REPORT DI APPROFONDIMENTO

Blockchain e Tokenizzazione degli Asset Finanziari

Smart contract e il futuro dei mercati dei capitali

Analisi indipendente sull'evoluzione della blockchain nella finanza istituzionale

Agosto 2026

Indice

Sintesi esecutiva

Negli ultimi anni la blockchain è passata dall'essere associata quasi esclusivamente alle criptovalute a diventare oggetto di investimenti significativi da parte delle principali istituzioni finanziarie mondiali. Il tema centrale di questa trasformazione è la **tokenizzazione degli asset**: azioni, obbligazioni, fondi, depositi bancari e collaterale (attivi dati in garanzia) possono oggi essere rappresentati mediante token digitali, la cui gestione viene automatizzata attraverso gli smart contract.

Questo report ricostruisce l'intero percorso di questa evoluzione: dal fallimento del progetto pionieristico dell'Australian Securities Exchange nel 2016, fino all'attuale fase di maturità tecnologica e regolamentare. Vengono analizzati i meccanismi tecnici della tokenizzazione, il funzionamento degli smart contract, il ruolo di stablecoin, deposit token e CBDC, e le infrastrutture — oracoli, bridge, staking — che rendono possibile l'utilizzo delle blockchain pubbliche in ambito finanziario.

Una parte centrale dell'analisi è dedicata al tema della **decentralizzazione**, mostrando come questa non sia una proprietà binaria ma multidimensionale, e confrontando in dettaglio le scelte progettuali di Bitcoin ed Ethereum. La conclusione principale è che l'adozione istituzionale della blockchain non rappresenta l'affermazione del paradigma *trustless* originario, bensì una **evoluzione delle infrastrutture dei mercati finanziari esistenti**, nella quale la fiducia viene ridistribuita tra protocolli informatici, smart contract e istituzioni regolamentate.

La tokenizzazione non rappresenta una rivoluzione nel significato originariamente attribuito alla blockchain da Bitcoin, bensì una profonda evoluzione delle infrastrutture dei mercati finanziari.

1. Introduzione

Negli ultimi anni la tecnologia blockchain è passata dall'essere considerata un'innovazione marginale, strettamente associata al mondo delle criptovalute, a rappresentare una delle aree di maggiore interesse per le principali istituzioni finanziarie mondiali. Banche d'investimento, gestori patrimoniali, infrastrutture di mercato e autorità di regolamentazione stanno infatti valutando come utilizzare questa tecnologia per modernizzare l'architettura dei mercati finanziari, con l'obiettivo di ridurre i costi operativi, aumentare l'efficienza dei processi e consentire la negoziazione di strumenti finanziari in modo continuo e automatizzato.

Questa evoluzione rappresenta un cambiamento significativo rispetto alla percezione che il settore aveva maturato negli anni successivi alla nascita di Bitcoin. Per oltre un decennio la blockchain è stata generalmente identificata con le criptovalute e con la forte volatilità che ha caratterizzato tali mercati. Le numerose crisi che hanno interessato il settore, il fallimento di importanti operatori e l'assenza di un quadro regolamentare sufficientemente definito hanno contribuito a mantenere le istituzioni finanziarie tradizionali su posizioni prudenti: la tecnologia veniva spesso considerata promettente sul piano teorico, ma ancora immatura per applicazioni sistemiche nei mercati regolamentati.

Negli ultimi anni questo scenario è progressivamente cambiato. L'evoluzione normativa in numerose giurisdizioni, l'interesse crescente delle banche centrali per le valute digitali, la diffusione delle stablecoin e soprattutto lo sviluppo della cosiddetta **tokenizzazione degli asset finanziari** hanno riportato la blockchain al centro dell'attenzione degli operatori istituzionali. In particolare, l'interesse della finanza tradizionale non riguarda tanto le criptovalute come nuova classe di investimento, quanto la possibilità di utilizzare l'infrastruttura blockchain per rappresentare digitalmente strumenti finanziari già esistenti e automatizzarne il ciclo di vita.

Numerose istituzioni finanziarie — tra cui grandi banche internazionali, gestori patrimoniali, borse valori e società che gestiscono le infrastrutture di clearing e settlement — stiano investendo centinaia di milioni di dollari nello sviluppo di piattaforme basate su blockchain. Secondo gli autori, tale fenomeno potrebbe trasformare profondamente il funzionamento dei mercati finanziari, rendendo possibile la negoziazione continua degli strumenti finanziari, l'automazione di numerosi processi amministrativi e una significativa riduzione dei tempi di regolamento delle operazioni.

Tuttavia, la crescente attenzione verso la blockchain non implica necessariamente l'adozione della filosofia originaria che ha ispirato la nascita di Bitcoin. Il progetto elaborato da Satoshi Nakamoto nel 2008 aveva come obiettivo la creazione di un sistema monetario **trustless**, cioè capace di funzionare senza la necessità di intermediari centrali. La blockchain utilizzata oggi dalla finanza istituzionale persegue invece finalità differenti: banche, gestori patrimoniali ed emittenti continuano a svolgere un ruolo centrale nell'emissione, nella custodia e nella gestione degli strumenti finanziari. Ciò che cambia è principalmente l'infrastruttura tecnologica utilizzata per registrare la proprietà degli asset e automatizzare alcuni processi operativi.

In questo senso, la blockchain non sostituisce il sistema finanziario esistente, ma si propone come una possibile evoluzione delle sue infrastrutture. L'innovazione non consiste nell'eliminazione degli intermediari, bensì nella loro integrazione all'interno di un ecosistema digitale caratterizzato da maggiore programmabilità, maggiore interoperabilità e tempi di esecuzione significativamente inferiori rispetto alle architetture tradizionali.

L'obiettivo di questo report è analizzare criticamente tale evoluzione, illustrando i principi della tokenizzazione degli asset finanziari, il ruolo degli smart contract, le caratteristiche delle principali blockchain pubbliche e i rischi tecnologici e sistemici associati alla loro crescente diffusione nei mercati finanziari.

2. Dalla crisi del progetto ASX alla nuova fase della tokenizzazione

L'attuale entusiasmo nei confronti della blockchain contrasta con quanto avvenuto soltanto pochi anni prima. Uno degli episodi più significativi nella storia dell'applicazione della tecnologia blockchain ai mercati finanziari è rappresentato dal progetto avviato nel 2016 dalla **Australian Securities Exchange (ASX)**.

All'epoca l'ASX annunciò l'intenzione di sostituire il proprio sistema di clearing e settlement, noto come CHESS (*Clearing House Electronic Subregister System*), con una nuova infrastruttura basata su tecnologia blockchain. L'iniziativa fu presentata come un progetto pionieristico e ricevette un'enorme attenzione mediatica, poiché avrebbe rappresentato il primo caso al mondo di una grande borsa valori nazionale che adottava un registro distribuito come infrastruttura centrale del proprio mercato.

Le aspettative erano elevate: si riteneva che la blockchain avrebbe consentito di semplificare il regolamento delle operazioni, ridurre il numero di intermediari coinvolti nei processi post-trading, migliorare la trasparenza e diminuire i costi operativi per tutti i partecipanti al mercato.

Il progetto, tuttavia, incontrò rapidamente difficoltà molto superiori alle previsioni iniziali. Nel corso dello sviluppo emersero problemi di natura tecnica, organizzativa e gestionale: la piattaforma non risultò in grado di garantire le prestazioni richieste da un'infrastruttura nazionale ad alta intensità di transazioni, mentre la complessità dell'integrazione con i sistemi esistenti venne sottovalutata. A questi aspetti si aggiunsero criticità nella governance del progetto e nella gestione dei rapporti con gli operatori di mercato.

170 milioni AUD

Investimenti svalutati integralmente dall'ASX dopo la cancellazione del progetto

Dopo anni di ritardi e numerose revisioni progettuali, il progetto venne definitivamente cancellato (destino comune a molti software di una certa complessità). L'ASX fu costretta a svalutare integralmente gli investimenti sostenuti, pari a circa 170 milioni di dollari australiani, e successivamente ricevette anche una sanzione per aver fornito al mercato informazioni considerate fuorvianti sullo stato di avanzamento del progetto. L'episodio venne interpretato da molti osservatori come la dimostrazione che la blockchain non fosse ancora sufficientemente matura per costituire l'infrastruttura portante di un grande mercato regolamentato.

A distanza di dieci anni il contesto appare profondamente diverso. Non è cambiata soltanto la tecnologia, ma soprattutto l'intero ecosistema entro cui essa opera: le autorità di vigilanza hanno progressivamente definito regole specifiche per gli asset digitali, numerose banche centrali hanno avviato sperimentazioni sulle valute digitali, il mercato delle stablecoin ha raggiunto dimensioni rilevanti e sono nate nuove infrastrutture dedicate alla tokenizzazione degli strumenti finanziari.

Anche la concorrenza ha contribuito ad accelerare questo cambiamento. Gli exchange di criptovalute non si limitano più alla negoziazione di asset digitali, ma puntano a offrire servizi finanziari sempre più simili a quelli tradizionali, entrando progressivamente nel mercato delle azioni, delle obbligazioni e di altri strumenti finanziari. Le infrastrutture storiche dei mercati hanno quindi iniziato a considerare la blockchain non più

come una minaccia esterna, bensì come una tecnologia da integrare nei propri sistemi per mantenere la competitività.

Il fallimento del progetto ASX non viene quindi più interpretato come il fallimento della blockchain in sé, ma come il risultato di una tecnologia introdotta in un contesto ancora prematuro, caratterizzato da limitata maturità tecnologica, scarsa standardizzazione e assenza di un quadro regolamentare sufficientemente definito.

3. Che cos'è la tokenizzazione

Il concetto centrale della nuova strategia adottata da Wall Street è la **tokenizzazione degli asset finanziari**. Questo termine indica il processo mediante il quale un'attività reale o un diritto economico viene rappresentato digitalmente attraverso un **token** registrato su una blockchain.

Dal punto di vista tecnico, un token è un'unità informatica che identifica un determinato diritto patrimoniale e ne consente il trasferimento tra soggetti diversi mediante la registrazione delle transazioni su un registro distribuito. Diversamente dalle criptovalute native, come Bitcoin o Ether, il token non costituisce necessariamente un nuovo strumento finanziario, ma rappresenta la versione digitale di un'attività già esistente.

Categorie di asset tokenizzabili

Possono essere tokenizzati praticamente tutti gli strumenti finanziari negoziabili. La tabella seguente ne riassume le principali categorie.

Categoria	Esempi
Strumenti di capitale	Azioni, ETF, quote di fondi comuni, fondi alternativi
Strumenti di debito	Obbligazioni, strumenti del mercato monetario, crediti commerciali
Depositi e liquidità	Depositi bancari, collaterale in operazioni repo
Asset reali	Materie prime, immobili, quote di fondi immobiliari
Strumenti derivati	Derivati OTC e strumenti collegati a indici o materie prime

Tabella 1. Attivi e passivi tokenizzabili.

La tokenizzazione non modifica la natura economica dello strumento finanziario sottostante. Un'obbligazione tokenizzata continua ad attribuire gli stessi diritti patrimoniali dell'obbligazione tradizionale; un'azione tokenizzata continua a rappresentare una partecipazione nel capitale sociale dell'emittente. Ciò che cambia è il modo in cui tali diritti vengono registrati, trasferiti e amministrati.

Nei sistemi tradizionali la proprietà degli strumenti finanziari viene gestita attraverso una complessa rete di intermediari composta da banche depositarie, central securities depositories (CSD), clearing house, transfer agent, registrar e paying agent. Ogni trasferimento richiede una serie di riconciliazioni tra registri differenti, con conseguenti costi operativi e tempi di regolamento che, sebbene notevolmente ridotti negli ultimi anni, rimangono ancora superiori a quelli teoricamente ottenibili mediante un'infrastruttura distribuita.

La tokenizzazione propone un paradigma differente: il registro distribuito diventa il punto di riferimento unico per la rappresentazione della proprietà degli strumenti finanziari e per la registrazione delle operazioni. In linea teorica, questo approccio consente di ridurre il numero delle riconciliazioni, semplificare il processo di settlement e creare strumenti finanziari direttamente programmabili attraverso gli smart contract, che saranno analizzati nella sezione successiva.

È importante sottolineare che la tokenizzazione non implica necessariamente l'utilizzo di blockchain completamente pubbliche e permissionless. Molte iniziative promosse dalle istituzioni finanziarie utilizzano infatti registri distribuiti autorizzati (*permissioned distributed ledger*), nei quali l'accesso alla validazione delle

transazioni è riservato a soggetti previamente identificati. In altri casi vengono invece utilizzate blockchain pubbliche, come Ethereum, sulle quali vengono emessi token rappresentativi di attività finanziarie reali.

Questa distinzione è fondamentale perché evidenzia come la tokenizzazione non coincida con la decentralizzazione assoluta. La maggior parte dei progetti sviluppati dalla finanza tradizionale mantiene infatti un forte controllo sugli emittenti, sugli intermediari e sulle procedure di conformità normativa, utilizzando la blockchain principalmente come infrastruttura tecnologica più efficiente e programmabile. In altre parole, l'innovazione non consiste nell'eliminazione della fiducia verso gli intermediari, bensì nella digitalizzazione e nell'automazione dei processi mediante una nuova generazione di registri distribuiti.

4. Gli smart contract: il vero motore della tokenizzazione

Se la blockchain costituisce l'infrastruttura sulla quale vengono registrati gli strumenti finanziari tokenizzati, gli **smart contract** rappresentano il meccanismo che rende tali strumenti realmente programmabili. È proprio questa programmabilità, più ancora dell'utilizzo di un registro distribuito, a costituire l'elemento di maggiore interesse per la finanza istituzionale.

Gli smart contract sono programmi che eseguono automaticamente determinate operazioni quando si verificano condizioni prestabilite. Esempi di tali operazioni in ambito finanziario sono: il pagamento automatico dei dividendi, il regolamento delle operazioni di compravendita, l'erogazione di prestiti e l'esecuzione automatica di altre attività normalmente svolte dagli intermediari finanziari. Questa definizione è corretta, ma rappresenta soltanto una parte del loro reale significato.

4.1 Origine del concetto

Contrariamente a quanto spesso si pensa, il concetto di smart contract è precedente alla nascita della blockchain. Nel 1994 il crittografo e informatico **Nick Szabo** introdusse l'idea di un contratto capace di eseguire automaticamente determinate clausole senza richiedere l'intervento di un intermediario, con l'obiettivo di trasformare alcune obbligazioni contrattuali in codice informatico. All'epoca, tuttavia, mancava un'infrastruttura distribuita capace di garantire che il programma fosse eseguito contemporaneamente da tutti i partecipanti senza la necessità di un'autorità centrale.

La nascita di Bitcoin nel 2008 risolse il problema del consenso distribuito, ma offrì soltanto un linguaggio di scripting volutamente limitato. Con Ethereum, introdotta nel 2015, il concetto di smart contract trovò finalmente una piattaforma sufficientemente flessibile da consentire la realizzazione di programmi complessi direttamente sulla blockchain. Da quel momento la blockchain cessò di essere soltanto un registro distribuito delle transazioni e divenne una vera piattaforma di elaborazione distribuita.

4.2 Che cos'è realmente uno smart contract

Dal punto di vista informatico, uno smart contract è un **programma deterministico** registrato sulla blockchain ed eseguito simultaneamente da tutti i nodi validatori della rete. L'aggettivo *deterministico* riveste un'importanza fondamentale: a parità di dati in ingresso, ogni nodo deve necessariamente produrre il medesimo risultato. Questa proprietà garantisce che nessun nodo possa modificare unilateralmente l'esito dell'elaborazione, che tutti i partecipanti condividano lo stesso stato del sistema e che il registro distribuito rimanga coerente.

Lo smart contract diventa quindi parte integrante della blockchain e ne eredita le principali caratteristiche: immutabilità, trasparenza, verificabilità, tracciabilità ed esecuzione distribuita. È importante osservare che il termine "contratto" può risultare fuorviante: nella maggior parte dei casi lo smart contract **non sostituisce il contratto giuridico**, bensì ne automatizza l'esecuzione. Il contratto legale continua infatti ad esistere; lo smart contract implementa la logica operativa necessaria affinché alcune clausole vengano applicate automaticamente. In altre parole, il codice non sostituisce il diritto, ma ne automatizza l'applicazione.

4.3 Una macchina a stati

Dal punto di vista dell'ingegneria del software, uno smart contract può essere interpretato come una **macchina a stati finiti (Finite State Machine)**. Ogni strumento finanziario attraversa infatti una successione di stati durante il proprio ciclo di vita: per esempio, un'obbligazione può evolvere secondo la sequenza illustrata di seguito.

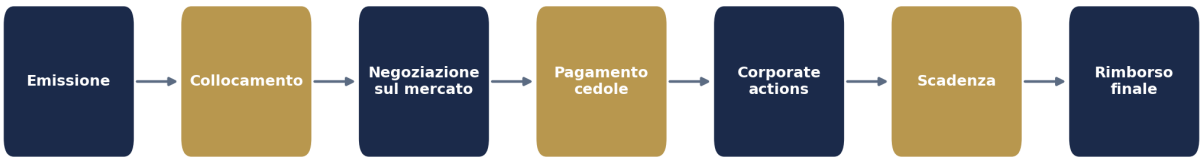

Figura 1. Ciclo di vita di un'obbligazione tokenizzata come macchina a stati finiti.

Ogni transizione tra due stati viene attivata automaticamente quando si verifica un determinato evento. Lo smart contract controlla tali transizioni applicando le regole definite al momento dell'emissione dello strumento: in pratica, il comportamento dell'obbligazione diventa parte integrante del titolo stesso. Questa rappresenta probabilmente la principale innovazione introdotta dalla tokenizzazione.

4.4 Gli smart contract nei mercati finanziari

Nei mercati finanziari tradizionali una singola operazione coinvolge generalmente numerosi soggetti: banca depositaria, broker, clearing house, central securities depository (CSD), transfer agent, registrar, paying agent, amministratore del fondo e società di gestione. Ognuno di essi svolge specifiche attività operative, molte delle quali consistono semplicemente nell'applicazione di regole perfettamente codificabili. Gli smart contract consentono quindi di incorporare tali regole direttamente nello strumento finanziario.

Ad esempio, un'obbligazione tokenizzata potrebbe:

- calcolare automaticamente gli interessi;
- verificare la data di pagamento della cedola;
- trasferire automaticamente il denaro agli investitori;
- aggiornare il registro dei possessori;
- effettuare il rimborso finale alla scadenza.

Analogamente, un ETF tokenizzato potrebbe:

- verificare periodicamente la composizione dell'indice;
- calcolare automaticamente il nuovo portafoglio;
- generare gli ordini di ribilanciamento;
- aggiornare il valore patrimoniale netto (NAV).

Lo stesso principio può essere applicato a fondi comuni, prestiti sindacati, operazioni repo, derivati OTC e numerosi altri strumenti. Proprio questa programmabilità rappresenta uno dei principali motivi dell'interesse mostrato oggi dal mondo della finanza verso la blockchain.

4.5 I vantaggi economici

L'introduzione degli smart contract produce vantaggi che vanno ben oltre la semplice automazione. Tra i principali benefici si possono evidenziare:

- riduzione dei tempi di regolamento;
- diminuzione delle riconciliazioni tra sistemi differenti;
- eliminazione di numerosi processi manuali;
- riduzione degli errori operativi;

- maggiore trasparenza delle operazioni;
- riduzione del rischio operativo;
- possibilità di negoziazione continua 24 ore su 24.

Da un punto di vista economico, gli strumenti finanziari cessano quindi di essere semplici rappresentazioni digitali di un diritto patrimoniale e diventano **strumenti finanziari programmabili** (*programmable financial assets*). Questa trasformazione potrebbe modificare profondamente il funzionamento delle infrastrutture di mercato nei prossimi anni.

4.6 I limiti degli smart contract

L'automazione completa introduce tuttavia nuove criticità. Un programma esegue esclusivamente ciò che è stato scritto nel codice: se il codice contiene un errore, l'errore verrà replicato automaticamente da tutti i nodi della rete. Inoltre, una volta distribuito sulla blockchain, uno smart contract può risultare molto difficile da modificare — una differenza sostanziale rispetto ai sistemi informativi tradizionali, nei quali gli errori software possono generalmente essere corretti mediante aggiornamenti centralizzati. Nel caso della blockchain, la correzione può richiedere nuove versioni del contratto oppure, nei casi più estremi, modifiche al protocollo della rete.

Esiste inoltre un secondo problema, ancora più rilevante: l'automazione elimina quella discrezionalità che caratterizza oggi molte decisioni operative. Durante una crisi finanziaria, ad esempio, una banca può decidere di concedere più tempo a una controparte prima di procedere all'escussione delle garanzie; uno smart contract non possiede questa flessibilità e, se le condizioni previste risultano soddisfatte, eseguirà automaticamente l'azione prevista. Per questo motivo il Fondo Monetario Internazionale e la Banca Centrale Europea hanno evidenziato come un'eccessiva automazione possa amplificare il rischio sistemico, soprattutto quando riguarda processi critici come il regolamento delle operazioni o le margin call.

5. Stablecoin e denaro tokenizzato

La tokenizzazione degli strumenti finanziari richiede inevitabilmente anche la disponibilità di una forma di **moneta digitale** con cui effettuare il regolamento delle operazioni. In un mercato tradizionale, infatti, ogni compravendita comporta due trasferimenti simultanei: quello della proprietà dello strumento finanziario e quello del denaro. Se il primo viene tokenizzato mentre il secondo continua a utilizzare i circuiti bancari tradizionali, i vantaggi della blockchain risultano inevitabilmente limitati. Per questa ragione il segmento oggi più sviluppato della tokenizzazione riguarda il **denaro tokenizzato**.

Forma di moneta tokenizzata	Emittente	Caratteristiche principali
Stablecoin	Soggetti privati	Ancorate al valore di una valuta legale; trasferimenti istantanei, operative 24/7
Deposit token	Banche commerciali	Depositi bancari tokenizzati; mantengono il legame diretto con il sistema bancario esistente
CBDC	Banche centrali	Valute digitali di banca centrale; ancora in fase di studio o sperimentazione nella maggior parte delle giurisdizioni

Tabella 2. Esempi di denaro tokenizzato (esistenti o in fase di realizzazione).

Le stablecoin costituiscono oggi il mercato più sviluppato: consentono trasferimenti praticamente istantanei e possono essere utilizzate ventiquattro ore al giorno, sette giorni su sette, superando i limiti temporali dei tradizionali sistemi di pagamento. La loro diffusione è uno dei fattori che ha contribuito a riaccendere l'interesse delle istituzioni finanziarie verso la blockchain, poiché permette di immaginare un ecosistema nel quale strumenti finanziari e denaro vengono regolati sulla medesima infrastruttura distribuita.

Anche numerose banche stanno sperimentando i **deposit token**, che presentano il vantaggio di mantenere il rapporto diretto con il sistema bancario tradizionale e con il quadro regolamentare esistente. Le **CBDC**, invece, sono ancora in fase di studio o di sperimentazione nella maggior parte delle giurisdizioni e il loro sviluppo procede con velocità differenti a seconda delle scelte delle rispettive banche centrali.

Dal punto di vista economico, il denaro tokenizzato rappresenta il complemento naturale della tokenizzazione degli asset: senza una forma di pagamento nativamente digitale, infatti, il processo di regolamento continuerebbe a dipendere da infrastrutture esterne, limitando buona parte dei benefici attesi dalla nuova architettura dei mercati finanziari.

6. Fondi monetari tokenizzati e nuovi strumenti finanziari digitali

Uno degli sviluppi più interessanti della tokenizzazione riguarda i **fondi monetari tokenizzati** (*Tokenized Money Market Funds — TMMF*), oggi considerati una delle applicazioni più mature della blockchain nel settore finanziario.

I fondi monetari tradizionali investono prevalentemente in strumenti a breve termine caratterizzati da elevata qualità creditizia e ridotto rischio di mercato, quali titoli di Stato, depositi bancari e commercial paper, con l'obiettivo di offrire agli investitori un rendimento relativamente stabile mantenendo un elevato livello di liquidità. La tokenizzazione non modifica la politica di investimento del fondo, ma interviene sulla modalità con cui le quote vengono emesse, trasferite e amministrate: ogni quota viene rappresentata da un token registrato su blockchain, mentre l'investitore continua a detenere lo stesso diritto economico sul patrimonio del fondo.

> 16 miliardi USD

Patrimonio in fondi monetari tokenizzati nel 2025, secondo il Financial Times — in rapida crescita rispetto ai pochi miliardi degli anni precedenti

Uno degli aspetti più innovativi consiste nella possibilità di integrare direttamente nello smart contract numerose funzioni amministrative. Ad esempio, il contratto può:

- calcolare automaticamente il valore della quota;
- distribuire giornalmente il rendimento maturato;
- registrare i nuovi sottoscrittori;
- aggiornare il numero delle quote in circolazione;
- verificare il rispetto dei limiti previsti dalla normativa;
- gestire automaticamente i rimborsi.

Nei sistemi tradizionali tali operazioni richiedono normalmente l'intervento coordinato della società di gestione, dell'amministratore del fondo, della banca depositaria e del transfer agent. La tokenizzazione consente invece di incorporare una parte significativa di tali attività direttamente nella logica applicativa dello strumento.

È tuttavia importante osservare che il fondo continua ad essere gestito da una società autorizzata e soggetta alla vigilanza delle autorità competenti: la blockchain non elimina quindi il ruolo della società di gestione, ma rende più efficiente il processo amministrativo. Questa distinzione è fondamentale per comprendere l'approccio adottato dalla finanza tradizionale — la tokenizzazione non sostituisce il quadro regolamentare esistente, ma digitalizza gli strumenti finanziari mantenendo invariati i principi fondamentali di vigilanza, custodia e tutela degli investitori.

7. La tokenizzazione del collaterale

Tra le applicazioni considerate più promettenti dalle infrastrutture di mercato vi è la tokenizzazione del collaterale. Nella maggior parte delle operazioni finanziarie una delle controparti fornisce attività finanziarie come garanzia dell'adempimento dei propri obblighi: titoli di Stato, obbligazioni societarie, azioni, quote di fondi o denaro.

Il collaterale è utilizzato quotidianamente in numerosi mercati:

- operazioni pronti contro termine (repo);
- derivati OTC;
- finanziamenti garantiti;
- prestito titoli (securities lending);
- operazioni di compensazione presso le clearing house.

Nei sistemi attuali il trasferimento delle garanzie richiede una serie di verifiche amministrative e contabili che coinvolgono depositari, clearing house e banche custodi. Questo processo, pur essendo estremamente affidabile, comporta inevitabilmente tempi operativi e immobilizza capitale che potrebbe essere utilizzato in altre operazioni.

La tokenizzazione modifica radicalmente questo paradigma: il collaterale viene rappresentato mediante token registrati sulla blockchain, e lo smart contract controlla automaticamente l'esistenza della garanzia, il suo valore aggiornato, il rispetto dei margini richiesti e l'eventuale rilascio della garanzia al termine dell'operazione. In teoria, il trasferimento della garanzia può avvenire contestualmente all'esecuzione della transazione, riducendo sensibilmente i tempi di regolamento.

Proprio questo è uno degli ambiti nei quali le infrastrutture di mercato vedono il maggiore potenziale della blockchain. La Depository Trust & Clearing Corporation (DTCC), principale infrastruttura post-trading del mercato statunitense, sta sviluppando piattaforme destinate alla tokenizzazione degli strumenti custoditi presso il proprio sistema, con l'obiettivo di aumentare l'efficienza nella gestione del collaterale.

Dal punto di vista economico, il principale beneficio consiste nella possibilità di aumentare la velocità di circolazione del collaterale (*collateral velocity*): una stessa attività finanziaria potrebbe essere riutilizzata più rapidamente in operazioni successive, riducendo la quantità complessiva di capitale necessario al funzionamento del sistema finanziario.

Naturalmente, questo vantaggio introduce anche nuove criticità. Una maggiore velocità di circolazione implica infatti una maggiore interconnessione tra gli operatori e potrebbe amplificare gli effetti di eventuali crisi di liquidità. Per tale motivo la tokenizzazione del collaterale rappresenta contemporaneamente uno dei principali fattori di efficienza e una delle possibili fonti di rischio sistemico.

8. Le azioni tokenizzate e le nuove infrastrutture di mercato

L'applicazione della tokenizzazione alle azioni rappresenta probabilmente l'evoluzione più visibile per gli investitori. In linea teorica, ogni azione emessa da una società potrebbe essere rappresentata mediante un token digitale registrato su blockchain, che continuerebbe ad attribuire gli stessi diritti patrimoniali e amministrativi dell'azione tradizionale:

- diritto ai dividendi;
- diritto di voto;
- diritto di partecipazione agli aumenti di capitale;
- diritto alla quota di liquidazione.

Cambierebbe esclusivamente l'infrastruttura attraverso la quale tali diritti vengono registrati e trasferiti.

Numerose infrastrutture di mercato stanno già sviluppando piattaforme dedicate a questo nuovo modello. In particolare, il Nasdaq sta studiando sistemi nei quali le azioni possano essere emesse e negoziate direttamente su infrastrutture blockchain, consentendo una gestione automatizzata delle principali corporate actions, quali distribuzione dei dividendi, frazionamenti azionari (stock split), aumenti di capitale e operazioni straordinarie.

Dal punto di vista operativo, uno dei principali vantaggi riguarda la possibilità di integrare l'intero ciclo di vita dell'azione all'interno dello smart contract. L'emittente potrebbe programmare direttamente:

- il pagamento dei dividendi;
- la data di stacco;
- il periodo di esercizio dei diritti di opzione;
- la gestione delle assemblee;
- l'aggiornamento automatico del libro soci.

Si ridurrebbe così la necessità di mantenere registri differenti presso più intermediari.

Un ulteriore vantaggio teorico consiste nella possibilità di estendere la negoziazione oltre gli attuali orari di apertura delle borse valori: mentre oggi gli scambi sono limitati alle sessioni di mercato, una piattaforma blockchain potrebbe consentire il trasferimento dei token ventiquattro ore al giorno.

Occorre tuttavia distinguere tra la possibilità tecnica e quella regolamentare. La tecnologia (anche quella attuale) consente effettivamente una negoziazione continua, ma ciò non significa che le autorità di vigilanza, le infrastrutture di mercato o gli emittenti decidano necessariamente di adottare un modello operativo aperto ventiquattro ore su ventiquattro: la definizione degli orari di negoziazione rimane infatti una scelta organizzativa e regolamentare, indipendente dalle capacità tecnologiche della blockchain.

Anche in questo caso emerge chiaramente la differenza tra innovazione tecnologica e trasformazione istituzionale. La blockchain rende possibili nuovi modelli operativi, ma la loro effettiva adozione dipende dalle decisioni degli operatori di mercato, delle autorità di vigilanza e del quadro normativo entro il quale tali mercati continueranno a operare.

9. Oracoli, bridge e staking: i nuovi elementi dell'infrastruttura blockchain

Quando si descrive una blockchain come un sistema "decentralizzato" si tende spesso a immaginare un'infrastruttura completamente autonoma, capace di funzionare senza alcun collegamento con il mondo esterno. In realtà, le moderne blockchain pubbliche, soprattutto quelle destinate ad ospitare applicazioni finanziarie complesse, dipendono da una serie di componenti infrastrutturali aggiuntivi che svolgono un ruolo essenziale nel loro funzionamento.

Tra questi assumono particolare importanza gli **oracoli**, i **bridge** e il sistema di **staking**: tre elementi che, pur essendo spesso trascurati nelle descrizioni divulgative della blockchain, costituiscono oggi alcuni dei principali punti di attenzione sotto il profilo della sicurezza e della decentralizzazione. Comprendere il loro funzionamento è indispensabile per valutare correttamente le opportunità offerte dalla tokenizzazione e, allo stesso tempo, i nuovi rischi introdotti dall'utilizzo di blockchain pubbliche come infrastruttura dei mercati finanziari.

9.1 Gli oracoli: il collegamento tra blockchain e mondo reale

Una blockchain può essere considerata, dal punto di vista informatico, come un **sistema chiuso**: tutti i nodi della rete condividono lo stesso registro e possono elaborare esclusivamente le informazioni già presenti al suo interno. Questo garantisce coerenza e sicurezza, ma comporta anche una limitazione fondamentale — la blockchain **non conosce ciò che accade nel mondo esterno**.

Uno smart contract, ad esempio, non è in grado di sapere autonomamente quale sia il prezzo corrente di un'azione, quale sia il tasso Euribor, il fixing giornaliero dell'oro, se una nave abbia raggiunto il porto di destinazione, se un titolo abbia pagato una cedola, quale sia il tasso di cambio euro/dollaro o se una banca centrale abbia modificato i tassi ufficiali.

Per ottenere queste informazioni è necessario ricorrere a un **oracolo** (*oracle*): un'infrastruttura software che acquisisce dati dal mondo esterno, ne verifica l'attendibilità secondo procedure prestabilite e li rende disponibili agli smart contract. L'oracolo svolge quindi il ruolo di **ponte informativo** tra due ambienti che, per loro natura, non possono comunicare direttamente. Dal punto di vista concettuale, uno smart contract può essere visto come un motore decisionale, mentre l'oracolo rappresenta il sensore che gli fornisce le informazioni necessarie per prendere tali decisioni.

Ad esempio, un'obbligazione indicizzata all'Euribor: lo smart contract è perfettamente in grado di calcolare l'importo della cedola, ma non conosce il valore dell'Euribor. L'oracolo legge quotidianamente il tasso pubblicato dall'autorità competente, lo trasmette alla blockchain e lo rende disponibile allo smart contract, che può così procedere al calcolo dell'interesse. Lo stesso principio vale per numerose applicazioni finanziarie: derivati, assicurazioni parametriche, fondi indicizzati, gestione del collaterale, strumenti collegati a materie prime e strumenti climatici.

È evidente che l'affidabilità dello smart contract dipende direttamente dalla qualità delle informazioni ricevute: un oracolo che trasmetta dati errati o manipolati può compromettere il corretto funzionamento dell'intero sistema. Per questo motivo gli oracoli rappresentano oggi uno dei principali punti di fiducia (*trust assumptions*) delle blockchain pubbliche. Negli ultimi anni sono stati sviluppati sistemi che cercano di ridurre tale rischio raccogliendo simultaneamente dati provenienti da numerose fonti indipendenti e calcolandone automaticamente un valore di consenso — ciò non elimina completamente il problema, ma ne riduce significativamente la probabilità.

Dal punto di vista architetturale, quindi, una blockchain completamente decentralizzata non è sufficiente da sola per garantire un sistema interamente decentralizzato: se le informazioni esterne provengono da un numero limitato di oracoli, una parte della fiducia si concentra inevitabilmente su tali soggetti.

9.2 I bridge: collegare blockchain differenti

Un secondo elemento essenziale è costituito dai **bridge**. Le blockchain sono generalmente progettate come ecosistemi indipendenti: Bitcoin, Ethereum, Solana, Avalanche e le altre reti non condividono automaticamente il proprio stato interno, e un token esistente su Ethereum non può essere trasferito direttamente sulla blockchain di Bitcoin. Per consentire il trasferimento di attività tra blockchain differenti vengono utilizzati i bridge.

Il funzionamento può essere descritto in modo semplificato attraverso quattro fasi:

- l'utente deposita il token sulla blockchain di origine;
- il bridge blocca (lock) tale token impedendone ulteriori trasferimenti;
- sulla blockchain di destinazione viene creato (mint) un nuovo token equivalente;
- quando l'utente desidera tornare alla blockchain originaria, il token sintetico viene distrutto (burn) e quello originario viene sbloccato.

Sarebbe più intuitivo che il bridge distruggesse il token originario e ne creasse uno nuovo sulla rete di destinazione. Ma qui nascerebbe un problema nel momento in cui si dovesse fare l'operazione inversa: tornare alla rete originaria. Il bridge infatti non possiede il controllo sulla creazione dei token originari, ovvero non possiede i diritti per innescare l'esecuzione dello smart contract che crea i token nella rete originaria. Quindi il processo si bloccherebbe. Alla rete di destinazione, invece, il bridge presenta i token "bloccati" come garanzia dell'emissione di quelli nuovi che si rivela essere una garanzia adeguata perché i vecchi token non possono più circolare, seppur continuando ad esistere e ad avere un valore. Questo crea un problema di sicurezza – come vedremo tra poco – ed è per questo che si sono inventati i token "cross-cahin" nativi. Un esempio è lo standard Omnichain Fungible Token (OFT) sviluppato da LayerZero. Qui il token è progettato fin dall'origine per esistere su più blockchain e quindi può essere distrutto in una blockchain e ricreato in un'altra evitando il problema principale della "doppia circolazione".

Dal punto di vista economico il bridge non trasferisce realmente il token, ma trasferisce piuttosto il diritto economico da esso rappresentato. Questa distinzione è fondamentale: il corretto funzionamento dell'intero processo dipende infatti dal bridge stesso, e se quest'ultimo viene compromesso, anche il collegamento tra le due blockchain viene meno.

Storicamente i bridge hanno rappresentato uno dei principali obiettivi degli attacchi informatici. Numerosi tra i più gravi furti di criptovalute degli ultimi anni hanno riguardato proprio vulnerabilità presenti nei bridge piuttosto che nei protocolli blockchain sottostanti. La ragione è intuitiva: mentre compromettere una blockchain pubblica richiede generalmente risorse economiche enormi, attaccare un bridge significa colpire un'infrastruttura molto più piccola che custodisce spesso attività di valore estremamente elevato. Dal punto di vista sistemico, quindi, i bridge rappresentano uno dei principali punti di concentrazione del rischio dell'intero ecosistema blockchain.

9.3 Lo staking e il consenso Proof-of-Stake

Un terzo elemento fondamentale riguarda il meccanismo di **staking**, strettamente collegato al funzionamento delle blockchain basate sul consenso **Proof-of-Stake (PoS)**. Per comprenderne il significato è utile confrontarlo con il sistema utilizzato da Bitcoin, che protegge la propria rete mediante il **Proof-of-Work**

(PoW), nel quale migliaia di computer competono per risolvere complessi problemi crittografici: la sicurezza deriva dall'enorme quantità di energia e potenza di calcolo necessarie per alterare la blockchain.

Ethereum, invece, dal settembre 2022 utilizza il Proof-of-Stake. In questo modello la sicurezza non deriva dal consumo di energia ma dal capitale economico messo a garanzia dai partecipanti (validatori), che depositano token della rete a titolo di garanzia. Se il validatore si comporta correttamente riceve una remunerazione sotto forma di nuove commissioni di rete; se invece tenta di alterare il protocollo oppure viola le regole previste, una parte del capitale depositato può essere confiscata — un meccanismo che prende il nome di **slashing**.

Dal punto di vista economico, il Proof-of-Stake sostituisce il costo energetico del Proof-of-Work con un rischio patrimoniale: l'incentivo a comportarsi correttamente deriva quindi dalla possibilità di perdere il capitale investito.

9.4 La concentrazione dello staking

Dal punto di vista teorico il Proof-of-Stake favorisce una partecipazione aperta. Nella pratica, tuttavia, il fenomeno si presenta più complesso: la maggior parte degli investitori non dispone delle competenze tecniche necessarie per gestire direttamente un nodo validatore, e molti preferiscono quindi delegare i propri token a grandi operatori specializzati. Nascono così le piattaforme di **liquid staking**, che raccolgono i token di migliaia di investitori e li utilizzano collettivamente per partecipare al processo di validazione.

Questo modello migliora l'efficienza economica del sistema ma produce inevitabilmente una certa concentrazione del potere di validazione: una quota significativa dello staking tende infatti a concentrarsi presso un numero relativamente limitato di operatori, come Lido. Dal punto di vista della decentralizzazione questo fenomeno rappresenta uno degli aspetti più discussi dell'attuale ecosistema Ethereum: la blockchain continua ad essere distribuita tra migliaia di nodi, ma il potere economico associato al processo di validazione può risultare significativamente più concentrato.

Questo non significa che Ethereum sia centralizzata: significa piuttosto che la decentralizzazione deve essere valutata considerando non soltanto il numero dei nodi, ma anche la distribuzione del capitale, la governance del protocollo e il funzionamento delle infrastrutture complementari.

Il grafico seguente sintetizza il numero di componenti aggiuntive — oltre al protocollo di base — da cui dipende oggi la sicurezza operativa dei due principali ecosistemi:

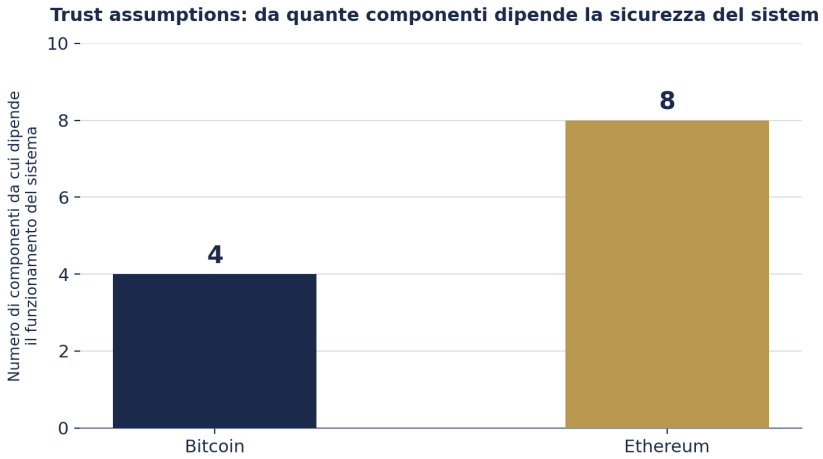

Figure 1. Numero indicativo di componenti infrastrutturali da cui dipende la sicurezza operativa dell'ecosistema (protocollo, oracoli, bridge, staking, provider RPC, layer 2, cloud, DeFi).

Questo non significa che anche le reti che adottano la PoW siano esenti dal rischio concentrazione. Per esempio la rete Bitcoin vede la partecipazione dei cosiddetti mining pool ovvero consorzi di validatori che si occupano dell'integrità della rete stessa.

9.5 La concentrazione nel mining

In teoria, Bitcoin è progettato affinché ogni miner possa partecipare indipendentemente alla validazione dei blocchi. Ogni partecipante mette a disposizione la propria potenza di calcolo (*hash rate*) e compete con tutti gli altri per risolvere il puzzle crittografico. La probabilità di trovare il blocco è proporzionale alla potenza di calcolo posseduta. In un sistema ideale, migliaia di piccoli miner indipendenti dovrebbero contribuire alla sicurezza della rete. Nella pratica, tuttavia, questo modello presenta un problema economico.

Supponiamo che un piccolo miner possieda lo 0,01% dell'hash rate mondiale. Statisticamente troverà circa:

$$144 \times 0.0001 \approx 0.0144$$

blocchi al giorno.

In altre parole, potrebbe trascorrere diversi mesi senza trovare alcun blocco, per poi trovarne improvvisamente uno. Il valore atteso del rendimento è corretto, ma la sua varianza è enorme.

Per un'impresa che deve pagare elettricità, personale e ammortamento degli ASIC (speciali macchine per implementare nel modo più efficiente possibili i calcoli di tipo *hash*), questa incertezza è difficilmente sostenibile.

Per ridurre questa volatilità sono nate le **mining pool**. Una mining pool raccoglie la potenza di calcolo di migliaia di miner. Quando la pool trova un blocco, il premio viene distribuito tra tutti i partecipanti proporzionalmente all'hash rate conferito. Dal punto di vista statistico il rendimento medio non cambia. Cambia però drasticamente il rischio. Invece di ricevere una ricompensa molto elevata una volta ogni parecchi mesi, il miner riceve piccoli pagamenti praticamente ogni giorno. Dal punto di vista economico è una forma di mutualizzazione del rischio.

Questa soluzione introduce però un nuovo rischio. Con il passare degli anni gran parte dell'hash rate mondiale si è concentrata in poche grandi mining pool. Ad esempio (i valori cambiano continuamente), può accadere che:

Mining Pool	Hash Rate
Pool A	28%
Pool B	22%
Pool C	18%
Pool D	11%

Le prime quattro pool possono quindi controllare quasi l'80% della potenza di calcolo della rete. Questo significa che il processo di costruzione dei blocchi risulta molto più concentrato di quanto suggerirebbe il numero complessivo dei miner.

Qui emerge una differenza fondamentale. Nel PoS, quando si delegano i propri token a un operatore di staking il validatore partecipa direttamente al consenso, il capitale delegato aumenta il suo potere di validazione e una quota crescente dello staking può concentrarsi presso pochi operatori. La concentrazione riguarda quindi il capitale che determina il consenso.

Nel PoW, di contro, la concentrazione presso poche mining pool delinea una situazione è più sottile. Il consorzio non possiede gli ASIC dei miner. Esso coordina semplicemente il loro lavoro. Il singolo miner può cambiare consorzio in pochi minuti. Di conseguenza la concentrazione è meno rigida rispetto al PoS. Il potere del consorzio deriva dal fatto che molti miner decidono volontariamente di collaborare.

Il vero rischio nasce quando uno o pochi consorzi controllano oltre il 50% dell'hash rate. In teoria potrebbero: censurare transazioni, rallentare la conferma di alcuni blocchi, effettuare attacchi di doppia spesa (double spending) ed impedire temporaneamente la finalizzazione di alcune transazioni.

È importante però chiarire un punto spesso frainteso. Neppure con il 51% dell'hash rate una mining pool può creare bitcoin dal nulla, modificare la politica monetaria, cambiare il limite di 21 milioni di BTC (circa) ed – infine – appropriarsi dei bitcoin appartenenti ad altri utenti. Può influenzare il processo di consenso, ma non riscrivere arbitrariamente le regole del protocollo. Tuttavia questi rischi sono – in parte – mitigati dal fatto che Bitcoin possiede un meccanismo di autodifesa economica. I miner hanno investito miliardi di dollari (spesso a debito) in infrastrutture e ASIC. Un attacco riuscito che compromettesse la fiducia nella rete provocherebbe un crollo del prezzo del bitcoin e, di conseguenza, una drastica riduzione del valore economico dell'attività di mining e dei loro investimenti. Gli incentivi economici spingono quindi i grandi consorzi a comportarsi correttamente. Inoltre, poiché i miner possono cambiare pool con relativa facilità, un pool che adottasse comportamenti ostili rischierebbe di perdere rapidamente gran parte del proprio hash rate.

Aspetto	*Proof-of-Work*	*Proof-of-Stake*
Fonte del potere	Potenza di calcolo (hash rate)	Capitale in staking
Principale rischio di concentrazione	Mining pool	Grandi operatori di staking
Facilità di migrazione	Elevata: il miner può cambiare pool rapidamente	Più limitata: dipende dal protocollo e dai periodi di unbonding
Investimento necessario	ASIC ed energia	Token della blockchain
Incentivo economico	Ricompensa per blocco e commissioni	Ricompense di staking e commissioni

Tabella 3. Confronto tra PoW e PoS.

10. Blockchain pubbliche: quanto sono realmente decentralizzate?

Numerose istituzioni finanziarie hanno scelto di sviluppare i propri progetti di tokenizzazione utilizzando blockchain pubbliche, in particolare Ethereum. Non vanno sottaciuti, tuttavia, anche alcuni elementi di criticità: tali infrastrutture dipendono da reti di validatori distribuiti e possano essere esposte a vulnerabilità informatiche che hanno causato perdite significative in diversi protocolli dell'ecosistema. Per questo motivo alcune grandi banche, come JPMorgan, preferiscono sviluppare registri distribuiti privati, mantenendo un controllo diretto sull'infrastruttura.

La questione della decentralizzazione è probabilmente uno dei temi più dibattuti dell'intero settore blockchain. Nel linguaggio comune una blockchain viene spesso definita semplicemente come "decentralizzata" oppure "centralizzata", ma questa classificazione risulta eccessivamente semplificata: la decentralizzazione non costituisce infatti una proprietà assoluta, ma un insieme di caratteristiche che riguardano differenti aspetti dell'infrastruttura.

È possibile distinguere almeno cinque dimensioni fondamentali:

Dimensione	Definizione
Consenso	Il modo in cui vengono validate le transazioni
Governance del protocollo	Il processo attraverso il quale vengono decisi gli aggiornamenti del software
Sviluppo del codice	Normalmente affidato a gruppi di sviluppatori con competenze altamente specialistiche
Distribuzione economica	La ripartizione dei token e del potere di validazione
Infrastrutture esterne	Oracoli, bridge, servizi di staking, wallet e provider cloud che rendono concretamente utilizzabile la blockchain

Tabella 4. Le differenti dimensioni della decentralizzazione.

Una rete può quindi risultare fortemente decentralizzata sotto alcuni aspetti e significativamente più concentrata sotto altri. Ethereum rappresenta un esempio particolarmente interessante di questo compromesso: dal punto di vista del consenso la rete coinvolge migliaia di validatori distribuiti geograficamente, ma dal punto di vista dello sviluppo l'evoluzione del protocollo è influenzata da un numero relativamente ristretto di sviluppatori altamente qualificati e dalla Ethereum Foundation, che svolge un ruolo importante nel coordinamento dell'evoluzione tecnica dell'ecosistema.

Anche molte delle applicazioni costruite sopra Ethereum dipendono da infrastrutture specializzate, quali oracoli, bridge e piattaforme di staking, che introducono ulteriori elementi di concentrazione. Di conseguenza, definire Ethereum semplicemente come "decentralizzata" non restituisce un'immagine completa della realtà: la rete presenta certamente un elevato grado di distribuzione rispetto ai sistemi finanziari tradizionali, ma continua a dipendere da numerosi soggetti che svolgono funzioni essenziali al suo funzionamento.

Questa osservazione è particolarmente rilevante nel confronto tra Bitcoin ed Ethereum sviluppato nella sezione seguente, dove emergerà come le differenti scelte progettuali abbiano portato alla nascita di due modelli profondamente diversi di decentralizzazione.

11. Bitcoin è davvero l'unica blockchain completamente decentralizzata?

La crescente adozione della blockchain da parte della finanza istituzionale ha riportato al centro del dibattito una domanda che accompagna questo settore fin dalla nascita di Ethereum (nel 2016): **esiste oggi una blockchain realmente decentralizzata oppure tutte le reti presentano, in misura diversa, elementi di centralizzazione?**

La risposta dipende innanzitutto dal significato attribuito al termine *decentralizzazione*. Se con questo termine si intende l'assenza di un soggetto che possa modificare unilateralmente il funzionamento della rete, censurare le transazioni o alterare arbitrariamente la storia del registro, allora Bitcoin rappresenta ancora oggi il riferimento più vicino a tale ideale. Se invece si considera la decentralizzazione come un concetto multidimensionale, comprendente governance, sviluppo software, distribuzione economica, infrastrutture esterne e capacità di evoluzione del protocollo, il quadro risulta inevitabilmente più articolato.

Per comprendere questa distinzione è necessario analizzare le differenti scelte progettuali adottate da Bitcoin ed Ethereum.

11.1 La filosofia progettuale di Bitcoin

Bitcoin nasce con un obiettivo estremamente specifico: creare un sistema monetario elettronico funzionante senza banche centrali né intermediari fiduciari. L'intero progetto riflette questa finalità — l'architettura è volutamente semplice, il linguaggio di scripting è limitato, le modifiche al protocollo vengono introdotte con estrema prudenza e la superficie di attacco è mantenuta quanto più ridotta possibile. Ogni nuova funzionalità viene valutata principalmente in funzione del suo impatto sulla sicurezza della rete.

Questo approccio ha comportato numerosi compromessi: Bitcoin non possiede smart contract complessi, non consente applicazioni decentralizzate paragonabili a quelle sviluppate su Ethereum e la sua programmabilità è limitata, tanto che molte applicazioni devono essere costruite al di fuori della blockchain principale. Tuttavia, proprio questa semplicità costituisce una delle ragioni della sua straordinaria robustezza: dopo oltre quindici anni di funzionamento continuo, la blockchain di Bitcoin non ha mai subito compromissioni del proprio protocollo di consenso.

La rete è oggi distribuita tra migliaia di nodi indipendenti localizzati in numerosi Paesi, mentre il processo di sviluppo del software è caratterizzato da un elevato livello di consenso tra sviluppatori, operatori economici e comunità degli utenti. L'assenza di una fondazione che governi il progetto rappresenta una delle principali differenze rispetto a molte altre blockchain: le modifiche vengono adottate soltanto quando una parte molto ampia dell'ecosistema decide volontariamente di installare il nuovo software, e di conseguenza il potere decisionale risulta estremamente distribuito.

11.2 L'approccio di Ethereum

Ethereum nasce con una filosofia profondamente diversa: l'obiettivo non consiste nella realizzazione di una moneta digitale, bensì nella costruzione di una piattaforma universale per applicazioni decentralizzate. Per raggiungere tale risultato il protocollo incorpora una macchina virtuale general purpose (Ethereum Virtual Machine) che consente l'esecuzione di smart contract arbitrariamente complessi — una scelta che ha favorito uno sviluppo straordinariamente rapido dell'ecosistema.

Su Ethereum sono oggi costruiti:

- protocolli di finanza decentralizzata (DeFi);
- stablecoin;
- fondi tokenizzati;
- NFT;
- sistemi di identità digitale;
- applicazioni assicurative;
- piattaforme di tokenizzazione.

La programmabilità rappresenta quindi il principale punto di forza della rete, ma comporta inevitabilmente una maggiore complessità: ogni nuovo livello funzionale aumenta il numero delle possibili vulnerabilità. Gli smart contract devono essere verificati, gli oracoli devono essere affidabili, i bridge devono essere sicuri e le piattaforme di staking devono operare correttamente. Di conseguenza, la sicurezza dell'intero ecosistema non dipende esclusivamente dal protocollo Ethereum, ma anche dall'insieme delle infrastrutture costruite sopra di esso.

Questo non costituisce necessariamente un difetto: è piuttosto la conseguenza naturale dell'obiettivo perseguito. Ethereum ha scelto di massimizzare la programmabilità; Bitcoin ha invece privilegiato la semplicità.

11.3 Un confronto tecnico

Le differenze possono essere sintetizzate nella seguente tabella.

Caratteristica	Bitcoin	Ethereum
Obiettivo principale	Moneta decentralizzata	Piattaforma programmabile
Consenso	Proof-of-Work	Proof-of-Stake
Smart contract	Molto limitati	Completi
Linguaggio di scripting	Essenziale	General purpose
Superficie di attacco	Ridotta	Maggiore
Oracoli	Generalmente non necessari	Fondamentali
Bridge	Utilizzo limitato	Ampiamente utilizzati
Governance	Molto distribuita	Più coordinata
Aggiornamenti	Molto conservativi	Più frequenti
Ecosistema applicativo	Limitato	Molto esteso

Tabella 5. Un confronto tra le principali caratteristiche di Bitcoin ed Ethereum.

La tabella evidenzia come Bitcoin ed Ethereum non rappresentino due versioni della stessa tecnologia, bensì due differenti compromessi progettuali. Bitcoin massimizza sicurezza, immutabilità e resistenza alla censura; Ethereum massimizza flessibilità, innovazione e programmabilità. Entrambi perseguono obiettivi differenti.

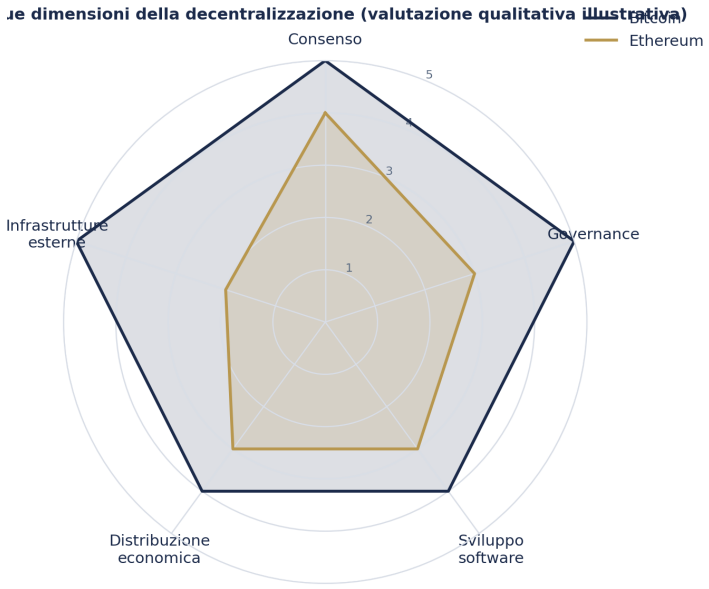

Figura 2. Confronto qualitativo e illustrativo tra Bitcoin ed Ethereum sulle cinque dimensioni della decentralizzazione discusse nel capitolo precedente (scala 1-5, valutazione indicativa basata sull'analisi qualitativa del presente report).

11.4 Una valutazione critica

Alla luce delle considerazioni precedenti è possibile formulare una riflessione più generale. Se si considera esclusivamente il protocollo di consenso, entrambe le reti possono essere considerate altamente decentralizzate. Se invece si prende in esame l'intero ecosistema operativo, emergono differenze sostanziali.

Ecosistema	Componenti da cui dipende
Bitcoin	Protocollo · Miner · Nodi · Sviluppatori
Ethereum	Smart contract · Oracoli · Bridge · Piattaforme di staking · Provider RPC · Layer 2 · Servizi cloud · Infrastrutture DeFi

Ogni nuovo componente introduce inevitabilmente nuove ipotesi di fiducia (*trust assumptions*). Per questa ragione molti ricercatori ritengono che Bitcoin rappresenti ancora oggi la blockchain pubblica maggiormente decentralizzata. Ciò non implica che Ethereum sia centralizzata: significa semplicemente che il livello complessivo di decentralizzazione deve essere valutato considerando l'intera architettura e non soltanto il protocollo di consenso.

> *Bitcoin rimane il sistema più vicino all'ideale originario di decentralizzazione concepito da Satoshi Nakamoto, mentre Ethereum rappresenta un compromesso tra decentralizzazione e programmabilità, scelto per rendere possibile un ecosistema applicativo molto più ampio.*

12. Conclusioni

L'interesse mostrato oggi da Wall Street (e dagli operatori finanziari in generale) nei confronti della blockchain rappresenta uno dei cambiamenti più significativi nella recente evoluzione dei mercati finanziari. Dopo una lunga fase durante la quale questa tecnologia era stata identificata quasi esclusivamente con le criptovalute, l'attenzione si è progressivamente spostata verso la possibilità di utilizzare registri distribuiti e smart contract per modernizzare le infrastrutture finanziarie esistenti.

Il tema centrale di questa trasformazione è la **tokenizzazione degli asset**. Azioni, obbligazioni, fondi comuni, strumenti del mercato monetario, depositi bancari e collaterale possono essere rappresentati mediante token digitali, consentendo una gestione più efficiente del loro ciclo di vita. La blockchain diventa così una piattaforma sulla quale registrare la proprietà degli strumenti finanziari, mentre gli smart contract ne automatizzano numerose funzioni operative, dal pagamento dei dividendi alla gestione delle corporate actions, fino al regolamento delle operazioni.

I benefici potenziali sono significativi. La riduzione dei tempi di settlement, la diminuzione delle riconciliazioni tra registri differenti, la programmabilità degli strumenti finanziari e la possibilità di negoziazione continua potrebbero modificare profondamente il funzionamento dei mercati dei capitali.

Tuttavia, questa evoluzione introduce anche nuove criticità. L'automazione non elimina il rischio, ma lo trasferisce dal comportamento umano al software: gli smart contract devono essere corretti, gli oracoli devono fornire dati affidabili, i bridge devono essere sicuri e le piattaforme di staking devono evitare concentrazioni eccessive del potere di validazione. Inoltre, l'incremento della velocità operativa potrebbe amplificare la propagazione degli shock finanziari, rendendo più rapida la trasmissione delle crisi di liquidità tra operatori fortemente interconnessi.

L'analisi della decentralizzazione mostra inoltre come sia necessario superare una visione semplicistica che distingue le blockchain soltanto tra "centralizzate" e "decentralizzate". La decentralizzazione è una proprietà multidimensionale che coinvolge il consenso, la governance, lo sviluppo del software, la distribuzione economica e le infrastrutture esterne. Da questo punto di vista Bitcoin ed Ethereum rappresentano due modelli profondamente differenti: il primo privilegia sicurezza, immutabilità e resistenza alla censura, mentre il secondo accetta una maggiore complessità per offrire una piattaforma altamente programmabile.

Il punto probabilmente più importante emerso nel corso di questa analisi riguarda però la natura stessa della blockchain adottata dalla finanza tradizionale. Le grandi istituzioni non stanno abbracciando il paradigma originario della **finanza trustless**, nel quale gli intermediari vengono eliminati. Al contrario, banche, gestori patrimoniali, depositari centrali, emittenti e autorità di vigilanza continueranno a svolgere un ruolo essenziale. La blockchain viene utilizzata come una nuova infrastruttura tecnologica sulla quale costruire mercati più efficienti, mantenendo però il quadro istituzionale e regolamentare esistente.

In questo senso, la tokenizzazione non rappresenta una rivoluzione nel significato originariamente attribuito alla blockchain da Bitcoin, bensì una profonda **evoluzione delle infrastrutture dei mercati finanziari**. La fiducia non viene eliminata: viene redistribuita tra protocolli informatici, smart contract e istituzioni finanziarie, dando origine a un modello ibrido nel quale innovazione tecnologica e regolamentazione convivono. È probabilmente questa, più che la diffusione delle criptovalute, la trasformazione destinata a caratterizzare il prossimo decennio dei mercati finanziari.