Anitec-Assinform

White Paper Attualità e prospettive della Blockchain per la crescita dell'economia italiana

a cura del Gruppo di Lavoro Cloud & New Technologies

Tavolo di lavoro Blockchain di Anitec-Assinform

Giugno 2021

ANITEC-ASSINFORM
Associazione Italiana per l'Information and Communication Technology
Tel. 02 00632801 - Fax. 02 00632824
C.F e P.I 10053550967

Sede e uffici di Milano:
Via San Maurilio 21, 20123 Milano

Uffici di Roma:
Via Barberini 11 00187 Roma

segreteria@anitec-assinform.it www.anitec-assinform.it

Anitec-Assinform

Sommario

Realizzato da:

Anitec-Assinform

Tavolo di lavoro "Blockchain":

Accenture
Argentea
Algowatt
Cisco Systems
Corvallis
Eustema
Exprivia
GPI
IBM
Infocamere
Leonardo
Liguria Digitale
Microsoft
Miller Group
Nokia
Oracle
Reply

EXECUTIVE SUMMARY

La Blockchain ha la possibilità di plasmare il mondo che ci circonda. Si può immaginare un futuro assai prossimo in cui il sistema delle valute e dei pagamenti verrà del tutto rivoluzionato, così come lo saranno i processi aziendali legati alla supply chain o alla logistica, e da ultimi – non per minore importanza – anche i rapporti tra cittadini e pubbliche amministrazioni. Eppure, ancora oggi, la Blockchain è una risorsa poco utilizzata nel mondo delle istituzioni e all'interno delle imprese. Per questa ragione, lo scopo che Anitec-Assinform si è prefissata è di redigere un documento che partendo dai primi elementi fondamentali – definizioni, storia, applicazioni di questa tecnologia – arrivi a illustrare i risultati attesi dall'applicazione e dell'investimento in Blockchain a livello di Sistema Paese. Nella scrittura ci si è avvalsi dei contributi delle aziende associate ad Anitec-Assinform, che intendono mettere a disposizione di imprese, istituzioni e – più in generale – dei portatori di interesse, esperienza, competenza e visione.

La Blockchain può essere definita come un tipo di registro distribuito – quest'ultimo a sua volta definibile come registro condiviso tra partecipanti a un sistema e sincronizzato tramite un meccanismo di consenso – che organizza le proprie transazioni in blocchi (raggruppamenti di transazioni), e in cui ogni blocco è collegato al precedente tramite un collegamento **crittografico**. Le transazioni nel registro sono ordinate e sequenziali e una volta che una transazione è stata aggiunta ad un blocco questa non può più essere modificata o eliminata. Si tratta di una tecnologia a supporto dei trasferimenti dei bitcoin, tuttavia, negli ultimi dieci anni si è evoluta in numerose direzioni andando ad assumere una miriade di forme e affrontando una lista apparentemente infinita di casi d'uso. È quindi fondamentale sottolineare il fatto che oggi pensare alla Blockchain non deve solo evocare l'immagine delle criptovalute in quanto le sue potenzialità applicative sono assai vaste.

A conferma di ciò, gli *use case* della Blockchain illustrati nel documento sono ben dodici, la maggior parte dei quali in settori cruciali per l'economia italiana, come ad esempio: l'agroalimentare, la moda, l'*automotive*, il turismo e la cultura, i servizi satellitari e l'energia. L'estrema varietà di applicazioni della Blockchain ne dimostra la grande adattabilità sia a *industry* diverse, sia a funzioni diverse nella catena del valore: se, da un lato, sono ormai classiche applicazioni della Blockchain per garantire la tracciabilità dei prodotti nell'industria *agrifood*, dall'altro, notevoli prospettive si aprono in relazione alla garanzia di qualità dei ricambi nell'a*utomotive* o per quanto riguarda le comunicazioni tra satelliti in ambito di servizi satellitari. In generale, l'immutabilità e l'inviolabilità di una Blockchain sono i caratteri che la rendono più appetibile per le aziende.

In questo momento il quadro normativo della Blockchain appare ancora rarefatto con ancora poche norme a disciplinarne usi e requisiti a livello sia europeo sia nazionale. Non mancano però le iniziative, l'esempio più rappresentativo in questo senso è rappresentato dal *Digital Finance Package*: un pacchetto di proposte della Commissione Europea volte a regolamentare quantomeno le applicazioni in ambito finanziario della Blockchain.

Non si pensi però che l'implementazione di soluzioni di Blockchain sia sempre scevra da difficoltà. Nel documento vengono individuati e sviluppati due tipi di *bottleneck*:

- quelli legati al *business*, vale a dire alla necessità di riorganizzare i processi aziendali quando si inizia a utilizzare la Blockchain;
- quelli legati alla tecnologia, cioè ai limiti tecnologici che ancora caratterizzano la Blockchain.

Esempio dei primi sono i necessari accorgimenti organizzativi che affrontano le aziende che desiderano utilizzare la Blockchain per gestire i loro database. Con l'introduzione della Blockchain non si potrà più cambiare un dato già scritto ma si dovrà aggiungerne uno nuovo (che avrà una marca temporale diversa) per cui, per una modifica, potrebbe essere necessario un processo di approvazione e un livello di accesso ai dati superiore. La conseguenza di ciò è che dovranno cambiare le procedure interne di accesso ai dati.

I colli di bottiglia legati alla tecnologia, invece, hanno tipicamente a che vedere con l'elevata capacità computazionale necessaria per adoperare la tecnologia.

Fatta questa premessa sulle difficoltà implementative, si può affermare che tra le aree applicative più promettenti per lo sviluppo della Blockchain vi sono senza dubbio:

- la supply chain,
- le valute virtuali;
- le identità digitali.

Per quanto riguarda la supply chain, una delle pratiche più in grado di esemplificare le potenzialità derivanti dall'implementazione di questa tecnologia è la **tokenizzazione di asset fisici** (Tokenized Physical Asset – TPA): gli asset/prodotti sono digitalizzati è inseriti in un sistema di Blockchain, si parla di TPA in ambito:

- Internet of Things, gli asset digitalizzati diventano connessi tra loro, creando un'identità unica e affidabile estesa a tutti i partner della supply chain che permette agli asset di interagire con loro;
- Physical Product Tracking, per dimostrare l'autenticità del prodotto lungo tutta la catena del valore sfruttando le caratteristiche di inviolabilità e immutabilità della Blockchain.

Sempre in ambito supply chain possono essere citate applicazioni relative ai pagamenti tra fornitori e acquirenti come i sistemi di *trade to settle* (T2S);

Le valute virtuali e l'infrastruttura dei pagamenti hanno rappresentato il "laboratorio" nel quale si sono sviluppate le prime Blockchain e oggi, data la popolarità raggiunta dalle criptovalute, ne sono probabilmente il lato più conosciuto. Individuiamo nel sistema delle valute virtuali una delle aree di maggiore potenzialità per il Paese.

Una criptovaluta è una valuta completamente virtuale, ciò significa che non ha una forma fisica come per le valute tradizionali. Il controvalore in valuta corrente è determinato esclusivamente dalla domanda e dall'offerta e non c'è un organismo regolatore centrale. Queste hanno inoltre il vantaggio di non avere teoricamente costi di intermediazione per le transazioni. Nel sistema delle valute virtuali il ruolo di mediatore tra domanda e offerta e di cambio tra valuta *crypto* e valuta *fiat* è assunto dai "cambiavalute virtuali".

Stabilire un ambiente legale favorevole al settore porterà l'Italia a essere competitiva e all'avanguardia in questa seconda rivoluzione digitale con l'effetto benefico di poter attirare capitali e investitori esteri. La strategia che dovrà adottare il legislatore dovrà essere quella di delineare un quadro normativo proattivo nei confronti del ruolo svolto dai cambia valute virtuali (es. coinbase) e che permetterà il consolidamento dei modelli di business; ciò contribuirà alla definizione di un'infrastruttura regolamentata per operatori di settore nell'ottica di un folte impulso innovativo per tutto il paese.

L'identità digitale è una delle sfaccettature più attuali dell'universo Blockchain. Essa può essere definita come "un insieme di dati che descrivono unicamente una persona, un'azienda o un oggetto e che vengono raccolti, memorizzati e condivisi digitalmente all'interno di un ecosistema di attori e attraverso tecnologie abilitanti per permettere l'accesso a servizi digitali a valore aggiunto". Si tratta di un autentico trasferimento del concetto di identità dal mondo fisico a quello digitale. Le implicazioni di un simile passaggio riguardano strettamente i temi della protezione dei dati e della privacy ragione per le quali si tratta di un'area applicativa che sfrutta le garanzie in termini di sicurezza della Blockchain come tecnologia abilitante. L'utilizzo della Blockchain, consentendo agli utenti di essere certi che i dati siano gestiti in modo corretto e autorizzato, ha permesso di aumentare il livello di decentralizzazione dei sistemi di identità digitale passando da un singolo gestore a una pluralità fino al paradigma emergente della Self Sovereign Identity.

Il mondo dell'identità digitale ci permette di delineare uno scenario potenziale legato all'utilizzo di soluzioni di Blockchain da parte del settore pubblico. Un modello decentralizzato, infatti, è particolarmente indicato in tutti i casi in cui non è possibile individuare un unico soggetto che eserciti funzioni di verifica e, più in generale, di gestione e di responsabilità complessiva sulle informazioni a livello nazionale.

Si consideri come le tecnologie Blockchain e DLT possano portare effettivo valore nei casi d'uso o contesti in cui l'insieme di più contributi possa costituire una nuova sorgente nazionale di informazioni per un determinato settore o ambito di riferimento.

In questi scenari, le condizioni sostanziali che possono portare all'applicazione di modelli decentralizzati sono principalmente l'assenza di un unico soggetto regolatore, in grado di intervenire sull'accesso e sulla modifica del dato, e l'economicità dell'utilizzo del paradigma di interoperabilità abilitato da Blockchain.

La presenza di queste caratteristiche rende interessante e attuabile il ricorso alla tecnologia Blockchain, in particolare in contesti individuabili nelle seguenti tipologie:

a) possibilità di interazione tra fonti pubbliche a carattere comunale/regionale/nazionale, la cui efficacia e fruizione può essere accelerata

e trasformata dalla condivisione dei dati derivante dall'interoperabilità (es. Sanità);

b) costituzione di nuove fonti informative pubbliche per rispondere a nuove esigenze emergenti; ad esempio, il caso delle Disposizioni anticipate di trattamento di cui alla legge 219/2017 e all'art. 1, commi 418-419 della legge 205/2017 ("DAT"), per le quali è previsto un pubblico registro tenuto dal Ministero della Salute e dei registri facoltativi regionali;

c) applicazioni in ambito cross-border, nelle quali l'interoperabilità dei registri distribuiti a livello internazionale, pur centralizzati a livello di singolo Paese, può assicurare una fonte certificativa di dati molto più efficace ed estesa.

Passando dal settore pubblico a quello privato, si può vedere come la Blockchain si stia rivelando un abilitatore cruciale per modelli per le emergenti *sharing economy* e *gig economy*. La *sharing economy*, ad esempio, si propone come modello orizzontale tra i diversi attori che condividono una risorsa, su fondamenta che si consolidano intorno al concetto di reputazione e fiducia.

Di fatto, tramite la Blockchain è possibile andare a sostituire figure di garanzia come notai, regolatori e creare nuove opportunità per aziende o mercati in un modo totalmente nuovo, lasciando la possibilità di sviluppo di nuovi modelli economici di condivisione delle risorse. L'introduzione di uno strumento tecnologico come Blockchain modifica non solo i modi in cui un bene viene scambiato, ma porta anche ad un cambiamento nelle abitudini sociali e aziendali, creando un nuovo tipo di valore, basato sulla decentralizzazione da un'autorità centrale e un nuovo modo di concepire gli scambi.

La possibilità di fare dell'Italia un paese all'avanguardia nello sviluppo e nell'applicazione di Blockchain non è mai stata concreta come ora. Il PNRR rappresenta un'opportunità senza precedenti per il diffondersi delle numerose soluzioni delineate nel corso del documento. Ad esempio, per quanto riguarda le potenzialità della Blockchain in ambito **auditability e certificazione**, di sviluppare delle applicazioni che permetterebbero alle amministrazioni pubbliche di certificare dei passi chiave di avanzamento di pratiche legate ai servizi o ai processi giudiziali, e ai cittadini di controllare in maniera trasparente l'avanzamento degli stessi in tempo reale. Altre applicazioni vedono affinità con il rilancio del Turismo (Missione 1), certificati vaccinali e green pass basati su Blockchain garantirebbero verificabilità ed interoperabilità con altri paesi, o nella Salute (Missione 6), nella tracciabilità dei prodotti medici e sanitari. Questi stessi vantaggi possono essere applicati ai processi delle filiere, con la protezione del Made in Italy ed il focus sulle filiere agricole ed economia circolare con gli obiettivi della Missione 2.

Non solo, la Blockchain va oltre gli utilizzi che la sfruttano per avere certificazioni affidabili; una promettente area applicativa è quella relativa all'interoperabilità dei dati (Trusted Data Sharing), in questo senso possibili progetti e investimenti dovrebbero riguardare: l'identità digitale (con un'evoluzione e estensione dell'attuale modello SPID per tutti i servizi della PA), certificati di proprietà di asset fisici (auto, immobili) legati alla digitalizzazione della P, gestione dei dati della cartella clinica elettronica, dati delle cartelle cliniche personali in un *wallet* univoco e controllato dal cittadino, compresi dati

genomici e sanitari elettronici interoperabili, esplorando anche applicazioni nel supporto ai *claim* assicurativi legati alla sanità.

Un'ulteriore potenzialità *Blockchain-enabled* legata al PNRR potrebbe riguardare l'automazione decentralizzata processi ("Smart Contracts"). L'automazione tramite smart contract può portare notevoli vantaggi in termini di efficienza, liquidità e finalità dei processi controllati. Nella Missione 1, 2 e 6, abbiamo visto molti esempi di processi che potrebbero giovare di una automazione, alcuni esempi possono essere:

- finanziamenti pubblici a PMI sulla base di condizioni predeterminate;
- servizi digitali ai cittadini attivati tramite il soddisfacimento di alcune condizioni;
- crediti fiscali "sbloccati" tramite il raggiungimento di parametri di sostenibilità.

Si è voluto concludere il documento con una riflessione riguardante il legame tra la Blockchain è un'altra importante tecnologia in rapida espansione e che è anch'essa al centrale per la nostra Associazione, l'Intelligenza Artificiale. Si tratta di due tecnologie diverse ma accomunate dalla centralità dei dati; è quindi opportuno che siano considerate insieme nell'ottica del piano di Trasformazione 4.0, anche considerando l'impegno del Governo a sostenere l'iniziativa Gaia-X in cui la definizione dei Data space fornisce il contesto allo sviluppo e applicazione di IA come di Blockchain.

1. PARTE PRIMA – PROFILI GENERALI

1.1 Obiettivi del documento

In questo documento si riporta lo stato attuale della Blockchain, e la sua probabile evoluzione, attraverso le lenti delle piattaforme tecnologiche applicabili su larga scala in Italia. Presupposto di base di questa analisi è che oggi ci si trovi in una finestra di opportunità senza precedenti per lo sviluppo e l'attuazione di soluzioni abilitate da questa tecnologia. L'ecosistema Blockchain negli ultimi anni è maturato costantemente e i progetti stanno acquisendo dimensioni sempre più significative: osservare, quindi, l'evoluzione delle applicazioni e l'elaborazione normativa – in particolare quella europea – ci consente di identificarne le principali sfide e i fattori di successo.

Lo sviluppo del commercio mondiale è stato il più grande creatore di ricchezza nella storia umana. Nel corso degli anni le imprese hanno affrontato importanti trasformazioni nel modo di scambiare beni e servizi, i mercati si sono profondamente trasformati e ampliati fino a diventare "globali" grazie a un rete di trasporti sempre più capillare ed estesa, a tecnologie sempre più sofisticate e affidabili, alla diffusione del digitale che ha dematerializzato i tanti confini fisici. La *servitization* e la crescita del mercato dei servizi ha accompagnato il commercio dei beni materiali, cambiando anche la natura delle catene del valore globale.

Una trasformazione, questa, che ha portato con sé una crescente complessità dovuta al numero e al tipo di paesi e prodotti coinvolti, alla imponente mole di regole che imprese, intermediari, commercianti e da ultimo consumatori devono conoscere e rispettare. Per questo, ancora oggi molte transazioni restano inefficienti e, soprattutto, vulnerabili.

La sfida principale della Blockchain è di riuscire a ridurre l'attrito nel mercato, costruendo una nuova scienza dell'organizzazione che abiliterà nuovi modelli di interazione tra imprese, consentendo così al Paese di avere un trampolino di lancio per incrementare le opportunità di lavoro e per creare ricchezza.

Lungo le pagine descriveremo quali fattori, tecnici e organizzativi possano modellare le piattaforme; e faremo alcune osservazioni e raccomandazioni per i cittadini, gli imprenditori e i responsabili delle politiche sulle base delle migliori pratiche. Si illustreranno le opportunità di utilizzo della Blockchain, quale strumento in grado di sostituire la tradizionale tecnologia di database. Inoltre, si delineeranno solidi impianti di governance in grado di fornire chiarezza su ruoli e responsabilità, in modo da facilitare la collaborazione e la condivisione tra le diverse parti interessate.

Concluderemo con una serie di raccomandazioni. Il Governo nel giugno 2020 ha promosso la costituzione di un gruppo di esperti per definire una Strategia per la Blockchain. Un percorso virtuoso che richiede oggi di passare dall'analisi e dalla visione, all'attuazione e allo sviluppo. L'Italia ha già un *track record* relativamente buono nella materia, ma per garantire la sua posizione di leader in questa nuova tecnologia, si dovranno sostenere gli investimenti su soluzioni di prossima generazione, consapevoli che, con la maturazione della Blockchain, aumenterà la necessità di standard sia per la tecnologia sia per la governance della stessa.

Riteniamo che in ogni caso ci sia bisogno di un approccio leggero e aperto al cambiamento, che sia effettivamente e indiscutibilmente a favore dell'innovazione, per consentire la sperimentazione. In tal modo il Paese sarà preparato alla potenziale adozione di massa di questa tecnologia.

1.2 Introduzione

Nel corso della storia, gli strumenti di fiducia – come monete, banconote, lettere di credito e sistemi bancari – sono nati per facilitare lo scambio di valore e proteggere gli acquirenti e i venditori, così hanno favorito le transazioni e quindi l'efficienza del mercato.

L'effetto sincrono dell'avanzamento tecnologico e della globalizzazione ha portato i volumi delle transazioni a crescere in modo esponenziale – si pensi, ad esempio, all'ascesa dell'Internet of Things. Per affrontare queste sfide, il mondo ha bisogno di reti di pagamento veloci e affidabili che forniscano meccanismi per stabilire la fiducia garantendo la trasparenza.

Una soluzione che è stata sviluppata per affrontare l'abuso di potere, la complessità, le inefficienze e i costi delle transazioni corrente è Bitcoin, ossia il sistema lanciato dallo pseudonimo Satoshi Nakamoto. È importante a questo punto chiarire che Bitcoin e Blockchain non sono la stessa cosa: Blockchain fornisce i mezzi per registrare e archiviare Bitcoin, ma la Blockchain può avere altri usi oltre a Bitcoin. Bitcoin non è altro che il primo caso d'uso di successo di questa tecnologia.

1.2.1 Cos'è una Blockchain?

Si tratta di un registro permanente del consenso che abbiamo raggiunto sullo status di una risorsa. È un marcatore temporale, quindi è solo una conseguenza del precedente, e ben più importante, consenso. Ivi è scritta la relazione tra il proprietario e la risorsa (se la possiede o controlla, se ha l'accesso ecc.). È chiamata "Blockchain" in quanto memorizza i dati delle transazioni in blocchi legati come in una catena. Blockchain è una delle principali scoperte tecnologiche dell'ultimo decennio. Una tecnologia che consente alle persone e alle organizzazioni di raggiungere un accordo e registrare in modo permanente le informazioni senza un'autorità centrale.

1.2.2 La nascita della Blockchain

Blockchain non è solo una nuova tecnologia che si può racchiudere in un singolo concetto. Originariamente inventata come la tecnologia a supporto dei trasferimenti dei bitcoin, negli ultimi dieci anni si è evoluta in molte direzioni, assumendo una miriade di forme e affrontando una lista apparentemente infinita di casi d'uso. Questo registro, replicato tra tutti i nodi e immutabile, facilita il processo di annotazione delle transazioni riguardanti le risorse. Queste ultime possono essere tangibili (una casa, una macchina,

contanti, ecc.) o immateriali (proprietà intellettuale, brevetti, diritti, marchio ecc.). Ciò ha implicazioni significative sul modo in cui pensiamo a molte delle nostre istituzioni economiche, sociali e politiche.

1.2.3 A cosa serve?

Blockchain può essere utilizzata per decentralizzare e automatizzare i processi in un gran numero di contesti. Le caratteristiche della Blockchain consentono a un gran numero di individui o entità, siano essi collaboratori o concorrenti, di raggiungere un consenso sulle informazioni e di memorizzarle immutabilmente. La Blockchain è importante perché ha il potenziale di trasformare le istituzioni e le strutture economiche, sociali e politiche fondamentali attraverso il meccanismo del decentramento. Come dimostra il successo del Bitcoin, la Blockchain offre un mezzo tecnologico relativamente facile per creare grandi mercati diretti, ossia *peer-to-peer*, per prodotti, servizi o informazioni, mettendo in discussione il ruolo degli attuali intermediari.

Ci sono tuttavia altre distinzioni utili. La prima si fonda sulle differenti possibilità di accesso e interazione con la Blockchain. Bitcoin è un esempio di Blockchain "senza autorizzazione": chiunque può leggere i dati e diventare parte della rete o fungere da “validatore”. Le Blockchain senza autorizzazione rappresentano la forma più decentralizzata di Blockchain, ma le Blockchain possono anche essere utili con un numero più limitato di soggetti, come nel caso delle implementazioni autorizzate (permissioned) di Blockchain. "Autorizzato" significa che l'accesso è in qualche modo limitato, ad esempio consentendone l’accesso solo a un determinato gruppo di partecipanti o validatori registrati.

Con i metodi tradizionali per registrare transazioni e tracciare le risorse, i partecipanti di una rete mantengono privatamente i loro registri; si tratta di un metodo che può essere costoso, perché coinvolge per lo più intermediari che applicano tariffe per il servizio offerto.

È anche vulnerabile, perché un sistema centrale (per esempio, una banca) può essere compromesso a causa di frodi, attacchi informatici o per errati comportamenti umani.

Da questo punto di vista, la Blockchain può rappresentare una soluzione utile proprio per aumentare il livello di fiducia di tutti i partecipanti alla rete, perché fornisce con la crittografia una prova su un insieme di transazioni, le quali non non possono essere manomesse, rendendo visibile qualsiasi azione di corruzione.

L'architettura Blockchain dà ai partecipanti la possibilità di condividere un libro mastro che viene aggiornato attraverso la replica peer-to-peer ogni volta che si verifica una transazione. La replica peer-to-peer comporta che ogni partecipante (anche chiamato nodo) possa ricevere o inviare transazioni ad altri nodi, e che i dati siano sincronizzati attraverso la rete durante il trasferimento.

1.3 Definizioni/ Modelli di governance

1.3.1 Definizioni

In questo nuovo campo, la terminologia sta continuamente evolvendo, per cui i tentativi di definizione formale degli elementi chiave non sempre trovano l'accordo di tutti gli interlocutori. Ciononostante, a livello internazionale esistono varie iniziative che si sono poste proprio questo scopo, prima tra tutte, il lavoro in corso dell'organo internazionale per la standardizzazione ISO. Questo documento prende come riferimento il lavoro che si sta portando avanti nel tavolo tecnico ISO TC 307, riportiamo di seguito le definizioni per gli elementi principali:

- ***Blockchain***: la Blockchain è una tipologia di registro distribuito che organizza le proprie transazioni in blocchi (un raggruppamento di transazioni) e in cui ogni blocco è collegato al precedente tramite un collegamento crittografico, formando una catena di blocchi. Le transazioni nel registro sono ordinate e sequenziali. Una volta che una transazione è stata aggiunta ad un blocco questa non può più essere modificata o eliminata. L'inclusione di una transazione all'interno di un blocco avviene tramite un meccanismo di consenso predefinito tra i vari partecipanti alla Blockchain. Il registro dei blocchi è condiviso con tutti i partecipanti alla Blockchain.

- ***Registro Distribuito***: Registro che è condiviso tra i vari partecipanti al sistema, e che è sincronizzato tramite un meccanismo di consenso. Un Registro distribuito non necessità di una struttura a blocchi come la Blockchain, ma utilizza comunque una struttura ordinata e sequenziale, nel quale transazioni sono aggiunte solo dopo aver raggiunto il consenso tra i partecipanti secondo il meccanismo in funzione nel sistema. Sistemi di registri distribuiti possono anche non replicare tutti i dati tra tutti i partecipanti al sistema, ma possono anche "isolare" o selettivamente replicare i dati solo tra i partecipanti ad una determinata transazione (es. Corda, Hyperledger).

- ***Registri che non richiedono permesso (permissionless)***: Sistema Blockchain o di Registri Distribuiti che non richiedono alcun permesso per partecipare al sistema, quindi chiunque può parteciparvi. Un esempio di sistemi di questo tipo sono Bitcoin ed Ethereum. Questi sistemi non hanno una singola proprietà, anzi, tecnicamente non sono di "nessuno". Lo scopo di un sistema "permissionless" è quello appunto di permettere a chiunque di partecipare e di contribuire al sistema. Questo previene qualsiasi tipo di censura sui dati in quanto nessun attore può prevenire che una transazione venga aggiunta. Allo stesso tempo questi sistemi non hanno regole di gestione chiare e definite, non essendo gestite "da nessuno", e i partecipanti al sistema non sono conosciuti.

- ***Registri che richiedono permesso (permissioned)***: Sistema Blockchain o di registri distribuiti che richiedono permesso per partecipare al sistema, o nel quale almeno un ruolo all'interno del sistema richiede dei permessi per essere concesso. Comunemente questi sistemi possono essere di proprietà di una o più entità, quindi di norma i partecipanti in un sistema "permissioned" sono conosciuti

in quanto necessitano appunto di permesso per partecipare. Questi tipi di sistemi hanno regole di gestione ben definite determinare da chi gestisce il sistema.

- ***Smart Contract:*** Gli Smart Contract sono programmi per computer memorizzati in un sistema di registri distribuiti o Blockchain, dove il risultato di qualsiasi esecuzione del programma è esso stesso memorizzato nella Blockchain o sistema di registri distribuiti. Gli Smart Contract possono esser visti come le regole di business ("business logic"), applicate alle transazioni che vengono eseguite nella Blockchain o sistema di registri distribuiti. Gli Smart Contract possono in alcuni casi rappresentare dei contratti nel senso legale del termine, ma non sono limitati a questo. Gli Smart Contract possono essere usati per automatizzare processi all'interno del sistema di registri distribuiti o Blockchain, in base a delle condizioni sia interne che esterne al sistema. Quando uno Smart Contract utilizza dati esterni al sistema, si appoggia a quello che viene definito un Oracolo, che rappresenta una fonte di dati affidabile esterna al sistema, sulla base dei quali lo Smart Contract viene eseguito. Un tipico esempio di Smart Contract potrebbe essere una copertura assicurativa in cui al verificarsi di un determinato evento quantificabile (es. cancellazione di un volo, quantità di pioggia caduta), paga automaticamente l'assicurato senza possibilità di intervento da parte dell'assicurazione o di altra entità terza.

- ***Prova di esistenza:*** prova che un determinato dato sia esistito in un determinato punto nel tempo, e che da quel momento non è più stato modificato. Questo termine viene comunemente chiamato anche "notarizzazione" nel settore.

- ***Asset Digitale:*** Asset che esiste solo in forma digitale o che è la rappresentazione digitale di un asset fisico, chiamato anche "gemello digitale".

- ***Crypto Asset***: Asset Digitale implementato usando tecniche crittografiche.

- ***Crypto Valuta***: Crypto Asset progettato per funzionare come strumento di scambio di valore

- ***Token:*** Un Token in questo contesto si riferisce ad un crypto asset che è tenuto all'interno di un sistema di registi distribuiti o Blockchain. Un token è una rappresentazione di un asset o di una utility. Un token può rappresentare un qualsiasi asset che sia fungibile e scambiabile, come per esempio merci o punti fedeltà.

- ***Protocolli di consenso:*** Blockchain è una rete decentralizzata che non prevede alcuna forma di autorità centrale che svolga il ruolo di certificatore (l'autorita' centrale delle Blockchain permissioned si limita, infatti, a determinare chi può accedervi). In assenza di autorità centrale, i protocolli di consenso rappresentano il meccanismo mediante il quale i nodi della rete prendono decisioni quali l'accettazione e la concatenazione di un nuovo blocco

1.3.2 I diversi modelli di governance delle DLT/Blockchain: requisiti e obiettivi

In ambito internazionale, e in particolare a livello normativo, sono attive numerose iniziative finalizzate a oggettivare quali siano gli elementi costitutivi della governance di una DLT (Distributed ledger Technology), tanto sul piano puramente tecnologico, quanto su quello organizzativo. Ai fini del presente capitolo, possiamo tentare di definire la governance di una DLT come "l'insieme di una serie di processi e regole attuative finalizzati a determinare le condizioni affinché un sistema DLT, possa operare in relazione ad un determinato contesto".

Le tecnologie DLT, seppur basate su una logica comune di decentralizzazione di una serie di attività e ruoli, si differenziano tra loro lungo una serie di dimensioni che spaziano dall'ambito organizzativo a quello tecnologico che si riflettono in processi e regole di funzionamento di questi sistemi diversi l'uno dall'altro.

Sul piano applicativo, laddove si decidesse di adottare una DLT per la messa in atto di specifici casi d'uso e applicazioni, la scelta e la configurazione di uno specifico sistema DLT e la sua stessa configurazione dovranno attuarsi in ragione di criteri di scelta che tengano conto delle caratteristiche tecniche del sistema stesso, dei processi e delle regole di funzionamento (governance) dello specifico sistema DLT. Tale scelta, in termini generali, dovrà altresì garantire il rispetto delle leggi e delle normative di natura cogente per quanto relativo alle funzionalità e casi d'uso implementati nell'ambito del dato sistema DLT.

Per usi di natura privata, la scelta di uno specifico sistema DLT, nel rispetto dei vincoli e delle condizioni di cui sopra, può essere dettata da sole ragioni di opportunità commerciale e/o di natura competitiva. In tale contesto, pertanto, la presente strategia può costituire un utile quadro di riferimento.

In ambito pubblico, tanto la scelta, quanto la configurazione di un sistema DLT dovranno essere operate partendo dalla natura dei casi d'uso che dovranno essere messi in atto dal sistema. La dimensione funzionale dell'applicazione determina, cioè, la necessità che il sistema DLT sia configurato opportunamente, sia dotato di regole e processi in grado di supportare specifiche funzionalità, garantisca determinate caratteristiche prestazionali e di sicurezza, assicuri il rispetto delle normative, regolamenti e leggi in vigore. A questo proposito è auspicabile che, dati la pervasività della tecnologia DLT, il suo vasto potenziale applicativo e il potenziale impatto sul Sistema Paese in termini di competitività ed efficienza, i soggetti preposti alla definizione dei suddetti sistemi regolamentari si adoperino per creare le condizioni opportune allo sviluppo di tali soluzioni, anche attraverso fasi di sperimentazione in una logica sandbox.

Tale approccio si rende tanto più necessario quanto più la declinazione dei principi cardine della legislazione viene tradotta in regole e normative tecniche che sono state naturalmente costruite in accordo ai principi dell'attuale paradigma tecnologico. Quest'ultimo, infatti, è basato sull'esistenza di autorità centrali e di registri centralizzati, pertanto di difficile interpretazione quando riferite a un paradigma tecnologico fondato sulla decentralizzazione del registro e su un'architettura applicativa distribuita, come nel caso di sistemi DLT.

Si rende pertanto necessario definire una tassonomia dei sistemi DLT che possa essere utilizzata nella scelta dei sistemi, in grado di supportare l'implementazione di specifici casi d'uso in un dato contesto di riferimento. Laddove il sistema DLT sia utilizzato per l'implementazione di funzionalità di natura pubblica, sarà necessario definire specifici criteri di natura tecnologica e organizzativa che derivano da esigenze di garanzia e tutela dei diritti, di sicurezza nazionale, e di ruolo della pubblica amministrazione, che il sistema DLT dovrà soddisfare come condizione necessaria ma non sufficiente.

Tassonomia dei sistemi DLT

Per poter definire una tassonomia dei sistemi DLT occorre identificare delle dimensioni di classificazione. Tali dimensioni potranno avere una relazione di tipo gerarchico e dovranno essere in grado di comprendere tanto gli aspetti tecnologici quanto quelli di governance di un sistema DLT. Inoltre, esse dovranno garantire la copertura di tutti i criteri che un sistema DLT deve necessariamente soddisfare in ragione del dominio di utilizzo (es: uso privato, Pubblica Amministrazione), esigenza applicativa, quadro di riferimento legislativo e regolamentare, dimensionamento tecnologico, caratteristiche prestazionali. Tale tassonomia, in ultimo, dovrà essere in grado di indirizzare verso la scelta della tipologia di sistema DLT suggerito o richiesto, in base agli elementi sopradescritti.

In assenza di una tassonomia condivisa a livello normativo e ai soli fini di identificare le dimensioni rilevanti per gli scopi del presente documento, si introducono le seguenti dimensioni di classificazione:

- Criteri di accesso al sistema DLT.
- Natura ed entità della Decentralizzazione.
- Tipologia del Meccanismo di Consenso.
- Presenza, natura e funzione di un sistema basato su token.
- Tipologia di Ruoli richiesti dal sistema DLT
- Modalità di gestione delle modifiche della Governance.

Ognuna delle dimensioni di classificazione può a sua volta essere suddivisa in sottocategorie, funzionali a una migliore stratificazione dei sistemi DLT che possa rendere più efficace l'identificazione della tipologia di sistema DLT adatta al contesto applicativo e ai vincoli ambientali imposti da un determinato caso d'uso.

Criteri di accesso al sistema DLT

L'accesso a una DLT coinvolge una molteplicità di attori partecipanti e concorrenti all'esperimento di una transazione che rivestono diversi ruoli. Sulla base delle definizioni di cui sopra, in coerenza con i principi attualmente richiamati all'interno del Comitato

ISO-TC307-SG6, si possono identificare tre tipologie DLT all'interno del quale classificare un dato sistema DLT:

<table>
<tr><td colspan="2">PERMISSIONLESS

Non è necessaria alcuna forma di autorizzazione per svolgere qualsiasi ruolo previsto dalla Governance di un dato sistema DLT.</td><td colspan="2">PERMISSIONED

Almeno uno dei ruoli previsti dalla Governance del sistema DLT prevede una forma di autorizzazione.</td></tr>
<tr><td>PUBBLICO

Tutti i nodi che compongono i sistemi DLT sono in grado di leggere dati e sottoporre transazioni.</td><td>NON APPLICABILE</td><td>PUBBLICO

Tutti i nodi che compongono i sistemi DLT sono in grado di leggere dati e sottoporre transazioni</td><td>PRIVATO

L'accesso alla scrittura e all'invio di transazioni è sottoposto a una forma di autorizzazione.</td></tr>
</table>

Tabella 1, tipologie dei sistemi DLT.

L'appartenenza di un sistema DLT a una delle tre possibili categorie costituirà, pertanto, un cardine attorno al quale costruire una specifica governance. La gestione della governance stessa sarà, altresì, differenziata in funzione della classificazione di cui sopra.

Indirizzo Strategico

Per la realizzazione di applicazioni di uso privato non si ritiene necessario porre limitazioni cogenti alla scelta di un Sistema DLT in base ai suoi criteri di accesso. Laddove, nell'ambito di una specifica applicazione decentralizzata, sia necessario utilizzare, ai fini di una transazione, dati provenienti da registri centralizzati o decentralizzati di natura pubblica, il cui utilizzo debba necessariamente essere associato all'oggetto o agli attori della transazione, sarà necessario identificare un soggetto responsabile di tale associazione.

Nell'utilizzo di un sistema DLT all'interno di funzionalità/prestazioni erogate da soggetti direttamente riferibili alla Pubblica Amministrazione, si ritiene opportuno sottolineare quanto segue:

- qualora siano previste, per l'accesso alla prestazione, forme di autenticazione/identificazione basate su registri centralizzati gestiti da entità della

Pubblica Amministrazione, tali prestazioni dovranno essere erogate nell'ambito di sistemi DLT di tipo Permissioned.

- A secondadella natura della transazione, degli elementi informativi necessari alla verifica e alla validazione della transazione stessa, della presenza di registri gestiti da entità della Pubblica Amministrazione, alcuni specifici Ruoli potranno essere soggetti a forme di autorizzazione e alcuni elementi infrastrutturali del Sistema DLT scelto dovranno essere sotto il diretto controllo di entità di natura Pubblica indicate dal soggetto pubblico erogante la prestazione.

- In dipendenza della natura della transazione, della sua rilevanza giuridica, e di considerazioni legate alla tutela dell'interesse nazionale e alla sicurezza, la tipologia di Sistema DLT Permissioned potrà essere di tipo pubblico o privato.

1.4 Casi d'uso

I concetti di Distributed Ledger Technology (DLT), Criptovalute e Smart Contract hanno catturato negli ultimi anni l'attenzione dell'opinione pubblica generando clamore e elevate aspettative, in altri termini creando *hype*. L'accoglienza entusiasta, alimentata dal successo del Bitcoin (una delle applicazioni della tecnologia Blockchain) e dall'esplosione di potenziali use-case hanno permesso alla Blockchain di guadagnarsi l'etichetta di tecnologia *disruptive* nel settore privato e in quello pubblico.

Le applicazioni Blockchain possono avere una portata molto ampia e implicazioni di natura politica, economica, sociale, tecnica, legale o ambientale. Sono molteplici i settori potenzialmente interessati: commercio, produzione, energia, industria, sanità, Pubblica Amministrazione, turismo e servizi. Ma la Blockchain non segue un modello "one-size-fits-all": anzi, le opportunità e le potenziali sfide di impiego della tecnologia Blockchain dipendono fortemente dal contesto, dall'applicazione e da caratteristiche settoriali.

Il presente paragrafo raccoglie numerosi esempi di applicazione della Blockchain in ambito aziendale con l'obiettivo è quello di fornire un'ampia panoramica di esperienze relative a funzioni e settori industriali diversi.

1.4.1 Settore Agroalimentare italiano

La società oggetto di questa referenza è un'azienda toscana che fornisce olio extra vergine di oliva a piena tracciabilità di provenienza da vari paesi come Italia, Spagna e Grecia. L'azienda connette migliaia di coltivatori e ispeziona frantoi in tutta Italia con aziende di miscelazione, imbottigliamento e spedizione, tramite il suo innovativo sistema di tracciabilità.

L'obiettivo dell'azienda è quello di produrre e esportare olio extra vergine di oliva italiano (EVOO – Extra Vergin Olive Oil) di alta qualità con la miglior certificazione possibile, sia a livello delle singole materie prime sia a quello della lavorazione delle medesime. Nel corso degli anni, l'azienda ha accumulato molta esperienza nella gestione della tracciabilità dei propri prodotti e ha perfino sviluppato un'app in grado di tracciare ogni bottiglia d'olio extra vergine d'oliva prodotta, fino al luogo d'origine. Per soddisfare la domanda del consumatore di prodotti alimentari di alta qualità certificati, l'azienda impiega una soluzione Blockchain in Cloud di tipo Permissioned basata su tecnologia Hypherledger Fabric. Utilizza questa soluzione da oltre 4 anni per monitorare e tracciare il suo marchio di EVOO dall'impianto di imbottigliamento italiano fino al porto di arrivo negli USA, per tener fede all'impegno continuo a fornire sempre più trasparenza nella catena della fornitura alimentare.

Le sfide di business erano le seguenti:

1. soddisfare le esigenze dei clienti in termini di piena trasparenza sulla provenienza dell'olio extra vergine d'oliva, creando un'unica fonte di verità che rifletta l'origine delle spedizioni di EVOO dall'impianto di imbottigliamento al porto di arrivo negli USA;

2. ottimizzare processi e scambio d'informazioni tra l'azienda e i partner commerciali: coltivatori d'olive, impianti di trasformazione, controllo di qualità, impianti di confezionamento e distributori;

3. ridurre i costi d'esercizio delle attuali procedure di certificazione e i processi cartacei per il trasporto dall'Italia agli USA

I risultati ottenuti sono stati:

1. consentita la portabilità delle informazioni nell'ambito di buona parte della catena di fornitura del produttore, connettendo gli svariati software di produzione e gestione del trasporto delle varie aziende tramite le REST API per la Blockchain, in modo da aggiornare e ottenere informazioni nel ledger distribuito;

2. ridotti i costi d'esercizio e l'errore umano, automatizzando ciascuna fase della tracciabilità: dall'impianto di imbottigliamento in Italia fino ai porti USA, aumentando la fiducia reciproca, la disponibilità a condividere le informazioni e la collaborazione per raggiungere obiettivi comuni;

3. implementati smart contract per stabilire termini commerciali e fornire alle parti accesso a una documentazione immutabile dei propri accordi, riducendo in tal modo i ritardi lungo la catena di fornitura e allo stesso tempo eliminando le controversie relative ai contratti e agli errori applicativi, aumentando fiducia e collaborazione all'interno della catena di fornitura.

Implementazione: l'Azienda ha iniziato a utilizzare in autonomia la Blockchain platform partendo da una semplice "proof of concept" agli inizi del 2018. Sono bastati 6 mesi dall'analisi di progetto e pianificazione a giugno 2018 fino alla prima spedizione di olio dall'impianto italiano per essere tracciata fino al porto negli Stati Uniti tramite Blockchain a gennaio 2019. La soluzione a tutt'ora è in produzione.

1.4.2 Settore Ittico

La supply chain del settore dell'industria ittica ha spesso attirato attenzioni negative su di sé a causa della mancanza di un sistema trasparente. Ad oggi, la supply chain del settore richiede processi – come quelli di registrazione – spesso manuali e suscettibili di errori. Inoltre, altre questioni che creano inefficienze nella supply chain del pesce sono le condizioni talvolta improprie di stoccaggio dei prodotti, truffe legate all'etichettatura e la presenza di pratiche non del tutto regolate.

A causa di questi problemi, la qualità e la sicurezza del prodotto che raggiunge i consumatori finali può essere compromessa e ciò minaccia la sicurezza economica del settore. In più, a causa del diverso tipo di frodi che possono essere messe in pratica lungo la supply chain, la fiducia tra venditori e consumatori è carente.

La tecnologia Blockchain può rivelarsi una panacea per i problemi di *verification* del settore ittico, consentendo di tracciare la merce dalla produzione alla distribuzione. Nomi importanti come Hyperledger hanno iniziato a usare questa tecnologia per risolvere le numerose questioni aperte che danneggiano l'industria ittica.

Il progetto Hyperledger Sawtooth sta rivoluzionando le supply chain portando tracciabilità e responsabilità attraverso la sua piattaforma Blockchain modulare. Viene utilizzato l'algoritmo di consenso PoET (proof of elapsed time) che permette agli attori coinvolti nel sistema di raggiungere un consenso in una situazione in cui le controparti non sono a conoscenza di informazioni riguardanti ciascuna di esse.

Sawtooth nell'industria del pesce permette al prodotto ittico di essere individuato nella supply chain attraverso dei sensori che trasmettono la posizione nello spazio e nel tempo dei prodotti della Blockchain. Questo permette ai compratori di accedere ad un registro comprensivo della provenienza del prodotto.

1.4.3 Settore del caffè

La supply chain del caffè è più lunga e complicata di quanto i consumatori possano pensare. La complessità risiede nel fatto che le coltivazioni si trovano spesso in aree del mondo remote e in via di sviluppo; in più, i prezzi volatili della merce e l'effetto dei cambiamenti climatici ne aumentano i profili di complessità. Inoltre, visto che il primo luogo di produzione sono spesso i paesi in via di sviluppo, non è raro che vengano riportati episodi di abusi e sfruttamento della forza lavoro.

La complessità del sistema fa della supply chain dell'industria del caffe un caso di studio ideale per comprendere il ruolo della Blockchain nel rendere più efficiente e trasparente l'intero processo.

Una startup di Denver (Colorado, USA), Bext360 sta utilizzando la Blockchain attraverso il suo macchinario "bextmachine". La macchina – utilizzando tecnologie di machine vision – è in grado di analizzare i chicchi di caffè (fino a 50 kg al minuto), elaborando un profilo di qualità per ogni produttore, i sacchi di caffè di vengono poi "tokenizzati" in modo da renderli tracciabili.

L'utilizzo della Blockchain nella supply chain del caffè porta ad avere ritorni in produttività, accordi equi con i produttori e trasparenza nell'intero sistema. Questo perché l'utilizzo della Blockchain, da un lato, assicura pagamenti diretti agli agricoltori non appena i prodotti vengono venduti, dall'altro, permette ai clienti di poter sempre controllare le informazioni relative alla tracciabilità del caffè che comprano.

1.4.4 Settore Moda

L'azienda oggetto di questo *use case* è un noto marchio con filiali in diversi paesi del mondo e continenti. Nonostante gli sforzi di alcuni marchi di moda per imporre condizioni di lavoro sicure e oneste nelle fabbriche da cui acquistano, resta ancora controverso il livello di attività svolte in regime di subappalto. La missione dell'azienda in oggetto è consentire ai propri clienti produttori di fornire visibilità alla catena di approvvigionamento tramite un'applicazione Blockchain che consente ai consumatori di sapere esattamente chi ha realizzato i loro prodotti, da quali materiali e in quali condizioni.

La società è riuscita a lanciare il progetto su Blockchain in soli 12 mesi. I primi clienti dell'azienda includono un designer messicano di scarpe intrecciate in pelle (eticamente artigianali) e un'etichetta tedesca di "moda equa" che utilizza un'app per mappare, verificare e archiviare le attività dei suoi fornitori. L'azienda archivia i dati in un database multi-modello disponibile in cloud, insieme a una *suite* di strumenti analitici necessari alle valutazioni; memorizza una varietà di documenti in formato JSON collegati all'applicazione, incluse copie di ordini effettuati da marchi con fornitori e immagini associate a prodotti, componenti, marchi, fabbriche, aziende agricole e così via. Avere l'infrastruttura, il database e l'applicazione Blockchain in esecuzione su un'unica piattaforma ha reso molto più facile espandere la piattaforma dell'Azienda, in modo celere e su larga scala.

Grazie a una architettura a microservizi, l'applicazione: acquisisce rapidamente immagini di fabric, integra nuovi fornitori o aggiunge ordini alla Blockchain. Il suo Container Engine per Kubernetes consente di eseguire più istanze contemporaneamente anche quando l'applicazione riceve migliaia di richieste contemporaneamente. Si tratta di una soluzione che può scalare in tempo reale grazie al Cloud, laddove siano necessari più capacità elaborativa e/o spazio d'archiviazione. Anche il networking e il backup sono altamente automatizzati, consentendo al cliente di avvalersi di un piccolo team di sviluppo, snello e concentrato su soluzioni aziendali, che aggiunge valore ai loro Clienti anziché coinvolgerli nella gestione operativa.

1.4.5 Settore Logistica

La soluzione Blockchain è utilizzata da un consorzio di aziende e fornisce il servizio per la gestione delle spedizioni globali in modo da consentire a spedizionieri, destinatari, fornitori di servizi logistici, NVOCC (Non Vessel Operating Common Carrier) e vettori marittimi di migliorare la pianificazione dei flussi e le consegne. Collegata a oltre 40 vettori marittimi, l'azienda sfrutta anche le fonti di big data e una piattaforma basata su cloud per offrire programmi di navigazione pluripremiati, visibilità, documentazione, gestione dei contratti, conformità e soluzioni di benchmarking.

La soluzione Blockchain è stata implementata per migliorare la gestione dei documenti nelle spedizioni, per migliorare i complessi processi della catena di approvvigionamento sfruttando una soluzione digitale affidabile nel settore delle spedizioni e della logistica che coinvolge spedizionieri, vettori, camionisti fino ad arrivare alle agenzie doganali. Il risultato è un'unica "versione della verità" e un *audit trail* immutabile a bassa latenza.

I processi di gestione dei documenti di spedizione sono infatti complessi e includono processi cartacei spesso datati che coinvolgono molti interlocutori in diversi paesi del mondo. Inoltre, le aziende di spedizioni globali hanno capacità tecniche e standard di dati molto diversi tra loro e scambiano documenti in formati spesso diversi, tra cui e-mail, moduli online e Electronic Data Interchange (EDI). In media, una singola spedizione può comportare più di 30 documenti scambiati da piu' parti, spesso con più revisioni dovute a errori umani, prima che la merce lasci il porto.

La soluzione Blockchain adottata semplifica il processo di documentazione di spedizione e aumenta la fiducia e l'efficienza nel sistema. Collegato tramite una piattaforma in Cloud di documentazione Blockchain, l'intero ecosistema di spedizione può ridurre le controversie, evitare sanzioni tardive da parte delle agenzie doganali, accelerare i tempi di consegna della documentazione e gestire meglio eventuali costi di fermo e/o penali. L'azienda ha stimato una riduzione del 65% del tempo necessario per raccogliere, consolidare e confermare i dati da più parti e per gestire i dati di spedizione ripetitivi in diversi documenti.

La gestione dei documenti è particolarmente estesa per i caricatori e i loro fornitori di servizi logistici con carichi specializzati. Ad esempio, la spedizione di merci pericolose richiede numerosi certificati per affermare che le merci dichiarate sono classificate e imballate correttamente. Alcuni dei contenuti del documento di spedizione vengono compilati ripetutamente in diversi moduli di dichiarazione. La soluzione Blockchain adottata riduce il rischio di dichiarazioni errate e accelera il processo di archiviazione, oltre a permetterne una rapida e immutabile verifica a posteriori, per qualsiasi motivo.

Inoltre, quando i documenti vengono presentati in modo accurato e tempestivo, il carico può procedere con il suo piano di spedizione secondo i programmi previsti, con effetti positivi anche sui costi di assicurazione dei trasporti stessi.

La tecnologia Blockchain fornisce *record* immutabili e una rete affidabile, permissioned in questo caso, per garantire documentazione sicura e tracciabile. Una soluzione per le

parti della supply chain per compilare automaticamente informazioni ripetute e verificate può aumentare notevolmente la precisione e l'efficienza dei dati per l'intero processo logistico. Nel caso specifico, inoltre, sono stati implementati dei “canali digitali” che permettono viste differenziate sui dati riservate alle diverse aziende parte della Blockchain.

1.4.6 Settore Automotive

In ambito automotive la Blockchain può essere considerata come una chiave che può aprire una vasta gamma di esperienze legate alla mobilità, sia per i clienti sia per i *manufacturer*. Per sfruttare appieno questo potenziale sarà necessario dotarsi di nuove soluzioni per consentire ai veicoli di interagire con un ecosistema molto diversificato di tecnologie e servizi, grazie al quale l'intero settore potrà sviluppare nuove modalità per monetizzare i propri dati e le proprie esperienze maturate lungo la catena del valore.

Figura 1, Evoluzione dei veicoli “connessi”.

Il passaggio dalla modalità tradizionale all’interazione a livello di ecosistema richiederà alle case automobilistiche e ai loro fornitori di reinventare il modo in cui veicoli, componenti e software interagiscono con il mondo esterno, posizionando i propri prodotti al centro di ogni transazione, tecnica o commerciale che sia. Ciò sarà possibile tramite tre aspetti chiave: **Digital Twin & Thread dei Veicoli**, **Network di Supply Chain** e **Trusted Digital Mobility Marketplaces**.

Digital Twin & Thread dei Veicoli.

La tecnologia Digital Twin e Thread, applicata alle auto, ai loro componenti e al software, aiuta a ottimizzare la catena del valore, oltre ad aumentare il valore di rivendita delle auto usate tramite certificati di manutenzione. Tutta la storia del veicolo, dalla culla alla tomba, può acquisire un valore economico, “monetizzabile” se considerato a livello di ecosistema. L’applicazione della Blockchain in questo ambito permetterebbe inoltre di creare un registro pubblico decentralizzato, trasparente e condiviso per la gestione dei

ricambi degli automezzi alimentato con dati la cui provenienza e qualità possono essere valutate in modo trasparente.

Oltre al tracciamento degli attori e degli asset, la Blockchain può essere usata per ridurre le attività manuali dovute – ad esempio - alla riconciliazione dei dati e/o documenti e contrastare i fenomeni di contraffazione e mercato nero, ad avere il controllo della «seconda mano», oltre che avviare meccanismi di premialità per i clienti virtuosi che scelgono di acquistare componenti autentici

Network di Supply Chain

Le auto moderne sono frutto di component hardware e software. In un contesto informatico, dove si ha la tendenza a rompere i data-silos appannaggio di architetture lightwave a microservizi, la Blockchain ha un approccio in controtendenza volto a colmare il vuoto applicativo, collegando le varie sorgenti dati dei partner in un ecosistema trasparente e real time.

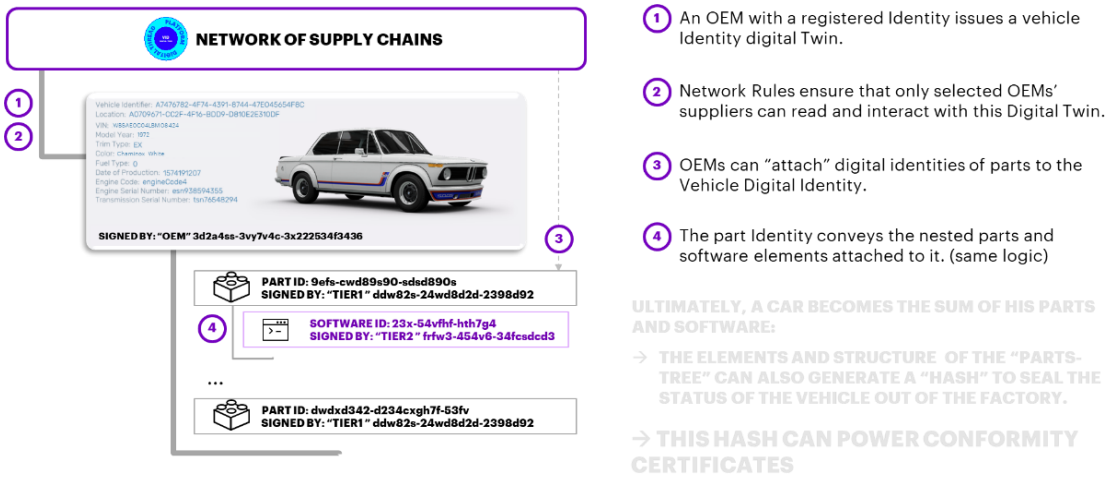

Figura 2. Scheda di funzionamento di un network di supply chain.

I sistemi multi-party, come le Blockchain e i Distributed Ledger, possono aiutare *manufacturer*, OEM e rispettivi partner a creare delle "zone di fiducia" tra le rispettive catene di fornitura in cui le informazioni di interesse vengono condivise tra i vari membri.

Trusted Digital Mobility Marketplaces

Le Digital Twin e Digital Thread, unite al Network delle Supply Chain abiliteranno nuovi modelli di business aperti ad altri attori che, operando in un contesto aperto e trasparente, possono partecipare traendo profitti.

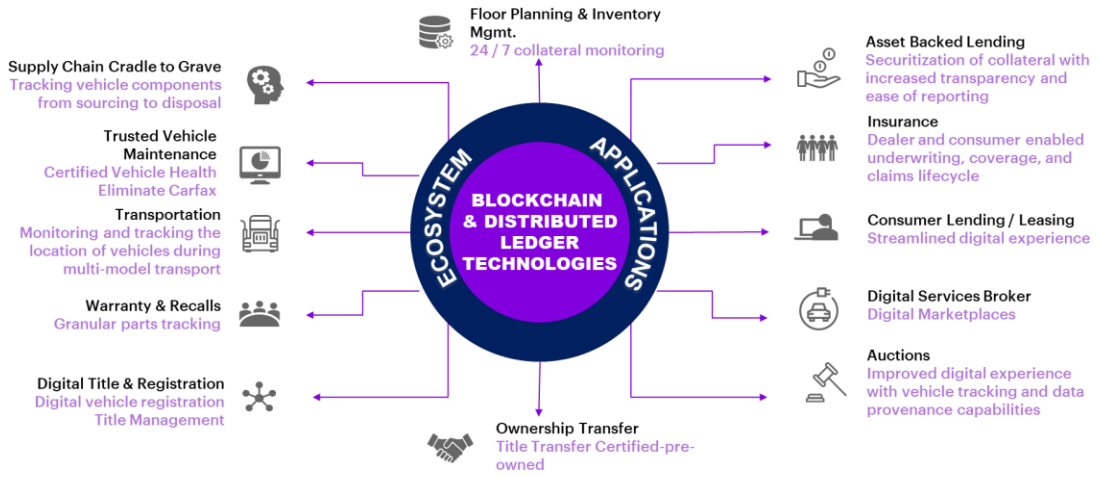

Figura 3, Schema di applicazioni della Blockchain nel mondo automotive.

A tal proposito è possibile citare come esempio

- The **Institutes RiskStream™ Collaborative**, un consorzio di player attivi in ambito Assicurativo che ha adottato la Blockchain per determinati *use case* legati al mondo Automotive, tra i quali la **First Notice of Loss** e la **Proof of Insurance**.

- Il **MOBI**, acronimo di "Mobility Open Blockchain Initiative", consorzio attivo con i suoi working group su sei aree tematiche:

    - **Vehicle Identity (VID)**, guidato da Renault, Ford e BMW con il supporto di Honda, Accenture, IBM e l'Hyperledger Foudation che ha l'obiettivo di definire una identità digitale verificabile del veicolo, utile per stabilirne l'esistenza, il controllo degli accessi, confermare la cronologia della proprietà e gli eventi chiave del ciclo di vita.

    - **Usage Based Insurance (UBI),** guidato da Ford, GM, Honda e Volkswagen con il supporto di Accenture, IBM, Reply, Swiss Re, che ha lo scopo di definire le regole e gli standard da seguire nell'adozione di un modello di assicurazione legata all'uso del veicolo

    - **Electric Vehicle Grid Integration (EVGI),** guidato Honda e General Motors (GM) cion il supporto di Accenture, AWS, IBM, Pacific Gas & Electric (PG&E) il Politecnico di Torino e altri partner, che ha lo scopo di incrementare e diffondere l'adozione di veicoli elettrici rendendo interoperabili le infrastrutture delle nazioni, player di industry, player di e-mobility e utilities in maniera da ottimizzare le reti e conseguire gli obiettivi di decarbonizzazione del pianeta.

- **Connected Mobility Data Marketplace (CMDM),** guidato da General Motors con il supporto di Accenture, Continental, IBM, Reply, e Toyota Insurance Management Solution (TIMS), che ha lo scopo di abilitare un marketplace digitale aperto a tutti i player – dai manufacturer agli assicuratori, dove far confluire la domanda e l'offera di un bene, non limitato al Vehicle-2-Grid (es. Vehicle to X Data Exchange).

- **Finance, Securitization, and Smart Contracts (FSSC)** per definire gli standard di interoperabilità in un ecosistema di Mobility-Finance

- **Supply Chain**, guidato da BMW e Ford con il supporto di Accenture, AWS, CEVT, IBM, IOTA, Marelli e altri partner che ha lo scopo di definire standard di interoperabilità e applicazioni della Blockchain in tutta la catena del valore relativa alla filiera automobilistica – dall'approvvigionamento, alla logistica e finanza e contabilità, inclusi gli OEM, fornitori e partner commerciali.

- Il **Blockchain in Transport Alliance (BiTA)**, dove centinaia di aziende attive nella global logistic sono unite in questo consorzio per discutere, ideare e definire gli standard Blockchain per il trasporto.

1.4.7 Settore Difesa e Aerospaziale

All'interno del settore "Difesa e Aerospaziale" si stanno esplorando nuovi modi di business legati a un nuovo modo di condividere i dati abilitato dai Distributed Ledger. Le aree di applicazione sono le seguenti:

Area di applicazione	**Problema**	**Soluzione "Blockchain-enabled"**
Servizi Post Vendita & After Market per gli OEM	Gli OEM cercano nuovi modelli di business in grado di andare oltre ai modelli tradizionali.	Grazie alle DLT è possibile garantire la legittimità delle informazioni, inclusa la qualità dei ricambi attraverso le registrazioni immutabili e la cronologia delle manutenzioni eseguite.
Trade & Supply Chain Financing	Gli OEM sono fortemente dipendenti dagli attori della Supply Chain e Terze Parti che ne gestiscono l'approvvigionamento.	La trasparenza e l'immutabilità offrono nuovi modelli di business basati sulla Proof-of-Ownership.

Indisputable Invoice	Le aziende subiscono perdite a causa dei mancati pagamenti e/o dispute sulla catena ordini-consegne-fatture-pagamenti, ad oggi risolto tramite attività manuali di controllo fortemente time-consuming.	La digitalizzazione degli asset (Ordini, Consegne, Fatture e Pagamenti) ed il tracciamento all'interno dell'ecosistema consente una riduzione dell'effort e la possibilità di automatizzazione tramite -smart contract
Supply Chain Network Resiliency	I dati organizzati in silos e/o applicazioni verticali, unite alla mancanza di connettività all'interno delle catene del valore inibiscono la tracciabilità e la provenienza delle merci.	Grazie al trust introdotto dall'utilizzo della Blockchain è possibile interconnettere le varie sorgenti e/o silos informativi, condividendo i dati tra i membri.
Shared parts depot	Per assicurare continuità nel servizio, le compagnie aeree devono mantenere riserve definite dei ricambi più importanti per le aeromobili.	Un network formato da grandi aeroporti potrebbe giocare un ruolo importante nella condivisione della disponibilità di questa tipologia di ricambi, a loro volta sfruttabili da molti partner e/o vettori.
Airline loyalty programs	I programmi fedeltà devono affrontare ritardi nella riconciliazione dei dati, oltre che far fronte a elevati costi amministrativi.	Un ecosistema basato su Blockchain, real time e disintermediato, semplifica le attività operative nonché gli aspetti legati agli exchange-rate tra i vari partner.
Certified Inspections for Leased Aircraft	Il processo di certificazione della qualità e conformità è cartaceo e time-consuming.	Registrare la manutenzione delle aerostazioni e velivoli all'interno della Blockchain può semplificare lo scambio delle informazioni e consentire l'automatizzazione dei controlli (ad esempio gestione dei bollettini tecnici)
Employee Certifications	Monitoring e Verifica delle qualifiche e/o certificazioni del personale.	Disporre sempre di un archivio affidabile e aggiornato di tutte le certificazioni dei dipendenti

Tabella 2, applicazioni Blockchain settore areospaziale/difesa.

Use case

La società in oggetto ha dimostrato interesse nell'applicazione della Blockchain per un sistema di monitoraggio della gestione avanzata dei ricambi e di interventi di manutenzione. L'imparzialità dell'autenticazione del dato, propria della Blockchain, risulta infatti una caratteristica cruciale nel processo di aggiornamento e condivisione di dati tra i fornitori dei servizi di manutenzione o della componentistica di ricambio, gli operatori sul campo e il cliente. L'utilizzo di una Blockchain privata risulta particolarmente adatto per tracciare in tempo reale il luogo e la motivazione degli interventi di manutenzione, siano essi periodici o straordinari.

Nel dettaglio, sono quattro gli enti coinvolti nel flusso primario degli eventi:

- Ente esecutore, incaricato di eseguire l'intervento di manutenzione
- Gestore rifornimento ricambi, incaricato di stilare la richiesta per la componentistica di ricambio
- Fornitore, incaricato della fornitura della componentistica di ricambio
- Ente autorizzatore, incaricato dell'autorizzazione degli interventi

Il flusso primario degli eventi si articola in cinque fasi (tra parentesi l'ente incaricato):

1. Notifiche assegnazione interventi (ente esecutore)
2. Eventi di ingaggio fornitore (gestore rifornimento ricambi)
3. Notifiche esecuzione interventi (ente esecutore)
4. Eventi spedizione / tracciatura materiale (fornitore)
5. Notifiche autorizzazione interventi (ente autorizzatore)

L'assenza di un ente esterno preposto alla certificazione dei dati consente un'assegnazione dinamica delle competenze, la registrazione pressoché immediata degli interventi e una razionalizzazione dei costi. Restano a disposizione di tutti gli enti coinvolti i dati, affidabili e aggiornati, sulle tempistiche di espletamento di ogni fase di una pratica. Ci si può, quindi, muovere agevolmente verso una gestione ottimizzata della manutenzione, analizzando le performance dei fornitori ma anche sviluppando algoritmi di manutenzione predittiva grazie a tecniche di AI/ML

1.4.8 Servizi satellitari

La società in oggetto, operante nel campo dei servizi satellitari, geo-informazione e sistemi di navigazione in rete, ha individuato diverse applicazioni della tecnologia Blockchain nell'ambito delle telecomunicazioni satellitari.

Introduciamo l'ambito dei servizi satellitari descrivendo brevemente le quattro tipologie di comunicazione satellitare:

- Satellite-to-Ground: per inviare i telecomandi (uplink) tra le stazioni a terra e i satelliti in orbita e ricevere (down link) i dati registrati ('payload', ovvero le immagini, telemetrie, stato del satellite, ecc.) dai satelliti. Tale comunicazione può avvenire esclusivamente nel lasso di tempo in cui un satellite si trova ad operare all'interno di un cono di comunicazione sovrastante la stazione a terra.

- Satellite-to-Satellite: poiché la comunicazione Satellite-to-Ground non è sempre possibile, è utile poter inviare telecomandi tra cluster di satelliti che condividono la stessa orbita.

- Ground-to-Ground: esistono diverse stazioni "Ground" sparse sulla superficie terreste che hanno la necessità di potersi interfacciare per gestire le richieste di uplink e downlink.

- Ground-to-User: il cliente finale ha la necessità di inviare la richiesta di acquisizione alla stazione a terra e di ricevere il payload una volta acquisito.

Le stazioni a terra sono gestite enti (statali, para-statali o privati) che mettono a disposizione, dietro compenso, l'utilizzo della stazione ad altri enti per le operazioni di uplink e downlink. La società in oggetto, ad esempio, gestisce il Centro Spaziale di Matera, una delle tre stazioni del Core Ground Segment dell'ESA, ma può dover ricorrere ad altre stazioni a terra nel caso in cui vi sia la necessità di eseguire operazioni di uplink o downlink con un satellite al di fuori del cono di comunicazione di Matera.

È quindi necessario poter certificare, in modo indipendente e con precisione, sia la durata di utilizzo di una stazione a terra che il flusso di dati scambiato tra il satellite e la stazione a terra. L'esigenza, opportunamente mutuata, è analoga per gli altri tre tipi di comunicazione satellitare.

Ci troviamo quindi in un tipico caso di applicazione della Blockchain: condividere e aggiornare informazioni tra soggetti appartenenti a enti diversi e aventi potenzialmente interessi contrastanti. Poter fare a meno di un ente terzo per certificare la veridicità dei dati va sicuramente incontro a una riduzione dei costi, ma non solo: trattandosi in alcuni casi di immagini militari classificate affidarsi a un ente esterno può non essere possibile.

Risulta quindi vantaggioso instaurare Blockchain di tipo consortium (o privato, ove necessario, si pensi all'ambito militare) per le quattro tipologie di comunicazione sopra citate.

Nello specifico sono state proposte le seguenti soluzioni:

- Satellite-to-Satellite: lo scopo è andare incontro alle nuove esigenze delle costellazioni di cubesat, microsat, fornendo la possibilità di instaurare comunicazioni Peer to Peer (P2P) per condividere i dati relativi all'orbita corrente, allo stato del satellite e soprattutto ai record presenti nel payload.

- Satellite-to-Ground: questo scenario può essere visto come estensione del precedente dove però anche le ground station diventano peer, in grado quindi di comunicare con la costellazione di satelliti instaurando canali per l'uplink dei telecomandi e il downlink delle immagini.

- Ground-to-Ground: sono state considerate le comunicazioni tra ground differenti o componenti software dello stesso ground per dare esecuzione a canali P2P protetti tramite Blockchain. In particolare, è stato sviluppato un communication system attraverso il quale i componenti possono registrarsi sulla Blockchain e scambiare messaggi e dati attraverso canali istituiti on-demand. Essi beneficiano del consenso globale grazie a una shared Blockchain che garantisce quindi un elevato grado di protezione. Per lo scambio dei dati è stato usato un file system distribuito.

- Ground-to-Users: si è studiato l'utilizzo della Blockchain per l'implementazione delle funzioni di authenication e authorization con la possibilità di creare dei federation agreement. In particolare, è stata sperimentata la parte di autenticazione per cui è stato implementato un sistema di Single Sign On basato su Blockstack.

1.4.9 Settore Farmaceutico

La supply chain del farmaco è una delle aree dell'ampio panorama "pharma" che può beneficiare maggiormente dalla Blockchain. Infatti, il tema dei medicinali contraffatti sta acquisendo una dimensione sempre più problematica tenuto conto che il mercato nero – che permette di fornire tali prodotti alle persone senza tracciamento – si sta espandendo. I rischi per la vita umana collegati all'assunzione di simili medicinali sono incalcolabili.

L'Organizzazione Mondiale della Sanità ha riportato un aumento vertiginoso nei ricavi dalle vendite di "fake drugs". Le popolazioni che soffrono di più il fenomeno della contraffazione sono quelle dei paesi in via di sviluppo dell'Asia e dell'Africa dove si stima che siano contraffatti dal 10 al 30 % dei farmaci sul mercato. Per questa ragione è di crescente importanza per i distributori e per i produttori il migliorare la tracciabilità e la sicurezza nella supply chain del farmaco.

Le vulnerabilità nella supply chain dei farmaci portano a molti punti dolenti come la scarsa visibilità per il tracciamento e l'autentificazione dei prodotti. L'introduzione della Blockchain in questi casi può portare diversi benefici. I prodotti possono essere etichettati con dei codici a barre e, una volta scannerizzati, i loro "records" possono

essere aggiornati in tempo reale durante il passaggio da un'entità all'altra nella supply chain. Le parti con autorizzazione all'accesso, tra cui i pazienti, potrebbero controllare tali registri in qualsiasi momento.

La natura immutabile della Blockchain fornisce la tracciabilità del farmaco dal produttore al consumatore e permette alle persone di controllare se il sistema ha avuto dei problemi in qualche punto del processo. Oltre ad assicurare l'integrità del prodotto e, quindi, evitare la contraffazione, la tecnologia Blockchain può aiutare a superare le difficoltà finanziarie che alcuni piccoli operatori e venditori al dettaglio affrontano durante la supply chain.

1.4.10 Settore Energy

Le aziende che operano nel campo dell'energia oggi si trovano di fronte a nuove sfide dettate dalle tematiche di fiducia/trust, globalizzazione e transizione energetica e decarbonizzazione. In questo contesto, la mancanza di visibilità e trasparenza nella catena del valore può essere risolta e semplificata tramite le piattaforme Blockchain, spesso in simbiosi con altre tecnologie come l'IoT e l'Intelligenza Artificiale.

In Italia, ad esempio, GSE ha deciso sviluppare delle proof of concept relative all'uso della Blockchain su tematiche di sostenibilità, sia per comprenderne i possibili vantaggi tecnologici, sia per capire quali evoluzione avrebbe potuto portare questa tecnologia, digitalizzando le due filiere energetiche rilevanti per il sistema paese: la filiera della ricarica di mezzi elettrici e alla filiera del biometano.

La Filiera Elettrica: un network di ricarica verde.

Per quanto riguarda il settore della mobilità e dei combustibili alternativi, la mobilità elettrica è oggetto di diverse critiche in merito all'effettivo contributo alla riduzione delle emissioni di CO_2 rispetto ai carburanti tradizionali, a causa principalmente delle fonti utilizzate per la produzione di energia elettrica e delle batterie. Per quanto queste critiche non siano prive di fondamento, dimostrano una visione limitata. Infatti, mentre da un lato è vero che è possibile, e necessario, fare di più (con l'utilizzo di energia 100% verde si può arrivare a una riduzione delle emissioni fino al 90%), già oggi con gli attuali mix energetici nazionali si hanno comunque delle riduzioni significative di CO_2 nell'intero ciclo di vita[1].

Vista la rilevanza dell'argomento, è stato sviluppato per la filiera eCar uno scenario che prevede la creazione di un network di ricarica verde che consenta di garantire che l'energia erogata dalle stazioni di ricarica sia almeno in parte verde. Al fine di incentivare l'utilizzo di energia verde per la ricarica, è stata ipotizzata una premialità che comporta l'erogazione di punti ("Token") calcolati sulla base dell'energia verde utilizzata dal cliente finale durante la ricarica del suo mezzo. Questi token possono essere utilizzati sia per

[1]Electric vehicles from life cycle and circular economy perspective, European Enviroment Agency. Disponibile online: https://www.eea.europa.eu/publications/electric-vehicles-from-life-cycle.

pagare successive ricariche del mezzo, sia possono essere spesi per acquistare prodotti e servizi da esercizi commerciali partner (e.g. Ristoranti).

Per rendere possibile tutto ciò, è necessario creare un ecosistema complesso che preveda la partecipazione di tutte le entità coinvolte nella filiera della mobilità elettrica, dai CPO (Charging point operator) agli eMSP (eMobility Service Provider), passando per i distributori di energia e i partner commerciali, fino ad arrivare al cliente finale. Il network di ricarica verde vede al centro il GSE, che oltre a certificare e abilitare i CPO e i partner commerciali a partecipare al network, gestisce tutta la parte di premialità. Inoltre, è prevista un'app dedicata nel quale i clienti finali possono visualizzare tutto il network di ricarica, i partner e gestire l'uso dei token. Per poter accedere al network di ricarica i CPO devono abilitarsi con GSE e devono rispettare la condizione di avere un contratto di fornitura di energia con garanzie di origine verdi e/o un'unità produttiva verde (e.g., pannello fotovoltaico).

All'interno del network, un ruolo fondamentale è svolto dagli eMSP, che continueranno a gestire tutto il processo di ricarica, ma saranno interfacciati con il GSE per la gestione degli account, l'aggiornamento della mappa delle colonnine e la generazione e utilizzo dei token; il cliente finale potrà acquistare i servizi e prodotti dei partner commerciali semplicemente utilizzando l'app GSE, all'interno della quale potrà selezionare i prodotti da acquistare e pagarli tramite un semplice QR code generato dal sistema.

La creazione di questo network, oltre a incentivare l'utilizzo di energia verde, grazie alle capacità di gestione di network complessi e all'integrazione della ricarica con la vendita di prodotti e servizi, può fungere da abilitatore di ulteriori forme di mobilità evoluta, in primis la smart mobility (mobilità intermodale).

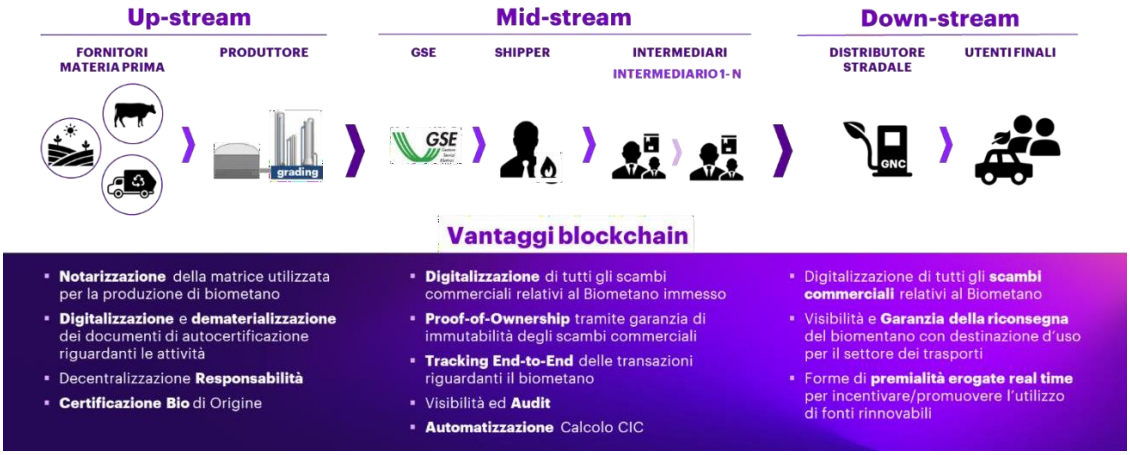

Figura 4. La Blockchain nel settore dell'energia.

La filiera del biometano

Il Biometano ad oggi non è particolarmente diffuso, tuttavia, il suo impatto sul futuro mix energetico sostenibile potrebbe essere molto rilevante. Il report "Outlook for biogas and biomethane: Prospects for organic growth" dell'IEA (Agenzia internazionale dell'energia), stima che i biogas potrebbero arrivare a coprire il 20% dell'attuale domanda mondiale di gas[2]. Inoltre, i biogas rappresentano una forma di carburante complementare a quella elettrica, trovando il loro utilizzo ideale nell'alimentazione dei mezzi pesanti a lunga percorrenza, per i quali l'autonomia e la velocità di rifornimento sono due fattori fondamentali. Lo sviluppo di biogas porterà inoltre allo sviluppo di nuovi modelli di business (e.g., «farming communities» o cooperative agricole per la produzione di feedstock), che garantiranno una gestione nettamente migliore degli scarti della filiera agricolo-alimentare.

Il biometano, diversamente dall'elettrico, ha tuttavia un grado di complessità superiore a livello di produzione e numero di attori coinvolti nell'ecosistema, se non altro per un grado di maturità "di sistema" inferiore. Infatti, nell'ecosistema biometano sono coinvolti una pluralità di attori originariamente non "affini", dai fornitori di materie prime (e.g., grandi complessi agricoli), passando per gli attori istituzionali come GSE e SNAM, fino ad arrivare ad attori più convenzionali, come shipper, intermediari, distributori e punti di erogazione.

Proprio per queste sue caratteristiche, l'uso della Blockchain in questo caso può essere un asset fondamentale: grazie alla sua natura distribuita e all'ampio utilizzo di smart contracts, è possibile regolare in real-time e senza bisogno di numerose rivalorizzazioni tutti i rapporti/transazioni fra gli attori della filiera, garantendo la certificazione e la tracciabilità del biometano. Anche per la promozione del biometano è stata previsto il medesimo sistema di premialità dell'elettrico per gli utenti finali che utilizzeranno il biometano per uso trazione, rafforzando l'idea di un ecosistema unico di mobilità sostenibile.

1.4.11 Settore Turismo e Viaggi

La rivoluzione digitale che ha investito l'ultimo decennio ha portato aziende, amministrazioni e organizzazioni a ripensare completamente i propri prodotti, servizi e modelli di interazione con i propri clienti/utenti, rispondendo così a esigenze e aspettative improvvisamente più sfidanti.

Il turismo è uno dei settori più economicamente rilevanti in modo innovativo e sostenibile: si tratta di un'industria dai mille indotti, capace da sola di avviare e sostenere il rilancio sociale, culturale ed economico di cui il Sistema Paese ha bisogno.

[2] IEA, 2018, "Outlook for biogas and biomethane: Prospects for organic growth". Disponibile online: https://www.iea.org/reports/outlook-for-biogas-and-biomethane-prospects-for-organic-growth

Un ecosistema potenzialmente aperto ed infinito, che coinvolge decine di settori come ad esempio:

- trasposti azionali ed internazionali (treni, aerei, navi, auto e autostrade);
- trasporti locali (autobus, metro, tram, autonoleggio, …);
- micromobilità (e-bike, monopattini, …);
- hospitality (hotel, b&b, case vacanze, …);
- ristorazione ed enogastronomia (bar, ristoranti, street food, …);
- intrattenimento (teatri, spettacoli, concerti, parchi tematici, acquari, …);
- sport/calcio (coppe e campionati nazionali/internazionali, sfide iconiche, …);
- eventi speciali (Palio di Siena, festival di Sanremo, fashion week, …);
- cultura (musei, mostre, siti archeologici,…);
- servizi diretti e indiretti (guide, organizzazione eventi, …);
- retail, local market & gdo (negozi, grandi firme, mercati, supermercati, …);
- artigiani (souvenir, botteghe locali, …);

Oggi il turista, anche inconsapevolmente, attraversa molti di questi settori affini al mondo del Turismo: ognuno di essi costituisce di per sé un'esperienza complessa che può esse arricchita se supportata da "casi d'uso" intelligentemente migliorati dalla tecnologia. La loro interconnessione eleverebbe a potenza l'esperienza del turista, sia esso un singolo viaggiatore, una coppia, una famiglia o, perché no, un normale residente turista per un giorno.

L'utilizzo di tecnologie basate su Blockchain abilita la costituzione di una piattaforma tecnologica a supporto dell'ecosistema del turismo su cui abilitare servizi funzionali e accessori all'ecosistema del turismo, secondo il paradigma tourism as a Platform.

Di seguito alcuni esempi di casi d'uso pensati per i diversi settori coinvolti in un tipico "journey" del turista:

Settore	Possibili applicazioni
Cultura (Musei, Mostre, Siti Archeologici, ...)	Profiling e Intrattenimento personalizzato (suggerimenti, percorsi dedicati, …), integrazione e gestione elettronica del Ticket, Scontistica e Loyalty, Integrazione con Social Media
Intrattenimento	Integrazione e gestione elettronica del Ticket, Scontistica e Loyalty, Integrazione con Social Media
Trasporti Nazionali ed Internazionali (Treni, Aerei, Navi, Auto e Autostrade)	Scontistica, Programmi di Loyalty dedicati e affiliati con i Vettori/Catene
Hospitality (Hotel, B&B, Case Vacanze, ...)	
Trasporti Locali (Autobus, Metro, Tram, Autonoleggio, …)	Gestione centralizzata degli account (no registrazioni/login dedicate per utilizzo dei servizi locali), Loyalty, Scontistiche, Integrazione e gestione elettronica del Ticket
Micromobilità (e-bike, monopattini, …)	
Ristorazione ed Enogastronomia (Bar, Ristoranti, Street Food, …)	Guide dedicate, Prenotazioni, Scontistica, Programmi di Loyalty dedicati
Servizi diretti e indiretti (Guide, Organizzazione eventi, …)	Accesso al catologo dei servizi, Integrazione e gestione elettronica del Ticket, Scontistica e Loyalty
Retail, Local Market & GDO (Negozi, Grandi Firme, Mercati, Supermercati, …), Artigiani (Souvenir, Botteghe locali, …)	Scontistica e Loyalty, Marketplace, Tax Refund

Tabella 3. Applicazioni della Blockchain in ambito turismo e cultura.

Tramite l'utilizzo di tecnologie innovative – come le Blockchain ed i Distributed Ledger – sarà possibile creare valore alla piattaforma per tracciare i consensi legati, ad esempio, ai processi di loyalty in grado di mettere in contatto tutti gli attori e i soggetti coinvolti in maniera trasparente e decentralizzata, così da facilitarne l'interazione e l'interoperabilità, anche grazie ad una serie di "contratti intelligenti" su una piattaforma di governance che consente ai diversi attori di agire in modo tracciato e sicuro

1.4.12 Settore Communication & Media

Il mondo Communication e Media può beneficiare dell'applicazione della tecnologia Blockchain in termini di Financial Infrastructure, Supply Chain, Decentralized Identity, Digital Rights Management e Digital Advertising.

Financial Infrastructure.

Fatturazione: gli smart contract possono disintermediare gli attuali processi di fatturazione, consentendo la riconciliazione dati e pagamenti automatici tra più roaming partner.

Supply Chain

Le soluzioni Blockchain consentono un controllo in tempo reale degli asset consentendone la tracciabilità end-to-end; la tecnologia utilizzata consentirà alle organizzazioni coinvolte di avere un'unica fonte dati certificata, sfruttando al contempo ulteriori aspetti abilitati dal modello a ecosistema, come il rilevamento delle frodi, la sostenibilità e l'analisi del successo delle operazioni con i clienti.

Decentralized IdentityCustomer Loyalty and Services: l'utilizzo della Blockchain consentirà di costruire un ecosistema dove ciascun attore può stabilire forme di premialità e logiche di earning/burning dei token.

Digital Rights Management

le piattaforme Blockchain, tramite il tracciamento, la verifica e i meccanismi di audit predefiniti, possono supportare la gestione e la distribuzione dei diritti, inclusi i pagamenti, finanziamenti, monetizzazione ed esecuzione dei contratti, abilitando l'ecosistema a un maggiore controllo dei contenuti digitali

Digital Advertising

Grazie alle piattaforme Blockchain è possibile eseguire il monitoring in tempo reale dei consumi e degli utilizzi in maniera incontrovertibile, abilitando così l'allocazione diretta dei compensi pubblicitari. La Blockchain può essere utilizzata per monitorare e verificare direttamente le *impression* degli annunci online, contrastando i fenomeni di frode pubblicitaria.

1.5 Contesto Normativo UE e stato dei lavori

1.5.1 Introduzione

Le tecnologie Blockchain e DLT si candidano quali possibili nuovi vettori di trasformazione dei sistemi economici e produttivi nonché delle pubbliche amministrazioni, promettendo un rapporto più trasparente tra cittadini e imprese attraverso una maggiore efficacia ed efficienza nell'erogazione dei servizi.

Sviluppare una visione di impatto di queste tecnologie, ovvero come possano cambiare le modalità in cui vengono gestite le informazioni e i processi, sta alla base della costruzione di una strategia programmatica. L'opportunità è l'abilitazione di un futuro di servizi più vicini alle persone e alle imprese, creando delle condizioni di maggior sviluppo e integrazione economica e sociale.

Trattandosi di tecnologie ancora in fase di completamento del proprio ciclo di sviluppo, è fondamentale maturare degli elementi di valutazione delle diverse opzioni di adozione disponibili, considerando gli specifici obiettivi dei relativi ambiti di applicazione.

Una regolamentazione efficace sarà inevitabilmente un presupposto fondamentale per l'implementazione di nuovi paradigmi di relazione tra amministrazioni e sistemi produttivi e sociali. La *governance* di modelli decentralizzati richiede policy condivise tra i partecipanti, nel rispetto di un ordinamento che rappresenti un quadro normativo stabilito per garantire gli interessi più ampi della società.

Le procedure della PA, del sistema economico e sociale richiedono certezza ed efficienza nelle transazioni informative e monetarie. In generale, i benefici appaiono rilevanti nel sostegno alla certezza del valore informativo e transazionale, assicurando la reperibilità di dati con piena validità giuridica e protetti da meccanismi che ne tutelano l'inalterabilità; si tratta di progettare un percorso di trasformazione compatibile con il modello giuridico di riferimento, garantendo la catena delle responsabilità e il sistema delle tutele.

Gli impatti della pandemia apparentemente non hanno modificato la strategia della Commissione europea in materia di Blockchain, che si sostanzia nella scelta di regolare il solo settore della finanza digitale e l'eGovernment, limitatamente ai servizi transfrontalieri. Nel documento programmatico per il 2021[3], la Commissione conferma la priorità delle proposte normative attualmente in sospeso e relative al settore della finanza digitale[4], mentre, in ambito PA, è tuttora attiva l'iniziativa European Blockchain Services Infrastructure (EBSI), finanziata dal programma Connecting Europe Facility (CEF), che mira a definire un set di standard per la realizzazione di un'applicazione in riuso (il c.d. Building Block) e garantire l'interoperabilità dei servizi pubblici transfrontalieri europei in ottemperanza al principio "una tantum"[5].

[3] COM(2020) 690 final.
[4] COM(2020) 594 final, COM(2020) 593 final.
[5] Regolamento (UE) 2018/1724.

A livello nazionale si segnala l'art. 8-bis del DL n. 135/2018 convertito in legge 11 febbraio 2019, n. 12che introduce e definisce le tecnologie basate su registri distribuiti e smart contract[6], stabilendone anche gli effetti giuridici. La normativa resta tuttavia inattuata in attesa della definizione degli standard tecnici, da adottare tramite linee guida di AGID.

1.5.2 Markets in crypto-assets regulation e il Digital Finance Package

Ci sembra opportuno, nonostante lo stadio ancora del tutto embrionale che ha la regolamentazione a livello EU della materia oggetto del presente white paper, operare un focus sulla già citata proposta normativa della Commissione Europea in ambito finanziario.

A fine settembre 2020, la Commissione Europea ha emanato una proposta di regolamento che avrà lo scopo di regolare il mercato dei crypto-asset: proposal of regulation for Markets in Crypto-Asset [7](MiCA). Questo nuovo atto si colloca nel quadro più generale del Digital Finance Package: un insieme di provvedimenti con lo scopo di sviluppare maggiormente la finanza digitale in termini di innovazione e competizione ma, allo stesso tempo, mitigare i rischi a essa correlati. Il MiCA è infatti accompagnato da altre due proposte di regolamento, le quali formano un trittico di regolamentazione del settore:

1. DLT Pilot Regime[8]

Questa proposta di regolamento avrà lo scopo di fornire i requisiti per le infrastrutture di trading e i sistemi per la liquidazione e compensazione delle security che si basano su tecnologie DLT. Tale "pilot regime", assimilabile a una regulatory sandbox quanto agli obiettivi perseguiti, si baserà su un sistema di permessi per operare su tali tipi di infrastrutture.

2. Digital Operational Resilience for Financial Sector (DORA)[9]

Lo scopo principale di questa ulteriore proposta è quello di rafforzare e armonizzare gli standard di sicurezza IT per la finanza digitale includendo quindi le soluzioni tecnologiche basate su Blockchain e Distributed Ledger che, chiaramente, operano attraverso tecnologie digitali e possono avere impatti sui consumatori a livello finanziario.

---

[7] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 COM/2020/593 final
[8] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a pilot regime for market infrastructures based on distributed ledger technology COM/2020/594 final
[9] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014
COM/2020/595 final

In particolare, avrà l'obiettivo generale di fornire un set unitario di regole per il settore (tenuto conto che, attualmente, le varie normative sono disciplinate in atti diversi come la direttiva NIS o le varie normative finanziarie EU). Tra gli interventi, vi è eliminare frammentazione del management della sicurezza IT, disciplinare i sistemi di reporting degli incidenti di sicurezza e fornire regole in tema di testing.

Fondamentale, per la Commissione, è assicurare certezza del diritto (il testo originale parla di "legal certainty") ecostruire un framework normativo di aiuto agli operatori del settore a operare nel mercato di riferimento. Secondariamente, il legislatore europeo vuole supportare l'innovazione, promuovere la protezione dei consumatori e degli investitori e infine garantire la stabilità finanziaria.

Tali fini sono chiaramente connessi al fatto che, almeno potenzialmente, i crypto-asset potrebbero causare instabilità al sistema finanziario nel suo complesso nonché, vista la frammentazione della regolamentazione, è ormai diventato urgente avere un quadro normativo di riferimento che sia uniforme per tutti i paesi dell'UE, chiaro e semplice per gli operatori del settore ed i consumatori.

In questo momento, infatti, non vi è certezza in merito al trattamento dei cypto-asset all'interno dell'UE ein particolare non è chiaro fino a che punto si applichi la normativa sugli strumenti finanziari..

In più, l'assenza di un quadro normativo e regolatorio comune a livello europeo mina la fiducia negli utenti verso l'utilizzo dei crypto-asset. Tutti elementi che, tra l'altro, limitano l'utilizzo degli "stable coin", i quali paiono essere lo strumento che garantisce stabilità ai prezzi di questi asset digitali e che potrebbero essere utilizzati largamente dal mercato e soprattutto dai piccoli investitori e risparmiatori.

Il regolatore europeo, in ogni caso, non punta a normare la tecnologia Blockchain e Distributed Ledger, ma dovrà semplicemente permettere le modalità di utilizzo della stessa per garantirne un uso sicuro. La legislazione non dovrà, quindi, favorire una specifica tecnologia o servizio ma essere maggiormente neutrale attraverso norme più generali e applicabili in molteplici situazioni. Allo stesso modo, dovrà essere "future proof" quindi essere aperta e capace di supportare gli sviluppi futuri di tecnologie che potrebbero nascere nei prossimi anni.

Pare ragionevole affermare che la strategia perseguita dall'Unione Europea sia quella di fornire un framework normativo che normi solo specifiche tipologie di token e crypto-asset che non sono assimilabili a degli strumenti finanziari quindi inserire normativa ad hoc all'interno di un quadro normativo già ben consolidato.

2. PARTE SECONDA – STRATEGIA E AZIONI RACCOMANDATE

2.1 Bottlenecks

La tecnologia Blockchain si sta affermando in modo dirompente nelle imprese, portando con sé un nuovo modo di validare e ottenere dati sicuri. Tuttavia, questa, non è esente da problematiche. In particolare, le aziende che intraprendono un percorso di implementazione di soluzioni Blockchain si ritrovano ad affrontare due macrotipi di problemi che creano dei colli di bottiglia nello sviluppo dei progetti; si tratta, da un lato, di problemi relativi al business e/o al management, dall'altro di problemi di natura strettamente tecnologica.

2.1.1 Bottlenecks legati al business

Le motivazioni che portano le aziende a cercare di mettere in pratica soluzioni *Blockchain enabled* sono molteplici, a titolo di esempio si possono citare: la necessità di ottimizzare i processi produttivi, la mancanza di "fiducia/sicurezza" nelle informazioni condivise con gli interlocutori esterni e/o addirittura con i fornitori dei fornitori, la necessità di proteggere processi e procedure interne all'azienda.

- Un tipico utilizzo della Blockchain a livello aziendale si ha quando si vogliono certificare dei processi di produzione, come ad esempio ISO 27001 sulla Information Security o il Modello 231 su rischi ambientali. Recentemente sono state introdotte soluzioni che, dall'interno di un database e adottando la tecnologia Blockchain, riescono "blindare" i dati rendendo impossibile la modifica di un dato scritto anche allo stesso Database Administrator. Più in generale, nei processi di "Governance, Risk & Compliance", la Blockchain porterà un valore aggiunto considerevole per il management permettendo di ottimizzare i processi di scrittura, revisione, approvazione, distribuzione e archiviazione di tutti gli adempimenti normativi richiesti.

  Certamente questo approccio cambierà il modo di lavorare perché limiterà pratiche che, pur essendo oggi considerabili come ordinarie, con l'introduzione della Blockchain non saranno più possibili. Ad esempio, non si potrà più cambiare un dato già scritto ma si dovrà aggiungerne uno nuovo (che avrà una marca temporale diversa), per una modifica potrebbe essere necessario un processo di approvazione e un livello di accesso ai dati superiori. La conseguenza di ciò è che **dovranno cambiare le procedure interne di accesso ai dati**.

Quando invece si considera il possibile impatto della Blockchain sull'intera catena del valore aziendale, sia a monte del proprio processo produttivo con i suoi fornitori che a valle verso i Clienti, le considerazioni di business ed i possibili bottlenecks sono ancora altri. Ci si può trovare di fronte ad almeno due modelli di attuazione:

a. in un caso si tratta di un'azienda "forte" che incoraggia la propria catena del valore ad adottare la Blockchain per scambiare le informazioni ed ottimizzare i processi produttivi;

b. più aziende, talvolta anche competitor tra loro, decidono di realizzare un consorzio e condividere le infrastrutture Blockchain per fare sistema.

Ciascuna di queste realtà presenta vincoli e opportunità diverse, ma in entrambi i casi i primi temi da affrontare e le domande a cui dare risposta sono molteplici ed in esse si nascondono possibili bottlenecks:

- Quale area produttiva può beneficiare di questa innovazione e quali i vantaggi di business?

- Quale potrebbe essere un progetto pilota significativo e con un rischio minimo?

- Che impatti avrà sulla strategia aziendale, sui processi di business, sulle persone, nella governance?

- Adottare la Blockchain mi darà un vantaggio competitivo e quali dei miei competitor lo stanno già facendo?

- Chi nella mia Azienda sarà in grado di tradurre nella Blockchain il know-how aziendale e quindi trasformare la tecnologia in *business value*?

Inevitabile sarà affrontare il **tema dei costi, considerando sia i costi tangibili sia quelli intangibili.** Tuttavia, mentre per i primi è verosimilmente più facile, o quantomeno la loro determinazione è oggettiva, per quelli intangibili è decisamente più complesso ed è necessaria una precisa volontà aziendale, un mandato importante, che voglia valutarli. Dopodiché potrebbe porsi il tema di come ripartire questi costi. Quindi se si pensa a una soluzione interna all'azienda diventa un discorso di Line of Business, mentre se si fosse in presenza di soggetti esterni potrebbe essere necessario stabilire delle metriche (costi per transazione, costi per documento ecc…).

- Un altro fattore da considerare sarà la tecnologia alla base della Blockchain che sceglieremo, vista però non tanto dal punto di vista delle performance o dei costi, bensì considerando l'ecosistema con cui la nostra azienda dovrà interagire. Sarà importante scegliere una tecnologia che permetta di interagire con aziende che oggi non sono presenti nella nostra filiera. È quindi importante scegliere uno standard aperto ove molti *software vendor* siano presenti, così da consentire una scelta tecnologica ampia che solo a quel punto consentirà di confrontare costi, servizi e funzionalità.

Un possibile standard di questo tipo è costituito dall'Hypherledger Fabric (HLF) della Linux Foundation Projects che oggi raggruppa oltre 170 entità di ogni ordine e grado che collaborano già da anni, che cresce e che rende possibile implementare soluzioni Blockchain sia on-premises che in Cloud che in modelli ibridi. In questo ecosistema, si potranno fare scelte di vendor e implementazioni diverse che nel tempo potranno essere estese o modificate, limitando il rischio di non riuscire ad integrare nuovi soggetti e

permettendo la sostituzione di un vendor qualora sia necessario e riducendone gli impatti su quanto già in essere.

2.1.2 Bottlenecks legati alla tecnologia

Le Aziende che si affacciano a questa tecnologia sono orientate a scegliere una tipologia di Blockchain privata (in gergo tecnico "*Permissioned*"). Tuttavia, nonostante le Blockchain private siano più performanti delle Blockchain pubbliche (dette anche "*Permissionless*"), alcune tipologie di Blockchain private rimangono ancora al di sotto del livello richiesto dalle imprese.

Problematiche tecniche che limitano le prestazioni della tecnologia Blockchain si diversificano in base alla piattaforma che si utilizza. Nonostante ciò, si possono generalizzare e identificare i problemi alla base di questa tecnologia. Di fatto i problemi relativi ai "bottleneck" sono spesso riconducibili all'elevato numero di transazioni che possono interessare una Blockchain e quindi alla scalabilità dei sistemi coinvolti; conseguentemente, ciò ha effetti sull'archiviazione dei dati oppure alla sua sicurezza e ai temi piu' strettamente connessi con il backup dei dati/blocchi.

1. Un primo possibile bottleneck da valutare nel medio periodo sarà la tipologia di implementazione: on premises o in Cloud?

Chiaramente una soluzione on-premises imporrà un dimensionamento dei sistemi, ma nel tempo rimarrà confinato nella dimensione scelta. Al variare del business e dell'utilizzo della Blockchain, il nostro sistema potrebbe essere stato sovradimensionato oppure non essere in grado di supportare tutto il traffico o le perfomance necessarie al business, richiedendo un ulteriore investimento per ampliarlo. Se nell'architettura sono inclusi soggetti esterni alla nostra Azienda, questi profili si ripercuoteranno su di essi sia in termini tecnologici che economici e, al momento della modifica, potrebbero avere impatti sui servizi.

Una implementazione in Cloud – intrinsecamente più scalabile – consente di rischiare di più, eventualmente "sbagliando" la configurazione iniziale e di assorbire agilmente le mutate necessità di business. Anche in questo caso occorre porre attenzione alla tipologia di Cloud da scegliere, possibilmente selezionando soluzioni che possono scalare "a caldo" ovvero senza la necessità di fermare e far ripatire i sistemi quando dovranno essere ampliati se il traffico Blockchain aumenta e, viceversa, ridurli al loro dimunuire (per contenere i relativi costi in modo dinamico).

2. Il volume dei dati con la Blockchain aumenta: un altro bottleneck

Come mostra il grafico della Figura 5, l'andamento di archiviazione della Blockchain Ethereum negli ultimi anni ha avuto un andamento quasi esponenziale in termini di utilizzo di memoria per archiviazione di dati, di fatto si è passati da 130GB del gennaio 2019 a 740GB ad oggi di dati archiviati per nodo. Questo fa ipotizzare che le meccaniche di archiviazione per la Blockchain siano diventate un collo di bottiglia e un fattore limitante per lo sviluppo e il miglioramento di questa tecnologia.

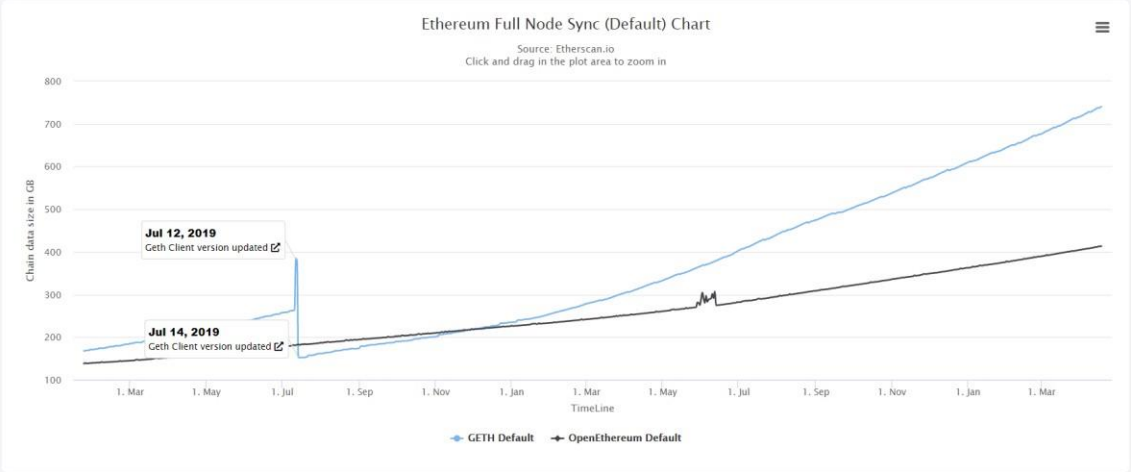

Figura 5 - archiviazione dati Ethereum[10]

Ci sono una varietà di soluzioni a questo problema, a esempio nel Bitcoin White Paper di Nakamoto conosciuto come "Il padre del Bitcoin", tutti i nodi sono suddivisi in tre categorie: "full node", "light node" e "miner node". Il light node avvia le transazioni di trasferimento e verifica il pagamento dopo che le transazioni siano state completate. Questo nodo a solo bisogno di conservare una copia dell'intestazione del blocco della proof-of-work (POW) e non tutto il dato. Il nodo full node verifica le transazioni e le trasmette a tutti i nodi miner, full node però deve mantenere una copia del blocco POW della catena. Il nodo nodo miner raccoglie le nuove transazioni nella sua catena ed inizia l'elaborazione per la risoluzione del "problema criptografico" del blocco. Quando un nodo miner trova la risposta alla soluzione, trasmette il blocco a tutti nodi. Tale divisione basata sulla capacità hardware dei nodi possono abbassare la soglia di ingresso della Blockchain in modo tale che, anche i terminali con prestazioni hardware non elevate come i dispositivi mobili possano accedere alla Blockchain più facilmente. Infatti, solo una volta che sia stata trovata la soluzione del blocco il dato verrà redistribuito su tutta la rete della Blockchain.

In Ethereum, lo sharding viene utilizzato per modificare il modo di validare le transazioni. Tradizionalmente, ogni transazione deve essere verificata da tutti i nodi della rete. Lo sharding rende possibile verificare ogni transazione da parte dei nodi in modo che i dati memorizzati su ogni nodo abbiano solo la parte del POW e non una copia della catena completa; per fare ciò si utilizza il file system Inter-Planetary File System (IPFS) per l'archiviazione dei dati nel sistema Blockchain. I nodi miner depositano i dati delle transazioni nella rete IPFS e come header l'hash IPFS restituito dalle transazioni nel blocco. Grazie alle caratteristiche della rete IPFS e dell'hash IPFS, il volume di dati è notevolmente ridotto, dunque in questo sistema di archiviazione, tutti i nodi sono uguali e devono solo mantenere le intestazioni del blocco di POW della catena.

[10] https://etherscan.io/chartsync/chaindefault

2.2 Supply chain e infrastruttura

2.2.1 Supply chain e Blockchain – esperienze e opportunità

Con il termine "Supply Chain" si identifica la catena di distribuzione relativa alle diverse attività logistiche delle aziende. Queste ultime hanno obiettivi specifici volti a coordinare strategicamente i vari membri coinvolti nelle attività di produzione, acquisto, logistica e approvvigionamento di un determinato bene.

Poiché il processo gestisce tutto il ciclo di vita del bene, materiale o immateriale, che spazia dal fornitore all'acquirente, la Blockchain tramite il suo sistema di attori può consentire il tracking di tutte le interazioni fisiche, incluse transazioni contabili e finanziarie, dei singoli beni trattati, apportando efficienze operative.

Le attività e gli step relativi alla Supply Chain, nonché le operazioni facilitate dall'utilizzo di Blockchain sono riportate nella Figura 8.

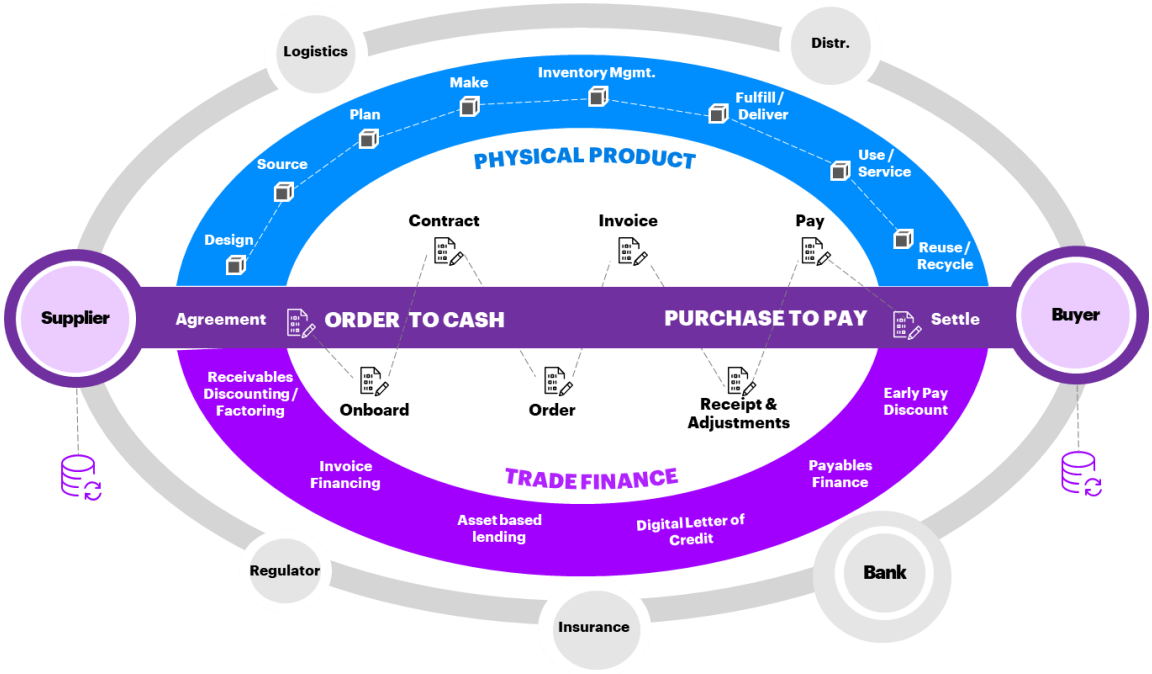

Figura 6. Schema dell'applicazione della Blockchain in ambito supply chain.

Dal Fornitore (Supplier) all'Acquirente (Buyer), è possibile:

- tracciare il prodotto fisico (Physical Product), tramite digitalizzazione del bene e successiva operazione di tokenizzazione (Tokenized Physical Asset – TPA).
- Attuare il processo di Trade Finance relativamente alle componenti finanziari e commerciali, tramite le operazioni di Trade-to-Settle (T2S) e Trade Finance (TF).

Di seguito, si offre dunque una panoramica sui vari *use case* e le esperienze conosciute in ambito supply chain.

Tokenizzazione Asset Fisici (TPA - Tokenized Physical Asset)

Le aree di applicazioni in ambito Blockchain degli asset fisici sottoforma di token sono due:

1. Internet of things & Digital Twin.

    - Sempre più asset fisici digitali diventano connessi tra loro, quindi creare un'identità unica e affidabile, estesa a tutti i partner della supply chain permettere agli asset di interagire con loro, abilitandone anche il tracking ed il controllo in tempo reale. Di seguito i diversi use case e clienti che hanno applicato:

        - Service-Based Business Models
        - Asset Transfer
        - Permissioned Data Collection & Sharing
        - Asset Access
        - Rights & Eligibility
        - Asset Identity
        - Asset Registration
        - Product Augmentation
        - Transparency

    - Esempi di Blockchain applicati al mondo Supply Chain in **ambito Internet of Things & Digital Twin** sono:

        - Daimler, Ford, GM in ambito Automotive, dove la Blockchain è usata per controllare i pezzi di ricambio dei veicoli in tempo reale.
        - FedEx, AveryDennison, 3M in ambito Industrial, dove i responsabili di trasporto e logistica grazie alla Blockchain possono monitorare le proprie risorse, prevedere guasti, migliorare i tempi di spedizione e condividere i dati con i partner
        - Boeing, GE Aviaton, Blockaviation, Rockwell Collins in Ambito Aerospace e Defense, dove i vari fornitori di parti e componenti

dei veicoli possono monitorare, in tempo reale, le loro apparecchiature e collaborare con gli OEM per migliorarne le prestazioni.

2. Physical Product Tracking.

- Spesso è necessario dimostrare l'autenticità del prodotto lungo tutta la catena del valore, utilizzando la Blockchain nei seguenti contesti:

  - Inventory Optimization
  - Brand Reputation
  - Traceability
  - Transparency
  - Authenticity
  - Product Condition
  - Shrink, Theft

- Esempi di utilizzo di Blockchain nel mondo Supply Chain in ambito Physical Product Tracking sono:

  - Kellog's, Mars, CertifiedOrigins Olio ExtraVergine d'Oliva Bellucci, Nestlè in Ambito Consumer Goods & Services, dove a fronte di una sempre più crescente richiesta da parte dei consumatori di conoscere qualità e provenienza delle materie prime dei prodotti (esempio l'origine, la sostenibilità ecc.), è stata usata la Blockchain per tracciare l'origine dei prodotti.
  - Adidas, LVMH, Walmart, CargoSmart, in Ambito Retail per ottimizzare la distribuzione.
  - Pfizer, Bayer, McKesson in Ambito Life Sciences per la distribuzione di farmaci e vaccini, tema centrale nei tempi complessi che stiamo vivendo.
  - Microsoft, Intel, Oracle, Retraced, Samsung Ambito High Tech, dove la Blockchain ha permesso di tracciare e assicurare l'originalità e autenticità dei prodotti durante tutto il loro percorso.

Lifecycle Management & Digital Thread

Il ciclo di vita degli asset (dall'origine al ritiro) non è limitato a una singola funzione aziendale (es. la produzione), ma è un processo che abbraccia e coinvolge anche altre figure aziendali come i progettisti, i fornitori, proprietari. Per ciascuno di essi la Blockchain può portare nuove tipologie di business associate ai seguenti casi d'uso:

- Trusted Asset History
- Secure Document Management
- Warranty & Recall Management
- Intellectual Property Security
- Confidential Manufacturing
- Service History
- Manufacturing Optimization
- Ecosystem Data Monetization

Esempi di aziende che si sono avvalse della tecnologia Blockchain applicandola al mondo Supply Chain in ambito Lifecycle Management & Digital Thread sono:

- BMW, FORD, ASBURY, MAN in Ambito Automotive, dove gli OEM hanno creato dei thread digitali per ottenere maggiore valore dei dati e dalle interazioni
- Boeing, GE Aviaton, Oracle, Blockaviation, Keepseablue, Rockwell Collins in Ambito Aerospace e Defense, dove grazie alla Blockchain è stato creato un albero genealogico dei veicoli arrivando ad avere una visione a 360 gradi del suo ciclo di vita.
- Caterpillar, Siemens, Rockwell Automotion in Ambito Industrial, dove l'utilizzo della Blockchain è stata associata ai moderni software PLM.

Customer Loyalty & Services

Per qualsiasi azienda i programmi fedeltà dei clienti costituiscono spesso una fonte di entrate importanti, sebbene siano molto complessi e richiedono l'interazione con diversi partner, transazioni complesse con parecchie attività manuali di riconciliazione dati – dai cataloghi premi (che coinvolgono diversi attori) ai tassi cambio dei singoli punti. Possiamo identificare – ad esempio – le seguenti aree applicative:

- Partner Onboarding/Offboarding
- Transactional Processing & Settlement
- Liability Tracking
- Multi-partner Promotion Campaign Management

Esempi di aziende che hanno utilizzato Blockchain applicata al mondo Supply Chain in ambito Customer Loyalty & Services sono:

- American Airlines, Hilton, Marriott, Southwest, MTO Global Co. Ltd. in **Ambito Travel,**
- Nike**,** P&G, Kellog's, CVS Pharmacy in **Ambito Consumer Goods & Services**

Trade to settle (T2S)

1. Procure to Pay/Order to Cash.
    - la condivisione di dati tra gli acquirenti, venditori, banche, provider logistica, autorità fiscali e varie normative, terze parti come compagnie di assicurazione e agenzie di controllo del credito può portare notevole valore aggiunto in quanto la Blockchain aggrega in maniera condiviso le informazioni ed i dati relativi all'owner della transazione / azione. Gli use case relativi sono i seguenti.
        - Know your vendor
        - Master Data
        - Credit Check & Risk Management
        - Onboarding
        - Regulatory Compliance
        - Order & Invoice Management
        - Proof of Delivery/ Goods Receipt
        - Disputes management
        - Dynamic Reporting & Status

- Esempi di utilizzo di Blockchain applicata al mondo Procure to Pay e Order to Cash sono i seguenti:

    - Cisco, Microsoft, Oracle, Lenovo, Nokia in ambito Ambito High Tech, dove la maggiore trasparenza su tutto il ciclo di approvvigionamento ha ridotto le operazioni manuali, semplificando l'onboarding degli operatori facilitando le operazioni con i fornitori.

    - Vodafone, Telstra, Singtel, Optus, AT&T in Ambito Communication&Media tramite la gestione delle fatture

    - Philip Morris International, Henkel, Unilever, Nestlè, Dyson in ambito Consumer Goods & Services dove tramite la Blockchain si sono ridotti i disallineamenti di quantità e prezzo, garantendo la riduzione della manualità delle operazioni e la perdita di entrate

    - Total, Equinor, BPin ambito Energy dove è stata ridotta la manualità delle operazioni, perdite di entrate e la non conformità.

2. Payment and Settlement

- Sebbene le innovazioni nei metodi di pagamenti siano state parecchie, le aziende sono ancora vincolate dal dover pagare i propri fornitori con metodi poco automatizzabili. Attraverso la Blockchain è possibile semplificare l'intero processo di pagamento, potendo anche effettuare una riconciliazione dei pagamenti con le fatture e la riconciliazione dei conti tra i partner di joint venture e tra le diverse entità della stessa società, che di solito sono diverse e funzionano in modo quasi indipendente.

    - Joint Venture Accounting

    - Production Revenue Accounting

    - HVAC

    - Intercompany Adjustments

    - Omni Channel Payment

    - Optimization of Cross border payments

    - Cash Application and Management

    - Reconciliations

Esempio di Blockchain applicata al mondo Finance per riconciliazione interaziendale con GE-General Electric, Oracle

3. Trade Finance

- In ambito TF (Trade Finance) i casi d'uso applicabili sono i seguenti.
  - Payables Financing
  - Invoice Financing
  - Factoring
  - Receivables Financing
  - SME/ Deep Tier Financing
  - Letter of Credit
  - Asset based lending
- Esempi di Blockchain applicata al mondo Trade Finance sono i seguenti:
  - Equinor, Baker Hughes, Conoco Phillips in ambito Energy, dove le società energetiche hanno sfruttato la Blockchain per semplificare le transazioni e relativa documentazione annessa per ottenere un accesso diretto al finanziamento delle materie prime
  - Santander, BNP Paribas, Arab Jordan Investment Bank, MUFG in Ambito Bank dove la Blockchain ha consentito alle banche di ridurre notevolmente i costi delle transazioni di alcuni prodotti come lettere di credito, garanzie, finanziamento di beni e materie prime.

2.2.2 Infrastruttura

Nelle varie esperienze di infrastrutture su progetti Blockchain, è possibile rilevare degli elementi comuni per il successo del progetto o dell'applicazione interessata, la Tabella 4 ne offre al lettore un panorama sintetico:

Componenti	Descrizione
Macchina Virtuale/Gestione del nodo	Elemento di Compute usato per ospitare il servizio. È possible usare soluzioni IaaS, PaaS docker / managed cloud

Infrastruttura "ledger agnostic", scelta del registro DLT	Quorum, Corda, Hyperledger, Ethereum
Tool di sviluppo per Smart Contracts	Developer kit integrato con infrastruttura per scrivere ed effettuare deployment di smart contracts
Gestione dell'identità	Servizio di federated identity per la soluzione
App Service	web application front end con API per far comunicare l'applicazione con l'infrastruttura di base
Monitoring	Insight di monitoraggio delle performance
Key Storage	Storage delle chiavi / encryptioning
Network	Network security groups, load balancers,
Storage	Storage per dati relativi alla soluzione
Database	Contract definitions, UI definitions, "off chain" storage
Estensioni Enterprise	REST-based API e message-based API per l'integrazione con i sistemi aziendali
Service Bus / Event Grid	Signing, hashing e routing per trasformare segnali esterni in un formato leggibile dalla API nativa del sistema Blockchain

Tabella 4, infrastrutture per progetti di Blockchain.

È preferibile scegliere una infrastruttura di *managed cloud services* per garantire scalabilità, sicurezza e facile integrazione di questi componenti, utilizzabili con un modello economico flessibile allineato all'effettivo consumo del servizio.

2.3 Piattaforme per le valute virtuali

2.3.1 Valute Virtuali

Il mercato delle criptovalute ha visto, nel tempo, una crescita esponenziale riscontrabile tutt'oggi: la capitalizzazione del settore da inizio 2021 e cresciuta del 192% in meno di quattro mesi.

Tutto ciò è stato possibile grazie a un crescente interesse e afflusso di nuovi utenti che si sono rivolti alle piattaforme di scambio per acquistare le criptovalute, oltre a un interesse sempre crescent, da parte di istituzioni e multinazionali, nel detenere e investire in bitcoin in primis, ma anche in altre criptovalute. Nel corso degli ultimi due anni molte istituzioni finanziarie hanno modificato profondamente la loro percezione cominciando a fornire ai propri clienti strumenti e possibilità che solo poco tempo fa sembravano impossibili.

In questo anno, abbiamo assistito anche all'approdo del primo cambia valute a wall-street, Coinbase la principale piazza di scambio degli Stati Uniti si è quotata al Nasdaq, già altri player internazionali come Kraken e nazionali come The Rock Trading hanno in programma la quotazione per il 2021-2022.

Nel panorama delle criptovalute, i cambia valute virtuali, ovvero le piattaforme online per la compravendita di criptovalute, sono di fondamentale importanza in quanto hanno fin dagli inizi soddisfatto la crescente domanda dei nuovi utenti.

Queste piattaforme gestite da società private permettono lo scambio di valute fiat (euro, dollaro USA, pound ecc.) con criptovalute e token, mettendo in contatto venditori e acquirenti tramite la coincidenza tra domanda e offerta. La coincidenza viene raggiunta tramite l'inserimento dei diversi ordini di acquisto e vendita all'interno di un libro (*orders book*), quando le due parti si trovano d'accordo avviene lo scambio e ciò determinerà l'aggiornamento della quotazione per quel bene.

È chiaro come i cambia valute virtuali svolgano un ruolo primario in costante crescita, insieme al settore. Diventa di fondamentale importanza sostenere e supportare questa industria che, anche in un periodo di crisi come quello che stiamo vivendo, continua a prosperare e creare posti di lavoro.

Un quadro normativo chiaro è vitale per fornire al settore un ambiente regolato in cui potersi sviluppare entro norme che non ne strozzino l'operatività; il rischio è quello di favorire piattaforme gestite da società con sedi legali in paradisi fiscali il cui operato risulta di difficile controllo.

I cambia valute virtuali sono in prima linea nella lotta al riciclaggio di denaro: dare loro un quadro chiaro permette questi di poter attuare le migliori procedure in merito ed evitare che gli utenti insieme ai capitali fuggano verso piattaforme poco chiare.

Siamo di fronte a una rivoluzione che sta investendo il mondo finanziario come non mai da oltre un secolo, secondo alcuni Bitcoin; con tutto ciò che ne deriva, la Blockchain, ha una capacità pari a quella di internet. Pertanto, stabilire un ambiente legale favorevole al settore porterà il Paese e l'Europa a essere competitive e all'avanguardia in questa seconda rivoluzione digitale riuscendo così ad attrarre capitali e investitori esteri.

In questo decennio, il numero di utenti è stato in costante crescita e a oggi è stimato intorno ai cento milioni, che nella quasi totalità si sono rivolti a cambia valute virtuali, come quelli menzionati poc'anzi, per acquistare le prime criptovalute. Nonostante negli ultimi mesi si stia riscontrando un forte incremento di utilizzatori di cambia valute virtuali decentralizzati, il primo scambio, cioè il passaggio da valuta fiat a criptovaluta, viene - nel 98% dei casi - fatto tramite cambia valute virtuali centralizzati.

Tutto ciò precisato, si osserva come l'emanazione di un quadro normativo proattivo nei confronti del ruolo svolto dai cambia valute virtuali permetterà il consolidamento dei modelli di business; ciò contribuirà alla definizione di un'infrastruttura regolamentata rivolta al mondo dei cambia valute virtuali e degli operatori di settore. Diventa quindi chiaro come la promozione del settore rappresenti un forte stimolo innovativo per tutto il paese.

2.3.2 Focus: le Infrastrutture dei pagamenti

Le criptovalute

Le prime idea di una moneta virtuale risale agli anni '90, quando l'evoluzione tecnologica e lo sviluppo della rete Internet fecero nascere l'esigenza di avere una moneta virtuale che sostituisse la valuta tradizionale nei commerci online.

Agli inizi degli anni 2000 vennero ideate le prime valute digitali che, poiché fondate sulla crittografia, presero il nome di criptovalute (o crittovalute).

Una criptovaluta è una valuta completamente virtuale, ciò significa che non esiste denaro fisico (monete o banconote) come per le valute tradizionali. Il controvalore in valuta corrente è determinato esclusivamente dalla domanda e dall'offerta, non c'è un organismo regolatore centrale.

Le criptovalute possono essere utilizzate esattamente per gli stessi scopi delle valute convenzionali: comprare e vendere beni, inviare denaro a persone o organizzazioni, ecc. Inoltre le criptovalute possono essere comprate, vendute e scambiate con le altre valute.

Esistono più di un migliaio di criptovalute diverse. Una delle prime a esser stata creata è il Bitcoin il quale è attualmente la criptovaluta più utilizzata.

Il sistema Bitcoin fu realizzato nel 2009 sulla base di un articolo pubblicato nel 2008 da un autore anonimo conosciuto con lo pseudonimo di Satoshi Nakamoto. La crescente diffusione del Bitcoin ha determinato un aumento del suo potere d'acquisto.

La rete Bitcoin

Il Bitcoin è un sistema basato sull'utilizzo di una particolare rete Blockchain, detta rete Bitcoin.

La rete Bitcoin è una rete peer-to-peer, simile alla rete Internet, in cui ogni partecipante è collegato ad alcuni degli altri nodi e in cui tutti partecipano allo stesso modo, ovvero nessuno ha privilegi rispetto ad altri. Ogni nodo coopera per mantenere un corretto funzionamento dell'intero sistema tramite la gestione di un database distribuito. Questo database tiene traccia di tutti gli scambi di bitcoin che sono stati effettuati.

La rete Bitcoin è totalmente decentralizzata. Non esiste una banca centrale o un ente di controllo che si occupi della coniatura della moneta, della gestione dei depositi di bitcoin e degli scambi di tale valuta.

Ciascun fruitore è responsabile dei propri bitcoin, in quanto non esiste un'entità, come può essere la banca nel caso dei conti corrente bancari, che si assuma la responsabilità in caso di furto o smarrimento della moneta. Inoltre, i pagamenti effettuati in bitcoin sono pagamenti diretti tra colui che invia il denaro e chi lo riceve, senza alcuna terza parte che funga da intermediario.

La struttura peer-to-peer della rete Bitcoin e la mancanza di un ente centrale rende impossibile per qualunque autorità, governativa o meno, bloccare la rete, sequestrare bitcoin ai legittimi possessori o svalutare la valuta creando nuova moneta. Pertanto, il tasso di cambio e il potere d'acquisto dei Bitcoin è dettato esclusivamente da domanda e offerta: più persone vogliono possedere bitcoin, più il valore di questi aumenta e sempre più servizi avranno interesse ad accettare pagamenti con questa valuta.

Wallet Bitcoin

Lo strumento indispensabile per poter accedere alla rete e, quindi, per poter possedere e spendere Bitcoin, è il wallet Bitcoin.

Un wallet o portafoglio Bitcoin è indispensabile per ricevere i pagamenti e per effettuarli; può inoltre mostrare il bilancio di tutti i bitcoin che contiene. Un wallet Bitcoin è l'equivalente, sulla rete Bitcoin, di un conto bancario. La chiave pubblica può essere paragonata all'IBAN associato a un conto corrente bancario, mentre la chiave privata ai dati di autenticazione che permettono di accedere al sistema home-banking del conto.

Transazioni

Gli scambi di Bitcoin tra gli utilizzatori di questa valuta vengono chiamati transazioni.

Le transazioni sono dunque il mezzo per trasferire una certa quantità di bitcoin posseduti da un utente a uno o più utenti. Possiamo paragonare una transazione a un biglietto su cui c'è scritto che il possesso di una determinata quantità di bitcoin passa da un mittente a un destinatario. Le transazioni permettono da un lato di spostare i bitcoin da un utente ad altri utenti, dall'altro di certificare il possesso di una certa quantità di bitcoin da parte di un utente.

Le transazioni sono composta da un campo *input*, che identifica la provenienza dell'importo, e da un campo *output* che rappresenta la destinazione dell'importo. Questo campo costituirà il valore di *input* della successiva transazione, dando luogo dunque ad una catena che collega tutte le transazioni. Ogni volta che viene creata una transazione è necessario che chi la crea dimostri di essere il legittimo proprietario dei bitcoin dichiarati nel campo *input*, ossia di essere il proprietario del wallet che ha ricevuto i Bitcoin nella transazione indicata nel campo inputs.

Per fare ciò si utilizza un sistema crittografico detto *Digital Signature* (firma digitale). Questo sistema garantisce la certificazione della propria identità, e si basa su una coppia di chiavi: la chiave pubblica e la chiave privata. La chiave privata serve per firmare un messaggio (le firme sono ogni volta diverse ma generate sempre a partire dalla stessa chiave), mentre la chiave pubblica è utilizzata per verificare l'autenticità della firma posta sul messaggio. Chi crea la transazione la firma con la chiave privata del proprio Wallet. L'autenticità di questa firma può essere verificata da qualsiasi utente Bitcoin utilizzando la chiave pubblica dello stesso Wallet.

Ogni transazione, dopo essere stata firmata, per far sì che assuma valore, viene comunicata all'intera rete Bitcoin, assieme alla chiave pubblica corrispondente alla chiave privata con cui si è firmata la transazione.

Dopo essere stata trasmessa a un nodo qualunque della rete Bitcoin, esso verifica che tutti i campi della transazione siano presenti e compilati correttamente e l'autenticità della firma. Se la verifica va a buon fine, il nodo la propaga agli altri nodi con i quali è connesso e, contemporaneamente, viene comunicato l'esito, a chi ha creato la transazione, del corretto inserimento della stessa nella rete tramite notifica. Se la transazione non supera la verifica, il nodo rifiuta la sua diffusione all'interno della rete, e anche in questo caso viene inviata una notifica.

Poiché una transazione è firmata e non contiene informazioni confidenziali, come la chiave privata o le credenziali dell'utente che effettua o riceve la transazione, può essere trasmessa pubblicamente senza usare particolari precauzioni. Diversamente dalle transazioni con carta di credito, per esempio, che contengono informazioni sensibili e possono essere comunicate solo attraverso reti cifrate e protette, una transazione Bitcoin può essere propagata attraverso qualunque tipo di rete, anche non cifrata. Il sistema Bitcoin ha trasformato il denaro in una struttura dati che rende praticamente impossibile fermare chiunque dal creare ed eseguire transazioni.

Una volta propagata nella rete, una transazione, per diventare effettiva, ovvero affinché i Bitcoin si "spostino" da un wallet ad un altro, deve entrare a far parte di un registro pubblico, la Blockchain. In esso le transazioni vengono raggruppate in "contenitori" denominati blocchi.

Il registro pubblico delle transazioni Bitcoin è condiviso tra tutti gli utenti Bitcoin e ognuno di essi partecipa al suo aggiornamento. Essa è stata concepita per assicurare la conservazione e la non reversibilità delle transazioni Bitcoin ed è la struttura su cui si appoggia l'intero sistema Bitcoin. La Blockchain è strutturata come un elenco ordinato di blocchi di transazioni. Ogni blocco è collegato al blocco precedente della catena; in questo modo è possibile risalire fino al primo blocco creato. La Blockchain è spesso visualizzata come una pila verticale, con i blocchi posizionati uno sopra l'altro e con il primo blocco creato come base della pila.

La parte più recente della Blockchain può subire delle modifiche, ma man mano che si ripercorre la catena, le sue componenti meno recenti sono sempre meno soggette a subire delle modifiche. Infatti, la probabilità che un blocco della Blockchain venga escluso dalla stessa diminuisce sempre più con il passare del tempo fino a diventare quasi nulla. I blocchi contenuti nella Blockchain da almeno un'ora si considerano stabili. I blocchi vengono inclusi nella Blockchain attraverso un procedimento chiamato mining.

Mining

Il mining è il processo tramite il quale blocchi di transazioni vengono inseriti nella Blockchain. Le transazioni contenute in tali blocchi si dicono confermate.

I blocchi da inserire nella Blockchain possono essere proposti da tutti i nodi della rete Bitcoin purché essi dispongano di elevata capacità computazionale e dell'intero protocollo Bitcoin (Il protocollo Bitcoin è un insieme di norme definite al fine di favorire la comunicazione tra i vari partecipanti alla rete Bitcoin e di regolamentare l'intero sistema Bitcoin. È disponibile su Internet ed è scaricabile da chiunque).

I nodi con tali caratteristiche sono detti miner e collezionano tutte le nuove le transazioni (quindi quelle non ancora inserite nella Blockchain) che considerano valide. Per selezionare quale blocco, tra quelli proposti, verrà inserito nella Blockchain, ogni 10 minuti, viene lanciata a tutti i miner una sfida matematica, per risolvere la quale sono necessari computer dotati di una grande potenza di calcolo.

All'interno del protocollo Bitcoin è descritto il metodo utilizzato dal sistema Bitcoin per gestire e regolamentare le operazioni effettuate dai miner nella rete. Questa regolamentazione fa sì che in media, per avere la conferma di una transazione, cioè l'aggiunta alla Blockchain di un nuovo blocco in cui è inserita, sia necessario attendere circa 10 minuti, tempo necessario alla risoluzione della sfida. È uso comune, per essere completamente sicuri che una transazione sia andata a buon fine, attendere che, oltre al blocco contenente la transazione, siano inseriti altri 5 nuovi blocchi nella Blockchain (per un totale, quindi, di circa 60 minuti di attesa). In generale però, per piccole transazioni quali per esempio il pagamento di una tazza di caffè, il commerciante può accettare la transazione senza aspettare la conferma, cioè i 10 minuti; ciò è equivalente ad accettare una banconota da 5 euro senza controllare se è contraffatta oppure no.

La quantità di Bitcoin coniati ammonta attualmente a 6,25 bitcoin per blocco minato. Ogni quattro anni, il protocollo dimezza tale quantità (halving) e ciò limita a 21 milioni il numero

totale di bitcoin che verrà creato. Così come la banca centrale stampa nuove banconote della valuta tradizionale, i miner creano nuovi bitcoin ogni volta che viene aggiunto un nuovo blocco nella Blockchain.

Un'ulteriore ricompensa per il miner che ha minato il blocco sono le commissioni che possono essere inserite nelle transazioni. Le commissioni costituiscono un incentivo per l'inclusione di una transazione in un nuovo blocco da minare.

Le commissioni possono essere calcolate in base alla dimensione, espressa in kiloByte, della transazione che si sta creando, e sono indipendenti dal numero di Bitcoin che essa sposta. Più in generale, le commissioni inserite nelle transazioni sono calcolate in base all'andamento del mercato all'interno della rete Bitcoin. Alcuni wallet possono calcolare e includere le commissioni automaticamente. Una transazione nella quale sono presenti delle commissioni è prioritaria, ciò significa che una transazione per cui si pagano maggiori commissioni viene inclusa più facilmente in un blocco; una transazione per cui non vengono pagate commissioni, invece, potrebbe subire dei ritardi nella conferma ma prima o poi sarà in ogni caso visionata. Il valore minimo di una commissione è stato fissato a 0.0001 bitcoin per kiloByte, tuttavia raramente le transazioni superano un kiloByte di dimensione.

Particolarità e Criticità

Riassumendo, il sistema tradizionale di Pagamento tramite Bitcoin funziona nel modo seguente:

- chiunque voglia possedere e scambiare Bitcoin si collega alla rete Bitcoin e crea un wallet. Il wallet contiene una coppia di chiavi: la chiave pubblica e la chiave privata;
- ogni scambio di Bitcoin viene effettuato mediante una transazione. Ogni transazione si riferisce a una precedente per certificare il possesso dei bitcoin che si stanno spostando con la transazione. Chi effettua la transazione, la firma con la propria chiave privata;
- per avere conferma che la transazione sia avvenuta, è necessario che questa venga inserita nel registro pubblico delle transazioni, la Blockchain. Ci sono dei nodi, i miner, che si occupano di proporre blocchi di transazioni da inserire nella Blockchain. Per il loro lavoro ricevono due tipi di ricompense: nuovi Bitcoin coniati nel momento in cui il blocco da loro minato è inserito nella Blockchain e le commissioni sulle transazioni che fanno parte del blocco da loro minato.

Il sistema Bitcoin presenta molti aspetti positivi, ma anche delle criticità.

Aspetti positivi

- **Innovazione**. Il Bitcoin, e più in generale le criptovalute, sono monete virtuali, create negli ultimi anni e basate su sistemi molto innovativi, che ben si adattano alle esigenze e alle tecnologie odierne. Questo potrebbe portare a un loro utilizzo sempre maggiore nella quotidianità.

- **Crittografia**. Il sistema Bitcoin si basa sulla matematica e in particolare su di una sua branca, la crittografia. Ciò garantisce un alto livello di sicurezza a tutto il sistema. Per esempio, il solo modo attualmente realizzabile per "rubare" Bitcoin da un wallet di cui non si è i legittimi proprietari, è entrare in possesso della chiave privata del wallet o rompere un sistema crittografico molto complesso. La sicurezza del sistema è quindi fondata sulla matematica e l'avanzamento della ricerca in alcuni sui settori. La sicurezza del wallet ricade invece nelle mani dell'utente che lo possiede e che ne gestisce la chiave privata.

- **Sistema distribuito**. La rete Bitcoin è distribuita in tutto il mondo e non esiste un ente centrale che la governi. Questo garantisce a tutti di potersi collegare a questa rete e di poter utilizzare la moneta.

- **Trasparenza**. Tutte le transazioni sono pubbliche ed è possibile tenerne traccia facilmente.

- **Pseudo-anonimato**. Le transazioni contengono solo gli indirizzi dei wallet del mittente e del/i destinatario/i. Le informazioni sui possessori di tali wallet non sono registrate in nessun database. In questo modo agli utenti è garantito un alto livello di anonimato. L'anonimato può non esser completo nel caso in cui l'utente fornisca un qualche legame tra il suo indirizzo wallet e la propria identità.

- **Accessibilità**. I pagamenti in Bitcoin necessitano unicamente di una connessione Internet per essere effettuati.

- **Facilità d'uso**. Esiste una grande quantità di applicazioni per computer e smartphone che permettono di gestire wallet Bitcoin, con funzionalità dedicate secondo le esigenze dell'utente. Generalmente, le applicazioni che gestiscono wallet su smartphone si servono dei codici QR (per esempio, per effettuare un pagamento creano una transazione mediante un codice QR), in cui sono inserite le informazioni necessarie a effettuare una transazione (importo, indirizzo wallet destinatario, ecc.).

Criticità

- **Tempi di conferma lunghi**. Nel sistema Bitcoin viene inserito un nuovo blocco nella Blockchain ogni 10 minuti circa. Per avere la certezza che una nuova transazione sia stata inserita definitivamente nella Blockchain è necessario aspettare che altri 5 blocchi siano stati aggiunti dopo il blocco contenente la suddetta transazione, per un tempo di attesa di circa un'ora in totale. Questo può limitare la diffusione del Bitcoin in contesti dove il destinatario del pagamento non può attendere un'ora per avere la certezza di essere stato pagato.

- **Volatilità del cambio**. Il valore economico del Bitcoin dipende dalla sua diffusione. Nonostante i tassi di cambio dei Bitcoin sembrino in alcuni periodi avere una certa stabilità, essi sono fortemente correlati a eventi politici, economici, sociali e all'utilizzo della valuta stessa.

- **Gestione della chiave privata**. La sicurezza di un wallet è direttamente legata alla corretta gestione della sua chiave privata. Se la chiave privata viene persa, il portafoglio diventa inutilizzabile e nessuno potrà mai più utilizzare i bitcoin che contiene.

- **Scarsa scalabilità**: il sistema sostiene circa 7 transazioni al minuto, mentre dovrebbe poterne consentire migliaia.

- Il **costo delle fee** è molto alto: per assicurarsi che una transazione venga inserita velocemente nel blocco è necessario impostare una fee molto alta, in passato, nel 2017, si è arrivati a toccare addirittura punte di 10 o 15 € a transazione.

Lightning Network

Per superare le limitazioni della rete di pagamento Bitcoin, è stata sviluppata dalla Community una nuova tecnologia, chiamata Lightning Network[11]

Lightning Network è un sistema decentralizzato progettato per gestire un elevato numero di pagamenti, anche di piccola entità (micropagamenti) con costi di commissione quasi nulli.

Lightning Network si basa sulla tecnologia messa a disposizione dalla Blockchain. Utilizzando delle transazioni Bitcoin su Blockchain, e sfruttando gli Smart Contract (programmi software inseriti nella Blockchain), è possibile creare una rete sicura in grado di consentire a chiunque di effettuare transazioni molto veloci, in grandi quantità, con costi di commissione ridotti.

Il Lightning Network sfrutta il concetto di Payment Channel:

Payment Channel

Per dare luogo ad un Payment Channel, due partecipanti creano una transazione sulla Blockchain, con la quale aprono il canale, definendo contestualmente l'importo (fund) che ciascuno di loro mette a disposizione del canale.

Da questo momento ciascuna delle due parti può effettuare delle transazioni di pagamento verso l'altra parte. Queste transazioni vengono tracciate su Lightning Network senza essere pubblicate sulla Blockchain. Ogni transazione si configura come aggiornamento del saldo di ciascuna delle due parti. Ogni transazione può avvenire se il saldo di partenza è superiore all'importo della transazione. Risulta valida solo la

[11] https://lightning.network/lightning-network-paper.pdf

transazione più recente. L'effettiva movimentazione contabile avviene al momento della chiusura del canale, che può essere effettuata unilateralmente da ciascuna delle due parti pubblicando sulla Blockchain la transazione più recente. Tutte le transazioni precedenti non vengono quindi inserite nella Blockchain.

Quindi:

- Le transazioni sono effettuate off-chain (fuori dalla Blockchain) presso i nodi degli utenti;
- La movimentazione dei bitcoin sulla Blockchain avviene quando viene fatto il broadcasting sulla rete della transazione più recente (chiusura del canale). Sulla Blockchain viene pubblicato solo l'ultimo balance delle transazioni del canale.
- Sulla Blockchain vengono registrate apertura canale (trasferimento fondi) e chiusura canale (contabilizzazione del saldo dei movimenti)

Micropagamenti

Lightning Network apre uno scenario particolarmente interessante per i micropagamenti, che attualmente vengono effettuati quasi esclusivamente in contanti. La velocità di transazione, il bassissimo costo di commissione e la mancanza di un sistema centralizzato di gestione rende possibile digitalizzare anche i pagamenti più piccoli.

Inoltre, questa modalità di pagamento consente di dare luogo ai micropagamenti automatizzati, che i vari servizi fruiti dai sempre più diffusi dispositivi connessi a Internet stanno cominciando a richiedere.

Pagamenti in streaming

Lightning Network consente di introdurre un nuovo concetto di *Pay per use*: possono essere impostati dei processi che prevedono di effettuare un pagamento ogni minuto (o addirittura ogni secondo) di fruizione di un servizio, come uno streaming video ad esempio. Il fornitore riceverà il pagamento in modo contestuale all'erogazione del servizio, ed il pagatore pagherà solo per il tempo di fruizione del servizio.

Oltre il Bitcoin

Lightning Network potrebbe essere utilizzato anche su altre criptovalute, dato che si tratta di un layer aggiuntivo da affiancare alla Blockchain nativa del Bitcoin. Inoltre, potrebbe anche consentire la nascita di nuovi soggetti che, sfruttando le potenzialità della rete, potrebbero offrire nuovi servizi di pagamento.

2.4 DLT/Blockchain a servizio dell'identità (EBSI, IBSI, Self Sovereign Identity)

2.4.1 Introduzione

Preliminare a ogni tipo di trattazione su quest'argomento è il definire cosa intendiamo con identità digitale. L'identità digitale è considerata "un insieme di dati che descrivono unicamente una persona, un'azienda o un oggetto e che vengono raccolti, memorizzati e condivisi digitalmente all'interno di un ecosistema di attori e attraverso tecnologie abilitanti per permettere l'accesso a servizi digitali a valore aggiunto".

In questa definizione sono quindi evidenziati i 4 fondamentali dell'identità digitale, ovvero:

- **Dati**
- **Ecosistema**
- **Tecnologie abilitanti**
- **Accesso a servizi**

All'interno di un ecosistema vi sono possibili ruoli che possono essere ricoperti dai vari attori presenti. È possibile identificare diverse funzioni che possono essere svolte:

Utente/Identità: utilizza l'identità digitale per integrare con altri attori nell'ecosistema;

Service Provider: fornisce i servizi rivolti all'utente finale, per i quali è richiesta una verifica dell'identità;

- Identity Provider: verifica i dati dell'utente, rilascia e gestisce l'identità digitale, trasferendo dati durante le interazioni;
- Certification Authority: assegna certificazioni e attributi all'utente;
- Technology Provider: fornisce la soluzione informatica e architetturale;
- Identity Verifier: verifica che i dati identificativi corrispondano a chi sta utilizzando le credenziali.

A seconda di quale e quanti di questi sono presenti e del modo in cui interagiscono tra di loro, si vengono a creare diversi ecosistemi con diverse strutture e caratteristiche.

Decentralizzazione della Digital Identity

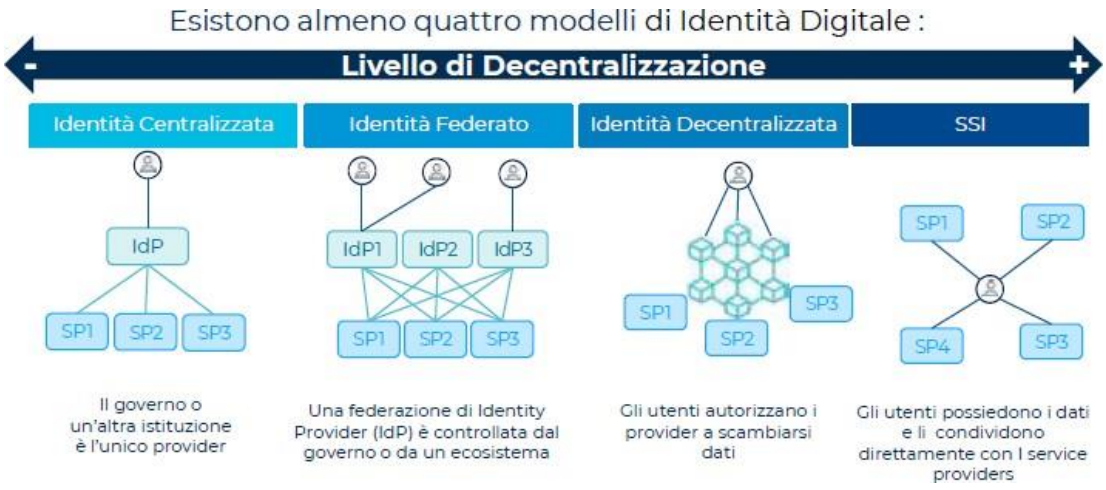

Figura 6. Modelli di identità digitale ordinati per livello di decentralizzazione.

Storicamente l'identità si basa su modelli centralizzati, dove un solo attore, solitamente il governo, viene chiamato a gestire l'identità di tutti. In questo contesto l'accesso ai vari servizi è consentito solamente tramite questo attore centrale, unico e soprattutto fidato.

Negli anni si sono sviluppati altri modelli alternativi che presentano dei livelli di decentralizzazione maggiori. Nello specifico sono stati individuati 4 differenti modelli: centralizzato, federato, decentralizzato e basato sul Self Sovereign Identity.

- **Identità digitale centralizzata**

  Nei modelli basati su un'identità digitale centralizzata, un ente centrale (Identity Provider) possiede e controlla un archivio unico che contiene le identità di tutti i soggetti. Solitamente questa terza parte fidata coincide con un 'entità governativa. Attraverso una soluzione di questo tipo l'utente può inserire i propri dati nel sistema e, caricando delle prove a supporto, l'ente centrale verifica la veridicità dei dati trasmessi e rilascia un'identità digitale unica e verificata. Gli utenti ogni qualvolta vorranno accedere a un servizio digitale offerto dal Service Provider, autorizzeranno il Service Provider ad accedere ai propri dati detenuti dall'unico Identity Provider. Il Service Provider, con il permesso dell'utente, potrà quindi accedere a questo database centralizzato per verificare l'identità dell'utente. Se i dati personali cambieranno, l'utente dovrà aggiornare le proprie informazioni nel database centralizzato una volta sola.

- **Identità digitale federata**

  In un sistema basato su identità digitale federata esistono due o più Identity Provider, che verificano le credenziali e rilasciano le identità digitali agli utenti.

L'utente può scegliere l'Identity Provider (IP) che preferisce e gli affida la propria identità. L'utente per poter accedere ai servizi digitali offerti dai Service Provider dichiara il proprio Identity Provider e autorizza il Service Provider ad accedere ai propri dati detenuti dall'Identity Provider. In questo modo non esiste un unico database centralizzato che archivia tutte le credenziali degli utenti, ma i dati sono archiviati su più database differenti.

- **Identità Digitale Decentralizzata**

  Con i modelli decentralizzati, più Identity Provider controllano l'archivio dell'identità dell'utente, ma nessuno conosce le informazioni di uno stesso utente. L'utente ha la possibilità di permettere a Service Provider e Identity Provider di condividere i dati con altri Service Provider. Le tecnologie Blockchain e Distributed Ledger abilitano questo modello consentendo agli utenti di essere certi che i dati siano gestiti in modo corretto e autorizzato.

- **Self sorvereign Identity (SSI)**

  Infine, con il massimo livello di decentralizzazione possibile, il modello della Self Sovereign Identity (SSI), abilitato dalle tecnologie Blockchain e Distributed Ledger, consente all'utente di non delegare la custodia e il controllo delle informazioni personali a un attore terzo. Il cuore di questo modello è la possibilità, da parte dell'utente di generare autonomamente un identificativo che può dimostrare di controllare; questo avviene con meccanismi crittografici simili a quelli che consentono di controllare fondi e account su Bitcoin o Ethereum. Le informazioni e la storia dell'utente sono invece rappresentate da claim, cioè da affermazioni che altre entità (individui, istituzioni etc.) fanno su di esso e che sono state da loro verificate.

  Le piattaforme Blockchain abilitano i modelli SSI, ma anche i modelli SSI possono rendere migliori le piattaforme Blockchain. In generale le tecnologie Blockchain consentono l'accesso utilizzando degli pseudonimi e l'identificazione non è richiesta. Vi sono alcune situazioni o applicazioni in cui l'identificazione è essenziale (es. Custodia, requisiti di legge, ...) in quanto l'identità ha un ruolo. È importante creare un ambiente in cui le caratteristiche di decentralizzazione siano mantenute, lasciando la possibilità di scambiare informazioni e dati in totale sicurezza e privacy.

2.4.2 Focus: Self-Sovreign Identity

Un sistema pubblico di identità digitale rappresenta un pilastro abilitante e fondativo per lo sviluppo di servizi governativi innovativi come del settore privato. Avere la certezza che gli individui siano coloro che affermano di essere è un prerequisito per garantire diritti e doveri del sistema sociale.

Per queste ragioni, il tema dell'identità è continuo oggetto di approfondimento ed evoluzione, anche per quanto riguardo le opportunità di adozione di paradigmi decentralizzati, abilitati da tecnologie Blockchain e DLT.

Ambiti di grande rilevanza per la vita dei cittadini (e delle loro organizzazioni) richiedono delle infrastrutture, sempre più digitali, che garantiscano un corretto rapporto tra individui e amministrazioni nei diversi contesti, basti pensare ad esempio a salute, sicurezza, fiscalità, proprietà, finanza.

Il settore pubblico assume perlomeno un duplice ruolo: certifica l'identità del cittadino e utilizza la stessa per garantire il corretto accesso ai servizi.

Al contempo non si può trascurare l'importante impatto sul settore privato e dell'economia, sia per consentire di operare secondo compliance normativa (es. di settore) che per finalità più strettamente di business.

In questo contesto, si sta affermando sempre con maggiore efficacia la convergenza tra modelli decentralizzati, implementabili tramite tecnologie Blockchain, ed il paradigma denominato "Self-Sovereign Identity", fondato sui seguenti principi:

- esistenza (indipendenza da terze parti);
- controllo (controllo della propria identità);
- accesso (possibilità di accesso ai dati della propria identità);
- trasparenza (di sistemi e algoritmi che definiscono e gestiscono l'identità);
- persistenza (il più a lungo possibile, idealmente per un tempo indefinito);
- portabilità (facilità di trasporto);
- interoperabilità (per essere utilizzata in modo più ampio possibile);
- consenso (per l'utilizzo della propria identità, e quindi poterne negare l'accesso/fruizione);
- minimizzazione (dati minimizzati in funzione della finalità);
- protezione (i diritti devono essere protetti).

Questo modello di identità, oltre a mitigare il problema della detenzione, possesso o ritenzione dei dati dell'utente da parte di attori terzi, potrebbe abilitare e stimolare scenari in cui il cittadino possa controllare e gestire un consapevole utilizzo e valorizzazione, anche economica, dell'informazione relativa a sé stesso, nel pieno rispetto del Regolamento UE n. 2016/679 - General Data Protection Regulation (GDPR).

L'integrazione tra Blockchain/DLT e SSI ha attivato iniziative e progetti[12] particolarmente significativi per la loro portata istituzionale (rif. integrazione con eIDAS) internazionale e perchè sostenuti da comunità e attori rilevanti da un punto di vista di dimensione e di competenza tecnologica. Attraverso la possibilità di condividere solamente le informazioni strettamente necessarie all'erogazione di un servizio, i sistemi SSI riescono già oggi a spingersi a livelli molto promettenti, garantendo l'utilizzo della propria identità e dei relativi attributi per creare attestazioni specifiche che dimostrano il possesso di determinati requisiti evitando al tempo stesso rivelarne completamente il contenuto a terzi.

2.4.3 Focus: Identità Decentralizzata (DID)

I dati delle nostre vite digitali e fisiche sono sempre più legati alle app, servizi e dispositivi che utilizziamo per accedere a una ricca serie di esperienze. Questa trasformazione di identità è stata troppo spesso esposta a violazioni, che interessano i nostri social, vita professionale e finanziaria. Ogni persona ha diritto a un'identità da possedere e controllare, per archiviare in modo sicuro elementi

della propria identità digitale e preservare la privacy. Una soluzione di identità decentralizzata (DID) per individui e organizzazioni garantisce comunità aperta, affidabile e interoperabile.

Una DID è composta di 7 elementi chiave:

1. Identificatori decentralizzati (DID) del W3C: ID che gli utenti creano, possiedono e controllano indipendentemente da qualsiasi organizzazione o governo. I DID sono identificatori univoci a livello globale collegati a infrastrutture a chiave pubblica decentralizzate (DPKI) con metadati composti da documenti JSON che contengono materiale a chiave pubblica, descrittori di autenticazione ed endpoint del servizio.

2. Sistemi decentralizzati (ad esempio,Blockchain e DLT): i DID sono radicati in sistemi decentralizzati che forniscono il meccanismo e le caratteristiche richieste per DPKI. Diverse società tanno partecipando nello sviluppo di standard e tecnologie in fase di sviluppo dalla comunità per consentire un vibrante ecosistema di implementazioni DID che supportari una varietà di Blockchain e ledger.

3. Agenti utente DID: applicazioni che consentono alle persone reali di utilizzare identità decentralizzate. Le app dell'agente utente aiutano nella creazione DID, gestione di dati e permessi, e firmare / convalidare input collegati a DID. Si può avere un'app simile a Wallet che può agire come agente utente per la gestione dei DID e dati associati.

[12] Si ricordano in particolare eSSIF (eIDAS SSI Bridge), Decentralized Identity Foundation.

4. DIF Universal Resolver: un server che utilizza una raccolta di driver DID per fornire un mezzo standard di ricerca e risoluzione per DID tra le implementazioni e sistemi decentralizzati e che restituisca il DID Document Object (DDO) che incapsula i metadati DPKI associati con un DID.

5. Hub di identità DIF: un file replicato mesh di archivi di dati personali crittografati, composto da istanze cloud ed edge (come telefoni cellulari, PC o altoparlanti intelligenti), che facilitano l'archiviazione dei dati di identità e interazioni di identità.

6. Attestazioni DID: attestati firmati DID che si basano su formati standard e protocolli. Consentono ai proprietari di identità di generare, presentare e verificare attestazioni. Questo costituisce la base della fiducia tra gli utenti di vari sistemi.

7. App e servizi decentralizzati (DApps): DID accoppiati a Identity Hub consentono la creazione di una nuova classe di app e servizi. Memorizzano i dati con Identity Hub dell'utente e operano entro i confini delle autorizzazioni a loro concessi.

Uno scenario di esempio:

Alice si è recentemente laureata al college. Può richiedere una copia digitale del diploma, rilasciato dall'università grazie alla sua DID. Può scegliere di condividere il suo diploma con chiunque, come un potenziale datore di lavoro, che può verificare in modo indipendente l'emittente del diploma, data di emissione e relativo stato di validità.

Si può creare ad esempio un servizio cloud, sicuro perché tutto in esso è crittografato con le chiavi private che vengono controllate dall'utilizzatore finale controllando tutto ciò che viene eseguito sotto la propria autorità.

3. PARTE TERZA – RISULTATI ATTESI

3.1 Sistemi di pagamenti

Con la nascita e lo sviluppo delle Criptovalute e della Blockchain e specialmente con l'impennata di valore e popolarità delle prime, si sta assistendo ad un sempre maggiore interesse a livello istituzionale nella materia, così da portare anche la BCE a studiare la fattibilità di un euro digitale.

Questo sarebbe una CBDC (Valuta digitale sostenuta da una Banca Centrale). Simili e ispirate alle criptovalute, ma da non confondere con queste, le CBDC sono la versione digitale della moneta fiat.

In sostanza l'euro digitale sarebbe l'equivalente elettronico dell'euro fisico in contanti. Una moneta virtuale con corso legale e garantita dalla Banca centrale europea, usata per i pagamenti nei Paesi europei sia da imprese che da cittadini per pagare in modo più veloce, sicuro e innovativo.

L'arrivo dell'euro digitale consentirebbe per la prima volta ai cittadini di depositare denaro direttamente presso la BCE, al di fuori delle banche commerciali.

Parallelamente, sei delle più grandi banche cinesi stanno promuovendo la nascente Central Bank Digital Currency (CBDC) a Shanghai. Esse stanno esortando commercianti e consumatori a scaricare il wallet della CBDC e a effettuare acquisti usando lo yuan digitale. Questo sistema aggirerebbe completamente i metodi di pagamento elettronici oggi utilizzati da milioni di utenti così da consentire alla banca centrale di ottenere un accesso più ampio ai dati sui pagamenti, e contemporaneamente sottrarre un po' di potere dalle grandi società private dei pagamenti.

Una nuova società denominata Finalità International, nata da un'idea di 14 importanti società finanziarie, ha posto le basi per il controllo di un sistema di cassa digitale basato su Blockchain e sul coin (moneta) chiamato "Utility Settlement Coin" (USC). L'USC può essere utilizzato per i pagamenti e come dispositivo che trasmette tutti i dati necessari per completare uno scambio di denaro.

Già nel settembre 2015, UBS Group, il gigante finanziario svizzero, ha collaborato con la società di Blockchain londinese Clearmatics, lanciando il concetto di un sistema di cassa digitale che consentirebbe ai mercati finanziari di effettuare pagamenti e regolare le transazioni in modo più rapido e sicuro tramite la tecnologia Blockchain.

Il colosso giapponese SoftBank ha lanciato le nuove Wallet Card SBC (Softbank Card 3.0). Le nuove carte offrono servizi di pagamento sia in valuta fiat che in asset digitali. L'obiettivo delle carte SBC è quello di migliorare le carenze dei wallet tradizionali, fornendo maggiore sicurezza e migliore accessibilità. Non si tratta di una semplice carta di debito in plastica, perché le nuove SBC saranno dotate di uno schermo LED sottile che mostra agli utenti il loro saldo in tempo reale, alimentato da una micro-batteria che può durare fino a tre anni. Avranno anche una loro app dedicata. Inoltre, grazie ad un ricevitore WiFi integrato, possono essere utilizzate anche come hot o cold wallet di criptovalute. Infatti, quando sono disconnesse fungono da cold wallet, ma non appena

vengono collegate alla rete diventano degli hot wallet utilizzabili per effettuare pagamenti in criptovalute o in valute fiat. Le wallet card SBC avranno anche tempi e costi di emissione ridotti.

Con queste carte SBC, Softbank vuol fare un passo in avanti nel settore dei pagamenti basati su Blockchain, creando una novità mai vista prima.

Oman Oil & Group Orpic, una delle più grandi aziende di petrolio e gas nel Sultanato dell'Oman, e HSBC Bank hanno eseguito la prima transazione su Blockchain del paese: una vendita di polipropilene all'Abu Dhabi National Carpet Factory. La transazione è stata effettuata utilizzando Corda, la piattaforma Blockchain open source di R3. L'utilizzo della Blockchain ha velocizzato i tempi di invio, ricevuta e visione della lettera di credito, e ha permesso alle parti di completare la transazione entro 24 ore a dispetto dei soliti 5-10 giorni.

BankDhofar, seconda banca dell'Oman per capitalizzazione di mercato, ha iniziato ad utilizzare la tecnologia RippleNet per i pagamenti transfrontalieri in India. "In meno di 2 minuti", attraverso l'utilizzo di un'applicazione di mobile banking, la banca è in grado di fornire bonifici transfrontalieri.

Delle 26 banche pubblicamente elencate in Cina, 12 adottano la Blockchain per vari casi di utilizzo nei loro sistemi. Queste variano da banche statali come al Bank of China, a banche private, come la China Merchants bank.

Ad oggi, più di 400 banche ed istituti finanziari nel mondo utilizzano la tecnologia Blockchain.

Il 90% dei membri dell'European Payments Council ritiene che la tecnologia Blockchain cambierà radicalmente il settore dei pagamenti entro il 2025. Infatti, il mercato dei pagamenti digitali è soggetto a una fortissima evoluzione poiché per troppo tempo è rimasto fermo su modelli consolidati. Purtroppo, ancora oggi la maggior parte delle transazioni a livello globale utilizzano sistemi antiquati di pagamenti che risultano lenti e che prevedono commissioni aggiuntive.

Una transazione economica da una parte all'altra del globo potrebbe anche impiegare fino a 7 giorni per poter essere eseguita. In questi anni c'è stata già una forte spinta per cercare nuovi modi per effettuare transazioni più veloci e sicure, garantire trasparenza ai clienti e alle autorità di regolamentazione e abbassare i costi di servizio, ma la tecnologia Blockchain rappresenta in questo momento l'evoluzione più radicale per ottenere tutto ciò.

La Blockchain permette di offrire a controparti, che non si conoscono per niente, un accordo sullo stato di un database, senza alcun intermediario e senza necessità di ulteriori controlli. La Blockchain costituisce un libro mastro che si auto-amministra in grado di fornire servizi finanziari sicuri e rapidi come le transazioni di denaro. Infatti, il problema della fiducia tra le controparti viene risolto cambiando totalmente il paradigma del sistema, ovvero fornendo una tecnologia in cui la fiducia è costruita intrinsecamente all'interno di essa. I vantaggi, pertanto, risultano evidenti: il non dover più eseguire

controlli sulle parti in causa rende la transazione più veloce e meno dispendiosa, abbassando se non annullando totalmente i costi di servizio.

Se una Blockchain creata da una Banca privata può abbassare tempi e costi di servizio, una Blockchain pubblica unica di pagamenti potrebbe portare all'obsolescenza dell'intero sistema bancario dei pagamenti, poiché quella pubblica potrebbe svolgere un ruolo pubblico da intermediario tra pagatore e pagato. Si pensi alle criptovalute come Bitcoin ed Ethereum, che sono costruite su Blockchain pubbliche utilizzate per inviare e ricevere denaro.

Le Blockchain pubbliche realizzate allo scopo di fornire sistemi di pagamento riducono e in alcuni casi annullano la necessità di terze parti fidate che si occupino di eseguire e verificare le transazioni. Le transazioni tramite Blockchain possono richiedere pochi minuti per essere regolate, costituendo un drastico abbattimento del tempo medio di elaborazione per i bonifici bancari.

Gli sviluppatori stanno anche lavorando per scalare soluzioni più economiche per elaborare più rapidamente le transazioni crittografiche. Bitcoin Cash e TRON, ad esempio, hanno transazioni a prezzi relativamente bassi.

3.2 Fonti certificative pubbliche

La Blockchain, nelle sue varie accezioni, si pone come possibile infrastruttura in grado di consentire la comunicazione tra sistemi e registri e abilitatore di nuove fonti di dati pubblici.

In questo contesto si ricorda innanzitutto che un pubblico registro costituisce la fonte primaria di certificazione dei dati dei soggetti a esso iscritti ed il legislatore ne assegna la responsabilità di gestione alle amministrazioni dello Stato, coerentemente con le rispettive funzioni istituzionali. Nell'attuale configurazione giuridica e organizzativa, i pubblici registri costituiscono uno dei pilastri del sistema di tutela dei diritti.

È importante quindi specificare come un modello decentralizzato sia particolarmente indicato in tutti i casi in cui non sia possibile individuare un unico soggetto che eserciti funzioni di verifica e, più in generale, di gestione e di responsabilità complessiva sulle informazioni a livello nazionale.

Si consideri, infatti, come le tecnologie Blockchain e DLT possano portare effettivo valore nei casi d'uso o contesti in cui l'insieme di più contributi possa costituire una nuova sorgente nazionale di informazioni per un determinato settore o ambito di riferimento.

In questi scenari le condizioni sostanziali che possono portare all'applicazione di modelli decentralizzati sono principalmente l'assenza di un unico soggetto regolatore, in grado di intervenire sull'accesso e sulla modifica del dato, e l'economicità dell'utilizzo del paradigma di interoperabilità abilitato da Blockchain.

La presenza di queste caratteristiche rende interessante e attuabile il ricorso alla tecnologia Blockchain, in particolare in contesti individuabili nelle seguenti tipologie:

- possibilità di interazione tra fonti pubbliche a carattere comunale/regionale/nazionale, la cui efficacia ed fruizione può essere accelerata e trasformata dalla condivisione dei dati derivante dall interoperabilità (es. Sanità);

- costituzione di nuove fonti informative pubbliche per rispondere a nuove esigenze emergenti; ad esempio, il caso delle Disposizioni anticipate di trattamento di cui alla legge 219/2017 e all'art. 1, commi 418-419 della legge 205/2017 ("DAT"), per le quali è previsto un pubblico registro tenuto dal Ministero della Salute e dei registri facoltativi regionali;

- applicazioni in ambito cross-border, nelle quali l'interoperabilità dei registri distribuiti a livello internazionale, pur centralizzati a livello di singolo Paese, può assicurare una fonte certificativa di dati molto più efficace ed estesa.

3.3 DLT/Blockchain come fattore abilitante la sharing economy e nuovi modelli di piattaforma

Negli ultimi anni, si è assistita a una crescita della tecnologia Blockchain, inizialmente utilizzata per la creazione di criptovaluta come ad esempio il Bitcoin. Negli anni la Blockchain tramite l'utilizzo degli Smart Contract che, ricordiamo essere veri e propri contratti digitali tra due o più parti, la Blockchain si è aperta la strada ad un nuovo modo di autenticazione dei dati digitali e non solo.

Come noto, la Blockchain non è altro che un registro distribuito immutabile in cui le informazioni sono condivise con i diversi soggetti che partecipano alla rete distribuita, ed è proprio il concetto "distribuita" che fa sì che questa tecnologia abbia tutte le caratteristiche per essere abilitata allo Sharing Economy. Infatti, la Sharing Economy si propone come modello orizzontale tra i diversi attori che condividono una risorsa, su fondamenta che si consolidano intorno al concetto di reputazione e fiducia.

Di fatto, tramite la Blockchain è possibile andare a sostituire figure di garanzia come notai, regolatori e creare nuove opportunità per aziende o mercati in un modo totalmente nuovo, lasciando la possibilità di sviluppo di nuovi modelli economici di condivisione delle risorse.

Senz'altro la tutela del bene condiviso è una funzionalità primaria della Blockchain, che rispecchia una proprietà importante di questa tecnologia, cioè la capacità di generare una nuova forma di fiducia, garantita da un'entità "neutrale", questo spinge non solo le aziende a un nuovo tipi di collaborazione, ma anche ad immaginare nuovi scenari socioeconomici tra soggetti privati. Questi nuovi scenari socioeconomici trainati dalla rivoluzione digitale che sta investendo la società attuale, trova in queste nuove tecnologie come la Blockchain il cambiamento di ruoli tra produttori/consumatori che

diventano interscambiabili, questo nuovo fenomeno prende il nome di “modello di piattaforma”.

Il fenomeno di “modello di piattaforma” trova riscontrano nelle aziende quali Amazon, Netflix, Facebook e Google le più grandi protagoniste che non si fermano a essere solamente piattaforme, ma anche produttrici di contenuti. D'altrondem in questi ultimi anni i maggiori produttori di contenuti nei social erano proprio gli utenti stessi, che caricando contenuti con immagini o articoli alimentavano l’industria dei social.

Si vede come questi modelli di piattaforma stiano cambiando gli obiettivi aziendali di molte aziende, che si fanno portatrici di nuovi contenuti “originali”, basti infatti pensare semplicemente ad Amazon e Netflix che oltre a detenere la piattaforma, cerca di allargare la propria posizione nel mercato dei contenuti audio visivi, facendo leva su un nuovo modo di usufruire i contenuti in maniera flessibile.

L’evoluzione delle nuove tecnologie come abbiamo visto influenza l’economia mondiale; l’introduzione di uno strumento tecnologico come Blockchain modifica non solo i modi in cui un bene viene scambiato, ma porta anche ad un cambiamento nelle abitudini sociali e aziendali, creando un nuovo tipo di valore, basato sulla decentralizzazione da un’autorità centrale e un nuovo modo di concepire gli scambi.

3.4 Conclusioni e Focus benefici sui settori interessati dal PNRR

Anitec- Assinform ritiene fondamentale pensare in maniera più approfondita a come una tecnologia innovativa e dirompente come la Blockchain possa essere strumentale al raggiungimento degli obiettivi stilati dal Piano Nazionale di Ripresa e Resilienza

In tale piano, essa viene menzionata solamente una volta per le attività di verifica e audit dei processi di e-procurement (“Status chain”) parte di una riforma che mira alla modernizzazione del sistema nazionale degli appalti pubblici per il sostegno delle politiche di sviluppo, attraverso la digitalizzazione e il rafforzamento della capacità amministrativa delle amministrazioni aggiudicatrici.

Tuttavia, gli ambiti di applicazioni sono molteplici e applicabili orizzontalmente alle Missioni riportate nel piano, ma si prova qui di seguito a focalizzarli partendo dalle caratteristiche abilitanti della tecnologia stessa:

- **Auditability e certificazione**

La funzione di “notarizzazione” può essere interessante per garantire trasparenza ed immutabilità di alcuni eventi chiave di processi pubblici e privati.

Nella Missione 1 si rilevano sinergie con il bisogno di garantire trasparenza nei **servizi digitali ai cittadini**, potendo quindi sviluppare delle applicazioni che potrebbero permettere alle amministrazioni pubbliche di certificare dei passi chiave di avanzamento di pratiche legate ai servizi **o ai processi giudiziali**, e ai cittadini di controllare in maniera trasparente l’avanzamento degli stessi in tempo reale.

Visto anche il focus sulle competenze, a valle di un percorso di formazione potrebbe essere notarizzato un certificato di apprendimento.

Altre applicazioni vedono affinità con il rilancio del **Turismo (M1),** certificati vaccinali e green pass basati su Blockchain garantirebbero verificabilità ed interoperabilità con altri paesi, o nella **Salute (M6),** nella tracciabilità dei prodotti medici e sanitari.

Questi stessi vantaggi possono essere applicati **ai processi delle filiere**, con la protezione del Made in Italy ed il focus sulle **filiere agricole ed economia circolare** con gli obiettivi della Missione 2.

In particolare, gli incentivi (fiscali e non) legati a Transizione 4.0 ed Ecobonus/Sismabonus potrebbero far leva sull'utilizzo di queste caratteristiche.

- **Interoperabilità e controllo dati - Trusted Data Sharing**

Ci sarebbe molto da dire sui modelli di interoperabilità di dati e la ripresa del controllo degli stessi da parte dell'utente finale grazie alla Blockchain, ma gli ambiti di focus che proponiamo sono:

  - **Identità Digitale e servizi al cittadino**: Evoluzione ed estensione dell'attuale modello SPID per tutti i servizi della PA allargata (ad es. Singapore, Honk Kong) con architetture di identità decentralizzata **(M1).**

  - **Tokenizzazione e mercati di scambio:** Realizzazione di un modello applicativo interoperabile tra amministrazioni e cittadini che abiliti scenari di tokenizzazione di asset fisici o immateriali e il relativo scambio/utilizzo in servizi dedicati, come: a) Certificati di proprietà di asset fisici (auto, immobili) legati alla digitalizzazione della PA (**M1);** b) Piattaforma di Tokenizzazione dei risparmi di CO2 legati ad un progetto ESG/Sostenibilità e relativo finanziamento, standardizzazione dei parametri di misurazione **(M2); c)** Sistema di incentivi basato su Blockchain ed interoperabile con mobilità pubblica per guadagnare token spendibili in servizi pubblici portando i cittadini a comportamenti di mobilità sostenibile **(M3).**

  - **Applicazioni nella salute (M6)**: Gestione dei dati della cartella clinica elettronica, dati delle cartelle cliniche personali in un wallet univoco e controllato dal cittadino, compresi dati genomici e sanitari elettronici interoperabili, esplorando anche applicazioni nel supporto ai claim assicurativi legati alla sanità.

- **Automazione decentralizzata processi ("Smart Contracts")**

L'automazione tramite smart contract può portare notevoli vantaggi in termini di efficienza, liquidità e finalità dei processi controllati. Essendo dei programmi software attivabili al soddisfarsi di alcune condizioni, potrebbero introdurre anche un aspetto di "gamification" su determinati servizi.

Nella Missione 1, 2 e 6, abbiamo visto molti esempi di processi che potrebbero giovare di una automazione, alcuni esempi possono essere:

- **Finanziamenti pubblici a PMI sulla base di condizioni predeterminate**
- **Servizi digitali ai cittadini attivati tramite il soddisfacimento di alcune condizioni**
- **Crediti fiscali "sbloccati" tramite il raggiungimento di parametri di Sostenibilità**

Per garantire che gli input che arrivino ai contratti automatici siano affidabili, dovrebbe essere approfondito il ruolo degli "oracoli", anche pensando all'aiuto che tecnologie come AI ed IoT possono apportare in termini di benefici per evitare input (maligni o determinati da errori) che possano alterare lo scopo stesso per cui era stato pensato il contratto.

Su tutti gli ambiti descritti nei precedenti 3 punti, riteniamo importante una partnership pubblico-privata per lo sviluppo di questi servizi che riesca a tener conto di **framework legale, infrastruttura tecnologica, governance e sistema di incentivi** per l'adozione effettiva da parte degli utenti finali.

3.5 Intelligenza Artificiale e Blockchain

Intelligenza Artificiale a Blockchain sono settori che coinvolgono tecnologie diverse e hanno anche problematiche molto diverse così come diversa è l'evoluzione attesa, influenzata da altri attori e fattori.

Tuttavia, entrambe hanno come punto di contatto i dati. L'IA parte dai dati per costruire significati e processi decisionali e Blockchain garantisce un controllo sull'integrità dei dati. Per questo motivo IA e Blockchain sono spesso accomunate (insieme a IoT - anche questa indipendente ma legata attraverso i dati che genera alle altre due).

Nella definizione di un piano di Transizione 4.0 queste tecnologie giocano un ruolo importante al punto da venir considerate complementari ma convergenti (insieme alle IoT)

È quindi opportuno che siano considerate insieme nell'ottica della Trasformazione 4.0, tanto più visto l'impegno del Governo a sostenere l'iniziativa Gaia-X in cui la definizione dei Data space fornisce il contesto allo sviluppo e applicazione di IA e dall'altro può beneficiare dell'utilizzo di Blockchain.