



ASSOLOMBARDA

o de

**Il futuro  
della blockchain.**

h ai

ella

in





# IL FUTURO DELLA BLOCKCHAIN



ASSOLOMBARDA

Il Libro Bianco è stato predisposto da Assolombarda, con il coordinamento di Jacopo Moschini, Coordinatore dello Steering Committee Blockchain, e con la supervisione scientifica del Prof. Francesco Bruschi del Politecnico di Milano.

*Per Assolombarda hanno partecipato ai lavori:*

Elena Ghezzi e Paolo Guazzotti (Area Industria, Energia e Innovazione).

*I contenuti del Libro Bianco sono stati sviluppati con il coinvolgimento dello Steering Committee Blockchain di Assolombarda (<https://www.assolombarda.it/innovare-per-competere/blockchain-partecipanti-allo-steering-committee>) e in particolare:*

Andrea Colmegna (Fastweb e Npo Sistemi), Cristiano Crippa (Dompé Farmaceutici), Mattia D'Alessandra (MSD Solutions), Pietro Gorgazzini (Primis Group), Renato Grottola (DNV GL), Pietro Lanza (Intesa-Gruppo IBM e IBM Italia), Fabio Maniori (Associazione Trusted Smart Contract), Giovanni Mocchi (Zucchetti), Sara Noggler (Polyhedra e San Marino Innovation), Paul Renda (Miller Group), Jacopo Sesana (Blockchain Italia e Blockchain Education Network Italia).

*Si ringraziano inoltre per i contributi:*

Massimo Brusa (Brusa), Giuseppe Cardinale Ciccotti (UniquID Italia), Vasco Ciresola (Zucchetti Software Giuridico), Marzia Chiesa (Sodai), Mattia De Vecchi (Prosume), Rudy Lazzarin (Flowdron), Alessandro Paganini (Tacchificio Villa Cortese), Silvano Pagliuca (Confindustria Chieti Pescara).

*Pubblicato:* 22 febbraio 2021

*Durante lo sviluppo del Libro Bianco alcuni referenti aziendali hanno intrapreso nuovi percorsi professionali; di conseguenza, per questi referenti sono indicate sia l'impresa con cui hanno iniziato l'esperienza sul Libro Bianco sia quella in cui oggi ricoprono posizioni.*

## Introduzione

Con questo volume si conclude l'esperienza dei Libri Bianchi di Assolombarda, il ciclo avviato nel 2018 e nato dalla visione strategica espressa da Carlo Bonomi, all'epoca Presidente di Assolombarda e ora Presidente di Confindustria. Sulla base del lavoro che diversi imprenditori e tecnici aziendali (successivamente organizzati nello Steering Committee Blockchain dell'associazione) avevano iniziato a sviluppare, Assolombarda ha individuato nella Blockchain una delle direttrici tecnologiche più promettenti, al punto da volerne fare l'oggetto del presente volume.

All'inizio del 2020, poco prima che la pandemia esprimesse tutto il suo effetto dirompente, Assolombarda pubblicava il suo Libro Bianco sul Futuro della Fabbrica. In quel Libro Bianco si sottolineava, tra le considerazioni e le raccomandazioni conclusive, la centralità degli "ecosistemi" nelle strategie di sviluppo e competitività aziendale. In particolare, si affermava che *"[n]ell'ecosistema, la dimensione del singolo nodo non è per forza determinante, quanto lo è invece il suo posizionamento strategico. La posizione strategica è definita in termini di gerarchia e numero di connessioni. [...] La convergenza tecnologica di questi anni – ad esempio di IoT e blockchain – contribuisce in modo significativo all'integrazione e all'efficienza di ecosistemi complessi, anche risolvendo tecnologicamente questioni più relazionali, come la fiducia tra i membri dell'ecosistema, la trasparenza delle transazioni, la visibilità e la condivisione degli accadimenti"*.

Gli ultimi 12 mesi hanno messo a dura prova, su scala globale, i sistemi di relazione classici su cui per lungo tempo si è fondato lo scambio sociale e anche la pratica economica. Interi set di valori, quali la *condivisione*, la *vicinanza* e per certi versi, la stessa *fiducia verso il prossimo* hanno assunto connotazioni diverse e sono risultati largamente indeboliti. Al contempo, la dimensione digitale si è rivelata il più efficace "collante" delle relazioni sociali e lo strumento principale a supporto della resilienza aziendale.

Questi fenomeni, in maniera naturale, hanno accelerato la presa di coscienza e reso più chiari i potenziali benefici legati alla *blockchain*, che dalle prime applicazioni in ambito finanziario, ha ampliato di molto il proprio raggio e oggi assume un ruolo sempre più significativo nel mondo produttivo.

La dimensione tecnologica, unita ai forti cambiamenti in atto a livello globale, pone le imprese di fronte a un cambio di paradigma, che consente sia di realizzare una maggiore interconnessione e cooperazione nell'ambito di filiere e di ecosistemi sia di abilitare nuovi modelli organizzativi e favorire la nascita di nuove figure professionali. Tutto questo richiede cambiamenti importanti all'interno dell'impresa e nel complesso di relazioni esterne.

Con questo Libro Bianco, Assolombarda intende contribuire a favorire nei confronti delle imprese e degli *stakeholder* pubblici e privati la conoscenza delle potenzialità di questa tecnologia, per poterne cogliere al meglio i vantaggi. Tuttavia, alla maggiore consapevolezza degli operatori è necessario associare la creazione di un contesto che sia idoneo e favorevole allo sviluppo delle applicazioni della *blockchain*. Da questo punto di vista, vi sono aspettative elevate riguardo ai contenuti e alle prospettive delineate dalla Strategia Nazionale sulla Blockchain, attualmente in corso di definizione. Le proposte e le raccomandazioni che chiudono il Libro rappresentano il contributo di Assolombarda verso una Strategia allineata alle elevate potenzialità a favore delle imprese.

L'Italia può giocare un ruolo fondamentale in relazione a questa tecnologia, anche a supporto della competitività delle nostre filiere strategiche. Siamo infatti nella top 10 mondiale dei Paesi con il maggior numero di progetti blockchain sviluppati tra il 2016 e il 2020. Un know-how importante e una testimonianza di apertura alla sperimentazione che rappresentano un'occasione da non perdere.

**Jacopo Moschini**

Coordinatore Steering Committee  
Blockchain Assolombarda



## Indice

<b>Parte 1 – Cos'è e come nasce la blockchain</b>	<b>10</b>
1.1 Incipit: Bitcoin	11
1.2 La blockchain	12
1.3 Denaro programmabile	13
1.4 Ethereum, il “world computer”	14
<b>Parte 2 – La tecnologia e le applicazioni</b>	<b>16</b>
2.1 Applicazioni	17
2.2 Livelli di decentralizzazione: le blockchain permissioned e permissionless	26
2.3 Piattaforme “istituzionali”	32
2.4 Applicazioni alla supply chain	35
<i>Approfondimento – Esperienze e casi applicativi</i>	41
<b>Parte 3 – Gli scenari</b>	<b>72</b>
3.1 A che punto siamo	73
3.2 Come cambierà la nostra vita	76
3.3 Ostacoli	77
<b>Parte 4 – Raccomandazioni</b>	<b>78</b>
Raccomandazioni	79



# **Cos'è e come nasce la blockchain**

# **1**

## 1.1 Incipit: Bitcoin

Nel 2008 un autore dalla natura misteriosa, dietro lo pseudonimo di Satoshi Nakamoto, pubblica su una mailing list dedicata alla crittografia un articolo in cui, combinando tecnologie già esistenti (firma digitale, reti di comunicazione peer-to-peer, funzioni di *hash*), descrive un sistema di “contabilità” di particolari oggetti digitali, i “Bitcoin”. Il sistema, basato su uno speciale registro contabile, avrebbe consentito lo scambio di questi oggetti via internet in modo sicuro, da parte di chiunque, senza identificazione e senza censura, implementando così un sistema di contante digitale *peer to peer*, vale a dire senza intermediari finanziari. La sicurezza è dovuta alla distribuzione del registro tra un numero grande a piacere di partecipanti al sistema (*i nodi*), che custodiscono e aggiornano il registro secondo regole precise.

Il protocollo descritto nell’articolo ha introdotto alcune novità rilevanti. La prima è un meccanismo che, per consentire ai partecipanti di mantenere il consenso sul contenuto del registro in evoluzione, richiede di spendere dimostrabilmente quantità significative di energia per aggiungere informazione, ricompensando con nuovi Bitcoin.

L’altro aspetto notevole riguarda la dinamica monetaria dei Bitcoin: quanti ne esistono all’inizio? Quanti ne verranno prodotti in futuro? A quale ritmo? La risposta a queste domande è deterministica, stabilita a priori, certa, e non modificabile. Il determinismo crea, per la prima volta nella storia, un bene *digitale* dimostrabilmente scarso, analogamente ai metalli preziosi.

Nel 2009 Satoshi passa alla pratica implementando le idee dell’articolo in un programma che consente agli utenti di partecipare alla rete con il proprio computer e di scambiare Bitcoin, creando delle sorte di conti bancari identificati da “indirizzi”, l’equivalente crittografico degli IBAN. I Bitcoin cominciano ad essere utilizzati come mezzo sperimentale di scambio del valore in alcuni circoli di entusiasti. Nel 2010 Laszlo Hanyecz,

## Parte 1 – Cos'è e come nasce la blockchain

un programmatore con base in Florida, compra due pizze dalla catena “Papa John”, pagandole 10000 Bitcoin, dando origine al primo caso documentato di utilizzo di Bitcoin per l’acquisto di un bene. Da allora visibilità e valore aumentano costantemente, con dinamiche altalenanti di violento apprezzamento (le cosiddette “bull run”) e successivo deprezzamento, che ogni volta portano il Bitcoin a stabilizzarsi su valori più alti, fino ad arrivare agli oltre 50.000\$ di oggi.

### 1.2 La blockchain

Il funzionamento di Bitcoin si basa su uno speciale registro di informazioni concatenate, al quale è possibile aggiungere informazione, ma non cancellarla, che prende il nome di “blockchain”. Volendo, si può immaginare la blockchain come una sorta di Twitter decentralizzato (cioè non controllato da una singola persona o società) e incensurabile, in cui chiunque può aggiungere dei *tweet*, ma nessuno può rimuoverli. In questo Twitter speciale valgono speciali “identità crittografiche”, composte da una chiave pubblica e una chiave privata. Chiunque può creare un’identità unica di questo tipo, con il più economico dei computer. La chiave pubblica rappresenta l’identificativo (lo *username*), quella privata la password, che consente di “firmare” digitalmente un qualsiasi documento a nome dello “username”.

Per impedire che qualcuno possa aggiungere tweet a ritmi tali da rendere la catena troppo lunga e inservibile (in gergo recente, per prevenire lo “spam” del registro), il sistema richiede di pagare, spendendo delle frazioni di Bitcoin, una piccola tassa per ogni aggiunta. L’utilizzo principale dei *tweet* è come “assegni” per trasferire valore: un utente, rappresentato da una chiave pubblica, può cedere del valore ad un altro indirizzo. Per farlo, prende un assegno che “controlla” e lo “gira” a qualcun altro, firmandolo digitalmente

(esempio: “giro questo assegno da 2 Bitcoin, attualmente di mia proprietà, a 13NYm7BZN2QkZdda1jdVTkKj3vnCQZYPygv. Firmato 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa). A questo punto 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa ha la disponibilità dell’assegno, e lo può girare a sua volta. Questi tweet che rappresentano delle “girate” si chiamano “transazioni”. Una transazione “spende” un assegno precedente, e ne crea uno nuovo, nella disponibilità di un altro indirizzo. Scorrendo questo gigantesco Twitter, chiunque può vedere quali sono gli assegni non ancora spesi, e solo chi possiede la chiave privata corrispondente all’indirizzo di un assegno non speso può girarlo.

### 1.3 Denaro programmabile

Oltre ad implementare un protocollo di trasmissione del valore, il sistema introduce il fondamentale elemento della *programmabilità*, sotto forma di condizioni complesse che possono essere specificate per la spesa di una transazione. Per esempio, si può specificare che un certo valore possa essere speso solo se cinque chiavi in un certo insieme di dieci si mettono d’accordo e firmano congiuntamente. La programmabilità apre diverse possibilità, tra le quali per esempio la creazione di fondi comuni, con vincoli flessibili, o configurazioni di *escrow*, nei quali degli utenti si scambiano valore ed eleggono un arbitro che ha il potere di risolvere eventuali dispute. Più in generale, la programmabilità introduce la possibilità di creare meccanismi automatici di movimento e trasmissione del denaro, aprendo la strada ad applicazioni finanziarie il cui funzionamento è garantito dalla blockchain. La programmabilità di Bitcoin, però, è limitata intenzionalmente, per evitare comportamenti imprevedibili e indesiderati (i famigerati “bug” del software). Se nel contesto della filosofia in cui si è sviluppato Bitcoin questa è considerata

## Parte 1 – Cos'è e come nasce la blockchain

una caratteristica positiva, alcuni sviluppatori pensano che valga la pena di esplorare le possibilità offerte da un sistema di programmabilità più potente ed espressivo.

### 1.4 Ethereum, il “world computer”

Nel 2013 Vitalik Buterin, uno sviluppatore attivo nel mondo delle criptovalute, propone Ethereum, un sistema che eredita molte delle caratteristiche di Bitcoin, ma che è dotato di un meccanismo di programmabilità molto più potente (in gergo informatico si dice “Turing completo”, che implica un’espressività equivalente agli altri linguaggi di programmazione, ad esempio quelli utilizzati per lo sviluppo di applicazioni). Il sistema viene proposto all’immaginario collettivo tramite l’immagine di un “computer mondiale” con caratteristiche notevoli: chiunque, “pagando” una certa quantità di *Ether*, la valuta nativa della piattaforma, può caricare del codice, che sarà quindi eseguito in modo trasparente, verificabile, incensurabile. I programmi eseguiti su Ethereum vengono denominati, per una serie di ragioni diverse, con l’espressione suggestiva (e in parte fuorviante) di *smart contract*. Ethereum generalizza Bitcoin nel senso che, per esempio, un sistema di contabilità come quello della criptovaluta di Satoshi è una delle tante applicazioni possibili. Ma l’ambizione degli smart contract è di offrire una nuova dimensione alla digitalizzazione: non solo aumentando l’efficienza di un processo, ma anche rendendone l’esecuzione *dimostrabilmente affidabile*, dimensione questa, capace di aprire la strada a possibilità inedite.

La nascita di Ethereum crea nei sistemi blockchain una tensione che ritroviamo ancora oggi: da una parte Bitcoin punta sull’immutabilità, sulla semplicità del protocollo, sulla dinamica monetaria predicibile e limitata (in questo senso il valore di Bitcoin è di essere un punto di riferimento per chi cerca una

“riserva di valore”, non dissimilmente dall’oro). Ethereum, invece, ambisce ad evolversi continuamente per migliorare prestazioni, superare limiti, utilizzare nuove tecnologie, ed oggi questo la porta ad essere il sistema attorno a cui orbita il maggior numero di sviluppatori.

Oltre a Bitcoin ed Ethereum, che sono indubbiamente le principali piattaforme blockchain, se ne contano molte altre, con l’ambizione di risolvere alcuni limiti e problemi delle due maggiori. I principali tra questi problemi sono l’efficienza energetica dovuta al proof of work, (cioè la necessità di spendere energia per estendere il registro), la quantità di transazioni che possono sopportare, la privacy (nonostante gli utenti siano pseudonimi, cioè in linea di principio non riconducibili a identità anagrafiche, è tuttavia possibile tracciare tutte le transazioni da indirizzo a indirizzo, spesso arrivando ad inferire l’identità dei soggetti o altre informazioni sensibili).

# **La tecnologia e le applicazioni**

# **2**

## 2.1 Applicazioni

La blockchain viene spesso citata come una tecnologia rivoluzionaria. Ma quali sono gli utilizzi possibili? La categoria di applicazioni in un certo senso più ovvia è quella dei **sistemi di pagamento**. Come si è visto, le valute associate alle piattaforme (Bitcoin, Ether) sono apprezzate economicamente e possono essere trasferite facilmente. Un vantaggio notevole rispetto agli altri sistemi di trasferimento digitale del valore è l'“universalità”: l'accesso alla rete senza richiedere neppure il possesso di un'identità anagrafica, aspetto molto significativo per l'inclusione finanziaria di quella enorme frazione di popolazione del pianeta che non ha attualmente accesso ai sistemi bancari. Altri vantaggi sono l'affidabilità, nel senso di robustezza della rete e di incensurabilità, e la già citata programmabilità. Non mancano però le debolezze: le principali blockchain possono al momento sopportare un ritmo di transazioni limitato e inferiore a quello degli altri circuiti di pagamento, hanno esperienze utente che in alcuni casi possono intimidire i meno esperti e soffrono, anche in virtù del loro non facile inquadramento, problemi di raccordo con le normative, per esempio quelle di antiriciclaggio, inquadramento fiscale etc. Va detto che l'ecosistema di sviluppo software che ruota attorno alle blockchain sta agendo, con entusiasmo e a ritmi significativi, per risolvere molti di questi problemi.

Collegati ai pagamenti ci sono i **sistemi di custodia**, i cosiddetti *wallet*. Gli attuali sistemi di custodia del valore (digitale) si basano su attori fidati e regolamentati. Le criptovalute, in qualche modo analogamente al contante, possono essere conservate direttamente dall'utente, tramite la conoscenza esclusiva della chiave privata, disintermediando di fatto la custodia. C'è però il rovescio della medaglia: se l'utente perde la chiave, non ha modo di recuperare i soldi. Questa dualità spesso viene presentata come inevitabile conseguenza dell'uso di criptovalute. In realtà la programmabilità consente di immaginare ed attuare

## Parte 2 – La tecnologia e le applicazioni

logiche di custodia molto più articolate, fantasiose e funzionali. Per esempio, è possibile definire wallet con meccanismi di *social recovery*: l'utente elegge un certo numero di altri utenti come "custodi", conferendo loro alcune prerogative sul suo account (es: un custode può bloccare il wallet di un suo "custodito" per un giorno; due terzi dei custodi possono cambiare la chiave del wallet, etc). In questo modo la responsabilità della custodia può essere distribuita secondo precise architetture su una struttura sociale con requisiti diversi da quelli "classici": ad un custode non viene richiesta solidità economica, ma affidabilità e diligenza nel gestire e proteggere le proprie chiavi. Questo tra l'altro non implicherebbe l'eliminazione dei custodi classici, ma la loro ridefinizione: gli utenti potrebbero decidere di scegliere come custodi in parte conoscenti prossimi e fidati, in parte professionisti o società specializzate. Esistono già esempi di questo tipo di wallet a custodia distribuita, tra cui Argent (<https://www.argent.xyz/>).

Cosa succede invece se si "decentralizzano" applicazioni "classiche", facendole girare su blockchain? Un esempio è quello dei **social network**. Un social network decentralizzato avrebbe alcune proprietà notevoli, tra cui una riguarda gli algoritmi che definiscono le politiche di formazione delle *timeline*, le informazioni che vengono mostrate agli utenti. Nei social network classici queste non sono direttamente conoscibili, e sono non di rado accusate di fomentare fenomeni come la formazione di *echo chamber* (gruppi di individui che rafforzano a vicenda le proprie convinzioni, invece di metterla a confronto con idee diverse), la propagazione di *fake news* etc. In un social network decentralizzato gli algoritmi sarebbero completamente trasparenti e conoscibili dagli utenti, e potrebbero addirittura implementare politiche che orientano verso comportamenti virtuosi (per esempio verificare le notizie che si condividono), facendo leva anche sulla possibilità di distribuire premi monetari. Esempi di social network di questo tipo sono Steemit, Mastodon, Peepeth.

Un'altra classe di possibilità offerte dagli smart contract è la creazione di **token**, cioè oggetti digitali con proprietà notevoli, tra cui la facilità di scambio tipica delle criptovalute, l'impossibilità di essere contraffatti, e la possibilità di definire arbitrariamente una dinamica "monetaria" che, una volta stabilita è pubblica ed immutabile. Le applicazioni dei token sono molteplici, tra le quali la possibilità di rappresentare:

- il diritto di utilizzo di un servizio, come i gettoni telefonici;
- qualche forma di diritto, come la proprietà di un bene fisico o finanziario, come il certificato di proprietà di un automezzo;
- i punti fedeltà di una catena di negozi e supermercati.

Rappresentare questi beni tramite token su blockchain offre diversi significativi vantaggi, tra i quali spicca l'interoperabilità. Per esempio, oggi nella maggior parte dei casi non è possibile utilizzare dei punti fedeltà altrove che presso l'emittitore. Creare sistemi in cui più attori emettono ed accettano reciprocamente punti fedeltà sarebbe complicato e costoso. Se i punti fossero rappresentati come token su una blockchain, la trasferibilità universale sarebbe *nativa*, e i punti sarebbero utilizzabili direttamente sulle piattaforme di scambio già esistenti. Questo apre la strada ad un altro insieme di applicazioni di scambio di valore, che vanno sotto il nome di *finanza decentralizzata*. Sfruttando le garanzie intrinseche di esecuzione deterministica ed affidabile è possibile implementare piattaforme che consentono forme di scambio del valore, sotto forma di token, che non richiedono garanti o intermediari. Al momento esistono diversi esempi, tra cui i **money market**, sistemi in cui gli utenti chiedono un prestito di un certo numero di token di un tipo, mettendo a garanzia token di un altro tipo. Un utente può decidere se prestare dei token, e percepire un interesse, oppure chiederne in prestito, mettendone altri a garanzia. Il funzionamento di queste piattaforme non è "sorvegliato" da nessun ente garante. Gli utenti traggono fiducia dalle garanzie di esecuzione del codice data dalla blockchain, piuttosto

che dalla responsabilità in capo ad un particolare soggetto noto (leggi: e non dal fatto che “dietro c’è una banca”). L’esempio più capitalizzato di money market al momento è Compound (<https://compound.finance/>). Altra classe emblematica è quella dei **prediction market**: piattaforme in cui è possibile proporre un quesito su accadimenti futuri (ad esempio: “Chi vincerà le prossime elezioni USA?”). Per ogni possibile esito vengono creati dei token che, ad evento occorso, frutteranno del valore se corrispondenti alla previsione corretta. I token possono essere scambiati in un mercato secondario, e le quote a cui vengono scambiati catturano l’opinione del mercato circa la probabilità di ciascun evento. Questo sistema ha il vantaggio di legare le previsioni ad un guadagno economico (o ad una perdita), diversamente da quanto avviene in altri contesti di previsione (per esempio quando viene interrogato un esperto in un salotto televisivo). Anche in questo caso, gli utenti non si fidano di “chi c’è dietro”, ma del codice che definisce i mercati, per come è scritto. Un esempio piattaforma di questo tipo è Augur (<https://www.augur.net/>)

Altra applicazione interessante sono le **lotterie senza perdita**, in cui un premio viene assegnato ad un vincitore, e alla fine tutti recuperano il prezzo del biglietto. L’esempio più famoso è PoolTogether (<https://www.pooltogether.com/>): gli utenti depositano del valore, sotto forma di token, all’inizio della settimana. Lo smart contract dell’applicazione mette i token depositati come prestito ad interesse su Compound. Alla fine della settimana, gli interessi derivanti dai token di tutti vengono raccolti e assegnati casualmente ad un partecipante, mentre tutti si riappropriano del capitale versato. Questa struttura mostra anche come le applicazioni possano essere composte: in questo caso, quella della lotteria utilizza il money market.

In virtù della loro capacità di distribuire la responsabilità dell’esecuzione di logiche e algoritmi le blockchain possono aiutare nella digitalizzazione di processi che coinvolgono attori di-

versi ed eterogenei. Esempi rilevanti sono la gestione delle *supply chain*, i sistemi di tracciamento, il contrasto alla contraffazione. In questi ambiti, la disponibilità di rappresentazioni digitali dell'informazione logistica, industriale, doganale, finanziaria consentirebbe di aumentare l'efficienza, la trasparenza, la consapevolezza dei consumatori, per esempio consentendo di rispondere a domande come "Da dove proviene questo prodotto? È importato legalmente? Da dove provengono i semilavorati da cui deriva?". Il funzionamento della *supply chain* richiede il coordinamento di molti attori: banche, dogane, venditori ed acquirenti, trasportatori, che comunicano tra l'altro emettendo documenti (bolle, lettere di credito, certificati etc) e si comportano seguendo protocolli e processi, che una digitalizzazione efficace deve poter rappresentare ed automatizzare per quanto possibile. Per apprezzare il possibile contributo specifico della blockchain, si consideri una condizione semplice ed astratta, che potrebbe fare parte di un processo: se gli attori X e Y hanno prodotto i documenti A e B con tutti i dati richiesti, un certo carico è ammesso al trasporto da parte di Z. La condizione su A e B può comprendere ragioni di natura e con origini diverse: A può essere una lettera di credito, che dice che il compratore ha una linea aperta con una banca, mentre B può essere un certificato di origine etc. In un sistema ideale la verifica che A e B sono presenti e conformi, e la segnalazione che il trasporto può avvenire potrebbero essere automatizzate. Ora, se il sistema informatico che verifica la condizione e dà il via libera appartiene (cioè è controllato) ad un attore particolare, su questo gravano grandi responsabilità, e gli altri potrebbero non essere disposti a delegare l'autorità che ne deriva. Idealmente, tutti gli attori interessati potrebbero volere verificare le condizioni, e allo stesso tempo sapere che anche gli altri interessati le hanno verificate, e che sono tutti d'accordo! Una blockchain consentirebbe, in questo caso, di definire il meccanismo di controllo su A e B tramite uno smart contract, la cui esecuzione sarebbe distribuita e verificabile, e sul cui esito convergerebbe l'accordo di tutti. In questo

## Parte 2 – La tecnologia e le applicazioni

tipo di contesti si utilizzano a volte sistemi in cui la validazione è distribuita su un numero limitato e noto di attori, a differenza di quanto avviene per i sistemi come Bitcoin ed Ethereum, dove chiunque può candidarsi ad essere validatore. Le blockchain di questo tipo vengono definite “permissioned” (in opposizione alle “permissionless”), riferendosi al fatto che i validatori devono far parte di un insieme abilitato. Questo ovviamente implica alcune differenze, anche sostanziali, in caratteristiche come l’immutabilità e l’incensurabilità.

Il vantaggio nell’uso di una blockchain è ancora più evidente quando i processi hanno dimensioni finanziarie. Per esempio, si consideri una compravendita tra A e B, dove entrambi gli attori vogliono essere garantiti (A vuol essere sicuro di essere pagato, B vuole pagare alla ricezione, a patto che siano rispettate certe condizioni). B potrebbe accantonare dimostrabilmente il valore necessario a pagare la merce tramite uno smart contract, che procederebbe automaticamente a pagare A, basandosi sulla ricevuta di ricezione, ovviamente digitalizzata, quando B riceverà la merce. Una meccanica di questo tipo oggi richiede la collaborazione di molti attori e l’interazione di sistemi diversi (la banca di A, la banca di B, il sistema informativo del trasportatore) e, crucialmente, qualche sistema che emetta l’ordine di pagamento. Con la blockchain, uno smart contract definito e “sottoscritto” multilateralmente da A e B, può coordinare l’esecuzione dei processi in modo autorevole e condiviso. Un ulteriore aspetto interessante è che gli smart contract possono essere utilizzati per allineare gli incentivi degli attori della filiera verso la produzione di dati affidabili, per esempio redistribuendo i vantaggi economici che provengono dall’incremento di affidabilità. Ad esempio, si potrebbero remunerare i trasportatori che concorrono alla raccolta di tracciamento di qualità, quando il prodotto viene venduto.

Un altro ambito applicativo a cui la blockchain può contribuire è quello dell’identità digitale. Il modello attualmente prevalen-

te è basato sugli Identity Provider, attori che identificano un utente, e poi “garantiscono” per lui presso un insieme ampio di fornitori di servizi. Il provider può essere riconosciuto ed abilitato a garantire per l’identità dei soggetti in ambito pubblico (si pensi ad esempio a SPID e agli identity provider eIDAS in ambito europeo), ma per molte applicazioni questo non è necessario (si pensi al login tramite Google e Facebook). Questo modello, se da una parte consente interessanti applicazioni dall’altra ha importanti limiti: è poco flessibile (i dati dell’identità per cui un identity provider può garantire sono definiti in anticipo, ed è difficile estenderli), è centralizzato (un attacco ad un identity provider preclude all’utente la possibilità di identificarsi), costringe l’utente a delegare la custodia e il controllo delle informazioni personali ad un attore terzo. Per risolvere questi e altri problemi è stato proposto un modello di identità detto “self sovereign”. La Self Sovereign Identity (SSI) è definita da una serie di principi, come il controllo e la minimizzazione (gli individui possono decidere esattamente quale parte di informazione mostrare, a differenza di quanto succede, per esempio, mostrando la patente durante un controllo). Il cuore di questo modello è la possibilità, per l’individuo, di generare un identificativo che può dimostrare di controllare, per esempio con meccanismi crittografici analoghi a quelli che consentono di controllare fondi e account su Bitcoin o Ethereum. Le informazioni e la storia dell’utente sono invece rappresentate da *claim*, cioè da affermazioni che altre entità (individui, istituzioni, etc) fanno su di lui. I *claim* sono rappresentati digitalmente, cosa che ne rende possibile la memorizzazione in diverse forme: su una chiavetta, crittografati nel *cloud*, stampati su carta. Inoltre sono digitalmente firmati, rendendo possibile a chiunque la verifica dell’integrità e della provenienza. In questo modello, l’utente può decidere, nelle sue interazioni con il mondo, di produrre i certificati, o parte di essi, che più ritiene utili: può per esempio presentare un certificato di laurea, senza mostrare la propria nazionalità, o il proprio sesso. L’individuo potrebbe anche decidere di valorizzare i pro-

## Parte 2 – La tecnologia e le applicazioni

pri dati, e di condividerli selettivamente, in modo consapevole, a fronte di un vantaggio o di un corrispettivo economico. Questo potrebbe a propria volta generare meccanismi redistributivi innovativi e dirompenti.

Quale ruolo gioca la blockchain in questo tipo di identità? Per capirlo si consideri il problema della revoca dei certificati: a differenza di un certificato fisico (es. una patente), uno digitale è difficile da revocare, perché può essere copiato indefinitamente (a differenza di quello fisico, unico, che può essere sequestrato). Una soluzione è ricorrere alle cosiddette *revocation list*: quando un emittitore vuole ritirare dei *claim*, o più in generale cambiarne lo stato, pubblica una lista con l'identificativo dei certificati da revocare, e la distribuisce. La modalità di pubblicazione della lista però deve soddisfare requisiti tecnicamente significativi: deve essere sempre accessibile online, non manomettibile, sicura rispetto ad attacchi, non censurabile. Questi oneri restringerebbero di molto il numero di soggetti in grado, più che di emettere, di revocare dei *claim*. Uno dei servizi offerti dalle blockchain, d'altra parte, è proprio un registro distribuito, altamente disponibile, non censurabile e permanente, che può essere utilizzato come riferimento dove registrare lo stato dei certificati. Questa accessibilità implicherebbe significativamente l'ampliamento della platea di soggetti in grado di rilasciare *claim*, moltiplicando la possibilità da parte del soggetto di raccogliere informazioni che lo riguardano. Ad esempio, la ricevuta di una bolletta potrebbe trasformarsi in un *claim* verificabile, consentendo all'utente (e solo a lui) di poter dimostrare a terzi quel particolare rapporto economico, e aprendo la possibilità di applicazioni e mercati inediti (ad esempio, gli utenti potrebbero dimostrare la propria affidabilità economico-finanziaria attingendo tra l'altro alla storia dei pagamenti delle proprie bollette, in modo sicuro e autonomo).

Un'altra classe notevole di possibilità sarebbe l'interazione identificata con *smart contract*: molte applicazioni interessanti, come l'emissione di token che rappresentano *securities*, richiede-

rebbero di identificare il possessore dei token per varie ragioni (si pensi, per esempio, all'antiriciclaggio). La soluzione oggi più rappresentata è la custodia di token da parte di attori terzi, come ad esempio una banca, che identificano l'utente. Questa soluzione ovviamente rischia di snaturare il potenziale disintermediante delle blockchain. Le credenziali verificabili consentirebbero invece di emettere token tramite smart contract che richiedono "intrinsecamente" al soggetto di identificarsi (oppure di dimostrare di essere identificabile in determinate situazioni), utilizzando dei *claim* rilasciati da un ente autorizzato al riconoscimento (per esempio, un identity provider SPID). Questo introdurrebbe ampi margini di manovra nella progettazione di applicazioni conformi alle regolamentazioni, senza sacrificare la disintermediazione.

Un altro settore di potenziale applicazione è la pubblica amministrazione, dove gli smart contract potrebbero essere utilizzati per rappresentare e implementare processi in modo trasparente e verificabile. Ad esempio, le regole per assegnare un posto all'asilo, al momento sono codificate su documenti "human readable" (leggi, regolamenti etc). Sempre più di frequente, il servizio (interfaccia con l'utente, esecuzione delle logiche di assegnamento, interazione con i funzionari pubblici) viene implementato digitalmente, ma il codice che implementa tali processi tipicamente non è pubblico, e la sua esecuzione è "opaca": l'utente non sa cosa stia succedendo, se le regole sono state implementate correttamente, a che punto si trova la sua pratica. Nel caso migliore, l'utente trae vantaggio dalla digitalizzazione in termini di velocità e facilità di accesso. Codificando le regole digitalmente tramite uno smart contract, la logica del servizio sarebbe nativamente osservabile e pubblica, e così anche l'esecuzione. L'utente (o chi per lui) potrebbe quindi esaminare il codice, verificare che codifichi correttamente le regole, sapere in che stato si trovi la sua pratica, utilizzare interfacce alternative per interagire con il processo. La digitalizzazione diventerebbe quindi uno strumento che consen-

te di conferire legittimazione all'implementazione di un particolare servizio. I problemi di privacy che ovviamente sorgerebbero sono affrontabili con gli strumenti offerti dalla crittografia.

### **2.2 Livelli di decentralizzazione: le blockchain permissioned e permissionless**

Come si è visto, una delle dimensioni che caratterizzano una blockchain è quella della “validazione”: chi decide, e come, quali sono le informazioni (le transazioni) da aggiungere di volta in volta nella blockchain? Visto che i dati sono immutabili, questa dimensione assume un'importanza cruciale. Gli attori che contribuiscono a decidere quali nuove transazioni inserire in ogni istante si chiamano tipicamente “validatori”. È chiaro che la definizione di chi siano i validatori, e in quale modo decidano collettivamente quali transazioni nuove inserire, è un aspetto fondamentale di una blockchain.

Per apprezzare l'importanza del comportamento dei validatori, consideriamo due tra le responsabilità che hanno:

1. Garantire che tutte le transazioni valide, proposte dagli utenti, siano inserite prima o poi nella blockchain. Questo equivale a dire che è possibile per chiunque interagire con la logica della blockchain, cioè che non vengono mai applicate censure. (Attenzione: questo non vuol dire che non sia possibile precludere ad alcuni utenti di fare qualcosa, ma solo che queste preclusioni devono essere chiaramente definite nelle applicazioni, e non possono essere applicate a livello dell'infrastruttura. La situazione è simile a quella di Internet: è ovviamente possibile sviluppare un'applicazione web alla quale possono accedere soltanto determinati utenti, ma non è possibile (o è molto difficile, e questa è una caratteristica saliente di inter-

net) impedire a chicchessia di accedere alla rete. Questo è un aspetto fondamentale della *value proposition* delle blockchain: non è possibile censurare l'accesso all'infrastruttura blockchain, solo determinare, con regole chiare e condivise, chi possa accedere alle applicazioni.

2. Accordarsi sempre su quale sia l'ordine delle transazioni ricevute.

Chi sono dunque, nella pratica, i validatori? Ci sono sostanzialmente due categorie di soluzioni differenti. Nell'approccio **permissioned**, i validatori sono un insieme di entità definite, identificate oppure pseudonime. Qual è la differenza? Come si è visto, in una blockchain, gli attori/utenti sono sempre identificati crittograficamente. Questo vuol dire che ogni interazione con il sistema da parte di un utente (ogni transazione) è associata, tramite una firma digitale, ad un codice identificativo, a cui ci si riferisce di solito con i termini di *address*, chiave pubblica o *account*. La crittografia garantisce che, per firmare a nome di un account, si debba conoscere la corrispondente chiave privata. L'account quindi costituisce in un certo preciso senso, e nell'accezione etimologica del termine, una forma di "identità": se due transazioni sono firmate dallo stesso account, vuol dire che sono state create dallo stesso individuo o entità (a patto ovviamente che nessun altro sia venuto a conoscenza della chiave privata). Di una identità "crittografica" può però non essere nota l'identità ufficiale, anagrafica di chi la controlla. La situazione è analoga ad un account anonimo su un social network (i post provengono dall'individuo o dagli individui che conoscono la password), ad un artista "anonimo" (si pensi ad esempio alle opere di Banksy), o all'entità dietro alla redazione del *whitepaper* che ha dato origine a Bitcoin, Satoshi Nakamoto.

Quando è invece possibile collegare un account ad una identità anagrafica, parliamo di attori identificati.

In un approccio *permissioned*, l'insieme dei validatori è definito a priori, al momento della creazione della rete. I validatori rice-

## Parte 2 – La tecnologia e le applicazioni

vono le transazioni dagli utenti, le verificano, le inseriscono in blocchi, e le aggiungono progressivamente alla catena. Per semplicità concettuale, possiamo immaginare che il meccanismo sia questo:

- a turno, un validatore viene scelto a caso dal sistema per generare il prossimo blocco;
- il validatore prescelto prende un certo numero di transazioni da quelle pendenti, e le racchiude in un blocco. Quindi firma il blocco, e lo propone come prossimo blocco da aggiungere;
- gli altri validatori ricevono il blocco, e votano se includerlo o meno. Se il blocco riceve un numero di voti superiori a una certa soglia (configurabile, ad esempio 10 su 20), tutti i nodi lo inseriscono nella catena.

Nella realtà ci sono molte sottigliezze ulteriori, ma questo modello semplificato permette di apprezzare alcune caratteristiche e conseguenze.

Cosa succede se un validatore decide di non inserire le transazioni provenienti da un certo account (che equivale a censurarlo, o impedirgli di interagire con la rete)? Se il comportamento è agito solo da quel validatore, al turno successivo, quando toccherà ad un altro, la transazione sarà inserita. Questo meccanismo quindi previene la censura, a patto ovviamente che non tutti i validatori siano intenzionati ad attuarla.

Cosa succede se un validatore non compila il blocco, quando è il suo turno? Un turno va perso, ma al turno successivo il validatore prescelto farà il suo dovere. Questo meccanismo impedisce che una minoranza di validatori possa arbitrariamente bloccare la rete.

Cosa succede se un validatore inserisce transazioni non valide? Gli altri validatori non “attestano” il blocco che ha prodotto, e questo non viene aggiunto alla catena.

Nelle soluzioni permissioned, la sicurezza della rete è garantita se c'è una certa frazione di validatori che si comportano onestamente (nel senso che seguono regole). In sintesi, il fatto

che ci sia una molteplicità di validatori rende più difficile il controllo malevolo della rete rispetto ad un sistema centralizzato, perché gli attori dovrebbero colludere. D'altra parte, la domanda fondamentale che sorge è: perché i validatori dovrebbero comportarsi onestamente? Perché non dovrebbero colludere per controllare la rete?

Per capire ulteriormente il senso della domanda, chiediamoci: in che modo i validatori potrebbero “controllare” la rete, facendola deviare dal suo comportamento “ideale”?

Ci sono diversi modi:

- censura: i validatori, colludendo, potrebbero sistematicamente impedire ad un utente di interagire con la rete, non includendo mai le sue transazioni in un blocco. Se la rete gestisce degli asset digitali, per esempio, questo equivale a congelare gli asset dell'utente, in modo simile al blocco di un conto corrente bancario;
- interruzione del servizio: i validatori potrebbero astenersi collettivamente dal fare avanzare la rete.

Torniamo alla domanda di cui sopra: perché i validatori dovrebbero comportarsi correttamente? Le ragioni possono essere diverse, ma sono riconducibili a *interesse* e *responsabilità*.

I validatori tipicamente hanno qualche interesse a fare funzionare correttamente la rete, e sono *responsabili* della correttezza del funzionamento. La responsabilità può essere di diversi tipi: le conseguenze di un comportamento scorretto possono essere danni alla credibilità, oppure possono configurare violazioni contrattuali o addirittura comportamenti illeciti.

Le blockchain *permissioned*, in sostanza, rispetto a sistemi centralizzati, consentono di distribuire in modo trasparente la responsabilità del funzionamento di un sistema di elaborazione su un insieme di validatori. Questo tipo di sistema ha alcuni vantaggi, il principale dei quali è che è semplice da configurare e mettere in opera, una volta che si è scelto un insieme opportuno di validatori.

## Parte 2 – La tecnologia e le applicazioni

I sistemi permissioned hanno però dei limiti: sono soggetti ad attacchi derivanti da collusione, e in generale da controlli e pressioni di vario tipo, come quella istituzionale.

Alla luce di queste considerazioni possiamo inquadrare la novità introdotta da Bitcoin: un sistema distribuito in cui l'insieme dei validatori è "aperto", nel senso che chiunque può concorrere al processo di validazione. Se nel caso delle permissioned il comportamento corretto dei validatori è funzione del loro *commitment* e della loro reputazione, cosa spinge i validatori in un sistema permissionless a comportarsi correttamente? E in che modo un candidato validatore viene scelto per compilare il prossimo blocco?

L'idea fondamentale, come si è visto, è quella di utilizzare dei sistemi di incentivi e disincentivi. Sostanzialmente: a un candidato validatore viene chiesto di investire del valore per essere scelto, e il suo sforzo viene ricompensato se si comporta correttamente, altrimenti il validatore perde il valore investito. Le reti permissionless sono quindi pensate per dare ai validatori ragioni economiche per comportarsi correttamente. Esistono due meccanismi principali per far impegnare ai candidati validatori del valore: *proof of work*, e *proof of stake*.

Nel proof of work, un candidato validatore investe del valore impegnandosi nella risoluzione di un problema che ha una forma specifica per il blocco che vuole proporre. Per risolvere questo problema, deve investire sia inizialmente in hardware che, in modo variabile, in energia elettrica. Maggiore è lo sforzo che profonde, maggiore è la probabilità che venga scelto ad ogni turno come validatore. Questo meccanismo è quello attualmente usato da Bitcoin e da Ethereum. La componente di incentivo ha due dimensioni: ad ogni validatore prescelto per generare un blocco, e che porta correttamente a termine il suo compito, viene riconosciuta una ricompensa (*block reward*) sotto forma di asset nativi del sistema (Bitcoin o Ether). Inoltre, gli utenti pagano, per ogni

transazione, una *fee* al validatore che inserirà la loro transazione in un blocco. L'ammontare della *fee* è a discrezione dell'utente che crea la transazione, ma i validatori saranno più propensi ad inserire nel blocco le transazioni che pagano le commissioni più alte. Questo crea un mercato in cui il valore delle commissioni da offrire per vedere la propria transazione inserita in un blocco entro un certo tempo varia con l'utilizzo della rete da istante a istante. Si noti come il valore che viene chiesto ai validatori renda "costoso" per un attore malevolo attaccare la rete. Il costo speso dai validatori (che nei sistemi *proof of work* si chiamano anche *miner*) deve essere remunerato attraverso i *block reward* o le *fee*, altrimenti fare il validatore non è vantaggioso. È rilevante come i *block reward* siano ottenuti creando nuovi token nativi, e vengono quindi in fin dei conti pagati dai possessori di token, attraverso l'inflazione di questi.

Un inconveniente del *proof of work* è che questo richiede il consumo di ingenti quantità di energia, che tra l'altro deve essere remunerata ai validatori. Un sistema alternativo è il *proof of stake*, in cui ai candidati validatori viene chiesto di impegnare del valore (lo *stake*), che può essere sottratto (*slashed*) in caso di comportamento scorretto. Il *proof of stake*, rispetto al *proof of work*, avrebbe diversi vantaggi, tra cui: costi più bassi con gli stessi livelli di sicurezza, maggiore decentralizzazione (non è necessario acquistare hardware ad-hoc), maggiore resistenza a certi tipi di attacchi.

In generale, una differenza significativa tra reti *permissioned* e *permissionless* è che, mentre nelle prime i validatori devono avere delle motivazioni intrinseche per comportarsi correttamente, nelle seconde l'incentivo è fornito direttamente dal protocollo, ed è di tipo economico. Questo porta anche ad una diversa stabilità prospettica dei due tipi di piattaforma.

Le due categorie sono anche percepite diversamente rispetto alla "controllabilità": secondo questa intuizione, una rete *permissioned* sarebbe più controllabile perché, facendo pressioni sui validatori, definiti ed in numero ridotto, sarebbe possibile manipo-

lare alcuni aspetti del comportamento (ad esempio si potrebbe fermare la rete, oppure impedire a qualcuno di accedervi, oppure ancora si potrebbe far “riscrivere” ai validatori parte della storia). All’opposto, una rete permissionless non sarebbe in nessun modo controllabile, e le applicazioni eseguite su di essa non sarebbero assoggettabili a nessun tipo di controllo, per esempio da parte delle autorità. Questo è però un malinteso che occorre risolvere. Una piattaforma permissionless può ospitare applicazioni e asset definiti da logiche arbitrarie, tramite codice informatico. All’interno delle applicazioni è possibile definire qualsiasi tipo di ruolo e di relazione. Questo vuol dire, per esempio, che si possono definire asset/token ai quali possono essere applicati vincoli e regole arbitrari, come la possibilità di congelamento, confisca, monitoraggio, et cetera.

### 2.3 Piattaforme “istituzionali”

Come si rapportano le istituzioni rispetto alle potenzialità applicative offerte dai sistemi che offrono cryptoasset e blockchain?

Gli atteggiamenti possibili in linea di principio sono diversi: diffidenza, ostilità, *endorsement* delle piattaforme esistenti, tentativo di realizzare infrastrutture decentralizzate ma a supporto istituzionale (e.g. blockchain con molti validatori istituzionali).

Ciò che si osserva è che la percezione del valore di certe proprietà delle criptovalute sta portando sempre più gli organismi economici/monetari a prendere posizione.

Una delle posizioni diffuse più recenti è l’intenzione di valutare la possibilità di implementare forme digitali di moneta istituzionale (le cosiddette Central Bank Digital Currencies, o CBDC).

Le CBDC sono rappresentazioni digitali delle monete con corso legale, emesse e controllate dalle banche centrali, e muterebbero alcune proprietà delle criptovalute, come la semplicità

di trasferimento tra *wallet* controllati direttamente dagli utenti, senza l'intervento di intermediari.

In linea di principio, è possibile implementare CBDC anche senza utilizzare tecnologie blockchain o DLT. In effetti il dibattito sulla tecnologia da utilizzare è al momento una delle dinamiche più accese tra banche centrali e regolatori. L'opzione delle tecnologie blockchain, d'altra parte, potrebbe avere alcuni vantaggi intrinseci, come la possibilità di definire smart contract che regolano lo scambio di valore, e una maggiore trasparenza/verificabilità delle politiche monetarie.

Intorno alla possibilità di utilizzare piattaforme blockchain per monete a corso legale, e più in generale per asset che si vorrebbero soggetti a regolamentazione e al controllo delle autorità dove necessario, si sono create delle *misconception*. Una delle più frequenti è quella secondo la quale se l'infrastruttura è intrinsecamente incensurabile, o non direttamente controllabile da qualche soggetto particolare come succede per i database "classici", e a differenza per esempio di Bitcoin ed Ethereum, non è possibile definire asset che siano soggetti all'azione istituzionale (si pensi ad esempio ad un sequestro su ordine dell'autorità giudiziaria). In realtà è del tutto possibile definire, anche nel contesto delle piattaforme permissionless, tramite smart contract, degli asset con proprietà arbitrarie, tra le quali essere controllabili da soggetti definiti ed identificati, quali ad esempio una banca centrale, o un'autorità giudiziaria.

Per quanto riguarda le infrastrutture per ambiti applicativi più ampi, l'Europa sta perseguendo un approccio sistematico alla definizione di una politica rispetto a queste tecnologie.

L'EBP (European Blockchain Partnership) punta alla definizione di linee guida e di infrastrutture che possano essere utilizzate a livello comunitario dagli stati membri per applicazioni prima di pubblica amministrazione, e successivamente anche private.

In particolare, uno degli obiettivi di EBP è la definizione, implementazione e *deploy* di una infrastruttura permissioned, con

## Parte 2 – La tecnologia e le applicazioni

validatori distribuiti tra gli stati membri, chiamata European Blockchain Services Infrastructure (EBSI).

Al momento sono allo studio diversi progetti pilota, tra i quali uno dei più rilevanti e potenzialmente innovativi riguarda l'identità digitale.

Come è noto, la possibilità di utilizzare/dimostrare l'identità in ambito digitale è un fattore fondamentale nello sviluppo dell'economia e della cittadinanza.

Gli strumenti attuali, come SPID, hanno dei limiti intrinseci (elevati costi infrastrutturali, bassa flessibilità, modello economico che non incentiva l'interoperabilità, centralizzazione). Come si è visto, nell'ambito della ricerca sulle identità digitali è stato sviluppato un modello di identità, detto *self sovereign*, definito da una serie di proprietà notevoli. Una delle implementazioni di questo modello ideale è l'identità basata su *credenziali verificabili*, cioè certificati digitali che possono essere emessi da individui ed entità, che vengono firmati digitalmente, e la cui autenticità può essere verificata immediatamente e facilmente.

L'identità basata sui certificati consentirebbe di digitalizzare efficacemente tutta l'informazione utilizzata nelle relazioni tra individui, imprese, e pubblica amministrazione, abbassando sensibilmente il costo delle verifiche, e abilitando flussi di automazione impraticabili con le tecnologie correnti. All'interno di EBSI viene sviluppato lo European Self-Sovereign Identity Framework (ESSIF), una piattaforma che implementa i principi della self-sovereign identity, con l'obiettivo di raccordarsi alla regolamentazione europea sull'identità digitale (eIDAS).

Una delle possibilità fondamentali offerte dalle blockchain, difatti, è la registrazione, immutabile, databile e facilmente dimostrabile, di informazioni di varia natura. All'interno di EBSI, un altro use case è una piattaforma per la notarizzazione di documenti come contratti, fatture, liste di presenza, etc.

## 2.4 Applicazioni alla supply chain

Uno dei settori potenzialmente suscettibili di applicazione/che sta ricevendo maggiore attenzione è la supply chain. Le supply chain sono sistemi complessi nei quali molti attori, con interessi potenzialmente contrastanti, si coordinano (cercano di coordinare) per il perseguimento di obiettivi industriali e commerciali differenti. In generale, la digitalizzazione può offrire vantaggi rispetto allo status quo in termini di efficienza e capacità di progettare/attuare processi di coordinamento. Qual è però il contributo specifico che può essere offerto dalle tecnologie blockchain e DLT?

Spesso, rispetto a questo ambito, i vantaggi della blockchain vengono prospettati con una certa leggerezza e improprietà (per esempio quando si dice sommariamente che una blockchain può “garantire la provenienza”).

In generale, ricordiamo che la blockchain offre la possibilità di implementare un’infrastruttura che consente di “eseguire” logiche in modo garantito, distribuendo la responsabilità su un insieme arbitrario di attori. Questa possibilità può essere sfruttata, come si è visto, per creare delle meccaniche che garantiscano gli attori in modo credibile ed efficiente in un’ampia gamma di interazioni.

Lo European Parliamentary Research Service ha condotto uno studio e redatto un rapporto nel quale esamina le potenzialità della blockchain in ambito supply chain ([https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641544/EPRS\\_STU\(2020\)641544\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641544/EPRS_STU(2020)641544_EN.pdf)).

Gli ambiti considerati sono:

- le transazioni commerciali;
- il finanziamento del commercio;
- il sistema di lettere di credito;
- il commercio in *open account*;
- i pagamenti cross-border;
- gli adempimenti amministrativi e doganali;

## Parte 2 – La tecnologia e le applicazioni

- la logistica;
- il monitoraggio e la tracciabilità (e la garanzia di provenienza).

Consideriamo i problemi e i possibili vantaggi che le blockchain possono offrire in questi ambiti.

Nelle transazioni commerciali, l'opportunità principale è quella di “decentralizzare” i mercati digitali, connettendo più o meno direttamente domanda ed offerta, in modo *peer-to-peer*. L'eliminazione degli intermediari consentirebbe una maggiore flessibilità e un risparmio sulle commissioni. La compliance con sistemi diversi nei rapporti cross-border può essere perseguita anche attraverso l'automazione possibile grazie agli *smart-contract*.

Nella digitalizzazione di contratti commerciali, uno dei potenziali vantaggi deriverebbe non solo dalla facilità di archiviazione o dalla maggiore facilità di accesso, ma anche dalla possibilità di “automatizzarne” l'esecuzione di alcuni aspetti in modo credibile. Per esempio, è possibile definire meccanismi di *escrow* nei quali un pagamento è automaticamente eseguito al verificarsi di certe condizioni. Tipicamente le modalità di verifica delle condizioni coinvolgono il consenso di più attori (ad esempio, un trasporto è stato perfezionato e gli obblighi doganali assolti). Questi strumenti possono automatizzare efficacemente il rapporto tra importatori, esportatori, assicurazioni, dogane, istituti di credito, etc. Tra i potenziali vantaggi dell'utilizzo di smart contract ci sono sicuramente la maggiore efficienza, dovuta all'accessibilità immediata e condivisa delle informazioni, e la possibilità di definire garanzie più credibili e strutturate, senza perdere in efficienza. Uno degli esempi di queste applicazioni è TradeLens (<https://www.tradelens.com/>).

La digitalizzazione e distribuzione del sistema di garanzia del credito tramite blockchain consentirebbe di velocizzare significativamente lo scambio di documenti e il controllo da parte di tutti gli attori della correttezza del processo. Inoltre, consentirebbe l'interoperabilità con altre dimensioni (per esempio l'emissione

di credito condizionato al verificarsi di certe condizioni del trasporto, o dei magazzini). Uno degli ostacoli nell'attuazione di questi progetti è il raccordo con le differenti norme che regolano, ad esempio, il riconoscimento legale delle lettere di credito.

Quello dei pagamenti internazionali è il caso d'uso originario dei sistemi blockchain, e i benefici sarebbero evidenti: minori costi di transazione, maggiore velocità, possibilità di automazione dei pagamenti nel contesto di condizioni predeterminate. È da notare come nel 2020 tutte le maggiori istituzioni monetarie internazionali abbiano cominciato a valutare lo sviluppo, e in alcuni casi anche a sperimentare l'utilizzo, di valute digitali che, anche quando non utilizzano delle blockchain come infrastruttura abilitante, mutuano alcune delle caratteristiche interessanti delle criptovalute, tra le quali la potenziale disintermediazione con il sistema bancario e la semplificazione delle transazioni.

Rispetto agli adempimenti amministrativi e doganali, l'opportunità è di aumentare il coordinamento e ridurre il tempo e il costo dell'espletamento, per esempio consentendo alle autorità doganali di accedere in modo controllato, garantito e trasparente alle informazioni necessarie direttamente alla fonte. Un'altra possibilità è l'automazione del pagamento dei dazi doganali. Queste soluzioni richiedono ovviamente il coordinamento di attori sia privati che istituzionali, cosa che a sua volta richiede il riconoscimento delle tecnologie da parte dei governi nazionali.

Un altro ambito di applicazione è lo scambio di informazioni tra agenzie pubbliche, come certificati sanitari, certificati di origine, licenze di import-export. Ad esempio, uno smart contract potrebbe richiedere, prima dell'inizio del trasporto di export, la comunicazione di un certificato fitosanitario da parte di un'agenzia del paese esportatore, e la dogana ricevente verrebbe avvisata in tempo reale del nullaosta.

Lo stesso principio potrebbe essere applicato alla comunicazione tra altre agenzie governative come le camere di commercio e agenzie di regolazione.

## Parte 2 – La tecnologia e le applicazioni

Nel campo della logistica, le possibili applicazioni riguardano la possibilità di raccogliere in modo più puntuale, diffuso e credibile le informazioni riguardanti la movimentazione delle merci, e di renderle disponibili in modo selettivo agli attori della filiera. Rispetto alle tecnologie digitali più “classiche”, i registri distribuiti consentono di coinvolgere gli attori in modo più semplice e meno problematico nella raccolta, elaborazione e utilizzo dei dati, poiché la gestione non è in carico ad un solo attore, ma è distribuita su tutti i soggetti coinvolti e interessati. Inoltre, i dati raccolti possono essere utilizzati per generare automatismi garantiti e trasparenti tramite smart contract.

La possibilità di coinvolgere attori della filiera in modo più efficiente ed ampio nella raccolta, condivisione selettiva e gestione dei dati, apre a sua volta diverse possibilità, anche nel campo della tracciabilità e delle garanzie di provenienza.

Normalmente la tracciabilità viene ottenuta associando degli identificatori univoci ai beni tracciati. Ottenere identificativi non falsificabili non è semplice né economico.

Uno degli approcci possibili è rilevare la posizione dei beni durante le fasi del trasporto, impedendo che un identificativo copiato venga utilizzato in due posizioni “incompatibili”.

Il problema che si presenta anche in questo caso riguarda chi debba gestire, e come, le informazioni sulla posizione dei beni. Come si è già visto, la distribuzione della responsabilità dei dati offerta dai sistemi a registro distribuito può offrire vantaggi fondamentali. Un'altra possibilità interessante è la definizione di politiche automatiche di redistribuzione del valore generato dalla tracciabilità. Per esempio, se un bene è stato correttamente tracciato, al momento della vendita si potrebbe riconoscere tramite uno smart contract una frazione del valore agli attori della supply chain che hanno contribuito al tracciamento.

Oltre ad abilitare meccanismi di tracciamento più efficienti ed efficaci, la raccolta dati tramite registri distribuiti consente più facilmente di dimostrare all'esterno (ad un ente regolatore, ad un

consumatore) proprietà e circostanze del processo di produzione e distribuzione di un determinato prodotto. Questo perché, oltre ad agevolare la raccolta dati, le transazioni di interazione con gli smart contract, registrate in modo non modificabile tramite logiche convenute, possono certificare le modalità con le quali i dati sono stati raccolti, attraverso prove facilmente verificabili.

Per riassumere, alcune tra le potenziali applicazioni dei sistemi blockchain e distributed ledger nelle supply chain riguardano:

- l'automazione di processi, dove sia problematico assegnare/delegare l'esecuzione delle logiche a singoli attori;
- la "notarizzazione" delle informazioni rilevanti ai fini della tracciabilità e della garanzia di processo e origine;
- la creazione di sistemi di incentivi che allineino gli attori verso comportamenti complessivamente vantaggiosi (e.g. raccolta di dati di qualità per la tracciabilità), anche attraverso logiche di redistribuzione dei vantaggi lungo la filiera.







## → Gestire l'integrazione delle fonti di dati negli studi clinici

*Dompé è un'azienda biofarmaceutica innovation-driven caratterizzata dall'impegno in ricerca e sviluppo per soddisfare esigenze terapeutiche fino ad ora insoddisfatte. Il progetto blockchain-based (D-chain) di integrazione tra eCRF (Electronic Case Report Forms) e software esterni è nato in maniera naturale dalla collaborazione interna tra il dipartimento di Open Innovation e quello di IT. "CRF" è l'acronimo di "Case Report Form": un modulo utilizzato per acquisire dati negli studi clinici sui dispositivi medici e farmaceutici.*

*Perché ci serviva la tecnologia blockchain? Sul mercato esistevano già soluzioni per l'integrazione delle varie fonti che alimentano il processo di gestione di eCRF, ma nessuno unisce i vantaggi di un sistema integrato tradizionale (dematerializzazione, aumento sicurezza, efficienza e velocità del processo) a quelli dei sistemi blockchain-based come la scalabilità a infrastrutture e software esistenti, la modularità, l'efficientamento nell'uso di software integrati, l'inalterabilità e la sicurezza dei dati. Un elemento centrale del progetto è il coinvolgimento degli Enti regolatori per aprire la strada allo sviluppo di standard utili per tutti gli stakeholder di queste nuove tecnologie. I principali sistemi e fonti dati che verranno integrati saranno i diari dei pazienti, i dati di laboratorio, le cartelle cliniche elettroniche, eTMF (Electronic Trial Master File) fino alla possibilità di integrare devices IoT per il monitoraggio dei pazienti. Il progetto verterà su più fasi: analisi delle sorgenti, standardizzazione e armonizzazione dati, design delle regole di comunicazione fra sistemi e privacy, design Smart Contracts per autorizzazione al trasferimento dati, integrazione eCRF con piattaforme esterne.*

*(Cristiano Crippa, ICT Corporate Manager Dompé, e Marco Mazzola, Research and Innovation Manager Dompé)*

### → Tracciabilità nel calzaturiero

*Tacchificio Villa Cortese (TVC) è una realtà storica e siamo partner delle più prestigiose griffe della moda internazionale nello sviluppo di tacchi per calzature di lusso.*

*Grazie alla collaborazione con MyChicJungle all'interno di un ampio processo di open innovation e di R&D, intendiamo avvalerci della tecnologia blockchain per migliorare i processi aziendali e, allo stesso tempo, guadagnare nuovi asset da sfruttare sia per certificare la qualità Made in Italy dei nostri prodotti e della nostra filiera, sia come messaggio da comunicare verso i nostri clienti business, così come verso il consumatore finale.*

*Recentemente, abbiamo avviato un test di “catalogo B2B online” accessibile via desktop e mobile in cui vengono mostrate diverse caratteristiche uniche dei nostri prodotti: analisi per la scelta dei materiali, dati di laboratorio, simulazioni meccaniche e di resistenza. Tutti questi dati provengono da fonti documentali, autoprodotte oppure certificate da terzi. Abbiamo anche adottato macchinari “4.0”, in grado di produrre dati diagnostici durante il processo produttivo. In questo scenario, la tecnologia blockchain sarà introdotta a diversi livelli, diventando parte integrante dei processi aziendali legati alla certificazione della qualità e sostenibilità del prodotto.*

*Crediamo che l'implementazione di questa tecnologia possa essere un valore aggiunto trasversale sia guardando all'interno della nostra organizzazione, al prodotto, ai processi produttivi, ai processi di Ricerca e Sviluppo, sia guardando verso l'esterno, alle aree tecniche di industrializzazione e produzione delle case di alta moda nonché al cliente utilizzatore finale.*

*La blockchain sarà dunque lo strumento attraverso il quale avremo la possibilità di tracciare e certificare verti-*

*calità tecniche del prodotto come le performances meccaniche e l'impatto ambientale del prodotto stesso, ma anche uno strumento di comunicazione per arrivare all'utilizzatore della calzatura che avrà la possibilità di vedere certificato il valore aggiunto di un prodotto di alta moda rigorosamente prodotto in Italia.*

*Grazie alla partnership strutturale con MyChicJungle lavoreremo congiuntamente all'ambizioso scopo di "allungare la catena", promuovendo ed allargando i vantaggi dell'implementazione di questa tecnologia nei processi produttivi della filiera calzaturiera al fine di tracciare e certificare non solo le caratteristiche verticali ai prodotti, ma tutto l'ingegno, la qualità, il know-how che fanno del settore calzaturiero uno dei migliori baluardi del Made in Italy nel mondo.*

*(Alessandro Paganini, Coe TVC Group)*

### → Tracciabilità nell'alimentare

*Brusa è un'azienda del biellese a conduzione familiare, attiva sin dal 1974 nella produzione di prodotti da forno. Impegnata in un percorso di sostenibilità e tracciabilità della sua produzione a tutela dei consumatori e delle filiere di produzione italiane e regionali, recentemente si è dedicata all'integrazione tecnologica della blockchain per portare amercato il primo prodotto in Europa tracciato end-to-end dal seme allo scaffale su blockchain pubblica. Attraverso la piattaforma autoconfigurante Propagate® sviluppata dalla Spartan Tech, Brusa ha implementato un tracking passivo (senza, cioè, alterare in alcun modo l'operatività della filiera) di ogni step della produzione e della distribuzione coinvolgendo tutti gli attori della propria supply chain: consorzio agricolo, mulino, logistica, impianto di produzione proprio e distribuzione GDO. Stampando sulla confezione un piccolo QR code, Brusa ha poi reso disponibile al consumatore finale la possibilità di visualizzare dal proprio smartphone l'intera filiera e verificare l'hash per ogni step significativo della stessa come prova certa ed immutabile di quanto avvenuto.*

*“Come Spartan Tech la nostra missione è rendere democratiche, quindi estremamente intuitive ed economiche, tecnologie esponenziali che troppo spesso arrivano in declinazioni accessibili per PMI e professionisti nel nostro paese con anni di ritardo rispetto al mercato internazionale, penalizzando la competitività del paese nel mondo.”*

*(Pietro Gorgazzini, co-founder Spartan Tech)*

*“Il nostro motto, ‘La qualità è coscienza’ sintetizza la visione del suo fondatore Secondino Brusa, una visione sabauda, con influssi Olivettiani, per il quale è sempre stato imprescindibile il legame sociale ed economico con il suo*

*territorio. Consumatori, collaboratori e aziende, sono soggetti tutti collegati da strette relazioni fiduciarie. Crediamo che la notarizzazione dei dati aumenti la trasparenza, la quale promuove un aumento della Coscienza, al fine di raggiungere una sempre maggiore Qualità sociale, ambientale, di prodotto, che sia etica e percepita.”*

(Massimo Brusa, Ceo Brusa)

### → Tracciabilità nei dispositivi medici

*L'emergenza determinata dal Covid-19 ha messo sotto pressione il mercato dei dispositivi medici, evidenziando limiti e vulnerabilità di filiere globali caratterizzate da produzione delocalizzata e da forte dipendenza nell'approvvigionamento da specifici mercati. Nel segmento dei dispositivi di protezione individuale, la crescita esponenziale della domanda ha generato tensione sui prezzi, favorendo l'immissione sul mercato di prodotti substandard corredati di certificazioni contraffatte. Ciò ha portato le stazioni appaltanti ad incrementare i livelli di controllo sulle catene di forniture, ottenendo tuttavia risultati spesso dubbi o insoddisfacenti e rivelando importanti falle nei meccanismi di controllo.*

*In questo contesto, DNV GL, ente indipendente che fornisce servizi di assurance a livello globale, ha sviluppato un progetto integrato di Trasparenza, Tracciabilità e Controllo della Catena di Fornitura basato sulla tecnologia Blockchain per supportare Giuntini S.p.A nella produzione di mascherine chirurgiche, realizzate in Italia. Il progetto è stato sviluppato combinando tecniche di ispezione e audit in campo ad una soluzione di tracciabilità digitale e monitoraggio continuo sviluppata con la piattaforma Blockchain VeChain, al fine di garantire l'integrità e l'immutabilità delle informazioni e dei dati raccolti lungo l'intera filiera, agevolandone al tempo stesso la verifica. DNV GL ha proposto a Giuntini un piano di controllo e monitoraggio della produzione identificando dati e momenti critici del processo di assemblaggio (lotti materie prime, location del sito produttivo, turni di produzione, date di movimentazione, risultati dei test, esiti dei controlli, azioni correttive). Le informazioni chiave e l'esito dei controlli lungo l'intera catena del valore sono stati*

*associati ai lotti di prodotto finito ed inseriti in VeChain fornendo immutabilità, trasparenza e verificabilità a tutti gli stakeholder coinvolti.*

*La soluzione proposta consente in ogni momento di associare ad uno specifico lotto di produzione tutte le informazioni critiche relative all'intera filiera, fornendo al tempo stesso evidenza delle verifiche e riducendo drasticamente e sostanzialmente il rischio di contraffazione a garanzia della sicurezza del prodotto.*

(Renato Grottola, Global Director Growth and Innovation, DNV GL)

### → Tracciabilità delle filiere industriali in Abruzzo

*Con l'obiettivo programmatico di favorire l'internazionalizzazione delle imprese del territorio, supportando la tutela del Made in Italy e la valorizzazione dei prodotti tipici, con particolare focus sul design e food&wine che tanta parte del PIL regionale costituiscono, abbiamo scelto di creare la Piattaforma "ABC AbruzzoBlockChain Tutela Certifica Promuovi Espandi" aperta a tutte le aziende del territorio delle province di Chieti e Pescara. Progetto nato grazie alle competenze messe a rete da Confindustria Chieti Pescara, con la compartecipazione della Camera di Commercio Chieti Pescara e del suo PID-Punto Impresa Digitale.*

*Nel concreto: siamo partiti da una condivisione dei vantaggi potenziali della Blockchain con alcune aziende eccellenti del territorio, settori tessile, design, trasformazione alimentare, enogastronomia. Sono stati identificati i building blocks fondamentali per l'avvio di un pilota Blockchain basato su piattaforma che implementa un sottoinsieme di caratteristiche. In tal modo si genera un sistema a fiducia incrementata che permette l'aggiunta di common knowledge sugli eventi notevoli delle filiere che avvengono tra più attori con interessi ed obiettivi potenzialmente contrastanti, al fine di abilitare controlli diffusi, ridurre i contenziosi e semplificare i passaggi di responsabilità anche nella presa in carico e nell'arricchimento progressivo dei dati.*

*Le principali motivazioni di adesione alla piattaforma? La certificazione di origine, dell'avanzamento ordine, delle fasi di lavorazione espletate in-house (certificato di proprietà), la possibilità di smart-payment, l'accreditamento committenze, la tracciabilità dei lotti, la messa a sistema di entità nella stessa filiera che non hanno rapporti diretti tra loro, l'allineamento con clienti già orientati alla blockchain (grandi catene di distribuzione).*

*Le aziende che aderiranno alla piattaforma non dovranno sostenere i costi di set up e potranno fare leva su tutte le funzionalità già predisposte grazie al contributo di CCIAA Chieti Pescara; è prevista solamente una minima quota di servizio. Già registriamo le prime adesioni alla piattaforma e si prevede di estendere l'utilizzo fino a 50-100 aziende nell'arco di tre anni.*

*La nostra più grande soddisfazione è di aver toccato il business di alcune PMI locali aprendo loro una strada difficile da percorrere in solitaria, abbiamo poi unito una nostra tipica concretezza che ha condotto il progetto velocemente nella attuale fase di execution.*

(Silvano Pagliuca, Presidente Confindustria Chieti Pescara)

### → Tracciabilità nello smaltimento dei rifiuti

*Sodai è una società di ingegneria ambientale e water management che opera nel settore della depurazione e del trattamento delle acque primarie e fluidi di processo per l'industria. Un'azienda che, per la sua attitudine alla trasparenza, alla sostenibilità e alla tutela del territorio, ha deciso di dare il via al complesso percorso di tracciabilità della filiera dei rifiuti attraverso l'integrazione della tecnologia blockchain. L'obiettivo è incrementare l'attenzione alle tematiche green e all'economia circolare e riuscire ad affermare con sicurezza la legalità nel processo, creando un paradigma che possa diventare di ispirazione e riferimento all'interno del settore. L'ambizione e la determinazione hanno permesso a Sodai di portare a mercato la prima soluzione end-to-end di tracciabilità di smaltimento rifiuti in Italia. Attraverso il supporto di Spartan Tech, Sodai ha implementato un tracking passivo (senza alterare l'operatività della filiera) di ogni step di gestione del ciclo rifiuti provenienti dal trattamento acque coinvolgendo tutti gli attori della propria supply chain: impianto, logistica, smaltitore. Dal gestionale Sodai è possibile risalire in modo semplice e immediato alle informazioni relative ad ogni ciclo di trattamento. Dati che, grazie alla notorizzazione su blockchain, evidenziano in modo preciso le attività svolte da ogni attore della filiera.*

*I vantaggi sono molteplici: una maggior tutela per gli attori coinvolti nel processo, grazie ad una chiara definizione delle attività svolte lungo la filiera; una maggior efficienza gestionale amministrativa grazie alla digitalizzazione del processo; l'incremento del livello di trasparenza verso l'esterno; una maggior facilità di interazione con enti di controllo; un'accelerazione del processo di circolarità.*

*“Riteniamo che la blockchain rappresenti un’opportunità per garantire certezza e trasparenza in un comparto caratterizzato da notevoli incertezze sia a livello interpretativo che gestionale. Per questo abbiamo scelto di fare un passo avanti, così da differenziarci dai nostri competitor, e dare trasparenza ed evidenza a tutte le fasi del processo, dalla raccolta, al trasporto fino all’impianto di trattamento. L’iniziativa ha raccolto grande interesse da parte dei nostri clienti, permettendoci di rafforzare il rapporto di collaborazione e iniziare a pianificare ulteriori sinergie congiunte. Notiamo che c’è crescente sensibilità rispetto ai temi dell’economia circolare e della sostenibilità, per questo abbiamo a diventare un punto di riferimento in Italia su tali tematiche.”*

(Marzia Chiesa, CEO Sodai)

### → Incentivare la sostenibilità

*La principale e potenziale caratteristica offerta da blockchain è quella di ridurre il costo della fiducia necessario al perfezionamento di una transazione, intesa come scambio informativo o di valore, garantendo al tempo stesso certezza della sua esecuzione.*

*La tecnologia si presta quindi, ad essere lo strumento ideale che abilita il passaggio da un'economia lineare ad un'economia circolare e premia i comportamenti sostenibili.*

*“San Marino Low carbon ecosystem” è il nome del progetto che prevede la creazione di un ecosistema in grado di promuovere l'adozione di comportamenti virtuosi da parte dei cittadini, finalizzati alla riduzione delle emissioni di CO2 e successivamente, all'implementazione di modelli di economia circolare. La piattaforma incentiva, infatti, pratiche virtuose e sostenibili come il risparmio idrico, la raccolta differenziata e la gestione dei rifiuti, premiando i cittadini tramite un Token di Utilizzo, che potrà essere utilizzato per usufruire di prodotti all'interno dell'ecosistema stesso.*

*Il cittadino torna al centro, sarà incentivato a seguire comportamenti virtuosi che potrà misurare e valorizzare visualizzandoli in tempo reale nel suo portafoglio digitale (wallet); la riduzione di CO2, derivante dall'adozione di un comportamento orientato alla sostenibilità, sarà calcolato da un opportuno algoritmo e premiato tramite il Carbon Credit.*

*L'introduzione dell'ecosistema low carbon rappresenta il primo esempio, a livello globale, di incentivazione attraverso l'utilizzo della blockchain e di un token di utilità.*

*La Repubblica di San Marino ha deciso con questa iniziativa di impegnarsi a raggiungere uno degli obiettivi di sviluppo sostenibile dell'Onu, diventando il primo paese ad emissioni zero entro il 2030.*

*Coniugare innovazione e circolarità è possibile. Significa, individuare soluzioni per ridurre gli sprechi, rigenerare i prodotti, ripensare i materiali, coinvolgendo l'intero modello di business in una trasformazione tecnologica e sociale. Significa, soprattutto, lavorare alla costruzione di una forte visione comune, che parta dai governi e arrivi alle aziende, ai cittadini, ai turisti.*

*Blockchain, grazie alle sue caratteristiche e alla tokenizzazione, consente la creazione di ecosistemi virtuosi, permette di creare opportunità di crescita e di nuovi modelli di business per le aziende in cui scienza e coscienza si sostengono l'un l'altra.*

(Sara Noggler, Relazioni Istituzionali San Marino Innovation)

### → Abilitare le comunità energetiche

*La Blockchain e, più in generale, i Distributed Ledger sono una delle innovazioni più rivoluzionarie in ambito Energy. Queste tecnologie sono destinate a ripensare le tradizionali dinamiche di produzione e vendita di energia, e, parallelamente a ciò, cambiare le abitudini dei consumatori, che già oggi chiedono alle Utility nuovi servizi e funzionalità.*

*Il nostro obiettivo è stato fin dall'inizio quello di realizzare una piattaforma per gestire gli scambi energetici tra prosumer, soggetti che in modo decentralizzato consumano e producono energia (prevalentemente da impianti fotovoltaici) nello stesso momento. I partecipanti alla comunità possono scambiare energia l'uno con l'altro e godere della produzione da impianti rinnovabili condivisi, con l'obiettivo di massimizzare l'autoconsumo, abbattendo così il costo della bolletta energetica.*

*La necessità ed il forte interesse per la tematica sono testimoniati ad esempio dal decreto emesso dal Ministero per lo Sviluppo Economico: grazie ad importanti incentivi a favore dell'autoconsumo nelle comunità energetiche, prevediamo che a breve nascerà un ampio numero di realtà caratterizzate dalla condivisione di asset di produzione da fonte rinnovabile.*

*Prosume sta collaborando con alcuni partner per affrontare questo nascente mercato, mettendo a disposizione la tecnologia blockchain per "notarizzare" e certificare tutte le informazioni prelevate da strumenti di misura installati all'uopo. Inoltre, attraverso smart contract è possibile cablare nella blockchain anche le logiche di calcolo per le procedure di settlement, finalizzate a contabilizzare in maniera corretta le posizioni economiche dei singoli membri delle comunità.*

*La blockchain si pone quindi come la tecnologia più adatta per garantire certezza, trasparenza ed immutabilità dei dati a tutti gli stakeholder coinvolti nelle comunità stesse, evitando discussioni su quanto avvenuto in campo e quanto ricalcolato per applicare le regole di riparto delle singole comunità. In definitiva, è la tecnologia che, forse più di tutte, potrebbe conciliare la creazione di nuovi servizi per gli utenti ed il cambiamento del mercato dell'energia.*

(Mattia De Vecchi, CEO Prosume)

### → **Notarizzare i contratti e gli scambi documentali**

*Flowdron è il più grande marketplace per dronisti e utenti, il cui obiettivo è di facilitare l'incontro tra dronista e utilizzatore del servizio. Flowdron ha deciso di continuare a potenziare le proprie funzionalità utilizzando la blockchain per certificare l'accordo tra dronista e cliente via blockchain, grazie all'accordo con l'Innovation Hub MyChicJungle. Tramite la blockchain sarà infatti possibile notarizzare tutti i documenti connessi ad una prestazione, garantendone così contenuto, data di emissione e parti coinvolte in maniera pubblica, immutabile e trasparente. Nell'ambito della comunicazione, del valore e della qualità di determinate tipologie di prodotti consumer, l'uso di documenti notarizzati su blockchain infatti permette di raccontare la storia dei propri prodotti in una nuova maniera, incentivando la trasparenza verso i consumatori e la comunicazione delle qualità dei propri prodotti grazie all'apertura verso il pubblico delle aziende. Analogamente, notarizzare un contratto su blockchain permette di "congelare" nel tempo il contenuto di quel contratto stesso, e di conseguenza facilitare la risoluzione di eventuali controversie che potrebbero sorgere.*

*"Credo fortemente nella blockchain che consente di gestire e aggiornare, in modo univoco e sicuro, un registro contenente dati e informazioni in maniera aperta, condivisa e distribuita senza la necessità di un'entità centrale di controllo e verifica."*

(Rudy Lazzarin, Founder Flowdron)

*"Come MyChicJungle il nostro intento è quello di implementare all'interno delle imprese un'innovazione personalizzata, efficiente e facilmente accessibile, pertanto nel tempo abbiamo creato applicazioni e software plug*

*and play integrati con tecnologia blockchain in grado di creare nuovi orizzonti di sviluppo per business operanti in diversi settori.”*

(Jacopo Moschini, Ceo MyChicJungle)

→ **Facilitare i rapporti notaio-cliente**

*Tra notaio e cliente, prima dell'avvio delle operazioni effettive inerenti all'atto, vengono sottoscritti alcuni documenti: preventivo, lettera di incarico, informativa privacy, ecc.*

*Questi documenti sono cartacei, firmati in originale e conservati negli archivi del notaio, con problemi di occupazione spazi fisici e lungaggini nella eventuale ricerca a posteriori.*

*Per facilitare il rapporto tra notaio e cliente, obbligati al distanziamento fisico in epoca di Covid, abbiamo realizzato CRM Notarile: una piattaforma cloud per la predisposizione e sottoscrizione digitale dei documenti citati e la contestuale conservazione con la tecnologia blockchain in rete Ethereum.*

*Conseguentemente le operazioni preparatorie all'atto vero e proprio sono svolte tra notaio e cliente in maniera digitale e telematica.*

*E mediante la soluzione Timesafe, i documenti sono salvati in rete Ethereum nel momento stesso della loro sottoscrizione dalle parti, con produzione immediata di un certificato di salvataggio in blockchain a disposizione del notaio e del cliente.*

*(Vasco Ciresola, Amministratore unico Zucchetti Software Giuridico)*

### **→ Gestire l'identità degli oggetti connessi nella gestione di flotte**

*Il tema dell'IoT genera la necessità di rispondere al grande tema della certezza dell'identità degli oggetti connessi. L'identità è fondamentale per ogni altra attività. La gestione corretta dell'identità degli oggetti costituisce un fondamento indispensabile per abilitare tutte le operazioni successive comprese le transazioni di valore economico.*

*L'IoT è in generale "trasferimento di dati" e tipicamente il trasferimento di informazioni verso il Cloud per creare per esempio, il Digital twin di un sistema fisico. Il punto chiave è nella creazione di un livello di fiducia tra le parti, nello specifico, tra chi crea l'infrastruttura che fornisce questi dati dal campo e coloro che ricevono queste informazioni per fare business ed eventualmente pagano per disporre di queste informazioni. Il tema è così critico che la maggior parte delle aziende che hanno digitalizzato il proprio business, attraverso l'IoT e i Digital twin, sono state costrette a possedere ed a installare e gestire la propria infrastruttura e i dispositivi sul campo per avere la certezza delle informazioni.*

*La fiducia è poi il presupposto fondamentale per le transazioni economiche e naturalmente per servizi a pagamento. Mentre le persone si affidano ad autorità terze e ai documenti da esse rilasciate per garantire l'identità e instaurare la fiducia, per le macchine, i sistemi e gli oggetti connessi non esiste una analoga autorità che possa creare un sistema fiduciario tra di essi. Uno dei punti chiave dell'IoT è come risolvere questo problema per abilitare lo scambio di informazioni e le transazioni di valore economico tra oggetti. La blockchain è una soluzione a questo problema.*

*La gestione del traffico aereo dei droni, che sono di fatto dispositivi IoT, è un caso specifico: Leonardo, nell'ambito*

*delle attività del consorzio D-Flight, impegnato nello sviluppo ed erogazione di servizi di gestione del traffico aereo degli UAV, ha realizzato sfruttando la soluzione della startup UniquiD un sistema prototipale basato sulla tecnologia Blockchain per gestire il traffico urbano di mezzi aerei di piccole dimensioni, di fatto dei dispositivi IoT volanti, in modo più rapido e sicuro.*

*L'applicazione della Blockchain al contesto dell'Unmanned Traffic Management, consentirà il diretto riconoscimento tra operatore, drone e piattaforma, in modo sicuro e certificato. In futuro, sarà possibile registrare, validare e autorizzare piani e missioni di volo, offrire servizi di billing e gestire le comunicazioni fra una moltitudine di UAV garantendo maggiore tracciabilità delle informazioni, sicurezza e privacy.*

*UTM e Blockchain, un binomio perfetto.*

*(Giuseppe Cardinale Ciccotti, CEO UniquiD Italia)*

## **→ Semplificare l'onboarding dei clienti e il processo di Know Your Customer**

*Come Intesa (Gruppo IBM) in collaborazione con CETIF e CherryChain, abbiamo avviato un progetto nazionale per gestire l'onboarding e il processo di Know Your Customer su tecnologia DLT/blockchain.*

*A giugno 2020 è stata avviata la sperimentazione di sistema, in collaborazione con le Authority, che ha coinvolto banche, compagnie di assicurazione, pubbliche amministrazioni e imprese del settore delle telecomunicazioni, GDO, energy, utility e altre. L'obiettivo della sperimentazione è quello di semplificare il processo di Onboarding per il cliente e contemporaneamente efficientare e migliorare il processo di Know Your Customer.*

*L'obiettivo principale è quello di semplificare, ridurre i tempi e i costi del processo di onboarding al fine di generare efficienza nei processi interni delle aziende coinvolte. L'iniziativa mira, infatti, alla condivisione delle informazioni necessarie ai processi di O-KYC tra i partecipanti all'ecosistema attraverso la creazione di un wallet che permetta al cliente di autorizzare il trasferimento delle proprie informazioni dal Custodian al Richiedente. Il tutto in linea con il regolamento GDPR sulla gestione dei dati, garantendo così la sicurezza dell'intero processo, un pieno controllo all'utente finale dei propri dati e una possibile remunerazione sotto forma di "token" spendibili all'interno dell'ecosistema.*

*L'iniziativa O-KYC nasce dall'esigenza, manifestata da tutti i player di sistema, di ridurre costi, tempi e complessità che incidono in modo rilevante sull'operatività di questi processi. La soluzione O-KYC è sviluppata all'interno di un percorso di sperimentazione su dati reali definito "Sandbox" già sperimentato in passato con successo. Il progetto*

## Parte 2 – La tecnologia e le applicazioni

*è supervisionato da uno Stakeholder Committee composto dagli aderenti all'iniziativa.*

*Siamo alla guida dell'iniziativa insieme a CeTIF Advisory e ci siamo occupati del coordinamento e dello sviluppo del progetto, nonché dell'adozione di un approccio di Compliance by Design. Il progetto conta sulle capacità di sviluppo ed integrazione applicativa di CherryChain, startup Fintech e sulla tecnologia blockchain in IBM cloud nell'ambito del programma Startup with IBM.*

*(Pietro Lanza, General Manager di Intesa e Blockchain Director di IBM Italia)*

### **→ Dare trasparenza alla gestione di finanziamenti e donazioni**

*Il progetto “Microcredito 2.0 per le popolazioni più vulnerabili”, progettato dal Politecnico di Milano, realizzato da KNOBS, e promosso da Helpcode Italia Onlus in collaborazione con Fondazione Cariplo, si focalizza sull'introduzione dell'innovazione tecnologica all'interno dei processi di finanziamento e donazione. Grazie all'utilizzo della tecnologia blockchain, il progetto consente di effettuare transazioni (anche internazionali) veloci, economiche ed eventualmente anonime, garantendo allo stesso tempo la trasparenza, la certificazione e la tracciabilità di tutti i trasferimenti (es: finanziamenti, donazioni, bonus, agevolazioni, ecc.) effettuati dagli utenti.*

*All'interno del sistema vengono utilizzati degli Smart Contract, ovvero dei contratti digitali operanti su blockchain, che consentono di gestire l'emissione di token (gettoni digitali che possono rappresentare asset fisici o virtuali, compreso il denaro) a fronte di donazioni/finanziamenti, ed il loro trasferimento tra utenti. In particolare, il progetto si è posto come obiettivo la realizzazione di un sistema prototipale per la gestione trasparente, certificabile e tracciabile delle donazioni. Utenti privati o istituzionali possono dunque sfruttare le potenzialità della tecnologia blockchain utilizzando una semplice ed intuitiva applicazione web che permette loro di effettuare donazioni verso Helpcode o direttamente verso i progetti supportati dalla Onlus stessa. Le donazioni vengono quindi convertite automaticamente in asset digitali (o token) che possono essere utilizzati dai destinatari della donazione per gli scopi definiti da Helpcode, garantendo al tempo stesso ai donatori visibilità sull'utilizzo dei fondi e la loro tracciabilità in tempo reale.*

*In particolare, il sistema prototipale implementato prevede la donazione di token a bambini, che potranno utilizzarli per sostenere la propria educazione, acquistando materiale scolastico o donando i token a degli alunni più grandi per poter ricevere in cambio un supporto allo studio, ovvero un mentoring scolastico. Gli studenti più grandi che hanno prestato il proprio servizio di mentoring, guadagnando a loro volta token, potranno utilizzarli per acquistare altri servizi, come ad esempio l'accesso all'istruzione universitaria. Le autorità che forniscono il servizio ricevendo pagamenti in token, come le università ad esempio, potranno richiedere all'organizzazione non-profit il rimborso in denaro corrispondente alla somma di token ricevuta dagli alunni, chiudendo in questo modo il cerchio di un'economia virtuosa e circolare.*

(Francesco Bruschi, Politecnico di Milano)

### → Abilitare il mercato secondario dei crediti

*La diffusione del COVID-19 ha determinato una crisi economica il cui superamento comporterà una trasformazione radicale, nella quale il credito avrà un ruolo cruciale sia nell'emergenza della gestione della crisi, che richiede iniezioni di liquidità nell'economia reale, sia nel finanziamento del cambiamento dei modelli di business. La mobilitazione, trasversale a paesi e aree geografiche, ha caratteristiche comuni e si articola in interventi di breve e medio periodo, di cui parte si consoliderà come infrastruttura del sistema del credito nel "new normal".*

*Questo contesto accresce necessità e valore di un mercato secondario del credito che consenta l'evoluzione da una gestione prevalentemente bancaria e originate to hold ad una gestione con modelli originate to distribute e originate to share che facilitino l'iniezione di capitali non bancari nell'economia reale.*

*Nello specifico, LoanXchain è un mercato secondario multilaterale di crediti, in cui lo scambio tra originator e investitori è basato su Corda, blockchain specifica per il sistema finanziario, a garanzia di semplicità e sicurezza nelle interazioni tra le parti. LoanXchain è una fintech che facilita la canalizzazione di capitali non bancari nell'economia reale, semplificando l'incontro tra domanda e offerta e supportando l'esecuzione della transazione di cessione del credito. Inoltre, opera come piattaforma di accesso a servizi a valore aggiunto forniti da terze parti per arricchire le informazioni funzionali alla valutazione dei portafogli proposti e all'esecuzione delle transazioni, sempre con attenzione a trasparenza, standardizzazione e economicità. Grazie ai vantaggi offerti dalla blockchain, la piattaforma può evolvere anche nella direzione di svolgere il ruolo di punto di incontro della domanda di finanziamento delle*

## Parte 2 – La tecnologia e le applicazioni

*imprese e la risposta da parte di banche e fintech, tracciando eleggibilità e utilizzo delle garanzie pubbliche previste, con semplicità di accesso e digitalizzazione di una parte significativa della documentazione richiesta.*

(Mattia D'Alessandra, Co-founder e CEO MSD Solutions)







# **Gli scenari**

**3**

### 3.1 A che punto siamo

Il Politecnico di Milano ha istituito, ormai da tre anni, un Osservatorio che si occupa di monitorare lo sviluppo delle tecnologie blockchain e delle loro applicazioni sia attuali che prospettive.

Dalle analisi dell'Osservatorio, nel 2020 emerge un mercato caratterizzato dall'aumento dei progetti internazionali, cresciuti del 59% rispetto al 2019, mentre gli annunci sono calati di quasi l'80%: un possibile segnale dell'uscita dallo "hype" e dello spostamento verso progetti più concreti. I casi che hanno visto la luce nel 2020 sono stati 267, di cui 70 sono annunci e 197 sono progetti implementativi; di questi, 83 sono operativi, 54 sono sperimentazioni, e 60 sono "proof of concept", cioè prototipi per valutazione di fattibilità. I continenti più attivi sono Asia e Europa, con 145 e 142 casi rispettivamente. I paesi più attivi sono invece Stati Uniti, Cina e Giappone, con 72, 35 e 28 casi rispettivamente. L'attività maggiore nel continente europeo si osserva in Italia (18 casi), in Francia (16 casi) e nel Regno Unito (15 casi).

L'ambito in cui si concentra l'attività maggiore è quello finanziario, con 59 progetti registrati nel 2020. Secondo viene il mondo della pubblica amministrazione con 37 progetti, il settore dell'agro-alimentare con 15 progetti, quindi la logistica con 11 progetti. Dal punto di vista dei processi interessati, 53 riguardano la gestione documentale, 49 la gestione della supply chain e 43 i pagamenti.

Concentrandosi sui 12 paesi più attivi nel periodo 2016-2020, si nota come i settori privilegiati varino da paese a paese. L'ambito finanziario è primo in 10 paesi su 12: Stati Uniti, Cina, Giappone, Australia, Italia, Francia, Regno Unito, Russia, Germania e Francia. Negli 85 progetti che coinvolgono aziende appartenenti a più nazioni, il settore finanziario è il più rappresentato, con un terzo dei casi.

### Parte 3 – Gli scenari

Le applicazioni di finanza decentralizzata, di cui si è parlato, contengono valore per circa 40 miliardi di dollari. A livello istituzionale si registra in Italia un'attenzione significativa, sia dal punto di vista regolamentare (Consob, per esempio, è molto attiva nel cercare di comprendere, inquadrare e raccordare il fenomeno), che economica. In particolare, il Ministero dello Sviluppo Economico si è fatto promotore di interventi di finanziamento come il Fondo Innovazione, di sperimentazione, in particolare nel campo del tracciamento (Made in Italy e Agrifood), e di studio e analisi, con la formazione di un tavolo di esperti, che ha prodotto un documento di indirizzo che è stato sottoposto a consultazione pubblica. L'Italia è anche attiva nella European Blockchain Partnership, che tra i suoi compiti annovera lo sviluppo di una infrastruttura blockchain validata dagli stati membri, e che possa ospitare applicazioni delle pubbliche amministrazioni (e non solo) europee. Infine, è da ricordare il decreto semplificazioni del 2019 che conferisce valore legale agli smart contract, anche se si è in attesa delle linee guida attuative dell'Agenzia per l'Italia Digitale (AGID).

Se si indagano gli obiettivi delle aziende che hanno implementato dei progetti, spicca il coordinamento dei dati più efficace ed efficiente tra più attori (per il 59% dei progetti), la verificabilità dei dati (24%), lo scambio di valore (13%) e la realizzazione di processi affidabili eseguiti su blockchain (4%).

Nel 2020 gli investimenti in Blockchain e Distributed Ledger da parte delle aziende italiane hanno subito un calo del 23% (23 milioni di euro vs. 30 milioni di euro nel 2019). Le cause della decrescita del mercato, che nel 2019 era in forte aumento, sono da individuare principalmente nell'impatto della pandemia da Covid-19 sui nuovi progetti: le aziende si sono concentrate sullo sviluppo dei progetti già avviati prima della pandemia, mentre sono poche quelle che ne hanno lanciati di nuovi. Il settore più attivo in Italia in termini di investimenti si conferma quello finanziario e assicurativo, con il 58% degli investimenti del 2020.

### ***3.1.1 Valore di mercato delle criptovalute e percezione pubblica***

Il valore di mercato delle criptovalute, e la percezione che ne hanno settori della società quali risparmiatori, investitori istituzionali, media, istituzioni, sono dimensioni di interesse ed interconnesse tra di loro.

Il contesto attuale vede un andamento del valore di mercato delle principali criptovalute per capitalizzazione (Bitcoin ed Ethereum) che, dopo aver toccato dei minimi a marzo 2020, ha aumentato il proprio valore, arrivando a superare ripetutamente i massimi storici nelle ultime settimane e mesi.

Formulare teorie che rendano conto in modo soddisfacente e consentano di prevedere il valore futuro delle criptovalute è ovviamente impresa ardua (se non proprio velleitaria), anche se in qualche modo necessaria.

Alcuni approcci evidenziano aspetti “tecnici”, come la politica monetaria deterministica e deflazionaria, che farebbe delle criptovalute, e in particolare di Bitcoin, un inedito “store of value”, cioè una riserva di valore con caratteristiche “economiche” competitive con quelle dell’oro, unite all’incensurabilità e alla transnazionalità. Altri sottolineano il valore di “utility” di token come l’Ether, che farebbe da “gas” con il quale pagare la creazione e l’utilizzo di smart contract. Secondo alcune spiegazioni sarebbero invece predominanti le dinamiche speculative, e in qualche caso giocherebbero un ruolo problematico alcuni token, tramite i quali le criptovalute vengono acquistate, il cui valore dovrebbe essere garantito da una riserva di dollari, l’entità della quale è però difficilmente verificabile.

In questo contesto, segnali interessanti arrivano dai mondi dell’investimento, anche istituzionale, delle grandi imprese, e delle istituzioni politiche e monetarie.

Per esempio: MicroStrategy, Tesla, Square, Mass Mutual e Mode hanno acquistato in totale oltre 5 miliardi di dollari in

### Parte 3 – Gli scenari

Bitcoin, mettendo la criptovaluta a capitale sociale. Altre come PayPal, Visa e Mastercard hanno permesso e permetteranno alla loro base di utenti di investire ed utilizzare Bitcoin, sfruttando il loro network internazionale.

Inoltre, diverse società - come ad esempio Fidelity, già nel 2018 - offrono agli investitori istituzionali la custodia di criptovalute.

### 3.2 Come cambierà la nostra vita

Blockchain è una tecnologia che potenzialmente può ridefinire il modo in cui pensiamo al valore e alla fiducia, nel contesto sociale ed economico. È molto difficile immaginare quali applicazioni di queste possibilità saranno più rivoluzionarie. Alcuni esempi, d'altra parte, sono già apprezzabili oggi, in forma embrionale, per esempio nella finanza inclusiva, che consente l'accesso ad una porzione molto più grande della popolazione mondiale, e in cui gli intermediari sono fortemente ridimensionati e il loro potere ridefinito. Una delle metafore per rappresentare una prospettiva delle Blockchain è l'“Internet of value”, cioè un mondo in cui il trasferimento di valore diventa infinitamente più semplice e versatile, proprio come l'informazione grazie ad Internet. Un'altra possibilità risiede nella creazione, grazie agli smart contract, di sistemi di incentivi, che possono creare fenomeni sociali ed economici nuovi, come ad esempio orientare il consumo energetico verso forme sostenibili. È poi possibile un cambiamento radicale del rapporto con le amministrazioni pubbliche, nel senso della trasparenza e della partecipazione. Fondamentale e generativa potrebbe essere, più in generale, la possibilità di sviluppare applicazioni che ad oggi richiedono il permesso di *gatekeeper* per dare garanzie di affidabilità e trasparenza, consentendo un rinascimento di applicazioni analogo a quello abilitato dall'avvento dei personal computer o di internet.

### 3.3 Ostacoli

Gli ostacoli che si frappongono allo sviluppo delle potenzialità delle Blockchain sono diversi. Una prima classe di questioni riguarda il raccordo con i sistemi normativi. La Blockchain nasce da un progetto cryptoanarchico, e parte del suo fascino deriva dalla sua capacità di creare potenti strutture di coordinamento che scavalcano quelle istituzionali. D'altra parte, la sinergia tra istituzioni e possibilità abilitate da questa tecnologia potrebbe aprire scenari di sviluppo ancora più significativi (si pensi ad esempio alla "tokenizzazione" di diritti come quello sulla proprietà, fisica o intellettuale).

Esistono poi problemi e limitazioni tecnologiche contingenti, come le prestazioni e la scalabilità, cioè la possibilità di gestire crescita significative nel ritmo delle transazioni, che potrebbero ostacolare (e di certo oggi lo fanno) l'adozione su scala globale. Al momento, il superamento di questi limiti impegna ingenti risorse intellettuali e di sviluppo, in una delle imprese più imponenti della storia dell'informatica.

Infine, ci sono degli ostacoli culturali. I vantaggi, per quanto fondamentali, sono in un certo senso più sottili rispetto a quelli implicati da altre tecnologie (ad esempio il 5G aumenta la velocità di trasmissione dei dati, o l'intelligenza artificiale consente di automatizzare compiti che oggi richiedono l'apporto umano). Comprendere le potenzialità di queste tecnologie richiede dei veri e propri cambi di paradigma culturale nell'approccio a dimensioni come la distribuzione del controllo e della fiducia. In questo senso, la Blockchain non è dissimile da internet, rispetto alle prospettive del quale qualche premio Nobel, nel 2005, disse che non avrebbe lasciato alcun segno significativo perché, in fondo, le persone "non hanno granché da dirsi".

# Raccomandazioni

4

Le iniziative che vedono la tecnologia Blockchain al centro della strategia di innovazione sono numerose e distribuite a diversi livelli, con applicazioni che trovano terreno fertile sia nel mondo della pubblica amministrazione sia in quello privato delle imprese, non limitatamente ai servizi finanziari. Non solo: si stanno definendo anche azioni di tipo istituzionale promosse dai singoli Governi o di tipo sovranazionale, come nel caso della European Blockchain Partnership lanciata dall'Unione europea. Per questo, è importante che anche l'Italia si attivi e che si creino le condizioni migliori, affinché questa rivoluzione possa essere guidata e non subita e perché possa esplicare al massimo tutte le sue potenzialità a vantaggio dell'intero sistema Paese.

Con questa finalità, si propongono di seguito alcune raccomandazioni con l'obiettivo di portare all'attenzione di tutti gli stakeholder delle linee guida utili a impostare e attuare le future azioni di sviluppo della Blockchain in Italia.

### **Raccomandazioni**

1. Posizionare il Paese come hub di innovazione, creare un'infrastruttura di servizi e tecnologia, supportata da un framework giuridico trasparente, basato su principi di neutralità tecnologica, conforme alle normative internazionali, in grado di attrarre investitori e capitali a supporto dell'economia. Nel prossimo futuro è necessario innanzitutto chiarire il contesto regolamentare, che attualmente è frammentato e non uniforme, poiché l'avvento della tecnologia Blockchain e l'adozione delle criptovalute sarà dirompente non solo a livello micro, ma avrà implicazioni di vasta portata nel panorama macroeconomico. Si ritiene che l'adozione di un approccio legislativo per principi e orientato al raggiungimento di scopi, evitando definizioni e casi troppo specifici, sia il più adeguato per massimizzare l'efficacia

#### Parte 4 – Raccomandazioni

normativa in termini di sviluppo della Blockchain e per porre le migliori basi per gli investimenti nel settore.

2. Favorire la cooperazione europea ed internazionale, anche con il coinvolgimento di organismi privati. La Blockchain è una tecnologia globale per natura, che travalica le barriere nazionali o settoriali. Per questo, è fondamentale presidiare le iniziative di sistema che si attivano a livello istituzionale internazionale o a livello di ecosistemi, prevedendo una partecipazione attiva volta a generare le condizioni più favorevoli atte a cogliere i benefici della tecnologia.
3. Utilizzare la tecnologia Blockchain e i vantaggi offerti dalla *tokenizzazione* e dagli *smart contract* per creare nuovi e innovativi modelli operativi e di business, anche in ottica di transizione verso un'economia circolare. Questi nuovi strumenti aprono scenari e opportunità oggi solo in piccola parte esplorati, ma di cui è già chiara la potenzialità nel rivoluzionare modelli di business esistenti e nel rendere possibile la nascita di nuove modalità operative e gestionali, anche ad esempio con riguardo agli obiettivi di sostenibilità. Se la Blockchain in alcuni casi è considerata una tecnologia ad alto consumo energetico, in realtà, oltre allo sviluppo di piattaforme sempre più efficienti, si stanno attivando anche molte iniziative che vedono l'utilizzo di Blockchain, *token* e *smart contract* per incentivare comportamenti virtuosi in ottica *green*. A titolo di esempio, la Blockchain può giocare un ruolo centrale nello sviluppo delle comunità energetiche, quale nuovo modello virtuoso di sviluppo sociale, urbanistico ed economico.

4. Promuovere l'informazione e la consapevolezza della Blockchain tra le imprese, le istituzioni e i cittadini, strutturando percorsi informativi, webinar, eventi e dibattiti. La Blockchain è una tecnologia che nasce in tempi molto recenti e per questo è ancora poco conosciuta, come evidenziato anche dalle ricerche: la consapevolezza circa le sue applicazioni e i suoi impatti è ancora troppo poco diffusa. Questo emerge anche se si guarda agli investimenti effettuati nel settore: seppur in uno scenario di rapida crescita, il loro valore assoluto è ancora limitato. Occorre, quindi, ridurre questo gap cognitivo, utilizzando un approccio *technology push*, che maggiormente si adatta alle fasi iniziali di introduzione di tecnologie innovative, quale è la Blockchain.
5. Promuovere la creazione e la diffusione di competenze sulla tecnologia Blockchain: formazione, upskilling, reskilling. Per velocizzare l'adozione di tale tecnologia, occorre agire anche sul fronte della formazione delle competenze necessarie. Ciò da un lato agevolerebbe la formazione di giovani su skills strategiche per il loro ingresso nel mondo del lavoro e l'aggiornamento o l'acquisizione di nuove competenze per chi già lavora, e dall'altro abiliterebbe le aziende all'adozione di nuovi modelli di business in linea con le più recenti evoluzioni digitali in atto. Infatti, la conoscenza e la corretta comprensione della tecnologia è il fattore chiave per la sua adozione e quindi per la sua più proficua diffusione.
6. Definire una politica di accompagnamento e accelerazione che consenta alle imprese di svolgere attività di ricerca, sviluppo, innovazione. L'evoluzione tecnologica sempre più rapida e l'inasprimento della competizione negli scenari globali richiedono alle imprese di investire

#### Parte 4 – Raccomandazioni

in modo significativo in ricerca e innovazione per restare al passo e possibilmente essere o diventare leader nei propri settori. Ugualmente, anche i singoli paesi e le macro-aree geografiche competono tra loro per conseguire una leadership sulle tecnologie emergenti. Per questo la definizione di framework e di politiche attive a supporto degli investimenti in R&I delle imprese diventa essenziale per la competitività non solo delle imprese, ma anche di sistemi territoriali in cui sono inserite ed operano. Sul fronte specifico della Blockchain, oltre alle politiche di incentivazione volte ad accelerare la transizione digitale, si apre l'opportunità di creare delle sandbox utili alle sperimentazioni. In particolare, si ritiene strategico promuovere l'attivazione di sandbox locali, che abilitino l'innovazione anche a livello, ad esempio, di ecosistema regionale.

7. Sostenere la creazione di ecosistemi per massimizzare l'utilizzo delle risorse. La Blockchain è una tecnologia che si potrebbe definire multi-attore, in quanto il suo modello stesso di funzionamento è basato su una molteplicità di nodi e il suo focus sono le transazioni tra più attori. Per questo, i suoi impatti vengono massimizzati nei casi di applicazione nell'ambito di ecosistemi. Risulta, quindi, particolarmente significativo per il nostro Paese l'utilizzo della Blockchain per supportare la difesa e la valorizzazione del Made in Italy, delle filiere strategiche e della valorizzazione dei distretti innovativi. La piccola e media impresa italiana ha oggi il forte bisogno di un sostegno sistemico per poter migliorare la tracciabilità, la trasparenza e la tutela dei propri marchi, sia all'interno della filiera di appartenenza sia nei confronti dei consumatori finali.

8. Promuovere il contributo della Blockchain in ottica di valorizzazione degli asset immateriali detenuti dalle aziende. Quando si guarda agli scenari competitivi internazionali, la corretta valutazione d'azienda è un tema strategico. La Blockchain, grazie all'ampio spettro delle sue possibili applicazioni, può giocare un ruolo anche nella direzione di una valorizzazione più completa del valore degli asset aziendali. Infatti, attraverso la Blockchain è possibile notarizzare gli asset immateriali (ad esempio, i dati) detenuti da un'azienda in un determinato momento e quindi contribuire ad abilitarne l'iscrizione all'interno dello stato patrimoniale. Ciò consentirebbe, in ultima istanza, di effettuare una valutazione d'azienda più completa.
9. Spingere sull'identità digitale attraverso l'utilizzo della Blockchain. L'identità digitale rappresenta un tema di valenza strategica, in quanto rappresenta un fattore abilitante per l'attivazione di servizi e modelli operativi innovativi. Per citare un possibile esempio, potrebbe facilitare l'erogazione di premialità ad incentivo dei comportamenti virtuosi. La Blockchain, con le sue caratteristiche, è una tecnologia che ben si presta alla sua realizzazione, anche in ottica di Self Sovereign Identity e di identità digitale non solo per le persone, ma anche per le cose.
10. Promuovere l'utilizzo della Blockchain come strumento efficace per contribuire ai processi di semplificazione e trasparenza della P.A. centrale e locale. La Blockchain può rivoluzionare il modo con il quale le amministrazioni pubbliche, le imprese e i privati interagiscono. Grazie a questa tecnologia, per la pubblica amministrazione è possibile rendere più efficienti ed efficaci sia i propri processi interni (ad esempio, per la notarizzazione di documenti nella gestione di pratiche amministrative), sia i

#### **Parte 4 – Raccomandazioni**

processi di gestione ed erogazione dei servizi verso imprese e cittadini (ad esempio, riducendo i tempi e i costi per la gestione delle domande di accesso a determinati servizi). Inoltre, grazie alla tracciabilità consentita dalla Blockchain, migliora sia il monitoraggio esercitabile da parte della pubblica amministrazione, ma anche la trasparenza offerta a imprese e cittadini. Puntare sulla Blockchain nel mondo pubblico, significa quindi intraprendere un percorso virtuoso verso una P.A. 4.0, rapida, snella, vicina alle esigenze dei cittadini e delle imprese.



## Note

## Note



ilfi

blo

## La visione di Assolombarda sul futuro della blockchain

Dopo il libro bianco su “Il futuro della fabbrica”, che aveva delineato gli scenari applicativi tecnologici alla base dell’evoluzione digitale delle imprese, questa pubblicazione effettua un affondo su una delle tecnologie a maggior potenziale: la blockchain, da alcuni definita come *l’Internet del valore*.

Una tecnologia emergente e in via di forte evoluzione, che dopo un iniziale avvio nel mondo finanziario, sta rapidamente coinvolgendo intere filiere industriali ed ecosistemi. Si delineano così nuovi scenari e nuovi modelli di business abilitati dalla blockchain in tutti i settori.

Il libro intende accompagnare verso la migliore comprensione della tecnologia e delle sue molteplici applicazioni e contribuire con proposte di policy alla creazione di un contesto idoneo e favorevole allo sviluppo della tecnologia e delle sue potenzialità.

Con questo libro Assolombarda prosegue la serie di volumi dedicati ai temi strategici per la crescita delle imprese, delle persone e del territorio.