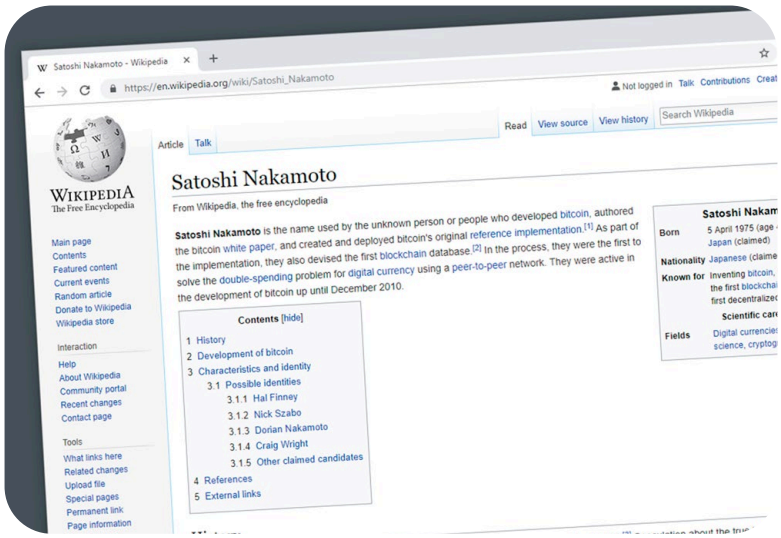
EDUCAZIONE CIVICA digitale

Come funziona la blockchain?

9 IMPRESE, INNOVAZIONE E INFRASTRUTTURE

AGENDA 2030



Ricky Of The World / Shutterstock

Satoshi Nakamoto è lo pseudonimo dietro cui si nasconde chi, nel 2009, ha introdotto il Bitcoin, la prima valuta digitale legale ad aver sostituito il classico meccanismo di autenticazione tramite un server centralizzato con una tecnica decentralizzata del «*consenso pubblico*» basata sulla *blockchain*.

1. La basi della blockchain

Una blockchain può essere vista come una serie illimitata e non centralizzata di atti notarili pubblici, immutabili, gestiti da un software dedicato. Nel software sono programmate le regole che, quando rispettate, permettono di portare a compimento, in automatico, un'operazione. La blockchain è di fatto un registro aperto, un libro mastro (*ledger*), in cui, basandosi sul concetto di fiducia, vengono registrate una serie di transazioni senza necessità di entità centrali deputate al loro controllo.

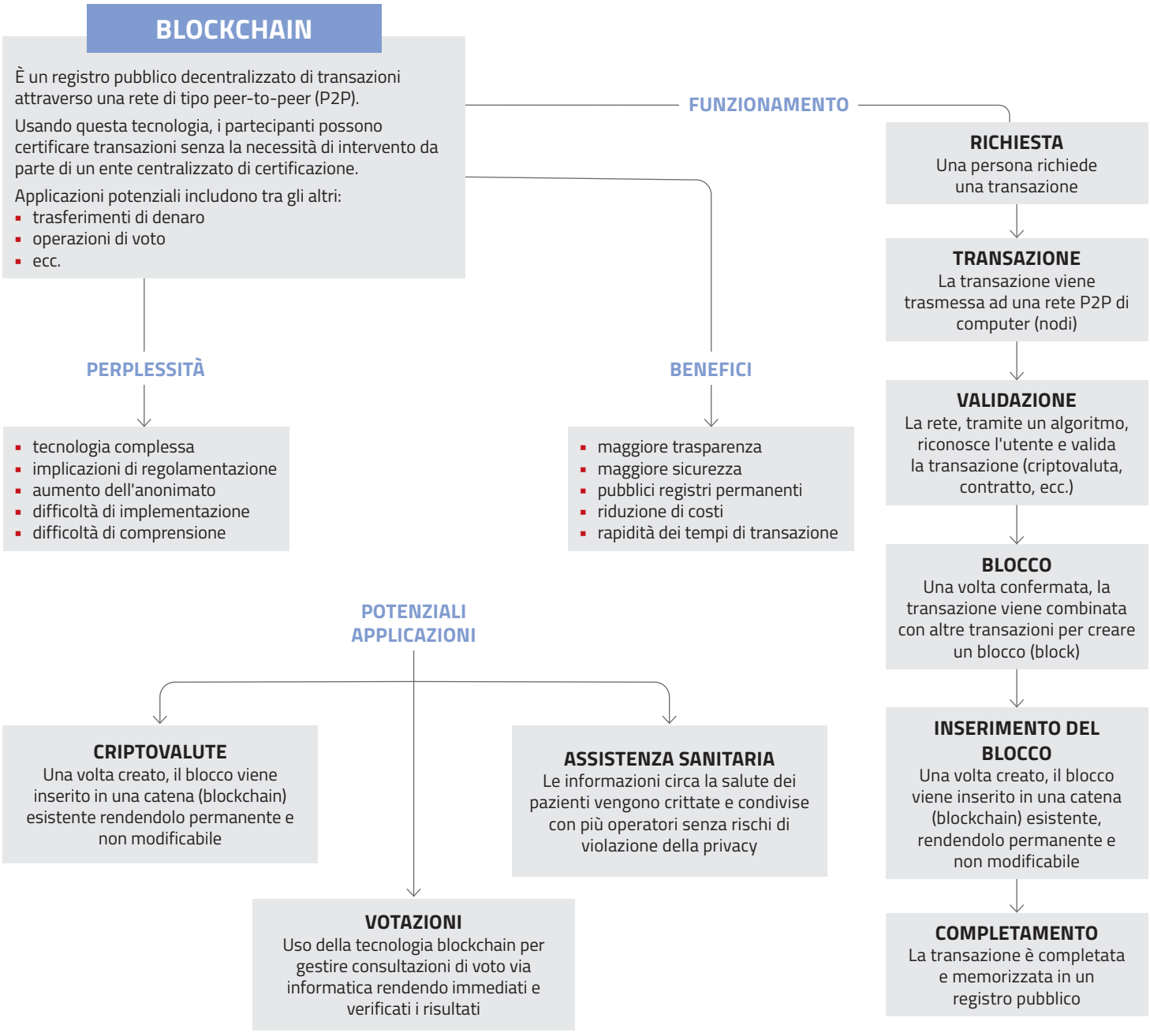
In genere, per la creazione di un'azienda o per una compravendita immobiliare, si ricorre a un notaio che verifica e certifica i presupposti di legge perché l'operazione possa avvenire; le transazioni economiche vengono effettuate in valuta corrente certificata da una banca centrale. Nell'approccio blockchain non ci sono né notai né banche centrali.

Tecnicamente, una blockchain è un particolare tipo di database distribuito e condiviso tra i nodi di una rete di computer che memorizza informazioni organizzandole in unità di archiviazione, denominate blocchi, collegate tra loro. Un blocco, una volta compilato, viene chiuso con una firma digitale immutabile e collegato all'ultimo blocco presente nella catena. Ogni nuovo blocco contiene anche la firma digitale del blocco a cui viene agganciato così da creare una sequenza temporale irreversibile.

La blockchain si basa su questi cinque concetti fondamentali:

- **Decentramento**. La blockchain è una rete P2P (Peer-to-Peer o Person-to-Person) in cui il controllo è distribuito equamente tra tutti gli utenti in modo tale che nessun partecipante possa hackerare, manipolare o chiudere la «catena di blocchi».
- **Integrità**. Nella blockchain tutti i partecipanti hanno il diritto di prendere decisioni: la fiducia nel sistema non è forzata ma guidata dell'utente. L'integrità si esplica nel modo in cui ogni utente è incentivato a partecipare in maniera attiva e costruttiva al funzionamento della rete.
- **Sicurezza**. Poiché la blockchain si basa su una rete distribuita, non esiste alcun punto centrale di controllo e nessun utente può danneggiare l'intera catena della rete con le proprie azioni. Con il meccanismo di crittografia avanzata PKI (*Public Key Infrastructure*) le transazioni sulla rete risultano protette ed è garantita l'autenticità degli utilizzatori.
- **Inclusione**. Tutti gli utenti sono indipendenti e possono partecipare senza alcuna discriminazione. Bitcoin, per esempio, consente a tutti, indipendentemente dal proprio livello economico, di investire nelle proprie capacità e di far parte della sua economia globale senza la necessità di avere un conto in banca.
- **Rispetto della privacy**. In un mondo digitale, dove si effettuano transazioni online per fare acquisti, trasferire pagamenti e verificare informazioni, garantire la privacy dei dati è fondamentale. La crittografia *Strong Hash Key*[1] usata nella Blockchain è sicura e permette lo scambio di dati su Internet senza rivelare la propria identità.

[1] In informatica, l'*hash* è una funzione matematica non invertibile che, sulla base di specifici algoritmi, fa corrispondere a una stringa, sequenza di caratteri di lunghezza arbitraria, un'altra stringa di lunghezza predefinita.



2. Tipi di Blockchain

Nella tabella che segue sono riassunti i principali tipi di Blockchain:

	Blockchain Pubblica	Blockchain Privata	Blockchain Federata/Consorzio
Accesso	Chiunque	Singolo ente (di solito limitato a una rete aziendale; una singola entità controlla l'appartenenza di chi opera)	Più enti (limitato a più reti aziendali; un consorzio controlla l'appartenenza di chi opera)
Partecipazione	Anonima senza abilitazioni	Solo identità abilitate con privilegi di accesso (certificati)	
Sicurezza	Meccanismo di consenso basato su prova di lavoro (*proof of work*) o di partecipazione (*proof of stake*)	Solo partecipanti abilitati con consenso a più voci o «approvazione selettiva» (utenti noti verificano le transazioni; solo i membri con accesso e autorizzazioni speciali possono gestire il registro delle transazioni)	
Velocità di transazione	Lenta	Leggera e veloce	

3. Applicazioni della blockchain

Anche se la blockchain è stata introdotta con il Bitcoin, rivoluzionando l'area della tecno-finanza (*Fintech*), i suoi meccanismi la rendono utilizzabile in molti settori classificabili in due ambiti principali: finanziario e non finanziario. In entrambi i casi si sta cercando anche di affiancare alla blockchain la potenza dell'intelligenza artificiale per sviluppare soluzioni intelligenti che possano migliorare e renderne più efficiente l'utilizzo.

4. Ambito finanziario

Oltre alle criptovalute (Bitcoin, Dash, Ethereum, ecc.), l'uso della blockchain si sta diffondendo molto velocemente in altre aree applicative che riguardano servizi bancari, finanziari e assicurativi (BFI – *Banking, Finalcial service, Insurance*).
Nella figura che segue è rappresentato graficamente l'iter di un'operazione di trasferimento di denaro (*money transfer*) dal portafoglio digitale (*digital wallet*) di un soggetto A verso quello di un soggetto B con la blockchain.

Bitcoin

Il Bitcoin è la prima moneta virtuale o criptovaluta introdotta sul mercato. Essa non è controllata da alcuna banca centrale che la distribuisce ma si basa sui due elementi fondamentali della rete P2P e dell'uso di algoritmi crittografici per validare e rendere sicure le transazioni.

I Bitcoin potenzialmente disponibili sono in un numero finito che tende a 21 milioni di esemplari; si stima che la creazione dell'ultimo Bitcoin, tramite la tecnica denominata «*mining*», avverrà intorno al 2140. L'operazione di mining ha un duplice obiettivo: generare nuovi Bitcoin e verificare la legittimità delle transazioni in criptovaluta sulla relativa blockchain. Il «meccanismo di consenso» del Bitcoin prevede che tutti i partecipanti (*stakeholder* o validatori) devono concordare quali transazioni sono da ritenersi legali, impedendo il verificarsi di truffe come, per esempio, la duplicazione di criptovaluta.

I blocchi concatenati della blockchain sono uniti matematicamente fra di loro. Ogni nuovo blocco genera una «prova di lavoro» (*Proof of Work* o PoW). Questa PoW, porta tutti i minatori di Bitcoin (*miner*), a concorrere alla ricerca di una soluzione valida per un problema matematico complesso che si concretizza nel determinare un valore hash di 64 caratteri. Nello specifico, i miner devono trovare un valore che, se aggiunto ad altre informazioni

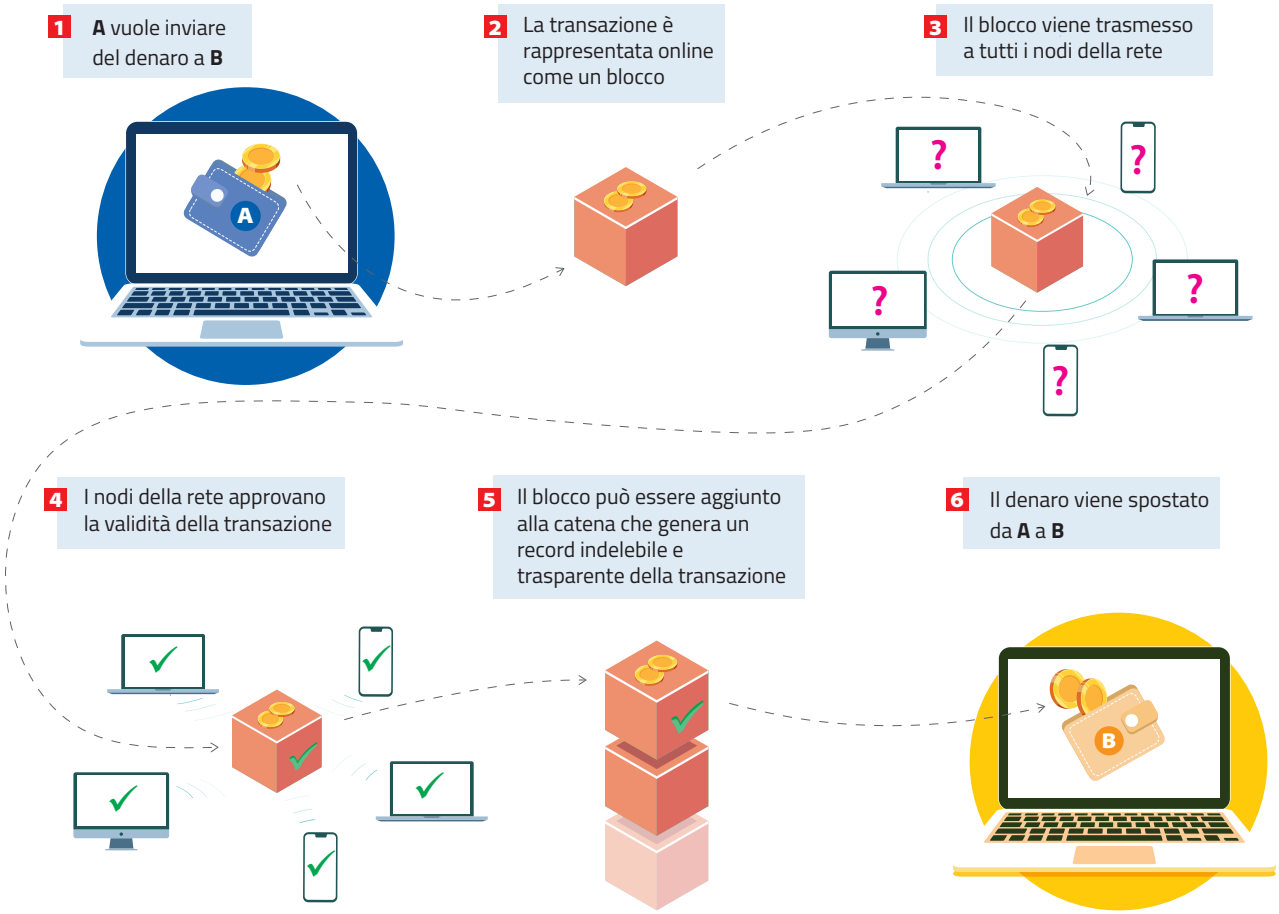


Figura 1 Esempio di *money transfer* con Blockchain.

presenti nel blocco della PoW, restituisca un determinato codice hash. I miner competono tra loro nella ricerca della soluzione e il primo che riesce a determinarla può generare il nuovo blocco. Quando un miner trova la soluzione, tutti gli altri miner, per evitare errori che potrebbero compromettere i blocchi già archiviati, dovranno validare il risultato trovato: solo allora il solutore otterrà la sua ricompensa (in Bitcoin) e il blocco verrà aggiunto a quelli già esistenti.
Per svolgere queste attività, ogni miner (cioè ogni nodo della rete) deve sostenere costi notevoli usando appositi software su un hardware potente, impiegando moltissimo tempo di calcolo e consumando di conseguenza notevoli quantità di energia elettrica (si stima che il mining di Bitcoin richieda più energia di quella usata da una nazione come la Finlandia).

Ogni quattro anni la quantità di Bitcoin corrisposta ai minatori a titolo di ricompensa per il loro lavoro viene dimezzata. Questo meccanismo programmato, detto *halving*, rende il Bitcoin una risorsa scarsamente disponibile e quindi resistente all'inflazione. Chi possiede della criptovaluta necessita di un portafoglio digitale dedicato (*wallet crypto*) che permette di archiviarla, conservarla, inviarla e riceverla tramite Internet. Ogni *wallet crypto* è dotato di un indirizzo unico, composto da lettere e numeri, equivalente ad un tradizionale IBAN. Ogni transazione effettuata tramite *wallet crypto* è irreversibile e non può essere annullata. Dal momento che tutte le chiavi crittografiche di accesso sono memorizzate su strumentazione informatica a livello individuale, è necessario averne molta cura per evitare di perderle irreversibilmente.
Un altro metodo di validazione previsto da alcune blockchain è quello relativo alla tecnica chiamata «prova di interesse in gioco» (*Proof of Stake* o PoS); tale metodo è stato proposto nel 2012 in alternativa al PoW per far fronte all'enorme consumo di energia richiesto da quest'ultimo. Con il PoS i nuovi blocchi non vengono minati ma «coniati». I partecipanti deputati a coniare nuovi blocchi vengono selezionati in modo pseudocasuale (in via prioritaria sulla base di quantità di valuta digitale posseduta). La PoS viene generalmente applicata a criptovalute pre-minate, valute la cui offerta complessiva è fissata sin dall'inizio, che non prevedono alcun premio per la creazione di nuovi blocchi ma che hanno come unico incentivo le commissioni di transazione associate agli specifici blocchi coniati. Nel modello PoS, l'ammontare di valuta posseduta da ogni utente è fondamentale e ne definisce il livello di attendibilità: più importante è il suo coinvolgimento (*stake*) nella criptovaluta, maggiore è la sua esposizione economica e quindi più alta sua affidabilità.

Altri settori finanziari

Le tecnologie incentrate su *asset finanziari* (come per esempio metalli preziosi, azioni, obbligazioni, valute) si concentrano sullo scambio di rappresentazioni digitali degli asset esistenti su un registro elettronico condiviso (non pubblico). La fiducia non si costruisce attraverso il mining ma direttamente tra i partecipanti. In questi casi le operazioni possibili includono cambi/emissioni estere, pagamenti in tempo reale, documenti di commercio. Nell'area dei servizi finanziari sono in atto molti esperimenti sulla blockchain per facilitare il trasferimento di beni o valuta, rendere trasparenti informazioni sulle operazioni su titoli azionari (*Trading*) e altre attività di finanza commerciale

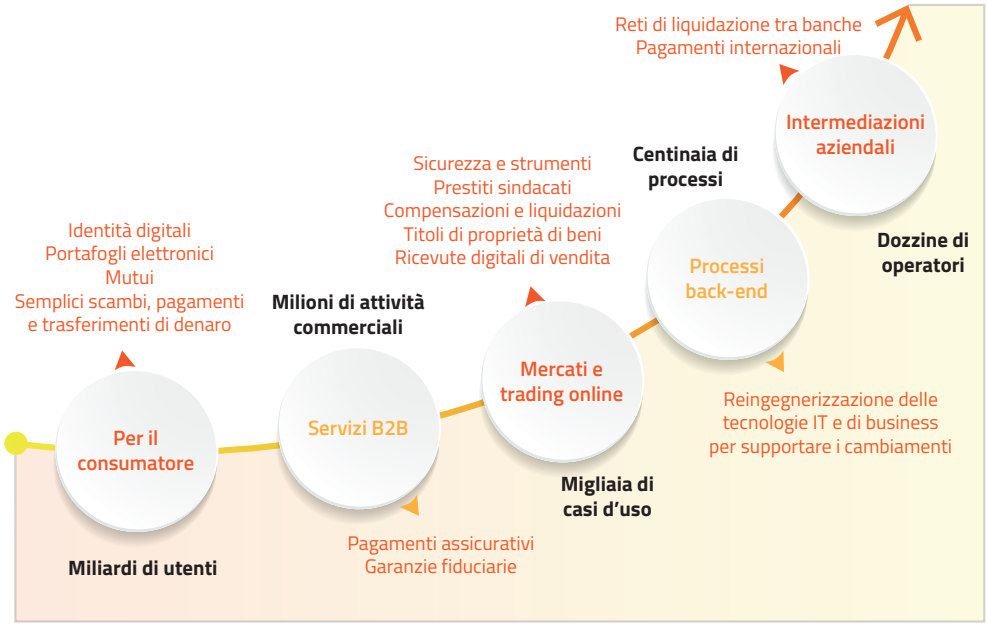


Figura 2 Andamento evolutivo della complessità e della richiesta della Blockchain nell'area della TecnoFinanza.

come i servizi B2B (*Business to Business*), cioè transazioni commerciali che intercorrono tra imprese industriali.

Un contratto intelligente (*smart contract*) è un contratto digitale archiviato su una blockchain che viene eseguito automaticamente quando sono soddisfatti certi termini e condizioni. Questi contratti sono gestiti da software che predefiniscono regole non modificabili relativamente a un determinato progetto: chi vuole partecipare deve accettarle e automaticamente, senza bisogno di ulteriori consensi, entra nel progetto. Per esempio, uno *smart contract* potrebbe prevedere i pagamenti in automatico delle controparti nei casi in cui sia prevista l'erogazione di un corrispettivo a fronte di forniture di servizi una volta avvenuta la fornitura.

5. Ambito non finanziario

Assistenza sanitaria

Il settore della sanità è molto interessato all'adozione della blockchain per definire tecnologie con cui le parti interessate (medici, pazienti, ospedali, farmacisti, laboratori di test) possano comunicare per gestire le informazioni sull'assistenza sanitaria in modo sicuro, affidabile e autentico.
Questo permetterebbe di:

- mantenere sicure le cartelle cliniche dei pazienti;
- creare una solida rete di comunicazione tra gli operatori sanitari;
- fornire ai medici informazioni precise e accurate sui pazienti per migliorare i servizi offerti;
- gestire in modo affidabile e autentico le transazioni di approvvigionamento farmaceutico;
- includere compagnie assicurative nella rete sanitaria per semplificare la liquidazione dei sinistri.

Altri settori non finanziari

L'idea di applicare la tecnologia blockchain sta trovando spazio anche in altri ambiti:

- **Energia**. Si stanno sviluppando soluzioni in grado di gestire gli elementi della catena del valore dell'energia, come la sua generazione, trasmissione, distribuzione e vendita al dettaglio. Contatori intelligenti abilitati alla blockchain possono alimentare i dati di consumo per una logica di sviluppo di contratti intelligenti di fornitura.
- **Approvvigionamento delle merci**. Si cerca di salvaguardare la catena di approvvigionamento delle merci (*supply chain*) contro tentativi di contraffazione proponendo nuove tecniche per la gestione delle sue transazioni e dei relativi finanziamenti. Obiettivo è anche quello di creare un'unica fonte di informazioni per dare visibilità della supply chain a livello globale.
- **Agricoltura**. Si punta a conseguire miglioramenti in termini di conformità, verificabilità, visibilità, trasparenza e integrità dell'ecosistema, tradizionalmente complesso, dei valori agricoli globali verso un commercio equo e sostenibile.
- **Diritto di voto**. Il diritto di voto assicura agli individui la possibilità di manifestare la propria volontà durante una consultazione di massa. Con l'uso della blockchain le votazioni potrebbero tenersi per via informatica rendendo i risultati immediati, trasparenti e verificati.

FISSA I CONCETTI IMPORTANTI

1 **Una blockchain consente di**

A archiviare transazioni Peer-to-Peer
B archiviare transazioni multi-utente
C rendere pubbliche id e password utente
D rendere immutabile una catena di transazioni

2 **Quale dei seguenti è un elemento base della tecnologia blockchain?**

A Registri privati volatili
B Rete strettamente gerarchizzata con client e server ben definiti
C Uso di tecniche di hashing
D Riduzione dell'anonimato

3 **I Bitcoin sono**

A una nuova valuta ormai riconosciuta a livello bancario internazionale
B una valuta legale riconosciuta solo da certi circuiti bancari
C una valuta illegale
D una criptovaluta

4 **I protocolli di consenso Proof of Stake**

A richiedono più energia del Proof of Work
B richiedono la stessa energia del Proof of Work
C richiedono meno energia del Proof of Work
D non richiedono energia

5 **L'esecuzione di un contratto intelligente**

A non implica mai un trasferimento di risorse
B viene registrato nella Blockchain
C può essere adattato, anche dopo la pubblicazione del contratto
D in ogni caso non può riguardare la fornitura di servizi o di merci

6 **Relativamente ai requisiti di sicurezza, quale dei seguenti punti deve essere soddisfatto durante l'aggiunta di un blocco in una blockchain?**

A Prevedere un'unica copia del blocco su uno specifico nodo della rete.
B Memorizzare in esso anche l'hash associato al blocco precedente.
C Prevedere diverse modalità di gestire la privacy.
D Non utilizzare di tecniche di hashing

7 **Una blockchain supporta la convalida delle transazioni con le stesse prestazioni di un classico sistema centralizzato?**

A Si, sempre.
B Dipende dai campi applicativi
C No, mai, perché la convalida – essendo basata su un processo di convalida distribuito – richiede molto più tempo di un classico sistema centralizzato.
D Non ha senso parlare di prestazioni in termini di velocità relativamente alla convalida di transazioni

8 **Perché fidarsi della blockchain e dei suoi attori?**

A Perché la blockchain si basa su un'organizzazione fiduciaria distribuita.
B Perché la blockchain si basa su un'organizzazione fiduciaria centralizzata.
C Perché è sempre nota l'identità precisa dei vari attori.
D Perché non è mai nota l'identità precisa dei vari attori.

9 **Quale delle seguenti voci afferiscono al mondo delle criptovalute?**

A Conto corrente.
B Wallet crypto.
C IBAN
D PKZ.

ATTIVITÀ

Attività

Un passaporto digitale per i veicoli. Si vuole valutare l'adozione di un passaporto digitale per i veicoli, per gestire la catena di manutenzione (interventi programmati o di emergenza, sostituzione di pezzi difettosi o usurati, certificazione del chilometraggio percorso)

Descrizione dello scenario

- Nel tempo, diversi partner (officine certificate) possono essere coinvolti nella manutenzione del veicolo.
- Il processo di qualità implica la possibilità di monitorare ogni processo di intervento sul veicolo in modo che i clienti siano costantemente informati sullo stato del loro mezzo.
- Certi interventi debbono essere fatti a scadenze prefissate pena la decadenza della garanzia della casa madre.
- Certificazione del chilometraggio percorso.

Domande

- Valutare questo tipo di organizzazione (eventuali pregi e difetti) nell'ottica della salvaguardia della garanzia del veicolo anche in relazione alla tempistica degli interventi.
- In questa situazione come può incidere l'uso della blockchain sulla garanzia dei veicoli e sugli aspetti economici a carico dei proprietari?
- Quale tipo di blockchain potrebbe essere adottato per supportare questo scenario?
- Come può essere gestita l'operazione di ricostruzione degli interventi effettuati (*backtracking*)? Quali potrebbero gli elementi chiave da archiviare nei blocchi della Blockchain?
- Quali vantaggi ci sarebbero per l'acquirente di un veicolo usato?
- La tecnologia blockchain in questo caso può essere considerata più o meno sicura rispetto ai certificati (timbri) rilasciati dell'officina?