Alessandro Ghiani

Blockchain: linee guida

Dai casi pratici alla regolamentazione

Con prefazione di Gianluca Duretto

Giappichelli

Prefazione

Ho il piacere di fare questa breve prefazione al libro dell'Avvocato Alessandro Ghiani, collega di studi della tecnologia blockchain e delle sue reali applicazioni di business. Questa importante tecnologia che negli ultimi cinque anni, con la sua più importante e diffusa applicazione, il re delle criptovalute, Bitcoin è uno dei termini ancora più ricercati su internet ed argomento ancora dibattuto e di moda. La diffusione mediatica ed una informazione molto riduttiva e poco attenta a quello che è la tecnologia, fino ad ora ha sempre nascosto, in un alone di mistero, il reale valore che è dietro alla blockchain, racchiuso in un nuovo concetto di "trust" o fiducia tra attori di un ecosistema decentralizzato.

L'avv. Ghiani affronta alcuni argomenti fondamentali della tecnologia blockchain, con un'analisi approfondita ed entusiastica da chi ne ha capito le reali potenzialità nella quotidianità ancora più che nella teoria dei primi entusiasti sostenitori delle criptovalute.

La trattazione dei campi di applicazione dove da questa tecnologia maggiormente si hanno vantaggi passa dalla filiera agroalimentare, che riesce a ridurre l'impatto negativo delle frodi alimentari, una delle più pesanti piaghe del settore, fino alla votazione elettronica in blockchain che mantenendo l'anonimato del votante, riesce a ridurre in modo assoluto pericoli di brogli elettorali anche migliorando la fiducia per la popolazione che potrebbe dare un sistema completamente trasparente sicuro ed inattaccabile di voto.

L'approfondimento di questioni, più specifiche della pratica

forense come la gestione dei contenziosi trova in un capitolo apposito insieme al punto della giurisprudenza attualmente in essere, una valida conclusione a questo lavoro.

Consiglio a tutti di leggere questo libro dove blockchain, criptovalute e la sua massima espressione Bitcoin sono trattate mai in modo banale e sempre con una vista al di la del futuro, quando tutto questo sarà di uso quotidiano.

Dott. Gianluca Duretto
Professore a contratto
Pagamenti elettronici, criptovalute e blockchain

Introduzione

"*Il problema non è mai la tecnologia, ma l'uso che se ne fa*"

Ciò che tutti sappiamo è che la tecnologia cambia la vita degli uomini, le loro abitudini, le loro aspettative. Ciò che spesso ignoriamo è che l'utilizzo della stessa tecnologia rispetta delle precise norme che rendono il progresso complementare ai principi che regolamentano le società civili, quindi soggetto al diritto delle comunità moderne.

È la tecnologia che deve adeguarsi al diritto oppure il diritto che deve tenere il passo frenetico della tecnologia?

Probabilmente questa domanda non ha una risposta univoca ma molteplici risposte.

Di per sé, invocando il principio della neutralità della tecnologia, secondo il quale essa si presenta inerte se non suscettibile di impulso da parte dell'uomo, nel momento in cui, però, inizia ad operare è necessario che lo faccia nel pieno rispetto delle norme.

Non sempre però le norme vigenti riescono ad assolvere al compito di disciplinarne gli utilizzi soprattutto quando il diritto è costretto ad esaminare nuovi fenomeni, a volte completamente inediti, al fine di generare tutele e garanzie adeguate. Solo lo studio e la promulgazione di nuove norme a presidio di altrettanto nuove fattispecie potranno garantire una adeguata cornice entro la quale operare.

La comprensione della tecnologia è essenziale per la costruzione delle norme ad essa sottese soprattutto in un contesto, quale quello attuale, in cui le fattispecie innovative generate dal-

la tecnologia risultano essere spesso già tangibili e di comune utilizzo.

Questa premessa vale per tutte quelle tecnologie emergenti che stanno prendendo forma in tanti aspetti della vita comune.

Studi economici e scientifici sostengono che nei prossimi cinque anni si attuerà un cambiamento tecnologico che neppure negli ultimi cinquanta anni si è verificato.

Tra le tecnologie che stanno trainando questa evoluzione esponenziale si annoverano l'AI (Artificial Intelligence), l'IoT (Internet of Things) e la blockchain.

La naturale interoperabilità di queste tre tecnologie cambierà radicalmente le abitudini di ciascuno di noi.

Sono stati già pubblicati diversi testi riguardanti blockchain e criptovalute che affrontano il tema a volte in modo particolarmente tecnicistico o relegandolo ad aspetti estremamente specifici e di settore come ad esempio, solo per menzionarne uno, l'analisi degli aspetti finanziari e speculativi che ruotano intorno a bitcoin.

Questo volume, nella sua stesura, semplice ed immediatamente comprensibile, ambisce a costruire un naturale collegamento tra tutti quei professionisti che vogliono trasformare la propria curiosità in approfondimento, senza però scoraggiarsi difronte ad un argomento nuovo e che impegna molti ambiti differenti.

Le nozioni tecniche poste alla base di questo compendio sono piuttosto intuitive e descritte, nella maggior parte dei casi, nell'ottica di un ipotetico lettore (che chiameremo confidenzialmente "Marco") il quale risulta essere il destinatario/usufruitore di tutte quelle applicazioni innovative collegate all'impiego della tecnologia blockchain.

I fenomeni descritti sono arricchiti da una ricorrente analisi dal taglio principalmente giuridico che evidenzia caso per caso le principali norme ad esso sottese.

Contrariamente alle proposte dei testi classici, partendo quindi dall'esperienza di Marco, si cercherà di sussumere gli elementi principali della regolamentazione dei fenomeni tecnologici legati all'uso della blockchain e del suo prodotto forse migliore, gli smart contract.

Si tratteranno quindi temi legati a bitcoin, conti correnti bancari e portafogli digitali, criptovalute, finanza decentralizzata, contratti ad esecuzione automatica, valorizzazione delle filiere, arte, identità digitale e molto altro.

Il filo conduttore della lettura sarà sorretto dai principi su cui si fondano tutte le applicazioni che utilizzano il protocollo blockchain: disintermediazione, trasparenza, decentralizzazione.

Buona lettura

1
I principi alla base della tecnologia blockchain

Come abbiamo già precisato, la prerogativa di questo testo non è certo quella di offrire una visione particolarmente tecnica del funzionamento delle blockchain ma renderne comprensibile l'operatività attraverso le sue principali applicazioni. Tale analisi non può però prescindere dalla focalizzazione dei principi che ispirano l'utilizzo di detto protocollo e che costituiscono un significativo cambio di paradigma culturale all'interno delle società moderne.

Concetti come disintermediazione e decentralizzazione ricorrono in ogni aspetto dell'impiego dei registri distribuiti ed in particolar modo delle blockchain che ne costituiscono di fatto una evoluta sottospecie. Per comprendere meglio il funzionamento di una blockchain immaginiamo che il nostro ipotetico lettore Marco, appassionato di cinema d'essai, si stia godendo la visione di "Tempi moderni", la famosissima pellicola del 1936 che ritrae un grande Charlie Chaplin alle prese con una catena di montaggio sulla quale, attraverso un rullo trasportatore, scorrono delle scatole. Ciascuno dei personaggi lungo la catena si adopera, orizzontalmente e senza gerarchia, per la realizzazione del risultato finale.

Trasponiamo ora il concetto in un ambito digitale.

Immaginiamo che quelle scatole siano blocchi di dati.

Immaginiamo che al completamento del blocco, i partecipanti alla catena, i cosiddetti nodi validatori, si adoperino per chiudere la scatola, ossia il blocco, e immediatamente dopo ripetano l'operazione sul blocco successivo.

Ogni volta che quel blocco di dati verrà chiuso, e solo in

quel preciso istante, il nostro buon Charlie Chaplin scatterà una fotografia del contenuto della scatola, cioè del blocco, creando un'impronta della stessa. Questa operazione viene identificata nelle funzioni di HASH e di Time Stamp le quali costituiranno l'incipit di dati del blocco successivo. Tale impronta di dati, come per tutti i blocchi precedenti, verrà racchiusa nel blocco seguente.

Questa attività permette, come nella antesignana catena di montaggio Chapliniana, di effettuare la concatenazione dei blocchi di dati attraverso una sequenza immodificabile. Il registro che contiene la trascrizione di tutte queste operazioni viene replicato, ipoteticamente all'infinito, tra tutti i partecipanti rendendo totalmente distribuito il data base.

La descrizione può apparire parzialmente complessa ma ciò che dobbiamo tenere a mente ora è che attraverso questo processo, che avviene in automatico, i dati replicati su questi registri distribuiti diventano incorruttibili generando un affidabile ecosistema di fiducia tra i partecipanti o i soggetti ad esso collegati attraverso le applicazioni che lo incorporano. Non esiste più un proprietario centralizzato del data base. Tutti i partecipanti sono proprietari dello stesso data base replicato. Per poter corrompere il data base distribuito diventa necessario un attacco al sistema che corrompa almeno il 51% dei data base andando a ritroso tra i blocchi ormai chiusi fino al dato da modificare. Tale operazione è attualmente impossibile a causa della impossibilità di generare una potenza di calcolo adeguata per poter inquinare il sistema. Inoltre tale sistema si sostiene concettualmente attraverso la generazione di incentivi per i partecipanti validatori, generati in criptovaluta, che rendono inclini questi ultimi a promuovere il sistema piuttosto che a sabotarlo.

La rivoluzione che introduce la blockchain è quindi insita nel concetto di disintermediazione.

I processi che abbiamo descritto, attraverso l'espediente visivo della pellicola cinematografica a cui Marco è particolarmente legato, ci mostrano come il sistema, secondo il funzionamento proposto, si sorregga senza la necessità che i partecipanti siano obbligati a fidarsi di un "*deus ex machina"*, di una

figura centrale che convalidi il loro affidamento, in buona sostanza di un comune intermediario.

Nell'utilizzo di protocolli blockchain, prendendo come esempio le più note transazioni di bitcoin in cui due soggetti possono scambiare velocemente ed in modo sicuro del valore digitale, non è mai necessario l'intervento di un intermediario che convalidi la transazione. Sarà il sistema stesso, attraverso la sua decentralizzazione ed i nodi validatori partecipanti a convalidare le transazioni in modo indipendente e verificabile, cristallizzandole ed attribuendo loro certezza assoluta.

C'è di più.

Abbiamo quindi individuato immediatamente il plusvalore che si ottiene nell'utilizzare un ecosistema rivoluzionario in cui ogni singola transazione o annotazione di dato su registri distribuiti diventa incorruttibile e certa.

Ma la domanda che a questo punto circola nella mente del nostro lettore Marco è la seguente: "Chi controlla queste transazioni?"

La risposta è: "Tutti!"

Infatti, ulteriore peculiarità dei sistemi basati su un protocollo blockchain di tipo pubblico e senza restrizioni all'accesso (definiti "permissionless") è la possibilità per chiunque di verificare l'avvenuta transazione attraverso una piattaforma definita "block explorer" cioè esploratrice proprio di quei blocchi di cui abbiamo precedentemente parlato. L'interrogazione del block explorer ci restituirà una traccia univoca della transazione recante la verifica della stessa.

Abbiamo compreso alcuni dei principi ispiratori della tecnologia blockchain e questo breve approfondimento ci permetterà di migliorare la percezione di quanto verrà proposto ed esaminato nelle successive pagine del testo.

Ma a chi dobbiamo l'intuizione e quindi la teorizzazione di questa architettura così differente dai sistemi tradizionali che tutti fino ad ora abbiamo conosciuto?

Il nome che risponde alla nostra domanda è Satoshi Nakamoto.

Chi è costui?

Prima di rispondere però facciamo un piccolo salto indietro al 2008, anno in cui è avvenuto il crollo della Lehman Brothers, la più grande Banca d'affari degli Stati Uniti e forse del mondo finanziario di allora.

"Troppo grande per fallire", si diceva in quegli anni, riferendosi proprio all'Istituto di Credito messo in crisi dall'insolvenza dei cosiddetti mutui "subprime", eppure, in quegli anni, l'imponderabile improvvisamente avvenne lasciando migliaia di persone senza più la certezza di potersi fidare di un soggetto istituzionalmente credibile, la banca, nel quale avevano riposto la propria assoluta fiducia .

Torniamo ora al citato Satoshi Nakamoto.

Il desiderio di costruire sistemi alternativi di fiducia ha spinto questo soggetto, di cui ancora oggi è ignota l'identità, celata dietro uno pseudonimo, a pubblicare un documento definito "whitepaper" o libro bianco in cui si teorizza un inedito sistema alternativo di pagamenti digitali attraverso l'utilizzo di bitcoin e della sua blockchain.

Che sia opera di un unico soggetto o di una comunità di sviluppatori, giuristi, visionari, il whitepaper di bitcoin apre la strada ad una visione del mondo disintermediata e legata a rapporti alla pari definiti appunto "peer to peer" o meglio ancora orizzontali, che sostengono un sistema che elimina del tutto il concetto di fiducia incarnata da un terzo riponendo invece la stessa nel sistema tecnologico.

Una autentica rivoluzione che nel corso degli anni ha portato queste concettualità ad una evoluzione che ha visto la sua applicazione in moltissimi ambiti che si spingono ben oltre bitcoin.

Alcune di esse le esamineremo nel proseguimento del testo, in una modalità principalmente votata alla concretezza e tangibilità delle soluzioni esaminate oltre che con un particolare occhio di riguardo più specifico per gli smart contract ed il proficuo connubio tra essi e la blockchain.

2
Glossario ragionato

Questo capitolo offrirà al lettore un elenco di definizioni ragionate, legate a fattispecie di matrice perlopiù tecnologica, utili a comprendere più agevolmente i concetti successivamente contenuti all'interno del testo.

Avere maggiormente chiara e sempre a portata di mano una descrizione del fenomeno tecnologico permette di maneggiarlo con più padronanza nell'esaminare le dinamiche giuridiche che si ingenerano nel momento in cui esso necessita o già impegna un contesto normativo di riferimento.

Ecco di seguito alcune definizioni:

Distributed ledger technology DLT

Si tratta di sistemi basati su un registro distribuito, ossia sistemi in cui tutti i nodi (computer) di una rete possiedono una copia identica di un database replicato che può essere letto e modificato in modo indipendente dai singoli nodi.

Blockchain

La blockchain, sottofamiglia delle DLT, è una catena di blocchi di dati condivisa e "immutabile" tra tutti i nodi partecipanti. È individuabile come un registro digitale le cui voci sono raggruppate in "blocchi", concatenati in ordine cronologico, in cui ogni blocco successivo contiene l'impronta del blocco di dati precedente. La sua integrità è garantita dall'uso della crittografia. Il suo contenuto una volta scritto non è più né modificabile né eliminabile, a meno di non invalidare l'intera struttura.

Blocchi

Sono costituiti dal raggruppamento di un insieme di transazioni unite per essere verificate, approvate e poi archiviate dai nodi partecipanti alla blockchain.

Transazioni

È l'insieme delle informazioni trascritte in un blocco a cui viene attribuita "data certa" e certezza dell'integrità del contenuto. Attestano, ad esempio, in modo immutabile il passaggio di valore da un soggetto ad un altro all'interno della blockchain di bitcoin.

Blockchain Permissioned

È una tipologia di blockchain il cui accesso è riservato a partecipanti autorizzati. Ad esempio una blockchain in cui sono custoditi importanti dati particolari o di dominio non pubblico (es. cartelle cliniche).

Blockchain Permissionless

Contrariamente alla precedente, si tratta di una blockchain il cui accesso è totalmente privo di limitazioni. Chiunque abbia intenzione di mettere al suo servizio la propria capacità computazionale di calcolo (un PC) può parteciparvi divenendo un nodo della stessa. L'esempio principe è la blockchain di bitcoin.

Peer to peer

In inglese, peer to peer, spesso abbreviato come p2p, significa "*tra pari*" e descrive un tipo di rete di comunicazione in cui ciascun nodo comunica direttamente con gli altri, senza passare attraverso la mediazione di un server centrale.

Decentralizzazione

Secondo questo principio, alla base delle architetture blockchain, le informazioni (i dati in genere) vengono trascritte non su un singolo ma su molteplici registri. Esse vengono così distribuite tra più nodi al fine di garantire sicurezza informatica, resistenza alla censura, resilienza dei sistemi.

Disintermediazione

Le piattaforme basate su sistemi blockchain consentono di gestire le transazioni senza intermediari, ossia senza la presenza di enti centrali ritenuti fidati e qualificati.

Algoritmo di consenso

Possiamo definire un algoritmo di consenso come il meccanismo attraverso cui un insieme di nodi blockchain, che non si conosce e non necessita di fidarsi l'uno dell'altro, raggiunge il consenso per validare una transazione.

Crittografia

La crittografia asimmetrica è un sistema di codifica della sicurezza informatica, chiamato anche "a chiave pubblica e privata" utilizzato nell'ambito della sicurezza informatica per codificare e decodificare i messaggi.

Criptovaluta

Il vocabolo criptovaluta o criptomoneta è l'italianizzazione del termine inglese cryptocurrency e si riferisce ad una rappresentazione digitale di valore basata sulla crittografia.

Bitcoin

È una criptovaluta e un sistema di pagamento valutario internazionale creato nel 2009 da un anonimo inventore (o gruppo di inventori), noto con lo pseudonimo di Satoshi Nakamoto.

Exchange

L'exchange di criptovalute è una particolare piattaforma su web, creata appositamente per poter scambiare tra loro criptovalute differenti ma anche di poter convertire in criptovalute altre valute a corso legale e forzoso (Dollaro, Euro etc.) e viceversa.

De.Fi.

La Finanza Decentralizzata (comunemente denominata anche Decentralized Finance – De.Fi.) è una forma sperimentale

di sistema finanziario che non si basa su intermediari finanziari centrali come broker, exchange o banche ed utilizza invece smart contract posizionati sulla blockchain [1].

Smart contract

Si definisce "smart contract" un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse [2].

Algoritmo

Un *algoritmo è* un ragionamento logico che serve per risolvere un problema ed è costituito da una sequenza finita di operazioni (dette anche istruzioni).

IoT

L'IoT (Internet of Things) è una rete di dispositivi connessi che possono comunicare tra loro e fornire dati agli utenti tramite Internet. I dispositivi IoT possono collegarsi a Internet e spesso dispongono di sensori che gli permettono di raccogliere dati. Collegati ad una blockchain attraverso gli smart contract assolvono la funzione di oracolo.

Oracolo

Gli oracoli blockchain sono servizi di terze parti che forniscono informazioni esterne a smart contract. Fungono da ponti tra le blockchain e il mondo esterno.

---

[1] Definizione di De.Fi. largamente condivisa tratta dal sito wikipedia.com.

[2] Definizione di Smart Contract tratta dal testo dell'art. 8-ter d.l. n. 135/2018).