First Personal Coin

Bitcoin

Le basi per orientarsi, valutare e formarsi un’opinione autonoma

Indice

Introduzione: una rivoluzione silenziosa che ha già iniziato a cambiare le regole

Blockchain e **Bitcoin** sono ovunque: nei **titoli di giornale**, nelle **conversazioni**, nelle decisioni di chi investe o fa impresa. Eppure la **comprensione reale** di cosa siano e come funzionino resta rara, anche tra chi lavora in settori direttamente coinvolti.

- Questo documento offre una **base solida** e **operativa**: cosa sia la blockchain, come funzioni, perché sia rilevante. Senza tecnicismi, senza spingere verso decisioni di investimento.
- Capirla è utile indipendentemente dal **punto di partenza**, che si lavori con asset, contratti, processi o si stia semplicemente cercando un orientamento affidabile in un settore spesso difficile da leggere.

Perchè questo tema conta

La tecnologia blockchain non è un fenomeno di nicchia destinato agli appassionati di informatica. È un'infrastruttura pubblica che tocca già oggi finanza, contratti, proprietà digitale, identità e molto altro.
Comprenderla è un vantaggio competitivo.

Che siate professionisti che vogliono orientarsi in un settore in rapida evoluzione, investitori che cercano una base concettuale per le proprie decisioni, o semplicemente persone curiose di capire di cosa parla davvero il mondo intorno a voi — **questo è il punto di partenza giusto**.

1. Il contesto: un cambiamento già in corso

Prima di entrare nella tecnologia, vale la pena **capire perché questo momento storico è diverso**. Negli ultimi anni, il comportamento degli investitori ha mostrato una tendenza strutturale verso l'**allungamento dell'orizzonte temporale**. In Italia, circa il 60% degli investitori retail dichiara oggi un orizzonte di investimento pari o superiore a cinque anni. Questo dato, apparentemente tecnico, diventa molto significativo quando lo si mette in relazione con la storia delle criptovalute.

Chi avesse investito in Bitcoin in qualsiasi momento del 2018 — anno segnato da un crollo severo dei mercati crypto — avrebbe comunque ottenuto rendimenti rilevanti entro il 2023. Chi avesse investito nel 2021, anche in prossimità dei massimi storici di allora, avrebbe attraversato una fase di forte correzione ma visto il mercato recuperare e superare quei livelli nel 2024. **Questo non è una promessa di rendimento futuro: i mercati non replicano meccanicamente il passato e il rischio rimane reale e significativo**.

È però un dato che pone una domanda precisa: **ha senso esporsi a un asset** — o più in generale, ignorare una tecnologia — **senza capirne il funzionamento di base?**

La risposta è no e non solo per ragioni di investimento. Come per qualsiasi decisione economica rilevante, la comprensione è il prerequisito di qualsiasi scelta consapevole.

2. Che cos'è la Blockchain: una definizione operativa

Il termine blockchain è la traduzione letterale di "**catena di blocchi**". Questa definizione, pur nella sua semplicità, descrive con esattezza l'architettura della tecnologia: una sequenza di unità di dati standardizzate — i blocchi — collegate le une alle altre attraverso un meccanismo crittografico che le rende inscindibili e immutabili nel tempo.

Ma la blockchain **non è solo una struttura dati**. È una struttura dati distribuita su una rete di computer — chiamati **nodi** — che non fa capo ad alcun server centrale, ad alcuna banca, ad alcun'autorità di supervisione. **Ogni nodo conserva una copia identica dell'intero registro delle transazioni**. Questa è la caratteristica che rende la blockchain "**decentralizzata**": non esiste un punto unico di controllo o di fallimento.

Definizione sintetica

Una blockchain è un **registro pubblico**, **distribuito**, **immutabile** e **decentralizzato**. Nessuno lo possiede interamente. Tutti possono consultarlo. Nessuno può alterarlo unilateralmente senza che l'intera rete se ne accorga e lo rigetti.

Su questa infrastruttura è possibile emettere unità digitali chiamate **coin**. La prima — e tuttora la più nota e capitalizzata — è il **Bitcoin**, concepita nel 2009 dal misterioso Satoshi Nakamoto con un obiettivo dichiarato: rendere possibili pagamenti diretti tra persone senza intermediari finanziari. Come vedremo, le applicazioni della blockchain si sono evolute ben oltre il pagamento, aprendo scenari che anche i fondatori non avevano previsto nella loro interezza.

3. I componenti fondamentali

Il blocco

Il blocco è l'**unità base della blockchain**. Si tratta di un contenitore digitale che raccoglie un insieme di transazioni verificate in un determinato intervallo di tempo. Ogni blocco contiene **tre elementi strutturali**:

- Le **transazioni registrate** in quel lasso di tempo, con tutti i dettagli relativi agli indirizzi coinvolti e agli importi trasferiti.
- Un **riferimento crittografico al blocco precedente** — tecnicamente chiamato hash — che costituisce il "sigillo" che lega ogni blocco al precedente in modo inviolabile.
- La **prova del lavoro computazionale svolto per validarlo**, che certifica che quel blocco è stato prodotto rispettando le regole della rete.

È il riferimento crittografico al blocco precedente a creare la catena. Modificare anche un solo dato in un blocco già scritto significa rompere il collegamento con tutti i blocchi successivi, rendendo la manomissione immediatamente rilevabile da qualsiasi nodo della rete.

I nodi

I **nodi sono i computer** che partecipano alla rete blockchain. Non sono server centralizzati sotto il controllo di un'unica entità: chiunque può, in linea di principio, diventare un nodo, a condizione di rispettare le regole del protocollo. **Ogni nodo conserva una copia completa del registro e partecipa attivamente alla validazione delle nuove transazioni.**

Questa distribuzione è il **fondamento della sicurezza della blockchain**. Per compromettere l'integrità del sistema, un attaccante dovrebbe controllare simultaneamente la maggioranza dei nodi della rete — uno scenario che su reti mature come quella di Bitcoin è economicamente e tecnicamente infattibile. Il costo di un simile attacco supererebbe di gran lunga i potenziali benefici.

Il registro distribuito

L'**insieme dei blocchi**, letti in **sequenza cronologica**, forma il **registro distribuito**: la **storia completa** e immutabile di ogni transazione mai avvenuta sulla rete. Questo registro non esiste in un unico luogo: è custodito, identico, su migliaia di computer distribuiti in tutto il mondo.

La **conseguenza è strutturale**: nessuno lo possiede, tutti lo possono consultare, nessuno può alterarlo unilateralmente. È una **proprietà senza precedenti nella storia dei sistemi di archiviazione dell'informazione**.

4. L'algoritmo di consenso: il meccanismo che rende tutto funzionante

La domanda più naturale a questo punto è: come fa una rete di migliaia di computer distribuiti nel mondo a **mettersi d'accordo su quale sia la versione corretta del registro**? Come si **evita** che soggetti malintenzionati **inseriscano transazioni false**? La risposta sta nell'**algoritmo di consenso**.

Questo meccanismo definisce le regole attraverso le quali i nodi della rete raggiungono un accordo collettivo su quale blocco aggiungere alla catena. L'algoritmo più noto — quello utilizzato da Bitcoin fin dalla sua nascita — si chiama **Proof of Work** e il suo funzionamento ha un'analogia illuminante: il **Sudoku**.

La metafora del Sudoku

Come nel Sudoku, trovare la soluzione per aggiungere un nuovo blocco è computazionalmente costoso e richiede un lavoro significativo — da cui il nome Proof of Work. Ma una volta trovata la soluzione, verificarne la correttezza è immediato per chiunque. La rete non si trova mai nella condizione di accettare soluzioni errate: la verifica è rapida, collettiva e incontrovertibile.

In pratica, migliaia di computer — chiamati **miner** — competono simultaneamente per trovare questa soluzione, consumando potenza computazionale ed energia. **Il primo che la trova trasmette il risultato all'intera rete**: gli altri verificano la correttezza in frazioni di secondo, il blocco viene aggiunto alla catena e la competizione ricomincia per il blocco successivo. Chi ha trovato la soluzione riceve Bitcoin come ricompensa: è il meccanismo con cui nuovi Bitcoin vengono immessi in circolazione.

Tempi di blocco e generazioni tecnologiche

Bitcoin aggiunge un nuovo blocco ogni circa 10 minuti — una scelta progettuale deliberata che privilegia la sicurezza massima rispetto alla velocità. Le blockchain di generazione successiva hanno fatto scelte diverse, ottimizzando per la velocità senza sacrificare la sicurezza attraverso algoritmi di consenso alternativi.

Blockchain	Tempo di blocco approssimativo
Bitcoin (BTC)	~ 10 minuti
Ethereum (ETH)	~ 12 secondi
Avalanche (AVAX)	~ 2 secondi
Solana (SOL)	< 1 secondo

Queste differenze riflettono scelte progettuali precise. Bitcoin privilegia la decentralizzazione massima e la sicurezza provata nel tempo, accettando la lentezza come compromesso necessario. Le blockchain più recenti cercano l'equilibrio tra velocità, sicurezza e scalabilità — il cosiddetto "trilemma della blockchain", uno dei temi centrali della ricerca in questo campo.

5. L’immutabilità: scrivere sulla blockchain è per sempre

Una delle proprietà più importanti — e per molti versi più sorprendenti — della blockchain è la sua **immutabilità**. Una volta che una transazione viene inclusa in un blocco e quel blocco viene aggiunto alla catena, quella scrittura diventa permanente. **Non può essere cancellata, modificata o revocata da nessuno.**

Questa caratteristica è al tempo stesso il **punto di forza assoluto** e il **vincolo più importante** della tecnologia. È il punto di forza perché garantisce l'**integrità del registro in modo matematico**, non fiduciario: non si tratta di fidarsi di un'istituzione che promette di non alterare i dati, ma di avere la certezza matematica che quei dati non possono essere alterati. È un vincolo perché significa che **eventuali errori** — un indirizzo di destinazione sbagliato, una transazione non voluta — **non possono essere corretti a posteriori.**

> Questa **irreversibilità** è il motivo per cui la comprensione della tecnologia precede qualsiasi operazione su di essa. Chi agisce sulla blockchain senza capire cosa sta facendo non ha rete di sicurezza.

6. La pseudonimia: privacy senza anonimato

Le vere blockchain sono **pubbliche** e **permissionless**: chiunque può partecipare senza chiedere il permesso a nessuno e chiunque può consultare l'intero registro delle transazioni. Questo potrebbe far pensare a un sistema in cui ogni movimento è visibile con tanto di nome e cognome. La realtà è più sfumata e il concetto che la descrive è quello di pseudonimia.

Gli utenti non operano sulla blockchain con il proprio nome reale. Operano attraverso indirizzi alfanumerici — sequenze di lettere e numeri generate crittograficamente — che fungono da pseudonimi. Una transazione tipica sulla blockchain di Bitcoin appare come un movimento di fondi da un indirizzo a un altro: nessun nome, nessun documento di identità, nessun riferimento anagrafico.

Pseudonimia ≠ Anonimato

La blockchain nasconde il nome, ma **non elimina la possibilità di identificazione**. Se un indirizzo viene associato a una persona reale — attraverso un exchange che richiede documenti di identità, attraverso analisi comportamentali o attraverso semplici errori di igiene digitale — tutta la storia delle transazioni legate a quell'indirizzo può essere ricostruita con precisione. **La protezione della privacy dipende da come si usano wallet, exchange e dati personali**.

Questa distinzione ha implicazioni pratiche molto concrete per chiunque operi con criptovalute. Le analisi on-chain sono oggi una disciplina sofisticata, utilizzata sia da autorità fiscali e investigative, sia da aziende private specializzate. Il registro pubblico è, per definizione, consultabile da chiunque abbia gli strumenti per farlo.

7. Da Bitcoin a Ethereum: l'intelligenza programmabile

Per i suoi primi anni di vita, Bitcoin è rimasto il paradigma unico della blockchain: un sistema per trasferire valore digitale in modo sicuro, decentralizzato e senza intermediari. Poi, nel 2015, è arrivato Ethereum a ridisegnare il perimetro di ciò che era possibile.

L'architettura di base è la stessa di **Bitcoin**: blocchi, nodi, registro distribuito, algoritmo di consenso. La differenza fondamentale è una sola, ma cambia tutto: **Ethereum** è una blockchain programmabile. Introduce la possibilità di eseguire programmi direttamente sulla rete distribuita. **Questi programmi si chiamano smart contract.**

Gli smart contract

Un smart contract è **codice che vive sulla blockchain**. Non è un contratto nel senso legale tradizionale — è un **programma**. Un programma che si esegue automaticamente quando si verificano determinate condizioni predefinite, senza bisogno di alcun intervento umano e senza possibilità di interferenza esterna.

La caratteristica fondamentale degli smart contract è la loro **incorruttibilità**: il **codice è visibile** a tutti, le **regole sono uguali** per tutti e l'**esecuzione è automatica**. Non c'è spazio per l'interpretazione discrezionale, per la corruzione o per l'errore umano nell'esecuzione. Una volta pubblicato sulla blockchain, lo smart contract fa esattamente quello per cui è stato scritto.

Un esempio concreto: l'affitto digitale

Per rendere tangibile il concetto, consideriamo un esempio pratico: l'**affitto di un appartamento gestito interamente da uno smart contract**.

1. L'**inquilino invia l'importo dell'affitto alla blockchain**, dove viene custodito in modo automatico dallo smart contract. I fondi non sono né dell'inquilino né del locatore finché le condizioni non si realizzano.
2. Una volta confermato il deposito, l'**inquilino riceve automaticamente una chiave digitale per accedere all'appartamento**. Nessuna intermediazione, nessun passaggio manuale.
3. Se entro la data stabilita **la chiave non viene inviata**, i fondi vengono **restituiti automaticamente all'inquilino**. Il contratto si annulla da solo, senza contestazioni.
4. Se **la chiave viene consegnata**, **i fondi vengono rilasciati automaticamente al locatore**. La chiave rimane valida esattamente per il periodo concordato, poi si disattiva.

> Nessun agente immobiliare. Nessun notaio. Nessuna fiducia cieca nell'altra parte. Lo smart contract agisce come un **intermediario neutrale**, automatico e trasparente: esegue esattamente quello per cui è stato programmato, né più né meno. Ogni passaggio è registrato sulla blockchain e verificabile da chiunque.

Gli smart contract sono alla base di applicazioni che oggi operano con miliardi di dollari in valore: finanza decentralizzata, mercati di asset digitali, sistemi di governance distribuita, emissione di token. Ma la logica sottostante è sempre quella dell'esempio dell'affitto: condizioni predefinite, esecuzione automatica, nessun intermediario

8. Le tipologie di blockchain: un ecosistema diversificato

Non tutte le blockchain sono uguali. Esiste una **classificazione fondamentale** che è importante conoscere, perché le differenze tra i tipi di blockchain ne determinano profondamente le possibili applicazioni.

- **Pubblica e permissionless**

  Chiunque può partecipare come nodo o come utente senza autorizzazione. Massima decentralizzazione. Esempi: Bitcoin, Ethereum.

- **Privata**

  L'accesso è controllato da un'entità centrale. Usata in ambito enterprise per applicazioni interne. Meno decentralizzata, più controllabile.

- **Consortium/Ibrida**

  Gestita da un gruppo di organizzazioni. Bilancia controllo e decentralizzazione. Usata in settori regolamentati come la finanza o la sanità.

Le blockchain **pubbliche e permissionless** — Bitcoin ed Ethereum in primis — sono quelle che più si avvicinano all'ideale originario della tecnologia: **sistemi aperti**, **senza custodi**, dove le regole del gioco sono **trasparenti** e **uguali per tutti.** Le blockchain private e ibride rispondono invece a esigenze di conformità regolamentare, privacy o controllo che certi settori richiedono.

Questa distinzione conta non solo dal punto di vista tecnico, ma anche da quello economico e strategico: una blockchain privata non offre le stesse garanzie di neutralità e trasparenza di una pubblica e viceversa non ha le stesse limitazioni operative.

9. Perchè questa tecnologia è rilevante: oltre la speculazione

Il dibattito pubblico sulle criptovalute si concentra quasi sempre sui prezzi: quanto ha guadagnato chi ha comprato Bitcoin nel 2015, quanto ha perso chi ha comprato nel novembre 2021. Questo è **comprensibile ma riduttivo**. I movimenti di prezzo sono la superficie, non la sostanza.

La sostanza è che la blockchain è la prima tecnologia nella storia che permette a due soggetti che non si conoscono e non si fidano reciprocamente di stabilire un accordo verificabile, immutabile e automaticamente eseguibile, senza dover ricorrere a un terzo garante — banca, notaio, stato, piattaforma tecnologica.

Le implicazioni di questo principio si estendono a un numero straordinario di domini:

- **Finanza**
  Trasferimento di valore senza intermediari bancari, accesso a servizi finanziari per popolazioni non bancarizzate, automazione di processi di clearing e settlement.

- **Proprietà e identità**
  Registrazione di titoli di proprietà immobiliare, certificati di autenticità per opere d'arte, gestione di identità digitali verificabili senza dipendenza da database centralizzati.

- **Supply chain**
  Tracciabilità di prodotti dalla produzione al consumatore finale, con verifica immutabile di ogni passaggio della filiera.

Governance

Sistemi di voto e deliberazione collettiva resistenti alla manipolazione, organizzazioni che funzionano attraverso regole codificate in smart contract anziché strutture gerarchiche tradizionali.

Contrattualistica

Automazione di accordi complessi — assicurazioni parametriche, derivati finanziari, accordi di licenza — che si eseguono automaticamente al verificarsi di condizioni misurabili.

Il punto centrale

La blockchain non è una tecnologia interessante perché Bitcoin è salito di prezzo. È una **tecnologia interessante perché risolve in modo nuovo e generale il problema della fiducia in contesti dove le parti non si conoscono**. Questo problema esiste in quasi ogni settore dell'economia.

10. I rischi che non si possono ignorare

Una trattazione onesta della blockchain non può limitarsi al potenziale senza esaminare i rischi reali. Questi esistono, sono significativi e ignorarli sarebbe un disservizio verso chiunque voglia approcciarsi a questo campo con serietà.

Volatilità

I mercati delle criptovalute sono tra i più volatili esistenti. Drawdown del 70-80% dai massimi non sono eventi eccezionali: sono accaduti più volte nella storia di Bitcoin ed Ethereum. Chi non è in grado di tollerare psicologicamente e finanziariamente questo livello di volatilità non dovrebbe esporsi a questi asset.

Rischio tecnico e di custodia

La blockchain è sicura come sistema. Ma la custodia degli asset digitali introduce rischi specifici: **wallet compromessi**, **chiavi private perse**, **exchange hackerati o falliti**. La responsabilità della sicurezza è interamente in capo all'utente. Non esiste un call center a cui chiedere il ripristino della password. Non esiste un fondo di garanzia. L'irreversibilità delle transazioni significa che **gli errori sono definitivi**.

Rischio regolamentare

Il **quadro normativo** sulle criptovalute è in evoluzione in tutti i principali paesi. Quello che è legalmente possibile oggi potrebbe essere soggetto a vincoli significativi domani. In Europa, il **regolamento MiCA** ha introdotto un **framework più chiaro**, ma l'implementazione è in corso e molte questioni rimangono aperte. Chi investe in questo spazio deve monitorare l'evoluzione regolamentare.

Scam e progetti inconsistenti

Il settore crypto ha attratto una quantità straordinaria di progetti **fraudolenti** o semplicemente privi di fondamenta solide. La capacità di distinguere tra un progetto serio e uno speculativo — o peggio, un'operazione truffaldina — richiede competenza tecnica ed economica. L'entusiasmo del mercato non è una garanzia di solidità.

Rischio e consapevolezza

Conoscere i rischi non significa evitare la tecnologia. **Significa approcciarla con gli occhi aperti**, con una valutazione consapevole di quello che si sta facendo e di quanto si è disposti a perdere. **La consapevolezza è la migliore forma di protezione.**

Conclusioni: la superficie di una rivoluzione

Blocchi, nodi, consenso, immutabilità, pseudonimia, smart contract.
Questi non sono termini tecnici da memorizzare: sono i mattoni concettuali di un nuovo modo di organizzare la fiducia e lo scambio economico in ambiente digitale.

Bitcoin ha dimostrato che è possibile trasferire valore in modo sicuro e verificabile senza intermediari. **Ethereum** ha dimostrato che è possibile automatizzare accordi complessi in modo trasparente e incorruttibile. Le blockchain di terza generazione stanno dimostrando che questo è possibile con velocità e costi operativi compatibili con applicazioni di massa.

Siamo ancora in una **fase di costruzione dell'infrastruttura**. Molte applicazioni che oggi sembrano promettenti non sopravviveranno alla selezione del mercato. Alcune che sembrano di nicchia diventeranno standard. La capacità di navigare questo territorio — cogliere le opportunità reali, evitare le insidie, distinguere la sostanza dal rumore — richiede una **comprensione progressiva e aggiornata**.

I concetti esplorati qui sono il punto di partenza. I passi successivi — custodia degli asset digitali, tokenizzazione, smart contract applicati, integrazione con l'intelligenza artificiale — richiedono lo stesso approccio: comprensione dei meccanismi prima delle decisioni. Il **percorso formativo** di FPC Academy è costruito esattamente su questa logica, con tre moduli progressivi per chi vuole andare oltre la superficie.

Lo scenario che ci attende

Capire la blockchain **non è un'opzione per pochi specialisti**. È una competenza destinata a diventare, nei prossimi anni, parte del bagaglio culturale di qualsiasi professionista che operi in economia, finanza, diritto o tecnologia.

About

First Personal Coin è uno **studio professionale** guidato da Mariano Carozzi, già promotore di Prestiamoci, prima piattaforma di P2P lending in Italia, e Chairman di Young Platform, con oltre vent'anni in ambito bancario e finanziario, affiancato da un team con background dirigenziale e consulenziale in ambiti finanziari, legali e tecnologici.

Le nostre **aree di lavoro** sono tre:

- **Progettazione** e **sviluppo** di piattaforme su blockchain per gestire governance condivisa, **transazioni** tra controparti e **tracciabilità** di filiera (DAO);
- **Consulenza** strategica e normativa su asset digitali e registri distribuiti, con un approccio compliance-first su MiCAR;
- **Formazione professionale** per chi opera in settori dove queste tecnologie stanno diventando infrastruttura.