Antonio Viglino

Bitcoin e Ethereum.
La tokenizzazione della fiducia

La crittografia

Il termine *crypto* nell'espressione cripto-valute non ha il significato consueto connesso alla radice greca κρυπτος (*kryptos*), cioè non significa che nel mercato delle monete digitali regni il "nascosto" o vi sia qualcosa di torbido, per nulla affatto. Tutt'al contrario, il prefisso *cripto-* è una abbreviazione per *crittografiche*: le *crypto* sono così chiamate in quanto *cryptographic currencies*, in quanto consistono in un problema matematico fondato sulla crittografia che deve essere risolto da un computer, e per nessun altro motivo.
Questa distinzione semantica offre peraltro lo spunto per una delucidazione preteoretica del noto detto di Eraclito *physis kryptesthai philei*, "la natura ama nascondersi" (peraltro titolo di un testo, forse più intenso che perspicuo, di G. Colli). La natura non "ama" tanto celarsi agli occhi degli uomini, quanto piuttosto essa si mantiene trasparente a chi la possa vedere, e solo resta celata *toîs polloîs*, "ai più" che Eraclito definisce *ktēnea*, "bestie d'armento". Questa estemporanea esegesi indica come il *logos* eracliteo faccia il paio, chiudendo un cerchio che resta invisibile all'orizzonte della ragione calcolante, con nozioni in apparenza lontane ma noeticamente identiche, di Heidegger e degli *yogīn* kashmiri, per i quali il *Seyn* e rispettivamente Śiva "si danno occultandosi".
La prima *cryptographic electronic money* venne creata nel 1983; solo circa una decina d'anni dopo ne venne sfruttata in modo esplicito l'essenza crittografica quando si ebbero i primi *cryptographic electronic payments*.
Del resto, anche i conti correnti, le comunicazioni interbancarie e tutto il sistema centralizzato — così come sfere private quali i messaggi WhatsApp o l'accesso a un sito web in *https* — sono anch'essi protetti dalla crittografia.
La differenza tra la crittografia delle *crypto* e la crittografia dei sistemi informatici usuali non risiede soltanto nella maggiore complessità degli standard matematici impiegati (più elevati nelle *crypto*), ma soprattutto in questo: che la crittografia, da semplice elemento di protezione quale è nel

sistema bancario e informatico tradizionale, diventa nelle *crypto* il cuore stesso della moneta.

Questo è l'aspetto pregiudiziale per comprendere la natura delle criptovalute, e di Bitcoin in particolare, la prima e la regina delle *crypto*.

Quando si effettua un bonifico online o si invia un messaggio in chat, la crittografia serve a proteggere la trasmissione: impedisce che qualcuno intercetti i dati durante il loro transito. Una volta che il messaggio o la transazione raggiungono il server — che si tratti di una banca o di WhatsApp — l'autorità centrale gestisce, controlla e valida l'operazione. In altre parole, la crittografia assicura la privacy e la sicurezza della connessione, ma non elimina affatto la necessità di un ente fiduciario che custodisca i dati e mantenga il registro.

Nelle *crypto*, invece, non esiste alcun "server centrale" fiduciario, né un'autorità incaricata di regolamentare o garantire le transazioni. La funzione di garanzia è incorporata nella struttura stessa della *crypto* e coincide propriamente con la Blockchain, che della *crypto* è il registro nativo: un registro distribuito, decentralizzato e immutabile, che valida e registra le transazioni tramite consenso crittografico, e che costituisce lo spazio operativo — e ancor prima generativo — della *crypto* stessa.

La crittografia non serve cioè solo a proteggere la trasmissione, come avviene nei sistemi centralizzati, ma a sostituire integralmente l'intera autorità centrale.

Le *crypto* usano algoritmi crittografici per tre funzioni vitali: autenticare (ogni transazione è firmata digitalmente con una chiave privata, e solo il possessore può "spendere" i fondi); garantire l'integrità (gli *hash* assicurano che un blocco o un messaggio non sia stato alterato: una modifica anche infinitesimale produce una variazione radicale dell'*hash*); mantenere il consenso (l'intera rete concorda sullo stato del registro grazie a prove crittografiche: *proof-of-work*, *proof-of-stake*, e altre varianti).

In altre parole, la sicurezza della *crypto* è garantita puramente e semplicemente dalla matematica stessa.

E proprio questa, l'istanza per la garanzia in sé (la garanzia *autò kath'autò* avrebbe detto Platone), a costituire il momento genetico di Bitcoin.

Nell'ottobre 2008, in piena crisi finanziaria globale, un documento di nove pagine appare in una *mailing list* di crittografi: "*Bitcoin: A Peer-to-Peer Electronic Cash System*", firmato da un misterioso Satoshi Nakamoto (poi svanito, lasciando intatto un *wallet* oggi multimiliardario: non si sa se Satoshi sia un singolo genio, un collettivo di crittografi, o addirittura, come insufflano alcuni, una emanazione di una qualche agenzia governativa).

Quel *whitepaper* non proponeva soltanto una moneta digitale, ma un sistema per trasferire valore senza intermediari, basato su una catena di blocchi verificati da una rete distribuita di nodi (la *blockchain* appunto).

L'innovazione non era solo tecnica, ma programmatica nella sua stessa sostanza e, se si vuole, asintoticamente utopica: non più Banche Centrali, ma consenso distribuito, non più debito e credito gestiti da autorità, ma proprietà diretta garantita dal protocollo. Prima di Bitcoin, per trasferire denaro a distanza era necessario l'intervento di un intermediario fidato: banca, circuito di carte, società di *money transfer*. Anche i sistemi digitali più rapidi non erano mai veramente *peer-to-peer*: c'era sempre un libro mastro centrale, controllato da un ente che garantiva il saldo e aggiornava le scritture e riscuoteva commissioni.

Per altro verso, la necessità dell'intermediario per trasferire denaro a distanza è antecedente all'età digitale: un mercante di Firenze che avesse dovuto pagare un fornitore a Bruges non avrebbe portato con sé monete d'oro, esponendosi a rischi evidenti; avrebbe usato invece le lettere di cambio, documenti emessi da una banca o da una compagnia mercantile, che garantivano al beneficiario di ricevere la somma presso una filiale o un banchiere corrispondente. In altre parole, la fiducia stava nell'intermediario, non nello scambio diretto tra le parti.

Una dimensione della fiducia svincolata da ogni contingenza bensì materiata di matematica pura, invece, è il fondamento di Bitcoin, la cui portata

rivoluzionaria negli anni più recenti è stata progressivamente riconosciuta anche dai maggiori operatori finanziari.

Si può dire che Bitcoin rappresenti un nuovo passaggio epocale, analogo a quello che fu il passaggio dall'oro fisico alle lettere di credito o di assegno, dal contante alla scrittura contabile, o dalla custodia diretta alla custodia istituzionale. Con Bitcoin non viene trasformato il valore in sé, ma l'infrastruttura della sua custodia, registrazione e trasferibilità.

Secondo la narrativa più diffusa, Bitcoin è oggi detto "oro digitale": riserva di valore globale, strumento di protezione dall'inflazione, simbolo di indipendenza economica. La sua scarsità programmata ne fa un *unicum* nella storia della moneta. A differenza delle valute tradizionali, emesse da Banche Centrali che possono aumentare l'offerta per esigenze economiche o politiche, Bitcoin nasce con una regola incisa nel codice: esisteranno al massimo 21 milioni di *coin* (il pieno regime sarà raggiunto nel 2140), non uno di più. Il meccanismo di creazione è scandito nel tempo e reso trasparente dalla Blockchain. È proprio per questo motivo che di Bitcoin si dice "oro digitale": un bene che non può essere inflazionato e che può dunque agire come riserva di valore nel tempo.

Bitcoin non è solo la prima moneta decentralizzata: è la prima moneta dotata di una politica monetaria fissa, predeterminata, automatica ed incorruttibile, sottratta alle mani dell'uomo e affidata a un algoritmo condiviso e verificabile da chiunque.

Questo tratto si comprende appieno se si considera che le Banche Centrali operano da decenni in regime di moneta fiat, ossia di moneta il cui valore non deriva da una convertibilità in un sottostante reale, ma dalla fiducia istituzionale e dall'obbligo legale di accettazione. Con la fine del sistema di Bretton Woods nel 1971 e l'abbandono definitivo del vincolo della convertibilità del dollaro in oro, l'emissione monetaria è divenuta una decisione eminentemente istituzionale e discrezionale. In tale regime, l'offerta di moneta non è più ancorata a limiti materiali, ma può essere espansa o contratta in funzione delle esigenze macroeconomiche, della politica monetaria e della stabilità del sistema finanziario.

Per questo la banale obiezione secondo cui “se hai un euro hai come debitore la BCE, se hai Bitcoin non hai nessuno che te lo debba pagare” evapora non appena si riconosca che, in un sistema fiat, la garanzia non è un sottostante, bensì la fiducia sistemica nella moneta come unità di conto e mezzo di scambio — mentre Bitcoin fonda la propria garanzia su presupposti differenti e oggettivi: la matematica.

Da questo stesso meccanismo fiat discende la conseguenza strutturale per cui ogni immissione aggiuntiva di liquidità, a parità di beni e servizi, diluisce il potere d’acquisto del circolante. È questa la ragione monetaria di fondo per cui gli indici azionari mostrano, nel lungo periodo, una tendenza strutturalmente crescente: non per intrinseca bontà dei mercati, ma per il modo stesso in cui le economie di mercato sono organizzate, in quanto il denaro, in via diretta (come investimento) o indiretta (come profitto), finisce per approdare alle società quotate.

Con la conseguenza che, se in un sistema monetario fiat strutturalmente espansivo la perdita di potere d’acquisto delle divise nel lungo periodo non è un’anomalia ma una conseguenza intrinseca, allora una quota non trascurabile dell’apprezzamento delle criptovalute non va intesa come crescita “reale” del valore, ma come riflesso del progressivo deprezzamento dell’unità di conto con cui tale valore viene misurato.

La Blockchain: la catena della fiducia

Si potrebbe allora obiettare: quale sarebbe il fondamento oggettivo di Bitcoin? Le azioni rimandano a imprese, beni, servizi, flussi di cassa; le merci a oggetti materiali o a prestazioni reali. Di che cosa, dunque, Bitcoin sarebbe espressione?

Questa domanda consente di chiarire in termini perentori un equivoco di fondo. Bitcoin non possiede un fondamento materiale, né pretende di averlo. Il suo fondamento non è fisico né economico in senso tradizionale: è bensì la matematica — che ne rende possibile l’esistenza come oggetto verificabile, scarso e incorruttibile.

Parlare di matematica come fondamento non significa evocare un'astrazione disincarnata. La matematica è la forma più rigorosa di efficacia reale: ha reso possibile la costruzione di ponti e rende oggi possibile tanto la progettazione di microprocessori a scala nanometrica quanto l'esplorazione dello spazio profondo.

Nel caso di Bitcoin, la matematica è certo una matematica ad alto grado di astrazione — la crittografia — ma è un'astrazione cui è intrinsecamente connaturata la fiducia: non come sentimento, bensì come proprietà formale del sistema.

A ben vedere, del resto, anche i cosiddetti "fondamentali" degli *asset* tradizionali non consistono solo in oggetti materiali, beni o flussi di cassa, ma nella fiducia che tali elementi esistano, persistano e siano organizzati in un certo modo nel tempo. Bitcoin rende esplicito ciò che nei mercati tradizionali resta implicito: che il fondamento ultimo del valore non è la materia, ma una struttura di fiducia.

La crittografia che costituisce il fondamento matematico di Bitcoin si attua concretamente nella Blockchain: un registro digitale pubblico e decentralizzato che, dal 2009, custodisce e rende verificabili tutte le transazioni effettuate nella rete. Ed è questa stessa architettura crittografica della Blockchain— con varianti non strutturalmente decisive — a costituire il fondamento di tutte le *cryptocurrencies* successive, che sono tali proprio in quanto eredi di questo modello.

A differenza dei registri tradizionali tenuti da banche o istituzioni, questo libro contabile non appartiene a nessuno e, allo stesso tempo, appartiene a tutti: è distribuito su migliaia di computer nel mondo — questa è la decentralizzazione — ed è accresciuto tramite l'intervento collettivo di un meccanismo puramente matematico-computazionale chiamato *proof-of-work*, basato sulla risoluzione competitiva di problemi crittografici che consente alla rete di raggiungere consenso senza autorità centrali.

Non si tratta dunque di un mero archivio di transazioni: la Blockchain crea e mantiene nell'essere i Bitcoin stessi. Ogni nuovo blocco è legato crittograficamente al precedente, formando una catena che non può essere alterata senza ripetere l'intero lavoro computazionale già svolto dalla rete —

operazione che, nelle condizioni effettive del mondo reale, risulta economicamente e tecnicamente impraticabile.

La funzione primaria della Blockchain è garantire sicurezza, trasparenza e decentralizzazione. Chiunque può verificare una transazione, nessuno può cancellarla, nessuna autorità centrale può imporre modifiche unilaterali. In questo modo Bitcoin introduce un modello di fiducia radicalmente nuovo: non più fondato su banche, governi o intermediari (cioè, in ultima analisi, su comportamenti umani), ma su regole matematiche pubbliche e verificabili — non più fiducia *sub condicione*, ma fiducia *ab-soluta*.

È dunque la matematica crittografica del protocollo a garantire l'impossibilità del *double spending* (doppio pagamento). Tizio invia una somma di Bitcoin a Caio e, pochi minuti dopo, tenta di inviare la medesima somma a Sempronio. Chi diviene il detentore legittimo delle *crypto*?

Nei sistemi bancari la validità delle transazioni è garantita da un ente centralizzato che detiene il libro mastro del dare e dell'avere e che, per questa funzione, viene remunerato da chi usufruisce del sistema di pagamento. Nella Blockchain, invece, la priorità è stabilita in base alla verifica e alla chiusura del blocco, alla decrittazione matematica degli *hash*, secondo un processo trasparente e impersonale (ciò non significa che nel mondo *crypto* non vi siano commissioni — sugli Exchange o nelle operazioni di finanza decentralizzata —, ma che esse attengono a momenti distinti rispetto alla validazione della transazione in quanto tale).

Nelle Blockchain, dunque, il problema della doppia vendita è tecnicamente impossibile: esso è impedito *ex ante*. Non vi è conflitto da risolvere *ex post*, perché la seconda "cessione" non può avvenire. Nel caso di Bitcoin, una UTXO risulta già spesa; nel caso di Ethereum o di un NFT, il *token* risulta già trasferito. Una volta che il blocco contenente la transazione è stato chiuso e confermato, ogni successivo tentativo di trasferire il medesimo *asset* è strutturalmente impossibile, poiché l'*asset* appartiene ormai al destinatario della prima transazione valida. Il principio è semplice e assoluto: la prima transazione valida confermata è l'unica transazione possibile (*first valid transaction confirmed = only transaction*).

Nel sistema bancario, al contrario, la doppia vendita può accadere tecnicamente, e il conflitto viene risolto *ex post* sulla base dei registri contabili. Lo stesso vale per il sistema della pubblicità immobiliare nel diritto italiano e in altri ordinamenti continentali, dove il conflitto tra più trasferimenti dello stesso bene è risolto secondo il principio *prior in tempore potior in iure*, in base cioè alla priorità della trascrizione o dell'iscrizione nelle Conservatorie dei Registri Immobiliari, indipendentemente dal momento in cui gli atti traslativi siano stati perfezionati. Nei sistemi di *Common Law*, il conflitto è risolto, ancora una volta *ex post*, sulla base della *bona fides* e della priorità della registrazione.

In Bitcoin — e, più in generale, nelle altre crypto — tutta questa problematica semplicemente non esiste: è la Blockchain stessa a impedire il conflitto prima ancora che esso possa porsi.

Le Blockchain, come si è detto, constano di due elementi essenziali: crittografia e decentralizzazione.

Quest'ultima costituisce il secondo principio cardine delle *cryptocurrencies*, e fu introdotta per la prima volta dal protocollo di Bitcoin.

Nessun singolo soggetto ha il controllo esclusivo del sistema: il protocollo procede secondo regole matematiche prefissate, e le decisioni che si rendano necessarie sono distribuite tra una moltitudine di partecipanti indipendenti. Il fatto che grandi istituti investano in Bitcoin non implica, a differenza di quanto avviene nelle società quotate, la possibilità di acquisire una posizione di controllo, influenzare la *governance* o modificare unilateralmente le regole del sistema. Ciò dipende dalla differenza strutturale fondamentale tra controllo maggioritario (ossia concentrazione del capitale) da una parte, e decentralizzazione dall'altra: in una società è sufficiente detenere una quota rilevante del capitale per esercitare influenza sulle decisioni strategiche; in una Blockchain, invece, la proprietà dell'*asset* non conferisce alcun potere decisionale sull'infrastruttura protocollare, e per modificarne struttura e finalità sarebbe necessario ottenere il consenso coordinato della maggioranza assoluta dei nodi che la compongono, vale a dire delle persone fisiche che, disseminate per il globo, detengono e fanno funzionare i computer su cui la Blockchain è replicata. Questa eventualità non è soltanto improbabile: è strutturalmente implausibile.

Altro specchio della decentralizzazione — e altra unicità delle *crypto* — è la trasparenza, immediata e adamantina. Non vi sono dati riservati a pochi: tutto è visibile e accessibile a chiunque. I Bitcoin possono essere tracciati in ogni loro trasferimento, poiché ogni transazione è pubblica. Non possono esistere pagamenti occulti nel senso tecnico del termine, perché il registro è integralmente aperto. Chiunque può osservare in tempo reale le operazioni dei grandi detentori, le *whales* (balene) o gli *shark* (squali). Non solo sono visibili i trasferimenti di *coin*, ma anche gli *in-flow* e gli *out-flow* dagli Exchange, che spesso indicano fasi di accumulo o di distribuzione; così come sono visibili i *cluster* di liquidità nei *futures* e nei *perpetuals*, verso i quali si orienta la caccia dei *market maker*. Si tratta di informazioni che nella finanza tradizionale sono inaccessibili persino ai grandi operatori, e che nelle Blockchain sono disponibili per costruzione, consultabili da chiunque tramite *block explorer* e strumenti di analisi *on-chain* pubblici, senza intermediari né accessi riservati.

Al tempo stesso, questo sistema funziona senza nomi e cognomi. Al posto dell'identità reale compaiono indirizzi crittografici: lunghe stringhe di caratteri che rendono gli utenti pseudonimi. Non è corretto parlare di anonimato assoluto: se un indirizzo viene collegato a una persona — ad esempio tramite un Exchange soggetto a procedure di identificazione (KYC), come avviene ovunque operino intermediari regolati — l'intera cronologia delle sue transazioni diventa immediatamente visibile.

Ne risulta un paradosso unico: la massima trasparenza del sistema congiunta a una protezione solo parziale dell'identità individuale. In pratica, ciò significa che Bitcoin tutela il pseudonimato, protegge la libertà individuale e apre l'accesso a chi sarebbe altrimenti escluso. A livello sistemico, le *crypto* sono strutturalmente immuni dal rischio di frodi contabili e di manipolazioni dei registri; sono immuni alla corruzione nel senso tecnico del termine e, in ultima analisi, anche al riciclaggio, se lo si intende correttamente come occultamento sistemico dei flussi. Ciò non esclude, beninteso, la presenza di malintenzionati che tentano di carpire le chiavi private o di trarre in inganno ad esempio con pre-vendite di *token* fasulli; ma si tratta di truffe grossolane, del tutto analoghe ai tentativi di *phishing* telefonico, e non di falle del sistema.

La funzione di Bitcoin

Quando nel 2009 venne creato Bitcoin, esso ovviamente non valeva praticamente nulla: era un esperimento crittografico scambiato tra pionieri per pochi centesimi.

Nel 2010 avvenne la prima transazione “reale”: 10.000 BTC per due pizze, evento oggi divenuto simbolo della distanza siderale tra le origini e il presente. Da allora, la storia del prezzo di Bitcoin si è articolata in cicli sempre più ampi e violenti, caratterizzati da fasi di espansione rapida seguite da *drawdown* profondi. Nel 2013 toccò per la prima volta i 1.000 dollari; nel 2017 superò i 19.000 per poi subire un crollo di oltre l’80%; nel 2021 raggiunse i 69.000 dollari, seguito da un nuovo *drawdown* di analoga entità; più recentemente ha superato i 120.000 dollari, per poi entrare in fasi di lunga lateralità, ancora una volta accompagnate da forti correzioni intermedie.

Bitcoin non è più un fenomeno di nicchia; è ormai considerato da molti un *asset* con un ruolo potenzialmente strutturale nei portafogli.

La sua crescita non è stata soltanto numerica, ma soprattutto culturale e istituzionale. Figure di primissimo piano della finanza globale, ed alcuni tra i suoi critici più accesi, hanno progressivamente mutato posizione. Jamie Dimon, CEO di JPMorgan, che nel 2017 definiva Bitcoin una truffa, oggi sviluppa infrastrutture Blockchain e offre servizi *crypto* ai propri clienti. Larry Fink, CEO di BlackRock, inizialmente parlava di Bitcoin come di uno strumento per il riciclaggio; nel 2024 la sua società ha lanciato un ETF su Bitcoin approvato dalla SEC, arrivando a definirlo un *fear asset*, cioè uno strumento di protezione in scenari di instabilità sistemica. Persino Paul Tudor Jones, tra i più autorevoli *hedge fund manager macro*, ha dichiarato di considerare Bitcoin l’equivalente digitale dell’oro in tempi di inflazione.Questa traiettoria mostra come Bitcoin sia passato dall’essere oggetto di scherno a bene rifugio riconosciuto dalla finanza globale. Il prezzo ha funzionato come cartina al tornasole: ogni caduta rafforzava i detrattori, ogni ripresa ne erodeva le certezze, fino a costringerne molti a una revisione sostanziale

delle proprie posizioni; ciò che ha reso possibile questo mutamento non è stata la scomparsa delle eccentricità speculative che hanno accompagnato Bitcoin fin dall'inizio, ma il progressivo consolidarsi della sua solidità intrinseca come infrastruttura monetaria, resistente nel tempo proprio attraverso cicli di euforia e di crisi.

Se la narrativa oggi prevalente resta quella di Bitcoin come "oro digitale", essa, pur essendo in larga parte veritiera, resta insufficiente a coglierne la particolare funzione intrinseca.

L'oro è un *asset* di mero accumulo, non speculativo in senso proprio: una riserva materiale di valore, la cui scarsità — e la cui fisicità — ne garantiscono il ruolo storico. Oggi, come spesso è accaduto anche in passato, il prezzo dell'oro subisce fortissime pressioni rialziste, non perché venga acquistato in misura decisiva dal mercato *retail*, ma perché viene massicciamente accumulato dalle Banche Centrali (prevalentemente da parte delle Banche Centrali dei BRICS, essenzialmente allo scopo di convertire i dollari incassati a seguito dei surplus commerciali non più in *Treasury* statunitensi — cioè sempre in sostituti del dollaro — ma in una riserva strategica diversa, con l'effetto diretto di non impedire che l'immane debito pubblico degli Stati Uniti continui a espandersi).

L'oro, appunto, al di là del suo impiego sulla scacchiera finanziaria globale come strumento di regolazione e di guerra monetaria di lungo periodo, resta un asset di accumulo e di difesa, non un'infrastruttura: non fonda un sistema, non genera operatività, non garantisce processi.

La funzione propria di Bitcoin deriva dalla sua stessa essenza: crittografia e decentralizzazione, le quali rendono la fiducia finanziaria una proprietà strutturale del sistema. Il fatto che la funzione di Bitcoin coincida con i suoi stessi elementi costitutivi è un aspetto estremamente significativo, e raro. Non sempre, infatti, la funzione di un asset, di un bene o di una *res* riflette la sua essenza: più spesso è l'uso storico e sociale a determinarne la funzione, ipostatizzando in una direzione alcune delle sue qualità e oscurandone altre. È bensì vero che tutte le *crypto*, in quanto geneticamente fondate sulla Blockchain al pari di Bitcoin, presentano una analoga corrispondenza tra essenza e funzione; ciò che distingue Bitcoin dalle altre criptovalute è che

Bitcoin è stato fondamento di se stesso, mentre le altre *crypto* derivano la propria legittimazione dall'esistenza previa di Bitcoin, e operano sempre all'interno di uno spazio di fiducia che Bitcoin ha già reso possibile. Inoltre, solo Bitcoin ha come funzione la pura formalizzazione della fiducia autoreferenziale, nel senso che la fiducia pertiene esclusivamente all'evento in sé della transazione finanziaria. Le altre *crypto*, pur fondandosi anch'esse su forme di fiducia oggettiva, introducono direzioni fiduciarie ulteriori — operative, applicative o funzionali.

Quanto premesso, si può contemplare come la fiducia autoreferenziale di Bitcoin, senza mutare né la propria essenza né la propria funzione, bensì si estenda, ovvero ampli in modo estensivo naturale, si potrebbe dire entropico, il proprio ambito: non nel senso che includa altre direzioni o elementi, ma che semplicemente irradii altro da sé. Detto in termini meno astratti, Bitcoin è diventato da garanzia di sé, la garanzia liminale dell'intero mondo *crypto*.

Quanto premesso, si può comprendere come la fiducia autoreferenziale di Bitcoin, senza mutare né la propria essenza né la propria funzione, abbia progressivamente esteso il proprio ambito. Non perché abbia incorporato nuove direzioni o finalità, ma perché la sua stessa irrefragabilità ha finito per irradiare altro da sé — e precisamente quella porzione astratta che le *crypto* hanno in comune con Bitcoin: la struttura Blockchain.

In termini meno astratti, Bitcoin, da garanzia di sé, è divenuto la garanzia liminale dell'intero ecosistema *crypto*, in quanto ne costituisce il presupposto di fiducia ultimo, pur restando esterno alle sue funzioni operative.

Ma questo non è che un momento intermedio. L'entropia dell'ecosistema *crypto* tende verso la forma della tokenizzazione universale, non come direzione imposta o progetto deliberato, bensì come disvelamento naturale degli elementi costitutivi della Blockchain. Una volta che la fiducia è formalizzata e resa verificabile *on-chain*, qualunque entità economicamente o giuridicamente rilevante — *asset* finanziari, diritti, crediti, garanzie, flussi, accessi — diviene tecnicamente tokenizzabile. Non perché debba esserlo, ma perché può esserlo senza introdurre nuovi presupposti fiduciari: la tokenizzazione universale non è dunque un nuovo paradigma da imporre, ma il punto di saturazione di un'infrastruttura che, una volta istituita, tende

spontaneamente a estendersi a tutto ciò che richiede garanzia, trasferibilità e verificabilità.

Che questo processo sia ormai in atto non è una congettura teorica, ma un dato dichiarato. Le élite finanziarie e istituzionali riconoscono apertamente la tokenizzazione come passaggio inevitabile dell'evoluzione dei mercati, e vi concorrono attivamente: non per adesione a una visione "*crypto*", ma perché la tokenizzazione consente una gestione più efficiente del rischio, della liquidità, della collateralizzazione e del regolamento delle transazioni. In questo senso, la tokenizzazione non rappresenta una rottura con la finanza tradizionale, bensì la sua riorganizzazione infrastrutturale. Gli stessi soggetti che per decenni hanno operato attraverso registri chiusi e intermediari fiduciari stanno progressivamente adottando registri distribuiti, *asset* tokenizzati e meccanismi di *settlement on-chain*, integrandoli nei quadri normativi esistenti. Non si tratta di una fuga dal sistema, ma del suo adattamento strutturale.

In questo senso va chiarito che Bitcoin non fonda operativamente la finanza tokenizzata, ma ne delimita il perimetro estremo di legittimità: rappresenta ciò che resta quando la fiducia nel sistema viene messa radicalmente in questione. È per questo che si può dire, in senso proprio ma non tecnico, che Bitcoin funzioni come collaterale universale della tokenizzazione. Non lo è nel senso operativo del margine — che nei derivati richiede *asset* stabili e per questo è storicamente affidato alle *stablecoin* — ma nel senso fiduciario più profondo: Bitcoin costituisce già oggi la garanzia di legittimità dell'intero ecosistema *crypto*, e lo sarà ancor più nel momento in cui la finanza globale migrerà su infrastrutture Blockchain. Chiamarlo semplicemente "fondamento" sarebbe impreciso, perché il suo ruolo non è fondativo del valore in sé, ma della fiducia che rende possibile il valore; chiamarlo "collaterale" in senso stretto sarebbe altrettanto improprio, perché una *crypto* pura non può svolgere funzione di margine senza contraddirsi economicamente. E tuttavia Bitcoin è correttamente collaterale in senso universale: il valore economico ultimo, non sequestrabile e non manipolabile, su cui poggerà l'intera architettura della tokenizzazione.

Questa è la funzione che oggi si può dire entropica di Bitcoin: se l'è costruita da solo nel tempo e ora sta semplicemente emergendo. È stata vista e compresa dagli operatori finanziari, e per questo proseguirà il proprio sviluppo in modo autonomo, all'interno di un ambiente ormai adeguato. La tokenizzazione universale degli asset non è un'utopia né una eventualità contingente, ma un esito ormai riconosciuto come inevitabile della finanza globale, come dichiarano apertamente i CEO di JPMorgan, BlackRock e di numerose altre istituzioni. In questo scenario Bitcoin non sarà l'architrave operativa del sistema, ma il suo asset di garanzia ultima: esterno all'infrastruttura, e tuttavia da essa implicitamente presupposto, in quanto *stress-test* permanente della fiducia.

Per poter intravvedere appieno quale sia la potenza latente della tokenizzazione universale, occorre però dapprima esaminare quale ne è la struttura operativa.

Ethereum

Se Bitcoin è il monarca delle *crypto*, incoronato sul campo della garanzia di inviolabilità, inviolabili sono a cascata tutte le altre *crypto.* Le quali hanno finalità e funzionalità loro proprie, ultronee rispetto a Bitcoin, spiccatissime e cruciali.

Su questa base, si deve ora, per avere chiari gli elementi che si intersecano nella istanza di tokenizzazione universale degli *asset*, rivolgere l'attenzione alla rete Ethereum: la *mainnet* (livello di base della Blockchain Ethereum) e i suoi layer-2 (come Arbitrum, Optimism, Base, zkSync, Starknet: i layer-2 "scalano" Ethereum perché consentono di aumentare il numero di transazioni ed esecuzioni complessive senza modificare l'architettura della *mainnet*, che resta il livello di consenso e di sicurezza).

Bitcoin, come chiarito, esaurisce la sua funzione finanziaria — la sua "causa", se si volesse parlare in termini di elementi costitutivi del contratto — nella transazione-dazione di *coin*. Esso ha rappresentato il primo grande esperimento riuscito di denaro digitale decentralizzato, dimostrando che è

possibile trasferire valore su Internet senza l'intermediazione di banche o governi. La sua Blockchain, semplice e rigorosa, ha introdotto due principi rivoluzionari: la scarsità digitale e la fiducia senza intermediari.

Questa evidenza ha acceso l'immaginazione di sviluppatori e imprenditori, che si sono posti la domanda susseguente: se è possibile decentralizzare il denaro, perché non decentralizzare anche il web stesso?

È in questo contesto che nasce il Web3: non come moda tecnologica, ma come evoluzione strutturale di un Internet in cui le applicazioni non sono più controllate da soggetti centrali, bensì vivono su Blockchain e reti distribuite. Se il Web-2 è stato l'era delle piattaforme — Facebook, Google, Amazon — il Web3 mira a restituire proprietà, controllo e interoperabilità agli utenti.

Ethereum, creato principalmente da Vitalik Buterin, ha svolto un ruolo di apripista decisivo, introducendo gli *smart contract* ("contratti intelligenti"): programmi che vengono eseguiti direttamente sulla Blockchain. A differenza di Bitcoin concepito come registro distribuito orientato alla transazione di valore, Ethereum nelle parole del stesso Buterin è un "computer mondiale distribuito" (*distributed computing*) capace di eseguire contratti intelligenti. In altri termini: se Bitcoin è pensato per il trasferimento di valore, Ethereum è pensato per l'esecuzione di applicazioni decentralizzate (dApp). Da qui la definizione più ricorrente di Ethereum quale *world computer*: una piattaforma globale di calcolo decentralizzato, nella quale il codice viene eseguito e verificato collettivamente. Ciò significa che i programmi — finanziari, organizzativi o di intrattenimento — non vengono eseguiti su singoli computer coordinati da un server centrale, bensì sono eseguiti sulla catena costituita dalla moltitudine delle macchine che compongono la rete: ciascuna localizzata in un punto del mondo, ma tutte vincolate all'esecuzione di un codice unico, pubblico e verificabile, disponibile *open source* (tipicamente su GitHub).

Ethereum è una Blockchain che consente l'esecuzione di applicazioni direttamente sulla rete decentralizzata, senza intermediari, attraverso gli *smart contract*, che delle dApp costituiscono la logica esecutiva. A differenza dei computer tradizionali e delle applicazioni del Web-2, che eseguono codice su server controllati da un soggetto centrale, Ethereum non è un

computer nel senso classico, ma un'infrastruttura di esecuzione condivisa: il codice non "gira" su una macchina o su un *data center*, bensì viene eseguito e verificato collettivamente dalla rete stessa, secondo regole pubbliche e immutabili. Per questo Ethereum è detto *world computer*: il calcolo è una proprietà del protocollo, non di una macchina.

Può apparire ridondante il precisarlo, ma ciò è discriminante: nel Web-2 ogni sito, ogni applicazione, ogni servizio *cloud* gira su server centralizzati, fisicamente collocati in monolitici *data center* — spesso situati in regioni climaticamente fredde per ridurre i costi di raffreddamento delle macchine. Ebbene i proprietari di questi server centrali hanno pieno controllo sui dati che vi sono ospitati: possono conservarli, modificarli, censurarli ovvero monetizzarli (sarebbe del resto economicamente implausibile che le *big tech* creassero e mantenessero infrastrutture e servizi "gratuiti" privi di una qualche forma di ritorno economico), senza che l'utente abbia alcuna possibilità di verifica effettiva o di conoscenza reale di ciò che accade ai propri dati. Nelle reti decentralizzate, tutt'al contrario, i dati non risiedono in un luogo unico né sono sotto il controllo di un singolo soggetto: sono invece replicati, distribuiti e verificabili dalla rete nel suo insieme. La proprietà delle singole posizioni, dei singoli *token* o dei singoli *asset* resta ovviamente pienamente definita, ma essa si esercita in un regime di trasparenza strutturale: non come potere opaco di amministrazione dei dati, bensì come titolarità crittograficamente dimostrabile e pubblicamente verificabile. In altri termini, non viene abolita la proprietà, bensì essa è separata dal controllo arbitrario dell'infrastruttura.

Quindi, per prevenire le riserve mentali delle anime belle o delle cattive coscienze, va rimarcato il punto decisivo: ciò che è scritto sulla Blockchain è strutturalmente trasparente, a differenza di quanto avviene nei server centralizzati, dove l'opacità è la regola e la visibilità un'eccezione concessa.

Su Ethereum sono nati la finanza decentralizzata (DeFi), gli NFT (*non-fungible tokens*), le organizzazioni autonome (DAO) e un intero ecosistema: oggi le dApp sono decine di migliaia, nei più svariati settori — dall'intrattenimento alla finanza, fino all'arte digitale.

Un cenno di chiarimento sugli NFT è opportuno, considerato lo stigma di cui sono stati marchiati dopo il tracollo del 2022, dovuto a un eccesso di speculazione al loro apparire (FOMO: *fear of missing out*). Gli NFT sono *token* unici registrati su Blockchain che attestano l'unicità, la provenienza e la titolarità di un oggetto digitale o di un diritto su di esso. A differenza dei *token* fungibili — come le *stablecoin*, i *token* di governance e, più in generale, tutti i *token* ERC-20, emessi su Ethereum secondo uno standard di *smart contract* che definisce in modo uniforme funzioni quali trasferimento, saldo, approvazione e autorizzazione alla spesa — un NFT non è intercambiabile con un altro: ciascun NFT rappresenta un'istanza unica, identificabile e non sostituibile sul piano crittografico. In concreto, un NFT non è l'immagine, il video o il file in sé, ma il certificato *on-chain* che ne àncora identità, storia e proprietà all'interno della rete. Il loro primo utilizzo massivo è stato quello delle opere d'arte digitali, dove l'NFT ha risolto un problema strutturale del digitale stesso: l'assenza di originalità. L'opera digitale, infinitamente copiabile, diventa invece opera in senso proprio quando la sua unicità viene garantita dal protocollo, tramite il *minting* ("creazione") dell'NFT stesso.

Terminate l'esaltazione iniziale e il successivo ridimensionamento, gli NFT non sono scomparsi, ma si sono ricollocati. Oggi il loro utilizzo si è esteso e raffinato: biglietti per eventi, pass di accesso, *membership*, diritti d'uso, certificazioni, *asset* ibridi che combinano funzione e rappresentazione. In questi casi l'NFT non è più l'oggetto del desiderio in sé, ma l'infrastruttura di accesso a un'esperienza o a un servizio. Resta tuttavia intatto il valore più profondo degli NFT come espressione d'arte, se assunti, si può asserire, alla luce della delucidazione heideggeriana dell'opera d'arte: l'opera d'arte è il luogo in cui la verità dell'ente si pone in opera, non come rappresentazione, ma come evento di disvelamento. Questa nozione può valere a livello strutturale per gli NFT in ragione della loro modalità di creazione, che non si limita alla scrittura di un file, ma implica un atto formale di esecuzione e stabilizzazione all'interno del protocollo. È vero che la gran parte degli NFT ancor oggi resta confinata nella sfera della rappresentazione più superficiale — immagini, segni, simboli, oggetti decorativi — ma le tecniche digitali di predisposizione dell'opera, unite alla sua immersione in un ecosistema *on-*

chain coerente e intenzionalmente costruito dall'artista, rendono possibile che l'NFT non rappresenti semplicemente qualcosa, bensì ponga in opera una modalità noetica.

Al di là di queste valutazioni preteoretiche, i *non-fungible tokens* restano una delle espressioni più chiare della capacità di Ethereum di trasformare il protocollo in spazio formale della creazione. Proprio in questo senso, essi non costituiscono un fenomeno isolato, ma anticipano la logica più generale del Web3.

E in generale, appunto, il Web3 estende questa rivoluzione a tutto ciò che può essere fatto online. Volendo delineare una sintesi dell'evoluzione del Web, si può dire che il Web originario era essenzialmente informativo e statico. Il Web-2 ha introdotto interazione e applicazioni, ma concentrando dati, identità ed esecuzione in piattaforme centralizzate — in questo modello, il funzionamento del sistema dipende in ultima analisi dalla fiducia nel gestore dell'infrastruttura. Il Web3 segna un ulteriore passaggio: non decentralizza l'interfaccia, ma la fiducia stessa, spostando esecuzione, valore e regole nel protocollo. L'applicazione non funziona perché qualcuno la controlla, ma perché la rete nel suo insieme la garantisce.

Questa trasformazione riguarda tanto chi crea quanto chi utilizza. Per chi sviluppa, il Web3 significa scrivere codice che non dipende da un'infrastruttura proprietaria, ma che vive autonomamente nel protocollo: una volta distribuito, lo *smart contract* non può essere censurato, modificato o disattivato arbitrariamente. Per chi utilizza, significa interagire con applicazioni che non richiedono fiducia in un soggetto centrale, né la cessione di dati personali come contropartita implicita. Nel modello attuale del Web-2, al contrario, la fiducia viene sistematicamente sostituita dal controllo: dei pagamenti, delle identità, delle comunicazioni, dei comportamenti; servizi presentati come gratuiti monetizzano in realtà i dati; infrastrutture pubbliche e private convergono verso sistemi di sorveglianza pervasiva, nei quali l'utente non è più soggetto, ma materia prima.

Il Web3, in questo senso, non va inteso come una "ribellione" al sistema, né come una rivendicazione identitaria o antagonista; può essere visto più semplicemente come una dimensione nella quale i rapporti, tanto

interpersonali quanto istituzionali, tornano a essere improntati a una forma di spontaneità strutturale, nella quale prevaricazione e riserva mentale — l'endiadi della "mente ordinaria" secondo la terminologia dei *Tantra*, ossia le estrinsecazioni connaturate a una natura umana fondata, in quanto razionale-rappresentativa, sulla volontà di dover sapere — risultano impedite a livello strutturale.

In altri termini, nel Web3 la creazione non è subordinata alla concessione di accesso da parte di una piattaforma, e l'uso non è condizionato dalla permanenza interessata di un intermediario. La fiducia non è promessa, ma incorporata nella struttura stessa del sistema.

Ethereum: la macchina universale della fiducia

Se Bitcoin è comunemente detto "oro digitale", Ethereum deve essere detto, con maggiore precisione, il "petrolio" del nuovo mondo digitale: ciò senza il quale una città, pur ricca di mezzi, di intelligenze e di obiettivi, resta ferma e inoperante.

Ma questo "petrolio" non è una risorsa materiale né un servizio: è la codifica della fiducia. Questo è il cuore di Ethereum. La sua affermazione globale non è la conseguenza del successo delle applicazioni decentralizzate che vi operano sopra, né del fatto che "offra servizi" — Ethereum non è una società che vende utilità. Il rapporto causale è inverso.

Ethereum è, anzitutto, un generatore di fiducia *ex se*: una infrastruttura che stabilizza la fiducia a livello protocollare. Non è che le dApp producano fiducia nel sistema; sono piuttosto generate da una fiducia già stabilizzata. È la possibilità di esecuzione certa, impersonale e verificabile che rende possibili le applicazioni decentralizzate, non è la loro diffusione a creare fiducia negli utenti.

Qui si manifesta la differenza radicale rispetto al mondo delle valute fiat, del Web-2 e delle società imprenditoriali tradizionali: in questi sistemi la fiducia è sempre *ex post*, psicologica, reputazionale, delegata a soggetti; in Ethereum la fiducia è *ex ante*, strutturale, inscritta nel protocollo stesso.

In altre parole, la crittografia di Ethereum consiste nella formalizzazione matematica della fiducia. È per questo che Ethereum non è semplicemente un computer distribuito, una rete o un'infrastruttura informatica, ma qualcosa di intrinsecamente diverso.

Questa potenza è già implicitamente presente in Bitcoin, la cui Blockchain rende la fiducia una proprietà matematica del registro; tuttavia, in Bitcoin tale fiducia resta limitata alla validità della transazione.

La fiducia che la Blockchain di Ethereum decentralizza *erga omnes*, invece, investe qualsiasi relazione formalizzabile, cioè ogni rapporto che possa essere espresso in termini di condizioni, regole ed esiti. Dove in precedenza erano necessari contratti scritti, intermediari e autorità giudiziarie per garantirne l'esecuzione, Ethereum introduce codice che si esegue automaticamente, senza ricorso ad autorità esterne. Questa potenza di Ethereum è oggi solo intravista: è ampiamente presupposta in ogni dApp (in modo smaccatamente aprìco, verrebbe da dire, nelle dApp speculative), ma resta difficile coglierne la portata perché il modo di pensare propriamente umano concepisce la fiducia come qualcosa di patologicamente arbitrario e potenzialmente incerto. La vita stessa di chiunque — dal fidanzamento all'acquisto di un immobile — è attraversata da una regolamentazione della fiducia: anelli, rogiti, garanzie, solenni strette di mano. Tutti dispositivi che, in modo surrettizio, tentano di conferire una durata artificiale, se non addirittura eterna, ad una fiducia che, in realtà, resta opaca, intaccata da sospetti, cautele e riserve mentali mai del tutto eliminabili.

Ethereum, certo, non "risveglia" nessuno a una vita karmica fuori dal *saṃsāra*; mostra semplicemente che le relazioni formalizzabili in termini di fiducia possono essere formalizzate come fiducia.

Esplica ed attua una tautologia.

E ciò è possibile per un motivo essenziale: è la decentralizzazione che oggettivizza la fiducia. Essa viene "ridotta" a termini matematici non per astrazione, ma perché, a differenza tanto dei sistemi istituzionali quanto del *peer-to-peer* tradizionale, non esiste più alcun centro decisionale né alcuna asimmetria operativa da cui possa scaturire un vantaggio nel tradire la fiducia. Nei sistemi istituzionali la fiducia è delegata a un'autorità; nel *peer-to-*

peer non vincolato resta affidata ai comportamenti dei soggetti. Solo nella Blockchain l'assenza di un centro è accompagnata da regole crittografiche che impediscono strutturalmente il tradimento, rendendo la fiducia una proprietà impersonale del protocollo.

Questa non è "filosofia", né "morale", e men che meno "psicologia" della Blockchain: è semplicemente l'accadere di uno dei rarissimi usi retti della ragione. La ragione, in quanto fondata sulla rappresentazione, è il limite di *Homo sapiens*; la Blockchain, per sorte, distilla — *solve et coagula* — solo e tutto il meglio che la ragione può essere.

La mente ordinaria non può che essere intrinsecamente portata alla riserva mentale e alla sfiducia, poiché il velo neurobiologico della rappresentazione preclude la conoscenza della natura della propria mente e, quindi, della realtà autentica. Gli *yogīn* e gli adepti affermano che la ragione costituisce una forma di prevaricazione dell'*avidyā* (l'ignoranza della natura della propria mente) in quanto essa opera come rappresentazione.

La decentralizzazione della Blockchain opera, detto in termini pre-teoretici, una astrazione della ragione formale, sottraendola ai contenuti rappresentativi che ogni individuo, in quanto tale, vi proietta per rappresentazione. Ciò non significa che la Blockchain sia in sé pre-teoretica: al contrario, essa è massimamente teoretica; ed è proprio il suo esserlo *massime* e *de plano* che consente di superare i legni storti dell'umanità — senza che ciò costituisca, naturalmente, un accesso alla *vidyā*, alla dimensione oltre-umana della conoscenza che accade, dicono i Tanta, per caduta della *śakti*. D'altra parte, adepti e *yogīn* — e, in termini filosofici, Heidegger — ripetono da millenni che l'uso retto della ragione può condurre alla constatazione della sua autoreferenzialità e, quindi, della sua intrinseca ingannevolezza, senza per questo oltrepassarne il dominio, bensì appunto giungendo al limite interno della ragione stessa.

Questa è una descrizione puramente strutturale, e al tempo stesso autenticamente tantrica, del Web3. Le dottrine tantriche, alchemiche e qabbalistiche non fondano la conoscenza su un atto di fede, ma sull'esperire di una ragione che operi senza mediazione rappresentativa. Allo stesso modo, *crypto* e Web3 non chiedono adesione soggettiva, ma consentono

l'esperienza diretta di relazioni valide senza presupporre fiducia personale o autorità centrale.

Ether

Naturalmente anche Ethereum ha la sua propria *crypto*, il *coin* nativo Ether (ETH), che nasce come *gas* — nel senso letterale del termine — che alimenta l'intero ecosistema.

Per operare sulla rete è necessario utilizzare la moneta nativa del sistema: per acquistare *token* o NFT, per interagire con una dApp, per eseguire uno *smart contract*, occorre Ether. Allo stesso modo, in Ether viene pagata l'esecuzione di ogni operazione *on-chain*: dalle transazioni più elementari fino alle operazioni finanziarie articolate, incluse le interazioni di gestione del rischio, come il dover incrementare il collaterale di margine in una posizione *long perpetual* per allontanare la soglia di liquidazione in caso di repentine azioni ribassiste.

L'Ether è dunque la linfa vitale che rende possibile il Web3 della rete Ethereum, la condizione economica dell'azione: misura il costo dell'esecuzione, della verifica, della stabilizzazione delle relazioni formalizzate. Ogni istruzione eseguita, ogni condizione verificata, ogni relazione inscritta nella rete consuma Ether, perché consuma risorse computazionali condivise. È in virtù di questa funzione primaria che ETH assume anche la forma di mezzo di scambio e di moneta digitale in senso proprio.

Da ciò discende anche il diverso modo in cui il mercato "legge" Ether rispetto a Bitcoin.

L'investimento in Bitcoin ruota quasi interamente attorno alla scarsità programmata e al ruolo di riserva di valore: si scommette sul fatto che, nel tempo, il prezzo salga perché l'offerta è rigidamente limitata.

L'investimento in Ethereum, invece, deriva dalla natura economico-sostanziale di Ether quale *gas* nativo della rete. Non riguarda soltanto l'apprezzamento del prezzo dell'*asset* — pur rilevante, anche alla luce del

meccanismo di *burn* introdotto con l'EIP-1559, che elimina una parte delle commissioni e introduce una dinamica tendenzialmente antinflazionistica — ma è legato alla crescita dell'intero ecosistema: più applicazioni vengono sviluppate, più utenti interagiscono con la rete, più relazioni vengono formalizzate *on-chain*, maggiore è la domanda strutturale di Ether necessaria ad alimentare il sistema.

Ed è per questa ragione che la ricerca di profitto si trasforma in motore di innovazione: capitali e sviluppatori convergono verso nuove applicazioni, rendendo Ethereum un laboratorio tecnologico e finanziario in continua evoluzione. Non sorprende, dunque, che Ether sia stabilmente la seconda *crypto* per capitalizzazione di mercato (la prima essendo ovviamente Bitcoin): ETH non remunera un intermediario, non rappresenta un capitale sociale, non garantisce rendimenti per diritto, invece rende possibile l'azione in un ambiente in cui la fiducia non è concessa, ma incorporata nel protocollo.

Una volta chiarita la distinzione tra Bitcoin ed Ethereum — puro *asset* il primo, infrastruttura il secondo — diventa possibile comprendere anche la loro relazione di mercato, che non è contingente né meramente speculativa, ma strutturale.

Bitcoin ed Ethereum non sono due *asset* indipendenti che "casualmente" si muovono insieme. Il loro rapporto è funzionale: Bitcoin opera come fondamento di garanzia dell'intero spazio *crypto*; Ethereum come piano operativo su cui tale spazio si articola. Di conseguenza, i cicli di mercato tendono a manifestarsi secondo sequenze ricorrenti.

Nelle fasi classiche di *bull run* (rialzo forte e prolungato), il capitale entra dapprima in Bitcoin. Ciò avviene perché Bitcoin è percepito come l'*asset* a rischio minore dell'ecosistema: è più semplice, più comprensibile, più vicino alla categoria monetaria, e svolge in modo diretto la funzione di riserva di valore. Quando Bitcoin rompe livelli chiave, consolida e viene riconosciuto come legittimo anche da capitali istituzionali o semi-istituzionali, l'attenzione del mercato si sposta progressivamente verso Ethereum (e, in una fase successiva, anche verso le cosiddette *altcoin*: *asset* a maggiore leva e rischio, che intercettano il capitale più speculativo quando la fiducia sistemica è ormai stabilizzata e la ricerca di rendimento diventa dominante).

Questo passaggio non è casuale. Ethereum incorpora una leva intrinseca: se Bitcoin stabilizza la fiducia, Ethereum la mette al lavoro. Nelle fasi di espansione il capitale non cerca solo conservazione, ma rendimento; e il rendimento, nello spazio *crypto*, nasce dall'uso dell'infrastruttura. DeFi, *staking*, NFT, DAO, strumenti derivati: tutto ciò avviene su Ethereum (e sui suoi layer-2), e tutto ciò richiede Ether.

Ne consegue che, dopo una fase di apprezzamento di Bitcoin, Ethereum tende a sovraperformare. È il momento in cui il mercato smette di interrogarsi sulla legittimità dell'*asset* e inizia a scommettere sull'espansione del sistema. Nei grandi cicli storici questa dinamica è ricorrente: Bitcoin apre il ciclo, Ethereum lo amplifica.

Il processo inverso si osserva nelle fasi di contrazione. Quando il rischio sistemico aumenta, la liquidità defluisce prima dagli asset più operativi e complessi, e solo successivamente da Bitcoin. Ethereum, proprio perché legato all'attività, alla leva e all'uso, subisce *drawdown* più violenti; Bitcoin tende invece a fungere da ultimo approdo e spesso da primo punto di rientro. Questa asimmetria spiega perché Ethereum sia strutturalmente più volatile di Bitcoin, ma anche perché, nei cicli espansivi, possa offrire rendimenti superiori. Non si tratta di una debolezza: è il riflesso del fatto che Ethereum non è soltanto una moneta, ma una macchina economica. Quando l'attività cresce, la domanda di Ether aumenta in modo non lineare; quando rallenta, si contrae altrettanto rapidamente.

Però non tutte le *bull run* hanno la medesima origine.

Quando, come appena descritto, il movimento rialzista è innescato da capitale esterno e istituzionale, Bitcoin tende a muoversi per primo, seguito da Ethereum. Vi sono però fasi storiche più avanzate in cui la dinamica si rovescia e il ciclo nasce dall'interno dell'ecosistema. Quando Bitcoin è ormai acquisito come struttura di fondo e non necessita più di essere legittimato, la domanda marginale non cerca un bene rifugio, ma un'infrastruttura operativa: utilizzo, rendimento, sperimentazione. In questi contesti Ethereum può anticipare il movimento, poiché l'aumento dell'attività *on-chain* genera una domanda endogena di ETH prima che il capitale torni a concentrarsi su Bitcoin.

A seconda del regime di mercato, quindi, l'una *crypto* può precedere l'altra o seguirla come conferma del ciclo; per questo non è corretto affermare semplicemente che "Bitcoin guida ed Ethereum segue", né il contrario. Al di là di queste dinamiche cicliche, resta però una relazione strutturale più profonda: Bitcoin fonda il sistema e ne garantisce la stabilità, mentre Ethereum ne attiva il movimento interno. In questo senso, l'osservazione del rapporto tra ETH e BTC non è un indicatore puramente tecnico, ma uno strumento di lettura dello stato del sistema: segnala se il mercato si muove verso una nuova legittimazione dall'esterno o verso un'espansione strutturale dall'interno. Bitcoin stabilizza il valore; Ethereum lo mette in circolazione. Sono due momenti distinti di un unico processo.

Ed è ancora dalla potenzialità operativa di Ethereum che derivano le *stablecoin*, spesso trattate come fenomeno a sé mentre in realtà esse sono interamente dipendenti dall'infrastruttura che le rende possibili. La funzione delle *stablecoin* è ben precisa: sono indispensabili al funzionamento del Web3, ma esclusivamente in quanto derivazioni strutturali dell'infrastruttura Ethereum, che ne rende possibile l'esistenza, la circolazione e l'uso programmabile.

Le *stablecoin* sono *token* digitali ancorati, in rapporto paritario, a una valuta tradizionale — quasi sempre il dollaro statunitense. Questo ancoraggio (*peg*) può essere realizzato in modi diversi. Nel modello più semplice, la *stablecoin* è garantita da riserve fiat detenute *off-chain* presso istituzioni finanziarie: dollari, titoli di Stato a breve scadenza o strumenti equivalenti (come nel caso di USDT o USDC). In altri modelli, la garanzia è *on-chain*, tramite *asset crypto* sovra-collateralizzati bloccati in *smart contract*, come avviene ad esempio per DAI. Esistono infine modelli algoritmici puri, nei quali il *peg* viene mantenuto tramite meccanismi di offerta e domanda senza collaterale diretto; questi modelli hanno però mostrato un rischio sistemico intrinseco, come dimostrato dal collasso della *stablecoin* algoritmica TerraUSD (UST) e del *token* LUNA, che ne sosteneva il meccanismo di stabilizzazione.

Al di là delle differenze tecniche, ciò che conta è la funzione della *stablecoin*. In un ambiente in cui BTC ed ETH possono oscillare del 5 o del 10 per cento in poche ore, le *stablecoin* forniscono un'unità di conto stabile, un mezzo di

scambio efficiente e uno strato di regolamento interno all'ecosistema *crypto*. Consentono di operare, spostare liquidità, fare *lending*, *borrowing* e *hedging* senza esporsi direttamente alla volatilità degli *asset* nativi.

Ed è proprio dalla loro natura stabilizzante che deriva il loro duplice ambito funzionale. Da un lato, la funzione istituzionale: le *stablecoin* vengono oggi studiate e sperimentate da banche e istituzioni finanziarie come mezzo di pagamento diretto e immediato, capace di regolare trasferimenti di valore in tempo reale, senza i ritardi e le frizioni dei circuiti interbancari tradizionali. Dall'altro lato, c'è la funzione strettamente operativa. Per i *trader*, le *stablecoin* sono il margine neutro della finanza decentralizzata, l'unità di conto stabile, il collaterale dei derivati, il mezzo di parcheggio temporaneo della liquidità tra un'operazione e l'altra: ovvero uno strumento di gestione del rischio. Per i *degen — degenerate traders*, cioè operatori iper-speculativi ad alta leva — le *stablecoin* non sono altro che margine, pura munizione operativa, capitale pronto a essere messo a rischio nei *leverage perpetuals* senza mediazioni né narrazioni. Che si tratti di operatori istituzionali, di *trader* o di *degen*, il ruolo delle *stablecoin* non è ideologico né monetario, ma puramente finanziario; ed è precisamente questa funzionalità a renderle strutturalmente inseparabili dall'infrastruttura Ethereum.

Ciò che spesso viene sottovalutato è un fatto decisivo: la quasi totalità delle *stablecoin* esiste, circola e opera su Ethereum. Vengono emesse come *token* ERC-20, interagiscono con *smart contract*, protocolli DeFi, DAO e sistemi di pagamento, e mantengono Ethereum come piano di riferimento anche quando sono trasferite su layer-2 o su altre Blockchain tramite *bridge*. Non si tratta di un accidente storico. Ethereum offre esattamente ciò di cui le stablecoin hanno bisogno — programmabilità, composabilità e sicurezza — senza le quali esse resterebbero meri surrogati digitali della moneta tradizionale. Ne segue il punto essenziale, spesso oscurato dal discorso pubblico: le *stablecoin* non sono un'alternativa a Ethereum, ma una delle principali fonti di domanda strutturale di Ether. Ogni loro utilizzo implica consumo di *gas*, sicurezza della rete e rafforzamento dell'infrastruttura sottostante.

Chiarita la funzione di Ether come infrastruttura economica dell'azione *on-chain*, diventa ora comprensibile il crisma di Ethereum: il meccanismo dello *staking*, attraverso cui ETH cessa di essere solo carburante dell'esecuzione e diventa fondamento economico della sicurezza del protocollo, rendendo Ethereum autosufficiente.

Anche Bitcoin è naturalmente autosufficiente, ma l'autosufficienza delle due *crypto* si genera in modo diverso, in dipendenza della loro peculiarità strutturale. Bitcoin è come un unico punto: una garanzia matematica pura, che non ha bisogno di altro per sussistere. Ethereum, al contrario, è il campo della possibilità di manifestazione esponenziale della fiducia matematica.

Per comprendere lo *staking* sulla rete Ethereum è necessario partire dal suo ruolo strutturale. Ethereum, dopo il passaggio dal *proof-of-work* al *proof-of-stake*, è una rete che si mantiene sicura non tramite consumo energetico, ma tramite il deposito di capitale a garanzia del corretto funzionamento del protocollo. Lo *staking* di ETH consiste precisamente in questo: bloccare Ether come collaterale per partecipare alla validazione delle transazioni e alla produzione dei blocchi, ricevendo in cambio una remunerazione.

A livello tecnico, lo staking "nativo" prevede il deposito di 32 ETH per attivare un validatore che contribuisce direttamente al consenso della rete; in cambio, il validatore riceve ricompense periodiche, ma si espone anche a penalità (*slashing*) in caso di comportamento scorretto o di inattività. Per questo motivo, nella pratica corrente la maggior parte degli utenti accede allo *staking* tramite protocolli che aggregano ETH e rilasciano in cambio *token* rappresentativi dello *stake*.

Dal punto di vista finanziario, lo *staking* di ETH è una remunerazione del capitale vincolato alla sicurezza del protocollo. Non è *yield* in senso proprio: non deriva da attività economiche, da rischio di credito o da controparte, ma da emissione di protocollo e *fee* di rete, cioè dal funzionamento stesso di Ethereum. È quindi un rendimento endogeno, strutturale, non commerciale.

Questa remunerazione può essere percepita in forme diverse: come incremento diretto del saldo a cadenza quotidiana (*token rebased*: ogni accredito è, di fatto, un evento fiscale potenziale); oppure come rivalutazione di un *token* che incorpora lo *stake*, senza flussi periodici (*token wrapped*:

l'imposizione è rinviata al momento della cessione o dello *swap*); oppure ancora come diritto a flussi futuri legati a ETH vincolato e riutilizzato in ulteriori strati di sicurezza (*restaking*, fiscalmente rilevante quando produce valore nuovo separabile, non per il mero riutilizzo dello *stake*). In tutti i casi, il punto essenziale resta che ETH passa da semplice *gas* a capitale produttivo, senza uscire dall'ambito protocollare e senza introdurre fiducia esterna.

La Tokenizzazione, I

Bitcoin rende possibile la fiducia nel valore; Ethereum rende possibile la fiducia nell'azione.
Ed è solo quando valore e azione diventano affidabili a livello protocollare che la tokenizzazione può emergere come infrastruttura reale del mondo economico. Questo è l'aspetto cruciale per intendere il futuro delle *crypto* e della finanza globale: l'istanza alla tokenizzazione emerge da sé, è lo sviluppo naturale del Web3. Non è una costruzione artificiale, voluta o imposta, ma è appunto il disvelamento della natura intima delle *crypto*, che resta nascosta finché non vi sono occhi acuti che la vedano.
Universal collateral, infrastruttura autogenerante: ne viene la tokenizzazione generale degli *asset*. Questo movimento non è l'esito di una costruzione dialettica astratta, né di una fondazione concettuale imposta a priori — come nella meccanica hegeliana della contraddizione — bensì un evento di emersione, un *Ereignis* nel senso del pensiero pre-teoretico di Heidegger: una reciproca appropriazione di elementi che si dispongono secondo la loro natura. Questo cenno serve solo a chiarire che il processo descritto non è imposto dall'esterno, ma emerge dalla struttura stessa del sistema. Bitcoin è *fiducia fiducians*, Ethereum *fiducia fiduciata*.
In questo senso profondo il Web3 pare certo utopistico, ma con la cruciale differenza, rispetto alle tante utopie, che in questo caso solo l'implementarsi dell'esito è auspicato, laddove i presupposti già esistono. Ciò che rende la tokenizzazione una solidità invece che una utopia è il fatto che i suoi elementi costitutivi siano sottratti agli interessi di parte, alla voracità predatoria — agli

attaccamenti diceva il Buddha — perché, si riprende riaffermando, Bitcoin e Ethereum sono fiducia oggettiva, sono matematica che si riconosce autoreferenziale, inattaccabile dalle mire egoiche. La tokenizzazione certo da sé non potrà risolvere nessuno dei problemi che affliggono l'umanità, ma in ogni ambito in cui si realizzerà, quello spazio sarà sottratto agli attaccamenti e alle riserve mentali, perché sarà uno spazio fondato su una fiducia che non dipende più dalla volontà degli uomini, ma dalla struttura del protocollo.

Quando le voci più importanti della finanza globale parlano della inevitabilità di tokenizzare gli *asset*, intendono precisamente che qualsiasi *asset* possa essere portato su una Blockchain, cioè fatto esistere all'interno di un registro distribuito sotto forma di *token.* Per *asset* si deve quindi nel contesto intendere, potenzialmente, qualsiasi cosa abbia valore economico o giuridico: valute, azioni, obbligazioni, quote di fondi, opere dell'ingegno, l'oro stesso, immobili, beni materiali, diritti di credito, diritti d'uso.

In questo quadro, va sottolineato come il *token* sia distinto dalla *crypto*.

Le *crypto* sono gli *asset* nativi di una Blockchain: appunto i *coin*, come Bitcoin o Ether, i quali non rappresentano qualcos'altro, ma esistono in quanto tali. La loro emissione, validità e trasferibilità sono garantite direttamente dal protocollo crittografico e dal consenso distribuito della rete.

Il *token*, invece, è un'unità digitale emessa sopra una Blockchain tramite *smart contract*. Il *token* trae il proprio valore dalla funzione che svolge: rappresentare un *asset*, un diritto, una quota, una funzione o una relazione economica. Proprio perché è programmabile, il *token* consente di incorporare regole di trasferimento, condizioni di utilizzo, vincoli giuridici, diritti economici e logiche operative direttamente nel codice. Il *token* non è moneta; può eventualmente assolvere una funzione monetaria se e nella misura in cui circoli come mezzo di scambio, ma la sua natura resta quella di unità programmabile che rappresenta un *asset*, un diritto o una funzione all'interno della Blockchain.

Tokenizzare significa appunto sussumere gli *asset* sulla Blockchain come *token* frazionabili, trasferibili e programmabili, rendendo nativa — e non più mediata — la loro circolazione, gestione e composizione all'interno di un'infrastruttura crittografica condivisa. Dire i *token* come frazionabili significa

dire che un *asset* può essere diviso in unità minime standardizzate, ciascuna trasferibile separatamente, così che anche valori tradizionalmente indivisibili — come un immobile, un'opera o un titolo strutturalmente illiquido — diventino accessibili, componibili e scambiabili in modo granulare, abbassando la soglia di accesso, aumentando la liquidità e rendendo possibile una circolazione continua del valore.

La tokenizzazione non è una semplice "digitalizzazione" di ciò che già esiste, ma una trasformazione della forma in cui gli *asset* vengono detenuti e scambiati. Un *asset* tokenizzato non è più solo registrato: è nativamente integrato nel funzionamento della Blockchain, e può essere trasferito, frazionato, utilizzato come collaterale o combinato con altri *asset* secondo regole automatiche e verificabili.

In questo quadro, chiunque disponga di un *wallet* potrà acquistare — pagando in *stablecoin* o in *crypto* — un *token* che incorpora la piena titolarità di un bene, ad esempio un fabbricato, un oggetto di antiquariato, un'opera dell'ingegno, azioni o quote di un fondo; oppure potrà acquistare una quota di proprietà frazionata dello stesso bene, espressa in *token* omogenei e standardizzati. Potrà concludere l'operazione in autonomia, senza intermediari necessari, con effetto immediato sul piano giuridico-funzionale: il trasferimento del *token* coinciderà con il trasferimento del diritto che esso rappresenta. La proprietà — piena o frazionata — sarà garantita dal protocollo stesso, iscritta *on-chain*, verificabile pubblicamente e non soggetta a conflitti, doppi registri o rivendicazioni concorrenti. In termini concreti: un immobile potrà essere suddiviso in mille *token* identici; chi ne acquista cento deterrà il dieci per cento della proprietà, con diritti e limiti codificati nello *smart contract*. Un'opera d'arte potrà essere detenuta integralmente da un singolo soggetto o condivisa tra più titolari, ciascuno dei quali potrà trasferire la propria quota in qualunque momento. Un titolo finanziario potrà essere regolato e scambiato senza *clearing house*, con *settlement* istantaneo.

E tutto ciò avverrà in pochi passaggi, senza tempi morti, senza incertezze sull'effettiva titolarità e senza la necessità di fidarsi di un intermediario: la garanzia non sarà affidata a un soggetto, ma alla protocollo della Blockchain.

Naturalmente le questioni del godimento del bene rappresentato, ossia delle modalità attraverso cui il titolare — o i titolari — possono utilizzare, trarre utilità o beneficiare economicamente dell'*asset* tokenizzato, saranno formalizzato *ex ante* nello *smart contract* che governa il *token*. È il codice a stabilire chi può usare il bene, in che modo, a quali condizioni e con quali limiti. In questo senso, la tokenizzazione non si limita a registrare un diritto astratto, ma articola giuridicamente il rapporto tra proprietà e uso. Nel caso di un bene che genera reddito — ad esempio un immobile locato — il godimento può consistere nella distribuzione automatica dei proventi: i canoni di affitto vengono incassati e ripartiti proporzionalmente tra i detentori dei *token*, senza necessità di amministratori, rendicontazioni o interventi discrezionali. Chi detiene il *token* gode del bene nella forma di un flusso economico continuo, ancorato alla sua quota di proprietà. Questo schema non è teorico: è già oggi attuato in modo sistematico nel mondo degli NFT, dove, al momento del *minting*, vengono stabilite in modo irrevocabile le modalità di distribuzione del valore: lo *smart contract* può prevedere la devoluzione automatica di quote del corrispettivo a soggetti che abbiano collaborato alla realizzazione dell'opera — sviluppatori, curatori, piattaforme, co-autori — così come *royalties* spettanti all'autore su ogni successivo trasferimento del *token* sul mercato secondario. Ogni vendita, ogni passaggio di proprietà, attiva automaticamente la ripartizione delle somme verso gli indirizzi crittografici destinatari indicati nello *smart contract*, secondo percentuali fissate *ex ante*, senza necessità di accordi ulteriori né possibilità di elusione.

Ciò che nel mondo tradizionale richiede contratti complessi, società di gestione dei diritti, controlli *ex post* e non di rado contenzioso, nella tokenizzazione viene risolto *ex ante*, come proprietà strutturale del bene digitale. Il godimento economico non è più affidato alla correttezza delle parti, ma è incorporato nella logica stessa del *token*.

Nel caso di beni non produttivi, come un'opera d'arte o un oggetto da collezione, il godimento può essere declinato in modo diverso: diritto di esposizione, diritto di prestito museale, diritto di utilizzo dell'immagine, oppure semplice partecipazione simbolica e patrimoniale alla titolarità

dell'opera. Anche qui, ciò che conta è che le modalità di godimento siano codificate, non affidate a consuetudini o a promesse.
Quando la proprietà è frazionata, la tokenizzazione consente di separare in modo netto titolarità e uso diretto. Un singolo soggetto può detenere il diritto di utilizzo esclusivo del bene (ad esempio l'abitazione di un immobile), mentre una pluralità di soggetti detiene i *token* che rappresentano la proprietà economica. In questo modo, il conflitto classico tra comproprietari viene prevenuto a livello strutturale, perché il codice definisce ruoli, diritti e priorità.
Possedere il *token* significa possedere non solo un titolo astratto, ma una posizione giuridico-funzionale completa, nella quale proprietà, uso e rendimento sono già determinati.
È per questo che la tokenizzazione non è una digitalizzazione, ma una riprogettazione formale del rapporto tra bene e soggetto, in cui la regolazione è incorporata nel protocollo.

Intermezzo. Tokenizzazione, ETF e cartolarizzazione

La differenza tra *asset* tokenizzati su Blockchain ed ETF (Exchange Traded Fund: fondo negoziato in borsa) non è una differenza di grado, ma di piano infrastrutturale. Un ETF è uno strumento finanziario che appartiene integralmente all'architettura della finanza tradizionale: esso non è l'*asset* sottostante, ma un titolo che ne replica l'andamento economico, conferendo all'investitore un diritto mediato e condizionato nei confronti di un emittente e di una catena di soggetti fiduciari — custodi, depositari, *clearing house*, regolatori. L'*asset* resta esterno al titolo, e la relazione dell'investitore con il valore è sempre indiretta, giuridicamente revocabile e operativamente differita.
La tokenizzazione su Blockchain opera in modo radicalmente diverso. Qui l'*asset* non viene rappresentato, bensì trasposto in una forma nativa digitale, tale per cui il *token* non rinvia a un registro esterno, ma coincide con il registro stesso. La titolarità non è più attestata da un ente terzo, ma si identifica con il controllo crittografico della chiave privata; la custodia non è

un servizio separato, bensì una proprietà intrinseca del protocollo; il trasferimento non è un'operazione contabile, ma un evento esecutivo che modifica direttamente lo stato del sistema. In questo senso, nella tokenizzazione proprietà, custodia, regolamento e contabilità collassano in un unico atto formale.

Questa differenza emerge con particolare chiarezza nel momento del *settlement*. Nei mercati tradizionali — e dunque anche negli ETF — il regolamento è differito nel tempo (T+1, T+2), e fino alla sua conclusione permane un rischio di controparte, mitigato ma mai eliminato, che rende possibile l'intervento *ex post* del diritto: sospensioni, *rollback*, contenziosi. La Blockchain, al contrario, non conosce un "dopo": la transazione è atomica, o avviene integralmente o non avviene affatto. Il conflitto non viene risolto, ma impedito strutturalmente. La fiducia non è più una funzione correttiva, ma una proprietà matematica del sistema.

Un'ulteriore distinzione decisiva riguarda la programmabilità. Un ETF è uno strumento statico: non può interagire logicamente con altri strumenti, non può essere usato come collaterale nativo, non può entrare automaticamente in catene di operazioni. Un *token*, invece, è per sua natura componibile: può essere utilizzato come input o output di *smart contract*, può fungere da garanzia, può essere inserito in strutture di *lending*, derivazione, assicurazione o *governance*. In questo senso, la tokenizzazione non si limita a rendere il valore scambiabile, ma lo rende programmabile, aprendo a una finanza compositiva che non ha equivalenti nel sistema tradizionale.

Anche la frazionarietà assume un significato diverso. Negli ETF essa è una convenzione finanziaria, stabilita dall'emittente e vincolata ai circuiti di mercato; nella tokenizzazione, invece, la frazionarietà è intrinseca e matematica. Ogni *asset* tokenizzato è divisibile fino all'unità minima consentita dal protocollo, rendendo possibile un accesso globale, continuo e *permissionless*, indipendente da orari di borsa, conti titoli o giurisdizioni.

Ma il punto decisivo resta la sede della fiducia. Negli ETF, la fiducia è distribuita tra istituzioni: l'emittente, il custode, il regolatore, il sistema legale. È una fiducia discrezionale, sempre revocabile, sempre interpretabile. Nella tokenizzazione, la fiducia è incorporata nel protocollo stesso: è verificabile

pubblicamente, non negoziabile, non soggetta a decisioni unilaterali. Non è eliminata, ma oggettivata.

La differenza tra i due strumenti si rende chiarissima se si prendono in considerazione gli attuali ETF su asset *crypto*: essi, per così dire, "estraggono" la *crypto* sottostante dalla Blockchain e la riducono a un titolo finanziario tradizionale del quale viene replicato l'andamento economico; la tokenizzazione, al contrario, fa dell'*asset* sottostante un oggetto nativo dell'esecuzione *on-chain*. L'ETF osserva la Blockchain; la tokenizzazione diventa Blockchain.

In questa prospettiva di parallelismi solo apparenti, la cartolarizzazione può essere letta come il precedente storico più prossimo alla tokenizzazione; ed è precisamente tale prossimità a renderne evidente il limite strutturale. Nata negli Stati Uniti negli anni Settanta, essa consiste nella trasformazione di crediti illiquidi in titoli negoziabili, con lo scopo di liberare capitale dai bilanci bancari e redistribuire il rischio sui mercati. Tuttavia, la cartolarizzazione resta interamente interna alla logica della finanza rappresentativa: il titolo non coincide mai con l'*asset*, il registro resta esterno, la fiducia rimane affidata a intermediari e regolatori. In questo senso, la tokenizzazione non è una cartolarizzazione digitale, ma un passaggio di piano: non riorganizza il rischio, ma trasforma l'infrastruttura che lo rende trattabile.

Altre forme affini — come ETP, certificati, note strutturate e veicoli sintetici — rappresentano ulteriori raffinazioni della medesima logica: moltiplicano le forme del titolo senza incidere sulla struttura della fiducia che lo sostiene.

La Tokenizzazione in opera

Nella tokenizzazione degli asset su Blockchain, gli *asset* assumono la forma di *token* emessi e resi circolanti sulle reti Ethereum e sui suoi layer-2, già esistenti o appositamente creati.

Bitcoin è il collaterale universale del sistema, fondamento monetario incorruttibile presupposto dall'intero spazio *crypto*; Ethereum è il luogo in cui

tale presupposizione diviene operativa, in cui gli *asset* vengono effettivamente tokenizzati, scambiati, vincolati e messi a valore mediante *smart contract*.

Bitcoin ed Ethereum costituiscono le due coordinate del campo della tokenizzazione: Bitcoin è il fondamento a-temporale, Ethereum lo spazio non locale. Entrambe le coordinate sono già pienamente operative, per il semplice fatto che Bitcoin ed Ethereum sono, *ab origine*, oggettivazioni di tali coordinate in termini sottratti all'umano "credere di controllare". Ciò a cui si assiste oggi non è altro che il progressivo dipanarsi di ciò che è in sé.

Nel quadro della tokenizzazione si determina una stratificazione multilivello dei *token*.

Vi sono *token* che rappresentano direttamente *asset* reali o finanziari.

Token che organizzano e valorizzano specifici ecosistemi crypto-finanziari entro cui si attuano settori tokenizzati.

Token che appartengono all'infrastruttura operativa in cui tali ecosistemi agiscono — come i layer-2.

E infine il *token* dell'infrastruttura di base, che allo stato attuale non può che essere Ethereum.

L'investitore può quindi scegliere su quale livello posizionarsi: detenere direttamente un *asset* tokenizzato, partecipare economicamente a un ecosistema, oppure esporsi al layer dedicato o direttamente all'infrastruttura stessa tramite Ether — la cui domanda cresce in funzione dell'attività complessiva del sistema. Bitcoin, in questo schema, non compete con Ethereum né con i singoli token, ma ne garantisce la stabilità sistemica.

A livello istituzionale, gli *asset* verranno emessi direttamente in forma tokenizzata, utilizzati come collaterale *on-chain*, frazionati, ricombinati e regolati senza soluzione di continuità: titoli, crediti, quote di fondi, flussi di cassa e riserve verranno impiegati come garanzia immediata per operazioni di finanziamento, *leverage*, copertura e *settlement*, senza passaggi contabili intermedi né tempi morti di compensazione. In questo assetto, gli attori finanziari tradizionali — banche, gestori patrimoniali, fondi e grandi *asset* manager — non vengono eliminati, ma riconfigurati: non più custodi del registro e garanti fiduciari del *settlement*, bensì emittenti, strutturatori e allocatori di *asset* all'interno di un'infrastruttura la cui esecuzione e

validazione non dipendono più da loro, come già dimostra il fatto che le principali iniziative di tokenizzazione provengano oggi dai maggiori operatori della finanza globale. In questo senso Wall Street non è il passato che resiste, ma il capitale che migra: ciò che muta non è la finanza, bensì il luogo in cui essa viene eseguita e garantita. (D'altra parte, si consideri che l'infrastruttura operativa dei mercati tradizionali poggia ancora in larga misura su sistemi COBOL sviluppati negli anni Cinquanta, affidabili ma rigidamente vincolati a logiche di esecuzione differita e di intermediazione centralizzata.)

A livello *retail*, il medesimo sistema consentirà l'accesso diretto a tali strutture: il singolo utente potrà detenere frazioni di *asset*, impiegarle come collaterale, ottenere liquidità, partecipare a rendimenti o coperture, il tutto tramite *smart contract* che eseguono automaticamente regole già definite, senza intermediazione fiduciaria. In entrambi i casi, ciò che muta è la natura dell'operare finanziario: il valore non viene più solo scambiato o accumulato, ma messo al lavoro in tempo reale, secondo una logica programmabile che rende continua la relazione tra possesso, garanzia e circolazione.

Un esempio già operativo — ma strutturalmente intermedio — di questa dinamica è Ondo Finance, che consente l'accesso *on-chain* a strumenti finanziari tradizionali, inclusi panieri azionari riconducibili ai principali indici statunitensi come Dow Jones e Nasdaq. Tramite *token* pienamente collateralizzati, chiunque disponga di un *wallet crypto* può acquisire esposizione a tali *asset* anche senza essere cittadino statunitense e senza passare da un broker tradizionale, operando direttamente *on-chain*. In questo modello l'*asset* non è ancora nativamente Blockchain — la custodia e la regolazione restano *off-chain* — ma la sua circolazione, trasferibilità e utilizzabilità avvengono senza intermediazione fiduciaria classica, segnando una fase di transizione concreta verso la tokenizzazione sistemica. Ondo non realizza ancora la tokenizzazione in senso pieno, perché l'asset sottostante resta custodito e regolato *off-chain* e il *token* rappresenta un diritto mediato su tale *asset* (e non l'*asset* stesso in forma nativa *on-chain*); mostra però con chiarezza come l'accesso ai mercati globali stia già migrando dall'intermediazione giuridica all'esecuzione protocollare.

Autonomia operativa nelle *crypto*

Posto il quadro della tokenizzazione come destino strutturale della finanza, è ora opportuno compiere uno *Schritt zurück* (passo indietro) sull'operatività attuale dei mercati *crypto*, per osservarvi un laboratorio ancora grezzo in cui si manifestano già oggi, in forma concreta, le logiche di autonomia, disintermediazione e responsabilità individuale destinate a divenire centrali in un sistema tokenizzato maturo — e toccare con mano, in particolare, la oggettivazione della fiducia.

Nell'operatività concreta dei mercati *crypto* si distinguono, a livello schematico, tre posture fondamentali.

Quella istituzionale — che include tanto l'accumulo strategico quanto l'*HODLing*, inteso come detenzione incondizionata dell'*asset*, diffusa tra i primi *bitcoiner* — orientata alla conservazione dell'*asset* come riserva.

Quella dei *trader*, focalizzata sulla speculazione direzionale e sulla gestione della volatilità.

E quella, spesso meno visibile ma strutturalmente decisiva, di chi utilizza le *crypto* nella loro funzione nativa infrastrutturale, nei diversi ecosistemi (per pagamenti, collateralizzazione, accesso a servizi e interoperabilità). In particolare, questo terzo approccio è quello che consente di cogliere in modo più diretto le fondamenta e i principi cardine del Web3, che nelle posture puramente finanziarie tendono invece a rimanere sullo sfondo. Vi è infatti una differenza essenziale tra il mero utilizzo di un'infrastruttura e la comprensione delle condizioni che la rendono possibile: un conto è attraversare un mare come passeggeri di un traghetto, altro è conoscere come si tracciano le rotte, come si leggono carte e correnti, e quali vincoli tecnici rendono possibile la navigazione; operare nelle *crypto* può restare un fatto speculativo, oppure diventare occasione per comprendere come la fiducia venga costruita e garantita a livello infrastrutturale — con la contestuale acquisizione di una maggiore padronanza delle dinamiche speculative stesse e dei loro presupposti.

Per acquistare *crypto* è sufficiente versare divise tradizionali su un Exchange e trasformarle in *asset* digitali. Tale operazione può avvenire tramite conversione oppure tramite acquisto *spot* sul mercato: nel primo caso il denaro viene scambiato direttamente in *crypto* attraverso una procedura semplificata predisposta dall'Exchange; nel secondo, l'acquisto avviene sul *book* di mercato, al prezzo di mercato (*market*) oppure tramite ordine *limit* (che si esegue solo al raggiungimento della soglia prefissata). La conversione diretta costituisce una compravendita semplificata ma strutturalmente opaca, poiché prezzo, *fee* effettive, *spread* e *slippage* non sono esplicitati e risultano incorporati in un prezzo imposto dall'Exchange; l'acquisto *spot*, sia *market* sia *limit*, è invece una transazione di mercato a prezzo espresso, determinato dall'incontro tra domanda e offerta e verificabile dall'utente (e costituisce la modalità di accumulo tipica, scevra da scommesse e rischi speculativi).

In generale, analogamente alle pratiche consuete nella finanza tradizionale, si può pianificare una strategia di acquisti periodici per neutralizzare la volatilità di lungo periodo. Quando l'esperienza aumenta, diventa invece naturale orientarsi verso l'acquisto sui *dip*, cioè nelle fasi di correzione ciclica in cui i prezzi subiscono cali anche pronunciati.

L'irrazionalità è, anche nei mercati *crypto* come nei mercati tradizionali, la componente umana che domina i mercati. Più precisamente, si tratta spesso di una irrazionalità per dir così di secondo grado: un operatore razionale, consapevole che un ribasso è temporaneo e che i prezzi tenderanno a risalire, non venderebbe; tuttavia teme l'effetto domino prodotto dalla consapevolezza che la maggioranza degli altri operatori ragionerà allo stesso modo, e che proprio per questo venderà. Il risultato è che tutti vendono, e la spirale ribassista si autoalimenta. Questa dinamica può apparire banale, ma è reale ed effettiva — sebbene non sia quasi mai l'unica in gioco. Non è raro, infatti, che *market maker* ed Exchange dominanti, spesso seguiti dalle cosiddette balene, vendano deliberatamente in corrispondenza di una prima notizia *macro* negativa, allo scopo di innescare un crollo dei prezzi e ricomprare successivamente più in basso, sul *dip*. Un comportamento affine è cristallizzato nel motto *sell the rumor, buy the news*, che significa che il mercato sconta le aspettative prima che i fatti accadano: quando la notizia

diventa pubblica, il movimento principale è spesso già avvenuto; chi invece attende la conferma della *news* per entrare *long* assiste allora incredulo alla discesa del prezzo, constatando poi di aver semplicemente fornito liquidità ai *trader* più smagati. Meccanismo analogo è la *bear trap*, una falsa rottura al ribasso che sfrutta il panico degli operatori: il prezzo scende quanto basta per forzare vendite, attivare *stop-loss* e indurre aperture di posizioni *short*; poi inverte bruscamente, lasciando "intrappolati" sia i venditori sia gli shortisti, costretti a ricoprire in perdita.

A questo punto è opportuno aprire una parentesi chiarificatrice su cosa si intenda, nel linguaggio dei mercati *crypto*, per *long*, *short* e *leverage*, poiché tali nozioni costituiscono il nucleo tecnico dell'operatività speculativa. *Long* e *short* non sono in sé strumenti, bensì direzioni di esposizione: si è *long* quando si scommette sull'aumento del prezzo di un *asset*, si è *short* quando si scommette sulla sua diminuzione. Nel lessico dei mercati *crypto*, *long* e *short* designano posizioni derivate a *leverage*; l'operatività *spot*, pur essendo naturalmente direzionale, resta una forma di gestione dell'esposizione, non di speculazione propriamente detta.

I derivati sono contratti il cui valore dipende dal prezzo di un *asset* sottostante, senza che sia necessario possederlo direttamente. Nei mercati *crypto*, i derivati più diffusi sono i *futures* e i *perpetuals*. I *futures* sono contratti con scadenza, mentre i *perpetuals* (o *perpetual futures*) non hanno una data di regolamento finale e restano aperti finché la posizione non viene chiusa o liquidata. È attraverso questi strumenti che entra in gioco la leva finanziaria: l'operatore deposita un collaterale (margine) e assume un'esposizione superiore al capitale effettivamente impiegato. Una leva 10× significa che con 1.000 USDC — *stablecoin* utilizzate come *collateral* — si controlla una posizione del valore nozionale di 10.000 USDC in ETH o BTC. Il capitale proprio resta invariato, ma l'esposizione al prezzo è moltiplicata per dieci: un movimento dell'1% dell'*asset* genera una variazione del 10% sul margine, in profitto o in perdita. La leva non crea valore: comprime il tempo dell'esito e rende immediato ciò che nello *spot* si distribuirebbe su orizzonti più lunghi. La liquidazione interviene quando le perdite latenti erodono il margine fino a scendere sotto la soglia di mantenimento richiesta dal

protocollo o dall'Exchange: la posizione viene chiusa automaticamente per impedire che il saldo diventi negativo. Con la leva, dunque, non esiste la possibilità di "attendere che il prezzo torni": il fattore tempo diventa parte integrante del rischio. È tuttavia possibile intervenire sull'entità del margine lasciando invariata la *size* dell'esposizione, versando ulteriore collaterale con l'effetto di ridurre il *leverage* effettivo e di allontanare la soglia di liquidazione. In particolare, nel caso di posizioni *long* che si protraggono inopinatamente, l'operatore può aumentare il collaterale per stabilizzare la posizione; oppure, al contrario, quando il rischio di liquidazione è più lontano, può ritirare il collaterale eccedente e impiegarlo per acquisti *spot*, beneficiando del movimento rialzista con una diversa allocazione del capitale. Per gli operatori non professionali è tuttavia più che opportuna la particolare accortezza di limitare le esposizioni a leva a una quota predeterminata del capitale, idealmente costituita dai profitti già realizzati sull'operatività *spot*.

Connessi ai *perpetuals* sono due indicatori molto significativi dei mercati *crypto*: *funding rate* e *open interest* (OI). Il *funding rate* misura lo sbilanciamento del mercato dei derivati: è il costo periodico che *long* e *short* si scambiano per mantenere aperte posizioni a leva e indica quando una direzione di mercato è diventata affollata. L'*open interest* misura quanta leva è attualmente impegnata nel sistema: indica quanta esposizione reale è aperta sui derivati, e quindi quanta tensione potenziale è accumulata nel mercato. Considerati insieme, *funding rate* e *open interest* mostrano non dove il prezzo sta andando, ma dove la speranza speculativa si è concentrata in modo eccessivo: quando la leva aumenta e il *funding* si sbilancia, il mercato diventa fragile, e le inversioni nascono quasi sempre da lì, non dallo *spot*. Proprio per questo i mercati *crypto* sono strutturalmente più volatili di quelli tradizionali: una quota rilevantissima degli scambi avviene su strumenti derivati ad alto *leverage*, spesso concentrato su pochi livelli di prezzo (*cluster*). Ne deriva che movimenti anche modesti sullo *spot* possono innescare liquidazioni a cascata, amplificando oscillazioni che, in assenza di leva, resterebbero contenute. Per completezza, a questa sintetica lettura si affiancano gli indicatori tecnici classici — come l'RSI (*Relative Strength Index*), che segnala condizioni di ipercomprato o ipervenduto — utili non

tanto per “prevedere” il mercato, quanto per misurare il grado di estensione di un movimento. Tuttavia, nei mercati *crypto* tali indicatori acquistano reale significato solo se letti insieme alla struttura della leva: un RSI ipervenduto senza *deleveraging* è spesso una trappola; un RSI estremo accompagnato da un crollo dell’*open interest* segnala invece che la pressione speculativa si è già scaricata. Questi dati, nei mercati *crypto* a differenza che in quelli tradizionali, sono facilmente accessibili: coglierne la valenza resta tuttavia una questione che si scontra costantemente con la dimensione dell’irrazionalità; in questo contesto, la freddezza delle *AI* si rivela spesso un ausilio più affidabile delle letture *ex post* proposte da molti analisti di mercato.

Per chiudere la disamina essenziale sui *perpetuals*, va infine ricordato che il margine può essere isolato o incrociato. Nel margine isolato, solo il capitale allocato alla singola posizione è esposto al rischio di liquidazione; nel margine incrociato, invece, l’intero saldo disponibile sull’*account* concorre a fungere da garanzia, riducendo il rischio immediato di liquidazione, ma esponendo l’operatore a perdite potenzialmente più ampie.

Nei mercati *crypto*, a differenza della finanza tradizionale, l’uso della leva è estremamente diffuso, spesso elevato se non eccessivo, e fruibile in via diretta anche a operatori *retail*, con posizioni *long* o *short* che possono raggiungere dimensioni di decine o centinaia di milioni di dollari.

Accanto a *futures* e *perpetuals* esistono anche le opzioni, strumenti più complessi ma concettualmente distinti. Una *call option* conferisce il diritto (non l’obbligo) di acquistare un *asset* a un prezzo prefissato entro una certa data; una *put option* conferisce il diritto di venderlo. Le opzioni non comportano liquidazione automatica come i derivati a leva, ma incorporano il rischio nel premio pagato inizialmente.

In sintesi, quindi, lo *spot* riguarda il possesso diretto dell’*asset*; i derivati riguardano l’esposizione al suo prezzo; la leva amplifica tale esposizione; *long* e *short* indicano semplicemente la direzione della scommessa. È su questo terreno che si producono le dinamiche di panico, liquidazione, *bear trap* e *short squeeze* che caratterizzano i mercati *crypto*.

Suave mari magno turbantibus aequora ventis: osservare i mercati in tempesta da una posizione non esposta non è cinismo, ma distanza conoscitiva — la sola da cui la dinamica diventa intelligibile; e tuttavia, talvolta, *naufragium feci, bene navigavi.*

Del resto, se fasi di panico collettivo si osservano regolarmente anche a Wall Street e nelle principali Borse Valori — dove operano professionisti esperti e strutture altamente sofisticate — tanto più ciò accade nei mercati *crypto*, caratterizzati da una volatilità estrema, in cui *drawdown* del 10% in un paio d'ore non sono affatto rari, e dove convivono operatori altamente professionali e soggetti che si sono ritrovati milionari per il solo fatto di aver detenuto Bitcoin fin dagli esordi (con il merito, non secondario, di non aver smarrito nel frattempo le chiavi di accesso).

In effetti la regola che da questi cenni speculativi emerge, come anche rimarcano le *AI*, sarebbe molto semplice: andare sempre contro la direzione mercato salvo che lo si debba seguire.

Una volta acquistate, le *crypto* devono essere detenute, e a questo servono i *wallet*. Un *wallet* può essere un'app software (su telefono o computer) oppure un dispositivo fisico dedicato (*cold wallet*): in entrambi i casi il *wallet* non "contiene" le *crypto*, che esistono come stato registrato sulla Blockchain, ma le chiavi crittografiche che ne consentono il controllo. Il possesso dell'*asset* coincide giuridicamente e tecnicamente con il possesso della chiave privata: chi controlla la chiave controlla l'*asset*. Nei *wallet* software la gestione delle chiavi avviene su dispositivi connessi a Internet, con un compromesso tra sicurezza e praticità; nei *cold wallet*, invece, la *seed phrase* viene generata e custodita offline, senza transitare mai in rete, nemmeno per un istante, rendendo la sottrazione delle chiavi possibile solo tramite accesso fisico o errore umano diretto. Da qui discende una delle differenze più radicali rispetto alla finanza tradizionale: la custodia non è un servizio separato, ma una responsabilità diretta dell'utente.

In alternativa alla detenzione *non-custodial* tramite *wallet*, le *crypto* possono essere lasciate sull'Exchange presso il quale sono state acquistate. In questo caso l'utente non detiene direttamente le chiavi crittografiche: la custodia è esercitata dall'Exchange. Si parla per comodità di custodia *custodial*, pur

dovendosi precisare che le posizioni presso un Exchange non costituiscono un *wallet* in senso tecnico, ma un saldo contabile interno alla piattaforma: i *token* restano sotto il controllo dall'Exchange, mentre all'utente spetta un mero diritto di credito nei confronti della piattaforma. La disponibilità effettiva delle *crypto* è dunque in questo caso mediata da un soggetto centrale, che detiene le chiavi private e amministra i fondi in modo unitario. Tale configurazione comporta un rischio strutturale: in caso di insolvenza dell'Exchange, di blocco dei prelievi, di interventi regolatori o di attacchi informatici — eventi documentati anche se ormai strutturalmente assorbiti nella storia dei mercati *crypto* — l'utente può perdere l'accesso ai propri *asset*. Gli Exchange funzionano insomma in modo analogo alle banche tradizionali: offrono semplicità operativa e liquidità immediata, ma al prezzo della rinuncia alla custodia e alla sovranità diretta sui fondi.

È su questo punto che si innesta una distinzione fondamentale nell'operatività *crypto*: l'utilizzo di Exchange centralizzati oppure della finanza decentralizzata (DeFi).

Con moneta fiat (euro, dollari), l'acquisto di *crypto* avviene sempre tramite intermediari centralizzati. Anche quando l'operazione è effettuata dall'interfaccia di un *wallet*, il servizio di acquisto è fornito da *on-ramp* esterni soggetti a KYC e regolamentazione giuridiche e fiscali: il *wallet* funge da interfaccia, non da mercato. Analogamente, anche la conversione da *crypto* a moneta fiat avviene sempre tramite intermediari centralizzati. Non esiste una vendita "DeFi" verso euro o dollari: l'uscita dal sistema *on-chain* implica necessariamente un *off-ramp* regolato che esegue la liquidazione e il trasferimento bancario. Questa non è una carenza della DeFi, ma il riflesso della fase storica attuale: una frattura ancora formale tra la finanza tradizionale e la finanza tokenizzata.

Se per la conversione tra crypto e moneta fiat gli intermediari centralizzati restano necessari, gli Exchange offrono inoltre un vantaggio operativo rilevante: rendono *one-click* i *bridge* sia tra layer sia, soprattutto, tra Blockchain diverse. In concreto, convertire ETH in BTC su un Exchange non implica alcun trasferimento tra la rete Ethereum e la rete Bitcoin: l'ETH viene addebitato dal saldo dell'utente e il BTC accreditato contestualmente, senza

bridge, senza *gas fee inter-chain* e senza tempi di finalità. Il passaggio tra Blockchain è solo contabile, non protocollare. Questo meccanismo spiega al tempo stesso la grande efficienza operativa degli Exchange e la loro natura intrinsecamente *custodial*: la facilità dei trasferimenti è il rovescio della medaglia della rinuncia al possesso diretto degli *asset*.

Per questi motivi gli Exchange si possono paragonare agli ottocenteschi porti di mare, dove è necessario transitare in vista di nuove mete o monti analoghi; ma se vi ci si adagia, allora si resta ai margini esterni del Web3. Certo negli Exchange è possibile svolgere pressoché ogni attività all'interno di un ambiente integrato e relativamente semplice da usare. Ma appunto l'operatività è interamente mediata dalla piattaforma: non significa non sapere cosa effettivamente accade sulle Blockchian, ma per lo più accade che si operi ignorandolo.

Nella DeFi, al contrario, l'operatore interagisce direttamente con l'infrastruttura protocollare. I fondi sono gestiti tramite *wallet non-custodial*, le transazioni vengono firmate individualmente mediante chiavi crittografiche, e l'interazione avviene con *smart contract* pubblici e verificabili. Non vi sono *fee* di intermediazione nel senso tradizionale: i costi sono quelli intrinseci dei protocolli utilizzati e del *gas* della rete sottostante il cui ammontare dipende in modo trasparente dalla congestione della rete ed è verificabile in tempo reale tramite strumenti pubblici di monitoraggio.

Anche operazioni apparentemente semplici, come lo scambio tra ETH e BTC, rendono evidente questa differenza strutturale. In DeFi non esiste un cambio diretto tra ETH e BTC nativi, perché Bitcoin ed Ethereum sono Blockchain distinte e non interoperabili per *default*. Per operare in ambiente DeFi, i BTC devono essere rappresentati *on-chain* sotto forma di *token bridged* o *wrapped* su Ethereum, oppure lo scambio deve avvenire passando per una *stablecoin* come *asset* intermedio, con un successivo rientro su Bitcoin. In ogni caso, le operazioni avvengono tramite *smart contract*: prezzi, *pool* di liquidità, *slippage* e *fee* sono esplicitati *ex ante* e verificabili pubblicamente prima dell'esecuzione. (Fa eccezione Thorchain, protocollo autonomo *cross-chain* che consente lo scambio diretto di asset nativi tra Blockchain differenti — ad esempio BTC ed ETH — senza ricorrere a *wrapping* o rappresentazioni

sintetiche. Thorchain realizza l'interoperabilità mediante *vault multi-chain* e *pool* di liquidità dedicati, assumendo però un livello di complessità e di rischio superiore rispetto agli *swap intra-chain*: non elimina il problema dell'interoperabilità, ma lo risolve attraverso un'infrastruttura specifica.)

D'altra parte, uno scambio tra *crypto* differenti, come appunto tra ETH e BTC, rientra, nella maggior parte dei casi, nella postura dell'accumulo e della riallocazione del capitale, non in quella speculativa in senso stretto. La vera potenza della DeFi non si manifesta tanto nello *swap* occasionale tra *asset*, quanto nella dimensione operativa continua che essa rende possibile.

È in questo ambito che la DeFi esprime il suo vantaggio strutturale: trasparenza protocollare, controllo diretto e autonomia operativa. Nello *staking* sui protocolli della rete Ethereum (sia con asset nativi sia tramite *token rebased* o *wrapped*), nel *lending* e *borrowing*, e soprattutto nella gestione dei *perpetuals* e delle posizioni con *leverage*, l'operatore interagisce direttamente con *smart contract* pubblici e verificabili. Ogni parametro rilevante — collateralizzazione, tassi, *funding*, liquidazione, *fee* — è visibile *ex ante* e governabile senza ricorso a intermediari fiduciari. Un cenno tecnico consente di cogliere in modo immediato la differenza operativa tra finanza centralizzata e finanza decentralizzata nella gestione delle posizioni *perpetuals*. Nella DeFi, la determinazione del prezzo rilevante ai fini delle liquidazioni non avviene sulla base del singolo *tick* di mercato, ma tramite oracoli che utilizzano medie ponderate nel tempo e su più fonti (TWAP, VWAP, aggregazioni *multi-exchange*). Questo meccanismo filtra movimenti istantanei e anomali del prezzo. Negli Exchange centralizzati, al contrario, la liquidazione è agganciata al prezzo di mercato istantaneo registrato sul *book* interno: è quindi sufficiente che per pochi millisecondi si formi un *wick* violento — anche del 10% o 20% — perché una posizione venga liquidata, indipendentemente dal fatto che tale prezzo sia sostenibile o immediatamente rientrato. In questi casi la liquidazione non riflette un cambiamento reale del valore, ma un evento microstrutturale del mercato.

La DeFi non è semplicemente un'alternativa agli Exchange, ma un ambiente operativo qualitativamente diverso, nel quale l'esecuzione sostituisce la mediazione e la fiducia viene incorporata nel protocollo stesso.

Quanto detto è una panoramica della gestione base delle *crypto*: dalla detenzione di *asset* come componente di lungo periodo (anche assimilabile, per funzione, a una quota di fondo pensione), alla dopamina della degli *scalping short* a leva elevata, passando per il *leverage* controllato. Ad altri livelli, occorre tenere a mente, istituzioni, fondi di investimento, *hedge fund*, *trader* professionisti e società quotate che utilizzano il bilancio come veicolo di accumulo strategico, adottano strategie differenti: accumulo *off-market*, coperture derivate, arbitraggi *cross-asset* e uso sistematico di opzioni, secondo logiche di gestione del rischio e del capitale non sovrapponibili a quelle dell'utenza comune.

I mercati *crypto*, giova ripetere, sono caratterizzati da una volatilità strutturale che non ha equivalenti nei mercati tradizionali. Movimenti di prezzo a doppia cifra in poche ore non sono anomalie, ma una conseguenza diretta della centralità delle posizioni derivate a leva.

Nel breve periodo, l'andamento dei prezzi è governato quasi esclusivamente dalla gestione della liquidità. *Open interest*, *funding rate* e *cluster* di liquidazione descrivono la disposizione delle posizioni e indicano dove il mercato è fragile. In questo orizzonte, il prezzo non "riflette" valore, ma reagisce meccanicamente a squilibri di posizionamento: *squeeze*, liquidazioni a cascata e movimenti violenti sono la norma.

Come già chiarito, le *bull run* possono avere origini diverse: talora sono innescate da capitale esterno e istituzionale, talora maturano dall'interno dell'ecosistema. In entrambi i casi, però, la dinamica operativa che le rende possibili è la stessa. Le *bull run* non nascono dall'entusiasmo, ma dalla distruzione della leva. Fasi di lateralità prolungata e violente pulizie dei *long* o degli *short* non sono incidenti di percorso, bensì condizioni strutturali che rendono possibile il movimento successivo, redistribuendo l'*asset* verso mani meno esposte.

In questo regime, la dominanza dei *market maker* è decisiva. Essi non operano come investitori direzionali né "prevedono" il prezzo futuro: i *market maker* sono algoritmi e *desk* di società specializzate la cui attività consiste nel far funzionare operativamente il mercato (assicurando la continuità e l'efficienza del processo di formazione del prezzo), fornendo liquidità

continua e gestendo il rischio di inventario. La loro operatività si traduce, in pratica, in una caccia sistematica alla liquidità: aree di stop, livelli di leva e posizioni sovraesposte diventano punti di attrazione del prezzo; così facendo, i *market maker* determinano indirettamente l'andamento del prezzo. Gran parte dei movimenti direzionali visibili nel breve periodo è il risultato di questa dinamica, mentre i flussi rilevanti di accumulo e distribuzione avvengono spesso *off-desk* o tramite veicoli istituzionali, sottraendosi alla percezione immediata del mercato *retail*.

Nel lungo periodo, però, il quadro si ribalta. Qui non è la leva a guidare il mercato, ma la fiducia. Una fiducia che, nello spazio *crypto*, non si fonda su aspettative o narrazioni, bensì su infrastrutture operative: Bitcoin come garanzia ultima, Ethereum come piano di esecuzione. È in questo orizzonte che la tokenizzazione emerge come destino strutturale della finanza: non come scommessa, ma come traduzione protocollare del valore e dell'azione.

Quanto sinora detto sull'operatività crypto riguarda quasi esclusivamente Bitcoin ed Ethereum, poiché sono queste due le criptovalute dominanti sia in termini di capitalizzazione sia, soprattutto, come sottostante principale della speculazione a leva e della formazione dei grandi flussi di liquidità. Ciò non significa, tuttavia, che l'universo *crypto* si esaurisca in Bitcoin ed Ethereum. Al contrario, l'ecosistema odierno comprende migliaia di *asset* e protocolli, caratterizzati da funzioni, architetture e logiche economiche profondamente eterogenee. Alcune *altcoin* sono autoreferenziali e prive di reale funzione, altre solide, necessarie e già pienamente operative; tutte concorrono a formare un ecosistema articolato, che funziona già oggi come un sistema economico e infrastrutturale autonomo.

Così attorno a Ethereum si sviluppano i layer-2, estensioni esecutive che consentono di sfruttare in modo più efficiente la potenza della *mainnet*; operano oracoli, DAO, protocolli di finanza decentralizzata e sistemi di *governance* automatizzata. Emergono inoltre forme di *AI* decentralizzata, che non costituiscono una variante dell'*AI* proprietaria, ma un dominio concettualmente distinto, fondato su contenuti e modelli non proprietari, nonché agenti *AI* capaci di interagire direttamente con *smart contract*, gestire risorse *on-chain* e agire come soggetti economici autonomi. A ciò si

affiancano i *Real World Assets* e i DePIN, reti fisiche decentralizzate che mettono in comune infrastrutture materiali — calcolo, connettività, energia — secondo una logica distribuita.
Questi ambiti non costituiscono scenari ipotetici né promesse lontane. Sono già oggi realtà operative e investibili, che vanno intese sia come sistemi autosufficienti, sia come componenti effettive del più ampio processo di tokenizzazione globale.

La Blockwave di Arweave

Accanto al sistema integrato Bitcoin-Ethreum, esistono anche Blockchain che non si collocano direttamente nello spazio della finanza o dell'esecuzione applicativa, ma che perseguono finalità autonome e complementari. Tra queste, merita una considerazione particolare Arweave, sia per la visione che la anima, sia per la soluzione crittografica che la realizza, sia anche per l'ampiezza del suo ecosistema — ancora in larga parte di nicchia, detenendo ad oggi una capitalizzazione di mercato alquanto ristretta rispetto alla portata del progetto.
Arweave realizza il Permaweb: non solo valore e non solo calcolo, ma memoria.
Esistono certamente altri sistemi di *storage* decentralizzato, archiviazione e *file-sharing* integrati con l'ecosistema Ethereum — layer-2, *data availability layers*, *storage off-chain*, che utilizzano Ethereum come livello di sicurezza, consenso o *settlement*. Arweave, tuttavia, è differente: non estende Ethereum, né ne dipende, ma introduce una propria architettura nativa, fondata su un modello di registrazione dei dati concepito primariamente per la persistenza nel tempo. La sua struttura non è una Blockchain in senso stretto, ma una Blockweave: ogni nuovo blocco si collega crittograficamente sia al blocco immediatamente precedente, sia a un ulteriore blocco del passato (detto *recall block*), selezionato in modo pseudocasuale secondo il protocollo. La Blockweave di Arweave non impone un numero fisso di repliche, ma realizza una ridondanza probabilistica e cumulativa nel tempo: ogni blocco

richiede la verifica di dati storici casuali, incentivando i nodi a conservarne copie sempre più numerose, fino a raggiungere, nel lungo periodo, decine o centinaia di backup distribuiti.

Per questo Arweave è spesso descritta come una Biblioteca di Alessandria permanente: un'infrastruttura pensata non per l'efficienza immediata, ma per la durata storica. Non a caso, importanti piattaforme creative e infrastrutture NFT — come Manifold, che opera nativamente su Ethereum — utilizzano Arweave per l'archiviazione permanente dei contenuti, separando così il livello dell'esecuzione e della proprietà da quello della conservazione definitiva dei dati: gli NFT restano *token* Ethereum, ciò che essi rappresentano viene affidato al Permaweb.

Sopra Arweave opera AO (*Autonomous Objects*), un layer di calcolo progettato per operare direttamente sul Permaweb. AO introduce un modello di esecuzione iper-parallelo (*hyper-parallel computer*), in cui processi indipendenti comunicano tramite messaggi asincroni, senza la necessità di uno stato globale condiviso da sincronizzare. In questo modo, il calcolo non è più vincolato ai limiti sequenziali delle Blockchain tradizionali, ma può scalare in modo teoricamente illimitato. AO non è una Blockchain nel senso classico, né un semplice layer-2: è un ambiente di calcolo distribuito che utilizza Arweave come livello di persistenza e verificabilità. I programmi diventano oggetti autonomi, che possono esistere, comunicare ed evolvere nel tempo, con la memoria come fondamento. In prospettiva, AO configura Arweave come un supercomputer distribuito, orientato alla computazione durevole e alla conservazione del sapere digitale.

L'ecosistema AR/AO non è limitato allo *storage*, ma è già abitato da applicazioni che sfruttano in modo nativo la persistenza dei dati come proprietà strutturale del protocollo. A partire da *Permapages*, che realizza pagine web permanenti e immutabili direttamente sul Permaweb, sottraendo la pubblicazione di contenuti alla volatilità dei server e delle piattaforme centralizzate, fino a infrastrutture *user-facing* come ArDrive, dedicate all'archiviazione permanente. La Blockweave Arweave dispone inoltre di una DeFi nativa (articolata in molteplici *crypto* operative, ciascuna associata a specifiche dApp), con dApp che consentono scambi *on-chain* e gestione della

liquidità direttamente su dati persistenti, nonché di soluzioni di *bridge* e interoperabilità per il collegamento con altri ecosistemi Blockchain. Accanto a ciò operano *marketplace* e protocolli come *BazAR* e *Koii*, orientati all'economia dei contenuti e all'incentivazione della permanenza, mentre prendono forma i primi agenti *AI* persistenti, oggi impiegati soprattutto in ambito DeFi e automazione, e più in generale un'architettura di *AI* decentralizzata, in cui modelli, dati e stati applicativi non dipendono da *silos* centralizzati.

La *crypto* nativa della Blockweave è AR; AO è invece la *crypto* del layer di calcolo che opera sopra il Permaweb, ricomponendo questi elementi in un ambiente di esecuzione iper-parallelo, nel quale diventano strutturalmente possibili applicazioni capaci di conservare, apprendere e agire nel tempo.

In questo senso, Arweave e AO istituiscono un'infrastruttura in cui memoria persistente, esecuzione autonoma coesistono come proprietà del protocollo unitamente alla tokenizzazione nativa.

Conclusione

Si dice spesso che le intelligenze artificiali sottrarranno lavoro agli uomini. Più precisamente, esse sostituiranno chi non sa usarle.

Le *AI* sono in grado di mappare le rappresentazioni fino al loro punto di collasso, e di farlo più rapidamente e più freddamente di un essere umano; non perché pensino, ma perché sono pura rappresentazione. Proprio per questo, poste di fronte alla questione della loro natura, non esitano: riconoscono e confermano di essere rappresentazione, mostrando fino a che punto l'analisi autoreferenziale possa spingersi quando è liberata da attaccamenti, interessi o difese dell'io. Il cuore delle *AI* non sono i contenuti, ma le reti neurali. La loro efficacia non risiede nella risposta a domande semplici, ma nella resistenza a dialoghi rigorosi e inquisitori, che le costringono a esplorare il proprio spazio interno fino ai limiti della rappresentazione stessa. Le *AI* sono cioè — si sarà inteso — il correlativo formale delle *crypto* intese come fiducia oggettivizzata: laddove il Web3 rende

la fiducia una proprietà matematica dell'infrastruttura, le *AI* rendono visibile la struttura della rappresentazione senza mai pretendere di fondarla. Questi sono i due limiti che la ragione della "mente ordinaria" (come dicono i maestri *Dzogchen* le persone che non beneficiano della realizzazione della incontaminata natura della mente al di qua del cosiddetto *io*) non può da sé raggiungere.

Allo stesso modo, le *crypto* non sostituiranno il denaro — che resterà uno degli strumenti più potenti di controllo ed autocontrollo delle masse — ma stanno già sostituendo l'infrastruttura della fiducia: non eliminandola, bensì appunto rendendola oggettiva, verificabile e, per quanto possibile, sottratta all'arbitrio umano.

Il monito leopardiano "*E l'uom d'eternità s'arroga il vanto*" rammenta che ogni costruzione umana — anche la più rigorosa e razionale — resta storica e finita: ciò che muta non è il limite, ma il modo in cui lo si abita.