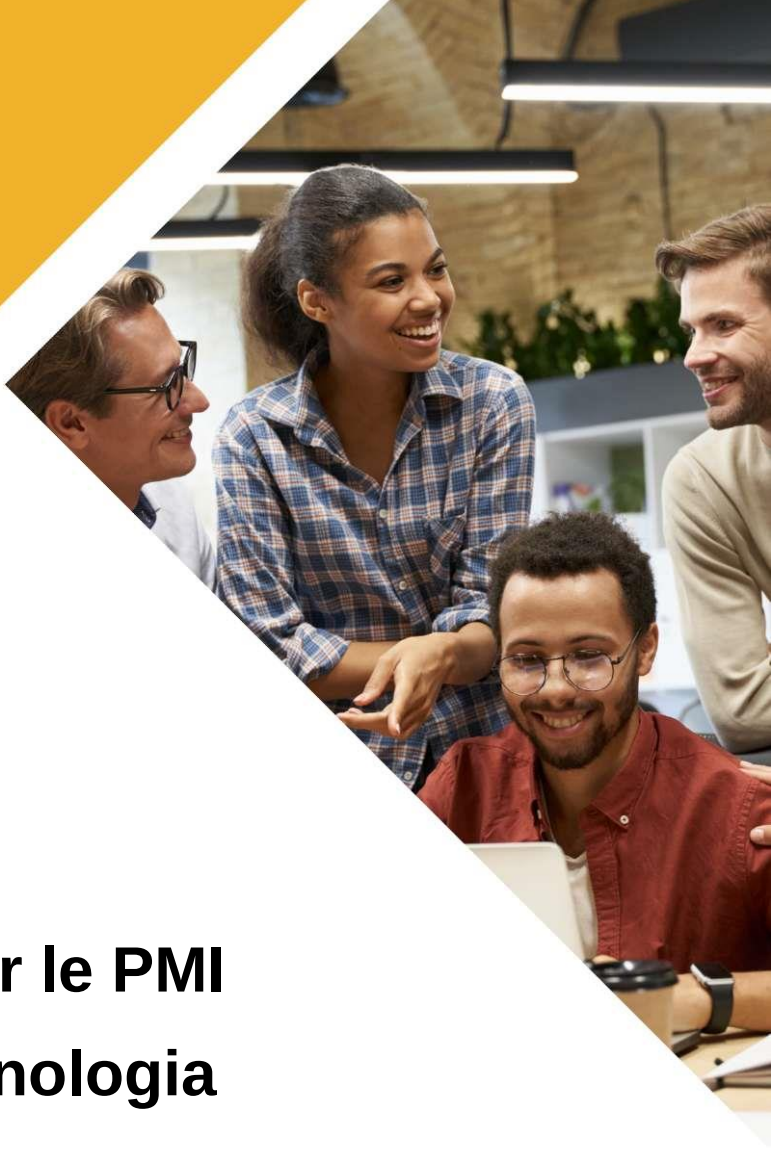


Guida per le PMI sulla tecnologia blockchain e Distributed Ledger

Italian DIGITAL SME Alliance

European DIGITAL SME Alliance

Con il supporto di:

CNA MILANO

ASSINTEL ASSOCIAZIONE NAZIONALE IMPRESE ICT

UNIONE ARTIGIANI della Provincia di Milano

ASSOCIAZIONE ITALIA4BLOCKCHAIN

INFORMAZIONI SU QUESTA GUIDA

Esperti:

Andrea Caccia

Paolo Campegiani

Antonio La Marra

Donato Russo

Daniele Tumietto

Coordinatore:

Omar Dhaher

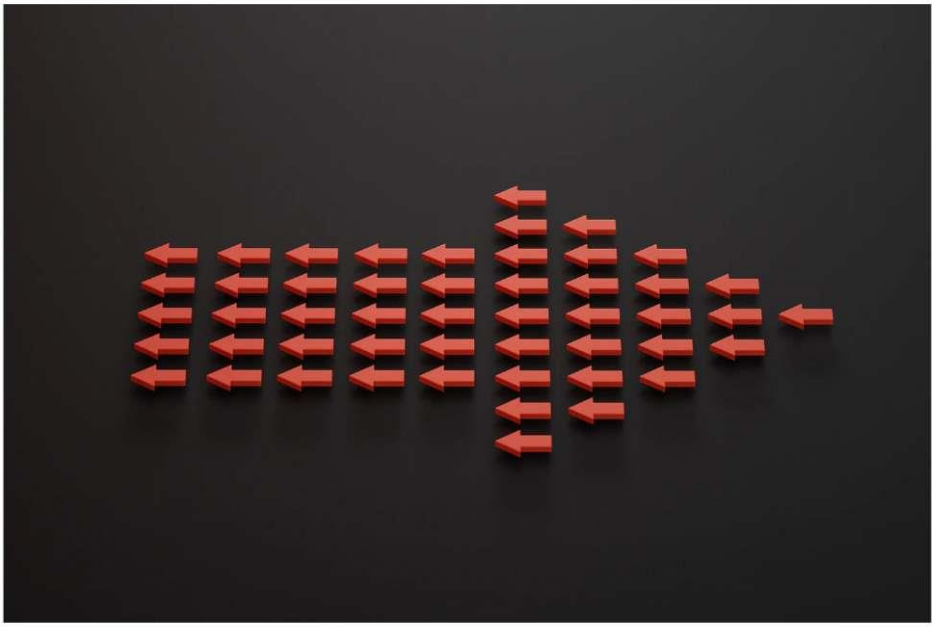
Pubblicato:

Aprile 2023

Questa guida mira a sensibilizzare le PMI nell'utilizzo corretto e appropriato della blockchain, elaborando sul contesto della presente quadro normativo Europeo e sull'importanza delle attività di standardizzazione.

La guida è stata elaborata nella sua versione originale in inglese dalla European DIGITAL SME Alliance e Small Business Standards (SBS).

La Guida è stata tradotta in italiano dalla Italian Digital SME Alliance con il contributo di ASSINTEL, CNA Milano, Italia4Blockchain e Unione Artigiani della Provincia di Milano.

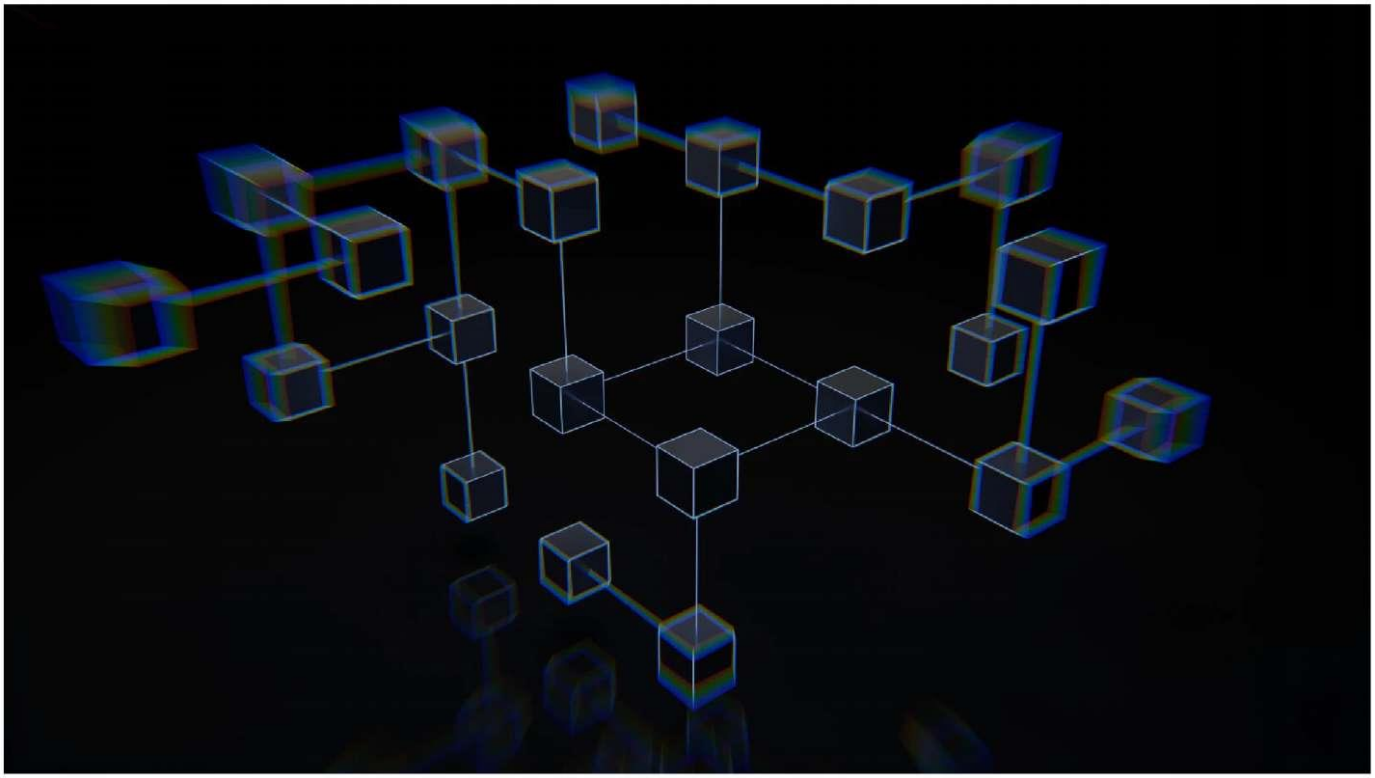


Elenco degli acronimi

AML	Antiriciclaggio
API	Interfaccia di programmazione delle applicazioni
BFT	Tolleranza ai guasti bizantina
DAO	Organizzazione autonoma decentralizzata
DApps	Applicazioni distribuite
EBP	Partenariato europeo Blockchain
EBSI	Infrastruttura europea dei servizi blockchain
eHDSI	Infrastruttura di servizi digitali per l'assistenza sanitaria online (eHealth)
eID:	Identificazione elettronica
eIDAS	Identificazione elettronica, autenticazione e servizi fiduciari
ESO	Organizzazioni europee per la standardizzazione
ESSIF	Quadro normativo europeo per l’identità auto-sovrana
EUDI	Identità digitale europea
GDPR	Regolamento generale sulla protezione dei dati
IoT	Internet delle cose
KYC	Conosci il tuo cliente
MiCA	Regolamento sui mercati dei cripto-asset
NFT	Token non fungibile
PoS	Proof-of-stake
PoW	Proof-of-work
SBS	Small Business Standards
SDO	Organizzazioni per lo sviluppo di standard
UI	Interfaccia utente
ZK Rollup	Rollup a conoscenza zero

INDICE DEI CONTENUTI

INTRODUZIONE



Negli ultimi anni, la European DIGITAL SME Alliance e Smal Business Standards (SBS) hanno pubblicato delle guide per sensibilizzare le PMI sulle tecnologie abilitanti come l'Internet delle cose o istruirle all'implementazione di standard specifici, come quelli sulla cybersecurity secondo le norme ISO/IEC 27001 e 27002.

Quest'anno, DIGITAL SME e SBS hanno preparato una guida su blockchain e DLT. Come tecnologia abilitante, la blockchain sta aiutando diversi settori a diventare più efficienti. L'agricoltura, il tessile, l'edilizia, l'ICT e la finanza utilizzano la blockchain per condividere e autenticare le transazioni in modo più rapido e decentralizzato o per migliorare la trasparenza della catena di approvvigionamento, combattendo le frodi e rafforzando la sostenibilità delle materie prime. La sezione 3 presenta quattro casi d'uso che mostrano come la blockchain possa rafforzare la sostenibilità nell'industria tessile, aiutare il settore delle costruzioni nelle certificazioni, garantire l'autenticazione e la fiducia nell'identificazione e rafforzare la risposta delle istituzioni alle questioni geopolitiche.

La blockchain trova applicazione in molti ambiti, anche a livello politico. Ad esempio, l'UE intende utilizzare la blockchain per rafforzare l'identificazione di persone e cose attraverso il regolamento eIDAS e ridurre le controversie contrattuali (soprattutto nell'economia dei dati) attraverso gli smart contract.

Gli standard sono essenziali per il funzionamento dell'identificazione elettronica e degli smart contract. Sono inoltre indispensabili per il funzionamento della blockchain nel suo complesso, poiché questa dipende da una struttura di database decentralizzati per i quali sono necessari standard per l'archiviazione, lo scambio di dati, la sicurezza e altri aspetti.

DIGITAL SME e SBS pubblicano questa guida con l'obiettivo di sensibilizzare le PMI sulla tecnologia e sul suo ruolo a sostegno dell'obiettivo dell'UE di guidare la trasformazione digitale e la transizione verde. La guida si rivolge ai manager delle PMI con l’obiettivo di fornire un'introduzione di base alla tecnologia blockchain, alle sue caratteristiche e alle aree in cui può essere utile per le attività quotidiane.

1. INTRODUZIONE A BLOCKCHAIN E DLT

1.1 Definizione di Blockchain e DLT

La Blockchain e la Distributed Ledger Technology sono un approccio sistematico e tecnologico al problema di trovare un accordo tra parti diverse su determinate circostanze. Per capire il problema, prendiamo come esempio il caso di un contesto sociale in cui un gruppo di amici deve decidere come trascorrere la serata, scegliendo tra andare al cinema o al ristorante. Ciascuna di queste scelte presenta opzioni diverse: quale film andranno a vedere? Quale ristorante potrebbe soddisfare tutti?

Molti di noi concordano sul fatto che questo tipo di decisione richiede molto tempo e che trovare una soluzione accettabile e gradita alla maggioranza delle persone può essere molto impegnativo. Questo problema è un'istanza specifica di un problema molto più generale: la costruzione del consenso (consensus-building) tra parti diverse.

La costruzione del consenso diventa più complicata quando ci spostiamo dal nostro ambiente sociale al mondo formale più rigoroso dei sistemi distribuiti, composto da sistemi autonomi, molto spesso gestiti da organizzazioni diverse e soggetti a organizzazioni diverse.

In un contesto normale, il consenso si raggiunge attraverso l'intervento di un'autorità centrale. Ad esempio, la banca centrale fornisce le garanzie per la valuta utilizzata dai cittadini. L'autorità centrale, tuttavia, è solitamente un ente burocratico, circostanza che rallenta le transazioni, mette a rischio la trasparenza e fa aumentare il rischio di frodi, come il riciclaggio di denaro. La frode si espande se l'autorità centrale non è indipendente in quanto gestita da uno stakeholder che persegue i propri interessi anziché quelli della società.

La blockchain si è rivelata la risposta alle inefficienze dei sistemi centralizzati. Il suo presupposto principale è rappresentato da un meccanismo di costruzione del consenso attraverso un sistema decentralizzato, in cui i partecipanti non possono agire in collusione o concordare qualcosa contrario alle regole, che aumenta la trasparenza, combattendo le frodi e dando vita a società più democratiche.

Per raggiungere questo obiettivo tecnico, la blockchain e la DLT sono definite come "un tipo di database decentralizzato, che elimina la necessità di un intermediario per elaborare, convalidare o autenticare le transazioni" [1].

L'invenzione del Bitcoin, nel 2009, da parte del gruppo di persone conosciuto con lo pseudonimo di Satoshi Nakamoto, ha rivoluzionato l'approccio alla costruzione del consenso, consentendo di raggiungerlo tra un numero quasi arbitrario di sistemi. Il sistema si basa su un approccio di teoria dei giochi. Si ipotizza un conflitto di interessi tra le diverse parti (sistemi distribuiti) e si progetta un insieme di meccanismi di incentivazione per aiutarle a raggiungere rapidamente un consenso.

Il consenso riguarda alcune transazioni, ovvero i trasferimenti di denaro virtuale (chiamato "bitcoin" con l'iniziale minuscola quando ci si riferisce alla valuta) tra diverse parti. Senza entrare nei dettagli sulle transazioni o sul modo in cui queste parti sono identificate nel sistema e potrebbero scambiarsi denaro, si evidenzia la presenza di un chiaro conflitto di interessi tra di loro.

Se A deve dare alcuni bitcoin a B (come parte di una transazione più ampia, ad esempio per pagare alcuni servizi o prodotti di B), A sarebbe ben felice di non pagare B (pur ricevendo i beni), mentre B, potendo scegliere, preferirebbe ricevere i bitcoin senza dare nulla in cambio. Ciò significa che sia A che B necessitano di un protocollo, ovvero un insieme di regole, con cui poter trovare un ragionevole compromesso. Questo problema che si verifica nel mondo digitale rispecchia ciò che accade nel mondo reale, dove generalmente A ripaga con denaro fisico B per i beni ricevuti. Molti meccanismi, di natura sociale, tecnica e legale, si fondano su questo scambio per renderlo sufficientemente sicuro per entrambe le parti.

[1] https://www.mas.gov.sg/development/fintech/technologies---blockchain-and-dlt

Nel mondo digitale, il problema risiede nel fatto che non possiamo fare affidamento solo su A o B, poiché esiste un conflitto di interessi, e prima dell'invenzione di Satoshi Nakamoto, dovevamo applicare un algoritmo di consenso primitivo noto come algoritmo BFT. In presenza di molte transazioni concomitanti (ad esempio, A ha una transazione con B e un'altra con C, poi c'è una transazione tra D ed E, ecc.), questi algoritmi non sono efficaci in quanto poco scalabili.

Bitcoin risolve questo problema raggruppando tutte queste possibili transazioni in blocchi e poi pone una sfida a chiunque sia interessato a risolverla: trovare una soluzione a un problema matematico, che richiede l'individuazione di un parametro che si inserisca in un punto specifico del blocco con tutte le transazioni, trasformando questo blocco "allargato" nella soluzione al problema. La soluzione è molto complessa da trovare (essenzialmente, richiede il controllo di tutti i possibili valori del parametro, fino a quando non si trova una soluzione soddisfacente), ma è molto semplice da verificare.

Per evitare qualsiasi falsificazione dei blocchi, oltre a contenere tutte le transazioni e questo parametro, ogni blocco contiene alcune informazioni sintetiche sul blocco immediatamente precedente nell'elenco. Supponendo che l'elenco dei blocchi sia composto da B1, B2, B3, B4 ..., il blocco B3 conterrà informazioni sintetiche (un collegamento crittografico) su B2; in questo modo, se B2 viene modificato dopo l'aggiunta di B3 alla catena, B3 non sarà più un blocco valido, e questo effetto si propagherà anche su B4 e tutti i blocchi successivi.

Questo è un approccio sostanzialmente probabilistico. Un avversario molto potente a cui non piace la struttura del blocco B3 (perché, ad esempio, contiene una transazione non gradita) è libero di calcolare un blocco B3 diverso (eliminando da esso la transazione non gradita) e di fornire blocchi alternativi (B4, B5, ecc.).

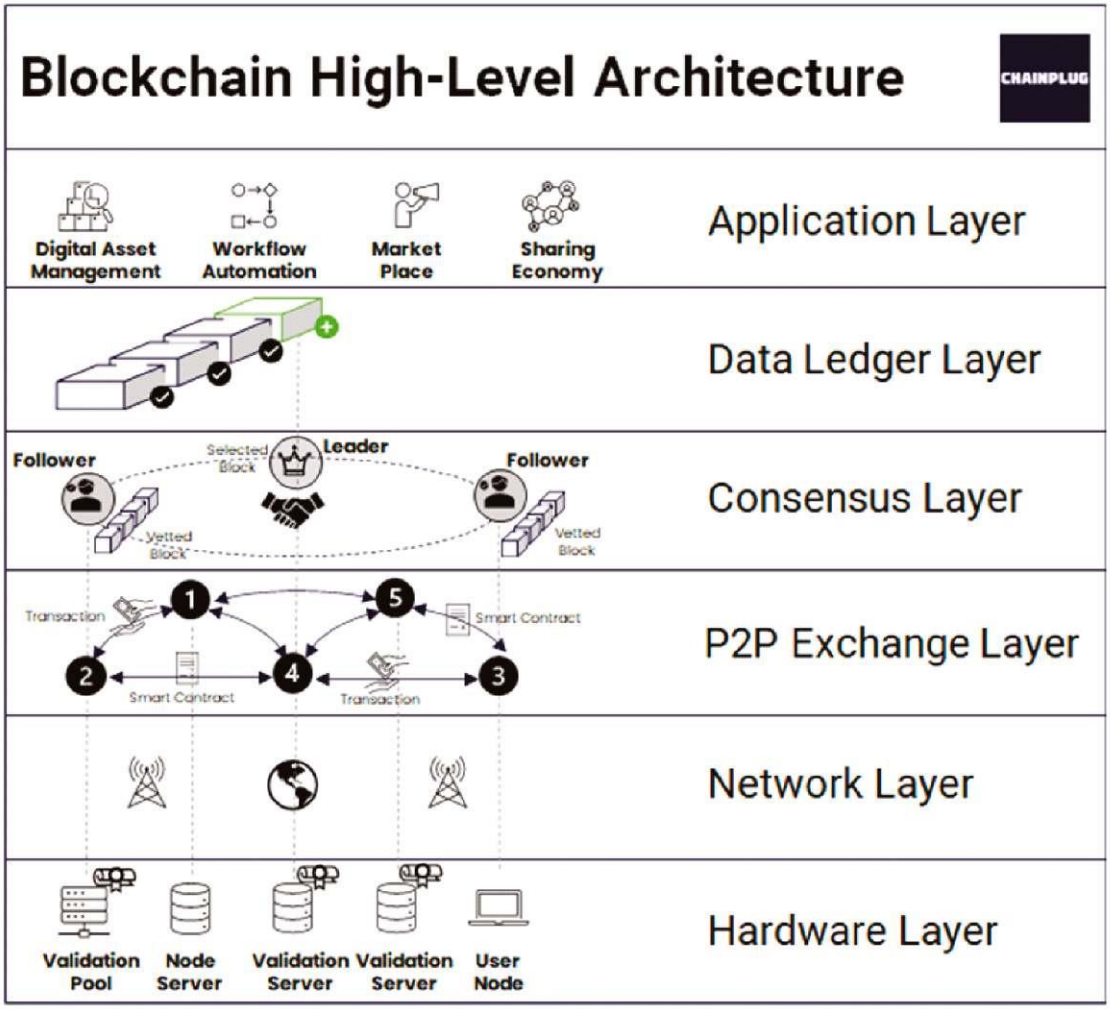
Nei prossimi paragrafi parleremo delle proprietà di un sistema blockchain. Ricapitolando, gli elementi che caratterizzano un contesto favorevole al successo dell'adozione di un sistema blockchain sono i seguenti:

1. Presenza di un gran numero di parti. Se il numero di parti è molto limitato (meno di venti), non c'è bisogno di un sistema blockchain perché gli algoritmi BFT saranno più veloci;
2. Queste parti sono entità paritarie, ovvero non c'è una parte che ha più potere delle altre nel decidere cosa è vero e cosa no. Ad esempio, una banca dovrà utilizzare un sistema blockchain per tenere traccia dei movimenti dei propri clienti, poiché ha più potere nel certificare i movimenti di un conto di risparmio rispetto al suo proprietario. Diversamente, per le interazioni con altre banche, la banca potrebbe scegliere di utilizzare un sistema blockchain, dato che sono tutte pressoché equivalenti.
3. Deve esistere una qualche forma di conflitto di interessi latente o possibile tra tutte le parti. Se tutte le parti sono disposte ad affidare a una tra esse un ruolo di coordinamento o di guida, allora questo leader potrebbe decidere in merito alle transazioni controverse.

In sintesi, le blockchain e, più in generale, i registri distribuiti sono un modo per creare un consenso tra entità alla pari (entità sullo stesso livello, che non possiedono un'autorità intrinseca maggiore delle altre) quando non è possibile presumere che tutti i partecipanti agiscano in buona fede.

1.1.1 I layer della blockchain

Il diagramma seguente mostra l'architettura di alto livello della blockchain.



L’architettura di blockchain è rappresentata da 4 layer:

1.1.1.1 Layer 0: Trasferimento dati e miner

Questo è il livello base dove è presente l’infrastruttura Internet, hardware e di connessione che permette il corretto funzionamento dei layer 1 come Bitcoin. Il layer 0 costituisce le fondamenta invisibili ma importanti quanto l'edificio stesso e può essere considerato un ponte tra Internet, il mondo fisico e la blockchain.

Nella tecnologia blockchain non c'è solo il software, ma anche un'infrastruttura di rete fisica che consente il funzionamento di una tecnologia complessa (la blockchain).

Il layer 0 permette di fare diverse cose:

Le blockchain possono interagire tra loro (interoperabilità)

- Cosmos è un esempio eccellente: crea un ecosistema di blockchain interoperabili grazie a un protocollo di comunicazione inter-blockchain chiamato Tendermint IBC. Altri esempi di questo livello sono Polkadot, Cardano e Avalanche.
- Per gli sviluppatori si tratta di soluzioni eccezionali. Se un'applicazione decentralizzata può essere eseguita su una blockchain, può automaticamente essere eseguita su altre blockchain se queste sono costruite con lo stesso layer 0.

Non è necessario investire altro tempo e risorse per costruire la stessa applicazione su un'altra catena.

Transazioni veloci ed economiche

- Con il protocollo Inter-Blockchain Communication, il consenso della Proof of Stake (PoS) può essere raggiunto su più catene ed è quindi possibile ottenere quasi immediatamente il risultato atteso. A livello funzionale, lo scopo è far approvare un blocco in modo che non possa più essere ritirato e sia quindi considerato irreversibile.

In questo modo, si ottengono transazioni più veloci e più economiche sugli scambi cross-chain.

Infrastruttura per sviluppatori

- Gli sviluppatori, infine, non devono partire da zero per costruire la loro blockchain, perché molte funzioni delle blockchain sono precostituite e pronte per essere implementate immediatamente.

1.1.1.2 Layer 1: blockchain

Il layer 1 è costituito dalle blockchain (Bitcoin ed Ethereum) che elaborano e finalizzano le transazioni sulla propria blockchain. È qui che avvengono processi come il consenso (PoW, PoS) e sono presenti tutti i dettagli tecnici come il tempo di blocco e la risoluzione delle controversie.

Questo layer è responsabile dei protocolli, dei meccanismi di consenso e di tutto ciò che garantisce la funzionalità di livello base di una blockchain e della criptovaluta (se presente). Viene anche chiamato Implementation Layer, alludendo alle possibilità di sviluppo.

Al centro del cosiddetto "trilemma" della blockchain vi sono i suoi tre aspetti principali[2]: decentralizzazione, sicurezza e scalabilità. Nessuna blockchain è ancora riuscita a soddisfare i tre criteri contemporaneamente. Altri esempi di questo layer sono Binance, Solana, Celo e Algorand.

Esiste un nuovo tipo di blockchain Proof-of-Stake Layer 1, come NEAR Protocol, sostenibile dalla progettazione, in virtù della sua neutralità climatica. Grazie alla scalabilità (100.000 transazioni al secondo), alle commissioni ridotte (<0,01 Dollari), a privacy shard (Calimero) e a una semplice procedura di onboarding che offre agli utenti un'esperienza familiare con il browser Web2, NEAR sta rapidamente conquistando il mercato.

1.1.1.2 Layer 2: velocità e scalabilità

Un aspetto non sempre chiaro che genera discussioni è ciò che si intende con Layer 2. La definizione non così comune deriva dalla considerazione che progetti diversi utilizzano il Layer 2 per attività diverse. Consideriamo, ad esempio, Lightning Network (un aggiornamento della scalabilità di bitcoin). Funziona come livello di implementazione secondario rispetto al Layer 1.

Dopo tutto, gli smart contract, caratteristica centrale di Ethereum e di molti altri protocolli Layer 1, sono applicazioni costruite direttamente sul layer di implementazione. Immaginiamo che il Layer 2 rappresenti il livello in cui vengono sviluppati gli aggiornamenti aggiuntivi e le applicazioni generalizzate prodotte nel Layer 1.

[2] Il problema è noto come Trilemma (secondo la definizione del fondatore di Ethereum Vitalik Buterin) e consiste nel fatto che, sulla base della loro attuale progettazione, le principali Blockchain, come Bitcoin ed Ethereum, non possono avere contemporaneamente le caratteristiche di decentralizzazione, sicurezza e scalabilità.

In generale, la decentralizzazione e la sicurezza sono caratteristiche presenti in tutte le Blockchain. Non si può invece dire lo stesso della scalabilità, ovvero la capacità di una Blockchain di adattarsi alla costante crescita del numero di nodi e utenti a cui è sottoposta e quindi di supportare un'elevata capacità transazionale e una crescita futura senza che le prestazioni ne risentano.

Uno dei problemi principali delle blockchain permissionless più famose è proprio quello della scarsa scalabilità. Diversi sviluppatori di Blockchain hanno proposto varie soluzioni e nuovi protocolli di secondo livello (Second Layers Protocol) con l'obiettivo di risolvere i problemi dei protocolli di livello inferiore per gestire il problema della scalabilità, senza tuttavia trovare una vera soluzione al Trilemma. A oggi, Agorand, la Blockchain ideata da Silvio Micali, è l'unica ad aver risolto il Trilemma al primo layer (First Layers Protocol).

Attualmente, il Layer 2 è l'area che suscita maggiore interesse. Da quando Ethereum ha mostrato la possibilità di utilizzare una blockchain generalizzata per sviluppare applicazioni ristrette e specifiche, molti sviluppatori e investitori si sono lanciati in questa impresa.

I Layer 2 sono considerati i layer di scalabilità e le integrazioni di terze parti sono utilizzate in combinazione ai Layer 1 per aumentare la scalabilità e le transazioni al secondo.

- Quando si sente parlare di rollup a conoscenza zero o rollup ZK[3], sidechain[4] , o di qualsiasi cosa abbia a che fare con la velocizzazione del throughput delle transazioni, è probabile che si tratti di Layer 2.
- Esempi di questo layer sono Polygon, Starknet, Arbitro e Optimism.

1.1.1.4 Layer 3: applicazioni

Il Layer 3 potrebbe diventare il livello di maggior successo in futuro, anche se al momento è poco apprezzato. Il Layer 3 è il luogo in cui le applicazioni generiche, sviluppate sul Layer 2, possono essere utilizzate per sviluppare soluzioni specifiche. Utilizzando tecnologie come smart contract, atomic swap o API, gli sviluppatori possono integrare soluzioni e creare applicazioni che svolgono funzioni estremamente verticali. I casi tipici in quest'ambito sono DeFi o NFT.

Volendo sintetizzare al massimo il concetto, si potrebbe affermare che il Layer 3 è considerato come l'interoperabilità ed è l'interfaccia utente (UI) con cui noi consumatori interagiamo effettivamente.

1.2 Perché usare la Blockchain

Attualmente, il primo motivo per cui si utilizza una blockchain è il trasferimento di valore (criptovalute). Questa tecnologia è cresciuta in maniera esponenziale grazie a Bitcoin. Il secondo motivo è la registrazione delle transazioni con un metodo a prova di manomissione non gestito/certificato da alcuna autorità terza designata.

In realtà, l'ambito di utilizzo della blockchain sarà molto più ampio nel medio-lungo termine, in quanto eliminerà gli intermediari nella gestione della fiducia. Oltre ad avere un enorme impatto economico, in quanto consentirà interazioni più rapide, questo aspetto ridurrà i costi e supporterà informazioni certificate, ma potrebbe anche riorganizzare profondamente il modo in cui le nostre società saranno governate in futuro.

L'abilitazione di transazioni affidabili direttamente tra due o più parti, autenticate da una collaborazione di massa e alimentate da interessi personali collettivi, limiterà infatti gli intermediari della fiducia (individui, aziende, governi) che possono distorcere il valore delle cose, la percezione della realtà (informazioni false), o addirittura limitare le libertà degli individui. Eliminando in qualche misura gli intermediari, si promuoverà anche una forte interoperabilità a sostegno di nuovi modelli di interazione che oggi sono fortemente limitati dai conflitti di interesse.

Blockchain private e pubbliche

La differenza principale tra blockchain pubbliche e private si basa sulla possibilità di registrare liberamente le informazioni.

[3] Un rollup a conoscenza zero è un protocollo di blockchain di Layer 2 che elabora transazioni, esegue calcoli e archivia dati off-chain, mentre detiene asset in uno smart contract on-chain. Naturalmente, le blockchain tradizionali di Layer 1 come Ethereum convalidano i blocchi e le transazioni on-chain.
[4] Una sidechain è una rete blockchain separata che si connette a un'altra blockchain - chiamata blockchain madre o mainnet - tramite un peg bidirezionale.

Una blockchain pubblica, o permissionless, non richiede alcuna autorizzazione per accedere ai dati registrati, per eseguire transazioni o per partecipare alla convalida delle transazioni e alla creazione di nuovi blocchi. Le blockchain pubbliche non presentano alcun filtro per i meccanismi di funzionamento e la partecipazione alla stipula delle transazioni, come nel caso dei più noti Bitcoin ed Ethereum.

Nel modello di blockchain privato, cosiddetto "permissioned", solo i partecipanti identificati e autorizzati dall'iniziatore della blockchain sono autorizzati a scrivere dati e a convalidare transazioni, mentre le informazioni sono visibili a tutti, anche se non sempre decifrabili e utilizzabili. Il tipo di blockchain privata è creato da un'entità creatrice che identifica i partecipanti e determina i limiti delle transazioni registrabili su tale blockchain.

Il processo di formazione del consenso (come il consorzio Blockchain) è controllato da un insieme preselezionato di nodi (le cosiddette blockchain parzialmente decentralizzate): questa gerarchia tra i nodi impedisce la perdita di informazioni di business intelligence. Quando si aggiungono informazioni, il sistema di approvazione non è vincolato dalla maggioranza dei partecipanti, ma da un piccolo numero.

Il sistema sembra ideale per le istituzioni o le grandi aziende che devono gestire catene di fornitura con una serie di attori, imprese, fornitori o subfornitori. Garantisce un livello di privacy più elevato, poiché non vengono concessi permessi di accesso o di lettura. I nodi sono ben collegati tra loro e qualsiasi malfunzionamento o errore può essere facilmente risolto. Le transazioni sono più economiche perché vengono verificate da pochi nodi con un'elevata potenza di elaborazione.

La differenza più rilevante tra i due tipi di blockchain è l'autenticità delle informazioni che determina le conseguenze tra il contenuto della transazione e il suo effetto. Nelle blockchain private, questo comporta delle difficoltà per l'utente che deve accertarsi della veridicità di un'informazione registrata.

2. CARATTERISTICHE DELLA BLOCKCHAIN E DELLA DLT

2.1 Sicurezza

Il termine blockchain è stato spesso usato in stretta relazione alla cybersecurity. Questi due termini non sono del tutto estranei: per mantenere un registro coerente, immutabile e distribuito sono state utilizzate diverse tecnologie come la firma digitale e le funzioni di hash. La tecnologia blockchain è stata utilizzata anche in alcuni prodotti per migliorare la sicurezza, soprattutto in termini di registrazione.

Tuttavia, è un errore considerare le blockchain e le applicazioni da esse derivate sicure di default. Negli ultimi tempi, come accade per le tecnologie più diffuse, sono stati sviluppati nuovi attacchi alle applicazioni blockchain (in particolare ai mercati delle criptovalute), che hanno avuto un impatto significativo sui portafogli personali causando la perdita del denaro investito, nella maggior parte dei casi non recuperabile.

Per contro, le criptovalute, come i bitcoin, sono state ampiamente utilizzate da ransomware[5] e cryptolocker e sono stati sviluppati nuovi attacchi nel tentativo di sfruttare l'hardware delle vittime per estrarre criptovalute come Monero e Bitcoin.

2.1.1 Sicurezza organizzativa

La tecnologia blockchain è utilizzata raramente per garantire aspetti specifici della sicurezza nel contesto di un'organizzazione estesa.

[5] Un malware utilizzato dagli hacker che blocca il sistema criptando i file e l'hacker chiede un riscatto per decriptarli. Per ulteriori informazioni sui malware consultare la Guida SBS sui controlli di sicurezza delle informazioni.

Quando è necessario tracciare i beni, o manca la fiducia reciproca tra i diversi attori, oppure quando è necessario un registro che possa essere sempre verificato, la blockchain è la risposta. Esistono alcuni progetti importanti, soprattutto nel settore agroalimentare che, grazie alla blockchain, consentono ai consumatori di tracciare i prodotti fino alla loro origine. Questo permette di aumentare la fiducia tra clienti e fornitori.

Per sicurezza dell'informazione si intende l'insieme di tecnologie, mezzi e procedure che garantiscono tre caratteristiche fondamentali dell'informazione: la **riservatezza,** ossia solo il destinatario può leggere il messaggio; l'**integrità,** ossia il messaggio non può essere manomesso senza che il destinatario riconosca la modifica; la **disponibilità,** ossia il destinatario è libero di scegliere quando leggere il messaggio.

Le tecnologie e le applicazioni blockchain sono utilizzate in particolare per garantire l'integrità nel senso di non ripudio: poiché i blocchi sono concatenati, nessun aggressore può alterare un messaggio senza che il sistema riconosca la modifica. Gli algoritmi della blockchain possono proteggere bene l'integrità. Poiché non esiste un punto centrale di fiducia e i nodi raramente sono distribuiti in diverse parti del mondo, è di estrema importanza garantire che, se uno dei nodi è compromesso, non possa causare alcun danno. Le tecnologie blockchain sono molto utili anche per garantire la disponibilità delle informazioni: poiché un nodo blockchain può essere eseguito in diverse parti della rete, si può ottenere una maggiore vicinanza rispetto a un classico sistema cloud. Ovviamente c'è un prezzo da pagare in termini di performance, perché l'inserimento delle informazioni richiede più tempo rispetto a un sistema cloud classico.

Per garantire l'integrità delle informazioni, la tecnologia blockchain fa leva sulle cosiddette funzioni di hash sicure che mettono il contenuto al riparo da eventuali modifiche. La funzione di hash si può paragonare a un riassunto digitale del testo. La modifica del testo ha un forte impatto sul riassunto risultante.

2.1.2 Sicurezza informatica

La sicurezza della blockchain richiede un approccio diverso rispetto alla sicurezza tradizionale, per determinati motivi:

1. In un ambiente blockchain non c'è fiducia reciproca tra peer e sistemi. Pertanto, tutti possono essere attori malevoli che cercano di perseguire i propri interessi. Di conseguenza, occorre esaminare ogni parte del software e ogni sistema che lo esegue.
2. Il tipo di blockchain utilizzato influenzerà i vettori di attacco impiegati. Ad esempio, le criptovalute possono essere soggette a schemi Ponzi[6], oppure gli investitori possono perdere tutto (è successo con le monete meme di Squid Game), perché chi aveva proposto l'investimento sparisce una volta incassato il denaro.
3. Gli algoritmi utilizzati per valutare la fiducia o per generare fiducia possono presentare bug o vulnerabilità che li rendono facilmente violabili.
4. La necessità di utilizzare un numero significativo di risorse per verificare che una transazione possa essere eseguita limita il numero di attori.
5. Il controllo dell'identità è un fattore chiave. Infatti, chi è in grado di creare molte identità false, può manipolare il mercato per promuovere un algoritmo o l'altro, mostrando un falso incremento dei progetti che utilizzano uno specifico algoritmo.
6. Gli influencer possono manipolare il mercato abbastanza facilmente. Un esempio a questo riguardo sono i tweet di Elon Musk che hanno dato impulso a Shiba Coin.

Anche se alcune di queste motivazioni non sono direttamente correlate agli attacchi informatici, sono comunque legate alla sicurezza informatica in quanto le persone colpite possono subire perdite di denaro, di reputazione o danni nella vita reale a causa di disinformazione o comportamenti scorretti.
[6]

[6] Secondo investopedia.com, uno schema Ponzi è una "truffa di investimento fraudolento che genera rendimenti per i primi investitori con il denaro ottenuto dagli investitori successivi".

Inoltre, la tecnologia blockchain è troppo spesso vista come una soluzione diretta e immediata per la sicurezza informatica. Purtroppo, le persone sembrano troppo attratte da soluzioni facili a problemi complessi. La dura verità è che i problemi complessi, come la sicurezza informatica, richiedono soluzioni semplici e un approccio attento.

L'angolo dell'esperto

Recentemente, un'azienda di nome Halborn ha rilasciato una versione specifica di Kali Linux per eseguire una valutazione delle vulnerabilità e test di penetrazione sulla blockchain. Se la blockchain fosse così sicura da non richiedere ulteriori test, pensate che un'azienda avrebbe investito tempo e denaro nella creazione della propria distribuzione Linux?

2.2 Identità di persone, organizzazioni, cose e dati

La verifica delle identità di diversa natura (persone, organizzazioni, cose e dati) è un problema vecchio quanto Internet. Negli ultimi anni sono state implementate diverse soluzioni, in particolare, sistemi di autenticazione basati su strumenti di autenticazione assegnati alle identità delle persone. Tecnologie simili possono essere utilizzate per l'identificazione delle organizzazioni, poiché in generale è possibile collegare un'organizzazione con figure umane a cui sono assegnati mezzi di identificazione. Questi mezzi di autenticazione si basano sull'uso di fattori di autenticazione come nomi utente e password per i livelli di base di garanzia, con fattori aggiuntivi (tipicamente fisici e biometrici) per supportare livelli di garanzia sostanziali ed elevati.

Per aumentare la sicurezza delle informazioni e dei dati (personali), sono state create password complesse. Tuttavia, le password copiate o craccate non hanno risolto il problema dell'accesso a un'enorme quantità di dati. L'Internet delle cose (IoT), dove gli oggetti fisici recuperano, generano e trasferiscono dati, pone nuove sfide all'identificazione degli oggetti connessi a Internet e dei dati che consumano e generano.

L'Unione europea, con il Regolamento eIDAS (electronic IDentification, Authentication, and trust Services), ha fornito un quadro normativo per l'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche a sostegno del mercato europeo comune.

Un'altra iniziativa chiave è l'European Self-Sovereign Identity Framework (ESSIF), parte dell'European blockchain service infrastructure (EBSI), un'iniziativa congiunta della Commissione europea e della European Blockchain Partnership (EBP). Si tratta di un approccio all'identità digitale che dà agli individui il controllo sulle informazioni e sui dati che utilizzano per dimostrare la loro identità a siti web, servizi e applicazioni in tutto il web, in linea con l'approccio adottato nel contesto della revisione del regolamento eIDAS (noto come eIDAS2) con il portafoglio europeo di identità digitale (EUDI).

Tuttavia, sia eIDAS2 che ESSIF fanno riferimento all'identità di persone e organizzazioni, ad esempio, portafogli per persone fisiche e giuridiche, eID e dispositivi IoT collegati all'identità di una persona fisica o giuridica. Le identità delle cose e dei dati, negli attuali scenari di condivisione dei dati, non possono essere gestite autonomamente come oggetti: allo stato attuale, manca un'identità delle cose automaticamente certificata e affidabile.

Il concetto di gemello digitale può aiutare a fornire una rappresentazione digitale delle caratteristiche rilevanti degli oggetti fisici in un modello digitale che ne rappresenti le relazioni e le dipendenze reciproche e con le persone, le organizzazioni e gli oggetti nativi digitali.

La tecnologia blockchain potrebbe superare l'incapacità di tali oggetti di interagire in modo diverso a ogni diversa transazione. Più in generale, l'esigenza è quella di supportare un'identificazione corretta, continua e decentralizzata di persone, organizzazioni, cose e dati come elemento fondante che abilita tutta una serie di applicazioni.

Ad esempio, è prevedibile che le "cose" - come i robot industriali e commerciali - una volta identificate in modo univoco siano in grado di effettuare o ricevere pagamenti al completamento di un determinato lavoro assegnato.

Un altro esempio riguarda il contesto del passaporto digitale dei prodotti (DPP), l'elemento chiave a sostegno della proposta di regolamento sulla progettazione ecocompatibile dei prodotti sostenibili[7] nell'ambito delle iniziative della Commissione per far sì che i prodotti sostenibili diventino la norma[8]. La divulgazione delle informazioni sul prodotto nel DPP sotto il controllo del suo proprietario dovrebbe poter avvenire in modo simile alle informazioni personali nell'identità auto sovrana per gli esseri umani.

Un'altra iniziativa politica in cui la blockchain ha un ruolo chiaro è il Data Act, in cui gli Smart Contract sono i mezzi previsti per supportare lo scambio di dati e la loro remunerazione, sulla base del concetto di Data Spaces.

Gli smart contract della Blockchain accoppiati alle identità e ai portafogli degli oggetti potrebbero quindi eseguire autonomamente le transazioni di pagamento relative ai servizi prestati, consentendo di convergere verso una soluzione unica per l'identificazione di persone, organizzazioni, cose e dati.

2.3 Autenticazione e autorizzazioni

Le blockchain e i registri distribuiti possono essere permissionless o permissioned, a seconda di come (e se) gli utenti devono essere riconosciuti dal sistema prima di interagire con esso.

In un sistema permissionless, l'unico requisito richiesto a un utente per creare una transazione con lo stesso è quello di aderire ad alcune specifiche tecniche. Ad esempio, nel protocollo Bitcoin, un utente può interagire con il sistema se possiede una chiave privata. Questa chiave, simile alla chiave privata necessaria per un sistema di firma digitale, potrebbe essere generata autonomamente dall'utente. Questo è l'unico modo per l'utente di effettuare transazioni con gli altri e consente di disporre completamente degli asset all'interno del sistema. Quando un utente possiede questa chiave, può firmare le transazioni sulla blockchain di Bitcoin. Questo approccio bottom-up ha però un chiaro svantaggio: se gli utenti perdono la chiave, non c'è un modo intrinseco per recuperarla; quindi tutti gli asset digitali associati a quella chiave (come i cripto-asset) andrebbero persi.

Le blockchain sfruttano l'approccio opposto, ovvero quello permissioned. In questo caso, gli utenti del sistema hanno un'identità prima di interagire con il sistema e devono autenticarsi prima di utilizzarlo. È molto simile a un servizio online tradizionale, in cui l'utente si autentica e poi accede alle proprie risorse (ad esempio, l'e-mail), gestendole come desidera. Questo approccio ha il vantaggio di consentire agli utenti di essere più protetti contro la perdita dei propri dati di accesso, poiché di solito è possibile recuperarli (in modo simile alla funzione di recupero della password fornita da un servizio online).

Sottolineiamo che la distinzione tra sistema permissioned e permissionless avviene a livello di protocollo. Sebbene il Bitcoin sia permissionless, al giorno d'oggi sarebbe molto difficile per un utente rimanere completamente anonimo durante le transazioni. In genere, l'utente effettua le transazioni attraverso alcuni intermediari specializzati, chiamati exchange, che devono identificare le persone in base alle norme antiriciclaggio (AML) o "conosci il tuo cliente" (KYC). Anche se gli utenti realizzano l'infrastruttura per l'accesso diretto all'infrastruttura Bitcoin, necessitano comunque di qualcuno con cui effettuare transazioni, e la controparte potrebbe essere costretta a identificare la parte corrispondente. Pertanto, la transazione è anonima solo a livello di protocollo e non a livello di interfaccia utente. Questo problema è spesso riferito alla centralizzazione delle blockchain, ritenuta una promessa mancata dai detrattori di questa tecnologia.

[7] https://environment.ec.europa.eu/publications/proposal-ecodesign-sustainable-products-regulation en
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0140

2.4 Governance

Attualmente non è presente una governance distribuita nelle blockchain, nonostante sia tanto importante quanto la decentralizzazione nella certificazione delle transazioni. Senza una governance decentrata, la definizione delle regole iniziali è in mano a un numero limitato di partner. Pertanto, è molto difficile scalare le blockchain per nuovi utenti che potrebbero avere esigenze e aspettative completamente diverse. Inoltre, l'accettazione di queste regole potrebbe persino essere altamente dannosa per gli utenti nel medio-lungo periodo, in un modo molto difficile da prevedere all'inizio, oppure i governi potrebbero decretarne l'inaccettabilità/illegalità dopo l'introduzione di nuovi standard e regole. Ciò implica anche che ogni blockchain avrà la propria architettura/codice e quindi non è possibile che un ampio gruppo di utenti definisca e concordi standard per ottenere l'interoperabilità. Decentramento o centralizzazione?

3. CASI D'USO A SUPPORTO DELLA STANDARDIZZAZIONE, DELLA SOSTENIBILITÀ E

La catena di distribuzione (supply chain) rappresenta oggi il terreno d'elezione per l'applicazione della tecnologia blockchain.

L'OCSE, la cui missione principale è sostenere e guidare i governi nella cooperazione per un'economia globale più equa, più forte e più pulita, aveva già evidenziato dati allarmanti, secondo i quali il valore del commercio internazionale di beni contraffatti ammontava a 461 miliardi di dollari. Dalle informazioni raccolte in collaborazione con le autorità doganali, è emerso che la contraffazione rappresenta il 2,5% del valore totale del commercio mondiale (comprese le contraffazioni alimentari).

Per un produttore è fondamentale poter ricostruire l'origine delle materie prime, dei semilavorati, nonché il luogo e il metodo di lavorazione dei prodotti, per evitare pesanti sanzioni penali e amministrative.

Per gli imprenditori, l'introduzione della nuova tecnologia blockchain può rappresentare quindi una garanzia di tutela e uno strumento di prevenzione della contraffazione, oltre che un mezzo per aumentare la sostenibilità del mercato di riferimento, con evidenti ricadute positive sul valore reputazionale.

Aspetti operativi e vantaggi della tracciabilità della blockchain

- Decentramento: distribuzione tra più nodi delle informazioni per garantirne la sicurezza informatica e la resilienza. Tracciabilità dei trasferimenti: possibilità di risalire all'origine esatta di ogni informazione.
- Disintermediazione: le transazioni sono gestite senza intermediari, cioè in assenza di entità centrali fidate.
- Trasparenza e verificabilità: immutabilità del registro, ovvero i dati registrati non possono essere modificati senza il consenso di tutti i partecipanti.
- Programmabilità dei trasferimenti: la possibilità di programmare determinate azioni, al verificarsi di determinate condizioni.

Va notato che l'impossibilità di modificare le informazioni inserite nei blocchi impedisce qualsiasi manomissione successiva. L'infrastruttura tecnologica è rafforzata dal sistema di certificazione temporale (data e ora in cui i dati vengono consolidati), in conformità con il regolamento eIDAS "Electronic Identification and Trust Services Regulation".

Vantaggi

Tracciabilità, trasparenza, sostenibilità: questi sono i vantaggi per un produttore che permette al suo consumatore di orientare liberamente le proprie scelte di acquisto.

Autenticità

Questa caratteristica rafforza il legame tra il marchio e il consumatore, che può verificare non solo l'autenticità del prodotto, ma anche le stesse fasi di lavorazione.

Riduzione dei rifiuti

La tracciabilità degli alimenti può aumentare l'efficienza dei processi della catena di approvvigionamento, migliorando la gestione delle scorte, riducendo gli sprechi alimentari e rafforzando le relazioni di filiera.

I seguenti casi d'uso illustrano le soluzioni offerte dalla blockchain ai problemi esistenti e il suo contributo al progresso dell'innovazione in molti settori con particolare attenzione alla sostenibilità.

Caso 1: L'anagrafe

Descrizione

In un Paese del terzo mondo, a causa di complessi processi storici e culturali, esistono più versioni diverse dell'anagrafe, gestite da autorità diverse. Alla nascita, i genitori scelgono un nome per il proprio figlio o la propria figlia che cresce con questo nome (ipotizziamo Luca). I genitori non registrano personalmente il nome presso la sezione locale dell'anagrafe, poiché la registrazione viene effettuata da un'altra persona, ad esempio un medico, un'ostetrica o un capo tribù. Luca è noto con questo nome all'autorità di polizia locale, che gestisce una copia dell'anagrafe per le proprie finalità.

Il problema

Un giorno, Luca decide di richiedere il passaporto, perché vuole fare un viaggio all'estero. Durante il controllo dei precedenti, i dati della copia dell'anagrafe in possesso della polizia confermano che il suo nome è Luca, ma i dati della copia dell'anagrafe in possesso del consiglio sanitario dicono altro: l'ostetrica lo ha registrato come John, perché lo riteneva un nome migliore o a causa di un errore di comunicazione con i genitori di Luca.

Dal momento che queste due fonti di dati sono ritenute entrambe autorevoli e non sono allineate, il problema appena sperimentato da Luca con il passaporto potrebbe ripetersi in futuro, quando richiederà altri documenti del suo Paese di nascita o sarà coinvolto in processi che richiedono queste informazioni.

La soluzione

Le blockchain e le DLT potrebbero essere efficaci nella gestione di questo tipo di discrepanze che si verificano quando due o più parti, ciascuna con una certa autorità su una questione specifica, devono trovare un accordo su una questione condivisa.

Nel caso di Luca, le diverse copie del registro dell'anagrafe, gestite da più autorità diverse a livello nazionale, regionale o locale, potrebbero dare a una blockchain o a una DLT il potere di attestare il loro consenso sul nome di Luca. Un approccio di alto livello prevederebbe una serie di fasi: nella prima, i diversi detentori dei dati si accordano sul nome di Luca (quindi, tutti concordano sul fatto che il nome di questa persona è, effettivamente, Luca: questo potrebbe accadere con un processo aziendale specifico i cui dettagli non sono di interesse in questa sede) e ognuno di loro, nella seconda fase, prevede una transazione il cui esito è un'affermazione del tipo "per me, la persona che chiamo Luca/John/... è effettivamente Luca". Ciascuno di questi registri non deve modificare i propri dati, ma dovrà essere dotato di un livello di conformità che consenta di attestare (autenticare) il raggiungimento di un accordo. Ognuno di questi registri partecipa alla blockchain, che in questo caso è un sistema privato permissioned: avere una copia della blockchain permette a ogni parte (titolare dell'anagrafe) di monitorare ciò che sta accadendo. La scrittura nella blockchain di una transazione composta da tutti questi diversi accordi sul nome di Luca certifica che tutte le parti concordano su questo punto.

Ipotizziamo ora che Luca voglia richiedere il suo fascicolo sanitario dal consiglio sanitario locale. Grazie al nuovo livello di conformità, quando il sistema rileva una richiesta a nome di Luca, capisce che Luca è conosciuto come John al consiglio sanitario locale e recupera le informazioni che lo riguardano con questo nome diverso.

Generalizzazione

Il lettore potrebbe pensare che la soluzione più efficace al problema di Luca sarebbe quella di modificare semplicemente i suoi dati all'interno di alcuni sistemi. Questa operazione potrebbe essere più o meno possibile a seconda dello stato tecnologico attuale di questi sistemi. Se si considera una generalizzazione più ampia, ad esempio a livello internazionale, l'approccio basato su blockchain e DLT risulta più efficace.

Ad esempio, gli Stati membri dell'UE fanno parte dell'infrastruttura di servizi digitali per la sanità elettronica (eHDSI), che consente a due Stati membri di scambiare alcuni dati sulla sanità elettronica quando, ad esempio, una persona nata nel Paese A ha bisogno di servizi medici nel Paese B. L'eHDSI stabilisce una connessione funzionante tra i due paesi. Tuttavia, l'intero processo di richiesta dei dati del paziente potrebbe fallire perché il Paese d'origine non è in grado di fornire tali dati in modo tempestivo, con una possibile degradazione dei servizi sanitari forniti dal Paese B. Ognuno di questi Paesi è uno Stato sovrano, quindi deve anche essere in grado di dimostrare che i dati sono stati richiesti e che sono stati forniti. La soluzione potrebbe essere la creazione di una blockchain condivisa da tutti gli Stati membri dell'UE, in cui questi due Paesi potrebbero memorizzare le richieste e le forniture di dati (non i dati veri e propri, solo le richieste e le risposte). Poiché questa blockchain è condivisa da tutti gli Stati membri dell'UE, se sorge un conflitto tra A e B, consultando velocemente il registro risulta subito chiaro se i dati sono stati forniti o meno[9].

Altre possibili generalizzazioni sono rappresentate dagli schemi di gestione dei crediti di carbonio. A ogni Paese è stata assegnata una determinata quantità di emissioni di CO_2, ma potrebbe inquinare di più acquistando crediti da Paesi più puliti. Anche in questo caso, poiché è necessario garantire che questo scambio non venga ripudiato in futuro, la soluzione potrebbe arrivare da una blockchain globale.

Abbiamo proposto una generalizzazione a livello internazionale solo perché rende più chiaro che per l'integrazione in un sistema globale le diverse organizzazioni potrebbero avere processi diversi. In sistemi più locali, potrebbe essere necessario stipulare questo tipo di accordi tra diverse parti, come i sistemi di assistenza sociale locali, le comunità energetiche locali e simili.

[9] Per approfondire, si rimanda a Castaldo, L., Cinque, V. (2018)

Caso 2: Il processo di certificazione nel settore delle costruzioni

Nel mercato internazionale di oggi, le organizzazioni vogliono essere conosciute per la loro adesione agli standard di assicurazione qualità e di produzione, come ad esempio, la certificazione dell'Organizzazione Internazionale per la Standardizzazione (ISO) e di altre organizzazioni indice di credibilità e fiducia tra consumatori, stakeholder e altri partner commerciali. In effetti, una certificazione di livello ISO garantisce che il richiedente soddisfi gli standard globali di settore, soprattutto in ambito commerciale.

L'industria delle costruzioni, come molti altri settori, deve certificare alcuni aspetti della produzione: dalla gestione della qualità alla gestione della salute e della sicurezza nei cantieri, e altro ancora. La certificazione è quindi una parte fondamentale del processo di costruzione. Ecco che cosa significa richiedere la certificazione ISO:

1. Il richiedente deve scegliere il tipo di certificazione ISO necessaria per il proprio settore edile.
2. Deve scegliere un organismo di certificazione ISO riconosciuto e credibile (ISO Registrar).
3. Deve presentare una domanda con l'apposito modulo indicando gli aspetti legati alla responsabilità, alla riservatezza e ai diritti di accesso.
4. L'organismo di certificazione ISO esaminerà tutti i documenti relativi alle varie politiche e procedure seguite nell'organizzazione. Il richiedente deve preparare un piano d'azione per eliminare eventuali lacune.
5. Successivamente, l'ISO Registrar condurrà un'ispezione fisica in loco per verificare le modifiche apportate all'organizzazione.
6. Non appena l'organismo di certificazione approva il sistema di gestione del richiedente, questi otterrà lo standard ISO richiesto.

A. Il problema

Un imprenditore edile, che aveva fatto domanda per un processo di richiesta-approvazione per ottenere una certificazione, ha dovuto affrontare una procedura lunga, costosa e dispendiosa in termini di tempo. Le certificazioni ISO e simili non soddisfano i nuovi e imminenti standard digitalizzati. Il recupero e lo scambio dei documenti richiedono molto tempo: le certificazioni vengono effettuate per lo più tramite carta, e-mail e file PDF.

La mancanza di tecnologia, oltre a prolungare i tempi necessari all'appaltatore per ottenere la certificazione, ha rappresentato un potenziale pericolo per la sua attività. L'appaltatore non riusciva a trovare un modo semplice per promuovere la certificazione ISO tra gli organismi di certificazione, le autorità, le autorità pubbliche e i clienti.

Frustrato da questo processo, l'appaltatore ha deciso di agire.

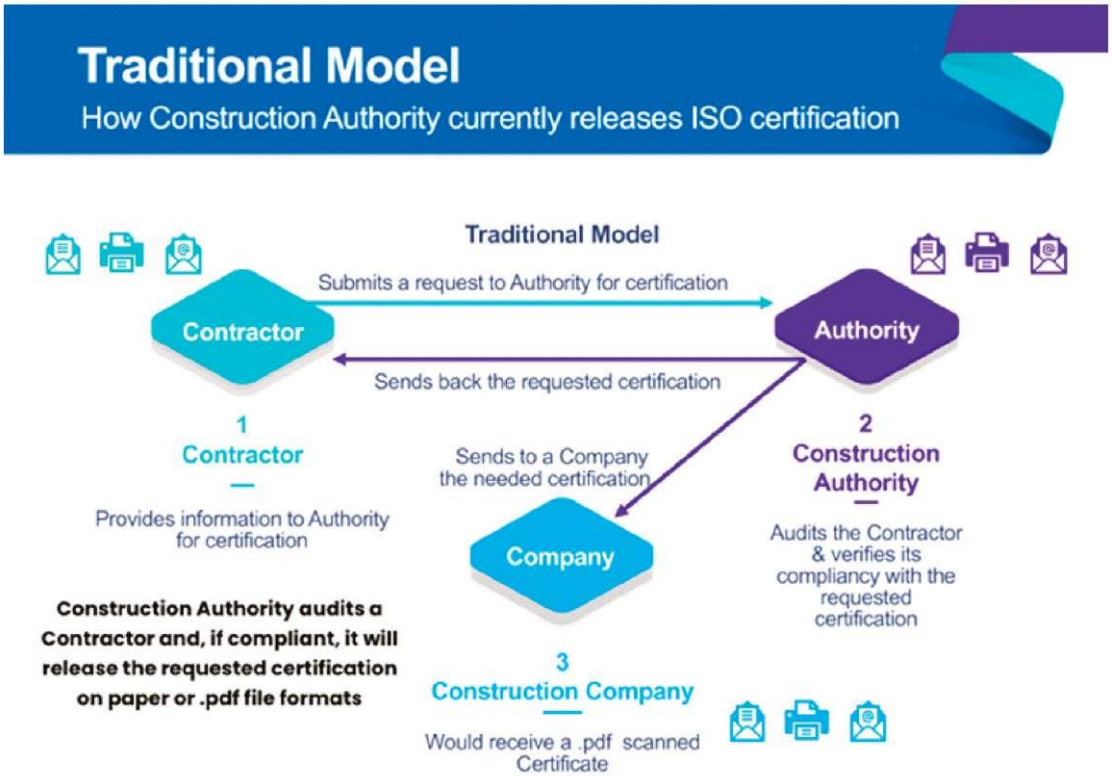


Figura 1- Processo di certificazione tradizionale

B. La soluzione

L'appaltatore ha contattato una software house (un'altra PMI) specializzata in applicazioni blockchain con l'obiettivo di migliorare il processo di certificazione. Per l'appaltatore, la sostenibilità è un fattore importante dal momento che la blockchain è ritenuta una tecnologia energivora.

Pertanto, l'azienda ha scelto una blockchain di Layer 1, progettata con criteri di sostenibilità. La tecnologia da sviluppare si integra sia con la tecnologia esistente dell'appaltatore sia con l'interfaccia dell'ente incaricato della certificazione. Entrambe le integrazioni devono avvenire tramite Application Protocol Interface (API).

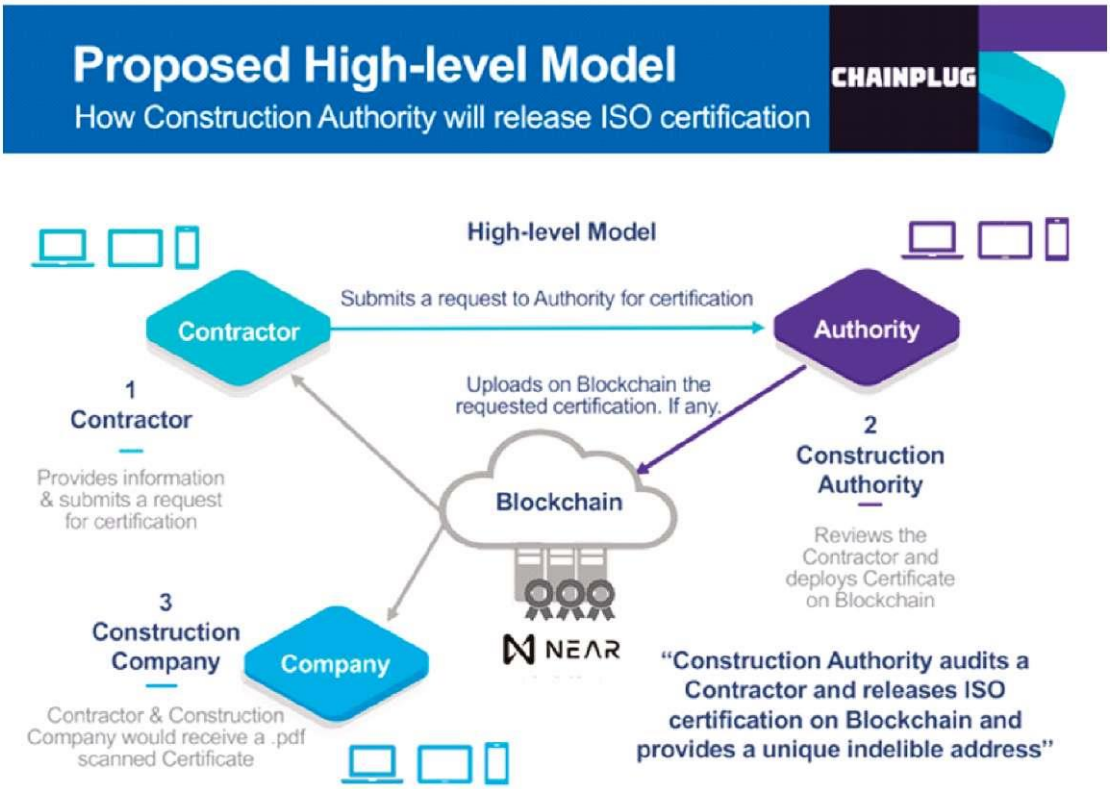


Figura 2- Modello di certificazione di alto livello (per gentile concessione di Chainplug e NEAR Protocol)

L'azienda incaricata di sviluppare la tecnologia ha creato una piattaforma collaborativa blockchain in cui il processo di richiesta-approvazione viene creato per mezzo di un'applicazione decentralizzata (DApp).

Con questa tecnologia, il processo di certificazione viene gestito attraverso un'applicazione che funziona sia su PC che su dispositivi mobili: un significativo miglioramento tecnologico.

Inoltre, il processo di scambio di documenti tra le parti diventa più agile ed efficiente: il flusso di lavoro di autenticazione permette di tenere traccia di chi ha fatto cosa e quando e di recuperare facilmente qualsiasi documento in qualunque momento.

- L'appaltatore invia una richiesta di certificazione all'organismo di certificazione prescelto.
- L'organismo di certificazione riceve la richiesta e la assegna internamente all'account responsabile del task.
- L'account accetta la nuova richiesta di certificazione e inizia a elaborarla.
- Tutti i documenti relativi alle varie politiche e procedure coinvolte nel processo di certificazione vengono scambiati e autenticati tramite DApp.
- Le varie fasi del flusso di lavoro di richiesta-approvazione sono corredate di marca temporale e visibili da entrambe le parti.
- Il processo in corso si conclude con l'approvazione e l'implementazione del certificato nella blockchain, oppure con il rifiuto, anch'esso implementato nella blockchain, o semplicemente con l'annullamento.

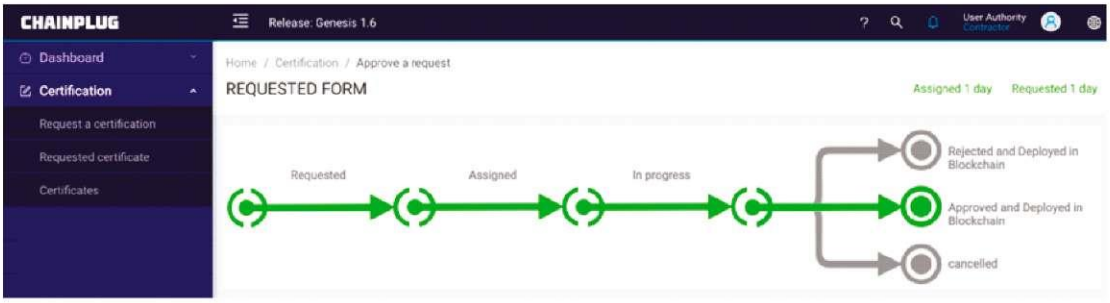


Figura 3 - Flusso di lavoro della richiesta-approvazione della certificazione

Per gentile concessione di Chainplug

L'implementazione di questa tecnologia fornisce il seguente risultato:

- L'appaltatore è in grado di ridurre sensibilmente i tempi, i costi e di semplificare in modo massiccio la gestione delle sue certificazioni, consentendo alla sua PMI di beneficiare dei più alti valori di privacy, trasparenza e automazione forniti dalla tecnologia blockchain: tutto questo, senza ripercussioni sull'ambiente.
- L'organismo di certificazione gode della stessa esperienza, con l'ulteriore vantaggio di poter offrire a tutti i suoi clienti il processo collaborativo, migliorando, velocizzando e riducendo i costi dei processi di certificazione.
- Essendo gestito da smart contract, il processo è anche in grado di definire anticipatamente le azioni correttive in caso di controversie tra le parti, riducendo/limitando così i costi legali.
- In più, le informazioni sulle certificazioni emesse sono state rese disponibili dall'appaltatore agli enti di regolamentazione e controllo, alle autorità e quindi pronte per qualsiasi tipo di audit, attraverso la fornitura di una chiave digitale a chi era interessato ad accedere alle certificazioni pubblicate sulla blockchain.

C. Generalizzazione

Il caso dell'imprenditore edile è ovviamente molto specifico, ma anche rappresentativo di molti casi simili di innovazione digitale basata sulle tecnologie di blockchain.

Che cosa li accomuna?

Molte produzioni e flussi di lavoro industriali prevedono:

- Processi di certificazione come quello qui delineato nel settore delle costruzioni, molto comuni e applicabili a un gran numero di ambienti produttivi e catene di fornitura.
- Certificazioni che non è possibile ottenere per molte aziende, specialmente per le PMI, soprattutto per la mancanza di risorse e conoscenze.
- Audit da parte di clienti, fornitori e autorità.

Queste caratteristiche non sono tipicamente riscontrabili nei processi tradizionali di certificazione, che sono ancora gestiti principalmente tramite carta, posta e file PDF.

In questi casi, l'adozione delle tecnologie di blockchain consente di rendere la raccolta dei dati più efficiente dal punto di vista dei costi, della velocità e della scalabilità. Tra le differenze più evidenti vi sono:

- la capacità di migliorare il grado di privacy, trasparenza, automazione e sostenibilità dei processi di certificazione;

- la democratizzazione del processo di certificazione, dal momento che un maggior numero di aziende, in particolare le PMI, può fornire ai propri lavoratori ambienti di lavoro più sicuri e ai propri clienti prodotti e servizi migliori senza impatto sull'ambiente;
- la capacità della tecnologia di blockchain di integrare sia l'Internet delle cose (IoT) che l'Intelligenza Artificiale, per monitorare costantemente i flussi di lavoro anche prevedendo gli eventi.

L'offerta di una piattaforma collaborativa e sostenibile è alla base dei moderni processi di certificazione basati sulla blockchain per Web3, che aumentano la fiducia in qualsiasi settore e proteggono l'ambiente.

Caso 3: Digitalizzazione dei distretti industriali tessili

Il caso riguarda diverse PMI italiane appartenenti a un distretto tessile che, da secoli, trasformano materie prime in filati. I loro prodotti costituiscono la base per la creazione di tessuti secondo processi obsoleti. Il processo di produzione è piuttosto semplice: diversi attori e fasi concorrono senza soluzioni di continuità alla realizzazione del prodotto finale. La materia prima è costituita da fibre che vengono filate (con una tecnica di torsione) per formare il filato. La fibra viene tirata, ritorta e avvolta su una bobina. I tessuti realizzati con i filati vengono poi trasformati in stoffe e indumenti.

Lo scopo essenziale della filatura è quello di ottenere un prodotto finale il più possibile omogeneo, cioè con caratteristiche uniformi di resistenza, titolo, colore, pulizia ed elasticità. In sostanza, la filatura è un insieme di operazioni che trasformano una fibra grezza in un filato. La filatura richiede fasi di lavorazione dei materiali indispensabili per la loro preparazione, che variano a seconda delle fibre utilizzate. Si parte dalla preparazione e dalla cardatura per arrivare alla filatura che può essere seguita da finissaggi strutturali o estetici come la Binatura[10], il lavaggio e la tintura.

Il distretto tessile presentato in questo caso si compone di numero piuttosto elevato di PMI (più di 7.000 aziende) che, operando in fasi specifiche del processo di produzione del filato, concorrono alla creazione di tessuti e indumenti.

A. Il problema

Alla luce delle tecnologie emergenti del Web3 (blockchain, IoT e Intelligenza Artificiale), le PMI del distretto incontravano difficoltà a passare, come distretto, a un processo innovativo tecnico-produttivo e gestionale congiunto. Le cause erano attribuibili a tre fattori fondamentali. La mancanza di:

- conoscenza delle tecnologie emergenti e di come applicarle al proprio settore;
- fondi da destinare all'innovazione;
- risorse umane in grado di portare a termine questo processo di digitalizzazione.

Pertanto, hanno deciso di unire le forze creando un'Organizzazione Autonoma Decentrata (DAO). Una DAO è una sorta di cooperativa tecnologica, abilitata alla blockchain, senza un organo di governo centrale e i cui membri condividono l'obiettivo di agire nel miglior interesse dell'entità.

In questo caso, l'obiettivo comune era la digitalizzazione collaborativa del Distretto Tessile. I principali benefici attesi dalle PMI appartenenti alla DAO riguardavano la possibilità di agire collettivamente, secondo una governance predefinita, in tutti gli aspetti del lavoro per:

[10] La binatura viene utilizzata per accoppiare più fili (da un minimo di due a un massimo di 12 su un unico rocchetto), come preparazione alla successiva fase di lavorazione: la torcitura. Questo processo viene eseguito sulle binatrici. Tutte le macchine per binatura sono di ultima generazione e dotate di controllo elettronico, per ottenere standard di qualità elevati. La torcitura è la fase cruciale della lavorazione e prevede che le bobine accoppiate vengano caricate sui torcitoi che torcono da 2 a 12 filamenti complessivamente, per ottenere un unico filo composto da più filamenti. I filati così ottenuti possono essere successivamente utilizzati nei più svariati campi di applicazione.

- condividere i problemi;
- trovare le relative soluzioni tecnologiche;
- finanziare il loro sviluppo;
- adottare le tecnologie,

quindi, digitalizzare congiuntamente il proprio distretto agendo come un'unica entità.

Inoltre, con l'aiuto di una ricerca del Ministero dello Sviluppo Economico italiano, in collaborazione con IBM, sono state identificate alcune importanti sfide di questo specifico ecosistema:

1. la difficoltà di digitalizzare, in modo collaborativo, l'apparato tecnico-produttivo distrettuale delle filiere esistenti e future;
2. il controllo della qualità dei prodotti e dei processi interni ed esterni (2a) e l'automazione della gestione di processi complessi (2b);
3. la promozione del benessere del personale (3a) e dell'ambiente (3b), nonché la manutenzione predittiva dei macchinari (3c);
4. l'integrazione e il controllo dell'ambiente di produzione con quello di stoccaggio (4a) e l'esternalizzazione dei flussi di lavoro (4b);
5. la semplificazione dei processi di convalida delle transazioni, sia all'interno che all'esterno del distretto tessile.

Di fronte a queste difficoltà che sembravano insormontabili, decisero che bisognava agire.

B. La soluzione

Le PMI in questione hanno contattato un'azienda (un'altra PMI) specializzata nella tecnologia di blockchain collaborativa e nell'innovazione digitale. L'azienda li ha introdotti al concetto di rete tecnologica aziendale abilitata supportata dalle blockchain e dalle DLT: un consorzio tecnologico blockchain o DAO.

Il primo passo compiuto dall'azienda è stato analizzare il contesto e le problematiche del settore tessile, utilizzando un approccio collaborativo per identificare le esigenze e le priorità. Ne sono derivate soluzioni tecnologiche che soddisfano le singole aziende e il distretto nel suo complesso.

Adottando collettivamente e/o integrando, tramite API, la tecnologia blockchain con quelle esistenti, le PMI hanno ricevuto tutti gli strumenti per gestire su un'unica piattaforma la richiesta-approvazione di certificazioni e transazioni, passando da un approccio da singola azienda a un approccio olistico alla filiera tessile.

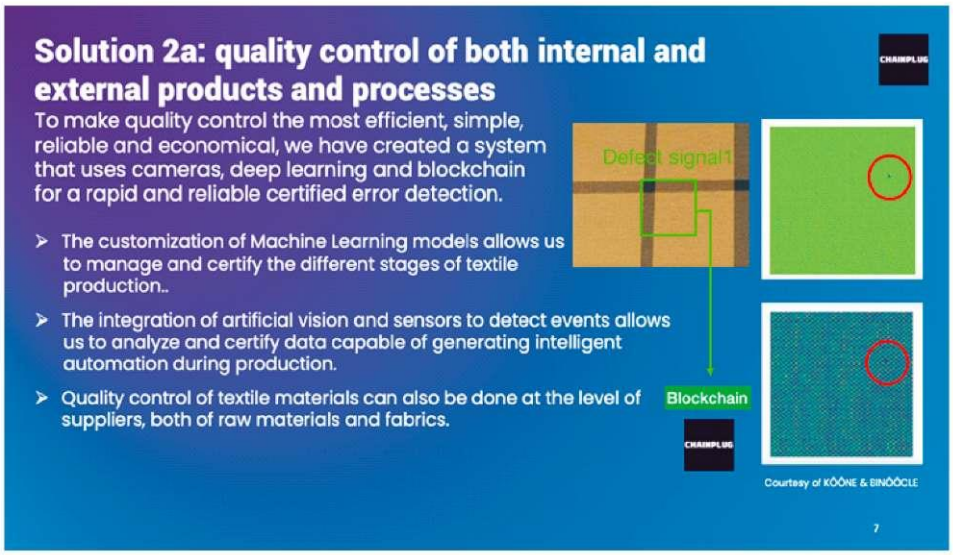
L'azienda è stata in grado di sviluppare e integrare facilmente le applicazioni per la digitalizzazione del distretto tessile sviluppando:

1. una piattaforma blockchain collaborativa peer-to-peer, che integra puntualmente IoT e AI, oltre ad altri software e tecnologie;
2. il controllo della qualità dei prodotti e dei processi sia interni che esterni (Figura: Soluzione 2a), e l'automazione della gestione di processi complessi (Figura: Soluzione 2b);
3. la promozione del benessere del personale (Figura: Soluzione 3a) e dell'ambiente (Figura: Soluzione 3b), nonché la manutenzione predittiva dei macchinari (Figura: Soluzione 3c);

4. l'integrazione e il controllo dell'ambiente di produzione e di stoccaggio (Figura: Soluzione 4a), e l'esternalizzazione dei flussi di lavoro (Figura: Soluzione 4b);
5. la semplificazione dei processi di convalida delle transazioni, sia all'interno che all'esterno del distretto tessile.

Inoltre, la piattaforma collaborativa ibrida blockchain, che integra l'Internet delle Cose (IoT) e l'Intelligenza Artificiale (AI), ha permesso di adottare senza soluzione di continuità queste tecnologie emergenti ponendo le basi per Web3, Metaverso e la creazione di nuovo valore. Si è così riusciti a facilitare l'integrazione e la collaborazione su un'unica piattaforma, fornendo alle PMI uno strumento per diventare competitive sia all'interno del distretto tessile locale che nei confronti delle grandi catene di valore internazionali.

Di seguito[11], le soluzioni da implementare a beneficio del Distretto Tessile DAO.



[11] Per gentile concessione di Chainplug

Solution 2b: automation of the management of complex processes

With the help of IoT and AI sensors, we have integrated into Chainplug a system that uses, in real time, artificial vision, sensors and tags to:

- detect and certify significant events in production processes in blockchain;
- generate intelligent and certified automation on the timeline of the production chain;
- automate the blockchain certification of both production processes and products;
- interface the Industry 4.0 technologies of customers, suppliers and Authrities with those belonging to the companies within the district.

Blockchain

Courtesy of KÖÖNE & BINÖÖCLE

9

Solution 3a: promotion of staff well-being

Thanks to AI models, integrated in Chainplug, it is possible to provide your employees and their families with an anonymous and certified system that:

- involves them in monitoring their psycho-physical well-being through interactions with the platform, also suggesting solutions to these problems with exercises to be done;
- allows the employer to assign their employee to tasks in line with their certified psycho-physical state;
- significantly reduces the risk of accidents at work and the liability of the employer and, possibly, to renegotiate the insurance premium at work;
- allows the creation of a sustainable work environment, also at a social level.

Blockchain

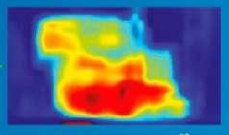
Courtesy of MIRRÖÖR & BINÖÖCLE

11

Solution 3b: promoting the well-being of the environment

We have created, by integrating artificial vision and intelligence, a system that quantifies, specifies and certifies the waste material.

- The dedicated software generates certified data on the quantity and quality of waste.
- It allows, through the integration of sensors and AI, to certify both the r materials and their disposal.
- The experimentation of integrating, within the yarn together with the raw material, of particular RFID antennas to produce traceable fabrics is being studied: from their "birth", to their "reuse", up to the "end of life".



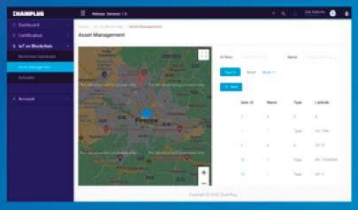
Blockchain

13

Solution 3c: predictive maintenance of machinery

It is based on the integration of IoT, IIoT and IoRT in Chainplug's IoT platform for sensor management and on the Chainplug's "Patent pending" process of certifying the identity of things' identities, called KYD, (Know-Your-Device), as well as on the application of machine learning models. The technology allows to:

- define the identity of the IoT through the blockchain registration of devices in the "Registrar of Things».
- define in a "Smart Contract" and record in blockchain: identity, SLA, documentation, guarantee and so on of the specific IoT.
- monitor and certify IoT activity in blockchain.
- record and certify, in an automated manner and according to predefined alert levels, the correct functioning of: sensors, machines, cobots and robots.
- In future developments, to autonomously send and receive payments, independently by the IoT, IIoT, IoRT used.



15

Solution 4a: integration and control of the production part with the storage one

A consortium for participation in the KYKLOS 4.0 program of the EU is under construction, is under construction. This will be used to study and experiment, through particular RFID fibres/antennas, the integration and control of the production part with the storage one. This application will allow companies to:

- intelligently arrange the RFID antennas along the "patch" and certify their production and storage.
- immediately identify the geo-localization of tissues, using a mobile device camera or augmented reality visor.
- to allow automated loading/unloading of yarns/fabrics, through the integration with the company's CRM/ERP and by means of RFID detectors;
- eradicate counterfeiting and theft of yarns and fabrics, as the digital identifier is "intertwined" with the raw material.

NB: The RFID fiber / antenna under study resists pressures up to 80 Pascal and up to 200 industrial washes.

10

Solution 4b: Outsourcing of workflows

Created through Chainplug's collaborative platform and thanks to the joint action of blockchain, IoT and AI through the API of the platform, to integrate it with quality control processes, both internal and external, supply-chains and technologies of various kind. The technology enables:

- the creation in Chainplug, through dedicated Smart Contracts, of outsourced, predefined and certified workflows.
- total control over the quality of the outsourced work.
- the elimination of legal fees related to product non-conformities and various disputes.
- accurate and certified management of the relationship with subcontractors and the certified maintenance of company's performance control.
- the ability to maintain effective integration of third party production and / or logistics processes.
- the certification and auditing of "third parties" and the work outsourced to them.

11

C. Generalizzazione

Il caso delle PMI del distretto tessile è ovviamente molto specifico, ma anche rappresentativo di molti casi simili di innovazione digitale basata sulla blockchain.

Che cosa li accomuna?

In quasi tutti i distretti produttivi, le PMI faticano a:

- conoscere e comprendere la blockchain e come applicarla alla propria attività;
- reperire i fondi da destinare all'innovazione;
- trovare risorse umane in grado di portare a termine questo processo di digitalizzazione.

Queste caratteristiche, condivise da diverse PMI, non sono un buon punto di partenza per affrontare il necessario processo di digitalizzazione in qualsiasi distretto industriale. Inoltre, le PMI corrono il rischio di voler digitalizzare la propria attività con tecnologie obsolete. Un altro fattore da considerare è il costo dello sviluppo e dell'implementazione di queste tecnologie emergenti, che è superiore a quello delle tecnologie generalmente adottate e disponibili.

In questi casi, la creazione di un consorzio tecnologico (una DAO):

- permette di creare una conoscenza condivisa, a livello di distretto, dei problemi comuni da risolvere attraverso la tecnologia blockchain;
- fornisce un ecosistema collaborativo basato su blockchain in cui la trasparenza, la privacy dei dati, l'automazione dei flussi di lavoro e la governance comune pongono le basi per nuovi modelli di business e per la generazione di valore;
- consente lo sviluppo collettivo delle tecnologie necessarie, permettendo così alle PMI di stabilire il livello di privacy desiderato per i propri dati e di permettersi l'innovazione.

L'adozione della tecnologia collaborativa blockchain comporta notevoli differenze rispetto all'attuale "status quo" tecnologico di qualsiasi distretto produttivo:

- la capacità di coordinare aziende eterogenee, in diverse fasi della produzione, creando flussi di lavoro intertecnologici, contribuendo così a ridurre drasticamente i silos e la frammentazione;

- la capacità di comunicare e di effettuare transazioni oltre i confini della fabbrica e dell'impresa (molto apprezzata per l'integrazione della catena di fornitura);
- la possibilità di eliminare/ridurre i costi delle cause legali definendo tramite gli smart contract i rimedi in caso di violazione ad opera di una delle parti;
- la capacità di validare e certificare automaticamente le transazioni tra le parti, anche di natura economica.

Offrire alle PMI e a tutti i membri di un distretto (e non solo) un unico punto di accesso a una piattaforma e a una tecnologia collaborative gestite in base al valore, pone le basi per flussi di lavoro e operazioni moderni, trasparenti e automatizzati basati su blockchain all'interno del distretto.

Caso 4: Il caso della backdoor di Huawei nelle apparecchiature di rete IoT - L'approccio europeo

La legge sulla spesa per la difesa nazionale degli Stati Uniti, firmata nell'agosto 2018, ha impedito al governo statunitense di acquistare apparecchiature da Huawei e ZTE (un altro produttore cinese di IoT), a causa delle accuse nei confronti del governo cinese sospettato di utilizzare queste aziende per spiare altri Paesi.

Anche diversi altri Paesi, tra cui Canada, India e Regno Unito, hanno espresso preoccupazioni simili in materia di sicurezza e spionaggio. Tuttavia, l'azienda ha ripetutamente negato qualsiasi coinvolgimento con fazioni politiche controverse o l'accusa che il governo cinese le imponesse di includere backdoor nelle apparecchiature di rete che vende.

A. Il problema

L'Internet delle cose (IoT) è una rete di oggetti fisici, "cose", dotati di sensori, software e altre tecnologie. I dispositivi IoT utilizzano sensori, software e altre tecnologie connesse a Internet per connettersi e scambiare dati con altri dispositivi e sistemi tramite Internet. Questi dispositivi vanno dai comuni apparecchi domestici (telecamere di sicurezza, dispositivi wi-fi, ecc.) a sofisticati strumenti industriali.

La contraffazione degli IoT è un grosso problema per il settore. Un'altra preoccupazione principale è che i dati inviati/ricevuti dagli IoT possano essere manipolati e inoltrati a terze parti indesiderate, mettendo fortemente a rischio la privacy, come nel caso delle antenne 5G di Huawei.

I produttori di dispositivi IoT e i loro clienti si trovano spesso ad affrontare una serie di problemi, tra cui:

- contraffazione dei dispositivi;
- perdita di privacy e sicurezza, a causa dei furti di dati;
- potenziali danni alla proprietà e all'azienda.

In un contesto che vede la graduale integrazione di "cose" come i cobot[12] e i robot nei flussi di lavoro delle industrie e delle organizzazioni, il problema sta assumendo una portata sempre più rilevante e sta raggiungendo un livello di pericolo per lo Stato in termini di sicurezza.

Pertanto, gli Stati Uniti e altri Paesi hanno deciso di prendere provvedimenti.

[12] Robot collaborativi

B. La soluzione

La soluzione adottata dagli Stati Uniti e da altri Stati è stata la messa al bando totale dei prodotti delle due aziende cinesi citate. La Commissione europea ha pubblicato una toolbox che dà il via libera ma limita il ricorso a vendor ad alto rischio: la toolbox impegna gli Stati membri a procedere congiuntamente, sulla base di una valutazione oggettiva dei rischi identificati e di misure di mitigazione proporzionate.

Un'importante misura di mitigazione potrebbe derivare dalla creazione di un rapporto di fiducia tra produttori e utenti dell'IoT. In questo modo si potrebbe eliminare il problema della contraffazione degli IoT e generare fiducia definendo l'identità auto-sovrana (SSI) di una "cosa" attraverso la certificazione fornita dalla tecnologia blockchain o adottando il passaporto digitale dei prodotti dell'UE.

Una volta applicate, le due soluzioni sopra descritte potrebbero:

- valutare in modo univoco l'identità di ciascun dispositivo IoT;
- vietare il contrabbando e la contraffazione dei dati;
- evitare danni alla proprietà, perdite di proprietà intellettuale e spese legali.

C. Generalizzazione

Ad esempio, stiamo assistendo all’adozione su larga scala di dispositivi sanitari e medici IoT indossabili, utili per vari motivi, tra cui:

- fare una diagnosi accurata;
- definire piani di cura;
- migliorare la sicurezza dei pazienti;
- semplificare l'assistenza domiciliare;
- monitorare costantemente i pazienti con malattie critiche, ecc.

Pertanto, fornire un'identità univoca alle cose potrebbe proteggere la nostra sicurezza come comunità sociale e comunità imprenditoriale, ma anche il nostro benessere e la nostra salute personale.

4. PRIORITÀ POLITICHE PER LA

4.1 La politica europea sulla blockchain

4.1.1 Commissione europea - eIDAS e smart contract

La Commissione europea ha adottato una proposta legislativa per lo European Data Act, che specifica i requisiti essenziali degli smart contract per la condivisione dei dati e richiede lo sviluppo di uno standard armonizzato[13] per facilitare l'introduzione degli smart contract a supporto dello scambio transfrontaliero di dati e la loro remunerazione.

Gli smart contract sono un concetto ben noto implementato nella blockchain e nella Distributed Ledger Technology (DLT). Nel 2017, l'ISO ha istituito un nuovo comitato tecnico (ISO/TC 307) per sviluppare standard sulle tecnologie blockchain e distributed ledger, come la norma ISO 22739[14], un vocabolario standard ora in fase di adozione come standard europeo, che include le definizioni tecniche di tutti i principali concetti in ambito blockchain e DLT, compresi gli smart contract.

La definizione tecnica di smart contract contenuta nella norma ISO 22739, accettata in generale da tutti gli organismi di standardizzazione, è la seguente:

> *Un programma per computer memorizzato in un sistema DLT*
> *in cui il risultato di qualsiasi esecuzione del programma è registrato sul registro distribuito.*

Il concetto di smart contract contenuto nella proposta di Data Act è una definizione legale e neutra dal punto di vista tecnologico:

> *Un programma per computer memorizzato in un sistema elettronico di registro distribuito*
> *in cui il risultato di qualsiasi esecuzione del programma è registrato sul registro distribuito.*

La norma ISO 22739 riconosce inoltre che "uno smart contract può rappresentare i termini di un contratto di diritto e creare un obbligo legalmente applicabile ai sensi della legislazione di una giurisdizione applicabile". Pertanto, l'uso degli smart contract nel contesto della proposta di Data Act è in linea con il possibile uso degli stessi già ben riconosciuto e identificato dall'ISO.

L'uso del termine "Electronic Ledger" invece di "Distributed Ledger Technology" nella proposta di legge sui dati è un collegamento diretto con eIDAS2[15], la revisione del regolamento eIDAS, che definisce un registro elettronico come:

> *Un registro elettronico di dati a prova di manomissione, che garantisce l'autenticità e l'integrità*
> *dei dati contenuti, l'accuratezza della loro data e ora e il loro ordine cronologico.*

4.1.2 Come si definisce la politica globale per la blockchain?

Blockchain e DLT sono tecnologie abilitanti fondamentali che stanno registrando una crescita significativa, soprattutto nell'UE. Secondo Statista.com, gli utili attesi dal mercato della blockchain nell'UE si attestano a circa 2 miliardi di Euro entro il 2023, mentre Business Market Insights prevede una crescita del mercato europeo della blockchain fino a circa 59 miliardi di Euro entro il 2028. La pandemia di COVID-19 ha accelerato l'adozione delle soluzioni blockchain, grazie alla maggiore fiducia offerta per le transazioni online.

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0068
[14] ISO 22739:2020 "Blockchain and distributed ledger technologies — Vocabulary", vedere https://www.iso.org/standard/73771 https://www.iso.org/standard/73771.
html. Lo standard è di fatto disponibile gratuitamente in anteprima al seguente link.
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281

Le banche europee stanno investendo di più nelle blockchain, mentre le compagnie di assicurazione sono in prima linea nell'adozione della tecnologia blockchain. Inoltre, le aziende europee, comprese le PMI, stanno mostrando progressi promettenti nell'introduzione di soluzioni blockchain sostenibili e verdi, utilizzando al contempo gli standard per migliorare la tracciabilità e la trasparenza. Ne è un esempio l'utilizzo degli standard UNECE per la tracciabilità delle materie prime nel settore tessile. La pandemia di COVID-19 ha evidenziato le sfide e le opportunità della trasformazione digitale, accelerando la necessità di digitalizzazione in tutti i settori come motore fondamentale per la ripresa. La trasformazione digitale per le imprese e le autorità pubbliche, insieme alla transizione green sostenibile - la Twin Transition - sono diventati i due pilastri dell'UE per la leadership globale.

L'UE ha riconosciuto tempestivamente il ruolo abilitante della blockchain come tecnologia di base, sia per la trasformazione digitale che per la transizione verde e ha sviluppato politiche che lo rispecchiassero. Infatti, la blockchain ha il potenziale di migliorare i processi in tutti i settori dell'economia e della pubblica amministrazione, costruendo fiducia e aiutando a tracciare i dati, che rimangono autentici e immutabili. Per quanto riguarda la trasformazione digitale, la Strategia sui dati della CE e la Strategia per la finanza digitale riconoscono il potenziale della blockchain come tecnologia digitale decentralizzata, che può consentire alle aziende e ai singoli di controllare meglio i flussi e l'utilizzo dei dati e creare uno spazio di dati finanziari per promuovere l'innovazione basata sui dati.

Per quanto riguarda la transizione verde, il Green Deal dell'UE e le proposte successive, come la revisione del pacchetto energia, l'Ecodesign e l'Iniziativa per i prodotti sostenibili - compreso il Passaporto digitale dei prodotti - sottolineano l'importanza delle tecnologie abilitanti e convergenti, come la blockchain, l'Internet delle cose e l'intelligenza artificiale, per guidare la transizione verde tra tutti gli attori economici e sociali. Ad esempio, l'uso della blockchain può consentire di tracciare e rendicontare le riduzioni delle emissioni di gas serra lungo l'intera catena di fornitura, compresi produttori, fornitori, distributori e consumatori.

Per raggiungere questi obiettivi, la CE ha lanciato il Partenariato europeo blockchain (EBP) e l'Infrastruttura europea dei servizi blockchain (EBSI), che consentiranno l’implementazione cross-settoriale della blockchain attraverso un unico mercato digitale per la blockchain. Tuttavia, l'evoluzione dell'infrastruttura EBSI può essere affrontata adeguatamente solo sviluppando l'interoperabilità con altre reti che saranno fornite dall'industria.

Le ambizioni dell'UE di diventare leader mondiale nella tecnologia blockchain si riflettono ulteriormente nella sua strategia per la blockchain, che mira a (1) costruire una blockchain paneuropea per i servizi pubblici; (2) sostenere la certezza del diritto; (3) colmare il divario degli investimenti finanziando la ricerca e l'innovazione; (4) promuovere la blockchain per la sostenibilità; (5) sostenere l'interoperabilità e gli standard; (6) sostenere lo sviluppo delle competenze in materia di blockchain. Nel suo sostegno alla strategia blockchain, la CE intende sostenere un "gold standard" per la blockchain che abbracci i valori europei e includa (1) la stabilità ambientale, (2) la protezione dei dati, (3) l'identità digitale, (4) la sicurezza informatica e (5) l'interoperabilità.

L'attuale attenzione per la blockchain come tecnologia in grado di aiutare l'Unione europea a perseguire la leadership nella transizione verde e a rafforzare la Sovranità Digitale dell'Europa può essere ricondotta alle seguenti proposte legislative:

- Regolamento generale sulla protezione dei dati, GDPR
- Data Act (proposta legislativa)
- Regolamento in materia di identificazione elettronica e servizi fiduciari (EUDI - eIDAS2) (proposta legislativa)

1. Regolamento sui mercati dei cripto-asset - MiCA (proposta legislativa)

Le proposte legislative di cui sopra (oltre al GDPR) dimostrano come la CE stia consolidando i propri sforzi verso la creazione di un mercato digitale unico per la blockchain. Ad esempio, il Data Act, una delle principali proposte legislative per il decennio digitale europeo, pone l'accento sugli smart contract, che si basano su blockchain e DLT.

La richiesta di smart contract per i data center nel Piano di lavoro annuale 2022 per la standardizzazione europea riflette il rapporto tra le politiche della CE e la standardizzazione. L'attenzione all'identità digitale europea (EUDI) attraverso la revisione dell'eIDAS e delle norme del GDPR aiuterà i produttori, i rivenditori, i banchieri, i consumatori/cittadini e altri attori delle catene di fornitura a fidarsi degli asset digitali europei. In cambio, la trasformazione digitale e la sovranità digitale dell'Europa verranno rafforzate.

Un altro aspetto importante della strategia per la blockchain riguarda le emissioni di CO_2. Uno degli obiettivi del MiCA è quello di sostenere le attività di crypto mining che contribuiscono alla mitigazione e all'adattamento ai cambiamenti climatici. Le proposte del MiCA per il panorama dei fornitori di servizi crittografici e degli asset crittografici in Europa e oltre, inoltre, cambieranno le carte in tavola per preservare la sovranità digitale dell'Europa.

4.1.3 Impatto del GDPR sulla blockchain

L'obiettivo principale è la creazione di un sistema coerente e armonizzato a livello europeo per la protezione dei dati personali, con un nuovo quadro europeo per la protezione dei dati. Pertanto, la Commissione europea ha approvato il Regolamento generale sulla protezione dei dati (GDPR), Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. Il Regolamento (UE) 2016/679 contiene alcuni nuovi principi di adattamento, integrazione e margini di flessibilità. Con riferimento a questo documento, sottolineiamo il principio di Responsabilità che rappresenta un'aggiunta importante perché introduce il passaggio dalla forma alla sostanza. Infatti, il responsabile del trattamento dei dati deve osservare i principi applicabili al trattamento dei dati personali che attestano il suo status.

Le caratteristiche della DLT come tecnologia decentrata, immodificabile e persistente devono essere valutate e coordinate con le disposizioni del Regolamento UE n. 679/2016 - GDPR, per disciplinare le ipotesi di trattamento centralizzato dei dati stessi, in quanto questo impone al titolare del trattamento una serie di obblighi che devono essere individuati di volta in volta. Di conseguenza, qualsiasi trattamento di dati personali effettuato tramite DLT o blockchain deve rispettare i principi fondamentali stabiliti dal GDPR: il principio di liceità del trattamento, il principio della privacy by design e il principio della privacy by default, che deve anch'esso basarsi sui presupposti di liceità del trattamento.

Questo perché un sistema basato su DLT o blockchain, che utilizza dati personali, rientra nell'ambito di applicazione della legislazione sulla protezione dei dati e deve quindi soddisfare diversi requisiti legali.

Altri aspetti critici ma molto importanti sono l'**immodificabilità** delle informazioni inserite nella blockchain se sono stati acquisiti anche dati personali rilevanti per la privacy e il collegamento con il diritto all'oblio, che prevede la possibilità di richiedere la cancellazione dei dati (art. 17 GDPR). Non si tratta di un diritto assoluto, in quanto mitigato dalla presenza di un interesse pubblico o dal verificarsi dei casi dettati dal comma 3 dell'art. 17 GDPR; garanzia del diritto di rettifica, ai sensi dell'art. 16 GDPR, di eventuali dati personali inesatti: da realizzarsi attraverso la richiesta di rettifica dei dati proveniente da tutti i partecipanti alla blockchain e successiva sottoscrizione dei dati così modificati.

Il **rispetto** del diritto alla portabilità dei dati (articolo 20 del GDPR) attraverso la fornitura al richiedente dei dati personali in un formato elettronico interoperabile con sistemi diversi dalla DLT o dalla blockchain originale. In ogni caso, la conoscenza dei principi di protezione dei dati è la logica che sta alla base della *"messa in atto di misure tecniche e organizzative adeguate",* tenendo presente che l'articolo 25 GDPR prevede i principi della Privacy by Design e by Default, ossia *"protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"*.

Si tratta di un obbligo generale secondo il quale: *"tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, e considerando i rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche rappresentati dal trattamento, sia al momento di determinare i mezzi del trattamento che al momento del trattamento stesso", il responsabile del trattamento "attua misure tecniche e organizzative idonee, come la pseudonimizzazione, per applicare efficacemente i principi di protezione dei dati, come la minimizzazione, e per integrare nel trattamento le garanzie necessarie a soddisfare i requisiti del presente regolamento e a proteggere i diritti degli interessati".*

In conformità ai principi della **Privacy by Design e by Default,** il titolare del trattamento deve mettere in atto *"misure tecniche e organizzative adeguate per garantire che per impostazione predefinita siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento"*. *In questo senso, "tale obbligo si applica alla quantità di dati personali raccolti, alla portata del trattamento, al periodo di conservazione e all'accessibilità". Ciò significa che queste "misure devono garantire che, per impostazione predefinita, i dati personali non siano resi accessibili a un numero indefinito di persone fisiche senza l'intervento della persona fisica".*

Quando un sistema DLT o blockchain contiene dati personali non può quindi prescindere dai principi di privacy by design fin dall'inizio, e i principi che devono essere considerati sono:

- limitazione delle finalità: i dati raccolti e trattati devono soddisfare una finalità predefinita e quindi avere uno scopo specifico, esplicito e legittimo, per poter essere ulteriormente trattati in modo non incompatibile con tale finalità. Il riutilizzo dei dati personali per uno scopo non previsto inizialmente è contrario al principio di limitazione della finalità;
- accuratezza: il principio richiede ai responsabili del trattamento di garantire che i dati personali siano "accurati e, se necessario, aggiornati". In caso contrario, devono essere "cancellati o corretti" senza indugio. Se l'unico scopo dell'applicazione è quello di documentare il verificarsi di un fatto in un certo momento, attraverso una marca temporale, non sembra esserci alcuna criticità rispetto al principio di accuratezza;
- minimizzazione dei dati e limitazione della conservazione: la minimizzazione consiste nella raccolta e nel trattamento di una quantità limitata di dati; tali dati devono essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per cui sono trattati. I dati possono essere minimizzati alla fonte o ridotti allo stretto necessario se importati da una fonte esistente. La mancata minimizzazione dei dati aumenta il rischio per i diritti e le libertà dell'interessato. Si raccomanda pertanto di progettare un sistema basato sulla DLT in modo tale che il requisito della minimizzazione dei dati sia considerato nella fase iniziale di progettazione, in conformità con il principio della privacy by design;
- riservatezza e integrità: i dati personali devono "essere trattati in modo da garantire un'adeguata sicurezza e riservatezza, anche al fine di impedire l'accesso o l'uso non autorizzato dei dati personali e delle attrezzature utilizzate per il trattamento" (Considerando 39 del GDPR). Per garantire questo principio occorre conoscere quali dati non devono essere divulgati a terzi e applicare misure tecniche e organizzative adeguate per prevenire la divulgazione dei dati. Nei sistemi basati su DLT, potenzialmente tutti o molti nodi potrebbero venire a conoscenza di dati personali. Pertanto, è necessario trovare un equilibrio tra la visibilità di alcuni dati per mantenere il sistema funzionale e distribuito e l'applicazione di misure tecniche per salvaguardare i dati personali da accessi non autorizzati;
- trasparenza: si tratta di un principio fondamentale della protezione dei dati, in quanto questi devono essere trattati in modo equo e trasparente. Gli interessati devono essere pienamente informati sugli aspetti rilevanti del trattamento dei loro dati, compresi lo scopo e l'ambito dei dati trattati sulla rete DLT.

Ulteriori requisiti previsti dal Regolamento GDPR che dovrebbero caratterizzare qualsiasi trattamento di dati personali sono: il diritto all'oblio (art. 17), l'immutabilità delle registrazioni (art. 17, paragrafo 3), il diritto di rettifica (art. 16), il diritto alla portabilità dei dati (art. 20), le informazioni da fornire agli interessati (artt. 13 e 14), il processo decisionale automatizzato (art. 22), la minimizzazione dei dati (art. 5, paragrafo 1, lettera c)), il diritto di accesso degli interessati (art. 15).

4.2 La politica cinese sulla blockchain e il suo impatto sulle PMI europee

Per quanto riguarda le iniziative globali, la Cina ha compreso molto chiaramente i vantaggi della tecnologia blockchain e si è preparata per la sua adozione a livello nazionale e internazionale. Ciò è stato espresso ai massimi livelli del governo cinese quando il presidente Xi Jinping ha sottolineato che "la tecnologia blockchain svolgerà un ruolo importante nel nuovo ciclo di innovazione tecnologica e trasformazione industriale" e che la blockchain "dovrebbe essere considerata come un'importante svolta nell'innovazione indipendente delle tecnologie di base"[16].

Per raggiungere questo obiettivo, l'iniziativa cinese ha istituito la rete di servizi basata su blockchain (BSN). Come si legge sulla sua homepage, BSN è una rete pubblica di infrastruttura globale cross-cloud, cross-portal e cross-framework utilizzata per distribuire e gestire tutti i tipi di applicazioni distribuite su blockchain (DApp). Per sostenere e facilitare l'adozione delle tecnologie blockchain, la società controllata dallo Stato ha creato due dipartimenti separati: nazionale e internazionale. L'attuale problema degli alti costi di sviluppo e distribuzione delle applicazioni blockchain viene gestito fornendo ambienti di risorse blockchain agli sviluppatori con costi di sviluppo, distribuzione, manutenzione e interoperabilità delle applicazioni blockchain estremamente ridotti e accelerando lo sviluppo e l'adattamento universale della tecnologia blockchain.

BSN offrirà tre servizi principali:

- servizi permissioned;
- servizi permissionless;
- servizi interchain.

I servizi permissioned sono già in esecuzione sul portale BSN Cina (non raggiungibile dall'esterno della Cina). A causa delle normative cinesi, i servizi permissionless saranno disponibili solo sul portale internazionale BSN e sui nodi urbani pubblici internazionali (PCN). Inoltre, il portale internazionale BSN consentirà agli utenti di tutto il mondo di accedere a soluzioni blockchain a basso costo.

Nel marzo del 2021, la tecnologia blockchain è stata menzionata per la prima volta in una bozza del 14° piano politico quinquennale della Cina. La versione finale è stata approvata dai legislatori e dai consiglieri cinesi al termine dell'incontro politico annuale.

Il documento ha delineato gli obiettivi della Cina per i prossimi cinque anni, sottolineando che la tecnologia svolgerà un ruolo sempre più importante nella pianificazione top-down del Paese. Secondo la bozza, l'uso di intelligenza artificiale, dei big data, del cloud computing e della blockchain dovrebbe fornire un contributo al PIL del Paese e "trasformare la Cina in un leader globale".

Con la sua forte autorità centrale, che pervade sia le attività personali che quelle commerciali, il governo cinese ha creato, insegna e vuole utilizzare la blockchain in modo diverso rispetto alla decentralizzazione. Come descritto dalla Zhejiang University, il governo cinese sta creando una blockchain con caratteristiche cinesi, in cui solo le blockchain permissioned sono ammesse in Cina. Ciò comporta una situazione in cui, qualora il governo cinese non possieda il diritto di modificare i dati, potrà cancellare l'intera catena contenente tali dati.

Pertanto, la "decentralizzazione tecnologica sotto la centralizzazione" potrebbe essere un rischio per le aziende non cinesi che vogliono accettare l'invitante offerta della blockchain di BSN Global.

Adottando le tecnologie di BSN Global Alliance le PMI dell'UE potrebbero andare incontro ai seguenti rischi:

[16] https://www.coindesk.com/markets/2019/10/25/president-xi-says-china-should-seize-opportunity-to-adopt-blockchain/

- Mancanza di trasparenza (chi ha accesso ai dati?)
- Perdita di dati, proprietà intellettuale, segreti aziendali e privacy
- Censura
- Perdita di sovranità.

Oltre a costruire la sua catena di approvvigionamento infrastrutturale, attraverso BSN Global la Cina ha quindi posto le basi per la sua infrastruttura tecnologica supportando la *"Nuova Via della Seta" mediante la "blockchain cinese"*.

Nonostante l'attrattiva dell'approccio cinese (basso costo e rapida adozione), è opportuno che le PMI europee (e non solo) evitino di sviluppare le proprie tecnologie tramite blockchain e DLT dove le autorità centrali hanno accesso o, peggio, il controllo delle tecnologie, per non incorrere nei rischi sopra citati.

5. STANDARD PER LA BLOCKCHAIN

5.1 Panorama della standardizzazione della blockchain in Europa - collegamento con le priorità politiche

Il piano continuativo per la standardizzazione delle TIC della Commissione europea, pubblicato annualmente, fornisce le priorità politiche per la standardizzazione della blockchain. Sebbene il Fintech sia l'argomento più importante, gli smart contract e l'identità elettronica stanno guadagnando terreno in virtù della loro importanza per il Data Act e il regolamento eIDAS. Il piano continuativo spiega che blockchain e DLT hanno il potenziale per diventare l'infrastruttura per servizi affidabili, decentralizzati e disintermediati. Inoltre, la blockchain è considerata una tecnologia per il mercato unico. Questo perché gli standard della blockchain possono ridefinire il modo in cui vengono effettuate le transazioni, riducendo così le frodi, rafforzando la conformità, la tracciabilità e il commercio all'interno delle catene di fornitura. Le applicazioni di blockchain e DLT si estendono ai seguenti settori:

- eHealth
- Istruzione
- eGovernment e registri pubblici
- Certificazione di sicurezza dell'Internet delle cose
- Intelligenza artificiale affidabile
- Sicurezza alimentare
- Gestione dei diritti di proprietà intellettuale
- gestione eID

5.2 Esigenze di standardizzazione

L'interoperabilità e l'armonizzazione rimangono i maggiori ostacoli alle transazioni tra Paesi e tra settori. Gli standard consentirebbero un'applicazione più agevole alle transazioni tra Paesi, come nell'esempio banche/assicurazioni di cui al paragrafo 3.1.2. L'interoperabilità è importante per eliminare o ridurre il vendor lock-in, decisivo per le PMI che vogliono fornire servizi basati su blockchain in qualsiasi settore (vedere sezione 3, sopra). Il Piano continuativo sulla standardizzazione delle TIC 2022 elenca le seguenti lacune:

- Governance e interoperabilità, quadri organizzativi e metodologie, schemi di valutazione dei processi e dei prodotti, linee guida per blockchain e registri distribuiti, tecnologie intelligenti, oggetti, dispositivi di calcolo distribuiti e servizi di dati.
- Identificazione dei casi d'uso rilevanti per l'UE (compresi i requisiti normativi dell'UE come GDPR, ePrivacy, eIDAS, TOOP, ecc.)
- Identificazione delle reali implementazioni di blockchain/DLT nell'UE e valutazione della necessità di standardizzazione, armonizzazione e formazione o adattamento della forza lavoro.
- Standardizzazione del funzionamento e implementazione di riferimento di registri e applicazioni distribuiti, con l'obiettivo di creare un ecosistema aperto di soluzioni industriali interoperabili
- Dovrebbe essere sviluppato un quadro generale per la governance delle reti europee basate sulla DLT per consentire il flusso di smart contract tra le diverse reti.
- Le ESO devono sviluppare gli standard necessari per l'introduzione di una moneta digitale programmabile (CBDC) e della token economy (imminente regolamento MiCA), in particolare per garantire l'interoperabilità con gli smart contract, i sistemi legacy, ecc.
- Le SDO devono sviluppare standard a supporto dei requisiti della proposta eIDAS2 relativi alla DLT.

5.3 Le diverse organizzazioni di standardizzazione coinvolte nella blockchain

Le seguenti organizzazioni sono impegnate nella standardizzazione della blockchain per colmare le lacune di cui sopra:

Organizzazione Internazionale per la Standardizzazione (ISO)	L'ISO TC 307 lavora sugli standard internazionali per la blockchain, concentrandosi sul miglioramento della sicurezza, della privacy, della scalabilità e dell'interoperabilità.
Istituto degli ingegneri elettrici ed elettronici (IEEE)	L' iniziativa IEEE blockchain comprende gruppi di lavoro orizzontali e verticali che si occupano di Dati, Interoperabilità, Governance, Identità e Smart Contract (orizzontale), Energia, IoT, Sanità, FinTech, criptovalute e asset digitali (verticale).
Unione Internazionale delle Telecomunicazioni (ITU)	Il Focus Group ITU-T sulla DLT lavora sui requisiti, sui criteri di valutazione e sul quadro di riferimento. Copre i settori della finanza, dell'energia, dei media digitali, della sanità elettronica, dei servizi pubblici e altre applicazioni verticali.
Consorzio del World Wide Web (W3C)	Il W3C ha recentemente istituito un Blockchain Community Group che si occupa di casi d'uso, applicazioni decentralizzate e asset digitali.
CEN / CENELEC	Il CEN-CLC/JTC 19 si concentra sulle esigenze specifiche di standardizzazione per supportare i requisiti legislativi e politici europei a sostegno dello sviluppo del mercato unico digitale dell'UE. Dà la priorità alla definizione di norme internazionali e sviluppa norme per specifiche esigenze e/o priorità di standardizzazione europee.
ETSI	L'Industry Specification Group (ISG) PDL dell'ETSI lavora su diversi argomenti relativi alla blockchain e mira a colmare una lacuna nel panorama di DLT, blockchain, criptovalute e altro ancora per evitare di rifare o duplicare gli standard esistenti.
OASIS	Il lavoro di OASIS si basa su progetti aperti. Il progetto OriginBX è un'alleanza globale di organizzazioni che lavorano su attestazioni fiscali e attributi commerciali digitali per la trasmissione transfrontaliera di dati utilizzando piattaforme legacy e blockchain. I progetti comunitari dell'EEA costruiscono standard e documentazione di alta qualità per il protocollo Ethereum.

Oltre al lavoro di standardizzazione di cui sopra, esiste una serie di organizzazioni e iniziative europee e globali sulla tecnologia blockchain e sulla standardizzazione, tra cui:

A EBSI - Infrastruttura europea di servizi blockchain

L'Infrastruttura europea di servizi blockchain (EBSI) è stata istituita nel 2018 quando gli Stati membri dell'UE, la Norvegia, il Liechtenstein e la Commissione europea hanno unito le forze per creare la European Blockchain Partnership (EBP).

Pur supportando inizialmente i servizi pubblici, si prevede che l'EBSI venga estesa alla cooperazione con il settore privato o con applicazioni private. Questa ambiziosa iniziativa della Commissione mira a rafforzare la leadership e l'autonomia dell'UE nel settore della blockchain, rispettando al contempo i suoi valori fondamentali: conformità al GDPR, sicurezza, interoperabilità e sostenibilità.

I casi d'uso iniziali dell'EBSI sono:

- Tracciabilità: sfruttare la potenza della blockchain per creare audit trail digitali affidabili, automatizzare i controlli di conformità nei processi sensibili ai tempi e dimostrare l'integrità dei dati;
- Diplomi: scambio facilitato e affidabile di diplomi accreditati in tutta Europa, "con una riduzione significativa dei costi di verifica e un miglioramento della fiducia nell'autenticità";
- Identità auto-sovrana: implementazione di un'identità digitale europea, "che consenta agli utenti di creare e controllare la propria identità a livello transfrontaliero senza dipendere da autorità centralizzate e che permetta la conformità con il quadro normativo eIDAS";
- Condivisione affidabile dei dati: attraverso la tecnologia blockchain i dati possono essere condivisi in modo sicuro e affidabile tra le autorità dell'UE, ad esempio tra le autorità doganali e fiscali.

Altri casi d'uso saranno aggiunti all'EBSI nei prossimi mesi. L'EPB sta lavorando sui tre casi d'uso seguenti:

- finanziamento delle PMI tramite blockchain attraverso l'emissione e la negoziazione di obbligazioni per PMI in tutta Europa;
- creazione di un pass europeo per la sicurezza sociale che consenta di accedere facilmente ai servizi di welfare in tutta Europa;
- migliore gestione dei processi di richiesta di asilo in tutta Europa.

Secondo le interviste con il personale della Commissione europea, ci sarà un flusso costante di nuovi casi d'uso che verranno auspicabilmente aggiunti all'EBSI, a seconda della domanda e del successo dei casi d'uso attuali. Inoltre, circa 50 milioni di Euro saranno messi a disposizione tramite l'EBSI per le sandbox che aiuteranno le start-up a distribuire le applicazioni che vogliono vendere in tutta Europa, consentendo loro di testare le applicazioni insieme alle autorità di regolamentazione in diverse aree per chiarire la situazione normativa e adattare le proprie soluzioni per renderle compatibili con la normativa esistente.

B Associazione internazionale per le applicazioni blockchain affidabili (INATBA)

L'Associazione internazionale per le applicazioni blockchain affidabili (INATBA) è stata fondata nel 2019 e conta attualmente circa 170 membri. INATBA offre agli sviluppatori e agli utenti delle tecnologie blockchain e distributed ledger (DLT) un forum globale. INATBA consolida il suo portafoglio internazionale come rappresentante dei principali stakeholder della blockchain per fornire analisi e necessità politiche più approfondite. Sfruttando i propri gruppi di lavoro per creare una discussione più ampia ed espandere la propria rete, INATBA è uno dei punti focali per collegare gli esperti europei con le iniziative internazionali di standardizzazione della blockchain. Il Comitato per gli standard dell'INATBA si occupa di incanalare i requisiti di standardizzazione dell'EBSI e di tenere l'INATBA al corrente degli sviluppi politici e di standardizzazione.

C. Iniziativa globale blockchain dell'ITU

Il Focus Group dell'ITU-T sull'applicazione della Distributed Ledger Technology (FG DLT) ha analizzato le applicazioni e i servizi basati sulla DLT che possono essere standardizzati dai Focus Group dell'ITU-T, identificando le migliori pratiche e le linee guida che possono supportare l'implementazione di tali applicazioni e servizi su scala globale. Inoltre, ha identificato il percorso che i gruppi di standardizzazione dell'ITU-T devono seguire per soddisfare le pressanti esigenze del mercato. Il gruppo ha sviluppato documenti di standardizzazione della sicurezza per i servizi interoperabili basati sulla DLT tenendo conto delle attività intraprese dai vari gruppi, organizzazioni per lo sviluppo di standard (SDO) e forum pertinenti, redigendo un kit di strumenti per gli standard che può essere utilizzato dai responsabili politici nazionali e dalle autorità di regolamentazione degli Stati membri dell'UIT.

Per supportare lo sviluppo di una documentazione di base per gli standard globali per le applicazioni e i servizi basati sulla DLT, gli obiettivi del focus group erano i seguenti:

- stabilire collegamenti e relazioni con altre organizzazioni che potrebbero contribuire alle attività di standardizzazione basate sulla DLT;
- descrivere l'ecosistema per le applicazioni e i servizi basati sulla DLT e identificare i ruoli e responsabilità delle parti interessate nell'ecosistema;
- identificare casi d'uso di successo per l'implementazione di applicazioni e servizi basati sulla DLT.

Inoltre, sono state formulate raccomandazioni per i futuri articoli di studio dell'ITU-T e le relative azioni per i vari gruppi di studio dell'ITU-T su:

- Concetti, copertura, visione e casi d'uso dei servizi basati su DLT.
- Caratteristiche e requisiti dei servizi basati su DLT.
- Quadro dell’architettura e tecnologie di comunicazione dei servizi basati su DLT.
- Analisi e valutazione dello stato attuale della DLT e della sua maturità.
- Ricerca sugli aspetti di sicurezza e privacy delle applicazioni e dei servizi basati su DLT.
- Esame dei mezzi per estendere la fiducia online utilizzando la DLT.
- Fornitura di una piattaforma per la condivisione dei risultati e per il dialogo sulle implicazioni politiche e normative della DLT tra le aziende che lavorano sulle applicazioni DLT e le autorità di regolamentazione di vari settori industriali/economici. Individuazione delle parti interessate con cui l'ITU-T potrebbe collaborare ulteriormente, delle potenziali azioni collettive e dei passi specifici successivi.

CONCLUSIONE

Le tecnologie abilitanti per innovare, produrre e fornire sono sempre più integrate nell'attività di ogni PMI e il loro utilizzo corrisponde naturalmente all'obiettivo a lungo termine della trasformazione digitale e della transizione verde, la cosiddetta Twin Transition. Le PMI sono integrate nelle catene di fornitura globali. Blockchain e DLT forniscono ottime soluzioni ai problemi esistenti in materia di autenticità e sostenibilità delle materie prime. In questo modo, aumenta significativamente la fiducia e si contribuisce alla svolta green nella produzione.

Con questa guida abbiamo voluto illustrare alle PMI i principi di base della blockchain e della DLT, spiegando come la blockchain possa aiutare le aziende a rafforzare la trasparenza e la sostenibilità delle operazioni.

La standardizzazione della blockchain è importante per scalare le soluzioni e ridurre i costi per le PMI, come dimostrato nei casi d'uso per l'edilizia e il tessile. Gli standard garantiscono anche la fiducia e consentono a tutte le parti interessate di concludere transazioni in un ambiente più sicuro. Anche l'aspetto geopolitico della standardizzazione della blockchain è importante e le PMI devono trovare un equilibrio tra soluzioni blockchain accessibili e l'applicazione dei valori europei, pur rimanendo aperte al commercio globale, come illustrato dal caso d'uso di Huawei.

La politica dell'Unione europea nei confronti della blockchain e il suo lavoro di standardizzazione per il raggiungimento di questi obiettivi definiscono lo scenario per le PMI in relazione alle aspettative del ruolo della blockchain nell'economia europea rispetto ad altri mercati internazionali.

BIBLIOGRAFIA

Commissione europea. (2022). Proposta di regolamento relativo all'istituzione di un quadro per l'elaborazione di specifiche per la progettazione ecocompatibile dei prodotti sostenibili e che abroga la direttiva 2009/125/CE. Bruxelles: Commissione europea. https://environment.ec.europa.eu/publications/proposal-ecodesign-sustainable-products- regolamento en (Recuperato il 15 novembre 2022).

Commissione europea. (2022). COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI sul fare dei prodotti sostenibili la norma. Bruxelles: Commissione europea. https:// eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0140 (Recuperato il 15 novembre 2022).

Commissione europea. (2022). PROPOSTA DI REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO IN MATERIA DI NORME ARMONIZZATE SULL'ACCESSO EQUO AI DATI E SUL LORO UTILIZZO (DATA ACT). https://eur- lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0068 (Recuperato il 15 novembre 2022).

Commissione europea. (2021). Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO che modifica il regolamento (UE) n. 910/2014 in materia di definizione di un quadro normativo per l'identità digitale europea. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281 (Recuperato il 15 novembre 2022).

Organizzazione internazionale per la standardizzazione. (2021, 21 dicembre). ISO 22739:2020 Blockchain e DLT (Distributed Ledger Technology) - Vocabolario. Organizzazione internazionale per la standardizzazione. https://www.iso.org/standard/73771.html (Recuperato il 15 novembre 2022).

European DIGITAL SME Alliance. (2022). Guida per le PMI sui controlli di sicurezza delle informazioni. Bruxelles. Recuperato da https://www.sbs-sme.eu/news/sbs-publishes-sme-guide-smes-information-security- controls

European DIGITAL SME Alliance. (2021). Guida PMI per l'Internet industriale delle cose (IIOT) - Focus speciale sulla sicurezza. Bruxelles. Recuperato da https://www.sbs-sme.eu/news/new-sme-guide-industrial- internet-things-helping-smes-through-d igital-transformation

Castaldo, L., Cinque, V. (2018). Registrazione basata su blockchain per lo scambio transfrontaliero di dati sulla sanità elettronica in Europa. In: et al. Sicurezza nelle scienze informatiche e dell'informazione. Euro-CYBERSEC 2018. Comunicazioni nelle scienze informatiche e dell'informazione, vol. 821. Springer, Cham. https://doi.org/10.1007/978-3-319-95189- 8 5

European DIGITAL SME Alliance. (2017). Guida per le PMI per l'implementazione della ISO/IEC 27001 sulla gestione della sicurezza delle informazioni. Bruxelles. Recuperato da https://www.digitalsme.eu/digital/uploads/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management.pdf

Regolamento (UE) 2016/679. Protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati e abrogazione della direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati). Parlamento europeo, Consiglio dell'Unione europea. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679 (Recuperato il 15 novembre 2022).

GLI ESPERTI

Andrea Caccia

Consulente senior, Project Manager, coordinatore della conformità a norme e regolamenti, dello sviluppo del prodotto su:

- Servizi fiduciari e tutti i prodotti e le tecnologie correlate, ad esempio eSignature, eSeal, eDelivery
- fatturazione e archiviazione elettronica
- blockchain e DLT

Andrea partecipa alle più importanti attività di normazione europea (ETSI, CEN, ISO, UNI/ UNINFO, OASIS).

Paolo Campegiani

Esperto di identità digitale e blockchain, responsabile della strategia e dell'innovazione di Bit4id, fornitore europeo di identità digitale. Rappresentante dell'azienda in numerose organizzazioni, tra cui INATBA, ECSO, EEMA, CEN CENELEC, ISO. Capo progetto del rapporto tecnico ISO sulla blockchain e l'identità digitale TR23249.

Omar Dhaher

Responsabile tecnologico senior presso DIGITAL SME. Coordinatore del gruppo di lavoro per gli standard di DIGITAL SME e del gruppo di lavoro SBS Digitalisation. Membro della Task Force Rolling Plan della piattaforma multi-stakeholder della CE sulla standardizzazione delle TIC. Esperto di TIC, politica industriale con riferimento ai quadri normativi delle telecomunicazioni, imprenditorialità, apprendimento basato sul lavoro, competenze digitali, ricerca e standardizzazione.

Antonio La Marra

Antonio La Marra è il CEO e fondatore di Security Forge. Security Forge è una startup che affronta il problema della condivisione sicura dei dati e della loro sovranità attraverso una piattaforma di sicurezza dei dati chiamata GUARDA. GUARDA si avvale di una tecnologia di controllo dell'utilizzo dei dati. Antonio ha un solido background tecnologico, avendo trascorso più di tre anni come assistente di ricerca presso l'IIT-CNR, dove ha avuto l'opportunità di lavorare con tecnologie straordinarie, tra cui il controllo dell'utilizzo, l'analisi del malware, l'hacking delle automobili.

Donato Russo

Pioniere della blockchain, pensatore europeo, innovativo, multidimensionale e dislessico: un leader della trasformazione digitale all'avanguardia del cambiamento, che guida e gestisce soluzioni digitali rivoluzionarie e consegna globale complessa a supporto della trasformazione IT sostenibile, del commercio più intelligente, dell'innovazione delle applicazioni e l'ascesa di Web3, DAO e Metaverso. Aiutando le aziende e le organizzazioni a definire, diffondere e monetizzare i valori, fa leva su competenze specifiche e su una leadership esemplare per garantire la crescita operativa e condivisa di un business sostenibile in qualsiasi contesto. Lungimirante e tenace. Membro di Extinction Rebellion. Incoraggia gli altri a creare consenso.

Daniele Tumietto

Consulente indipendente, senior advisor, innovation manager. Daniele è anche professore a contratto presso la Link Campus University di Roma (Italia), la POLIMI Graduate School of Management di Milano e la O.M. Università Beketov di Kharkiv (Ucraina).

Membro di diversi comitati tecnici per la standardizzazione (UNI/UNINFO, CEN, ISO, ITU, UN/CEFACT) in materia di sostenibilità, ESG ed economia circolare, fatturazione elettronica, e-procurement, eBusiness e servizi finanziari, eIDAS, GDPR e protezione dei dati personali, blockchain e DLT, Industria 4.0, Intelligenza Artificiale e tecnologie quantistiche.

Italian DIGITAL SME Alliance

@ITdigitalSME

European DIGITAL SME Alliance

digitalsme.eu

@EUdigitalsme