potrebbe costituire un limite difficilmente superabile nel caso in cui una porzione molto ampia della popolazione mondiale intendesse usarla come metodo di pagamento.

Blockchain Privata o Federata

Una piattaforma Blockchain privata prevede che alcune attività sulla stessa eseguite siano soggette al **controllo di un ente centrale che definisce alcune regole**. Nel novero di tali attività troviamo quelle che permettono di **assegnare le autorizzazioni** a soggetti **noti** che possono accedere al registro distribuito.

Questo assunto si pone in antitesi con lo sfruttamento dei benefici connaturati alla disintermediazione offerta dalle Blockchain pubbliche, poiché di fatto tutte le operazioni sono soggette al controllo e alla gestione dell'ente centrale nel quale si deve aver fiducia. Le transazioni, infatti, sono validate solo da chi ne ha diritto in base a quanto stabilito dall'ente centrale medesimo.

Restano i **benefici di immutabilità** (comunque discutibile per via della possibilità di "biforcare" unilateralmente la catena, modificando quindi lo storico) e di **distribuzione** dei dati su un ampio numero di nodi, nonché il superamento dei problemi di scalabilità e sostenibilità energetica delle Blockchain pubbliche.

Una via di compromesso tra la Blockchain pubblica e quella privata è rappresentata dalla Blockchain **federata** o **consorziata**, dove il processo di validazione del consenso è attuato da individui o organizzazioni, come per esempio un consorzio di istituti finanziari clienti di un'azienda, **noti** e **preselezionati** da un'entità terza fidata.

Si presuppone un certo livello di fiducia esistente tra i soggetti federati, il che riduce la necessità di un meccanismo di validazione come la Proof-of-Work, aprendo la possibilità di usare per lo stesso fine meccanismi meno gravosi dal punto di vista della scalabilità e consumo energetico.

La federazione può quindi **distribuire il potere** e le **responsabilità** tra i suoi membri secondo **modelli di governance** che possono variare in base agli scopi della piattaforma e mitigare la centralizzazione del potere insita nella Blockchain privata.

Tokenizzazione

Descriviamo ora sommariamente (nell'economia di questo contributo) cosa significa il termine "**tokenizzazione**" e perché è importante farlo all'interno di questo Position paper.

Prima però di addentrarsi nel dettaglio è opportuno fornire alcune definizioni di base[2] che consentono di meglio collocare il processo di tokenizzazione nel contesto di una Blockchain.

[2] Le definizioni e le argomentazioni che seguono sono tratte dal libro "Tutto su blockchain" di Roberto Garavaglia, Hoepli editore, aprile 2018

Proponiamo, quindi, il significato dei seguenti termini: **asset**, **criptoasset** e **token**.

Con **asset** intendiamo ogni entità materiale o immateriale suscettibile di valutazione economica soggettiva; i diritti connessi all'utilizzo e allo sfruttamento delle attività, materiali o immateriali che siano, si possono concentrare in titoli finanziari rappresentativi dei diritti stessi. Gli asset sono scambiabili su piattaforme di scambio tradizionali (anche non basate su Blockchain).

Con **criptoasset** vogliamo riferirci a una **rappresentazione digitale di valore** resa univoca grazie all'impiego di meccanismi crittografici; i criptoasset possono essere "depositati" e **scambiati** su piattaforme Distributed Ledger, rispettando le regole di un protocollo di Blockchain e, in questo caso, si parla di "**asset nativi**".

Con **token** significhiamo una "legatura digitale" della legittimazione di un diritto al titolo rappresentato dal criptoasset che consente di creare un legame tra un bene fisico (oppure un bene "off chain", ossia che sta al di fuori della Blockchain) e un asset nativo delle Blockchain.

Il token è **scambiabile** su piattaforme Distributed Ledger.

Condivisa questa (indispensabile) tassonomia, parliamo, orbene, del legame dell'**asset nativo** presente su alcune Blockchain permissionless e permissioned con il mondo degli scambi in un'economia reale. L'asset nativo (e i sistemi che lo supportano) si rende molto utile in tutti quei casi in cui si voglia ottenere garanzia dell'**immutabilità di una transazione** e della corretta esecuzione di un codice informatico che deve produrre un risultato inconfutabile.

Può avere molto senso, pertanto, sfruttare una tecnologia che riesce a **riprodurre il concetto di scarsità nel mondo digitale**, per offrire prove incontrovertibili dell'avvenuta transazione di un bene fisico (pensiamo ad una proprietà) ma anche di un bene immateriale (come la quota di un fondo, un diritto d'autore o un brevetto) se attribuissimo al criptoasset il valore di un gettone o, appunto, di **token**.

Al fine di meglio comprendere il complesso sistema che ruota intorno ai concetti di token e di tokenizzazione, può rendersi utile ricorrere alla metafora del gettone telefonico (in uso qualche anno fa…), con cui era possibile effettuare delle chiamate a pagamento tramite i telefoni pubblici. Il valore monetario attribuito al gettone era variabile nel tempo ed il suo consumo (o, meglio, il suo utilizzo) era legato ad una **logica programmata** nel sistema telefonico associata allo "scatto" (il famoso scatto telefonico che ha preceduto la tariffa a tempo).

Attribuendo un valore nominale al criptoasset, ovvero legandone **la legittimazione di un diritto al titolo che esso rappresenta**, si crea quel legame tra un bene fisico e un asset nativo delle Blockchain. Un asset che, in quanto digitale, è scambiabile su piattaforme Distributed Ledger e diviene **perno di un sistema transazionale**, in cui **la validità dei negozi giuridici sottostanti** è garantita da un sistema matematico tale da ricreare quel rapporto di fiducia, anche tra estranei, senza bisogno di una terza parte intermediaria.

Importante è dunque capire che, mediante un procedimento di tokenizzazione, è possibile conferire anche ad asset non digitali alcune caratteristiche tipiche delle Blockchain permissionless o permissioned, fra cui:

- la **programmabilità**, laddove l'esecuzione di una transazione su Blockchain può essere vincolata a un set di regole predefinite e "cablate" all'interno del token che determinano

come (o dove) può essere impiegato il sottostante rappresentato dal token stesso;

- la **verificabilità** e la **tracciabilità**, laddove tutte le transazioni effettuate mediante token su una Blockchain permettono di mantenere una traccia immutabile degli scambi avvenuti tramite (l'impiego di) ciò che il token rappresenta, su un registro distribuito verificabile da terze parti.

Sperimentazione, PoC, annunci e casi: la mappa della Blockchain nel mondo

La Blockchain si sta avvicinando con prudenza al mondo reale. A dispetto del fortissimo interesse mediatico registrato negli ultimi due anni, i progetti basati sull'utilizzo delle tecnologie dei "Registri Distribuiti" si muovono prevalentemente in un ambito di sperimentazione.

Se si tasta il polso ai progetti, anche estremamente importanti, in corso in tutto il mondo, si vede che l'approccio delle imprese e delle organizzazioni punta ad arrivare in "produzione" solo dopo un percorso, rigoroso e attento, di test.

Nella maggior parte dei casi muoversi verso la Blockchain vuol dire oggi adottare la strategia dei Proof of Concept (PoC), ovvero una sperimentazione guidata, protetta e gestita dai diversi, spesso numerosi attori coinvolti nei progetti.

L'Osservatorio Blockchain & DLT sta seguendo questo fenomeno da tre anni partendo dalla convinzione che la Blockchain porta a un profondo cambio paradigmatico che consente alle imprese e alle organizzazioni di entrare in una dimensione "transazionale" in assenza di fiducia definita come Internet of Value.

Il presupposto di base è nella logica della Blockchain che permette il trasferimento di asset di valore in forma digitale garantendone la unicità con un sistema di algoritmi e di regole crittografiche capaci di gestire, grazie a una procedura di consenso, le modifiche di un registro distribuito, sul quale vengono tracciati, in modo univoco e immutabile, i passaggi di valore.

Il registro distribuito e il sistema di consenso fanno della Blockchain una piattaforma adatta alla gestione di processi transazionali e di business in ambienti complessi, dove non esiste naturalmente una situazione di fiducia tra le parti coinvolte.

Per questa ragione la Blockchain è identificata come la tecnologia "della fiducia", permettendo a imprese e organizzazioni di costruire un nuovo valore e di proteggerlo in forma collaborativa con altre imprese o organizzazioni.

Partendo da questa premessa l'Osservatorio ha identificato alcuni criteri per cui può avere senso valutare di applicare una soluzione blokchain-based rispetto a tecnologie tradizionali. Tali condizioni sono necessarie, ma non sufficienti per l'applicabilità della Blockchain:

- Interazione con numerosi attori: per gestire le relazioni solo tra 2 o 3 attori, la Blockchain non è necessaria, mentre potrebbe essere utile se vi sono molti attori coinvolti che vogliono interagire.
- Mancanza di fiducia tra gli attori: se gli attori si conoscono molto bene e si fidano tra di loro, non hanno bisogno della soluzione Blockchain; mentre potrebbero averne bisogno quegli attori che non si fidano tra loro o non hanno mai identificato una terza parte fidata.
- Eterogeneità degli attori: se gli attori coinvolti sono molto simili con esigenze similari, è più facile trovare un accordo comune senza bisogno della Blockchain, mentre potrebbe portare del valore se gli attori hanno obiettivi differenti e contrastanti che potrebbero essere regolati da Smart Contract.

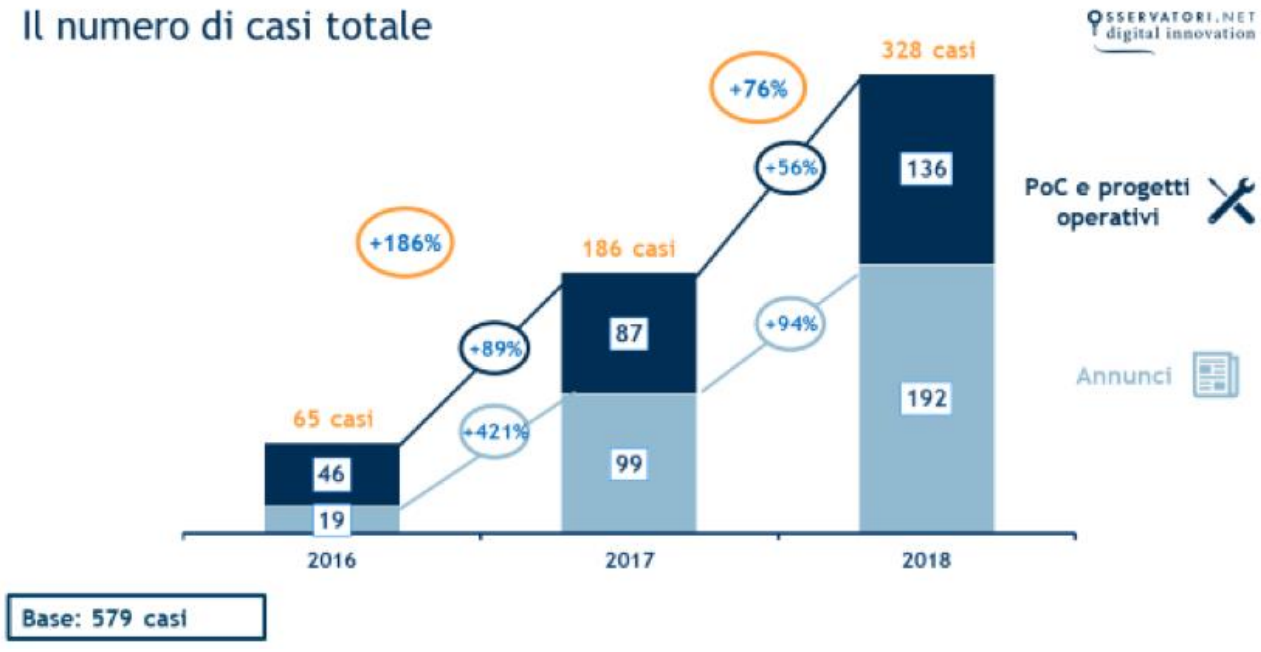
- Necessità di condividere le informazioni: se gli attori non vogliono condividere le informazioni con altri attori, allora le soluzioni basate su registri distribuiti non sono adatte, mentre la Blockchain può portare valore se vi è la necessità di condividere le informazioni tra più attori.
- Importanza di trasparenza e immutabilità delle informazioni: se le informazioni da condividere possono essere modificate a posteriori, allora la Blockchain non è la soluzione ottimale, mentre la Blockchain può garantire l'immutabilità del registro
- Presenza di un asset univoco da trasferire: se non vi è la possibilità di identificare un asset univoco da tracciare, allora la Blockchain non è necessaria; mentre può essere estremamente utile per tracciare i trasferimenti di un asset univoco.
- Digitalizzazione: se non è possibile automatizzare alcuni processi e alcune procedure perché è necessario un intervento umano per l'esecuzione di un contratto, allora le tecnologie basate su Smart Contract potrebbero non essere di aiuto, mentre aiutano dove è possibile definire degli algoritmi per regolare le transazioni di asset digitali.

L'Osservatorio ha mappato la realtà della Blockchain nel mondo prendendo in esame, da gennaio 2016 a dicembre 2018, 579 casi costituiti da 269 Proof of Concept e progetti operativi e 310 annunci di progetti.

Da questa mappatura è emerso un primo dato legato alla vitalità del fenomeno: nel 2016 i casi erano complessivamente 65, costituiti da 46 PoC e progetti operativi e 19 annunci.

Nel 2017 i casi sono saliti a 186 (87 tra PoC e progetti e 99 annunci) per arrivare ai 328 del 2018 che a fine dicembre 2018 contavano 136 Proof of Concept e 192 annunci.

La progressione è evidente anche se i valori assoluti restano ancora limitati.



Il mercato sceglie indiscutibilmente le soluzioni basate su Blockchain private rispetto a quelle basate sulle pubbliche. I progetti o gli annunci basati su Blockchain pubbliche nell'orizzonte temporale 2016-2018 (contando le unità su ogni anno) sono complessivamente 47. Il 90% del mercato attuale guarda alle Blockchain private.

Gli attori più attivi che stanno investendo nella tecnologia sono quelli del mondo finance che rappresentano il 48% dei progetti con 280 casi, di cui 126 nel 2018. A fine 2016 i casi finance erano l'80%, a fine 2017 erano il 61% mentre a dicembre 2018 erano il 48%.

Dalla fase "paura" con cui 10 anni fa hanno reagito alla Blockchain banking e finance sono oggi profondamente coinvolti nello sviluppo e rappresentano senza ombra di dubbio il settore che più di altri si sta muovendo, sia per non perdere quel ruolo di "Trust provider" che la Blockchain potrebbe sottrargli, sia per sfruttare questa piattaforma in vista di una diversificazione della propria azione sul mercato.

Le pubbliche amministrazioni a loro volta sono estremamente attive e totalizzano 59 casi di cui 39 nel 2018. Appare qui evidente che temi come identità digitale ed e-voting, solo per citare due esempi, rappresentano due territori di sperimentazione dove sicurezza e privacy sono fondamentali.

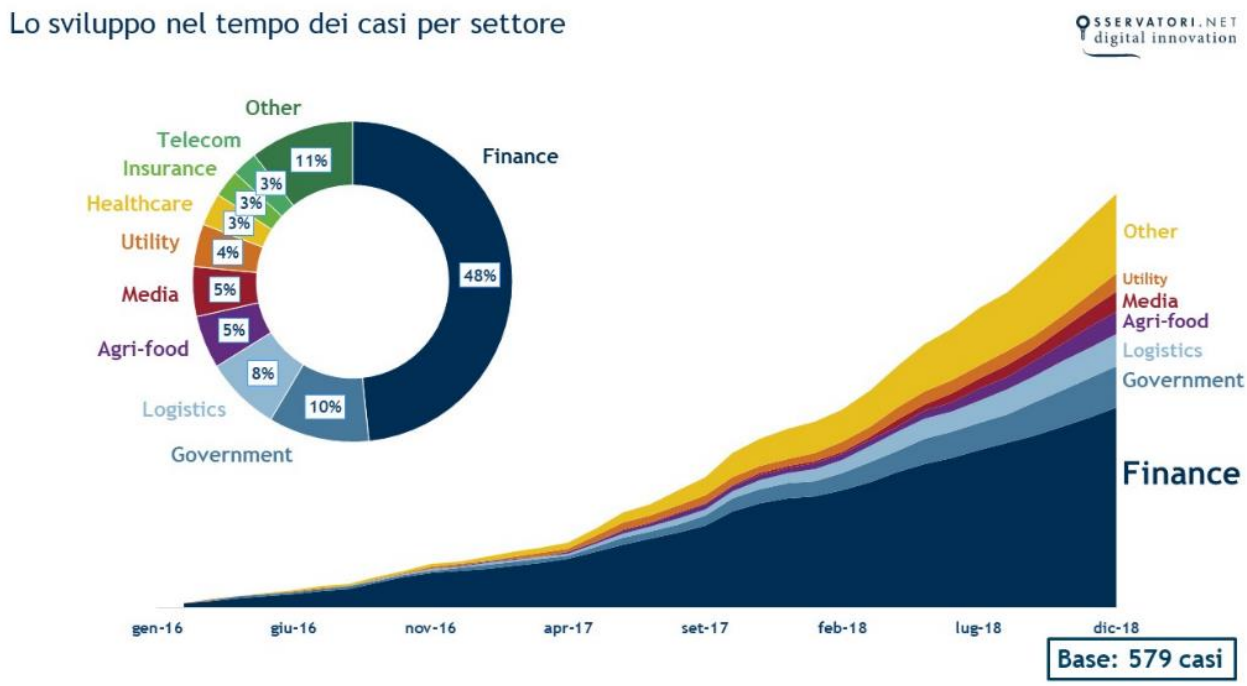
Il mondo dei trasporti, anche grazie al ruolo di importanti consorzi, conta 44 casi (29 nel 2018) con esperienze internazionali che hanno raccolto grande attenzione mediatica anche per l'impegno e l'importanza delle imprese e delle organizzazioni coinvolte.

L'agrifood con 31 casi mostra una dinamica molto positiva (24 casi sono del 2018) e sembra rispondere in modo nuovo alla domanda di protezione e valorizzazione del Made in Italy.

Anche il mondo media ha visto una importante accelerazione e dei 29 casi complessivi 27 sono del 2018 e vedono il forte coinvolgimento di autori e interpreti per cercare risposte nuove, ancora una volta sulla leva della fiducia, per l'annoso problema del rispetto dei copyright.

Una nota a parte merito il mercato delle utility dove i casi (25 di cui 14 nel 2018) fotografano forse solo in modo parziale un fenomeno che sta cercando nella Blockchain un nuovo modo per gestire il grandissimo e importantissimo tema delle microvendite in forma P2P, ad esempio di energia tra microproduttori (famiglie o piccole aziende) con un potenziale ruolo di coordinamento o gestione della rete da parte delle utility. Un fenomeno che sta contribuendo a cambiare lo scenario del mercato dell'energia.

Telecom, insurance, healthcare, airline, automotive, luxury e più genericamente altri 111 casi di cui 69 avviati nel 2018 completano il quadro di riferimento che trova nella lettura dei trend una indicazione importante.



L'altro dato rilevato che può dare ulteriori indicazioni sull'importanza di sicurezza e privacy dei dati è quello dei processi sui quali imprese e organizzazioni guardano alla Blockchain. Una classifica questa che dice forse di più di quella precedente evidenziando che a prescindere dai mercati Payment, Data & Document management, Tracking & Supply Chain sono senza dubbio i processi che mettono in moto la maggior parte dei progetti (401 su 579). Il payment in particolare conta 138 casi (79 nel 2018), Data & Document management arriva a 137 casi (83 nel 2018) mentre Tracking & Supply Chain è a 126 di cui 78 nel 2018.

La Blockchain, più di altre innovazioni ha la necessità di arrivare nelle imprese e nelle organizzazioni attraverso un percorso strutturato, con una crescita di competenze in grado di gestirne l'enorme potenziale e di ridurre e controllare i fattori di rischio.

Nell'analisi del Blockchain journey attuale effettuato dall'Osservatorio Blockchain & Distributed Ledger del Politecnico di Milano emergono alcuni importanti elementi di debolezza che si possono configurare in fattori di rischio.

Nella contrapposizione tra scettici e visionari il punto di sintesi purtroppo vede prevalere le perplessità. A livello di visione tecnologica le imprese si dibattono tra chi sostiene che la Blockchain "non porterà innovazione" e chi crede che "contribuirà a migliorare alcuni processi". Nel caso di una visione sul proprio settore la convinzione diffusa è che l'impatto sarà medio-basso.

Questo approccio si fa sentire a livello di organizzazione e in termini di commitment: la Blockchain non è guidata da un team dedicato ma da diverse persone in modo destrutturato, mentre il commitment sui progetti è prevalentemente indirizzato alla comprensione della tecnologia e degli use case. Non ultimo il fatto che anche a livello di budget mancano le "idee chiare".

L’impatto della Blockchain sui modelli di governance

In questo capitolo tratteremo dei modelli di governance, analizzando congiuntamente:

- l’impatto su di essi prodotto dalle Blockchain;
- l'adozione dei nuovi modelli di governance nella scelta di soluzioni basate su Blockchain.

Parlando di governance non vogliamo solo riferirci al tema della regolamentazione, ma intendiamo condurre il lettore a un uso pragmatico del termine che consente di costruire quell’equilibrio fra innovazione, persone e imprese, da cui dipende il successo (o l’insuccesso) di qualsiasi innovazione. Definiamo, dunque, “Governance” come l'insieme dei principi, delle regole e delle procedure che riguardano la gestione e il governo di una società, di un'istituzione, di un fenomeno collettivo e proviamo a comprendere come tale insieme possa contemperare (essendone a sua volta contemperato) la progettazione e lo sviluppo di soluzioni che intendono avvantaggiarsi delle Blockchain.

Modelli di governance

Riprendendo alcune definizioni del Capitolo La Blockchain: considerazioni di base, entriamo in un dettaglio necessario ad affrontare il tema della governance e distinguiamo tre diverse tipologie di Blockchain, in funzione del sistema con cui viene governata l’infrastruttura basata sull’adozione di DLT:

- **Private**, dove un’entità centrale “trusted” assegna le autorizzazioni a soggetti noti che possono accedere al ledger;
- **Ibride (consortili o confederate)**, dove il processo di validazione del consenso è attuato da individui o organizzazioni, come per esempio un consorzio di istituti finanziari clienti di un’azienda, noti e preselezionati da un’entità terza “trusted”;
- **Pubbliche**, dove chiunque può leggere e presentare transazioni sul ledger, partecipando come membro del network alla loro verifica e convalida.

Governance, fiducia, consenso

In relazione ai modelli di governance è possibile distinguere in almeno tre categorie che, opportunamente raggruppate come mostrato in Figura 4, permettono di comprendere quali siano le correlazioni funzionali e amministrative con la fiducia necessaria al corretto funzionamento di una Blockchain e il consenso sulla validazione delle transazioni in essa registrate:

- **Governo centralizzato,** tipico di alcune Blockchain private;
- **Governo centralizzato e controlli distribuiti,** tipico di alcune Blockchain private delle Blockchain ibride;
- **Governo condiviso e controlli distribuiti,** tipico delle Blockchain pubbliche.

FASI/MODELLI	FIDUCIA	CONSENSO
GOVERNO CENTRALIZZATO	Solo in alcuni individui noti e predeterminati è riposta la fiducia	Lo scambio di beni viene validato da un'entità centrale senza chiedere il consenso di nessuno
GOVERNO CENTRALIZZATO E CONTROLLI DISTRIBUITI	Solo in alcuni individui noti e predeterminati è riposta la fiducia	Lo scambio di beni viene validato raggiungendo un consenso distribuito tra più validatori preselezionati
GOVERNO CONDIVISO E CONTROLLI DISTRIBUITI	La fiducia è riposta in chiunque dimostri matematicamente di esserne in grado, risolvendo un complicato enigma crittografico	Lo scambio di beni viene garantito e validato raggiungendo un consenso distribuito solo tra chi vuole essere un validatore (potenzialmente chiunque potrebbe essere un validatore)

Figura 4: Matrice delle correlazioni Governance, Fiducia, Consenso (fonte "Tutto su Blockchain", R. Garavaglia, Hoepli, aprile 2018)

L'influenza delle Blockchain sui modelli di governance

Se con governance vogliamo significare, come in precedenza affermato, l'insieme dei principi, delle regole e delle procedure che riguardano la gestione e il governo di una società, di un'istituzione, di un fenomeno collettivo, capiamo ora come, alla luce delle correlazioni mostrate in Figura 4, sia indispensabile accettare le modulazioni (e le loro gradualità) poste in relazione alla fiducia ed al consenso.

Si avrà infatti che, più ci si affranca da un modello (consolidato e tradizionale) di Governo Centralizzato muovendosi in direzione di una decentralizzazione, tipica delle Blockchain permissionless, maggiore sarà l'incidenza di un processo di democratizzazione. La presenza di un modello di governance condiviso (o, se si preferisce, l'assenza di un modello di governo centrale) può rappresentare l'espressione democratica di un sistema decisionale, dove una pluralità di soggetti può esprimere il proprio voto per il conseguimento di obiettivi condivisi: una sorta di **e-democracy** che può essere estesa anche alla corporate governance (*rectius*, alle corporate governance).

Proprio perché la governance delle Blockchain permissionless è basata su un modello condiviso, non esistendo un unico decisore centralizzato in grado di determinare risoluzioni, quando si vogliono cambiare le regole è necessario che i nodi componenti la Blockchain stessi siano d'accordo. Ed è proprio nel solco di tale determinazione che è possibile inserire l'avvicendarsi delle cc.dd. **Hard Fork** durante le quali, il propagarsi dei loro effetti sulla rete, fa emergere alcuni rischi che pongono in pericolo l'affidabilità e l'immutabilità delle transazioni avvenute.

Tenendo in considerazione questi aspetti basilari, nei prossimi paragrafi analizzeremo l'impatto sulla **governance del cambiamento tecnologico**, ipotizzando di porsi nei panni di un'azienda tradizionale che mostra interesse nello sviluppo di soluzioni basate su Blockchain per offrire un

nuovo servizio o, semplicemente, per efficientare i processi produttivi e de-opacizzare alcune filiere di controllo.

Successivamente, analizzeremo anche l'impatto sotto il profilo della **corporate governance**, immaginando di trattare una proposizione di business innovativa progettata, offerta e gestita tramite la costituzione di una nuova società o mediante la creazione di uno spin-off.

Impatti sulla governance del cambiamento tecnologico

L'impresa che volesse investire nel cambiamento abilitato dalle Blockchain, dovrebbe innanzitutto porsi alcuni interrogativi su come intende accettare, preventivamente e consapevolmente, l'impatto che la nuova soluzione basata su tecnologie Distributed Ledger avrà inevitabilmente sui modelli di governance precedentemente adottati.

Nello specifico, l'organo dirigente, anche sulla effettiva capacità o disponibilità dell'azienda a gestire il cambiamento, dovrebbe auspicabilmente valutare i seguenti aspetti:

- in quale misura si ritiene possibile prevedere che le (nuove) regole di governo siano condivise, accettate e attuate da una pluralità di attori;
- in che modo si ritiene realizzabile una distribuzione dei controlli sotto il profilo tecnologico, operativo e sistemico;
- quali sono gli accorgimenti, sotto il profilo della mitigazione dei rischi, che si intendono attuare, in considerazione dell'ampliamento di una base di soggetti che, a diverso titolo, potrebbe invalidare decisioni assunte secondo modelli di centralizzazione deliberativa, o validare nuove risoluzioni poste al vaglio secondo un metodo di validazione maggiormente inclusivo di terzi (a votazione);
- con quali modalità di distribuzione dei costi e dei ricavi si pensa di progettare gli investimenti necessari all'implementazione della soluzione, tenendo conto di una struttura di governo societario che potrebbe modificarsi grazie alla presenza di un maggior numero di attori coprotagonisti (si veda a tal proposito anche il successivo paragrafo che descrive l'impatto della Blockchain sulla corporate governance);
- quali sono (o saranno) gli impatti sui modelli di business, laddove la nuova soluzione, in virtù di un'apertura verso potenziali soggetti "new prosumer" abilitata dalla Blockchain, sarà recepita in operativo (evoluzione dal web 2.0 al web 3.0);
- in che modo si progetta una migliore compliance, prevedendo il necessario coinvolgimento dei regulators nazionali e sovranazionali;
- quali livelli di compromesso si è disposti ad accettare tra le esigenze di scalabilità e fiducia distribuita sulla Blockchain; decisione, questa, da cui dipende (o da cui è dipesa) la scelta del protocollo di consenso distribuito.

Rispondere a questi interrogativi non è semplice; tuttavia, riteniamo sia utile, se non indispensabile, che le organizzazioni affrontino le suddette questioni innanzi alla progettazione di una soluzione basata su Blockchain e, prevedibilmente, prima di avviare in concreto qualsiasi investimento. In tal senso, un "audace pragmatismo" nelle scelte che l'organo dirigente dovrà operare è fortemente suggerito.

Impatti sulla corporate governance

Affrontiamo ora la disamina degli impatti che la Blockchain potrebbe produrre sotto il profilo del governo societario, nel caso in cui sia scelta in ambiti che incidono sul core business aziendale, intendendo con ciò offrire al lettore una prima valutazione delle opportunità e dei rischi che soluzioni basate su Distributed Ledger possono porre, in funzione della diversa graduazione di decentralizzazione dei processi di governo e di controllo come declinata nella precedente matrice riportata in Figura 4.

Nel nostro ordinamento è prevista la possibilità di adottare **tre sistemi alternativi** di governance societaria:

- il **sistema tradizionale** (altresì detto ordinario) che prevede la presenza di un Consiglio di Amministrazione con funzioni amministrative e di un Collegio Sindacale con funzioni di controllo sull'amministrazione, entrambi di nomina assembleare;
- il **sistema monistico** che prevede l'esercizio dell'amministrazione e del controllo, rispettivamente in carico al Consiglio di Amministrazione (assemblearmente nominato) e a un Comitato per il controllo sulla gestione;
- il **sistema dualistico**, che prevede la presenza di un Consiglio di Sorveglianza, di nomina assembleare, e di un Consiglio di Gestione nominato dal Consiglio di Sorveglianza.

L'efficacia della decentralizzazione apportata dalla Blockchain può – almeno in teoria - meglio giustificarsi (o spiegarsi) se si prendono in considerazione il sistema monistico e quello dualistico.

Sia il modello monistico sia quello dualistico si differenziano dal modello tradizionale perché non presumono una separazione netta tra l'organo che gestisce la società e l'organo che controlla detta gestione.

In particolare, nel modello dualistico di amministrazione e controllo è prevista la presenza di un **Consiglio di Sorveglianza**, i cui membri sono nominati dall'**Assemblea degli Azionisti** e di un **Consiglio di Gestione** nominato dal Consiglio di Sorveglianza.

La gestione aziendale è, pertanto, affidata ad un Consiglio di Gestione che ha l'esclusiva responsabilità della gestione dell'impresa e compie tutte le operazioni necessarie all'attuazione dell'oggetto sociale. L'organo di controllo è il Consiglio di Sorveglianza.

Durante la vita della società è lo stesso organo di controllo (ossia il Consiglio di Sorveglianza) che nomina e revoca i componenti del consiglio di gestione. Pertanto, i soggetti deputati all'amministrazione della società sono diretta espressione dell'organo che procederà al controllo dell'amministrazione stessa.

Orbene, appare utile rimarcare in questo documento come, ogni qualvolta una nuova impresa si accinga a progettare proposizioni (o anche solo a definirne le strategie) che intendono avvalersi del supporto di una (o più) Blockchain, debba opportunamente (saper) valutare quali possano essere anche i necessari cambiamenti da apportare alla governance societaria.

L'evoluzione della Blockchain, infatti, conduce alla possibilità di costituire delle **organizzazioni decentralizzate** (o "DO – Decentralized Organization"), che possono arrivare ad essere anche **autonome** (si parla in questo caso di "DAO – Decentralized Autonomous Organization") tramite

l'adozione di "entità algoritmiche" laddove giuridicamente riconosciute, come, ad esempio, attualmente previsto in uno Stato federato Americano dalla "Delaware General Corporation Law" (vigente nello Stato del Delaware, appunto).

Le DO gestiscono direttamente sulla Blockchain: **sistemi di voto**, **contabilità**, **registro dei soci**, **produzione**, **scorte**, **ordini** e così via. In queste organizzazioni decentralizzate le informazioni sono gestite ed elaborate da umani (non da macchine) che verificano il flusso delle informazioni. In questo modo gli umani continuano a esercitare una supervisione dell'organizzazione perché controllano, in qualche misura, le fonti delle informazioni, le regole e i codici di condotta aziendali.

Nel modello delle DAO, differentemente da quello delle DO, il processo decisionale non è più soggetto al controllo umano, bensì è come se fosse nella responsabilità della DAO stessa, realizzato da un insieme di Smart Contract e di agenti autonomi tra loro interconnessi e tutti dotati di un capitale iniziale espresso in criptoasset. Attraverso un set di regole predefinito e auto-applicabile codificato nei **Distributed Contract**, possono essere eseguite da un'organizzazione autonoma decentralizzata attività imprenditoriali o sociali (sia online sia offline) in completa autonomia, ovvero senza bisogno di alcun intervento umano.

Diversamente da ciò che talvolta accade nelle tradizionali organizzazioni gerarchiche (o verticistiche), dove la gestione del flusso di informazioni e l'applicazione dei controlli può presentare opacità, le DAO provano a intervenire alla base del problema, creando un ambiente software open source basato su logiche di controllo partecipative tipiche delle Blockchain (sia permissionless sia permissioned) in cui vigono protocolli di regolamento del consenso distribuito fra partecipanti trasparente, sicuro e verificabile.

Da queste brevi riflessioni si può quindi dedurre come, in particolare per i sistemi monistico/dualistico e con riferimento alla composizione (o componibilità su base elettiva) del Comitato per il controllo sulla gestione, del Consiglio di Gestione e del Consiglio di Sorveglianza, l'adozione delle Blockchain potrebbe avere (*rectius* debba avere) effetti che, si auspica, siano valutati in fase di progettazione strategica.

Regulatory Environment

Come molte altre innovazioni tecnologiche, quali l'avvento di Internet o del cloud computing, la Blockchain presenta una serie di sfide ai regolatori delle diverse nazioni, soprattutto per quanto riguarda le criptovalute che possono avere importanti ripercussioni sui mercati finanziari.

Questa innovativa architettura dati permette di creare asset virtuali univoci che possono essere scambiati senza bisogno di intermediari responsabili attraverso internet. Infatti, si parla di una evoluzione da internet delle informazioni ad internet del valore.

Quindi, come internet ha introdotto o accentuato problemi legali come quello della proprietà intellettuale delle informazioni che venivano scambiate per quel mezzo, così la Blockchain introduce un nuovo set di problemi, come ad esempio la legittimità dei diritti di proprietà di asset fisici registrati su una Blockchain pubblica.

Anche in questo caso il regolatore si trova di fronte ad una tecnologia che pone nelle mani di individui ed istituzioni nuovi poteri e deve trovare il modo di regolarli, da un lato assicurando la salvaguardia dei diritti, dei beni e della sicurezza dei propri cittadini e dall'altro evitando di limitare i benefici che derivano dal nuovo approccio allo scambio di valore.

Alcuni dei principali aspetti che le normative si trovano a dover inquadrare in un perimetro regolamentato sono ad esempio:

- La possibilità di presentare informazioni trascritte sulla Blockchain come prova in tribunale;
- La possibilità per le aziende di accettare pagamenti in cryptovaluta;
- Le modalità di tassazione dei proventi in cryptovaluta;
- I rischi di frode e riciclaggio che derivano dalla possibilità di transare sulla Blockchain indipendentemente dai confini geografici in cui si opera.

Oggi è particolarmente importante per una nazione prestare molta attenzione alle leggi che la regolano, in quanto quello legale è uno dei principali aspetti che gli imprenditori valutano nel decidere se fondare la propria azienda innovativa in un paese piuttosto che in un altro e che gli investitori considerano nel decidere dove mettere a frutto i propri risparmi.

Queste leggi devono ricercare un delicato equilibrio tra la protezione degli interessi dei propri cittadini e l'abilitazione di iniziative innovative a valore aggiunto i cui effetti sono spesso imprevedibili. Ricerca, questa, che non può prescindere da una profonda comprensione da parte del regolatore delle potenzialità che introducono nuove tecnologie.

La bolla speculativa delle ICO del 2017 ha scosso i mercati finanziari abbastanza da catturare l'attenzione dei regolatori di diversi paesi nel mondo che si stanno adoperando per fare i conti con i business basati sulla Blockchain e gli approcci variano di molto tra nazioni.

I paesi che hanno attratto più investimenti per diversi motivi legati alla sfera regolamentare e/o alla presenza di importanti mercati finanziari sono la Svizzera, il Liechtenstein, Malta, Hong Kong e Singapore. La Cina invece ha adottato una politica ostile a questo tipo di iniziative, impedendo di fatto le ICO e gli exchange di cryptovalute.

A metà strada tra l'approccio Cinese e quello delle realtà più piccole e permissive menzionate sopra, troviamo gli Stati Uniti che non si oppongono allo sviluppo di startup nel mondo crypto, ma ne inquadra gli oneri di compliance in un perimetro legislativo pre-esistente, con le regole dell'attuale mercato finanziario sotto la vigilanza della SEC, e che spesso sono in conflitto con, ad esempio, gli obiettivi di democratizzare l'accesso al mondo degli investimenti che viene di nuovo aperto solo ad investitori accreditati.

Al sito map.bitlegal.io si può trovare una mappa che a colpo d'occhio illustra quali sono i paesi nel mondo con le politiche più e meno accomodanti per lo sviluppo di iniziative in ambito Blockchain.

Alcuni aspetti legali e contrattuali degli Smart Contracts

Una possibile chiave di lettura: l'analisi sociologica del diritto

Nell'affrontare le principali tematiche giuridiche che rilevano in tema di Blockchain e Smart Contracts, un utile "strumento" (per l'analisi e l'interpretazione di queste nuove tecnologie) può essere la cosiddetta analisi sociologica del diritto[3].

Tale corrente di pensiero, prescindendo da analisi sulla liceità di determinate condotte o di realtà in cui l'essere umano coopera o si relaziona con gli altri, analizza i fenomeni umani da un punto di vista meramente fenomenologico, per il solo fatto che esistono e si evolvono.

In altre parole, in base a dette analisi, modalità di cooperazione o di rapporto tra esseri umani possono essere di diverso tipo e avere "forme" diverse.

Il concetto di autonomia e, in un certo senso, di "auto-regolamentazione" non è un concetto nuovo nel panorama giuridico attuale né, tantomeno, nella storia del diritto.

Basandosi sulla concezione del diritto come forma di regolazione della condotta[4] si può capire, infatti, come la medesima, essendo molto ampia, possa ricomprendere qualsiasi comportamento che segua "regole" di diverso tipo: siano esse puramente consuetudinarie, o basate sulla legge "del più forte" o anche, semplicemente non scritte, ma aventi ad ogni modo forza cogente tra i membri di una comunità.

L'uomo, per regolare le proprie condotte ed "auto-regolarsi", ha da sempre elaborato svariati metodi e meccanismi sia per regolare i rapporti in generale, inclusi quelli sociali, sia per risolvere eventuali dispute o conflitti.

Ciò è avvenuto senza che i soggetti privati (ed in questo concetto possono rientrare anche le aziende)

[3] Chiamata anche "Law & Society". Vedere in primis i lavori di Max Weber, in particolare, "Max Weber on Law in Economy and Society".
[4] Si veda, per un approfondimento: Bussani "Il diritto dell'Occidente", Barberis "Europa del diritto" o Rodotà "La vita e le regole: tra diritto e non diritto.

ricorressero al sistema legale "formale" o "tradizionale", cercando forme di regolazione informali o comunque non regolamentate da istituzioni pubbliche.

Per operare secondo questo sistema informale, è necessario utilizzare mezzi che mettano in grado il soggetto di conoscere le regole e quindi di poterle rispettare: in certi casi con il semplice passaparola, in altri tramite la consuetudine sedimentatasi negli anni oppure anche attraverso forme di regolamentazione digitali (come i social network).

Negli ultimi anni, l'evoluzione del mondo digitale ha permesso alle tecnologie informatiche di introdurre nel panorama legale "informale" **nuovi strumenti**, e, fra gli altri, due di questi sono proprio la Blockchain e gli Smart Contracts.

Tali nuovi strumenti permettono agli operatori economici, quindi anche alle persone "comuni", di operare in modo informale utilizzando dei nuovi supporti dati dalle tecnologie digitali e possono aiutarci a dimostrare, ancora una volta, come il diritto si stratifichi e utilizzi diverse forme per operare.

Definizione e caratteristiche principali degli Smart Contracts

Sebbene una definizione univoca e collettivamente condivisa non sia ancora presente, possiamo definire gli Smart Contracts come un set di funzioni codificate che permettono l'esecuzione di un codice da parte di un computer, un protocollo che elabora in modo deterministico (con identici risultati a fronte di identiche condizioni) le informazioni che vengono raccolte o in esso inserite e che persegue, come finalità principale, quella di produrre effetti giuridici tra le parti coinvolte[5].

Quali sono le componenti principali individuabili in uno Smart Contract?

In primis, la sua esecuzione automatica in presenza di determinate condizioni o avvenimenti. Il carattere automatico può avere svariati benefici, tra cui, solo per citarne un paio:

- efficienza in termini di costi minori per eventuali intermediari;
- relativa velocità di esecuzione.

Secondariamente il fatto che, una volta "avviato" lo Smart Contract, i termini in esso contenuti si eseguono senza possibilità di interruzioni (anche se vi sono potenzialmente altre condizioni che potrebbero comportare delle sospensioni o dei cambiamenti).

Gli Smart Contracts, almeno in linea teorica, non hanno bisogno di un soggetto terzo che ne garantisca l'esecuzione (usando una terminologia anglosassone, il suo c.d. *enforcement*). Sono, almeno in linea teorica, progettati per eseguirsi **senza errori** e in un lasso di **tempo** ragionevolmente **breve**.

[5] La Chamber of Digital Commerce, nel suo paper del settembre 2018 denominato "Smart Contracts: Is the Law Ready?" fa una distinzione tra Smart Contract e Smart Legal Contract definendo questi ultimi come "A smart contract that articulates and is capable of self-executing, on a legally-enforceable basis, the terms of an agreement between two or more parties" (pag. 12).
Mentre la BCE, nella sua analisi di ottobre 2017 denominata "Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks" definisce gli smart contracts come "contractual-type arrangements embedded in a software" (pag. 35).

Inoltre, anche se questa caratteristica potrebbe essere vista come un limite, sono **deterministici** in quanto, ad un dato input, l'output derivante sarà inevitabilmente sempre lo stesso.

Il primo esempio di Smart Contract è rappresentato dalla c.d. "*vending machine*" la quale altro non è che il distributore automatico che dispensa oramai beni di qualunque genere, da prodotti di farmacia a snack passando per bibite o tabacchi[6].

A stretto rigore "il distributore automatico" rappresenta perfettamente uno Smart Contract perché, al verificarsi di una o più condizioni (in questo caso, l'inserimento della quantità di denaro necessaria per l'acquisto) la macchina eroga il bene richiesto in modo automatico (e l'esecuzione della transazione non può essere interrotta).

Le reazioni di fronte a queste nuove tecnologie, in particolare con riferimento agli Smart Contracts, sono state molte e delle più disparate: chi li sostiene ed è profondamente convinto dei vantaggi ritiene (addirittura) che gli Smart Contracts potranno soppiantare interamente l'utilizzo dei contratti tradizionali[7] e modificare profondamente le dinamiche ed i processi legati al trasferimento di proprietà e possesso[8] mentre, chi è più scettico, non vede negli Smart Contracts ne una componente intelligente ne, tantomeno, un contratto vero e proprio[9].

Quel che sicuramente appare lampante, in un momento in cui l'entusiasmo e il c.d. *hype* verso queste tecnologie sta diventando un sano e concreto realismo, è che queste tecnologie possono essere estremamente efficaci in determinati settori ma pongono (ancora) notevoli questioni giuridiche.

"Code is Law" e la "Net-neutrality"

Come analizzato dal Prof. Lessig nei suoi primi studi riguardanti il cyberspace, il **codice** è l'architettura che sorregge internet e la Blockchain. Tale architettura è in grado di condizionare i comportamenti umani che avvengono grazie al mondo digitale[10].

Parafrasando le parole dello stesso Prof. Lessig, "[...] *nel cyberspace dobbiamo capire come un differente "codice" regoli - come l'hardware ed il software (cioè il "codice" del cyberspace) - permettano al cyberspace di esistere e di essere allo stesso tempo regolato*"[11].

L'idea fondamentale esaminata in questo paragrafo è sinteticamente rappresentata dal concetto di "*code is law*" con il quale si tende a descrivere il fenomeno per cui determinati soggetti (siano essi persone fisiche, aziende o pubbliche amministrazioni) tendono a sostituire o ad incorporare leggi o

[6] Il primo teorizzatore di questo concetto è stato Nick Szabo nei primi anni novanta, per una lettura del suo (ormai) celebre articolo: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

[7] Byrne "Do Lawyers have a Future?" https://www.thelawyer.com/issues/online-september-2016/do-lawyers-have-a-future-2/; Sonderegger "Blockchain: Can Smart Contracts Replace Lawyers?" https://abovethelaw.com/2018/02/blockchain-can-smart-contracts-replace-lawyers/

[8] TMD Studio Ltd "Will Blockchain Radically Change The Real Estate Industry? https://medium.com/studiotmd/will-blockchain-radically-change-the-real-estate-industry-c99d596ab999

[9] https://monax.io/learn/smart_contracts/

[10] Lawrence Lessig "Code and other Laws of Cyberspace" 1999 Basic Books.

[11] Lawrence Lessig "Code 2.0" 2006, pagina 20.

regolamenti attuali in regole tecniche scritte attraverso dei codici software[12].

Tali codici, grazie ad internet, hanno creato un nuovo ambiente dove le persone possono esprimersi, collaborare, condividere o semplicemente "esistere". Come ogni nuovo artefatto umano anch'esso è dotato di regole; le quali sono essenzialmente regolate, come detto sopra, da *software codes*.

Nel mondo digitale attuale, il codice sta progressivamente assumendo le funzioni più tradizionali del diritto ma, allo stesso tempo, parrebbe che lo stesso diritto stia prendendo alcuni dei connotati tipici dei codici informatici.

Tale caratteristica è sicuramente rappresentata dalla Blockchain e dai rapporti che vi si formano: il rapporto che sussiste tra *miners* è regolato dal **protocollo** alla base della Blockchain e dalle regole di **consenso** con cui la Blockchain stessa è stata impostata.

In tal modo, basandosi sul consenso distribuito, i *miners* e le altre parti coinvolte hanno l'autorità di far rispettare le regole di cui questa comunità si è dotata.

Alcune soluzioni adottate in seguito all'avvento di internet (su cui la tecnologia Blockchain di fatto si basa) potrebbero applicarsi allo stesso modo: in primis vale la pena considerare il principio della "*net-neutrality*", la neutralità della rete.

La c.d. "network neutrality" permette che non avvenga una discriminazione sulla base dei tipo di dato o eventualmente degli attori coinvolti nelle comunicazioni; sulla base di questo principio si potrebbe, *mutatis mutandis*, imporre ai *miners* di processare ogni transazione in modo neutrale senza alcuna discriminazione.

Quale approccio adottare per bilanciare innovazione e controllo rispetto ai reati o alle condotte genericamente illecite è e sarà un'impresa complessa e delicata: è recentissimo l'appello da parte del **Parlamento Europeo** nei confronti della Commissione per compiere un assessment e valutare esattamente dove, come e fino a che punto regolare l'uso di tale tecnologia[13].

Il rapporto tra diritto e informatica: problemi di "trasposizione"

Quali possono essere i vantaggi di uno Smart Contract inserito su una Blockchain?

L'automazione permette l'esecuzione senza intermediari ed elimina di fatto la componente umana dall'esecuzione stessa, limitando di molto (in certi casi) il rischio di inadempimento.

Ciò comporta che alla "componente umana", quindi ai soggetti che decidono di regolare una transazione attraverso uno Smart Contract, rimane solamente il compito della preparazione e dell'accurato studio delle clausole così da avere una **impostazione iniziale** che più si avvicina alla

[12] Tale slogan è attribuito al Prof. Lessig ma deriva da una precedente definizione coniata da Joel Reidenberg "Lex Informatica" (Lex Informatica: The Formulation of Information Policy Rules through Technology 1997).
[13] Questo il report "on Blockchain: a forward-looking trade policy" disponibile al seguente link: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2018-0407&format=XML&language=EN

volontà delle parti ed evita quindi incomprensioni e, di conseguenza, eventuali vizi.

Ne consegue, come difficoltà iniziale, la sfida di tradurre in un linguaggio "*machine readable*" termini o espressioni che poco si prestano a questi usi così predeterminati.

In aggiunta, potrebbe presentarsi il caso in cui siano le parti stesse, in modo perfettamente consapevole, a non voler esprimere in modo chiaro alcuni termini del contratto o alcune definizioni dello stesso per lasciare spazio a flessibilità ed aggiustamenti in corso d'opera.

Ciò è particolarmente evidente anche dal punto di vista del legislatore, dove leggi o regolamenti vengono scritti appositamente in modo ampio (o addirittura vago) per lasciare poi, alla c.d. "*law in action*" o ai giudici, a seconda dei casi, il compito di interpretare o applicare al caso concreto la fattispecie[14].

Alcuni esempi sono doverosi sotto il profilo delle difficoltà ermeneutiche e di trasposizione di concetti giuridici in linguaggio informatico:

- **Diligenza/negligenza**: in determinate situazioni è lasciata alla discrezionalità del giudice valutare il grado di diligenza o negligenza di una condotta.
- **Forza maggiore**: eventi di vario tipo che sono imprevedibili e fuori dal controllo umano e che, di fatto, rendono impossibile (o eccessivamente oneroso) l'adempimento delle obbligazioni delle parti.
- **Obbligazione di mezzi** o **di risultato**: possono sorgere dei casi in cui sia difficile individuare il tipo di obbligazione a cui un soggetto è tenuto, per determinate figure professionali (si pensi agli avvocati in primis) tale distinzione è relativamente facile da effettuare ma in altre ipotesi, tale tassonomia risulta di difficile individuazione e richiede il supporto di altre categorie giuridiche[15].

Esiste quindi una c.d. *way-out*? Una soluzione seppur provvisoria?

Con l'avvento della tecnologia Blockchain e l'inizio dello studio dei suoi impatti legali, si è iniziato a parlare di "*legal engineer*" o di "*legal tech*" con l'intento di trovare una **nuova definizione** ad un settore che ha i caratteri dell'eterogeneità e che mira ad unire mondi, quello informatico e quello giuridico, che sono stati, almeno fino ad oggi, tendenzialmente incompatibili.

L'unione di questi due settori potrebbe portare alla comparsa di operatori o di **nuove figure professionali** in grado di coniugare le capacità e le conoscenze dei due ambiti (cioè quello informatico e quello giuridico) e quindi un giorno (probabilmente non molto lontano) potremo avere un "*giurista capace di programmare*" o un informatico in grado di trasferire concetti giuridici su un codice (od un algoritmo).

La possibilità di convertire il linguaggio giuridico in codice presenta, come osservato, delle grosse sfide, sia in ambito di progettazione, sia per la risoluzione di eventuali problemi legali che, almeno per ora, rimangono nell'alveo della speculazione ad alto livello.

[14] La probabile prima comparsa della frase "law in books and law in action" è attribuibile al Prof. Roscoe Pound nel 1910, uno dei primi teorizzatori del c.d. "realismo giuridico" (legal realism).

[15] A tal proposito si prenda l'esempio di un contratto di consulenza generica: in determinate situazioni, per valutare quale livello di responsabilità deve venir attribuito, soccorrono categorie giuridiche come la negligenza o la colpa grave. In questi casi va commisurata la situazione con le ragionevoli aspettative del caso concreto.

Considerando anche la diversità delle piattaforme Blockchain ad oggi esistenti (ed i relativi sistemi di governance adottati, si pensi soltanto a bitcoin o alla criptovaluta EOS) una soluzione "piglia tutto" (o "*one size fits all"* come direbbero gli inglesi) in cui si adottano regole generali valevoli per tutti i tipi di Blockchain e per i relativi Smart Contracts, non pare né fattibile né utile comportando rischio di essere troppo generica e conseguentemente inutilizzabile.

Proprietà giuridico/legali di uno Smart Contract e liabilities connesse

Gli Smart Contract e il diritto dei contratti

Un contratto è generalmente identificato come un "incontro delle volontà di due o più parti" o, usando una definizione prettamente codicistica, come un "*accordo di due o più parti per costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale*"[16].

I suoi requisiti sono essenzialmente quattro: l'accordo delle parti, l'oggetto, la causa e la forma.

Parte degli studiosi attribuisce allo Smart Contract solo "una parte" delle caratteristiche di un contratto stesso: alcuni ritengono che lo Smart Contract inserito all'interno di una Blockchain possa servire come pubblicità dello stesso perché un accordo è già avvenuto "a monte" dell'inserimento nella Blockchain stessa[17].

Altri ritengono, seguendo questo filone, che solo alcune parti di un contratto (in particolare, quelle più meccaniche cioè meno soggette ad interpretazioni o a variabili di sorta) possano venire inserite nella Blockchain stessa.

Alcuni studiosi parlano di uno Smart Contract come di un "processo meccanico automatico" (o automatizzato) più che di un "contratto automatico" nella definizione riportata nella parte introduttiva[18].

Nel "mondo umano", in un momento antecedente all'avvio di uno Smart Contract, vi sarà comunque un incontro delle volontà delle parti al fine di giungere ad un accordo e quindi ad un contratto. Solo allora, cioè solo al termine di eventuali negoziazioni, la transazione potrà avvenire e la stessa potrà essere "inserita" o trasposta con il mezzo o sul supporto ritenuto più adatto (in questo caso uno Smart Contract).

Le parti contrattuali, però, potrebbero anche optare per utilizzare come unica fonte delle loro obbligazioni lo Smart Contract stesso (ciò avviene già da alcuni anni nel settore finanziario)[19].

Nel diritto dei contratti spesso avviene che le parti decidano di regolare completamente i loro rapporti attraverso le obbligazioni contenute nel contratto stesso: tali casi si riscontrano prevalentemente nei **sistemi di common law** in cui vengono volutamente limitate le "ingerenze" del diritto statuale (con la conseguenza di dover regolamentare all'interno dei contratti anche i

[16] Art. 1321 Codice Civile italiano.
[17] Per un approfondimento si veda: UNOPS "The Legal Aspects of Blockchain".
[18] Werbach e Cornell, Contracts ex Machina, Duke Law Journal 2017.
[19] Si vedano, a tal proposito, gli esempi analizzati da Surden nella parte 2 del suo paper "Computable Contracts" (2012).

minimi particolari e le conseguenze di ciascun comportamento).

In aggiunta, vengono usualmente previste le c.d. "*order of precedence*", con le quali le parti possono disciplinare quali documenti risultano avere la precedenza nel caso si presentino discrepanze o problemi interpretativi fra i vari documenti che compongono l'accordo contrattuale[20].

Considerando quanto sopra descritto e per poter sfruttare pienamente le caratteristiche degli Smart Contracts, parrebbe essere di maggiore utilità per le parti di un contratto di prevedere che **l'intero accordo contrattuale** (comprensivo dell'offerta e dell'accettazione con relative condizioni) **sia scritto in un linguaggio informatico e venga totalmente inserito su una Blockchain**. Tale soluzione parrebbe (quantomeno) più efficace in un'ottica di riduzione di alcuni costi di transazione nonché in termini di enforcement (anche se non risolverebbe eventuali problemi di contenzioso).

Sebbene la soluzione di trasporre completamente l'accordo contrattuale all'interno di uno Smart Contract possieda notevoli vantaggi, anche la previsione di "**soluzioni ibride**" in cui, per esempio, solamente alcune obbligazioni contrattuali (in genere quelle più semplici e quindi convertibili in linguaggio informatico) vengono inserite in modo immutabile su uno Smart Contract *Blockchain-based*, lasciando una parte "*off-chain*", permetterebbe di avere maggiore flessibilità ed autonomia alle parti coinvolte[21].

Appare doveroso evidenziare che molte giurisdizioni, in particolare in ambito europeo, pongono restrizioni e bilanciamenti legislativi per riportare eventuali squilibri contrattuali o (semplici) poteri negoziali in una situazione di "parità": si pensi ai contratti firmati tra un'azienda e dei consumatori.

In tale contesto sarebbe probabilmente più semplice la diffusione di Smart Contracts nell'ambito delle relazioni "**business to business**" (B2B) quindi nei contratti stipulati tra organizzazioni economiche piuttosto che nell'ambito "**business to consumer**" (B2C).

Più interessante pare esaminare come gli Smart Contracts possano operare laddove, a seguito di modifiche di condizioni, le parti contrattuali debbano ridiscutere eventuali clausole: la legge prevede espressamente casi in cui un'obbligazione contrattuale si estingua, o una parte possa eccepire l'inadempimento della prestazione della controparte o, infine, casi in cui le parti possano regolare o modificare determinati termini contrattuali (per es. nei casi di impossibilità sopravvenuta di cui all'art. 1256 del codice civile italiano o nei casi in cui una prestazione risulti, in un momento successivo alla stipula, particolarmente onerosa).

Per riflettere queste casistiche previste da tempo dal legislatore, anche gli Smart Contracts dovrebbero "dotarsi" di previsioni analoghe. Tale peculiarità però si scontra, ad esempio, con le caratteristiche intrinseche di una Blockchain.

Ma come regolare una situazione in cui uno Smart Contract è presente all'interno di una Blockchain?

La tecnologia Blockchain permette transazioni "*trust-less*" grazie al suo registro distribuito e quindi non necessita di intermediari di fiducia o di una c.d. *clearing house* (caratterizzata invece da un registro centralizzato o dal suo libro mastro) che diano validità alla transazione stessa o ne

[20] Si prenda il caso di complessi contratti che hanno ad oggetto appalti internazionali o che regolano transazioni internazionali di vario genere.
[21] Per un approfondimento si veda: De Filippi, Wright "Blockchain and the Law" 2018, part 2 chapter 4.

permettano, in un certo senso, la conoscenza all'interno dell'ordinamento giuridico grazie a diverse forme di pubblicità. Inoltre, la Blockchain può venire in aiuto in transazioni tra svariati soggetti (c.d. *many to many*) quindi quando vi sono una pluralità di soggetti che, in assenza di fiducia, vogliono comunque avere garanzie sulla transazione ed il suo buon esito.

Nel mondo digitale questo può portare indubbiamente dei grandi benefici come l'abbattimento di eventuali procedure o lungaggini, assicurare un corretto salvataggio delle transazioni e un reporting delle attività preciso e sostanzialmente immediato.

Sebbene di difficile implementazione, uno Smart Contract potrebbe per esempio prevedere la possibilità di inserire ulteriori parti di codice in un secondo momento: in altre parole, lasciare delle "righe vuote" in caso di necessità. Oppure potrebbe prevedersi la possibilità di "sovrascrizione" richiamando parti di uno Smart Contract inserito su una Blockchain e, con appositi rimandi o richiami, prevedere per la comunità che alimenta e sostiene la Blockchain, di fare riferimento ad un determinato contratto inserito in uno blocco successivo e che "annulla e sostituisce" il precedente blocco contenente il vecchio contratto da modificare[22].

Tali esempi sono, al momento attuale, meramente delle ipotesi a cui dovranno seguire ulteriori e più approfonditi studi, soprattutto in termini di fattibilità.

Nel recente passato, di fronte ad eventuali errori, la comunità che compone una Blockchain ha optato generalmente per dei c.d. "fork" (siano essi hard o soft) con i quali, in buona sostanza, è avvenuta una divisione rispetto all'originaria Blockchain. Basti pensare ai casi di bitcoin cash o di ethereum classic.

Altri profili giuridici di rilievo: legge applicabile e foro competente

Nella presente sottosezione analizzeremo brevemente alcune tematiche giuridiche che coinvolgono gli Smart Contracts: in sostanza evidenzieremo alcune problematiche riguardanti quale legge applicare ad uno Smart Contract e quale giudice dovrebbe venir chiamato a decidere in caso sorgesse un contenzioso.

Uno Smart Contract *Blockchain-based* presenta la caratteristica di essere replicato su tutti i nodi che compongono la Blockchain; ciò permette di avere un elevato numero di copie del registro e delle transazioni in esso contenute: la difficoltà di stabilire **quale legge applicare ad uno Smart Contract** risiede nel fatto che potrebbe essere complesso determinare l'esatta locazione del bene (se esso fosse puramente digitale) e/o capire quale è la prestazione caratteristica che è rappresentata dallo Smart Contract.

In ambito europeo potrebbero venire in aiuto atti legislativi già operativi quali il Regolamento 593/2008[23] chiamato "**Regolamento Roma 1**" che, se correttamente adattato alle circostanze di uno Smart Contract e/o a seguito di una valutazione caso per caso, potrebbe fornire un valido supporto agli operatori del diritto[24].

[22] Alcune considerazioni di questo tipo sono presenti in: Raskin "The Law and Legality of Smart Contracts" 2017.
[23] Il testo completo del Regolamento 593/2008 è disponibile qui: https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=celex%3A32008R0593
[24] Sul tema, fra gli altri, si veda anche il contributo della Chamber of Digital Commerce chiamato "Smart Contracts: Is the Law Ready?" 2018.

Tema altrettanto interessante e dai tratti fortemente simili riguarda l'attuale difficoltà nel **determinare il giudice territorialmente competente** in caso di contenziosi che coinvolgono uno Smart Contract.

Se la transazione regolata dallo Smart Contract riguarda un bene fisico parrebbe di semplice soluzione determinare la giurisdizione sulla base dell'esatta posizione fisica del bene in questione al momento della conclusione dello Smart Contract.

Ma se invece si tratta di un bene puramente digitale (come una cryptomoneta o un servizio online) e le parti non hanno regolato ex ante tale tematica?

Al momento attuale non sono presenti soluzioni giuridiche condivise e il rischio che si corre è quello di ottenere una frammentazione delle soluzioni che diventi un ostacolo alle transazioni: come altri autori sollevano, risulta attualmente necessario lavorare su un **framework condiviso** o su delle linee guida che, a livello internazionale, determinino o aiutino a determinare quale giudice possa essere territorialmente competente in caso di contenziosi su Smart Contracts[25].

La situazione italiana attuale

Il legislatore italiano ha recentemente introdotto i concetti di Blockchain e Smart Contract nell'ordinamento giuridico nazionale: nel decreto-legge 135/2018 (convertito con la legge 12/2019) sono state, infatti, inserite le definizioni di Blockchain e di Smart Contract, disciplinandone altresì il valore giuridico[26].

Il provvedimento in esame definisce le "tecnologie basate su registri distribuiti" (quindi di fatto la Blockchain) come 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. Con riferimento al valore probatorio generato dall'utilizzo della Blockchain viene previsto che la memorizzazione di un documento informatico attraverso l'uso della Blockchain produca gli effetti giuridici della validazione temporale elettronica di cui al Regolamento UE 910/2014 in materia di identificazione elettronica (Regolamento EIDAS).

La stessa legge, come anticipato, si occupa altresì degli Smart Contract, definiti come programmi per elaboratore che operano su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente le parti sulla base di effetti predefiniti dalle stesse. Gli Smart Contract, se conformi ai requisiti che dovranno essere definiti dall'Agenzia per l'Italia Digitale, potranno soddisfare il requisito della forma scritta previa identificazione informatica delle parti interessate.

Il legislatore italiano ha voluto creare un panorama di maggiore certezza giuridica nei confronti di Blockchain e degli Smart Contract, anche in considerazione del forte interesse della pubblica amministrazione italiana rispetto a questa materia.

[25] Per un approfondimento si veda anche de Caria "A Digital Revolution in International Trade? The International Legal Framework for Blockchain Technologies, Virtual Currencies and Smart Contracts: Challenges and Opportunities".
[26] Il testo completo della legge 12/2019 è disponibile qui:
http://www.gazzettaufficiale.it/eli/id/2019/02/12/19G00017/SG

Si tratta, tuttavia, di una regolamentazione di livello nazionale che dovrà necessariamente confrontarsi con un panorama giuridico più ampio e potrebbe essere soggetta a future modifiche o integrazioni, così come avvenuto nel passato per la regolamentazione del documento informatico e delle firme elettroniche in cui l'Italia è stata uno dei primi paesi a prevedere una normativa a livello nazionale (poi modificata molte volte per adeguarla a direttive o regolamenti dell'Unione Europea).

.

Blockchain e Privacy

Il nuovo Regolamento europeo per la protezione dei dati personali
Il mondo della data protection ha vissuto negli ultimi anni una forte rivoluzione, dettata dall'entrata in vigore del Regolamento UE n. 2016/679 il c.d. "GDPR".

Il Regolamento persegue due obiettivi fondamentali: da un lato, adeguare la normativa, risalente al 1995, alle nuove tecnologie, dall'altro armonizzare ed uniformare la normativa a livello europeo, creando un quadro normativo comune.

Il GDPR, all'articolo 5 fissa i principi del trattamento. In particolare:

- **liceità e correttezza:** impone una corretta informazione dei soggetti interessati circa la raccolta, l'utilizzo ed il trattamento dei loro dati.

- **trasparenza:** non attiene solamente al contenuto dell'informazione relativa al trattamento, ma anche alle modalità con cui esso è formulato e veicolato; si estende anche ai successivi rapporti tra interessato e titolare e/o responsabile.

- **pertinenza e adeguatezza:** per garantire che vengano raccolti solo quei dati effettivamente funzionali al perseguimento delle finalità per cui sono stati raccolti.

- **non eccedenza e principio di necessità: principio** secondo cui è opportuno ridurre al minimo l'utilizzo di dati personali, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Agli interessati (soggetti cui i dati personali si riferiscono) devono anche essere garantiti una serie diritti. In riferimento alla tecnologia Blockchain, giova ricordare il diritto di accesso (che prevede la possibilità per l'interessato di conoscere quale trattamento di dati è in atto e le relative informazioni), il diritto di rettifica e integrazione (correzione di inesattezze ed integrazione di informazioni non complete) ed, infine, il diritto alla cancellazione e "oblio" (la pretesa alla cancellazione dei dati da parte dell'interessato nel caso in cui ricorrano determinate presupposti).

GDPR e Blockchain

Appare subito evidente come le principali caratteristiche che rendono unica la tecnologia Blockchain, possono entrare in contrasto con quanto previsto dal GDPR.

Molti dei diritti e degli obblighi specificati nel GDPR sembrano in contrasto con la modalità di memorizzazione utilizzata dalla Blockchain, in quanto essa è progettata in modo che i dati, una volta riportati al suo interno, non possano essere modificati e/o cancellati. Questa immutabilità è una proprietà chiave della tecnologia, ma genera problemi circa l'esercizio del diritto alla cancellazione o alla rettifica dei dati.

Anche in merito al diritto di accesso, sorge il problema del soggetto a cui occorre rivolgersi per ottenere le informazioni richieste, non essendovi sempre un titolare identificato. Inoltre, anche se l'interessato riesca a identificare e comunicare con un nodo specifico (in questa situazione, identificato come titolare del trattamento), lo stesso non sarebbe in grado di rispondere a questa richiesta, non riuscendo a fornire le informazioni necessarie.

Altra problematica risiede nel campo di applicazione territoriale in relazione al trattamento, poiché chiunque può utilizzare una piattaforma Blockchain pubblica. Si può pertanto ritenere che gli operatori di tali piattaforme, ove offrano servizi agli interessati nell'UE, debbano applicare il GDPR.

In linea di principio pare ragionevole sostenere che, proprio per come è strutturata una Blockchain pubblica non sembra essere il luogo adatto in cui inserire dati personali. Per quanto possa essere rispettato il principio di trasparenza secondo cui tutto quello che viene registrato sulla rete è sempre noto a tutti i partecipanti in maniera sicura e non modificabile, tutti i dati sono pubblici e visionabili da tutti gli utenti della rete.

Ecco perché, comunque, i problemi sopra esposti non necessariamente possono essere risolti semplicemente passando da una Blockchain pubblica ad una Blockchain privata, a meno che non venga progettata per far sì che ogni singolo dato sia leggibile solo dalle parti che ne hanno assolutamente bisogno e diritto, e possa essere rettificato o cancellato su richiesta dell'interessato, perdendo la caratteristica dell'immutabilità.

Infatti, è possibile progettare un sistema, basato sulla tecnologia Blockchain, in modo tale che i dati personali non siano memorizzati nella catena stessa, ma all'interno di una banca dati separata "*off-chain*" in forma criptata, andando poi a riportare nella Blockchain l'hash di riferimento. I dati delle transazioni conterrebbero quindi solo le informazioni necessarie per accedere ai dati personali nella banca dati separata, limitando il trattamento dei dati personali, favorendo il principio di minimizzazione di cui al GDPR.

Rispetto a quanto appena riportato e vista la maggior predisposizione delle Blockchain permissioned nei confronti della data protection, degli adempimenti richiesti del rispetto dei principi della materia, i prossimi paragrafi prenderanno in considerazione proprio questa tipologia di Blockchain.

Quale trattamento di dati personali nella Blockchain permissioned?

La prima nozione da conoscere è quella di dato personale, con la quale viene definita qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online (come l'indirizzo IP) o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Alcuni esempi di dati personali sono i dati anagrafici, gli indirizzi e-mail, il codice fiscale, l'IBAN, il numero di telefono e di fax, l'impronta digitale, il badge, una fotografia, la password, dati necessari per la misurazione-gestione-monitoraggio del rischio di credito, etc.

Per trattamento, invece, s'intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali (come

la raccolta, la registrazione, la conservazione, la modifica, la consultazione, la cancellazione, ecc.).

Se gli utilizzatori della piattaforma sono persone fisiche, gli indirizzi dei loro wallet (del mittente e del destinatario) sono considerati dati personali, insieme alle loro chiavi pubbliche. Pertanto, gli utilizzatori di una Blockchain possono trattare dati personali durante l'invio, la verifica e la memorizzazione dei dati delle transazioni.

Poiché la chiave pubblica è una lunga serie di caratteri (quasi casuali) non c'è, di base, la possibilità che questa riveli informazioni sul suo proprietario.

Se invece, ad esempio, qualcuno utilizzi lo stesso indirizzo per multiple transazioni, allora cominciano a crearsi dei "modelli". Questi possono, se combinati con altri tipi di informazioni, essere utilizzati per identificare indirettamente i singoli utenti.

Per questo motivo, negli ultimi tempi sono state trovate soluzioni di offuscamento degli indirizzi. La più comune è chiamata "third-party indirection service" e consiste nel chiedere a terzi di aggregare molte transazioni Blockchain e registrarle sul registro, utilizzando la propria chiave pubblica.

A questa tecnica, ovviamente, possono essere affiancate soluzione di hashing. La questione se i dati oggetto di hash debbano essere considerati ancora dati personali è attualmente oggetto di un acceso dibattito: non tutti gli algoritmi di hashing sono uguali.

Il nocciolo della questione potrebbe essere costituito dall'individuazione di potenziali rischi di reversibilità o di correlabilità.

Per quanto riguarda il rischio di reversibilità, un attacco rilevante potrebbe riuscire ad invertire l'hash, come sottolineato dal gruppo di lavoro "articolo 29" (Working Party article 29): "if the range of input values the hash function are known they can be replayed through the hash function in order to derive the correct value for a particular record. For instance, if a dataset was pseudonymised by hashing the national identification number, then this can be derived simply by hashing all possible input values and comparing the result with those values in the dataset" (WP246, Opinion 05/2015 on Anonymisation Technique).

Tuttavia, è possibile progettare una piattaforma Blockchain in modo tale che i dati personali non siano memorizzati nella catena stessa, ma in forma cifrata all'interno di una banca dati separata "off-chain".

I dati delle transazioni conterrebbero quindi solo le informazioni necessarie per accedere ai dati personali nella banca dati separata (l'hash). In questo modo, è possibile limitare il trattamento dei dati personali ed evitare di conservare tali dati nella catena a blocchi, favorendo il principio di minimizzazione di cui al GDPR. Inoltre, le suddette informazioni comunque non sono sempre riferibili ad una persona fisica identificabile.

Emerge chiaramente come tutto questo sia possibile quando ci si muove all'interno di uno spazio maggiormente "controllato", in una Blockchain permissioned. Anche se il fatto che i membri di una Blockchain di questo tipo siano vincolati da termini e condizioni contrattuali non significa, ad esempio, che tutti siano legittimati da un valido motivo per poter vedere i dati di ciascun soggetto partecipante.

Ecco che in questo caso l'impatto del GDPR si presenta sotto il nuovo principio di data protection by design. Quest'ultimo impone di considerare tutte le possibili implicazioni di un nuovo prodotto/servizio, che hanno un impatto sui dati personali di una persona fisica, sin dalla progettazione dello stesso in modo tale da minimizzare a priori non solo la raccolta dei dati, ma anche i trattamenti successivi effettuati.

La difficile individuazione dei ruoli privacy

In una rete Blockchain esistono due tipi di nodi:

- nodi di convalida: questi possono aggiungere dati al registro, secondo un algoritmo concordato (il meccanismo di consenso);
- nodi partecipanti: memorizzano copie aggiornate dei dati. A seconda della tecnologia utilizzata, non tutti i nodi possono necessariamente memorizzare tutti i dati. Se un utente è collegato ad un nodo partecipante, può aggiungere nuovi dati al registro, ma questi dati devono essere inviati prima al nodo partecipante, e poi ad un nodo di convalida.

In materia di protezione dei dati personali, sono previste tre figure principali:

- titolare del trattamento: colui che decide mezzi e finalità del trattamento;
- responsabile del trattamento: chi tratta i dati per conto del titolare e secondo sue istruzioni;
- soggetto interessato: la persona di cui vengono trattati i dati.

Quindi, ipotizzando che alcune organizzazioni decidano di creare una piattaforma Blockchain c.d. "permissioned", con un ristretto numero di nodi affidabili, esse che hanno creato la piattaforma determinano i mezzi di elaborazione progettando la piattaforma, stabilendo quali dati memorizzare nella Blockchain e come elaborarli (attraverso il protocollo di consenso).

Questi soggetti andranno anche a determinare lo scopo del trattamento, configurandosi quindi come titolari del trattamento.

La Commission Nationale Informatique & Libertés (CNIL), autorità garante francese per la protezione dei dati personali, nella sua analisi della tecnologia Blockchain e GDPR sostiene che un partecipante deve configurarsi quale titolare del trattamento quando:

- è una persona fisica e l'operazione di trattamento dei dati personali è connessa ad un'attività professionale o commerciale (cioè quando l'attività non è strettamente personale);
- è una entità giuridica che registra i dati personali su di una Blockchain.

Quando più titolari decidono di trattare i dati personali in una Blockchain per una finalità comune, la CNIL raccomanda che i partecipanti siglino in un accordo tutto ciò che riguarda la responsabilità del trattamento da parte degli stessi. In caso contrario, tutti i partecipanti saranno considerati come contitolari del trattamento.

In una Blockchain, secondo la CNIL, possono esistere due tipi di responsabili del trattamento:

- sviluppatori di "Smart Contract", che trattano i dati personali per conto del titolare del

trattamento dei dati;

- miner, che convalidano le transazioni per conto del titolare.

Il trasferimento dei dati

Il GDPR impone condizioni per i trasferimenti di dati personali dall'UE verso paesi terzi (al di fuori del c.d. SEE - Spazio Economico Europeo), per cui i titolari del trattamento devono assicurarsi di disporre di una adeguata base giuridica per il trasferimento dei dati.

Le piattaforme distribuite sono però concepite, per impostazione predefinita, senza confini: in genere chiunque, ovunque, può scaricare l'intero archivio delle transazioni e iniziare ad operare comportando conseguentemente un trasferimento di dati verso paesi terzi.

Non essendo perseguibile la via del consenso implicito per i trasferimenti internazionali, anche alla luce del fatto che il GDPR stabilisce che il consenso debba essere specifico e inequivocabile, le condizioni d'uso della piattaforma dovrebbero prevedere un consenso chiaro ed esplicito dell'interessato oppure dovrebbe sussistere un'adeguata base giuridica alternativa.

In ogni caso, esistono delle condizioni a cui un titolare del trattamento deve sottostare per il trasferimento dei dati all'estero.

Il GDPR prevede che i dati personali possono essere trasferiti generalmente solo verso paesi terzi se sono ritenuti "adeguati" dalla Commissione Europea (che sono stati oggetto di una decisione di adeguatezza) oppure, in caso di mancanza di quest'ultima, o se il titolare del trattamento può introdurre adeguate garanzie che i dati saranno trattati in modo coerente con tale trattamento legge.

L'esercizio dei diritti degli interessati

Gli interessati hanno il diritto di ottenere un giusto trattamento dei propri dati personali. Tali diritti comprendono il diritto di accesso, alla rettifica dei dati personali inesatti e alla cancellazione dei dati, tuttavia, la capacità di soddisfare tali richieste varia a seconda di come una piattaforma Blockchain è stata pensata ed impostata.

Le Blockchain permissioned possono supportare meglio tali necessità poiché è chiaro a chi un interessato può rivolgersi per esercitare i propri diritti.

La CNIL osserva che è tecnicamente impossibile accogliere la richiesta di cancellazione presentata da un interessato quando i dati sono registrati su una Blockchain. Tuttavia, quando i dati registrati sono cifrati attraverso validi algoritmi, il titolare del trattamento può rendere i dati praticamente inaccessibili.

Queste soluzioni tuttavia non comportano, in senso stretto, una cancellazione dei dati, visto che i dati esisterebbero ancora nel blocco, pertanto è preferibile evitare di registrare su di una Blockchain dati in chiaro o non cifrati.

Concludiamo questo capitolo indicando due documenti essenziali per il dibattito su questi temi:

- Blockchain. Solutions for a responsible use of the blockchain in the context of personal data; CNIL-Commision Nationale Informatique & Libertés;
- Blockchain and the GDPR; The European Union blockchain Observatory and Forum.

Le attività di standardizzazione

Perché standard su Blockchain

Prima di analizzare quali sono le attività di standardizzazione in corso sulle tecnologie Blockchain e Distributed Ledger Technologies (BDLT) è utile provare a comprendere quale può essere l'utilità di avere standard in questo ambito posto che finora l'uso massivo di queste tecnologie è stato in ambito criptovalute, ognuna delle quali nata spontaneamente e operante come un'isola a sé stante.

In realtà gli utilizzi più promettenti delle tecnologie BDLT che stanno emergendo e si stanno consolidando, in aree diverse dalle criptovalute, sono ambiti dove gli standard possono svolgere un ruolo abilitante chiave.

Le tecnologie BDLT abilitano principalmente l'implementazione di infrastrutture di notarizzazione che non prevedono la necessità di una governance centralizzata pur garantendo resistenza alla manomissione delle informazioni e sicurezza attraverso protocolli e tecniche crittografiche che garantiscono consenso condiviso, distribuzione delle risorse e disintermediazione dando disponibilità di dati aggiornati e affidabili in tempi ragionevoli a tutte le parti interessate e collegate all'infrastruttura. Per approfondimenti si vedano le altre parti di questo documento.

La disponibilità di standard per questo tipo di infrastrutture può svolgere un ruolo abilitante fondamentale in quanto, a differenza del caso delle criptovalute, le esigenze fondamentali sono la possibilità di integrare servizi ed applicazioni gestite da soggetti diversi e garanzie sufficienti di disponibilità, integrità ed origine delle informazioni e delle transazioni.

L'esigenza naturalmente è anche quella di avere standard che devono essere il più possibile globali che tengano però conto della compliance con le esigenze specifiche europee, legate ad esempio all'esigenza di compliance con le normative in materia di protezione dei dati personali (quali il Regolamento Europeo n 679/2016 - GDPR).

La mancanza di interoperabilità crea limiti tecnici che la Commissione europea cerca da tempo di eliminare per realizzare il mercato interno (si veda ad esempio il Libro bianco sul completamento del mercato interno, 14 giugno 1985, COM (85) 310 def).

In ambito BDLT è però particolarmente complesso sviluppare degli standard, dato che si tratta di un mercato con potenzialità elevate ma immaturo dove le uniche applicazioni su larga scala sono ad oggi le criptovalute che sono un fenomeno nato dal basso e piuttosto refrattario a regole imposte dall'esterno. Inoltre, si tratta di tecnologie tipicamente "orizzontali" e gli standard devono poter supportare da un lato una elevata molteplicità di applicazioni in ambiti disparati, dall'altro la compliance a regole comuni, si pensi ad esempio al già citato GDPR ma anche ad eIDAS per identità e servizi fiduciari.

Le attività di normazione tecnica in corso si svolgono a livello internazionale nel comitato tecnico ISO/TC 307. In Europa, per monitorare i lavori internazionali al fine di identificare eventuali carenze rispetto ad esigenze europee e quindi portarle e discuterle sui tavoli ISO, è stato creato congiuntamente da CEN e CENELEC il Focus Group Blockchain and Distributed Ledger Technologies.

Le aree di standardizzazione si concentrano su due aspetti principali:

- l'interoperabilità, identificando architetture di riferimento ed elementi base interoperanti e per consentire l'utilizzo dell'infrastruttura da parte di qualsiasi applicazione che necessita di servizi di notarizzazione;
- la compliance, per consentire la garanzia di livelli di sicurezza e affidabilità accettabili e il rispetto di norme vincolanti come iquelle in materia di protezione dei dati personali.

L'uso di standard può supportare entrambe queste esigenze e, nei prossimi paragrafi, verrà presentata una panoramica delle principali attività in corso a livello europeo e internazionale.

I lavori in ambito ISO

ISO/TC 307 "Blockchain and distributed ledger technologies" è un Comitato Tecnico che è stato istituito in ISO per rispondere alla crescente necessità di standardizzazione in questo settore.

L'ISO garantisce modalità di lavoro concordate a livello internazionale e gli obiettivi principali che si pone per migliorare la sicurezza, la protezione dei dati personali e l'interoperabilità al fine di facilitare l'uso a livello globale di questa tecnologia.

Ciò è particolarmente importante sia lato offerta, per supportare una competizione corretta in un mercato che vede la presenza di molte PMI che sviluppano prodotti, soluzioni e servizi basati su questa tecnologia, sia lato domanda, che richiede strumenti interoperabili e che garantiscano livelli certi di compliance, sicurezza e affidabilità.

ISO/TC 307 è stato suddiviso in vari gruppi per indirizzare in modo strutturato le varie aree di interesse:

- WG 1 "Foundations", che ha il compito di definire un vocabolario e un'architettura di riferimento comuni;
- WG 2 "Security, privacy and identity" si occupa di aspetti chiave per il futuro di queste tecnologie, in particolare qui rientrano privacy e identità che, in Europea, si declinano in compliance con i regolamenti GDPR ed eIDAS;
- WG 3 "Smart Contracts and their applications" che indirizza la tematica dei contratti intelligenti e come renderli giuridicamente vincolanti;
- WG 5 "Governance" si pone l'obiettivo di definire delle linee guida in uno degli ambiti più importanti e potenzialmente controversi;
- SG 2 "Use cases" è un gruppo di studio che mantiene un elenco di use case che sono utilizzati per mappare il lavoro degli altri gruppi su casi reali;
- SG 7 "Interoperability of Blockchain and distributed ledger technology systems" è un altro

Gruppo di studio che affronta gli aspetti di interoperabilità in modo trasversale rispetto agli altri gruppi;

- JWG 4 “Blockchain and distributed ledger technologies and IT Security techniques” è un Gruppo di lavoro congiunto con ISO/IEC JTC 1/SC 27 che consentirà di indirizzare le tematiche in ambito sicurezza sulla linea dei lavori di SC27 ovvero della nota famiglia di norme ISO/IEC 27000, portando quindi in ambito Blockchain una metodologia ed esperienza che sono riconosciuti leader a livello mondiale.

I lavori in ambito CEN/CENELEC e nazionale

Per far fronte in modo strutturato alle esigenze che nascono in ambito europeo e mappare queste esigenze sui lavori in corso a livello internazionale è nato un Focus Group in ambito CEN/CENELEC, due dei tre enti di standardizzazione riconosciuti a livello UE.

Il Focus Group CEN/CENELEC “Blockchain and Distributed Ledger Technologies” ha prodotto il white paper “Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies”.

Il Libro bianco affronta temi prioritari quali lo sviluppo sostenibile, l'identità elettronica, la privacy e la protezione dei dati fornendo 26 raccomandazioni e mettendo in evidenza casi specifici di utilizzo europeo. In particolare, la protezione dei dati personali è l’area sulla quale è più urgente un intervento in quanto il GDPR da un lato è una normativa molto stringente e, dall’altro, ha comunque un'applicazione regionale mentre ISO opera a livello globale, è necessario che l’Europa inizi ad avere un ruolo diretto nello sviluppo di standard in quest’area.

Quanto al contesto italiano è stata istituita la Commissione UNI/CT 532 in seno ad UNINFO che svolge attività di mirror rispetto a quelle internazionali ed europee. È infatti fondamentale che qualunque contributo nazionale tenga conto della collocazione dell’Italia nel contesto europeo e mondiale.

Conclusioni

La disponibilità di standard per infrastrutture basate su BDLT è determinante per passare da progetti pilota o “proof of concept” a un utilizzo di tipo industriale. Svolgerà un ruolo abilitante in quanto le esigenze fondamentali per l’uso di Blockchain da parte delle organizzazioni si riferiscono soprattutto alla possibilità di integrare servizi e applicazioni gestite da soggetti diversi dando a tutte le parti interessate garanzie sufficienti di disponibilità, integrità ed origine delle informazioni e delle transazioni.

Gli standard punteranno a dare una risposta a questioni come:

- la garanzia di livelli di sicurezza adeguati, rendendo comparabili le caratteristiche di sicurezza di un’infrastruttura basata su BDLT rispetto ad una tradizionale e permettendo alle parti interessate una valutazione del rischio;

- la conformance legale in aree come protezione dei dati personali e identità digitale dove in Europa ci sono regolamenti molto stringenti (GDPR ed eIDAS);
- indirizzare il problema dell'interoperabilità per consentire l'utilizzo di questa tecnologia in contesti che sono tipicamente internazionali e con la coesistenza di numerosi attori che devono interagire con ruoli differenti.

Cyber attacchi

Prima di affrontare tematiche relative alla sicurezza, si ritiene utile fornire di seguito un elenco di attacchi che riguardano l'ambito Blockchain su cui è stata effettuata un'analisi seguendo la metodologia già applicata per il Rapporto Clusit (per maggiori dettagli si veda https://clusit.it/rapporto-clusit/).

Tale metodologia considera:

- incidenti collezionati a partire da fonti aperte
- news riguardanti esclusivamente attacchi informatici (escludendo le notizie su nuove vulnerabilità o le analisi di ricercatori)
- attacchi considerati gravi

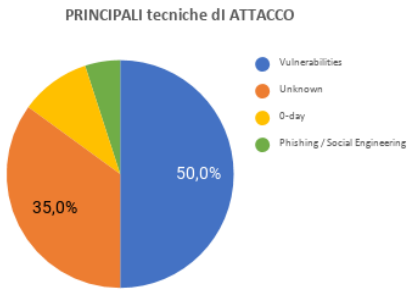


Figura 5: Principali tecniche di attacco, Fonte Clusit

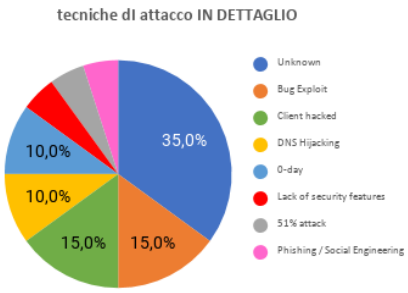


Figura 6: Dettaglio tecniche di attacco, Fonte Clusit

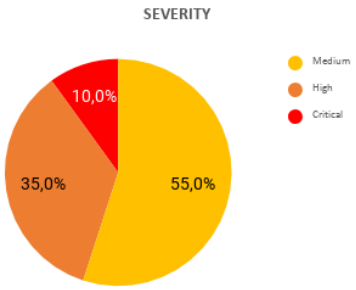


Figura 7: Severity secondo la classificazione Clusit, Fonte Clusit

Si noti che ogni incidente censito è riferito alle criptovalute che, pur non essendo il focus principale di questo paper, rappresentano il bene di maggior interesse per gli attaccanti essendo immediatamente monetizzabili.

Di seguito riportiamo l'elenco degli incidenti più significativi selezionati secondo i seguenti criteri:

- gravità dell'impatto immediato;
- innovazione della tecnica utilizzata per perpetrare l'attacco;
- severità delle conseguenze;
- persistenza di grandi rischi associati a tecniche note (come ad esempio bug nel codice, DNS Hijacking, client vulnerabili, …).

Bug nel codice:

17 febbraio 2017

Il Team di ***Zerocoin*** ha avvisato i propri utenti di aver trovato un bug nel suo codice: un errore tipografico su un carattere.

Il bug era stato sfruttato da un attaccante permettendogli di riutilizzare le sue prove valide esistenti per generare ulteriori transazioni di spesa con Zerocoin.

L'attaccante ha generato transazioni per 403.050 Zcoin, successivamente venduti quasi interamente con un profitto complessivo di 410 BTC.

Zerocoin ha scoperto l'attacco quando ha constatato che il totale delle monete coniate non corrispondeva al totale delle transazioni effettuate.

https://zcoin.io/important-announcement-zerocoin-implementation-bug/

DNS Hijacking e sospensione del servizio:

20 dicembre 2017

Il popolare exchange di cryptocurrency ***EtherDelta*** ha avvisato i propri utenti di aver subito un attacco al suo server DNS.

Come risultato dell'attacco EtherDelta ha dovuto sospendere il servizio per 2 giorni, invitando gli utenti a non utilizzare il sito.

Gli hacker hanno *spoofato* il dominio di EtherDelta per indurre gli utenti ad inviare denaro e sono stati così in grado di rubare oltre 300 ETH (circa $ 265,000 all'epoca dell'attacco).

https://securityaffairs.co/wordpress/67146/cyber-crime/exchange-etherdelta-dns-attack.html

Maggiore furto noto:

26 gennaio 2018

L'exchange di cryptovalute giapponese ***Coincheck*** ha subito il più grande furto noto in cui sono stati rubati 500 milioni di NEM, l'equivalente di $ 524 milioni.

Coincheck non è stata in grado di individuare la causa dell'attacco ma molti sospettano che la mancanza di portafogli *multi-sig* dell'exchange, in cui sono necessarie più chiavi per autorizzare una transazione, sia parte integrante delle vulnerabilità che hanno facilitato l'hack.

http://fortune.com/2018/01/26/bitcoin-price-coincheck-nem-mt-gox/

Client vulnerabili:

15 marzo 2018

Dei cybercriminali sono stati in grado di guadagnare oltre $ 20 milioni dirottando ***nodi Ethereum*** mal configurati esposti su Internet.

Un primo gruppo di attaccanti ha effettuato una scansione del web alla ricerca di porte JSON-RPC 8545 per trovare client *geth* insicuri che eseguivano nodi Ethereum esposti su Internet.

In questo modo sono stati in grado di rubare 3.96234 unità di Ether.

Successivamente un altro gruppo di cybercriminali ha sfruttato lo stesso sistema per rubare un totale di 38,642 Ether (più di $20,500,000 calcolato sul prezzo al momento dell'attacco).

https://thehackernews.com/2018/06/ethereum-geth-hacking.html

0-day:

04 aprile 2018

Un attaccante ha sfruttato un bug nel codice della cryptomoneta Verge per estrarre monete di Verge (XVG) alla velocità quasi impossibile di 1.560 XVG al secondo (equivalente a $ 78 / s).

L'hacker ha realizzato circa 15,6 milioni di XVG (circa $ 780.000) con un attacco durato solamente tre ore.

Il team di sviluppo di Verge ha corretto il bug con un hard-fork dell'intero codice per ripristinare la Blockchain in uno stato precedente all'attacco.

https://www.bleepingcomputer.com/news/cryptocurrency/hacker-uses-exploit-to-generate-verge-cryptocurrency-out-of-thin-air/

DNS Hijacking tramite dirottamento rotte BGP:

24 aprile 2018

MyEtherWallet.com, un servizio web di wallet Ether, ha subito un DNS Hijacking tramite il dirottamento delle rotte BGP che ha reindirizzato il traffico destinato ai server Amazon utilizzati dal servizio.

Gli utenti che hanno provato ad accedere a MyEtherWallet nel corso dell'attacco sono stati reindirizzati ad una versione falsa del sito web e, successivamente, hanno subito il furto delle chiavi private del proprio wallet, che l'hacker ha utilizzato per svuotare i conti.

Gli amministratori di MyEtherWallet hanno cercato di avvisare gli utenti su Twitter invitandoli a non connettersi al sito.

Il falso sito Web era inoltre facile da individuare in quanto era stato utilizzato un certificato TLS autofirmato che causava un errore in tutti i moderni browser. Nonostante ciò, durante le due ore in cui l'attacco ha avuto luogo, l'attaccante è stato in grado di realizzare 215 Ether (equivalenti a $160,000).

https://www.bleepingcomputer.com/news/security/hacker-hijacks-dns-server-of-myetherwallet-to-steal-160-000/

La Governance della security nei progetti DLT

Uno degli aspetti che maggiormente preoccupa nel garantire la sicurezza durante un progetto che adotti la tecnologia Blockchain è l'effettivo coinvolgimento dei reali stakeholder, la definizione di ruoli e mansioni adeguati sia in fase di implementazione che di mantenimento.

Il rischio che il servizio e l'infrastruttura tecnologica vengano forniti da parti terze direttamente ai process owner è altissimo. Questo porterebbe, come già accade per altri servizi, ad un mancato coinvolgimento degli staff che dipendono dal CIO, dal CISO e dall'Audit, solo per fare alcuni esempi.

Si teme che l'aspetto di "novità", di disruption, di percezione del servizio possa portare a comportamenti difformi rispetto a quanto normalmente si applica ad un nuovo fornitore di un servizio software. Il timore si fonda su tutte le inefficienze ed i problemi che si sono sperimentati in alcune organizzazioni nell'adozione di "nuove tecnologie" come è stato il cloud diversi anni fa.

Anche in realtà strutturate, con processi formalizzati di selezione del fornitore, rigide regole per il procurement IT (ad esempio processi di change, incident, access, vulnerability e log management efficaci e calati in un contesto maturo), il rischio di avviare un progetto ignorando totalmente le procedure aziendali e abilitando un servizio innovativo a gestire dati aziendali in un ambiente di produzione rischia di essere alto.

Per le aziende e Pubbliche Amministrazioni meno organizzate formali e mature la probabilità che avvenga rasenta la certezza.

Che ruolo dovrebbero avere quindi le diverse strutture aziendali in un progetto che coinvolga la Blockchain?

A nostro parere gli stessi attori che presidiano il tema sviluppo/adozione del software per risposta ad esigenza di business dovrebbero conservare gli stessi ruoli e dovrebbero assicurare che vengano applicati gli stessi processi/prassi virtuose già in uso anche a questa tecnologia, come fosse un gestionale o un CRM.

Non è pensabile, infatti, che non esistano tutte le verifiche di sicurezza, ma anche funzionali, di compliance, di gestione, di verifica, che insistono su tutte le altre tecnologie/servizi aziendali.

Quando si adotta una soluzione Blockchain è altresì importante definire un processo di integrazione in cui vengono valutati tutti i possibili rischi e impatti della nuova soluzione sia sui processi aziendali che sulle altre soluzioni già esistenti all'interno del perimetro aziendale.

Le problematiche che risultano da questo processo di pianificazione dovrebbero essere soppesate con cura e utilizzate per indirizzare le scelte tecnologiche. Va comunque tenuto presente che l'integrazione all'interno dei processi aziendali può richiedere un certo impegno e quindi è necessario stanziare le giuste risorse. Occorre, inoltre, definire specifiche policy che vanno integrate opportunamente con quelle già esistente, ponendo particolare attenzione a possibili conflitti.

Nel caso siano già definiti processi formalizzati di audit per le soluzioni software aziendali, è importante valutare che questi siano applicabili anche alla nuova tecnologia. La natura decentralizzata della Blockchain, per esempio, potrebbe rendere inapplicabile il processo di audit

già definito.

Per comprendere meglio questo punto basti pensare al caso di una Blockchain pubblica. L'idea di fare audit sul codice e su eventuali algoritmi è possibile, mentre, svolgere attività di audit sulle macchine fisiche con lo scopo di verificare il rispetto di requisiti prestabiliti potrebbe risultare improponibile.

L'impatto della Blockchain sull'Information Security

I più critici nei confronti di questa tecnologia, esasperati dall'hype di attenzione che questa ha avuto su giornali ed a convegni, chiedono continuamente "perchè dovrei usarla?".

La domanda non è solo sensata, è necessaria. I rischi di adottare una DLT più per la sua notorietà che per effettive esigenze aziendali o di considerarla una panacea di ogni male sono, purtroppo, attualmente molto elevati.

Per questa ragione analizzare l'eventuale business case nel quale si vorrebbe adottare una DLT, per avere ben chiari rischi e benefici che la sua adozione comporterebbe, diventa indispensabile per la buona riuscita del progetto.

La Blockchain ha molti vantaggi, spesso gli unici ad essere nominati in articoli e conferenze, ma possiede anche aspetti di minor efficacia, inadeguatezza e soprattutto, se non implementata correttamente, può introdurre vulnerabilità come altre tecnologie di cui abbiamo maggiore esperienza.

Iniziamo con analizzare la DLT rispetto alla classica terna RID, riservatezza, integrità e disponibilità, in potenza e nelle prassi, relativamente ai dati conservati.

	Tecnologia tradizionale	**Blockchain**
Riservatezza	• è necessario assicurare una politica di access-control efficace • è possibile crittografare le informazioni in molti modi diversi	• fa della trasparenza e dell'accessibilità da parte di più soggetti il proprio punto di forza, quindi la riservatezza non è la priorità • necessità di pseudo anonimato vengono gestite con soluzioni non "by design"

Integrità	• è necessario assicurare una politica di access-control efficace • è necessario assicurare che l'intero contesto, compreso quello infrastrutturale, sia presidiato correttamente	• è il vero e principale punto di forza: immodificabilità del dato storico, traccia di tutte le attività • il suo essere distribuita impedisce ad un singolo di alterare l'informazione
Disponibilità	• è necessario implementare un backup, un piano di disaster recovery	• essendo distribuita dovrebbe essere ridondante e resiliente per definizione

*Tabella 1: confronto di disponibilità, riservatezza e disponibilità di una tecnologia tradizionale rispetto ad una DLT - **Aspetti strutturali-teorici***

La teoria molto spesso si scontra con la reale applicazione in un contesto aziendale governato da esseri umani. In questo contesto un nuovo progetto di adozione di una DLT, se gestito correttamente, con una fase di analisi e di disegno svolte correttamente, potrebbe portare all'implementazione, "by design", di accortezze che per altre soluzioni presenti in azienda anni non vengono prese in considerazione o vengono ritenute eccessivamente onerose da implementare.

Tuttavia, la scarsa esperienza su questa tecnologia potrebbe, invece, portare a subire errori di immaturità, alcuni dei quali potrebbero avere poi strascichi nel tempo.

	Tecnologia tradizionale	**Blockchain**
Riservatezza	• le politiche di access control rischiano di essere storicamente parzialmente efficaci • la crittografia non è implementata ed implementarla è ritenuto eccessivamente oneroso	• si dà per scontato che il dato sia condiviso e quindi il rischio è chiaro • i vari scenari d'uso potrebbero essere presi in considerazione per adottare le corrette misure

Integrità	• le politiche di access control rischiano di essere storicamente parzialmente efficaci • il contesto infrastrutturale è troppo spesso sottovalutato	• il contesto infrastrutturale potrebbe essere ininfluente
Disponibilità	• spesso il backup non tiene conto dell'integrità del dato	• essendo distribuita dovrebbe essere ridondante e resiliente per definizione

*Tabella 2: confronto di disponibilità, riservatezza e disponibilità di una tecnologia tradizionale rispetto ad una DLT - **Aspetti di reale implementazione***

Da questo confronto emerge come la Blockchain possa contribuire in modo significativo a progetti ove l'integrità sia l'obiettivo principale, portando con sé il benefit della distribuzione del dato. Allo stesso modo conferma che le sue peculiarità non la rendono adatta a qualsiasi contesto, a prescindere dai requisiti, e che quindi debba essere considerata come solo uno degli strumenti a disposizione dell'organizzazione per raggiungere i propri obiettivi specifici, soddisfando "by design", in alcuni casi, esigenze che tecnologie tradizionali possono soddisfare a fronte di effort di progettazione/gestione maggiori.

Garantire la qualità e la sicurezza del codice

Perché è importante?

In un futuro prossimo, dove tecnologie Blockchain saranno presumibilmente integrate in molteplici campi della nostra società, imprecisioni nel codice potrebbero creare danni importanti. In relazione alla specifica applicazione, la risoluzione del problema potrebbe rivelarsi un'impresa non affatto semplice. La storia ci insegna come quelle che in un certo istante è, superficialmente, la scelta giusta, in una prospettiva a lungo termine potrebbe rivelarsi un problema rilevante.

Un esempio non troppo recente, ma che può aiutare a comprendere meglio quello di cui si sta parlando, è il così detto *Y2K*, anche conosciuto come *Millennium Bug*. La scelta di definire l'anno solamente con due sole cifre negli anni Novanta aveva un senso soprattutto in ottica di risparmio di risorse. Con il passaggio nel nuovo millennio però questa scelta ha rischiato di avere un impatto incredibile su diverse realtà. Il ricordo delle preoccupazioni di quel momento e le risorse economiche investite per valutare il reale rischio legato al Millennium Bug e come mitigarlo dovrebbe in qualche modo renderci critici e attenti nell'utilizzo di nuove tecnologie che si basato su linguaggi di programmazione totalmente nuovi in settori strategici come la finanza o la contrattualistica.

La stessa Blockchain, per quanto relativamente recente, ci ha mostrato che questo rischio non è affatto trascurabile. Basti pensare alla vulnerabilità di Bitcoins (CVE-2018-17144) scoperta a settembre 2018 che se sfruttata avrebbe potuto causare un *Denial of Service* e conseguenti problemi di inflazione. Un altro incidente che ha avuto una certa risonanza è quello che ha colpito l'organizzazione DAO *(Decentralized Autonomous Organization)* iniziata sulla Blockchain *Ethereum* accaduto a giugno 2016 che ha permesso ad un attaccante di rubare all'equivalente in dollari di circa 70 milioni. Il problema in questo caso non è dipeso direttamente da Ethereum ma dalla specifica applicazione che è stata costruita su questa Blockchain.

Nell'utilizzo di un nuovo linguaggio di programmazione è buona norma non solo capire la sintassi da utilizzare ma comprenderne a fondo il funzionamento. Dal punto di vista della sicurezza diventa particolarmente rilevante il linguaggio utilizzato per implementare gli Smart Contract.

Vulnerabilità di sicurezza possono essere dovute al fatto che l'esecuzione del contratto stesso segue una logica leggermente diversa da quella aspettata e che si credeva di aver implementato. Particolare attenzione andrebbe posta ai dettagli nella gestione degli errori e delle eccezioni.

In generale, crediamo che sia doveroso prendere in considerazione tutti i possibili rischi legati all'utilizzo di nuove tecnologie all'interno di settori strategici come, ad esempio, quello finanziario. La non maturità del codice può potenzialmente sfociare in problematiche estremamente importanti che impattano con forza anche sulle risorse economiche dell'azienda stessa che l'ha adottate. È fondamentale valutare attentamente che una tecnologia di tipo Blockchain sia davvero quella più idonea a rispondere alle esigenze di business, in particolar modo, pesando i possibili benefici con i possibili rischi commisurati al bene da proteggere.

Garantire la qualità e la sicurezza del codice: l'infrastruttura

Inoltre, non va nemmeno sottovalutata l'importanza dei sistemi che ospitano i nodi. Vulnerabilità sui nodi potrebbero essere utilizzate per by-passare la sicurezza di una Blockchain, anche quando realizzata in modo opportuno. Per comprendere meglio questo concetto, si potrebbe pensare ad un caso eccezionale per cui avendo una Blockchain privata con limitata decentralizzazione, si riesca a prendere il controllo di più della metà dei nodi. In questo modo, sarebbe possibile alterare completamente la struttura della Blockchain stessa rimuovendo alcuni blocchi e introducendone altri.

Garantire la qualità e la sicurezza del codice: il backend

Negli ultimi anni si è registrata una diffusione della tecnologia Blockchain in diversi ambiti. La maggior parte dei progetti sono basati su software di tipo open-source, nel resto della sezione anche chiamati con l'acronimo *OSS* (Open Source Software).

Per questa ragione, alcune problematiche tipiche dell'OSS impattano potenzialmente anche le soluzioni Blockchain. In questa sezione viene posta particolare attenzione all'integrazione tra soluzioni aziendali e Blockchain basate su codice open-source. L'integrazione può diventare particolarmente critica quando entrambi devono rispondere a problematiche di business ben

definite.

Lo sviluppo del codice all'interno di progetti open-source è aperto a tutti, indipendentemente dalle abilità dei programmatori che intendono contribuire. Generalmente lo sviluppo è totalmente decentralizzato senza una distribuzione chiara delle responsabilità. Il risultato è che chiunque può fare qualunque cosa senza nessun ruolo chiave che orchestra l'intero progetto.

Idealmente tutto questo può permettere uno sviluppo più rapido per il semplice fatto che, in linea di principio, il numero di sviluppatori potrebbe essere di gran lunga maggiore rispetto a un progetto aziendale chiuso in cui le risorse sono limitate. Altro apparente vantaggio è che il tutto è a costo zero in considerazione del fatto che per questi tipi di progetti i contributi sono spesso su base volontaria.

C'è una certa convinzione comune che OSS sia generalmente più sicuro dei progetti chiusi perchè il codice sorgente continua ad essere indefinitamente a disposizione della comunità e quindi, teoricamente, revisionabile da un gran numero di persone. Si ritiene perciò che il processo di *bug fixing* sia assicurato. Per la legge dei grandi numeri sembrerebbe lecito ritenere in effetti che la qualità della revisione in termini di sicurezza possa essere molto alta in quanto svolta da più persone e fortemente preparate tra loro.

Nella realtà dei fatti la situazione risulta essere leggermente differente. Basti pensare alla lunga lista di errori di programmazione che hanno impattato sulla sicurezza dell'OSS molto tempo dopo il loro rilascio. Tanto per citare un incidente, relativamente recente, che ha generato effetti negativi su un gran numero di realtà è la vulnerabilità conosciuta come *Heartbleed* (Heartbleed, 2018). Bug di sicurezza della popolare libreria crittografica *OpenSSL* (OpenSSL, 2018), Heartbleed permetteva ad un attaccante di aggirare la protezione fornita dal protocollo *TLS/SSL* e di poter accedere ad informazioni potenzialmente confidenziali.

Considerando la grande diffusione della libreria OpenSSL, è sorprendente come una tale vulnerabilità sia rimasta inosservata per un lungo periodo forse anche di un paio di anni. Un altro caso, che a nostro avviso, vale la pena di richiamare è il più recente *Equifax* data breach. Questo incidente è dipeso ad una vulnerabilità del framework open-source (Apache Struts) utilizzato per realizzare il portale.

Questo è uno dei tanti esempi che dimostrano come progetti open-source non sono sinonimo di sicurezza. Le ragioni possono essere molteplici. La possibilità per chiunque di contribuire allo sviluppo di codice open-source è sicuramente un grosso vantaggio in termini di abbattimento dei costi. Questo però non garantisce in nessun modo che la qualità del software sia adeguata. Un possibile rischio è quello di avere nuovi pezzi di codice con un'alta frequenza ma che, anche se funzionanti, presentano importanti falle di sicurezza facilmente sfruttabili da un attaccante.

L'affidabilità di un software è legata all'expertise degli sviluppatori, alla loro dedizione e al livello dei test eseguiti prima del rilascio, oltre che alle regole e best practice volontariamente adottate. La preoccupazione principale durante lo sviluppo di un software è sovente legata al suo corretto funzionamento rispetto alle aspettative ed obiettivi perseguiti. L'approccio "security by design" non è ancora del tutto integrato nella cultura dello sviluppo software. I progetti su Blockchain basati su codice open-source non sono immuni a tutto questo, soprattutto considerando che vengono portati avanti senza alcun formale meccanismo di software assurance a garanzia dell'esecuzione di test e della gestione delle anomalie riscontrate.

L'idea che sotteso allo sviluppo di software per Blockchain open-source ci sia un processo di revisione del codice in termini di falle di sicurezza, a nostro avviso, non rispecchia la realtà. Inoltre, anche nel caso in cui la review venga davvero eseguita, non c'è nessuna garanzia che il livello di qualità sia adeguato. Valutare il codice in termini di sicurezza e possibili vulnerabilità richiede competenze specifiche che non sono poi così comuni, specialmente tra i programmatori. Il fatto che il numero di sviluppatori possa essere elevato può tradursi in un'alta frequenza di aggiornamento del codice da revisionare. Un ritmo estremamente elevato si traduce in un alto carico di lavoro per il *reviewer* che potrebbe diventare difficilmente sostenibile soprattutto se fatto in modo volontario e totalmente gratuito, come spesso viene erogato l'apporto ai progetti OSS.

In ragione del fatto che chiunque possa contribuire allo sviluppo del codice e che non sia previsto nessun processo di identificazione dello sviluppatore, non andrebbe trascurata la possibilità che all'interno dell'OSS sia inserito volontariamente del codice malevolo. Scelta che si rileverebbe strategica nel caso specifico in cui il software venga utilizzato all'interno di organizzazioni pubbliche o private. In tali casi diminuirebbe la possibilità di individuazione del codice malevolo minuziosamente progettato, da parte di revisori non particolarmente preparati e comunque da un processo di revisione non svolto ad opera d'arte. Alla luce di ciò una *best practice* potrebbe essere quella di fare un *assessment* del codice prima dell'integrazione e affiancare alla soluzione stessa un processo di *vulnerability management*.

Lo scenario descritto ha voluto prendere spunto dallo sviluppo tipico di un prodotto OSS, poiché facilmente osservabile da chiunque. Tuttavia, anche progetti di sviluppo centralizzati, gestiti da una azienda, consorzio o altra entità "garante e promotrice" del servizio potrebbero soffrire di tutti i problemi descritti se non venisse adottata la corretta politica di software assurance, con un solido processo di auditing e vulnerability management. Questi processi oggi sono troppo spesso trascurati nello sviluppo di prodotti ben più blasonati e storici, quindi il timore è che la bassa sensibilità verso il tema, se trascurata in fase di adozione di una tecnologia DLT possa trasformarsi in un incidente dall'alto impatto o in errore sistemico di difficile gestione in seguito.

Nell'implementare una soluzione basata su Blockchain non bisogna dimenticarsi dell'importanza di garantire un alto grado di sicurezza su tutti i sistemi informatici che, direttamente o indirettamente, sono coinvolti nella soluzione stessa. Una vulnerabilità su uno di questi sistemi potrebbe comunque permettere ad un attaccante di svolgere azioni malevole quali, ad esempio, il furto o alterazione della Blockchain stessa.

Nel mondo Blockchain, la prova della titolarità di un qualcosa è data dalla dimostrazione di essere a conoscenza di un segreto che, tecnicamente, si concretizza in una *chiave* privata. Generalmente questo segreto viene salvato in un *wallet*, che a sua volta viene protetto da una password. È fondamentale non sottovalutare la sicurezza dei wallet e la robustezza della password utilizzata. Sarebbe opportuno definire policy per la password e processi di vulnerability assessment e patch management anche sui wallet.

Garantire la qualità e la sicurezza del codice: il front end

Tutte le considerazioni del capitolo precedente valgono evidentemente per lo sviluppo di qualsiasi applicazione. Tuttavia, quando si affronta il tema "user interface", è opportuno fare qualche ulteriore rilievo.

Se il back-end è un contesto riservato a tecnici, a specialisti esperti, presumibilmente dotati di formazione, competenza ed esperienza adeguata, l'applicazione usata quotidianamente per gestire

le informazioni è utilizzata da diversi stakeholder, con competenze che nella quasi totalità dei casi non sono tecniche di dettaglio.

Per questa ragione la software assurance deve garantire non solo che il software sia il più possibile esente da errori, vizi, bug o vulnerabilità, ma che permetta anche all'utente di operare correttamente aiutandolo a gestire anche aspetti afferenti la sicurezza. Un'interfaccia utente efficace, infatti, permette non solo di minimizzare l'errore umano, che potrebbe compromettere la riservatezza, integrità o disponibilità del dato, ma anche di intercettare eventuali anomalie.

Si pensi all'evoluzione che hanno avuto i browser in questi anni nel segnalare all'utente la presenza della crittografia e la sua affidabilità: da un piccolo lucchetto in basso a destra, per molti utenti indistinguibile da un'icona sulla pagina, si è arrivati per successivi miglioramenti a colorare l'indirizzo del sito visitato. La stessa attenzione andrebbe posta nello sviluppo delle applicazioni di accesso al dato, tenendo conto anche del contesto più complesso da gestire, l'end-point e dell'integrazione con eventuali altre applicazioni.

L'end point, infatti è molto più esposto a minacce che possano compromettere la sicurezza del dato. Si pensi ad un malware che registri quel che avviene sullo schermo: vanificherebbe tutta la crittografia utilizzata per la comunicazione client-server.

Si considerino inoltre tutti i rischi, nello sviluppo e nell'uso, di funzionalità non sviluppate per essere utilizzate da un programma auto consistente, ma per essere integrate all'interno di una applicazione più completa già in uso (es. software per la gestione sinistri per una assicurazione che implementi gli Smart Contracts, gestione del magazzino per una azienda che implementi la tracciatura delle merci, etc). Assicurarsi che le funzionalità introdotte non portino con sé nuovi rischi o vulnerabilità è un must per qualsivoglia organizzazione che si appresti ad adottare questa tecnologia.

Garantire la qualità e la sicurezza del codice: gli Smart Contracts

Sarebbe buona norma, inoltre, separare il processo di assessment del codice della Blockchain da quello degli Smart Contract in ragione della loro diversità. A livello intuitivo, la Blockchain potrebbe essere immaginata come l'infrastruttura vera e propria su cui poi aggiungere lo specifico servizio da implementare che presumibilmente si concretizza con uno Smart Contract. Se da una parte, potenzialmente, una Blockchain può soffrire delle stesse vulnerabilità di una qualsiasi altra soluzione software, dall'altra l'aggiornamento del codice può risultare assai più complicato. Nel peggiore dei casi, variare in modo significativo una Blockchain (per esempio cambiando le regole utilizzare per il consenso) potrebbe portare ad un *hard fork*. In questo caso coesistono due differenti Blockchain per via della non compatibilità del nuovo codice con il vecchio.

Quando si pensa all'aggiornamento del codice bisogna anche tenere presente la natura decentralizzata della Blockchain stessa e la dislocazione spaziale dei nodi.

Anche per soluzioni basate su Blockchain continua ad essere valida la regola in base alla quale ogni volta che si aggiunge un nuovo componente al sistema, questo rappresenta potenzialmente un rischio. Per la Blockchain un nuovo componente significa, generalmente, uno Smart Contract. In questa ottica, è fondamentale soppesare ogni volta la vera necessità del componente con il rischio ad esso correlato.

Gli Smart Contract possono essere implementati in modo completamente indipendente dalla Blockchain e dai suoi nodi. Normalmente, una volta che uno Smart Contract viene invocato da una transazione, questo inizia la sua esecuzione automatica e non può più essere fermato. L'aggiornamento del codice e, quindi, il patch management inteso nella sua eccezione standard (come per il software tradizionale) non è applicabile agli Smart Contract.

Indipendentemente dalla specifica Blockchain, si potrebbero pensare a delle vie fantasiose ed alternative per aggiornare un contratto. In caso di Ethereum e Solidity, solo a titolo di esempio, si potrebbe pensare di creare un contratto che non fa altro che richiamare un altro contratto che rappresenta la versione più aggiornata dello Smart Contract vero e proprio.

Un'altra possibile alternativa potrebbe essere quella di affidare quanta più logica possibile a librerie esterne che possono essere facilmente aggiornate. Si registra comunque una tendenza a ricercare modalità per rendere gli Smart Contract aggiornabili. Una tecnica comune è quella di separare la logica e i dati in due contratti separati.

È importante però tenere presente che tutto questo rappresenta però una forzatura che in un certo senso è contraria all'idea stessa di Blockchain e Smart Contract. Questa dinamicità rischia di creare una serie di vulnerabilità che possono essere facilmente sfruttate da un attaccante.

Resta pacifico, tuttavia, che essendo gli Smart Contracts di fatto dei "programmi" possano essere affetti da errori di programmazione e la creazione di un processo teso a prevenirli, identificarli e correggerli sia indispensabile per qualsiasi organizzazione li voglia adottare. Ben consci della totale mancanza di esperienza del mercato nel debugging o nella code review di uno Smart Contract.

Garanzie a contorno del funzionamento del "codice" dello Smart Contract

I così detti *fail-safe,* per cui viene progettato un software in modo tale da limitare i danni in caso di malfunzionamento, non sono facilmente implementabili agli Smart Contract per via della loro natura immutabile. È possibile anche implementare Smart Contract in modo tale che la loro esecuzione possa essere alterata o terminata con una transazione ad hoc. Come precedentemente accennato, anche in questo caso bisogna comunque considerare il rischio correlato. Difatti questa funzionalità, se non opportunamente progettata, potrebbe essere sfruttata da un attaccante che altera la normale logica di esecuzione in modo da trarne beneficio.

Inoltre, gli Smart Contracts, per loro stessa natura, utilizzano spesso degli "oracoli", vale a dire delle fonti esterne da cui approvvigionarsi di informazioni utili all'automatismo codificato.

Selezionare con cura le fonti, valutarne correttamente l'autorevolezza e l'affidabilità sarà una nuova sfida da affrontare visto l'enorme numero di ambiti che uno Smart Contract potrebbe coprire in futuro.

Inoltre, plausibilmente senza avere il controllo dell'oracolo, sarà necessario assicurarsi della correttezza dell'informazione e dell'assenza di manipolazioni. Spesso gli oracoli potrebbero essere nella disponibilità della "parte avversa" vale a dire di stakeholder che hanno interessi opposti ai miei.

***Esempio**: Potrei avere uno Smart Contract che mi attiva l'assicurazione RC della moto quando la accendo e la disattiva quando la spengo, così da avere un pay-per-use. Potrei manomettere il dispositivo IoT che veicola le informazioni alla Blockchain, riprogrammando il sensore perché dica "motore acceso" solo quando la moto è a terra a seguito di un incidente. Questo mi permetterebbe di non pagare l'assicurazione ogni volta che uso la moto, ma di avere copertura in caso di incidente.*

Blockchain come opportunità per strumenti a supporto dell'information & cyber security

Le caratteristiche della Blockchain ne rendono interessante la sua adozione per supportare quei processi aziendali relativi alla cybersecurity in cui l'aspetto di conservazione dei dati è più critico. Infatti, le tecnologie basate su Blockchain forniscono nativamente integrità, immutabilità, consistenza, e disponibilità mediante una architettura distribuita.

Di seguito si riportano alcuni ambiti applicativi, sui quali la comunità dei vendor potrebbe a breve convogliare propri investimenti di ricerca e sviluppo.

Log Management

Un'importante applicazione della Blockchain riguarda la **gestione sicura dei log**, in particolare in contesti enterprise dove è cruciale la garanzia di immutabilità di tale tipologia di dati. Si pensi, ad esempio, ai log gestiti dalle società di telecomunicazioni che sono di potenziale interesse per indagini da parte della magistratura.

La caratteristica di immutabilità dei file di log garantita dalla Blockchain può essere sfruttata anche al servizio della **compliance alla direttiva NIS** (attuata in Italia a partire da Giugno 2018, nell'ambito servizi offerti da Operatori di Servizi Essenziali e da Fornitori di Servizi Digitali). In tale ambito, la Blockchain contribuisce a **supportare le esigenze di notifica in caso di incidente** richieste dalla Direttiva **grazie alle caratteristiche di integrità e notarizzazione**. Infatti, una delle azioni tipiche che si riscontrano nell'ambito di cyber-attacchi è quella della modifica dei file di log al fine di rimuovere le tracce dell'attacco.

L'utilizzo della Blockchain può rivelarsi una soluzione efficace per rendere sicura la memorizzazione dei file di log da due punti di vista: potrebbe supportare una **replicazione dei log su una infrastruttura distribuita** e permette di fornire una **evidenza della parzialità del dato in caso di manomissione**. Eventuali problemi legati alla confidenzialità possono essere affrontati introducendo tecniche di cifratura.

Si tenga presente nel disegno di una soluzione di Blockchain di quali siano i desiderata e di eventuali problemi strutturali, quale può essere la gestione di milioni di righe da inserire, con il relativo mastodontico effort computazionale ed i relativi tempi per il raggiungimento del consenso.

Se il progetto prevede la registrazione sicura di pochi log la cui integrità è strategica è pensabile inserire nella Blockchain direttamente il log.

Se lo scopo è, ad esempio, solo garantire l'integrità dei log di un datacenter, nella Blockchain potrebbe essere registrato esclusivamente l'hash dei log, con la frequenza voluta.

Identity and Access Management (IAM)

Un ulteriore ambito di applicazione della Blockchain nella gestione della cybersecurity è quello dell'**Identity and Access Management** (*IAM*). Mantenere le informazioni circa gli utenti e i loro diritti nell'ambito organizzativo è una attività critica dal punto di vista della sicurezza e che va protetta adeguatamente. In tale ambito, l'integrità è un aspetto fondamentale. Infatti, una manomissione di tali informazioni può potenzialmente mettere a rischio qualsiasi asset informatico dell'organizzazione.

Il sistema di protezione classico di tali informazioni è principalmente basato sul controllo di accesso. Integrare tali informazioni con una verifica di integrità crittografica è un valore aggiunto notevole perché rende impossibile una manomissione di tali informazioni che non lasci traccia.

Una soluzione basata su Blockchain, oltre ad avere questa caratteristica, fornisce nativamente replicazione e sincronizzazione dei dati su più server con una elevata disponibilità. Inoltre, normalmente variazioni di tali dati sono effettuate nell'ambito di un workflow che prevede richieste e autorizzazioni specifiche per ciascuna realtà aziendale. La corretta esecuzione di tali workflow è un punto critico su cui una manomissione può far leva per ottenere diritti di accesso addizionali.

Il concetto di Smart Contract, supportato da molte soluzioni, è di fatto un modo per eseguire del codice con gli stessi livelli di sicurezza che la Blockchain offre per transazioni più semplici. Per questo motivo tale strumento può essere utilizzato per realizzare con un livello di sicurezza elevato cambiamenti ai dati di IAM.

Resta da valutare, in ogni caso, il tema della riservatezza e della gestione a norma di legge di tali dati, in quanto personali.

Certification Authority

Strettamente legato alla IAM è quello della gestione dei certificati ed in particolare del loro stato. Infatti, l'emissione o la revoca di un certificato dovrebbe essere capillarmente diffusa con un alto livello di integrità.

Una soluzione basata su Blockchain fornisce nativamente integrità e distribuzione pressoché istantanea degli aggiornamenti. Questo permetterebbe di gestire informazioni che già le CA gestiscono abitualmente, in un'ottica "by design", senza integrare quindi diversi strumenti, integrandoli tra loro, ma avendo un repository che prevede molte delle necessarie feature a garanzia direttamente nel proprio core applicativo.

DNS

In qualche modo legata trasversalmente alla sicurezza di un gran numero di servizi è la gestione del Domain Name System (DNS). L'integrità e la disponibilità dei dati forniti da un DNS aziendale è importante per evitare disservizi o intrusioni. Sistemi basati su Blockchain forniscono tali caratteristiche nativamente. Inoltre, permettono di realizzare l'aggiornamento dei dati sulla base di

workflow realizzati tramite Smart Contracts con le stesse caratteristiche menzionate per gli aggiornamenti dei dati nello IAM.

Anche questo tema, spesso sottovalutato, troverebbe nello strumento Blockchain nuova vita, permettendo di gestire il problema con maggiore efficacia.

Tracciamento attività audit

Ulteriore attività legata alla cyberscurity per cui è importante l'integrità è il tracciamento e la memorizzazione delle attività di audit di sicurezza che vengono svolte a vari livelli sugli asset. Memorizzare in una Blockchain gli eventi legati all'esecuzione degli audit permette di avere una visione univoca e immutabile della storia di tali azioni e dei loro risultati. Questo permette di tracciare indietro nel tempo lo stato dell'auditing legato ai vari asset e fornire una documentazione crittograficamente certificata della bontà della gestione della cybersecurity.

Inutile dire che gli stessi ragionamenti valgono per tutte le attività di audit, anche non strettamente legate alla cybersecurity.

Autori e licenza d’uso

In rappresentanza di Clusit e dell’Osservatorio Blockchain del Politecnico di Milano, hanno partecipato a questo lavoro le seguenti persone:

Luca Bechelli, *Comitato Scientifico Clusit*

Mauro Bellini, *Digital360, Giornalista*

Piero Bologna, *Partners4Innovation, Legal Consultant*

Andrea Caccia, *UNINFO, Presidente UNI/CT 532 Blockchain & DLT*

Fabio Cappelli, *EY*

Anna Cataleta, *Partners4Innovation, Senior Legal Advisor*

Sossio Di Fiore*, EY*

Gabriele Faggioli, *Clusit, Presidente*

Roberto Garavagli, *Management Consultant & Innovative Payments Strategy Advisor*

Federico Griscioli, *Partners4Innovation*

Dominick Leiweke, *Consulting & Development Strategies*

Enrico Micillo, *EY*

Alessio Pennasilico, *Associazione Informatici Professionisti, Presidente*

Maurizio Pizzonia, *Università degli Studi Roma Tre, Ricercatore universitario e docente di cybersecurity*

Valeria Portale, *Osservatorio Blockchain, Direttrice*

Andrea Reghelin, *Partners4Innovation, Associate Partner*

Guido Sandonà, *Bulgari, Consigliere Direttivo Clusit*

Sofia Scozzari, *Clusit, Comitato Scientifico*

Gabriele Tori, *Partners4Innovation, Legal Consultant*

Alessandro Vallega*, Consigliere Direttivo Clusit*

Questo lavoro è concesso con la licenza Creative Common Attribuzione - Non commerciale - Condividi allo stesso modo 3.0 Italia (**CC BY-NC-SA 3.0 IT**)