LUISS

DIPARTIMENTO DI IMPRESA E MANAGEMENT

Corso di laurea in *Economia e Management*

Cattedra di *Statistica applicata ed Econometria*

Blockchain: Innovazione Digitale nelle Operazioni Finanziarie

Relatore

Luigi Laura

Candidata

Giuseppe Ceroni

Matr. 474041

Anno Accademico 2023/20

Introduzione 3

1.La tecnologia blockchain e le sue declinazioni 7

1.1 Origini ed evoluzione 7

1.2 Tipologia di blockchain e funzionamento 11

1.3 Vantaggi e svantaggi della blockchain 12

2. Il Ruolo della Normativa Italiana nella Gestione dei Rischi della Blockchain 16

2.1 Cenni riguardo il quadro normativo comunitario e nazionale 16

2.2 Profili giuridici della Blockchain 19

2.3 L'intervento del legislatore italiano 22

3. Nuovi orizzonti normativi 25

3.1 Le sfide per la sicurezza e la privacy 25

3.2 Verifica delle identità digitali 28

3.3 La gestione dei diritti digitali 32

4.Blockchain e le sue implicazioni economiche e finanziarie 35

4.1 Smart contracts 35

4.2 Blockchain per il settore finanziario 37

4.3 Strategie delle banche centrali 40

Bibliografia 43

Introduzione

Negli ultimi anni, l'evoluzione tecnologica ha apportato significativi cambiamenti in molti settori, con effetti profondi sull'economia globale. In questo scenario, la blockchain si è affermata come una delle innovazioni più promettenti, capace di rivoluzionare le operazioni finanziarie e numerosi altri ambiti. Nata per supportare le criptovalute, la blockchain ha rapidamente ampliato il suo campo di applicazione, diventando una tecnologia fondamentale per la gestione di dati e transazioni in modo sicuro, trasparente e decentralizzato.

La blockchain può essere descritta come un registro distribuito e immutabile, dove le informazioni sono archiviate in "blocchi" collegati tra loro in una catena sequenziale. Questo sistema garantisce la sicurezza delle transazioni attraverso tecniche di crittografia avanzata e un meccanismo di consenso decentralizzato, riducendo la dipendenza da intermediari tradizionali come banche o autorità centrali. A differenza dei modelli finanziari convenzionali, la blockchain non richiede la fiducia in un singolo ente o soggetto, ma si basa su una rete distribuita di nodi che convalidano e registrano le transazioni, rendendo il processo più democratico e potenzialmente meno costoso.

L'innovazione portata dalla blockchain ha avuto un impatto dirompente soprattutto nel settore finanziario. Grazie a questa tecnologia, è stato possibile sviluppare nuove forme di pagamento digitale, come il Bitcoin, che ha rappresentato la prima applicazione pratica della blockchain. Il successo del Bitcoin ha dimostrato come una moneta digitale, basata su una rete decentralizzata, potesse funzionare senza l'intervento di banche centrali o enti di regolamentazione tradizionali. Tuttavia, la blockchain non si limita alla creazione di valute digitali. Oggi, essa viene utilizzata per creare contratti intelligenti (smart contracts), gestire identità digitali e proteggere i diritti di proprietà intellettuale tramite tecnologie come il Digital Rights Management (DRM).

Le origini di questa tecnologia risalgono a molto prima del 2008. Una delle prime forme primitive di un sistema simile alla blockchain è stato osservato sull’isola di Yap, in Micronesia, dove un registro pubblico distribuito veniva utilizzato per tracciare la proprietà di enormi pietre denominate "Rai", utilizzate come moneta. Questo modello di scambio, basato su registri pubblici e condivisi,

ha anticipato in modo sorprendente i principi fondamentali della blockchain odierna, dimostrando l'importanza della trasparenza e della condivisione delle informazioni nelle transazioni.

Il settore bancario e finanziario ha visto nella blockchain un'opportunità per ottimizzare processi complessi e migliorare l'efficienza delle transazioni. Grazie alla sua natura decentralizzata, la blockchain offre soluzioni innovative per la gestione delle transazioni internazionali, spesso caratterizzate da tempi lunghi e costi elevati. L'utilizzo della blockchain potrebbe ridurre significativamente queste inefficienze, permettendo la liquidazione immediata delle transazioni e la gestione automatica dei pagamenti tra istituzioni finanziarie. Oltre ai vantaggi operativi, la tecnologia blockchain offre anche un alto livello di sicurezza grazie all'immutabilità dei dati registrati e all'utilizzo di tecniche crittografiche avanzate che proteggono le informazioni da manipolazioni e attacchi informatici.

Nonostante i vantaggi evidenti, l'adozione della blockchain nel settore finanziario e in altri settori non è priva di sfide. Uno degli aspetti più controversi riguarda l'elevato consumo energetico delle reti blockchain basate sul Proof of Work (PoW), un meccanismo di consenso che richiede una grande potenza di calcolo per validare le transazioni. Questo ha portato a preoccupazioni riguardanti l'impatto ambientale della blockchain, spingendo molte aziende e organizzazioni a cercare alternative più sostenibili, come il Proof of Stake (PoS), che riduce significativamente il consumo di energia.

Inoltre, le questioni legate alla privacy e alla sicurezza dei dati sollevano preoccupazioni significative. La blockchain è intrinsecamente trasparente: ogni transazione è visibile a tutti i partecipanti della rete, il che può rappresentare un rischio per la protezione delle informazioni sensibili. Sebbene le transazioni sulla blockchain siano eseguite tramite pseudonimi, questo livello di anonimato potrebbe non essere sufficiente a garantire una totale protezione della privacy degli utenti. A questo proposito, alcune soluzioni avanzate, come la crittografia omomorfa e le zero-knowledge proofs, stanno emergendo come potenziali strumenti per rafforzare la privacy pur mantenendo l'integrità delle transazioni.

Oltre alle problematiche tecniche, la diffusione della blockchain incontra ostacoli di natura normativa e giuridica. A livello globale, i governi e le istituzioni finanziarie stanno cercando di trovare un equilibrio tra la promozione dell'innovazione e la necessità di regolamentare un settore che presenta rischi per la sicurezza e la stabilità economica. In Europa, il Regolamento MiCA (Markets in Crypto-Assets), recentemente adottato, rappresenta un tentativo significativo di creare un quadro normativo armonizzato per le cripto-attività e le tecnologie basate su registri distribuiti.

Anche in Italia, l'adozione della blockchain è stata accompagnata da interventi normativi specifici, come il Decreto Fintech, che ha introdotto misure urgenti relative all'emissione e alla circolazione di strumenti finanziari in forma digitale.

L'obiettivo di questa tesi è fornire un'analisi approfondita della blockchain e delle sue implicazioni per il settore finanziario, esplorando sia le opportunità che le sfide che essa presenta. Verranno analizzate le diverse tipologie di blockchain, il loro funzionamento e le possibili applicazioni in ambito economico e finanziario. Inoltre, verrà esaminato il quadro normativo che regola l'adozione di questa tecnologia, con particolare attenzione al ruolo delle istituzioni italiane ed europee nella gestione dei rischi e nella promozione di un uso responsabile e sicuro della blockchain.

Infine, la tesi si soffermerà sui nuovi orizzonti aperti dalla blockchain, che spaziano dalla gestione delle identità digitali alla protezione dei diritti digitali, fino alla creazione di modelli di business decentralizzati. Concludendo, sarà analizzato il potenziale impatto della blockchain sull'economia globale, tenendo conto delle previsioni più recenti, secondo cui entro il 2025 una significativa porzione del PIL mondiale potrebbe derivare da attività legate alla blockchain.

1.La tecnologia blockchain e le sue declinazioni

1.1 Origini ed evoluzione

Le origini storiche di un sistema di scambio simile alla blockchain attuale vengono fatto risalire ad una piccola isola dell'arcipelago Micronesia, intorno al 500 d.C., in particolare sull'isola di Yap[1]; dove si sviluppò, con il tempo, un sistema di pagamento che presentava molte affinità con i moderni sistemi di criptovalute.

A quei tempi, infatti, gli scambi venivano portati a termine attraverso l'utilizzo di una pietra denominata "Rai"; questa pietra, che risultava essere una vera e propria moneta, era costituita da un disco circolare di roccia calcarea e poteva raggiungere pesi e dimensioni notevoli; le più grandi arrivano ad una altezza di 13 piedi ed a un peso massimo di 4 tonnellate; la peculiarità della roccia calcarea con cui erano costruite queste monete risiedeva nel fatto che il tempo e l'erosione aveva consentito ad altri minerali di infiltrarsi e risultava quindi impossibile contraffare questo tipo di pietra, rendendolo quindi il sistema di pagamento ideale.

A causa del suo peso e della derivante difficoltà che si riscontrava nello spostamento, si andò incontro ad un'innovazione che avrebbe modificato completamente il modo di eseguire scambi in tutto il mondo; si sviluppò, infatti, un sistema basato su dei registri pubblici e distribuiti.

Ogni proprietario di una pietra Rai aveva, infatti, una copia del registro che riportava i diversi cambi di proprietà che caratterizzavano la moneta, perciò, quando veniva eseguita una transazione, tutti i possessori del registro dovevano aggiornarlo scrivendoci il nome del nuovo proprietario.

Con questo metodo vennero quindi eliminati tutti i problemi relativi a furti e transazioni non autorizzate.

In Micronesia, duemilacinquecento anni fa, venivano quindi eseguiti scambi non attraverso il possedimento fisico della pietra ma, attraverso la negoziazione dei diritti di proprietà relativi alle pietre stesse.

Questo sistema era reso possibile dal fatto che ogni transazione eseguita veniva annunciata pubblicamente alla popolazione, che decideva se validarla o meno.

---

[1] Si veda*:" Il primo Bitcoin? È nato nel 1400 in Micronesia*".
Disponibile a: https://www.financialounge.com/news/2017/11/13/primo-bitcoin-micronesia/

La differenza principale tra i metodi di pagamento contemporanei e postumi ed il Rai si va a rintracciare nel fatto che nell'isola di Yap non risultava esserci un sistema centralizzato ed un autorità centrale con il compito di controllare gli scambi e le transazioni sull'isola, poiché questo sistema era basato sulla premessa fondamentale che l'informazione della transazione veniva posta a conoscenza di tutta la popolazione e veniva testimoniata dalla presenza del nome del nuovo possessore della pietra sui registri detenuti dagli abitanti dell'isola.
La presenza di questi registri garantiva l'assenza del problema della doppia spesa, in quanto attestavano che, una volta completata una transazione, questa non poteva essere ripetuta.
Questo meccanismo veniva inoltre sostenuto dal fatto che tutti i possessori del registro potevano verificare che la transazione fosse già avvenuta.
Questo sistema aiutava inoltre a capire anticipatamente se una transazione sarebbe andata a buon fine oppure no poiché si poteva dedurre se chi stesse cedendo il diritto di proprietà sulla pietra ne avesse effettivamente il diritto.
Un ulteriore sicurezza apportata da questo nuovo sistema di scambio si rintracciava nel fatto che se si fosse voluto eseguire una transazione fraudolenta sarebbe stato necessario alterare tutti i registri presenti sull'isola e convincere tutte le persone aventi un registro della validità dell'operazione; ciò evitava quindi la manipolazione delle transazioni e la conseguente acquisizione illecita dei beni.
Questo sistema, introdotto sull'isola di Yap intorno al 500 d.C., basato sulla presenza dei registri con la prova scritta dei diritti di proprietà sul bene, è stato utilizzato per secoli avvenire dalle istituzioni bancarie e finanziarie per le validazioni di scambio di moneta o beni ed è stato la base di partenza per il processo tecnologico evolutivo che ha portato all'introduzione della blockchain.
Il sistema di pagamento nell'isola di Yap è un esempio che ci fa capire in modo semplice ed efficacie i processi che si trovano alla base del meccanismo di funzionamento della blockchain.
Possiamo però rintracciare, in tempi più recenti, la vera introduzione e sviluppo di questa tecnologia.
Un primo esempio significativo in tempi moderni dell'introduzione della blockchain è il protocollo BitTorrent, uno dei primi sistemi peer-to-peer (ovvero un tipo di rete di comunicazione in cui ciascun nodo comunica direttamente con gli altri, senza la mediazione di un server) per la condivisione dei file; questo tipo di sistema può essere visto come un precursore della blockchain. Con BitTorrent, ogni partecipante della rete possedeva una copia frammentata del file, suddiviso in parti e condivisa con gli utenti.

La svolta di questa tecnologia, però, è arrivata nel 2008 con la creazione del Bitcoin, una criptovaluta che ha rivoluzionato il sistema finanziario globale.

Il Bitcoin fu portato a conoscenza del grande pubblico quando una persona, nota con lo pseudonimo di Satoshi Nakamoto, pubblica su internet un articolo titolato:" Bitcoin: un sistema di moneta elettronica peer-to-peer[2]"; questa pubblicazione poneva le basi per la creazione e la diffusione del sistema di pagamento "trustless" basato su blockchain ancora ad oggi più utilizzato ed importante al mondo.

La spinta che portò Satoshi Nakamoto a creare questo innovativo sistema di valuta virtuale fu la crescente sfiducia verso le banche e le istituzioni finanziarie centralizzate e la volontà di dar vita un sistema di scambio di risorse libero, pubblico e senza alcuna interferenza da organizzazioni statali. Il processo di innovazione digitale dei sistemi di validazione delle transazioni è stato poi fortemente accentuato dalla crisi economica dei mutui subprime e del debito sovrano con conseguente sfiducia degli investitori nel sistema bancario tradizionale e crescente forte sviluppo di questa nuova tecnologia.

Il Bitcoin opera grazie ad una serie di blocchi di informazioni, che contengono dettagli sulle transazioni e sono collegati tra loro formando una catena. Questa struttura viene appunto definita "Blockchain". La tecnologia si fonda su una rete di computer che condividono un registro digitale distribuito, nel quale viene conservata una copia di tutte le transazioni eseguite sulla rete. Questo meccanismo garantisce un livello di sicurezza estremamente elevato e rende molto difficile la manipolazione: per alterare una transazione, infatti, un attaccante dovrebbe modificarla su tutti i computer della rete, che possono essere migliaia o addirittura milioni. Questa fase della blockchain appena descritta può essere definita come: la "*prima generazione*".

Dopo 7 anni dall'invenzione del Bitcoin e dalla crescente popolarità del sistema basato sulla blockchain, nel 2015 si entrò nella cosiddetta "*seconda generazione*".

Questa innovazione fu introdotta dalla creazione della blockchain basata sulla criptovaluta Ethereum, che risultava essere la prima blockchain programmabile; l'introduzione di questa nuova valuta digitale ha fatto in modo che tale tecnologia potesse essere utilizzata per molte nuove applicazioni.

Con l'innovazione di Ethereum è stato anche introdotto il concetto di "*Smart contract*" il quale ha premesso ai programmatori di tutto il mondo di creare applicazioni decentralizzate su blockchain.

---

[2] Si veda*:" Bitcoin: un sistema di moneta elettronica peer-to-peer".*
Disponibile a: https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf

L'ultimo atto nel processo evolutivo della blockchain è stato raggiunto recentemente ed ha a che fare con il processo di validazione delle transazioni; questo processo è sempre stato essenziale per qualsiasi blockchain in quanto consente di garantire che ogni transazione sia eseguita correttamente e non vi sia alcun problema derivate da frode o dalla doppia spesa.

Agli inizi, per la validazione delle transazioni, veniva adoperato un sistema di consenso chiamato Proof of Work (Pow)[3], con il quale i "minatori" sfruttavano le capacità di calcolo del proprio computer per risolvere problemi matematici complessi ed aggiungere un nuovo blocco alla catena.

In particolare, il funzionamento del Proof of Work si articola in 3 fasi principali: come prima operazione gli utenti vendono o acquistano criptovaluta ed i dati di queste transazioni vengono uniti insieme in un blocco; in seguito i minatori di criptovalute competono per essere i primi a risolvere un complesso problema matematico riuscendo, una volta battuti i competitors, ad avere il diritto di elaborare il blocco di transazioni; come step finale viene scelto casualmente un nuovo miner che si aggiudica il diritto di aggiungere un nuovo blocco alla catena (blockchain) e per questa sua azione quest'ultimo verrà ricompensato con una quantità variabile di criptovaluta.

Questo sistema risulta essere ancora ad oggi il meccanismo di validazione delle transazioni più adoperato al mondo in particolare viene utilizzato sulle blockchain di Bitcoin e Dogecoin.

Tuttavia, tale sistema, ha manifestato diverse criticità legate, soprattutto, all'elevata richiesta di energia necessaria per la validazione di ogni transazione dovuta allo sfruttamento della potenza computazionale dei computer; ciò ha determinato un crescente allarme in relazione al grande impatto ambientale che questa tecnologia comportava. Con il tempo, pertanto, sono stati sviluppati sistemi di validazione alternativi al PoW, tra cui il principale: il Proof of Stake (PoS)[4].

Il Proof of Stake è il meccanismo per il quale vengono scelti dei partecipanti alla blockchain per la convalida delle transazioni e l'aggiunta di nuovi blocchi.

Con questo sistema non veniva più utilizzata la potenza computazionale del computer ma, la validazione delle transazioni fu affidata ai "validatori".

Questi validatori vengono selezionati casualmente per validare le transazioni e vengono ricompensati per il loro contributo.

---

[3] Si veda:" *Proof of work: cos'è e come funziona*" (2023) Disponibile a: https://www.forbes.com/advisor/it/investire/criptovalute/proof-of-work-significato/

[4] Si veda: "*Proof of Stake: cos'è e come funziona*" (2024). Disponibile a: https://www.forbes.com/advisor/it/investire/criptovalute/proof-of-stake-significato/

Questo processo sta ottenendo un grande successo nel mondo delle criptovalute tanto che Ethereum, la seconda moneta virtuale per capitalizzazione di mercato dopo Bitcoin, sta eseguendo la transizione dal Proof of Work al Proof of Stake.
Questo metodo di validazione delle transazioni risulta essere molto più efficiente, richiedendo molta meno energia rispetto al sistema del Proof of Work, riducendo quindi sensibilmente l'impatto ambientale.

1.2 Tipologia di blockchain e funzionamento

La blockchain nasce come una tecnologia pubblica, disponibile a tutti e, soprattutto, aperta; con il fine di poterla migliorare e di creare una partecipazione attiva all'interno di essa.
Successivamente al grande sviluppo che questa tecnologia ottenne, molte aziende e governi cominciarono ad interessarsi alla blockchain con il fine di poterla utilizzare nei loro progetti aziendali futuri o adoperarla per snellire apparati burocratici lenti e macchinosi.
Proprio da questa differenza di scopo tra aziende, governi e comunità aperte si andarono a creare tre tipi principali di blockchain: le blockchain pubbliche o permissionless, le blockchain private e le blockchain ibride.

- La blockchain pubblica o permissionless: è stata la prima tipologia di blockchain sviluppata e si riferisce ad una tecnologia in cui chiunque può accedere liberamente. Tutti possono quindi leggere e validare le transazioni e si viene premiati per aver utilizzato la propria potenza di calcolo per la convalida di un blocco. Per raggiungere questi obiettivi, in blockchain pubbliche, devono essere presente numerose misure di sicurezza che vanno a garantire che nessun malintenzionato possa facilmente manometterne il funzionamento.
- La blockchain privata: caratterizzata da un amministratore che regola l'accesso a nuovi membri che vorrebbero partecipare alla blockchain; questo sistema potrebbe ricordare il modello centralizzato bancario ed in parte risulterebbe essere vero se non fosse per il fatto che questa tipologia di blockchain garantirebbe una maggiore efficienza ed uno snellimento dell'apparato burocratico garantendo anche un miglior scambio di dati tra le parti. Questa tipologia di blockchain è quella che negli ultimi anni ha avuto maggiore applicabilità a livello societario ma anche in enti governativi ed istituzioni finanziarie. Diverse società hanno infatti iniziato ad

introdurre la blockchain nel loro ecosistema organizzativo, tra le quali troviamo IBM e Ernst & Young.

- Le blockchain ibride: risulta essere un misto tra la tipologia di blockchain privata e quella pubblica in quanto non vi è un singolo amministratore che gestisce l'intero sistema (come in quella privata) bensì sono presenti più "nodi" autorizzati che controllano e verificano tutte le transazioni.

Il funzionamento di questa tecnologia si basa sulla combinazione tra la firma digitale e la marca temporale che garantiscono che la transazione monetaria siano identificate in modo sicuro ed univoco. Questo sistema ha come fondamento la presenza di un registro pubblico e condiviso, di un libro, in cui sono presenti tutte le transazioni e si aggiorna nello stesso momento e su tutti i nodi che partecipano alla rete. Tutte le operazioni presenti da singoli nodi sono autenticate e confermate attraverso una tipologia di crittografia definita a chiave asimmetrica, questo meccanismo di crittografia garantisce l'identità digitale di chi ha autorizzato gli scambi.
La caratteristica principale di questo sistema risiede nel fatto che la validazione delle transazioni ed il suo funzionamento non è garantito da un ente centrale, bensì la veridicità delle transazioni viene controllata da tutte le persone presenti nella catena. Infine, la registrazione di tutte le operazioni in un registro condiviso permette di conservare, in una bacheca dati consultabile pubblicamente, tutti i dati relativi alla transazione come, per esempio, gli ammontari o le date di esecuzione delle transazioni.[5]

1.3 Vantaggi e svantaggi della blockchain

Nei paragrafi precedenti abbiamo parlato della blockchain in generale, ripercorrendo sia lo sviluppo che questa tecnologia ha avuto nel tempo ma anche le sue diverse tipologie che negli anni sono state sviluppate. Adesso ci soffermeremo sugli svantaggi ma, soprattutto, sui vantaggi che questa nuova tecnologia comporta.
Tra gli svantaggi principali della blockchain annoveriamo: "

- *il basso livello remunerativo, soprattutto su blockchain che utilizzano il sistema di consenso del Proof of Work in quanto, come detto nei paragrafi precedenti, con questo sistema di consenso, coloro che validano le transazioni hanno un*

[5] Si veda*:" Blockchain: cos'è e come funziona*"
Disponibile a: https://www.borsaitaliana.it/notizie/sotto-la-lente/blockchain.htm

altissimo dispendio energetico quindi, elevati costi, a fronte di pochi ricavi che vengono distribuiti solo a colui che ha completato la validazione per primo, rendendo quindi nullo il lavoro che altri stavano compiendo per la validazione dello stesso blocco.

- *Gli attacchi 51%: sono il tipo principale di attacco informatico che può essere eseguito contro le reti blockchain. Un attacco di questo genere può verificarsi su una rete se un'entità riuscisse a controllare più del 50% della potenza di hashing della rete ("uno dei termini più usati nel mondo del mining di criptovaluta è hash rate o tasso di hash. Questo termine si riferisce al valore numerico all'interno di ogni criptovaluta che utilizzi l'estensione Proof of Work (PoW). Il valore indica la quantità d'operazioni computazionali che un miner o la rete di miner sono in grado di eseguire complessivamente. Tutto questo al fine di risolvere gli enigmi crittografici derivati dalla funzione crittografica utilizzata dalla criptovaluta[6]"), questo consentirebbe eventualmente di interrompere la rete escludendo o modificando intenzionalmente l'ordine delle transazioni. Nella teoria questo sarebbe uno dei più se non il più grande svantaggio che questa tecnologia comporta se non fosse che, in pratica, non c'è mai stato un attacco del 51% riuscito alla blockchain Bitcoin; infatti, a mano a mano che la rete diventa più grande risulta sempre più difficile portare a termine con successo un attacco del 51% sulla rete.*
- *Modifica dei dati: altro svantaggio dei sistemi blockchain risiede nel fatto che una volta che un operatore inserisce dei dati, questi risulteranno essere difficilmente modificabili. La modifica dei dati, infatti, sulle blockchain risulta essere molto difficoltosa e dispendiosa in quanto comporterebbe l'abbandonamento di un'intera catena per intraprenderne una nuova, eliminando quindi i dati presenti in quella messa da parte.*
- *Crittografia: la blockchain utilizza il sistema crittografico definito "a chiave pubblica o asimmetrica"; sistema nel quale ad ogni attore coinvolto nel sistema è associata una coppia di chiavi, una risulta essere pubblica e quindi disponibile a tutti, mentre l'altra privata quindi personale e segreta. Questo sistema, infine, si basa su due assunzioni principali ovvero che la chiave privata non può essere*

[6] Si veda*:" Che cos'è l'Hash Rate?", 2020*
Disponibile a: https://academy.bit2me.com/it/qual-è-il-tasso-di-hash/

in alcun modo ricavabile da quella pubblica e che se con una delle due chiavi si dovesse cifrare un messaggio allora quest'ultimo potrà essere decifrato solo dalla chiave corrispondente. Lo svantaggio principale di questa tecnologia risiede nel fatto che se un utente dovesse perdere la propria chiave privata, allora il proprietario non riuscirebbe più ad accedere al fondo corrispondente perdendo quindi tutto ciò che si trovava al suo interno.

- *Inefficienza del sistema: in particolare le blockchain che utilizzano come meccanismo di validazione delle transazioni il Proof of Work sono le meno efficienti; questa conclusione deriva dal meccanismo di funzionamento di questo sistema in quanto risulta essere altamente competitivo e ogni volta che viene completato un blocco, solo un "miner" viene ricompensato, sprecando di fatto tutto il lavoro degli altri che avevano provato a validare il blocco. Questo meccanismo ha portato alla creazione di un ambiente molto competitivo, dove si cerca di aumentare in ogni modo la potenza computazionale del proprio computer, portando quindi ad un aumento, non sostenibile, del consumo di elettricità. Nonostante gli svantaggi, questa tecnologia presenta dei vantaggi unici che porteranno la blockchain ad essere utilizzata globalmente e tra i tanti annoveriamo:*
- *Condivisione dei dati: i dati presenti sulla blockchain sono archiviati in migliaia di dispositivi, questo fa in modo che la rete sia estremamente resistente verso guasti tecnici o cyber attacchi, in quanto ogni nodo della catena è in grado di archiviare una copia del database, quindi anche se un nodo dovesse essere attaccato ed andare offline non influenzerebbe la disponibilità e la sicurezza della rete; al contrario dei database convenzionali dove un guasto tecnico o un cyber attacco influenzerebbe l'intero sistema, portando a conseguenze potenzialmente catastrofiche.*
- *Inalterabilità: una volta che un blocco viene confermato è molto improbabile che quest'ultimo venga annullato, rendendola così un'ottima tecnologia per archiviare documenti finanziari o qualsiasi altro dato per cui è richiesta la firma digitale in quanto ogni traccia viene archiviata, in modo definitivo, su di un registro pubblico, consultabile da tutti quanti.*
- *Sistema "trustless": ad oggi siamo abituati che per la validazione delle transazioni ci si deve affidare alle due parti coinvolte o al massimo ad un intermediario, come una banca o una società di fornitura di servizi di pagamento,*

con questa tecnologia ciò non sarà più necessario in quanto è la rete stessa a verificare le transazioni attraverso un sistema chiamato mining; proprio per questo motivo la blockchain è un sistema che viene definito "trustless". Un sistema basato su questa tecnologia, quindi, non annulla solamente il rischio di fidarsi di una singola società o organizzazione ma ha come altro vantaggio la riduzione dei costi complessivi e le commissioni di transazione eliminando quindi intermediari e terze parti."[7]

[7] Si veda *"Vantaggi e svantaggi della blockchain"* (2018).
Disponibile a: https://www.binance.com/it/square/post/42837

2. Il Ruolo della Normativa Italiana nella Gestione dei Rischi della Blockchain

2.1 Cenni riguardo il quadro normativo comunitario e nazionale

Promuovere l'adozione delle tecnologie digitali è stata, negli ultimi anni, una priorità sia al livello europeo sia per il governo italiano e, più in generale, per tutti gli stati membri dell'Unione.

L'UE, allo scopo di scongiurare una frammentazione giuridica e normativa dei singoli stati per la blockchain, ha fermamente sostenuto l'introduzione di una normativa comune avanzando proposte legislative atte a tale scopo specie nell'ambito delle cripto-attività al fine di aumentare gli investimenti e garantire la protezione dei consumatori e degli investitori.

In tale ottica è stato di recente emanato il Regolamento (UE) 2023/1114 relativo ai mercati delle cripto-attività ("MiCA" – Markets in Crypto-Assets).

Tale Regolamento rappresenta un significativo passo in avanti nel contribuire a ridurre l'incertezza normativa e dare ordine al mercato delle cripto-attività.

L'Unione Europea, infatti, con il MiCA, interviene con l'obiettivo dichiarato di creare un quadro normativo solido e armonizzato nel campo delle cripto-attività, e persegue lo scopo non limitandosi a riconoscere il potenziale delle tecnologie blockchain e del registro distribuito (DLT), ma rispondendo anche alla necessità di affrontare le sfide legate alla sicurezza, alla tutela dei consumatori e alla stabilità dei mercati finanziari. In effetti, l'intervento attuato è indirizzato a promuovere un ecosistema digitale che spera di essere innovativo e competitivo, regola al contempo l'uso di cripto-attività in modo responsabile e sostenibile, e sostiene lo sviluppo di nuovi modelli di business legati alla tecnologia a registro distribuito (DLT) e della blockchain il cui potenziale, per sviluppare nuovi modelli di business e attività economiche, è ampiamente riconosciuto.

In effetti, le cripto-attività rappresentano una delle principali applicazioni della tecnologia a registro distribuito (DLT); si tratta di rappresentazioni digitali di valore o diritti che hanno il potenziale di offrire vantaggi significativi ai partecipanti al mercato, compresi i detentori al dettaglio. L'evidenza dimostra come le cripto-attività stesse possono semplificare i processi di raccolta di capitali e rafforzare la concorrenza, offrendo un approccio innovativo e

inclusivo al finanziamento, particolarmente utile per le piccole e medie imprese (PMI) e, quando utilizzate come mezzo di pagamento, possono rendere i pagamenti più economici, veloci ed efficienti, specialmente su base transfrontaliera, riducendo la necessità di intermediari.

Come detto, l'obiettivo (del MiCA) è creare un contesto normativo che non solo stimoli l'innovazione, ma che porti anche benefici concreti a tutti i cittadini europei, migliorando l'accesso alle nuove opportunità e contribuendo al progresso economico e tecnologico dell'Unione; in sintesi, il regolamento MiCA si propone di bilanciare l'innovazione tecnologica con la protezione degli investitori e la stabilità finanziaria, creando un quadro normativo che faciliti lo sviluppo e la competitività del settore delle cripto-attività in Europa.

Prima del regolamento MiCA, infatti, il quadro normativo europeo risultava piuttosto frammentato. Alcune cripto-attività, in particolare quelle classificabili come strumenti finanziari ai sensi della direttiva 2014/65/UE del Parlamento Europeo e del Consiglio, erano già soggette alla normativa dell'Unione in materia di servizi finanziari.

Per queste cripto-attività, esisteva già una regolamentazione completa che copriva sia gli emittenti che le imprese coinvolte, garantendo così un contesto regolatorio solido e chiaro.

Tuttavia, molte cripto-attività non rientravano nel campo di applicazione della legislazione europea sui servizi finanziari, come previsto dalla Direttiva 2014/65/UE (MiFID II) e dal Regolamento (UE) n. 600/2014 (MiFIR).

Fatta eccezione per le normative antiriciclaggio, in particolare la Direttiva (UE) 2015/849 (AMLD), non esistevano regole specifiche per i servizi legati a queste cripto-attività non regolamentate**.** Ciò comportava una mancanza di disciplina su aspetti cruciali**,** come il funzionamento delle piattaforme di negoziazione (non coperte da MiFID II), lo scambio di cripto-attività con valuta fiat o altre cripto-attività, e la custodia e amministrazione delle cripto-attività per conto dei clienti.

L'assenza di un quadro normativo in questi settori esponeva i possessori di cripto-attività a rischi considerevoli, soprattutto in ambiti non coperti dalle norme sulla tutela dei consumatori, come stabilito dalla Direttiva 2011/83/UE sui diritti dei consumatori.

Inoltre, tale mancanza di regolamentazione generava rischi significativi per l'integrità del mercato, tra cui abusi di mercato (Regolamento (UE) n. 596/2014) e crimini finanziari.

Per far fronte a questi rischi, alcuni Stati membri avevano adottato regolamentazioni specifiche per le cripto-attività non coperte dalla legislazione UE sui servizi finanziari**,** mentre altri hanno legiferato autonomamente in questo settore. L'assenza di un quadro normativo unificato a livello dell'Unione minava la fiducia degli utenti nelle cripto-attività**,** rappresentando un ostacolo significativo allo sviluppo di un mercato unico per queste tecnologie.

Questo vuoto normativo comportava la perdita di opportunità legate a servizi digitali innovativi, strumenti di pagamento alternativi e nuove fonti di finanziamento per le imprese nell'UE.
Le aziende che utilizzavano cripto-attività non godevano di certezza giuridica riguardo al loro trattamento nei diversi Stati membri, frenando i loro sforzi di innovazione digitale**.**
Peraltro, questa mancanza di un quadro normativo comune, se si fosse protratta troppo a lungo, avrebbe certamente condotto ad una frammentazione delle regolamentazioni nazionali, falsando la concorrenza nel mercato unico e rendendo difficile l'espansione transfrontaliera dei prestatori di servizi legati alle cripto-attività, favorendo l'arbitraggio normativo.
Ora sebbene i mercati delle cripto-attività siano ancora relativamente piccoli e non rappresentino attualmente una minaccia per la stabilità finanziaria, esiste la possibilità che in futuro i consumatori adottino su larga scala cripto-attività che mirano a stabilizzare il loro valore rispetto a specifiche attività o panieri di attività e, naturalmente un tale sviluppo potrebbe comportare ulteriori sfide in termini di stabilità finanziaria, regolare funzionamento dei sistemi di pagamento, trasmissione della politica monetaria e sovranità monetaria, come già discusso nei contesti del Sistema europeo di banche centrali (SEBC) e della Banca centrale europea (BCE).
Il regolamento dell'Unione Europea per i mercati delle cripto-attività si è posto la realizzazione di diversi obiettivi chiave, in risposta alle sfide e alle opportunità presentate da questo settore emergente.
In primo luogo, il quadro normativo chiaro e armonizzato ha sostenuto l'innovazione e promosso la concorrenza leale**,** permettendo ai prestatori di servizi per le cripto-attività di operare su base transfrontaliera e facilitando l'espansione e la crescita del mercato senza barriere normative eccessive. Per quanto riguarda la protezione degli investitori e la stabilità dei mercati, poi, il regolamento introduce misure specifiche che garantiscono un elevato livello di tutela per i detentori al dettaglio e preservano l'integrità dei mercati delle cripto-attività, inclusi requisiti di trasparenza e di informativa per prevenire frodi e malpratiche.
La normativa, inoltre, cerca di facilitare l'accesso ai servizi bancari per i prestatori di servizi per le cripto-attività**,** promuovendo una maggiore integrazione tra i servizi finanziari tradizionali e quelli basati su cripto-attività, e permettendo alle imprese di operare più agevolmente in tutto il mercato unico europeo.
Il regolamento cerca, altresì, di evitare di imporre oneri regolamentari eccessivi**,** garantendo che le normative non penalizzino le imprese e mantenendo la competitività del mercato europeo a livello globale, senza compromettere l'innovazione e la crescita del settore delle cripto-attività.

Sul punto sono chiamate in causa l'Autorità Europea degli Strumenti Finanziari e dei Mercati (ESMA) e l'Autorità Bancaria Europea (EBA) ovvero i regolatori europei dei mercati finanziari, per elaborare norme tecniche dettagliate relative all'informativa ambientale e ai principali indicatori energetici, definendo metodologie e presentazioni necessarie per garantire chiarezza e coerenza nelle informazioni sugli impatti ambientali delle cripto-attività.
Come detto anche il legislatore nazionale, nell'ambito dell'evoluzione della tecnologia Blockchain e della crescente esigenza di definire schemi normativi in grado di disciplinarne l'applicazione, ha sentito l'esigenza di dettare una regolamentazione volta ad introdurre una definizione legale di blockchain e smart contract.
Ciò è avvenuto con il D.L. 135/2018 convertito con modificazioni dalla L. 11.02.2019 n. 12 (G.U. 12.02.2019 n.39) che sarà oggetto di compiuta analisi nel successivo paragrafo 2.3.
Va, inoltre, segnalata l'emissione, in data 18.03.2023, del D.L. n.25 del 17.03.2023 (c.d. Decreto Fintech) convertito con modificazioni dalla L. n.52 del 2023 in materia di emissione e circolazione di strumenti finanziari in forma digitale (Digital Securities).
Detto decreto attua il Regolamento UE, 2022/858 (DLT Pilote Regime) e, come vedremo, contribuisce a creare un contesto più favorevole per lo sviluppo delle tecnologie emergenti come la blockchain.

2.2 Profili giuridici della Blockchain

L'esame delle relazioni che intercorrono tra blockchain e diritto deve, necessariamente, prendere le mosse dall'analisi del contesto normativo di riferimento con particolate *focus* su alcuni aspetti significativi di questa tecnologia, che sollevano questioni nell'interazione con normative preesistenti, in particolare quelle relative alla protezione dei dati.
Per comprendere il rapporto tra diritto e blockchain, è necessaria una premessa: come in altri ambiti tecnologici, il diritto deve dialogare con altri sistemi di regole, in particolare la "*lex informatica*" o "*digitalis*", ossia le norme che governano il mondo informatico.
Il codice giuridico deve quindi interagire con quello algoritmico per essere efficace.
Le regole informatiche influenzano i comportamenti umani, poiché abilitano azioni, collegano effetti e determinano quali informazioni fornire.
La "*lex informatica*" ha il potere di condizionare qualsiasi forma di regolamentazione, compresa quella giuridica. Di conseguenza, il diritto deve intervenire sulla tecnologia, affinché ciò che è

giuridicamente lecito sia parte del possibile tecnologico, rispettando i principi dell'ordinamento e tutelando i diritti. In alcuni casi, il diritto può sfruttare la stessa tecnologia per disabilitare azioni illecite.

Nel rapporto tra blockchain e diritto, il giurista deve trovare un equilibrio: la tecnologia non deve prevalere sul diritto, ma allo stesso tempo il diritto non deve limitare le potenzialità della tecnologia. Un'eccessiva limitazione rischierebbe di rendere il diritto inefficace.

L'analisi giuridica della blockchain deve necessariamente partire dalla comprensione della tecnologia stessa, poiché proprio nelle sue caratteristiche emergono potenziali criticità per il diritto.

Le tecnologie basate su registri distribuiti (DLT) e la blockchain, come loro specifica declinazione, si distinguono per disintermediazione, decentralizzazione, immodificabilità dei dati, meccanismi di consenso alternativi, trasparenza e sicurezza, programmabilità, solidità nonché l'uso di funzioni di hash e crittografia asimmetrica.

Queste caratteristiche variano a seconda del tipo di blockchain: *permissionless*, aperte a tutti (come Bitcoin), *permissioned*, accessibili solo con autorizzazione, o ibride, dove un gruppo selezionato di nodi ha un ruolo maggiore nel consenso. Partendo da questi requisiti e principi, la blockchain è divenuta la declinazione in digitale di un nuovo concetto di "fiducia" al punto che alcuni ritengono che la blockchain possa assumere anche un valore per certi aspetti "sociale e politico". In questo caso la blockchain può essere inquadrata come una piattaforma che consente lo sviluppo e la concretizzazione di una nuova forma di rapporti sociali, che grazie alla partecipazione di tutti è in grado di garantire a tutti la possibilità di verificare, di controllare e di disporre di una totale trasparenza sugli atti e sulle decisioni, che vengono registrate in archivi che, come detto, hanno la caratteristica di essere inalterabili, immodificabili e, dunque, immuni da correzioni.

Queste caratteristiche, unitamente a quelle sopra richiamate, possono essere così sintetizzate:

- decentralizzazione delle informazioni: tutti i dati sono distribuiti tra i nodi così da garantire una maggiore sicurezza del sistema;
- tracciabilità degli elementi: ogni dato salvato nel registro è tracciabile in quanto si può risalire da ogni transazione a tutte le informazioni come tra provenienza e le modifiche subite;
- trasparenza: le informazioni contenute nel registro sono visibili a tutti i nodi della rete;

- solidità: il registro è regolato da un meccanismo di consensi. Questo comporta che nessun dato possa essere nascosto o alterato senza che gli altri partecipanti ne vengano a conoscenza;
- disintermediazione: il meccanismo della validazione delle informazioni attraverso il consenso di tutti i nodi della rete, rende superfluo ogni tipo di intermediazione volta alla certificazione delle informazioni stesse;
- programmabilità: la tecnologia blockchain consente di programmare le transazioni e cioè rende possibile il loro inserimento/modifica al verificarsi di determinate condizioni.

Passando dagli aspetti tecnologici a quelli giuridici, le caratteristiche della blockchain emergono anche negli atti normativi europei e nazionali. A livello europeo, rileva la risoluzione del Parlamento europeo del 3 ottobre 2018, che evidenzia come queste tecnologie possano migliorare l'efficienza e la trasparenza delle transazioni, pur ammettendo che i rischi non siano ancora del tutto noti. In Italia, l'art. 8-ter del decreto-legge 135/2018 definisce le DLT e gli smart contract, specificando che la memorizzazione di documenti attraverso DLT ha effetti giuridici simili alla validazione temporale elettronica.

Uno dei principali problemi legati all'uso della blockchain riguarda la protezione dei dati personali, regolata dal GDPR e dalla normativa italiana.

La blockchain, con la sua immodificabilità e la replica dei dati, si scontra con alcuni principi fondamentali della protezione dei dati, come la minimizzazione e la limitazione della conservazione. Inoltre, la difficoltà nell'individuare i responsabili del trattamento dei dati nelle blockchain *permissionless* pone ulteriori problemi.

Il rapporto tra blockchain e diritto presenta sfide complesse, soprattutto in relazione agli smart contract e alla protezione dei dati personali. È necessario un maggiore coordinamento tra le normative nazionali ed europee, così come un approccio proattivo che incorpori i principi giuridici nelle tecnologie stesse.

La blockchain offre opportunità, ma deve essere accompagnata da una regolamentazione giuridica adeguata per esprimere appieno il suo potenziale.

2.3 L'intervento del legislatore italiano

Come detto al precedente punto 2.1, il legislatore italiano, al pari di quello comunitario, si è dimostrato molto sensibile rispetto al crescente utilizzo delle tecnologie digitali dando vita ad interventi governativi dedicati al finanziamento di start-up innovative (digitali) e alla promozione e supporto economico dell'intelligenza artificiale come mezzo per adeguare ed aggiornare le pratiche di business.

In questo contesto, la blockchain in generale, e nello specifico la sua applicazione nel campo delle criptovalute, è stata al centro degli ultimi sforzi del governo per promuovere l'innovazione.

L'evoluzione della normativa su blockchain e criptovalute avvenuta negli ultimi anni ha trovato la propria consacrazione nel già richiamato Decreto-legge n.135 del 2018 con il quale, come detto, è stata introdotta una definizione legale di blockchain e smart contract.

In particolare, all'art. 8 *ter*, comma 1, del citato D.L., le tecnologie basate su registri distribuiti ("*distributed ledger"* - DLT) sono state definite come quelle tecnologie: *"che fanno uso di un libro mastro condiviso, distribuito, replicabile, accessibile simultaneamente, con un'architettura decentralizzata basata sulla* crittografia *tale da consentire la registrazione, validazione, aggiornamento, memorizzazione di dati verificabili da ciascun partecipante, non alterabile e non modificabile."*

Il Decreto-legge n. 135 del 2019, all'art. 8 *ter*, comma 2, fornisce anche una definizione di "smart contract" come *"un programma per elaboratore che opera su tecnologie basate sui registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dall'entrata in vigore della legge di conversione del presente decreto".*

In sostanza, sulla base della riferita definizione, uno smart contract non è un contratto ma un programma per elaboratore; è cioè una sequenza di istruzioni rivolte ad una macchina, evidentemente scritte in un codice da questa eseguibile.

Non è questa la sede per un esame critico della citata normativa e delle problematiche che la stessa pone sotto un profilo giuridico trattandosi, comunque, di un primo importante passo del legislatore italiano volto a dare una disciplina univoca ad una materia la cui crescente

applicazione e costante evoluzione richiederà, in ogni caso, non pochi ulteriori interventi normativi sia correttivi che di adeguamento alle nuove tecnologie.
L'ordinamento giuridico italiano non include, a differenza di quanto visto in relazione alla blockchain e agli smart contract, una definizione generale di criptovalute.
Questo ha portato ad un acceso dibattito sul poter considerare o meno le stesse criptovalute come valuta o come beni dal punto di vista legale.

Questa non è solo una questione teorica, in quanto avrebbe un effetto immediato su una serie di livelli, compreso il fatto che le criptovalute siano o meno mezzi di pagamento adeguati.
Dopo non poche incertezze, il consenso maggioritario si è orientato sul ritenere le criptovalute soggette allo stesso regime giuridico delle valute che non hanno corso legale in Italia, ad esempio valute superate, come la Lira italiana, che è stata sostituita dall'Euro, e valute di un altro paese.
In base a questa teoria, se un pagamento contrattuale è stipulato in una criptovaluta, mentre il creditore non ha diritto al pagamento in una valuta diversa da quella contrattualmente pattuita, il debitore può effettuare il pagamento anche nella valuta avente corso legale al tasso di cambio della data di scadenza dell'obbligazione di pagamento.
Per quanto riguarda la natura giuridica delle criptovalute, che, come detto, non godono di una specifica definizione normativa, i tribunali italiani non si sono sempre allineati con la maggioranza degli interpreti.

La Corte di Cassazione ha considerato, ad esempio, la vendita online di Bitcoin come la promozione di strumenti finanziari, mentre il Tribunale di Firenze ha etichettato alcune criptovalute, che erano tenute in deposito presso un e-wallet e exchange outfit poi divenuto insolvente, come "beni fungibili" (Tribunale di Firenze, sentenza n. 18 del 2019).
Da segnalare anche una sentenza del Tribunale di Brescia del 2018 (decreto n. 7556 del 18 luglio 2018) con la quale sono stati chiariti i requisiti che le criptovalute devono possedere per poter essere versate come capitale sociale di una Società a Responsabilità Limitata (in senso lato, l'equivalente italiano di una società a responsabilità limitata). Infatti, la Corte ha confermato che le criptovalute sono ammissibili per essere versate come capitale sociale a condizione che il loro valore sia determinabile, tipicamente come determinato in scambi ampiamente utilizzati.
Per quanto riguarda la determinazione della natura giuridica delle criptovalute, la sentenza del Tribunale di Brescia non ha fatto ulteriore luce, in quanto si è limitata a ricordare che per la legge italiana, sia i beni che i servizi, oltre al contante, possono essere versati come capitale sociale.

Benché, come detto, l'ordinamento italiano non preveda una definizione generale di criptovalute, una definizione statutaria di "valute virtuali" ai fini antiriciclaggio è stata inserita nel decreto legislativo n. 90 del 2017, che ha recepito in Italia la quarta direttiva antiriciclaggio, come segue:
"[Una] rappresentazione digitale di valore, che non è stata emessa o sostenuta da una banca centrale o da un'autorità pubblica e che non è necessariamente ancorata a una valuta legale, ma che è utilizzata come mezzo di scambio per l'acquisto di beni o servizi o a fini di investimento, e può essere trasferita, memorizzata o negoziata elettronicamente."
L'obiettivo dello statuto che include la definizione è stato quello di catturare la più ampia gamma possibile di beni digitali per evitare che siano utilizzati per il riciclaggio di denaro e per facilitare il terrorismo.

Il regolatore bancario e l'organo di vigilanza finanziaria, Consob, hanno evidenziato i rischi, rispettivamente per il sistema bancario e per gli investitori italiani, di affidarsi a tecnologie e beni di investimento ancora non regolamentati.
Dal punto di vista della protezione dei dati, gli scambi di criptovalute e i fornitori di servizi di portafoglio di criptovalute devono essere considerati come controllori di dati per quanto riguarda le chiavi private dei loro clienti così come qualsiasi altro dato personale che trattano.
Infatti, uno degli obblighi più significativi che devono assolvere ai sensi dell'articolo 32 del Regolamento generale sulla protezione dei dati dell'UE, è quello di adottare e mantenere misure di sicurezza adeguate all'esito di un Data Protection Impact Assesment *ad hoc*.
Un importante passo del legislatore nella disciplina degli strumenti finanziari digitali è stato, tuttavia, effettuato con l'introduzione del D.L. n.25 del 17.03.2023 (c.d. "decreto fintech") convertito, con modificazioni, con L. n.52/2023 che introduce nel quadro normativo italiano misure urgenti relative all'emissione di "strumenti finanziari digitali".
Tale normativa rappresenta un primo approccio del nostro legislatore per l'apertura del settore finanziario nello scambio di *token* che rappresentano classi di strumenti tradizionali quali azioni ed obbligazioni.

Il decreto Fintech si è reso necessario ai di adeguare l'ordinamento italiano al Regolamento UE 2022/858 (c.d. "DLT Pilote Regime"). Quest'ultimo disciplina l'emissione e la circolazione degli strumenti finanziari in forma digitale prevedendo la possibilità, per determinati operatori di mercato, di costituire piattaforme di negoziazione di strumenti finanziari digitali.

3. Nuovi orizzonti normativi

3.1 Le sfide per la sicurezza e la privacy

La tecnologia blockchain, che ha rivoluzionato profondamente il settore delle transazioni digitali, continua a esercitare un'influenza significativa su aspetti fondamentali come la sicurezza dei dati sensibili e la tutela della privacy degli utenti. La struttura decentralizzata e immutabile di questa tecnologia rappresenta un elemento chiave nella garanzia della sicurezza: ogni transazione è crittografata e legata permanentemente alle operazioni precedenti, generando una catena di blocchi che risulta estremamente difficile da alterare. Questo sistema di protezione rende i dati pressoché invulnerabili a manipolazioni esterne, rafforzando notevolmente la fiducia nel suo utilizzo.

Tuttavia, se da un lato la blockchain pubblica assicura un elevato livello di sicurezza, dall'altro la tutela della privacy degli utenti rappresenta una sfida complessa.

Anche se le transazioni avvengono tramite pseudonimi, la totale trasparenza della rete fa sì che ogni operazione sia visibile a tutti. Ciò può destare preoccupazioni, specialmente quando si tratta di proteggere informazioni sensibili come dati personali o finanziari.

Sebbene l'uso di pseudonimi consenta agli utenti di mantenere un certo livello di anonimato, la natura trasparente della blockchain rende tracciabili tutte le transazioni, permettendo potenzialmente a chiunque di monitorare i flussi di denaro o le attività commerciali di un determinato utente.

Per far fronte a queste problematiche, una delle soluzioni più promettenti è rappresentata dall'adozione di blockchain private o autorizzate.

In questi sistemi, solo un gruppo selezionato di partecipanti ha il permesso di accedere ai dati e di verificare le transazioni, limitando così l'esposizione delle informazioni sensibili. Oltre a ciò, sono state sviluppate tecniche avanzate di crittografia, come le "*zero-knowledge proofs*[8]" o "*i*

[8] Sono una famiglia di tecnologie crittografiche che permettono di dimostrare la veridicità di un'affermazione senza dover rivelare le informazioni che la riguardano. Le ZKP sono alla base di una delle principali soluzioni di scalabilità Layer 2, i cosiddetti rollup, sviluppati con l'obiettivo di aumentare il volume (throughput) e la velocità delle transazioni su blockchain e circoscrivere così sia la congestione della rete che i costi di transazioni troppo elevati.

sistemi di crittografia omomorfa[9]", che consentono di proteggere i dati senza compromettere l'integrità e la trasparenza della catena. Questi approcci mirano a trovare un equilibrio tra la necessità di trasparenza, che è fondamentale per il funzionamento della blockchain, e l'esigenza di garantire una maggiore riservatezza per le informazioni personali.

Un ulteriore aspetto critico riguarda la sicurezza delle chiavi private, poiché la loro perdita o compromissione può comportare conseguenze gravissime, come la perdita del controllo sui portafogli digitali o il furto dei fondi. Nonostante la blockchain offra una robustezza intrinseca contro le manomissioni non è del tutto immune agli attacchi informatici o alla sottrazione di credenziali. Le attuali architetture decentralizzate delle criptovalute continuano a presentare vulnerabilità simili a quelle riscontrate nei sistemi tradizionali, come il furto di dati o di password, esponendo gli utenti al rischio di perdere i propri beni digitali se le chiavi private vengono compromesse.
Nonostante tali criticità, l'uso dello pseudonimato ha svolto un ruolo cruciale nella rapida diffusione di criptovalute come Bitcoin. La possibilità di effettuare transazioni senza dover ricorrere a complesse infrastrutture di identificazione o all'autorizzazione di terze parti ha accelerato l'adozione di queste tecnologie su larga scala. In definitiva, sebbene la blockchain abbia dimostrato di essere una tecnologia estremamente sicura e innovativa, le questioni legate alla privacy e alla protezione delle chiavi private richiedono un'attenzione continua. Il futuro di questa tecnologia dipenderà in gran parte dalla capacità di bilanciare in modo efficace la trasparenza necessaria per il funzionamento della rete con le esigenze sempre più pressanti di sicurezza e riservatezza degli utenti.

Secondo le previsioni presentate durante l'ultimo World Economic Forum, entro il 2025 il 10% del PIL globale potrebbe derivare da attività e servizi basati su tecnologie Blockchain. Tuttavia, questo scenario dovrà confrontarsi con le normative esistenti, in particolare il GDPR[10], il regolamento europeo sulla protezione dei dati.

---

[9] In matematica e in particolare in algebra, un omomorfismo è una funzione tra due spazi che presentano la stessa struttura algebrica.
La crittografia omomorfa è un termine che rappresenta dunque tutti quegli algoritmi di crittografici che mappano le proprietà algebriche dello spazio dei messaggi in chiaro di partenza nello spazio dei crittogrammi (ovvero dei messaggi cifrati) di arrivo.

[10] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Permangono tuttavia, al momento attuale, molte incertezze sulle modalità per le quali la trasparenza e la privacy possano interagire in maniera costruttiva e priva di rischi.
Nella tecnologia moderna coesistono due tipologie principali di blockchain: quelle definite *permissionless*, che non necessitano di un'autorizzazione, e quelle *permissioned* che, contrariamente alle precedenti, necessitano di autorizzazione.
In particolare, con riferimento a quest'ultima tecnologia, le transazioni avvengono all'interno di un ecosistema chiuso in cui tutti i dati registrati e le identità degli utenti facente parti della rete rimangono riservate.

Lo scenario descritto ora dovrà fare i conti con diverse normative che a livello statale e comunitario stanno venendo implementate; prima fra tutte il già citato GDPR.
Questo nuovo regolamento avrà un impatto rilevante su tre aspetti fondamentali della tecnologia blockchain, che fino ad ora risultano essere i più critici:

- I dati memorizzati sulla blockchain sono immutabili ed una volta inseriti questi non posso quindi venire eliminati, sollevando dubbi sulla compatibilità di questo problema con il diritto di cancellazione ("*diritto all'oblio*").
- La natura decentralizzata della blockchain implica che il controllo sui dati sia decentralizzato e diviso tra tutti i partecipanti della rete. Questa caratteristica risulta andare in aperto contrasto con le esigenze del GDPR, che richiede la presenza di un responsabile per la protezione dei dati, ruolo che, ovviamente, i *miners* non possono assumere.
- Gli smart contract potrebbero essere considerati parte del processo decisionale automatizzato, introducendo potenziali problematiche legate alla possibilità di contestare tali decisioni.

Le caratteristiche che, fino ad oggi, hanno definito il valore della blockchain risultano essere in aperto contrasto con i principi del GDPR, in particolare, i principali punti critici di questo processo di controllo della privacy e della trasparenza all'interno della tecnologia blockchain risultano essere: la pubblica accessibilità a tutti i partecipanti dei dati registrati e la permanenza fissa degli stessi all'interno del sistema. Sarà fondamentale capire come conciliare la protezione dei dati personali con un sistema che gestisce grandi quantità di informazioni e come rispettare i requisiti relativi al tempo di conservazione all'interno di un contesto in cui l'archiviazione è indefinita.

Nonostante queste sfide, l'integrazione tra Blockchain e GDPR potrebbe offrire opportunità interessanti, come l'adozione della "sicurezza by design", favorendo la pseudonimizzazione (disassociando i dati dall'identità individuale) e la minimizzazione dei dati (condividendo solo le informazioni strettamente necessarie). Questo approccio di protezione dei dati nella Blockchain si basa su diversi strumenti come la chiave pubblica del mittente, la chiave pubblica del destinatario, un hash crittografico che rappresenta il contenuto della transazione e la data e l'ora della transazione.

L'hash crittografico è unidirezionale e non consente di ricostruire il contenuto della transazione. Inoltre, se nessuna delle parti associa la propria chiave pubblica a un'identità nota, non è possibile risalire agli individui o alle organizzazioni coinvolte. Questo garantisce che, anche se la Blockchain è pubblica, non vengano divulgate informazioni personali.

3.2 Verifica delle identità digitali

Attualmente, circa 850 milioni di persone non possiedono un'identificazione ufficiale, mentre miliardi di individui con un documento legale non dispongono di adeguate tutele per la loro privacy nell'ambito dell'economia digitale.

L'uso di un'identità digitale decentralizzata permette alle persone di partecipare in modo più sicuro ed efficace all'economia digitale.

Attraverso credenziali di identità verificate, gli utenti possono assicurare la loro privacy, mantenendo il controllo sui propri dati personali; inoltre, le tecnologie che supportano l'identità digitale decentralizzata possono apportare benefici anche in altri campi di utilizzo come quello ambientale o ancora quello della governance.

L'ID digitale decentralizzato basato su blockchain offre un livello superiore di protezione della privacy rispetto ai sistemi centralizzati, che sono più vulnerabili all'abuso dei dati personali ed a violazioni su larga scala. In questo modello, gli identificatori ed i metadati dell'ID digitale possono essere collegati a una blockchain pubblica decentralizzata, mentre i dati personali restano fuori dal registro, conservati nei portafogli digitali controllati dall'utente.

Questo approccio alla privacy risolve un problema di vecchia data delle soluzioni di identità precedenti, noto come "*effetto panopticon*[11]".

[11] Il filosofo Jeremy Bentham, fondatore dell'utilitarismo ed uno dei principali sostenitori della separazione tra stato e chiesa, fu il primo che teorizzò una tipologia di prigione in cui i prigionieri sarebbero stati sotto costante

Per spiegare il concetto di "*panopticon*", si può pensare ad un fornitore di social network che offre agli utenti un servizio di "single sign-on[12]" per accedere ad altri siti web. In questo caso, il "fornitore di identità" funge da intermediario centrale, facilitando la condivisione di informazioni verificate, come richiede il modello del web2[13].

Anche se questo approccio può offrire alcuni vantaggi per la privacy, come la condivisione limitata di informazioni, il fornitore di identità rimane coinvolto in ogni transazione quindi ogni volta che l'utente utilizza questo sistema, il fornitore sa con chi sta interagendo e quali informazioni vengono condivise, osservando costantemente tutte le sue attività, proprio come nella metafora del "panopticon".
La comunità che si occupa della gestione dell'identità ha cercato di risolvere il problema del "panopticon" per anni, introducendo soluzioni innovative come le architetture "a doppio cieco", dove uno scambio di identità avviene tra il fornitore di identità ed un servizio digitale per ridurre la sorveglianza continua. Tuttavia, queste architetture sono complesse e difficili da implementare su larga scala a causa della crescente domanda globale di ID digitali verificati e rispettosi della privacy.

La soluzione proposta dal web3[14] elimina la necessità di un fornitore di identità centralizzato; sfrutta, invece, un'infrastruttura blockchain pubblica, permettendo agli utenti di conservare i metadati della propria identità digitale e mantenere i dati personali offline all'interno di un

---

sorveglianza, senza sapere però di venire osservati. Questa tipologia di carcere viene appunto definita Panopticon o panottico

[12] Metodo di autenticazione che consente agli utenti di accedere usando un set di credenziali per più sistemi software indipendenti.

[13] Il termine, apparso nel 2005, indica genericamente la seconda fase di sviluppo e diffusione di Internet, caratterizzata da un forte incremento dell'interazione tra sito e utente: maggiore partecipazione dei fruitori, che spesso diventano anche autori; più efficiente condivisione delle informazioni, che possono essere più facilmente recuperate e/o scambiate con strumenti peer to peer o con sistemi di diffusione di contenuti multimediali.

[14] Web3 viene usato per descrivere la prossima generazione del World Wide Web ed è generalmente associato all'idea di un Internet decentralizzato, ancora più aperto e incentrato sull'utente, costruito sulla tecnologia blockchain e su altre tecnologie distribuite.
Il termine Web 3.0 è stato coniato dal fondatore di Polkadot e co-fondatore di Ethereum Gavin Wood nel 2014, per riferirsi a un ecosistema online decentralizzato basato sulla blockchain.
La finanza decentralizzata (DeFi) è un concetto chiave nella teorizzazione del Web 3.0: gli utenti possono utilizzare gli strumenti finanziari ed effettuare transazioni senza dover affidarsi a intermediari come broker, banche o borse centralizzate.

portafoglio digitale. Le credenziali verificate, come una laurea rilasciata da un'università o un documento d'identità legale emesso da un ente governativo, sono firmate digitalmente e memorizzate nel portafoglio dell'utente.
Quando l'utente deve presentare una credenziale, può verificare l'autenticità della firma crittografica confrontandola con la chiave pubblica dell'emittente, pubblicata in un registro accessibile a tutti. Questo sistema offre all'utente pieno controllo su quali informazioni condividere e con chi, permettendo allo stesso tempo la condivisione sicura delle credenziali per scopi di conformità come il know-your-customer (KYC[15]).
Le tecnologie per l'identificazione digitale decentralizzata stanno avanzando rapidamente.
Diverse tecnologie di base sono già state testate e standardizzate dal W3C[16], l'organismo responsabile degli standard web. Recenti sviluppi indicano che il ruolo della blockchain nell'ID digitale continuerà a crescere.

A sottolineare l'importanza che questa innovazione sta ricoprendo, nel 2022, Vitalik Buterin, fondatore di Ethereum, ha co-scritto un documento intitolato "Decentralized Society: Finding Web3's Soul", introducendo il concetto di "soulbound tokens" (token legati all'anima), una nuova funzionalità nativa della blockchain per far avanzare il campo dell'identità digitale.
La gestione dell'identità è un processo complesso che include l'identificazione, l'autenticazione e l'autorizzazione degli individui per l'accesso a sistemi, reti e applicazioni. Per ridurre il rischio di frodi, furti di identità e violazioni dei dati, vengono implementate soluzioni robuste di identità digitale.
Sempre più aziende stanno esplorando l'uso di un approccio decentralizzato, basato sulla blockchain, per la gestione delle identità, sfruttando la natura immutabile e sicura di questa tecnologia.

[15] Il KYC, acronimo di Know Your Customer (letteralmente: "conosci il tuo cliente"), è l'insieme di procedure che devono essere attuate da alcuni istituti e professionisti per obbligo di legge. Queste procedure servono per acquisire dati certi e informazioni sull'identità dei loro utenti e clienti.
Le procedure KYC, come si è detto, costituiscono obbligo di legge e sono solo una parte degli adempimenti normativi dettati dalle più ampie direttive europee antiriciclaggio (racchiuse sotto l'acronimo di AMLD – Anti Money Laundry Directives), il cui ultimo aggiornamento è stato recepito in Italia con il decreto legislativo 90/2017.
[16] Organismo di coordinazione delle attività sul web, attraverso l'apposizione di regolamenti e linee standard per promuovere la sua continua evoluzione.

La verifica dell'identità basata su blockchain, che sfrutta la tecnologia del registro distribuito, si presenta come una soluzione promettente per il mercato dell'Identity and Access Management[17] (IAM). Questa tecnologia offre un metodo sicuro per la gestione e conservazione delle identità digitali, sia per le aziende che per gli utenti finali. Oltre a prevenire potenziali violazioni di dati su larga scala, potrebbe consentire agli individui di mantenere il controllo completo sulla propria identità digitale, un concetto noto come Self-Sovereign Identity (SSI).

Negli ultimi anni sono state sviluppate diverse soluzioni di identità basate su blockchain, incluse iniziative a livello governativo. Ad esempio, nel 2018, il Programma Alimentare Mondiale (WFP) ha utilizzato un sistema di identificazione su Ethereum per distribuire aiuti umanitari.
Un'altra iniziativa importante è il progetto ID2020, una collaborazione globale che mira a definire il futuro della gestione delle identità digitali. Tra i partner figurano BLOK Solutions e Accenture, entrambe startup specializzate in servizi di identità digitale basati su blockchain.
Secondo uno studio di Allied Market Research[18], il mercato delle soluzioni di gestione dell'identità blockchain, che nel 2021 valeva 156.8 milioni di dollari, potrebbe crescere fino a 77.8 miliardi di dollari entro il 2031. Governi, enti sanitari e aziende del settore retail sono previsti come i principali promotori di questa crescita nei prossimi anni.
Il modello di identità autogestita (SSI, Self-Sovereign Identity) si basa sul principio che l'identità digitale è interamente controllata e posseduta dall'utente.

Con la SSI, gli individui hanno il diritto di gestire e condividere diversi aspetti della loro identità in vari contesti e domini. Ciò significa che è l'utente a decidere come e quando i propri dati vengono utilizzati, piuttosto che aziende o organizzazioni a cui si inviano moduli online. Le identità SSI possono essere memorizzate localmente sullo smartphone dell'utente o distribuite su una rete blockchain.
Questo sistema funziona come un passaporto elettronico, utilizzando identificatori decentralizzati[19] (DID) per permettere la gestione di identità digitali verificabili e

[17] Identity and Access Management (IAM) gestisce il ciclo di vita end-to-end delle identità e dei diritti degli utenti per tutte le risorse aziendali, sia nei data center sia nel cloud. È un controllo fondamentale della sicurezza del cloud in quanto autentica gli utenti e regola l'accesso a sistemi, reti e dati
[18] Si veda: *"Decentralized Identity Market Size, Share, Competitive Landscape and Trend Analysis Report, by Type, by Enterprise Size, by End User: Global Opportunity Analysis and Industry Forecast, 2021-2031"*

[19] Un Identificatore Decentralizzato (DID) è un ID unico emesso da una piattaforma decentralizzata, che funge da prova di proprietà dell'identità digitale

decentralizzate. I DID rappresentano l'equivalente crittografico delle credenziali verificabili (VC), come nomi utente e password.
Nel 2017 InfoCert, Certification Authority, parte del gruppo Tecnoinvestimenti, ha annunciato la sua partecipazione al progetto della Sovrin Foundation[20], un'organizzazione non profit con sede negli USA, per il lancio del Sovrin Network, il primo sistema al mondo, scrivono loro, per la gestione di identità digitali distribuite e decentralizzate (self-sovereign digital identity). La Sovrin Network è basata su tecnologia blockchain anche denominata "distributed ledger" e quindi consente a persone e organizzazioni la creazione di identità digitali da gestire in completo controllo e in maniera indipendente da singoli enti o organizzazioni governative.

Sovrin è una rete open source progettata per la gestione delle identità digitali online. La rete è costituita da nodi distribuiti, gestiti e amministrati da entità affidabili chiamate Steward. Ogni nodo contiene una copia del registro, utilizzato per verificare la validità delle credenziali emesse all'interno della rete. Grazie a Sovrin, le organizzazioni possono evitare il fardello normativo legato alla conservazione di grandi quantità di dati, che, come noto, sono vulnerabili al furto.

3.3 La gestione dei diritti digitali

L'era digitale ha aperto nuove opportunità per la diffusione e condivisione di contenuti, ma ha anche sollevato importanti questioni sulla protezione della proprietà intellettuale. In questo contesto, la Gestione dei Diritti Digitali (DRM) si presenta come un insieme di tecnologie e protocolli creati per tutelare, gestire e regolare l'accesso e l'uso dei contenuti digitali.
Lo stesso parlamento europeo aveva inteso l'importanza di regolare e proteggere la distribuzione delle opere; questa linea di pensiero venne tramutato in azione dalla direttiva 2001/29/CE del 22 maggio 2001, la quale, al paragrafo 55 recita:

> " *lo sviluppo tecnologico agevolerà la distribuzione delle opere, in particolare in rete, il che comporterà la necessità per i titolari dei diritti di identificare meglio l'opera o i materiali protetti, l'autore dell'opera o qualunque altro titolare di diritti e di fornire informazioni sui termini e sulle condizioni di utilizzo dell'opera o di altro materiale protetto, così da rendere più facile la gestione dei diritti ad essi connessi. Si dovrebbero incoraggiare i titolari, quando mettono in rete opere o altri*

materiali protetti, a usare contrassegni indicanti, tra l'altro, la loro autorizzazione, oltre alle informazioni di cui sopra".

Il DRM è stato introdotto con l'obiettivo di trovare un equilibrio tra la condivisione dei contenuti digitali e la salvaguardia dei diritti dei creatori e detentori dei diritti. Attraverso l'uso di sistemi DRM, i proprietari possono avere un controllo più efficace sulla distribuzione e l'uso dei loro contenuti, contrastando la pirateria e assicurando una giusta remunerazione per il lavoro creativo.
Il DRM, ovvero Digital Rights Management, è un insieme di tecnologie e processi ideati per proteggere la proprietà intellettuale e gestire i diritti relativi ai contenuti digitali, come musica, video, software e altro ancora.

Il principale scopo del DRM è permettere ai proprietari di contenuti di controllare chi può accedere, distribuire e utilizzare i loro materiali digitali.
Tra i metodi di protezione impiegati nel DRM vi sono la crittografia, i sistemi di gestione delle licenze e i meccanismi di autenticazione. Questi strumenti assicurano che solo gli utenti autorizzati possano accedere ai contenuti e che l'accesso avvenga in conformità con le condizioni stabilite dai titolari dei diritti.
Attraverso tali sistemi, i creatori e i detentori dei diritti possono stabilire regole specifiche sull'utilizzo dei loro materiali digitali, come il numero di riproduzioni consentite, la durata dell'accesso e i dispositivi autorizzati per la visualizzazione.
Il Digital Rights Management (DRM) presenta una serie di vantaggi e svantaggi nella protezione della proprietà intellettuale e nella gestione dei diritti digitali.
Tra i principali benefici del DRM c'è la capacità di proteggere i contenuti digitali dalla pirateria e dall'accesso non autorizzato. Attraverso l'uso di tecniche di crittografia e gestione delle licenze, i proprietari dei contenuti possono limitare l'accesso ai loro materiali solo agli utenti autorizzati, garantendo così un controllo maggiore sulla distribuzione e l'uso dei loro lavori.

Un altro vantaggio del DRM è la possibilità di applicare restrizioni personalizzate su come i contenuti digitali possono essere utilizzati. Ad esempio, i proprietari possono impostare regole specifiche riguardo al numero di riproduzioni, alla durata dell'accesso o ai dispositivi autorizzati, offrendo maggiore flessibilità nella gestione dei diritti.
Tuttavia, il DRM presenta anche alcuni aspetti negativi.
Una critica comune è che le restrizioni imposte possono limitare l'utilizzo legittimo dei contenuti da parte degli utenti che li hanno acquistati. Ad esempio, potrebbe essere difficile copiare,

condividere o trasferire i contenuti tra dispositivi, riducendo così la flessibilità e l'usabilità per gli utenti.

Inoltre, l'implementazione del DRM può comportare costi aggiuntivi per i proprietari dei contenuti, poiché è necessario investire in tecnologie e infrastrutture per proteggere e gestire i materiali digitali. Questi costi possono aumentare il prezzo finale dei prodotti per i consumatori.

Infine, alcuni critici mettono in dubbio l'efficacia del DRM nel prevenire la pirateria. Anche se i sistemi DRM sono progettati per impedire la duplicazione non autorizzata, i pirati informatici riescono spesso ad aggirare queste protezioni, rendendo meno utile l'investimento in tali soluzioni per alcuni detentori di diritti.

4.Blockchain e le sue implicazioni economiche e finanziarie

4.1 Smart contracts

La crescente diffusione della Distributed Ledger Technology (DLT), e in particolare della blockchain, ha portato ad un approfondimento della disciplina e alla parallela diffusione dei cosiddetti "smart contract".

Il termine "smart contract", tradotto come "contratti intelligenti", si riferisce comunemente all'integrazione di clausole contrattuali in un software, con esecuzione automatica e senza bisogno dell'intervento di terze parti.

Più precisamente, uno smart contract indica un accordo negoziale giuridicamente vincolante, in cui alcuni o tutti i termini vengono certificati o eseguiti automaticamente da un programma informatico su una rete a registro distribuito.

Uno smart contract può essere descritto come un codice digitale che fornisce garanzie basate su condizioni predefinite concordate tra le parti coinvolte. In pratica, le parti stabiliscono una condizione che, se soddisfatta o meno, avvia automaticamente un'azione o una serie di azioni.

L'idea degli smart contract fu introdotta per la prima volta dall'informatico e crittografo Nick Szabo nel 1997. Szabo, noto per i suoi studi su blockchain e crittografia, è considerato un'autorità in questo campo, tanto da essere stato associato a Satoshi Nakamoto, il creatore ancora sconosciuto, di Bitcoin.

Un esempio semplice per illustrare il funzionamento degli smart contract è quello di un distributore automatico: inserendo 50 centesimi, si ottiene un caffè; con 1 euro, si riceve il caffè e 50 centesimi di resto, tutto in modo automatico.

Un altro esempio riguarda un ipotetico sistema di sicurezza per auto. Uno smart contract potrebbe essere programmato per garantire che solo il legittimo proprietario possa accedere alle chiavi crittografiche necessarie per far funzionare il veicolo. In caso di mancato pagamento di un prestito, lo smart contract potrebbe trasferire automaticamente il controllo delle chiavi all'istituto di credito fino alla risoluzione del debito, senza bisogno di intermediari o procedure complesse.

Uno smart contract si distingue per la sua capacità di eseguire automaticamente le azioni al verificarsi di una determinata condizione o evento specifico. Una volta attivato il processo, i termini stabiliti si applicano autonomamente, senza possibilità di essere bloccati o modificati. Questo processo offre numerosi vantaggi, tra cui una significativa riduzione dei costi legati agli intermediari, oltre a garantire rapidità e sicurezza nell'esecuzione delle operazioni. In questa prospettiva, ed in linea teorica, gli smart contract non dovrebbero necessitare di un soggetto che garantisca il cosiddetto "contract enforcement[21]", ossia l'esecuzione forzata del contratto, e dovrebbero operare senza generare errori nell'implementazione.

Il legislatore italiano, comprendendo l'importanza che questo processo di digitalizzazione stava assumendo, ha introdotto il concetto di smart contract nel nostro ordinamento giuridico con il decreto-legge n. 135/2018 convertito con la legge n. 12/2019 dove venne inserita, per la prima volta, la definizione e la disciplina di questa nuova tecnologia che recita come segue:

> *" 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. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto".*

Gli smart contract operano attraverso semplici istruzioni del tipo "se/allora", scritte nel codice e registrate su una blockchain, comunemente Ethereum, anche se esistono altre piattaforme come Cardano e Ripple che supportano smart contract.
Una rete di computer esegue le azioni quando le condizioni predefinite vengono soddisfatte e verificate. Queste azioni possono includere l'emissione di un biglietto, la registrazione di un veicolo o l'effettuazione di un pagamento. Una volta completata la transazione, la blockchain si aggiorna, rendendo l'operazione immutabile e resistente a manipolazioni.
Uno smart contract può includere tutte le clausole necessarie per garantire ai partecipanti che l'azione sarà completata correttamente. Per definire i termini, è necessario stabilire come le

[21]Definito come il processo per garantire che i termini concordati dalle parti in un contratto siano soddisfatti ed eseguiti come previsto. Questo processo aiuta a mantenere la fiducia e l'equità tra le parti ed è essenziale per il buon funzionamento delle transazioni commerciali e personali.

transazioni e i dati sono rappresentati sulla blockchain, concordare le regole del "se/allora", considerare le eccezioni e creare un sistema per risolvere eventuali controversie.

Lo smart contract viene programmato da uno sviluppatore, che inserisce le regole nel codice e le carica su una blockchain come Ethereum, dove tutti i computer connessi alla rete mantengono una copia del contratto.
Chiunque può utilizzare uno smart contract se ha token ether, che può essere acquistato su exchange di criptovalute, e un wallet digitale (come Metamask) per conservare e inviare ether.
Gli smart contract rappresentano una soluzione promettente per decentralizzare i servizi Web3 e le applicazioni DApp[22](Decentralized Application), ma presentano alcune limitazioni. Poiché sono scritti da persone, possono contenere errori che richiedono tempo per essere individuati e corretti attraverso revisioni e audit. Inoltre, la sicurezza della blockchain e delle applicazioni DeFi basate su di essa non è ancora stata completamente messa alla prova.
Un'altra sfida significativa riguarda la gestione della variabilità e della casualità tipiche del mondo reale. Gli smart contract, per ora, mancano della "flessibilità" necessaria per tenere conto delle complessità e del fattore umano nelle situazioni reali.
Questo svantaggia la blockchain rispetto alle soluzioni tradizionali centralizzate: per risolvere articolate dispute ci rivolgeremo ancora a giudici e avvocati, ma forse un giorno gli smart contract riusciranno a chiarire tutto in poche stringhe di codice.

4.2 Blockchain per il settore finanziario

Le tecnologie dell'informazione e delle telecomunicazioni hanno un impatto rilevante sull'evoluzione dei mercati finanziari, facilitando l'offerta di servizi più efficienti, l'ingresso di nuovi attori e ampliando la concorrenza. Tra le innovazioni più rilevanti, la tecnologia "blockchain", alla base delle valute digitali, sta suscitando un crescente interesse nel settore finanziario per i suoi potenziali effetti positivi sui processi che supportano l'erogazione dei servizi finanziari.

[22] Le DApp sono applicazioni simili alle app tradizionali, con la differenza fondamentale che al posto di appoggiarsi su server centralizzati sfruttano le piattaforme blockchain ed il loro network distribuito.

La tecnologia blockchain sembra offrire soluzioni efficienti in tutti quei contesti in cui è necessaria l'interazione tra un gran numero di utenti. Essendo una tecnologia innovativa e ancora in fase di sperimentazione, la ricerca accademica svolge un ruolo fondamentale nell'analizzare i potenziali utilizzi della blockchain, andando oltre il settore finanziario. Tra le possibili applicazioni si ipotizzano l'utilizzo per la regolamentazione delle transazioni, sia monetarie che di titoli, la gestione delle lettere di credito e l'amministrazione di registri pubblici, come il catasto o l'anagrafe. Esistono anche pareri divergenti sull'opportunità di utilizzare questa tecnologia indipendentemente dall'asset digitale sottostante ampliando notevolmente lo spettro di utilizzo della blockchain.

Andremo adesso ad analizzare le macroaree nelle quali questa tecnologia può davvero essere un game-changer, soffermandoci in particolare sul settore finanziario:

- Pagamenti e liquidazioni immediati: Iniziamo con una delle operazioni più comuni nel settore finanziario: inviare e ricevere pagamenti. Ciò include non solo i pagamenti da parte dei clienti, ma anche le transazioni tra istituti finanziari e banche, che possono variare da piccole a grandi somme di denaro.
- In questo contesto, la blockchain offre transazioni rapide e a basso costo, risolvendo così due delle principali criticità dei sistemi bancari tradizionali. Esistono già numerose blockchain che si distinguono per l'efficienza e l'economicità delle transazioni, e si prevede che nel lungo termine potrebbero prevalere sui metodi tradizionali di trasferimento fondi.

Un altro vantaggio da considerare riguarda l'efficacia che la blockchain apporterebbe nella gestione delle transazioni da parte delle banche. Attualmente, gli istituti bancari utilizzano piattaforme proprietarie, spesso incompatibili tra loro, con conseguenti inefficienze e ritardi operativi. L'adozione di una soluzione comune e indipendente come la blockchain ridurrebbe significativamente i costi e aumenterebbe la velocità delle transazioni rispetto ai sistemi attuali.
Infine, un aspetto rilevante legato ai trasferimenti di denaro è rappresentato dalla possibilità di liquidazioni automatiche offerte dagli smart contract. Essendo contratti immutabili registrati su una blockchain, gli smart contract garantiscono che le liquidazioni avvengano automaticamente al verificarsi di una condizione predefinita, eliminando il rischio che una delle parti non rispetti i termini di pagamento.

- Riduzione dei costi: Il secondo vantaggio, strettamente legato al primo, è il risparmio complessivo derivante dall'adozione della tecnologia blockchain nei processi aziendali. Le transazioni effettuate tramite blockchain hanno costi estremamente ridotti (solitamente frazioni di centesimo) rispetto a quelle effettuate tramite i canali bancari tradizionali.

Inoltre, implementando soluzioni basate su blockchain ecologiche, si potrebbe ridurre significativamente l'impatto ambientale, ottimizzando un settore come quello bancario, che attualmente contribuisce all'emissione di decine di tonnellate di CO2 ogni anno.

- Riduzione del rischio di frodi: Uno dei problemi più persistenti nel settore finanziario è certamente quello delle frodi. Ogni anno, a livello globale, si verificano episodi di riciclaggio e corruzione che comportano perdite per miliardi di dollari, danneggiando lo sviluppo economico trasparente e legale.

La Blockchain, per sua natura, è un registro digitale condiviso e immutabile. Ciò significa che tutte le operazioni registrate sono visibili e verificabili da chiunque, grazie a un timestamp che ne attesta la data e l'ora.
Qual è il vantaggio principale di questo sistema? La tracciabilità. Come in una supply chain, anche nella Blockchain è possibile monitorare ogni movimento di denaro, riducendo notevolmente il rischio di transazioni fraudolente. Sebbene la Blockchain non rappresenti una soluzione definitiva a tutte le problematiche legate alla criminalità, costituisce comunque un potente strumento per contrastare frodi e riciclaggio.

- Eliminazione dell'intermediario: Uno dei motivi per cui la blockchain è considerata una tecnologia rivoluzionaria è il concetto di "disintermediazione". Essa elimina la necessità di terze parti o intermediari in vari processi e filiere.

Un esempio evidente è quello delle criptovalute, il cui scopo principale è decentralizzare, sottraendo alle banche centrali il controllo sulla creazione e il valore del denaro.
Nel settore finance e fintech, la blockchain, attraverso l'uso degli smart contract, potrebbe eliminare figure professionali non strettamente necessarie, riducendo i costi operativi.
Un esempio pratico è quello delle liquidazioni: grazie agli smart contract, queste possono essere automatizzate attraverso clausole che si attivano in base al verificarsi di un determinato evento, rendendo il processo più efficiente.

In conclusione, il settore bancario risulta uno se non il principale settore che beneficerebbe dall'introduzione di questa nuova tecnologia

4.3 Strategie delle banche centrali

Fin dalla loro nascita, le banche centrali hanno costantemente adattato le proprie funzioni per rispondere alle esigenze del settore dei pagamenti, in particolare per garantire stabilità finanziaria e attuare politiche monetarie efficaci.

Le banche centrali forniscono al sistema finanziario una risorsa sicura: la moneta di banca centrale, che rappresenta il nucleo del sistema. È grazie alla convertibilità della moneta privata in moneta di banca centrale che si mantiene la stabilità del suo valore; questa moneta svolge un ruolo fondamentale nell'unificare le diverse componenti del sistema dei pagamenti, garantendo l'integrazione e l'unicità della valuta.

Questo è particolarmente importante in una zona monetaria unificata come l'area dell'euro, dove la moneta della banca centrale, sia in forma di contante che di riserve, può essere utilizzata per regolare pagamenti tra diversi paesi, garantendo che un euro abbia lo stesso valore indipendentemente dal luogo, sia esso Parigi o Roma.

Per continuare a svolgere questo ruolo chiave, la moneta di banca centrale deve rimanere al passo con i progressi tecnologici, conservando la sua attrattiva come mezzo di pagamento. Le banche centrali non devono restare indietro rispetto alla trasformazione digitale, anzi, devono guidare l'innovazione finanziaria e promuovere la modernizzazione in modo sicuro. L'Eurosistema sta lavorando attivamente in questa direzione.

Un esempio concreto di questo impegno è lo sviluppo dei pagamenti al dettaglio e il progetto dell'euro digitale, che mira a rendere la moneta di banca centrale disponibile in formato digitale, oltre che in contanti.

Un importante passo avanti è stato raggiunto con il primo esperimento di trasferimento transfrontaliero di una valuta digitale di banca centrale (CBDC), condotto dalla Banca dei Regolamenti Internazionali (BIS) di Basilea. Anche se il tema può sembrare di nicchia, l'evento è significativo: per la prima volta, è stato effettuato uno scambio di valute digitali tra banche centrali utilizzando una blockchain (Distributed Ledger Technology, DLT), con meccanismi simili a quelli alla base del Bitcoin.

L’esperimento ha permesso a tre banche centrali di gestire il flusso delle loro CBDC e monitorare le transazioni in modo trasparente. Questo successo ha segnato l’avvio della terza fase di un progetto iniziato diversi anni fa, con l’obiettivo di creare una rete utilizzabile dalle banche centrali e disponibile in open source.

Il progetto ha avuto inizio con la collaborazione tra la Hong Kong Monetary Authority (HKMA) e la Bank of Thailand (BOT) sotto il nome di Project Inthanon-LionRock, conclusasi a gennaio 2020. Dopo 18 mesi di ulteriori sviluppi, il progetto è passato alla fase successiva, coinvolgendo nuove istituzioni, anche se non è ancora chiaro quanto tempo sarà necessario per completare la terza fase.

Il trasferimento transfrontaliero di fondi attraverso CBDC su una DLT rappresenta un’opportunità che diventerà sempre più attraente, come affermato da Benoît Cœuré, capo del BIS Innovation Hub. Questo prototipo di multiple Central Bank Digital Currencies (mCBDCs) ha dimostrato che è possibile realizzare pagamenti transfrontalieri in tempo reale, più economici e sicuri. Il test ha richiesto solo pochi secondi per il trasferimento, rispetto ai giorni normalmente necessari con i sistemi attuali, e con costi dimezzati.

Un altro aspetto interessante di questo esperimento è la collaborazione tra il BIS Innovation Hub di Hong Kong, l’autorità monetaria di Hong Kong, la Banca centrale della Thailandia, il Digital Currency Institute della Banca Popolare Cinese e la Banca centrale degli Emirati Arabi Uniti. Questa cooperazione internazionale rappresenta un importante segnale, non solo dal punto di vista tecnologico ma anche politico.

La piattaforma mCBDC, attiva 24 ore su 24 e sette giorni su sette, dimostra il potenziale delle valute digitali e della DLT per migliorare l’efficienza dei pagamenti internazionali. Secondo Bénédicte Nolens, capo del BIS Innovation Hub di Hong Kong, l’adozione di pagamenti transfrontalieri più veloci ed economici potrebbe favorire il commercio e lo sviluppo economico, soprattutto in regioni che non beneficiano di un sistema bancario di corrispondenza.

L’internazionalizzazione delle CBDC non è solo un’iniziativa delle singole banche centrali, ma fa parte di un piano del G20 volto a creare un sistema di pagamenti transfrontalieri più rapido, economico e resiliente. Questo progetto, parte di una strategia globale, porterà a un cambiamento significativo nell’ecosistema dei pagamenti internazionali.

In questo contesto, diverse banche centrali stanno sviluppando le proprie monete digitali. Paesi come la Giamaica hanno già annunciato il lancio della loro CBDC, mentre la Cina sta sperimentando l’e-yuan in alcune città e si prepara ad utilizzarlo durante le Olimpiadi invernali del 2022.

Sebbene sia presto per dire che nulla sarà più come prima, il test delle mCBDC lascia intravedere un futuro di trasformazione. Tuttavia, resta il rischio di "disintermediazione" eccessiva delle banche commerciali, che potrebbero essere escluse dai sistemi di pagamento, un problema che le banche centrali non vogliono affrontare. Una possibile soluzione è limitare l'importo di CBDC che ciascun individuo può detenere, riducendo anche le preoccupazioni legate alla privacy. Nonostante queste sfide, la digitalizzazione della moneta è ormai avviata, e il percorso che seguirà è ancora da definire.

Bibliografia