V. Criptovalute: al di là del fenomeno alla moda

A meno di 10 anni dalla loro comparsa, le criptovalute[1] sono emerse dall'oscurità e hanno cominciato a suscitare un vivo interesse in aziende e consumatori, nonché in banche centrali e altre autorità. Attraggono l'attenzione perché promettono di sostituire la fiducia in istituzioni consolidate come banche commerciali e centrali con quella in un nuovo sistema completamente decentralizzato, basato sulla blockchain e sulla tecnologia a essa collegata, la DLT (distributed ledger technology, o tecnologia a libro mastro distribuito).

Questo capitolo intende capire se le criptovalute potrebbero avere un ruolo in quanto moneta: al di là del fenomeno alla moda, quali problemi economici specifici possono risolvere (se ne possono risolvere) le criptovalute attuali? Il capitolo inizia con una panoramica del contesto storico. Numerosi episodi di instabilità monetaria e valute cadute in disuso mostrano che gli assetti istituzionali tramite i quali viene fornita la moneta sono molto importanti. Questa panoramica mostra che l'essenza della moneta "buona" è sempre stata la fiducia rispetto alla stabilità del suo valore. E affinché la moneta sia all'altezza del compito che le è attribuito – agire come un dispositivo di coordinamento per facilitare le transazioni – è necessario che il suo volume si adegui efficacemente all'andamento dell'economia e che la sua offerta sia elastica per rispondere alle fluttuazioni della domanda. Ciò richiede assetti istituzionali specifici, ed è per questo che sono state create le banche centrali come le conosciamo oggi, autonome e responsabili del loro operato.

Il capitolo continua poi con un'introduzione alle criptovalute e analizza i limiti economici inerenti alla decentralizzazione della fiducia su cui esse si basano. Affinché tale fiducia possa essere mantenuta, è necessario che la grande maggioranza della potenza computazionale sia controllata da operatori onesti della rete, che ogni singolo utente verifichi la storia delle transazioni, e che l'offerta della criptovaluta sia predeterminata dal suo protocollo. La fiducia può evaporare in qualsiasi momento a causa della fragilità del consenso decentralizzato tramite il quale vengono registrate le transazioni. Ciò non solo mette in discussione la definitività dei pagamenti individuali, ma significa anche che una criptovaluta può semplicemente smettere di funzionare, portando a una completa perdita di valore. Inoltre, anche nel caso in cui sia possibile mantenere la fiducia, la tecnologia delle criptovalute è poco efficiente e comporta un grande impiego di energia. Le criptovalute non possono adattare il loro volume alla domanda di transazioni, sono inclini alla congestione e oggetto di forti oscillazioni di valore. A conti fatti, la tecnologia decentralizzata delle criptovalute, sebbene sia sofisticata, rappresenta uno scadente sostituto del solido sostegno istituzionale della moneta.

Ciò detto, la tecnologia potrebbe essere promettente per altre applicazioni, come la semplificazione dei processi amministrativi relativi al regolamento delle transazioni finanziarie. Ma questo resta da dimostrare. Di fronte alle molteplici questioni sollevate dalle criptovalute, il capitolo si conclude con un'analisi delle risposte sul piano delle politiche, tra cui la regolamentazione degli utilizzi privati della tecnologia, le misure necessarie per evitare usi indebiti delle criptovalute e le delicate questioni sollevate dall'emissione di valuta digitale da parte delle banche centrali stesse.

L'ascesa delle criptovalute in prospettiva

Un buon modo per capire se una nuova tecnologia potrebbe essere un'aggiunta realmente utile al panorama monetario esistente è fare un passo indietro e passare in rassegna le principali funzioni della moneta in un'economia e quello che ci insegna la storia riguardo ai tentativi falliti di creare nuove monete private. Successivamente ci si può chiedere se una moneta basata su questa tecnologia potrebbe migliorare in qualche modo l'attuale panorama monetario[2].

Una breve storia del denaro

La moneta gioca un ruolo chiave per la facilitazione degli scambi economici. Prima dell'avvento del denaro, migliaia di anni fa, i beni erano scambiati principalmente con la promessa di rendere il favore in futuro (ovvero tramite lo scambio di "pagherò")[3]. Tuttavia, con la crescita delle società e dell'attività economica, divenne più difficile tenere un registro di pagherò sempre più complessi, e i rischi di insolvenza e di regolamento cominciarono a essere fonte di preoccupazione. La moneta e le istituzioni che la emettono nacquero per far fronte a questa crescente complessità e alla relativa difficoltà di mantenere la fiducia.

La moneta ha tre ruoli fondamentali e complementari. È: (1) un'unità di conto, ovvero un parametro che facilita il confronto tra i prezzi dei beni che compriamo, così come il valore delle promesse che facciamo; (2) un mezzo di scambio: un venditore lo accetta come mezzo di pagamento, con l'aspettativa che qualcun altro farà la stessa cosa nei suoi confronti; e (3) una riserva di valore, che permette agli utilizzatori di trasferire il potere d'acquisto nel tempo[4].

Per adempiere a queste funzioni, la moneta deve avere lo stesso valore in luoghi diversi e mantenere un valore stabile nel tempo: decidere se vendere un determinato bene o servizio è molto più facile se si è sicuri che la valuta che si riceve in cambio ha un valore garantito in termini di potere d'acquisto presente e futuro. Un modo per raggiungere questo obiettivo è tramite vere e proprie monete merce con un valore intrinseco, come sale o grano. Ma la moneta merce di per sé non sostiene lo scambio in modo efficace: potrebbe non essere sempre disponibile, è costosa da produrre e scomoda da scambiare, e può essere deperibile[5].

L'espansione dell'attività economica richiedeva monete più pratiche, che potessero rispondere alla crescente domanda, che potessero essere usate in modo efficiente nel commercio e che avessero un valore stabile. Tuttavia, la sfida più importante è sempre stata quella di mantenere la fiducia negli assetti istituzionali tramite i quali la moneta viene fornita. In tutto il mondo, in diversi contesti e in momenti diversi, la moneta cominciò a dipendere dall'emissione da parte di autorità centralizzate. Nell'antichità, il sigillo di un sovrano certificava il valore di una moneta per le transazioni. Più tardi, vennero create cambiali con intermediazione bancaria che i commercianti usavano al fine di limitare i costi e i rischi di viaggiare con grandi quantità di monete[6].

Tuttavia, l'esperienza storica ha anche messo in luce un dilemma di fondo: le valute a offerta flessibile possono anche svalutarsi con facilità[7]. Storicamente, gli episodi prolungati di monete stabili sono senza dubbio più l'eccezione che la norma. Anzi, la fiducia è venuta meno così frequentemente che la storia è diventata un cimitero di monete. Musei di tutto il mondo dedicano intere sezioni a questo cimitero: per esempio, nella sala 68 del British Museum troviamo pietre, conchiglie, tabacco,

innumerevoli monete metalliche e pezzi di carta e molti altri oggetti che non sono più accettati come mezzi di scambio e costituiscono ora la collezione di questa sala. Alcuni finirono vittime dell'espansione del commercio e dell'attività economica, dato che erano diventati inadeguati per un uso su larga scala, alcuni uscirono di scena quando l'ordine politico che li supportava si indebolì o crollò e molti altri caddero vittime dell'erosione della fiducia nella stabilità del loro valore.

La storia dimostra che la moneta può essere fragile, sia che venga fornita attraverso mezzi privati, in una logica concorrenziale, sia che venga fornita da uno Stato sovrano, come monopolista. La solidità della moneta emessa da una banca dipende da quella delle attività che la sorreggono. Le banche sono state create per trasformare i rischi e pertanto, in alcune circostanze estreme, la fiducia nella moneta emessa privatamente può svanire da un giorno all'altro. Ma nemmeno i sistemi sostenuti dallo Stato, in cui il garantire la fiducia nello strumento è un compito centralizzato, hanno sempre funzionato bene, al contrario: un esempio ben noto è la svalutazione delle monete emesse dai principi tedeschi all'inizio del XVII secolo, passata alla storia come Kipper- und Wipperzeit[8]. E ci sono molti altri esempi, fino al Venezuela e allo Zimbabwe dei giorni nostri. Evitare usi indebiti da parte dello Stato è quindi un elemento chiave nell'elaborazione degli assetti monetari.

La ricerca di un solido puntello istituzionale per la fiducia nella moneta alla fine sfociò nell'affermazione delle banche centrali odierne. Una prima tappa fu la creazione di banchi pubblici autorizzati nelle città-Stato europee, tra il XV e il XVII secolo. Queste banche emersero per migliorare i commerci fornendo mezzi di pagamento efficienti e di elevata qualità e centralizzando una serie di operazioni di compensazione e regolamento. Istituite in snodi commerciali come Amburgo, Amsterdam, Barcellona, Genova e Venezia, servivano a stimolare il commercio internazionale e più in generale l'attività economica[9]. Nel corso del tempo, molte di queste banche cominciarono a funzionare in modi simili a quelli delle attuali banche centrali. Le banche centrali ufficiali, così come le conosciamo oggi, spesso sono emerse anche come reazione diretta a esperienze negative con una moneta decentralizzata. ad esempio, i fallimenti delle banche non regolamentate (*wildcat banking*) negli Stati Uniti portarono alla creazione del Federal Reserve System.

Il sistema monetario e di pagamento attualmente in vigore

Nell'epoca moderna, il modo testato, fidato e resiliente per generare fiducia nella moneta è la banca centrale indipendente. Una banca centrale indipendente significa finalità concordate, ovvero obiettivi chiari di politica monetaria e di stabilità finanziaria, indipendenza operativa, amministrativa e in materia di strumenti e rendicontabilità democratica per garantire ampio supporto politico e legittimità. Le banche centrali indipendenti hanno largamente raggiunto il loro obiettivo di salvaguardare l'interesse economico e politico della società ad avere una valuta stabile[10]. In questa configurazione, la moneta può essere appropriatamente definita come una "convenzione sociale indispensabile sostenuta da un'istituzione statale che rende conto del suo operato e gode della fiducia dei cittadini"[11].

In quasi tutte le economie moderne, l'offerta di moneta avviene tramite un'alleanza pubblico-privato tra la banca centrale e le banche private, con la banca centrale al centro del sistema. I depositi bancari elettronici sono il mezzo principale di pagamento tra gli utenti finali, mentre le riserve della banca centrale sono il mezzo di pagamento tra le banche. In questo sistema su due livelli la fiducia è generata tramite banche centrali indipendenti e rendicontabili, che sostengono le riserve

attraverso le loro disponibilità di attività e le norme operative. A sua volta, la fiducia nei depositi bancari è generata tramite diversi mezzi, fra cui la regolamentazione, la vigilanza e i sistemi di assicurazione dei depositi, che in molti casi sono sostenuti in ultima istanza dallo Stato.

Per adempiere al loro mandato di mantenere un'unità di conto e un mezzo di pagamento stabili, le banche centrali assumono un ruolo attivo nella vigilanza, nella supervisione e in alcuni casi nella fornitura dell'infrastruttura dei pagamenti per le loro valute. Tra i ruoli delle banche centrali, vi è quello di assicurare che il sistema dei pagamenti funzioni senza intoppi e verificare che l'offerta di riserve risponda in modo appropriato alle variazioni della domanda, incluse quelle infragiornaliere, in altre parole garantire un'offerta di moneta elastica[12].

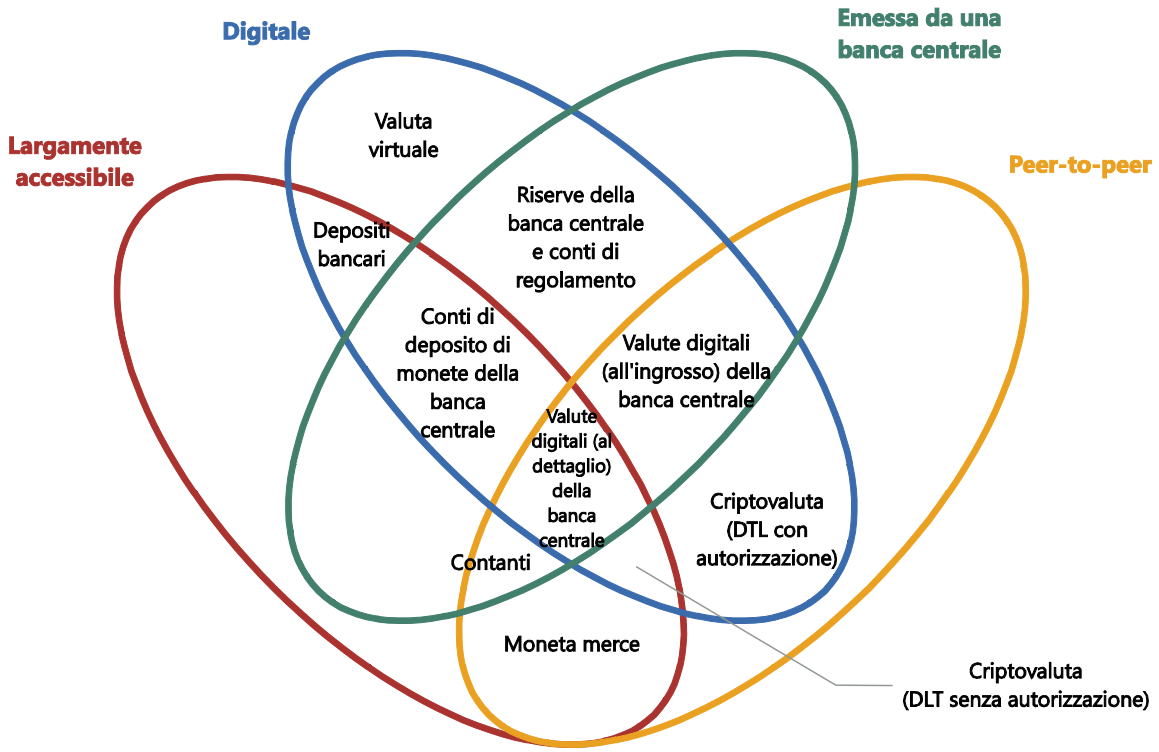
Grazie al coinvolgimento attivo delle banche centrali, i diversi sistemi di pagamento oggi utilizzati sono sicuri, presentano un buon rapporto costi-efficacia, permettono scalabilità e godono della fiducia rispetto al fatto che un pagamento, una volta effettuato, è definitivo.

I sistemi di pagamento sono sicuri e presentano un buon rapporto costi-efficacia, gestendo volumi elevati e adeguandosi a una crescita rapida senza quasi nessun uso indebito e a costi moderati. Un elemento importante che ha contribuito alla sicurezza e al buon rapporto costi-efficacia è la scalabilità. Nelle economie sofisticate di oggi, il volume dei pagamenti è enorme, pari a svariati multipli del PIL. Malgrado questi ingenti volumi, l'espansione dell'uso dello strumento non porta a un aumento proporzionale dei costi. Ciò è importante, perché un elemento fondamentale di qualsiasi moneta e sistema di pagamento efficace è quanto largamente viene utilizzato da acquirenti e venditori: quante più persone sono collegate a un determinato sistema di pagamento, tanto maggiore è l'incentivo a usarlo.

Gli utenti non devono avere fiducia solo nella moneta in sé, ma anche nel fatto che un pagamento verrà effettuato prontamente e senza intoppi. Un attributo operativo auspicabile è quindi la certezza del pagamento ("definitività") e, collegata a essa, la possibilità di contestare transazioni che potrebbero essere state eseguite in modo non corretto. La definitività richiede che il sistema sia in linea di massima esente da frodi e rischi operativi, sia al livello delle singole transazioni individuali sia al livello del sistema nel suo complesso. Una vigilanza forte e la rendicontabilità delle banche centrali contribuiscono a sostenere la definitività e, di conseguenza, la fiducia.

Se oggi la maggior parte delle transazioni avviene tramite mezzi che sono supportati in ultima analisi dalle banche centrali, nel corso del tempo è emersa un'ampia gamma di mezzi di pagamento pubblici e privati. Possono essere efficacemente riassunti con una tassonomia definita "il fiore delle monete"(grafico V.1).[13]

Il fiore delle monete: una tassonomia della moneta Grafico V.1



Fonte: adattato da M. Bech e R. Garratt, "Criptovalute delle banche centrali", *Rassegna trimestrale BRI*, settembre 2017.

Il fiore delle monete distingue quattro proprietà chiave delle monete: l'emittente, la forma, il grado di accessibilità e il meccanismo di trasferimento del pagamento. L'emittente può essere una banca centrale, una banca, o nessuno, come quando la moneta prendeva la forma di una merce. La sua forma può essere fisica, come ad esempio le monete metalliche o una banconota di carta, o digitale. Può avere un largo accesso, come i depositi delle banche commerciali, o un accesso più ristretto, come le riserve delle banche centrali. Un'ultima caratteristica riguarda il meccanismo di trasferimento, che può essere peer-to-peer (tra privati) o tramite un intermediario centrale, come per i depositi. La moneta si basa generalmente su una di due tecnologie basilari: i cosiddetti "token" o i conti. La moneta sotto forma di token, ad esempio le banconote o le monete fisiche, può essere scambiata in contesti peer-to-peer ma questo tipo di scambio dipende principalmente dalla capacità del beneficiario di verificare la validità dell'oggetto di pagamento (con i contanti, il rischio è la contraffazione). Al contrario, i sistemi basati su un conto dipendono essenzialmente dalla capacità di verificare l'identità del titolare del conto.

Criptovalute: la promessa sfuggente di una fiducia decentralizzata

Le criptovalute manterranno le loro promesse? O finiranno per essere delle curiosità effimere? Per rispondere a queste domande è necessario definirle in modo più preciso, al fine di capire la tecnologia che le supporta e analizzare i limiti economici che vi sono associati.

Un nuovo petalo nel fiore delle monete?

Le criptovalute aspirano a diventare una nuova forma di valuta e promettono di mantenere la fiducia nella stabilità del loro valore tramite l'uso della tecnologia. Sono costituite da tre elementi.: primo, un insieme di regole (il "protocollo"), cioè un codice informatico che specifica il modo in cui i partecipanti possono effettuare le transazioni; secondo, un ledger (libro mastro) che conserva la storia della transazioni; terzo, una rete decentralizzata di partecipanti che aggiornano, conservano e leggono il ledger delle transazioni seguendo le regole del protocollo. Con questi elementi, sostengono i fautori di questa tecnologia, la criptovaluta non è soggetta agli incentivi potenzialmente controproducenti delle banche e delle entità sovrane.

Nella prospettiva della tassonomia del fiore delle monete, le criptovalute combinano tre caratteristiche chiave: in primo luogo, sono digitali, aspirano a essere un mezzo pratico di pagamento e fanno affidamento sulla crittografia per evitare contraffazioni e transazioni fraudolente; in secondo luogo, sebbene siano create da un soggetto privato, non c'è nessuna attribuzione di passività, ovvero non possono essere riscattate, e il loro valore deriva solo dall'aspettativa che continueranno a essere accettate da altri utenti: ciò le rende simili a una moneta merce (sebbene siano prive di qualsiasi valore intrinseco); infine, permettono scambi digitali peer-to-peer.

Ciò che contraddistingue le criptovalute rispetto ad altre monete digitali private, come i depositi bancari, è lo scambio digitale peer-to-peer. I conti bancari digitali esistono da decenni. E "valute virtuali" emesse da soggetti privati – ad esempio quelle usate in giochi online multiplayer di grande successo come World of Warcraft – hanno anticipato le criptovalute di un decennio. Al contrario di queste monete, i trasferimenti delle criptovalute possono, in linea di principio, avvenire in un contesto decentralizzato, senza bisogno di una controparte centrale che effettui lo scambio.

La tecnologia a ledger distribuito nelle criptovalute

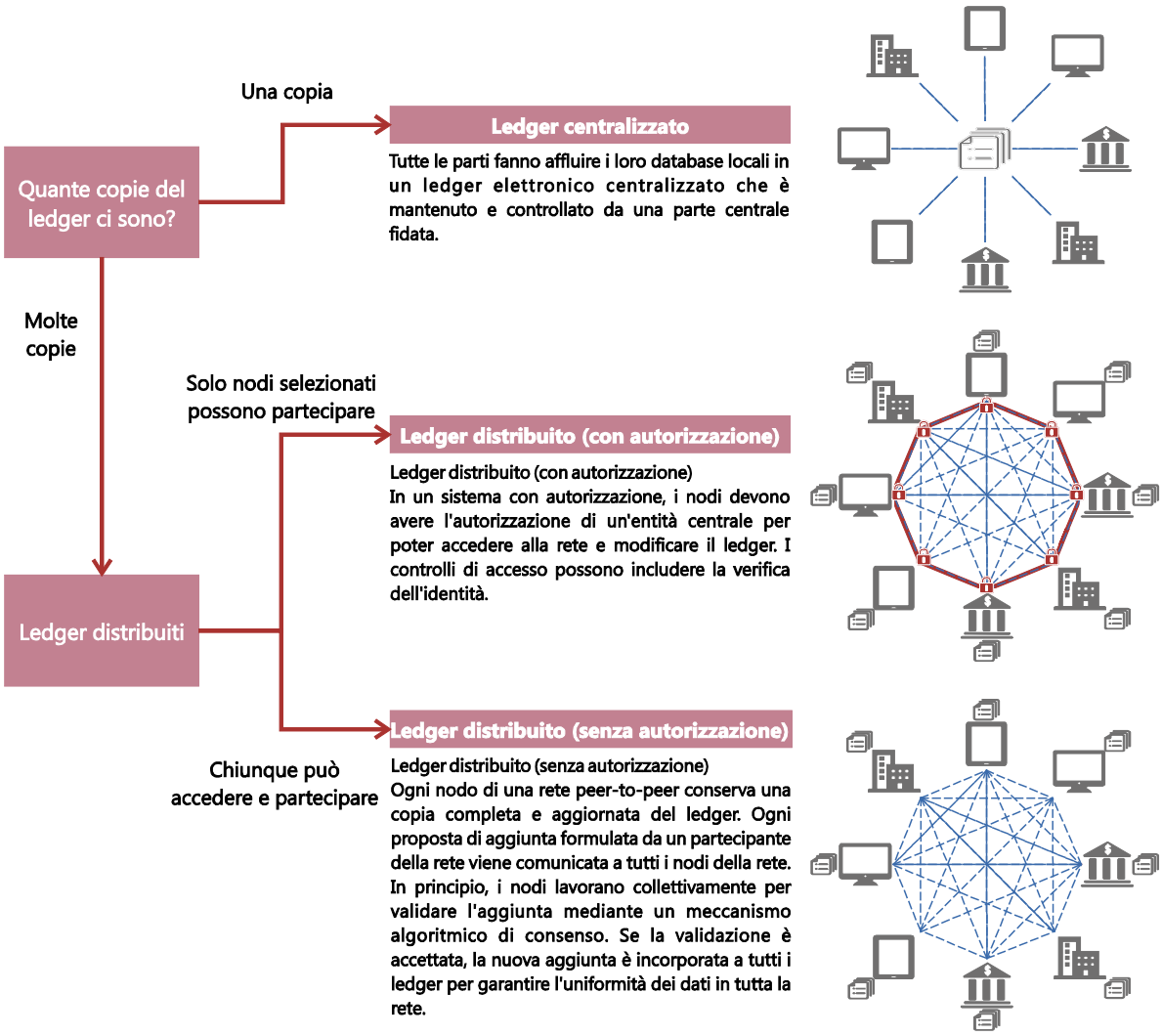
La sfida tecnologica dello scambio digitale peer-to-peer è come risolvere il cosiddetto "problema della doppia spesa". Ogni forma digitale di moneta è facilmente replicabile e può quindi essere spesa in modo fraudolento più di una volta. Le informazioni digitali possono essere riprodotte più facilmente delle banconote fisiche. Per risolvere il problema della doppia spesa delle monete digitali è necessario, come minimo, che qualcuno mantenga un registro di tutte le transazioni. Prima delle criptovalute, l'unica soluzione era che ci fosse un agente centralizzato incaricato del registro e della verifica di tutte le transazioni.

Le criptovalute risolvono il problema della doppia spesa tramite un registro decentralizzato, il cosiddetto "distributed ledger" (libro mastro distribuito). Questo ledger può essere considerato come un file (si pensi a un foglio di calcolo Microsoft Excel) che comincia con una distribuzione iniziale della criptovaluta e registra la storia di tutte le transazioni successive. Una copia aggiornata integrale del ledger è conservata da ogni utente (ed è questo che lo rende "distribuito"). Con un ledger distribuito, lo scambio peer-to-peer di moneta digitale è fattibile: ogni utente può verificare direttamente nella sua copia del ledger se un trasferimento è stato effettuato e che non vi siano stati tentativi di doppia spesa[14].

Tutte le criptovalute fanno affidamento su un ledger distribuito, ma vi sono delle differenze nel modo in cui il ledger viene aggiornato. Si possono distinguere due grandi categorie, che divergono in modo sostanziale dal punto di vista della configurazione operativa (grafico V.2).

Ledger centralizzato e ledger decentralizzati con/senza autorizzazione

Grafico V.2



		Moneta elettronica privata basata su un sistema fiduciario	Criptovalute emesse privatamente	
			Con autorizzazione	Senza autorizzazione
1	Conservazione dei saldi/posizioni	Ledger (conti) conservati centralmente da banche e altre istituzioni finanziare	Conservazione decentralizzata del ledger	
2	Verifica per evitare la doppia spesa	Criterio basato sull'identità	Criterio peer-to-peer: il ledger distribuito può essere verificato per vedere se un'unità specifica di una valuta è già stata spesa	
3	Trattamento delle transazioni	Conti aggiornati dalla banca	Aggiornamento del ledger tramite nodi fidati	Aggiornamento del ledger tramite proof-of-work Regola di seguire la catena più lunga
4	Criterio definitività/regolamento	Regolamento finale tramite banca centrale	Regolamento nella criptovaluta stessa	Criterio probabilistico della definitività tramite la regola di seguire la catena più lunga
5	Elasticità dell'offerta	Politica della banca centrale, ad esempio riguardo il credito infragiornaliero	Il protocollo può essere modificato dai nodi fidati	Determinato dal protocollo
6	Meccanismi per creare la fiducia	Reputazione di banche e banche centrali, vigilanza bancaria, prestatore di ultima istanza, leggi sul corso legale, indipendenza e rendicontabilità della banca centrale, verifiche antiriciclaggio e contro il finanziamento del terrorismo, cybersicurezza	Reputazione delle società emittenti e dei nodi Nodi fidati, alcuni dei quali possono essere soggetti a regolamentazione	La proof of work richiede una maggioranza computazionale onesta

Fonti: adattato da H. Natarajan, S. Krause e H. Gradstein, "Distributed ledger technology (DLT) and blockchain", Gruppo della Banca mondiale, *FinTech Note*, n. 1, 2017; BRI.

Una di queste due categorie si basa su una DLT con autorizzazione (permissioned). Queste criptovalute si avvicinano ai meccanismi di pagamento convenzionali per il fatto che, al fine di evitare usi indebiti, il ledger può essere aggiornato solo da operatori fidati della criptovaluta, spesso definiti "nodi fidati" (trusted nodes). Questi nodi sono selezionati da un'autorità centrale (ad esempio la società che ha sviluppato la criptovaluta) e soggetti alla sua supervisione. Di conseguenza, sebbene le criptovalute che si basano su sistemi con autorizzazione si distinguano dalla moneta convenzionale per il modo in cui il registro delle transazioni viene conservato (decentralizzato invece che centralizzato), hanno in comune con essa il fatto di fare affidamento su istituzioni specifiche come fonte di fiducia di ultima istanza[15].

Allontanandosi in modo più radicale dalla configurazione prevalente, basata su un'istituzione, una seconda categoria di criptovalute promette di generare fiducia in un contesto integralmente decentralizzato, utilizzando una DLT senza autorizzazione (permissionless). Il ledger che registra le transazioni può essere modificato solo tramite un consenso degli operatori della valuta: tutti possono partecipare, ma nessuno possiede una chiave speciale per modificarlo.

Il concetto delle criptovalute senza autorizzazione è stato illustrato, nel caso del Bitcoin,[16] in un libro bianco scritto da un programmatore anonimo (o da un gruppo di programmatori) sotto lo pseudonimo "Satoshi Nakamoto", che proponeva una valuta basata su un tipo specifico di ledger distribuito, la "blockchain". La blockchain è un tipo di ledger distribuito che viene aggiornato in gruppi di transazioni chiamati "blocchi". Questi blocchi sono poi concatenati sequenzialmente tramite l'uso della crittografia per formare la blockchain (catena di blocchi). Questo concetto è stato applicato a moltissime altre criptovalute[17].

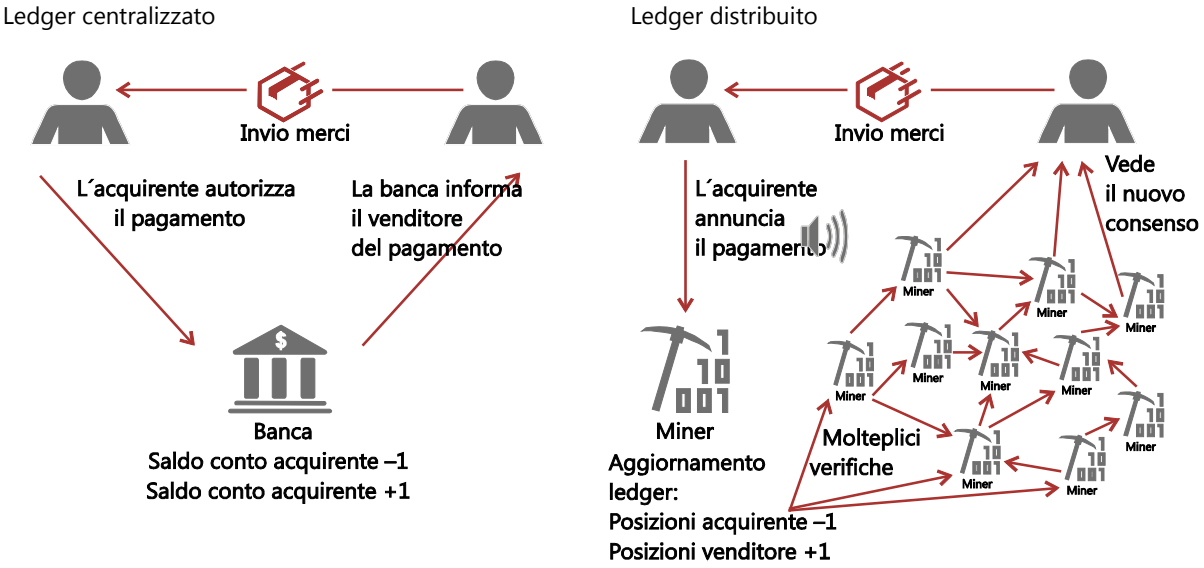
Le criptovalute senza autorizzazione basate su una blockchain hanno due gruppi di partecipanti: i "miner" (minatori, estrattori), che agiscono da contabili, e gli "utenti" che vogliono effettuare una transazione in criptovaluta. Di per sé, l'idea alla base di queste criptovalute è semplice: invece di una banca che registra le transazioni in modo centralizzato (grafico V.3, diagramma di sinistra), il ledger è aggiornato da un miner e l'aggiornamento è successivamente conservato da tutti gli utenti e i miner (diagramma di destra)[18].

Alla base di questa configurazione, la caratteristica principale di queste criptovalute risiede nell'applicazione di una serie di norme (il "protocollo") che intendono allineare gli incentivi di tutti i partecipanti allo scopo di creare una tecnologia di pagamento affidabile che non necessiti di un agente centrale fidato. Il protocollo determina l'offerta dell'attività in modo da contrastare la svalutazione: per esempio, nel caso del Bitcoin, stabilisce che possono esistere solo 21 milioni di bitcoin. Inoltre, il protocollo è progettato in modo da garantire che tutti i partecipanti rispettino le regole per interesse personale, cioè che producano un equilibrio in grado di reggere da solo. Si osservano tre aspetti chiave.

In primo luogo, le norme prevedono un costo per l'aggiornamento del ledger. Nella maggioranza dei casi, questo costo è dato dal fatto che l'aggiornamento richiede un "proof-of-work", ovvero una prova matematica che è stata eseguita una certa quantità di lavoro computazionale , che a sua volta richiede costose attrezzature e impiego di energia elettrica. Dato che il processo di proof-of-work può essere paragonato al processo di "dissotterrare" numeri rari tramite calcoli laboriosi , viene spesso definito come mining (scavo, estrazione)[19]. In cambio del loro lavoro, i miner ricevono delle commissioni dagli utenti e, se è specificato dal protocollo, criptovalute di nuovo conio.

Transazioni valide in un conto bancario/ledger centralizzato e in una criptovaluta senza autorizzazione

Grafico V.3



Un acquirente compra un bene da un venditore, che avvia la spedizione dopo aver ricevuto la conferma del pagamento. Se il pagamento viene effettuato tramite conti bancari – ovvero tramite un ledger centralizzato (diagramma di sinistra) – l'acquirente manda le istruzioni di pagamento alla sua banca, che corregge il saldo del conto addebitando l'importo pagato dal conto dell'acquirente e accreditandolo sul conto del venditore. In seguito la banca conferma l'avvenuto pagamento al venditore. Se invece il pagamento viene effettuato tramite una criptovaluta senza autorizzazione (diagramma di destra), per prima cosa l'acquirente annuncia pubblicamente un'istruzione di pagamento che stabilisce che la sua posizione in criptovaluta viene ridotta di un'unità, mentre quella del venditore viene incrementata di una. Dopo un determinato lasso di tempo, un miner include questa informazione di pagamento in un aggiornamento del ledger. Successivamente, il ledger aggiornato viene condiviso con altri miner e utenti, ognuno dei quali verifica che l'istruzione di pagamento recentemente aggiunta non sia un tentativo di doppia spesa e che sia stata autorizzata dall'acquirente. Il venditore osserva poi che il ledger che contiene l'istruzione di pagamento è quello comunemente usato dalla rete di miner e utenti.

Fonte: adattato da R. Auer, "The mechanics of decentralised trust in Bitcoin and the blockchain" *BIS Working Papers*, di prossima pubblicazione.

In secondo luogo, tutti i miner e gli utenti di una criptovaluta verificano tutti gli aggiornamenti del ledger, il che spinge i miner a includere solo transazioni valide. Le transazioni valide devono essere avviate dai detentori dei fondi e non devono essere tentativi di doppia spesa. Se un aggiornamento del ledger include una transazione non valida, viene rifiutato dalla rete e i premi (reward) del miner sono annullati. La verifica di tutti gli aggiornamenti del ledger da parte della rete di miner e utenti è quindi essenziale per incentivare i miner ad aggiungere solo transazioni valide[20].

In terzo luogo, il protocollo specifica le regole necessarie per raggiungere il consenso riguardo all'ordine degli aggiornamenti del ledger. Di solito, questo viene fatto creando incentivi per i singoli miner a seguire la maggioranza computazionale di tutti gli altri miner quando applicano gli aggiornamenti. Questo coordinamento è necessario, per esempio, per risolvere i casi in cui i ritardi di comunicazione fanno sì che miner diversi aggiungano aggiornamenti in conflitto tra loro, ovvero aggiornamenti che includono serie diverse di transazioni (cfr. riquadro V.A).

Con questi ingredienti chiave, per un individuo risulta costoso – seppur non impossibile – falsificare una criptovaluta. Per riuscire a effettuare una doppia spesa, un contraffattore dovrebbe spendere la sua criptovaluta con un commerciante e produrre in segreto una blockchain falsa in cui tale transazione non sia registrata. Dopo aver ricevuto la merce, il contraffattore pubblicherebbe la blockchain falsa, cioè invertirebbe il pagamento. Ma questa blockchain falsa emergerebbe come la catena

comunemente accettata solo se fosse più lunga di quella che il resto della rete di miner ha prodotto nello stesso lasso di tempo. Affinché un attacco di doppia spesa vada a buon fine necessita quindi di una quota sostanziale della potenza computazionale della comunità di miner. Detto in altro modo, per usare le parole del libro bianco originale del Bitcoin, una criptovaluta può superare il problema della doppia spesa in modo decentralizzato solo "se nodi onesti controllano la maggior parte della potenza [computazionale]"[21].

Valutazione dei limiti economici delle criptovalute senza autorizzazione

Le criptovalute come il Bitcoin promettono di fornire non solo un comodo mezzo di pagamento basato sulla tecnologia digitale, ma anche un nuovo modello di fiducia. Tuttavia, la realizzazione di questa promessa dipende da una serie di presupposti: il fatto che la larga maggioranza della potenza computazionale sia controllata da miner onesti, il fatto che gli utenti verifichino la storia di tutte le transazioni e il fatto che l'offerta di valuta sia predeterminata da un protocollo. Capire questi presupposti è importante, perché sollevano due domande basilari sull'utilità delle criptovalute. La prima è: questo metodo complicato per cercare di realizzare la fiducia non va a scapito dell'efficienza? La seconda è: è sempre e realmente possibile realizzare la fiducia?

Come lascia intendere la prima domanda, un limite potenziale in termini di efficienza è l'enorme costo che comporta generare una fiducia decentralizzata. Ci si potrebbe aspettare che i miner competano fra loro per aggiungere nuovi blocchi al ledger tramite il processo di proof-of-work fino a quando i loro profitti stimati scenderanno a zero[22]. Le attrezzature individuali gestite dai miner possono ospitare una potenza computazionale pari a quella di milioni di personal computer. Al momento della stesura del capitolo, l'energia elettrica totale utilizzata per l'estrazione (mining) di bitcoin era equivalente a quella di economie di medie dimensioni come la Svizzera, e anche altre criptovalute usano ingenti quantità di energia elettrica (grafico V.4, diagramma di sinistra). Per dirla nel modo più semplice possibile, la ricerca di una fiducia decentralizzata è diventata rapidamente un disastro ambientale[23].

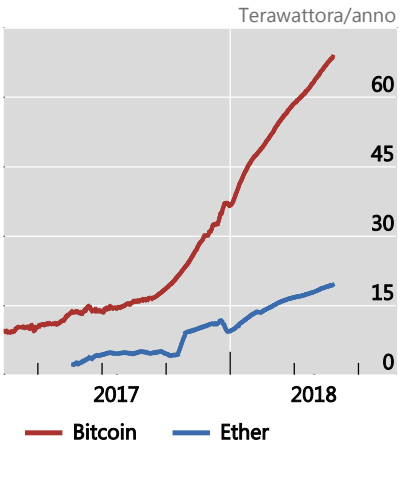
Ma i problemi economici di fondo vanno ben al di là della questione energetica. Hanno a che fare con il compito chiave della moneta: promuovere "esternalità di rete" tra gli utenti e servire quindi da dispositivo di coordinamento per l'attività economica. A questo riguardo, le lacune delle criptovalute risiedono in tre aree: scalabilità, stabilità del valore e fiducia nella definitività dei pagamenti.

Innanzitutto, le criptovalute semplicemente non permettono una scalabilità come le monete sovrane. Al livello più elementare, affinché le criptovalute mantengano la promessa di una fiducia decentralizzata, è necessario che ogni singolo utente scarichi e verifichi la storia di tutte le transazioni mai effettuate, comprese le informazioni relative all'importo pagato, all'acquirente, al beneficiario e altri dettagli. Dato che ogni transazione aggiunge qualche centinaia di byte, il ledger cresce notevolmente nel corso del tempo. Per esempio, al momento della stesura del capitolo la blockchain del Bitcoin stava crescendo di circa 50 GB all'anno e aveva raggiunto più o meno i 170 GB. Di conseguenza, per far sì che le dimensioni del ledger e il tempo necessario per verificare tutte le transazioni (che aumenta di pari passo con le dimensioni del blocco) restino gestibili, le criptovalute presentano limiti considerevoli in termini di volume delle transazioni (grafico V.4, diagramma centrale).

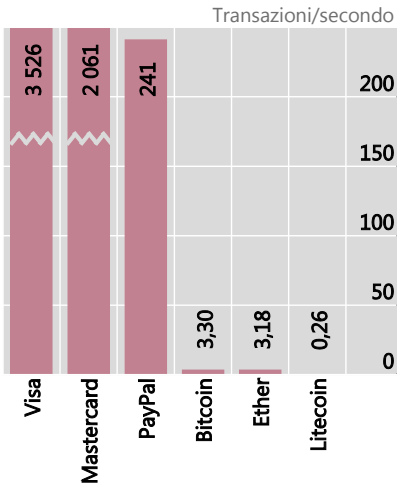
Consumo energetico e questioni di scalabilità

Grafico V.4

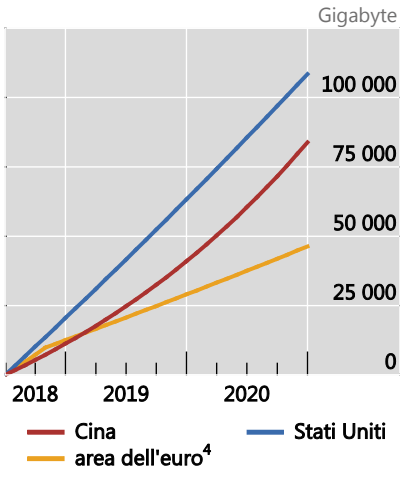
Impiego energetico di criptovalute selezionate[1]



Numero di transazioni al secondo[2]



Dimensioni ipotetiche del ledger per criptovaluta al dettaglio a livello nazionale[3]



[1] Stimato. [2] Dati per il 2017. [3] La dimensione ipotetica della blockchain/ledger qui presentata è calcolata ipotizzando che, a partire dal 1° luglio 2018, tutte le transazioni al dettaglio non in contanti della Cina, degli Stati Uniti o dell'area dell'euro siano elaborate tramite una criptovaluta. I calcoli si basano sulle informazioni relative al numero di transazioni non in contanti tratte da CPIM (2017) e suppongono che ogni transazione aggiunga 250 byte al ledger. [4] BE, DE, FR, IT e NL.

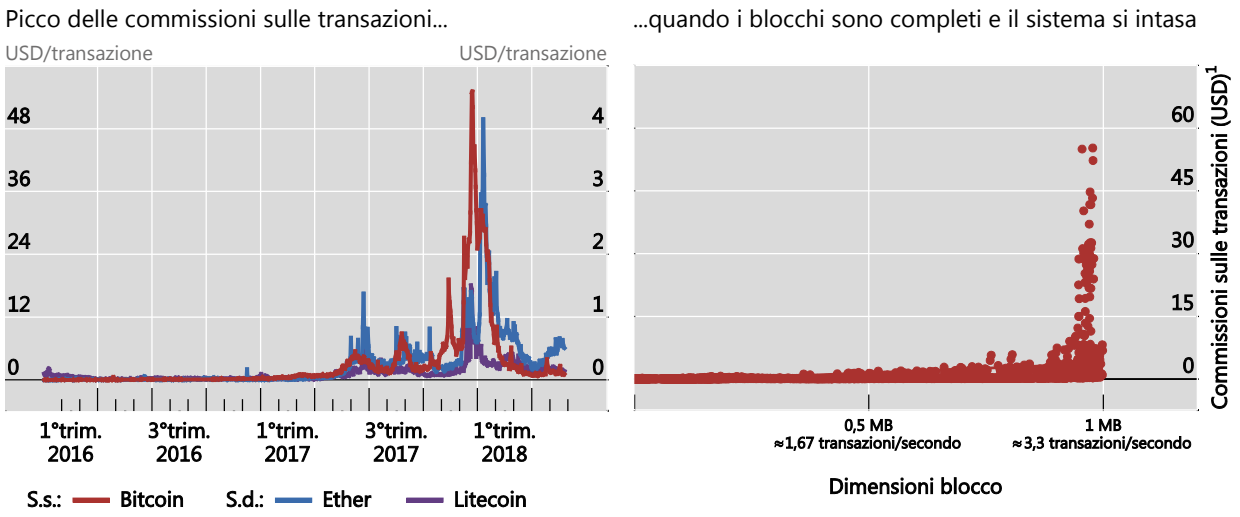
Fonti: Comitato per i pagamenti e le infrastrutture di mercato (CPIM), *Statistics on payment, clearing and settlement systems in the CPMI countries*, dicembre 2017; www.bitinfocharts.com; Digiconomist; Mastercard; PayPal; Visa;; elaborazioni BRI.

Un esperimento mentale illustra l'inadeguatezza delle criptovalute come mezzo di pagamento quotidiano (grafico V.4, diagramma di destra). Per elaborare il numero di transazioni digitali al dettaglio attualmente gestite dai sistemi nazionali di pagamento al dettaglio di paesi selezionati, anche facendo delle supposizioni ottimistiche la dimensione del ledger crescerebbe al punto di superare largamente la capacità di memoria di un comune smartphone nel giro di pochi giorni, quella di un comune personal computer nel giro di poche settimane e quella dei server nel giro di pochi mesi. Ma il problema va ben al di là della capacità di memoria perché riguarda anche la capacità di elaborazione computazionale: solo dei supercomputer sarebbero in grado di tenere il passo con le verifiche delle transazioni in entrata. I relativi volumi di comunicazione, con milioni di utenti che si scambiano file dell'ordine di grandezza di un terabyte, potrebbero provocare un black out di internet.

Un altro aspetto della questione della scalabilità riguarda il fatto che l'aggiornamento del ledger è soggetto a congestione. Per esempio, nelle criptovalute basate su una blockchain, al fine di limitare il numero di transazioni che possono essere aggiunte al ledger in un dato momento, è possibile aggiungere nuovi blocchi solo a intervalli prestabiliti. Quando il numero delle transazioni in entrata è tale che i blocchi aggiunti più di recente raggiungono già il limite massimo consentito dal protocollo, il sistema si intasa e molte transazioni si ritrovano ad aspettare in fila. Dato che la capacità ha una soglia massima, le commissioni si impennano ogni qual volta la domanda di transazioni raggiunge tale soglia (grafico V.5). In certi casi è capitato che le transazioni abbiano dovuto aspettare in fila per parecchie ore, interrompendo il processo di pagamento. Ciò limita l'utilità delle criptovalute nelle transazioni della vita quotidiana, come il pagamento di un caffè o di iscrizione a una conferenza, per non parlare dei pagamenti all'ingrosso[24]. Pertanto, più persone usano una criptovaluta, più difficili diventano i pagamenti. Questo nega una proprietà essenziale

Le commissioni sulle transazioni nel corso del tempo e in relazione al volume di transizioni

Grafico V.5



[1] Commissione sulle transazioni pagata ai miner nel periodo 1° agosto 2010–25 maggio 2018, medie giornaliere.

Fonti: www.bitinfocharts.com; elaborazioni BRI.

della moneta odierna, ovvero il fatto che più persone la usano più cresce l'incentivo a usarla[25].

La seconda questione chiave sulle criptovalute riguarda l'instabilità del loro valore, che nasce dall'assenza di un emittente centrale incaricato di garantire la stabilità della valuta. Le banche centrali ben gestite riescono a stabilizzare il valore interno della loro valuta sovrana adattando l'offerta dei mezzi di pagamento alla domanda di transazioni. Lo fanno con frequenza elevata, in particolare durante i periodi di tensione del mercato, ma anche durante i periodi normali.

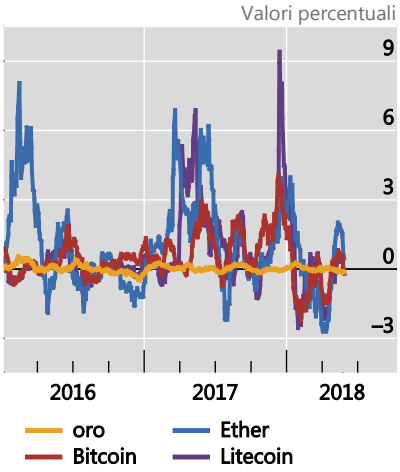
Al contrario, perché vi sia fiducia nel valore di una criptovaluta è necessario che l'offerta sia predeterminata da un protocollo, e questo impedisce che sia elastica. Ogni oscillazione della domanda si traduce quindi in una variazione della valutazione. Di conseguenza, le valutazioni delle criptovalute sono estremamente volatili (grafico V.6, diagramma di sinistra). Verosimilmente, inoltre, non sarà possibile rimediare per intero a questa instabilità intrinseca tramite migliori protocolli o strumenti di ingegneria finanziaria, come illustrato dal caso della criptovaluta Dai: sebbene fosse stata agganciata al dollaro statunitense a un tasso di uno a uno, ha toccato un minimo di $0,72 appena qualche settimana dopo il suo lancio, a fine 2017. Altre criptovalute, ideate per avere un valore stabile, hanno anch'esse subito fluttuazioni notevoli (diagramma centrale).

Questo esito non è un caso Mantenere l'offerta del mezzo di pagamento in linea con la domanda di transazioni richiede la presenza di un'autorità centrale, generalmente la banca centrale, che abbia la facoltà di espandere o contrarre il proprio bilancio. In certi casi, l'autorità deve anche essere pronta a operare in controtendenza rispetto al mercato, anche quando ciò significa assumere dei rischi sul suo bilancio e assorbire una perdita. In una rete decentralizzata di utenti di criptovalute non c'è nessun agente centrale con l'obbligo o l'incentivo di stabilizzare il valore della valuta: ogni qual volta cala la domanda di una criptovaluta, scende anche il suo prezzo.

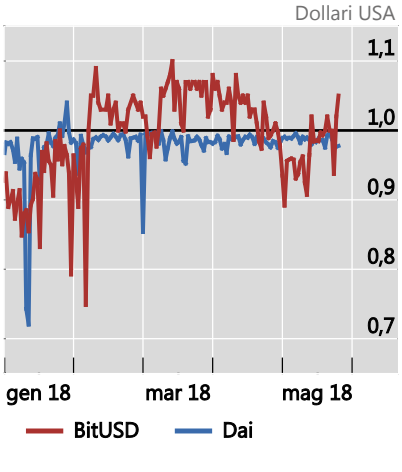
Volatilità di criptovalute selezionate e numero di criptovalute

Grafico V.6

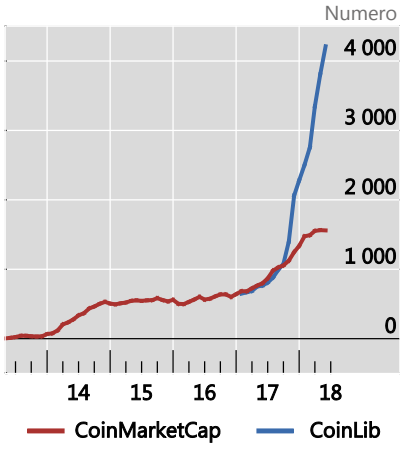
Le principali criptovalute sono relativamente volatili[1]



Oscillazioni di valore delle "stable coin"[2]



Il numero di criptovalute cresce rapidamente[3]



[1] Medie mobili a 30 giorni dei rendimenti giornalieri. [2] Prezzo minimo giornaliero. [3] Con base nelle istantanee mensili di due diversi fornitori. CoinMarketCap include solo le criptovalute con un volume minimo di contrattazioni su 24 ore di $100 000; CoinLib non ha una soglia.

Fonti: www.bitinfocharts.com; www.coinlib.io; www.coinmarketcap.com; Datastream.

Un altro fattore che contribuisce all'instabilità delle valutazioni è la velocità con cui vengono create nuove criptovalute, tutte tendenzialmente sostituibili l'una all'altra. Al momento della stesura del capitolo, ne esistevano diverse migliaia, anche se la proliferazione rende impossibile elaborare stime affidabili del numero di criptovalute esistenti (grafico V.6, diagramma di destra). Come dimostrano le esperienze di banche di emissione private del passato, l'esito di un'emissione copiosa di nuove valute raramente è la stabilità.

La terza questione riguarda la fragilità della fiducia nelle criptovalute, dovuta all'incertezza riguardo alla definitività dei pagamenti individuali e alla debolezza della fiducia nel valore delle singole criptovalute.

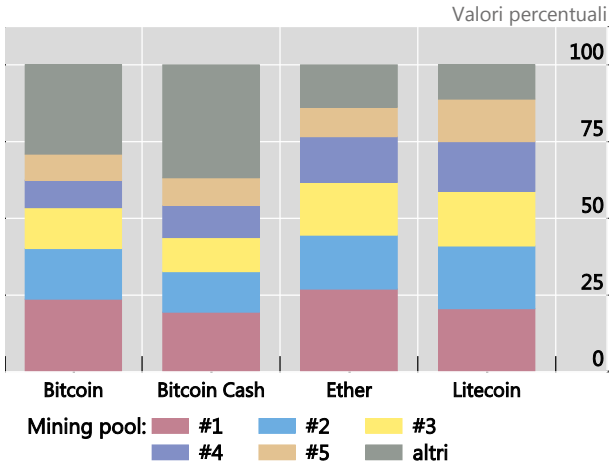
Nei sistemi di pagamento convenzionali, una volta che un singolo pagamento si immette nel sistema nazionale di pagamenti e in ultima istanza nei registri contabili della banca centrale, non può essere revocato. Al contrario, le criptovalute senza autorizzazione non sono in grado di garantire la definitività dei pagamenti individuali. Prima di tutto perché, sebbene gli utenti possano verificare che una specifica transazione è inclusa nel ledger, possono esistere versioni rivali del ledger di cui essi ignorano l'esistenza. Il risultato può essere che la transazione non va a buon fine ad esempio quando due miner aggiornano il ledger quasi simultaneamente: dato che solo uno dei due aggiornamenti può sopravvivere, la definitività dei pagamenti effettuati in ogni versione del ledger è probabilistica.

La mancanza di definitività dei pagamenti è aggravata dal fatto che le criptovalute possono essere manipolate da miner che controllano una potenza computazionale importante; si tratta di una possibilità reale, considerata la concentrazione che caratterizza l'attività di mining in molte criptovalute (grafico V.7, diagramma di sinistra). Non è possibile capire se sia in corso un attacco strategico perché l'autore dell'attacco rivelerebbe il ledger (falso) solo dopo essere sicuro del risultato. Ciò implica che la definitività rimarrà sempre incerta. Per le criptovalute, ogni

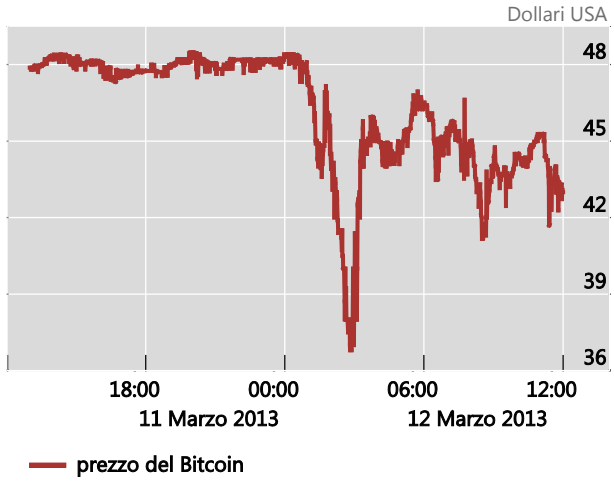
La concentrazione dell'attività di mining e il valore del bitcoin durante una biforcazione temporanea

Grafico V.7

L'attività di mining è fortemente concentrata in tutte le criptovalute



Valore del bitcoin durante una biforcazione temporanea nel 2013[2]



[1] Dati per i gruppi di mining più grandi al 28 maggio 2018. [2] Dinamiche di prezzo del Bitcoin durante la biforcazione dell'11-12 marzo 2013.

Fonti: www.btc.com; www.cash.coin.dance; CoinDesk; www.etherchain.org; www.litecoinpool.org.

aggiornamento del ledger è accompagnato da un proof-of-work aggiuntivo che l'autore di un attacco dovrebbe riprodurre. Di conseguenza, se la probabilità che un pagamento sia definitivo aumenta con la crescita del numero di successivi aggiornamenti del ledger, essa non raggiunge mai il 100%[26].

Non solo è incerta la fiducia nei singoli pagamenti, ma è fragile anche il puntello della fiducia in ogni criptovaluta. Ciò è dovuto alla biforcazione (forking), un processo in cui un sottogruppo di detentori di una criptovaluta si mette d'accordo per usare una nuova versione del ledger e del protocollo, mentre altri continuano ad attenersi a quella originaria; in questo modo, una criptovaluta può dividersi in due sottoreti di utenti. Gli esempi negli anni recenti non mancano, ma è particolarmente rilevante un episodio dell'11 marzo 2013, perché – in contraddizione con l'idea di realizzare la fiducia tramite mezzi decentralizzati – è stato risolto grazie a un coordinamento centralizzato dei miner. Quel giorno, un aggiornamento sbagliato del software ha portato a delle incompatibilità tra una parte della rete del Bitcoin che stava effettuando il mining con il vecchio protocollo e un'altra parte che utilizzava un protocollo aggiornato. Per diverse ore, due blockchain separate hanno continuato a crescere; quando la notizia di questa biforcazione si è diffusa, il prezzo del bitcoin è crollato di quasi un terzo (grafico V.7, diagramma di destra). La biforcazione è stata poi risolta tramite uno sforzo coordinato in cui i miner hanno temporaneamente abbandonato il protocollo e ignorato la catena più lunga. Ma molte transazioni sono state annullate ore dopo che gli utenti le avevano date per definitive. Questo episodio mostra con quanta facilità le criptovalute possano scindersi, causando perdite significative di valore.

Un aspetto ancora più preoccupante di questi episodi è che la biforcazione può essere sintomatica di una lacuna sostanziale: la fragilità del consenso decentralizzato legato all'aggiornamento del ledger e, assieme ad esso, della fiducia di fondo nella criptovaluta. L'analisi teorica (riquadro V.A) suggerisce che il coordinamento sul

modo in cui il ledger è aggiornato potrebbe venir meno in ogni momento, avendo come risultato una perdita di valore totale.

Nel complesso, le criptovalute decentralizzate presentano molte lacune. Le principali inefficienze derivano dall'estremo livello di decentralizzazione: creare la fiducia necessaria in un contesto del genere spreca quantità enormi di potenza computazionale, la conservazione decentralizzata di un ledger di transazioni è inefficace e il consenso decentralizzato è vulnerabile. Alcuni di questi problemi potrebbero essere risolti mediante nuovi protocolli e altri miglioramenti[27], ma altri sembrano intrinsecamente legati alla fragilità e alla limitata scalabilità di questi sistemi decentralizzati. In definitiva, ciò segnala che la lacuna sostanziale delle criptovalute risiede nella mancanza di un assetto istituzionale adeguato a livello nazionale.

Al di là della bolla: come utilizzare la tecnologia a ledger distribuito

Come moneta le criptovalute non funzionano, ma la tecnologia che ne è alla base potrebbe essere promettente in altri campi. Un esempio degno di nota è quello dei servizi di pagamento transfrontalieri di volumi minori. Più in generale, comparata alle soluzioni tecnologiche centralizzate convenzionali, la DLT può essere efficace in contesti di nicchia, dove i benefici di un accesso decentralizzato superano i costi operativi più elevati del mantenimento di molteplici copie del ledger.

In verità, queste soluzioni di pagamento sono sostanzialmente diverse dalle criptovalute. Un esempio di uso recente di questa tecnologia per un progetto non a scopo di lucro è il sistema Building Blocks, basato su una blockchain, del Programma alimentare mondiale, volto a gestire i pagamenti per gli aiuti alimentari destinati ai profughi siriani in Giordania. Nel Building Blocks l'unità di conto e, in ultima istanza, il mezzo di pagamento è la moneta sovrana, quindi si tratta di un sistema di "criptopagamento", ma non di una criptovaluta. Inoltre, è controllato centralmente dal Programma alimentare mondiale, e per una valida ragione: un iniziale esperimento basato sul protocollo senza autorizzazione Ethereum aveva avuto come risultato transazioni lente e costose. Successivamente il sistema è stato ripensato per funzionare tramite una versione con autorizzazione del protocollo Ethereum. Così facendo, i costi di transazione sono stati ridotti del 98% rispetto a quelli delle alternative bancarie[28].

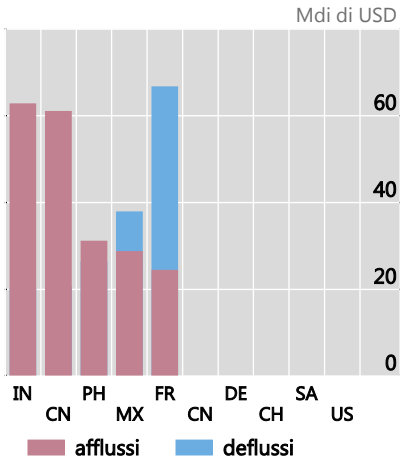
I sistemi di criptopagamento con autorizzazione potrebbero avere un potenziale anche per i trasferimenti transfrontalieri di volumi minori, che sono importanti per quei paesi con una parte importante della propria forza lavoro che vive all'estero. Gli afflussi di rimesse a livello mondiale ammontano complessivamente a oltre $540 miliardi all'anno (grafico V.8, diagrammi di sinistra e centrale). Attualmente, le forme di pagamento internazionale coinvolgono vari intermediari, il che implica costi elevati (diagramma di destra). Ciò detto, se è vero che i sistemi di criptopagamento sono un mezzo per rispondere a questo tipo di esigenze, anche altre tecnologie sono in corso di studio e non è ancora chiaro quale di esse risulterà essere la più efficace.

Casi d'uso più importanti riguardano probabilmente la combinazione di criptopagamenti, sofisticati codici self-executing e sistemi di dati con autorizzazione. Alcuni protocolli di criptovalute decentralizzate come Ethereum permettono già contratti "smart", che effettuano automaticamente i flussi di pagamento per i derivati. Per ora l'efficacia di questi prodotti è limitata a causa della bassa liquidità e delle inefficienze intrinseche delle criptovalute senza autorizzazione. Ma la tecnologia su cui si basano può essere adottata dalle borse ufficiali in protocolli con autorizzazione

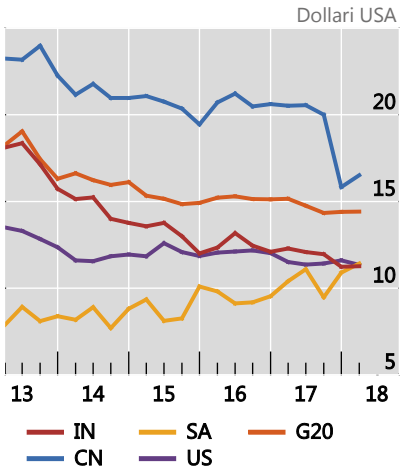
Indicatori del volume e del costo delle rimesse Grafico V.8

I volumi delle rimesse sono in aumento, e questo determina...

...un ingente volume di pagamenti di valore minore tra coppie di valute spesso illiquide[1]...



...a costi medi elevati[2]



[1] Dati per il 2016. [2] Costo medio totale per la spedizione di $200 con tutti i fornitori di servizi di trasferimento di denaro del mondo. Per CN e IN, costo medio totale per il paese ricevente; per G20, SA e US, costo medio totale per il paese speditore.

Fonti: Banca mondiale, *Remittance Prices Worldwide*, remittanceprices.worldbank.org; Banca mondiale; elaborazioni BRI.

che usano la moneta sovrana come supporto, semplificando l'esecuzione del pagamento. Il valore aggiunto della tecnologia deriverà probabilmente dalla sua capacità di semplificare i processi amministrativi relativi a transazioni finanziarie complesse, come il credito al commercio (riquadro V.B). Un elemento cruciale, tuttavia, è che nessuna di queste applicazioni richiede l'uso o la creazione di una criptovaluta.

Implicazioni sul piano delle politiche

L'ascesa delle criptovalute e della tecnologia che ne è alla base solleva una serie di questioni sul piano delle politiche. Le autorità sono alla ricerca di soluzioni che permettano di garantire l'integrità dei mercati e dei sistemi di pagamento, proteggere i consumatori e gli investitori e salvaguardare la stabilità finanziaria nel suo complesso. La lotta all'uso illecito di fondi rappresenta una sfida importante. Allo stesso tempo, le autorità vogliono preservare gli incentivi a lungo termine all'innovazione e difendere in particolare il principio "stesso rischio, stessa regolamentazione"[29]. Questi sono obiettivi ampiamente ricorrenti, ma le criptovalute pongono anche nuove sfide e, potenzialmente, richiedono l'elaborazione di nuovi strumenti e approcci. Uno degli interrogativi relativi alle criptovalute riguarda l'opportunità che le banche centrali emettano le proprie valute digitali (central bank digital currency o CBDC).

Sfide poste dalle criptovalute in materia di regolamentazione

Una prima sfida chiave in materia di regolamentazione è quella relativa alle norme antiriciclaggio e alla lotta contro il finanziamento del terrorismo. Ci si chiede se, e in che misura, l'ascesa delle criptovalute abbia permesso di eludere in parte le norme

sopracitate, come gli standard per l'identificazione della clientela ("know-your-customer"). A causa del loro carattere anonimo, è difficile quantificare in che misura le criptovalute siano usate per sfuggire ai controlli sui movimenti di capitali o alle tasse o, più in generale, per effettuare transazioni illegali. Ma episodi come la forte reazione di mercato del Bitcoin alla chiusura di Silk Road, un importante mercato di droghe illegali, suggerisce che una parte non trascurabile della domanda di criptovalute derivi da attività illecite (grafico V.9, diagramma di sinistra)[30].

Una seconda sfida riguarda le norme di sicurezza e altre regolamentazioni volte a garantire la protezione di consumatori e investitori. Un problema comune è costituito dal furto digitale. Date le dimensioni dei ledger distribuiti, la difficoltà di maneggiarli e gli elevati costi di transazione, molti utenti accedono alle loro posizioni in criptovalute tramite terzi, come i fornitori di "crypto wallet" o i "crypto exchange" (borse di criptovalute). Paradossalmente – e in netto contrasto con la promessa originaria del Bitcoin e di altre criptovalute – molti utenti che avevano optato per le criptovalute perché non si fidavano di banche e governi si sono ritrovati a fare affidamento su intermediari non regolamentati. Alcuni di essi (come Mt Gox o Bitfinex) si sono rivelati fraudolenti o sono stati vittima di attacchi di hacker[31].

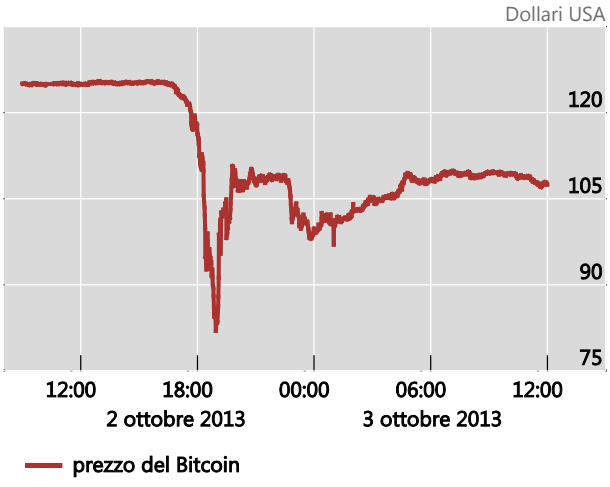
I problemi di frode affliggono anche le ICO (initial coin offerings, offerte iniziali di moneta). Un'ICO comprende una messa all'asta di una serie iniziale di monete di criptovalute per il pubblico, i cui proventi in certi casi garantiscono diritti di partecipazione in un'iniziativa imprenditoriale di nuova costituzione. A dispetto degli avvertimenti delle autorità, gli investitori si sono gettati sulle ICO, nonostante siano spesso legate a progetti di business non trasparenti, per i quali vengono fornite informazioni scarse e non verificate. Molti di questi progetti sono risultati essere truffe piramidali (grafico V.9, diagramma di destra).

Una terza sfida, più à lungo termine, riguarda la stabilità del sistema finanziario. Rimane da vedere se l'uso diffuso delle criptovalute e dei relativi prodotti finanziari self-executing porterà all'emergere di nuove vulnerabilità finanziarie e rischi sistemici.

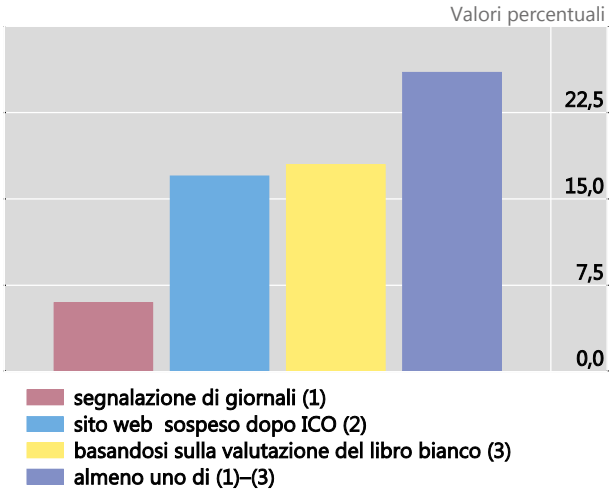
La chiusura di un mercato illegale e la legittimità delle ICO

Grafico V.9

Marcata reazione dei prezzi delle criptovalute alle chiusure di mercati illegali[1]



Si ritiene che una quota considerevole di ICO sia fraudolenta



[1] Il prezzo del Bitcoin durante la chiusura di Silk Road a ottobre 2013.

Fonti: C. Catalini, J. Boslego e K. Zhang, "Technological opportunity, bubbles and innovation: the dynamics of initial coin offerings", *MIT Working Papers*, di prossima pubblicazione; CoinDesk.

Sarà necessario monitorare attentamente i prossimi sviluppi. Inoltre, considerati i nuovi profili di rischio di queste tecnologie, sarà necessario un miglioramento delle competenze degli organismi di regolamentazione e di vigilanza. In alcuni casi, come per l'esecuzione di pagamenti di valore elevato e di volumi ingenti , potrebbe essere necessario allargare il perimetro della regolamentazione e includere entità che usano le nuove tecnologie, al fine di evitare la costituzione di rischi sistemici.

Le autorità di regolamentazione del mondo intero riconoscono in larga misura la necessità di rafforzare le norme esistenti o di crearne di nuove, nonché di monitorare le criptovalute e le criptoattività associate. In particolare, un recente comunicato dei Ministri finanziari e dei Governatori delle banche centrali del G20 sottolinea alcune problematiche relative alla protezione di consumatori e investitori, all'integrità del mercato, all'evasione fiscale e alla lotta contro il riciclaggio di denaro e il finanziamento del terrorismo, e invoca un monitoraggio costante da parte degli organismi internazionali di normazione. Invita inoltre la Financial Action Task Force a proseguire con l'attuazione degli standard applicabili a livello mondiale[32].

Tuttavia, l'elaborazione e l'effettiva attuazione di standard rafforzati non sono una sfida da poco. Le definizioni giuridiche e regolamentari non sono sempre conformi alle nuove realtà. Le tecnologie sono utilizzate per varie attività economiche, che in molti casi sono regolate da organismi di vigilanza diversi. Per esempio, attualmente le ICO sono utilizzate da imprese tecnologiche per raccogliere fondi per progetti che non hanno nessun legame con le criptovalute. Queste offerte iniziali di moneta non sono diverse, se non semanticamente (si tratta di monete in vendita all'asta invece che di azioni), dalle offerte pubbliche iniziali (OPI) nelle borse consolidate, quindi sarebbe naturale che le autorità di regolamentazione mobiliare applicassero le medesime politiche di regolamentazione e vigilanza. Ma alcune ICO ricoprono anche il ruolo di "utility token" che promettono l'accesso a software come videogiochi. Questa caratteristica non costituisce un'attività di investimento e richiede invece l'applicazione delle leggi per la protezione dei consumatori da parte degli organismi competenti[33].

Operativamente, il principale elemento di complicazione è che le criptovalute senza autorizzazione non rientrano facilmente nei quadri regolamentari esistenti. In particolare, manca un'entità o una persona giuridica che possa essere coinvolta nel perimetro regolamentare. Le criptovalute vivono nel loro regno digitale, dove non ci sono nazioni, e possono funzionare in buona parte separatamente dagli assetti istituzionali esistenti o da altre infrastrutture. Il loro domicilio legale – sempre che ne abbiano uno – può trovarsi offshore o non essere chiaramente identificabile. Di conseguenza, possono essere regolamentate solo in modo indiretto.

In che modo le autorità possono attuare uno schema di regolamentazione? È opportuno fare tre considerazioni.

In primo luogo, l'affermarsi delle criptovalute e delle criptoattività obbliga a ridisegnare i confini dei quadri normativi, che devono adattarsi a una nuova realtà in cui le le linee che delimitano le responsabilità delle diverse autorità di regolamentazione all'interno delle giurisdizioni e tra di esse sono sempre più indistinte[34]. Dato che le criptovalute sono per loro natura mondiali, solo una regolamentazione coordinata a livello mondiale può avere qualche possibilità di essere efficace[35].

In secondo luogo, l'interoperabilità delle criptovalute con entità finanziarie soggette a vigilanza potrebbe essere gestita. Solo le borse regolamentate possono fornire la liquidità necessaria affinché i prodotti finanziari basati sulla tecnologia a

ledger distribuito non siano altro che mercati di nicchia, e i flussi di regolamento devono in ultima istanza essere convertiti in moneta sovrana. Le norme fiscali e patrimoniali per le istituzioni regolamentate che vogliono operare in attività legate alle criptovalute potrebbero quindi essere adattate. Le autorità di regolamentazione potrebbero controllare se, e in che modo, le banche rilasciano o ricevono criptovalute come garanzie collaterali.

In terzo luogo, la regolamentazione può concentrarsi su entità che offrono servizi specifici per le criptovalute. Per esempio, per garantire un'azione efficace contro il riciclaggio di denaro e il finanziamento del terrorismo, la regolamentazione potrebbe focalizzarsi sul momento in cui la criptovaluta è scambiata con una moneta sovrana. Altre leggi e regolamentazioni esistenti relative ai servizi di pagamento si concentrano sulla sicurezza, l'efficacia e la legalità del loro utilizzo. Questi principi potrebbero essere applicati anche ai fornitori di infrastrutture per criptovalute, come i "crypto wallet"[36]. Per evitare lacune, la regolamentazione idealmente dovrebbe essere simile, a grandi linee, e attuata in modo coerente nelle varie giurisdizioni.

Le banche centrali dovrebbero emettere valute digitali?

Un'altra questione di medio termine collegata riguarda l'emissione di CBDC, incluso il problema di chi dovrebbe avere accesso a esse. Le CBDC funzionerebbero in modo simile ai contanti: inizialmente la banca centrale emetterebbe una CBDC, ma essa, una volta emessa, circolerebbe tra le banche, le società non finanziarie e i consumatori senza un ulteriore coinvolgimento della banca centrale[37]. Una CBDC di questo genere potrebbe essere scambiata bilateralmente tra operatori del settore privato usando ledger distribuiti senza richiedere alla banca centrale di tenere traccia delle transazioni e di correggere i saldi. Sarebbe basata su un ledger distribuito con autorizzazione (grafico V.2), con la banca centrale che stabilirebbe chi agisce come nodo fidato.

La differenza tra una CBDC per uso generico e le passività digitali esistenti delle banche centrali – saldi dei conti di riserva delle banche commerciali – potrebbe sembrare tecnica, ma in realtà è fondamentale per le sue ripercussioni sul sistema finanziario. Una CBDC per uso generico – emessa per consumatori e imprese – potrebbe incidere in modo sostanziale su tre aree chiave dell'attività delle banche centrali: pagamenti, stabilità finanziaria e politica monetaria. Un recente rapporto elaborato congiuntamente dal Comitato per i pagamenti e le infrastrutture di mercato e dal Comitato sui mercati evidenzia le considerazioni di fondo[38], concludendo che i punti di forza e i punti deboli di una CBDC per uso generico dipenderebbero da caratteristiche di progettazione specifiche. Il rapporto osserva altresì che, oltre al fatto che non sono ancora emersi candidati di rilievo, questo tipo di strumento comporterebbe vulnerabilità finanziarie sostanziali, mentre i benefici sono meno evidenti.

Attualmente, le banche centrali stanno monitorando con attenzione le tecnologie, mantenendo al tempo stesso un approccio cauto riguardo alla loro implementazione. Alcune stanno valutando i pro e i contro dell'emissione di CBDC con uno scopo più ristretto, limitate alle transazioni all'ingrosso tra istituzioni finanziarie. Queste valute digitali non metterebbero in discussione l'attuale sistema a due livelli, ma avrebbero come obiettivo il miglioramento dell'efficacia operativa degli assetti esistenti. Sino ad ora, tuttavia, gli esperimenti con questo tipo di CBDC per le transazioni all'ingrosso non hanno dato risultati sufficientemente convincenti da spingere a una loro immediata emissione (riquadro V.C).

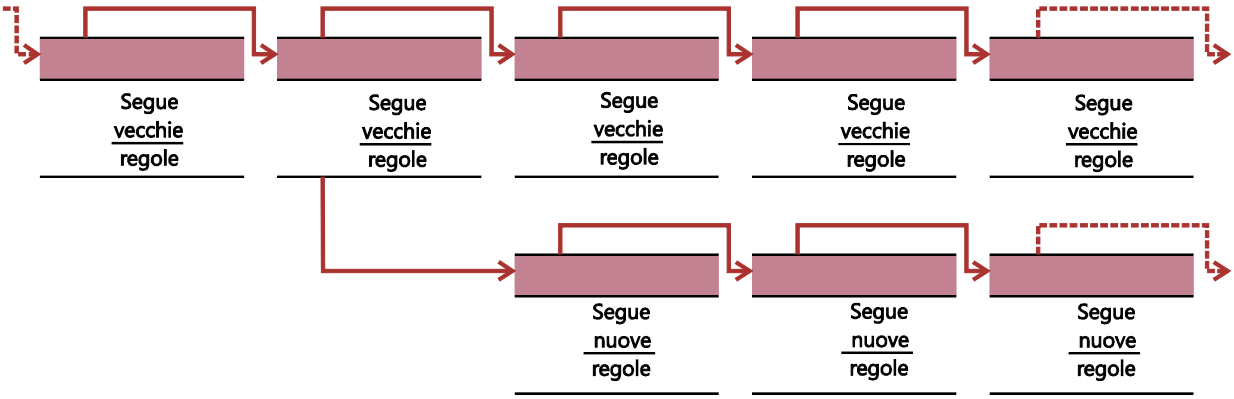
Riquadro V.A

Biforcazione e instabilità del consenso decentralizzato nella blockchain

La biforcazione ha contribuito alla crescita esplosiva del numero di criptovalute (grafico V.6, diagramma di destra). Per esempio, nel solo mese di gennaio 2018 sono emerse le biforcazioni Bitcoin All, Bitcoin Cash Plus, Bitcoin Smart, Bitcoin Interest, Quantum Bitcoin, BitcoinLite, Bitcoin Ore, Bitcoin Private, Bitcoin Atom e Bitcoin Pizza. Queste biforcazioni possono emergere in molti modi diversi, alcuni permanenti e altri temporanei. Uno di essi viene definito "hard fork" (grafico V.A). Emerge se alcuni miner di una criptovaluta si coordinano per cambiare il protocollo con un nuovo insieme di regole incompatibile con quello vecchio. Questo cambiamento potrebbe riguardare molti aspetti del protocollo, come la dimensione massima autorizzata dei blocchi, la frequenza con cui i blocchi possono essere aggiunti alla blockchain, oppure un cambiamento del processo di proof-of-work richiesto per aggiornare la blockchain. I miner che passano alle nuove regole iniziano dalla vecchia blockchain ma aggiungono poi blocchi che non sono riconosciuti dai miner che rispettano le vecchie regole. Questi ultimi continuano la costruzione della blockchain esistente seguendo le vecchie regole. In questo modo crescono due blockchain separate, ognuna con la sua storia di transazioni.

Esempio di un hard fork

Grafico V.A



Fonte: BRI.

La frequenza degli episodi di biforcazione potrebbe essere sintomatica di un problema inerente al modo in cui viene creato il consenso nella rete di miner decentralizzata di una criptovaluta. Più in generale, la questione economica di fondo è che il consenso decentralizzato non è unico. La regola secondo cui si deve proseguire la catena più lunga incentiva i miner a seguire la maggioranza computazionale, ma non stabilisce in modo inequivoco il percorso della maggioranza stessa. Per esempio, se un miner crede che l'ultimissimo aggiornamento del ledger sarà ignorato dal resto della rete di miner, diventa più conveniente anche per lui ignorarlo. E se la maggioranza die miner si mette d'accordo per ignorare un aggiornamento, si crea un nuovo equilibrio. In questo modo possono sorgere equilibri aleatori, ed è quello che è successo spesso, come segnalato dal fenomeno della biforcazione e dall'esistenza di migliaia di blocchi "orfani" (Bitcoin) o "zii" (Ethereum) che sono stati annullati retroattivamente. Altri timori rispetto alla solidità dell'aggiornamento decentralizzato della blockchain riguardano gli incentivi dei miner a effettuare strategicamente una biforcazione ogni volta che l'ultimo blocco aggiunto da un altro miner include commissioni elevate sulle transazioni, che possono essere deviate annullando il blocco in questione tramite una biforcazione①.

① Per un'analisi dell'unicità dell'aggiornamento della blockchain, cfr. B. Biais, C. Bisière, M. Bouvard, e C. Casamatta,"The blockchain folk theorem", *TSE Working Papers*, n. 17-817, 2017. Per un'analisi delle ragioni strategiche per la creazione di una biforcazione, cfr. M. Carlsten, H. Kalodner, S. M. Weinberg, A. Narayanan (2016), "On the instability of Bitcoin without the block reward.", *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*.

Riquadro V.B

La tecnologia a ledger distribuito nel credito al commercio

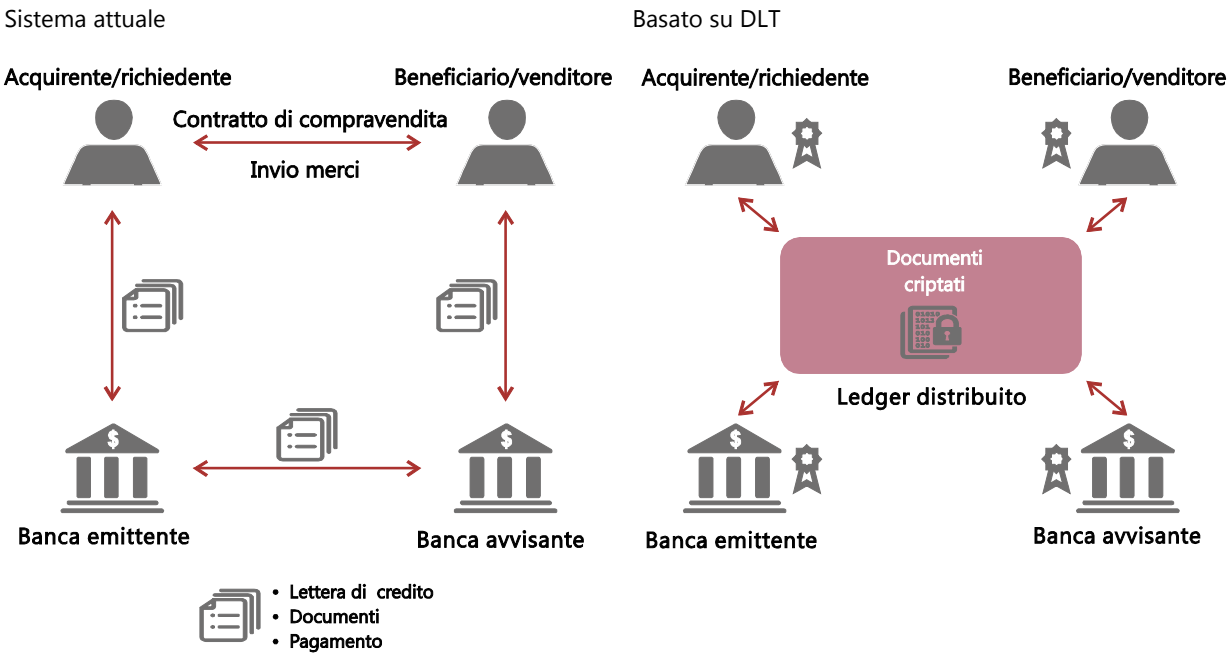
L'Organizzazione mondiale del commercio stima che l'80-90% del commercio mondiale faccia affidamento sul credito al commercio. Quando un esportatore e un importatore concordano uno scambio, l'esportatore spesso preferisce essere pagato in anticipo, per evitare il rischio che l'importatore non effettui il pagamento dopo aver ricevuto i beni. A sua volta, l'importatore preferisce ridurre il suo rischio richiedendo una documentazione attestante la spedizione dei beni prima di avviare il pagamento.

Il credito al commercio offerto da banche e altre istituzioni finanziarie permette di conciliare le esigenze delle parti coinvolte. Il più delle volte, una banca nel paese di origine dell'importatore emette una lettera di credito che garantisce il pagamento all'esportatore, dopo aver ricevuto la documentazione sulla spedizione, come ad esempio una polizza di carico. A sua volta, una banca nel paese dell'esportatore può concedere credito all'esportatore in cambio di questa garanzia e riscuotere il pagamento dalla banca dell'importatore per completare la transazione.

Nella sua forma attuale (grafico V.B, diagramma di sinistra), il credito al commercio è macchinoso, complesso e costoso. Necessita di molti scambi di documenti tra l'esportatore, l'importatore, le loro rispettive banche e gli agenti che effettuano le verifiche materiali dei beni spediti a ogni posto di controllo, nonché le autorità doganali, le agenzie pubbliche di finanziamento delle esportazioni o le compagnie che assicurano le merci spedite. Il processo spesso implica una gestione amministrativa cartacea. La DLT può semplificare l'esecuzione dei contratti sottostanti (diagramma di destra): per esempio, un contratto smart potrebbe automaticamente sbloccare il pagamento all'esportatore dietro l'inserimento di una polizza di carico valida nel ledger. Inoltre, la maggiore disponibilità di informazioni su quali spedizioni sono già state finanziate potrebbe anche ridurre il rischio che gli esportatori ottengano illegalmente un credito più volte per la stessa spedizione da parte di banche diverse.

Come funziona il credito al commercio su un ledger distribuito?

Grafico V.B



Fonte: adattato da www.virtusapolaris.com.

Riquadro V.C

Le valute digitali all'ingrosso delle banche centrali

Negli ultimi decenni le banche centrali hanno sfruttato le tecnologie digitali per migliorare l'efficienza e la solidità del sistema di pagamenti e, più in generale, del sistema finanziario. La tecnologia digitale ha permesso alle banche centrali di risparmiare sulla fornitura di liquidità ai sistemi di regolamento lordo in tempo reale. Collegando questi sistemi tramite il Continuous Linked Settlement (CLS o regolamento contestuale su base continuativa), le banche commerciali del mondo regolano migliaia di miliardi di operazioni in cambi 24 ore su 24, ogni giorno. Il CLS contribuisce a rimuovere il rischio "Herstatt" (il rischio che una banca corrispondente coinvolta in un'operazione in cambi si ritrovi in difficoltà finanziarie prima di pagare la valuta estera equivalente al ricevente designato), che prima rappresentava un rischio importante per la stabilità finanziaria. Più recentemente, è aumentata in tutto il mondo la rapidità dei pagamenti al dettaglio e le banche centrali stanno promuovendo e facilitando attivamente questa tendenza.

In linea con la volontà generale di esplorare nuove tecnologie di pagamento, le banche centrali stanno anche sperimentando CBDC per transazioni all'ingrosso. Queste sono versioni basate su token dei tradizionali conti di riserva e di regolamento. L'interesse per le CBDC all'ingrosso basate sulla DLT dipende dal potenziale che potrebbero avere queste tecnologie nel miglioramento dell'efficienza e nella riduzione dei costi operativi e di regolamento. I guadagni potrebbero essere sostanziali, nella misura in cui molti degli attuali sistemi di pagamento all'ingrosso gestiti dalle banche centrali si basano su tecnologie obsolete e costose da mantenere.

Ci sono due sfide chiave che riguardano l'implementazione delle CBDC all'ingrosso. In primo luogo, i limiti della DLT senza autorizzazione si applicano anche in questo caso, il che significa che le CBDC devono essere modellate sui protocolli con autorizzazione. In secondo luogo, le scelte progettuali per la convertibilità delle riserve delle banche centrali all'interno e all'esterno del ledger distribuito devono essere applicate con cautela, in modo da sostenere la liquidità infragiornaliera minimizzando allo stesso tempo i rischi di regolamento.

Alcune banche centrali, tra cui la Bank of Canada (progetto Jasper), la BCE, la Bank of Japan (progetto Stella) e la Monetary Authority of Singapore (progetto Ubin) hanno già effettuato esperimenti con sistemi di regolamento lordo in tempo reale all'ingrosso con CBDC basate su DLT. Nella maggior parte dei casi, le banche centrali hanno scelto un approccio fondato sul digital depository receipt (DDR), per mezzo del quale la banca centrale emette token digitali su un ledger distribuito, i quali sono coperti e riscattabili dalle riserve presso la banca centrale detenute in un conto segregato. I token possono poi essere utilizzati per effettuare trasferimenti interbancari su un ledger distribuito.

Le banche centrali stanno attualmente rendendo noti i risultati di questi esperimenti: nella fase iniziale, ognuno di essi è riuscito in buona parte a replicare gli attuali sistemi di pagamento di importi rilevanti; tuttavia, i risultati non sono stati chiaramente superiori a quelli ottenuti tramite le infrastrutture esistenti"①.

① Cfr. Bech M. e R. Garratt, "Criptovalute delle banche centrali," *Rassegna trimestrale BRI*, settembre 2017; e Comitato per i pagamenti e le infrastrutture di mercato e Comitato sui mercati, *Central bank digital currencies*, marzo 2018.

Note di chiusura

[1] La terminologia su questo tema è in continua evoluzione, con le conseguenti ambiguità giuridiche e regolamentari. L'uso del termine "criptovalute" in questo capitolo non intende indicare nessuna visione particolare sulla natura dei sistemi basati su protocollo che ne sono alla base: di regola, possiedono alcune caratteristiche delle valute sovrane, ma non tutte, e il loro trattamento giuridico varia a seconda delle giurisdizioni. In alcuni casi, il capitolo fa riferimento a criptovalute o criptoattività specifiche, a titolo di esempio. Questi esempi non sono esaustivi e non devono essere interpretati come un sostegno da parte della BRI o dei suoi azionisti a qualsivoglia criptovaluta, società, prodotto o servizio.

[2] Su questo tema, cfr. anche Carstens (2018a,c).

[3] Graeber (2011) afferma che il denaro cominciò a diffondersi solo con l'invenzione del conio, introdotto in Cina, India e Lidia quasi simultaneamente, attorno al 600-500 a.C. Illustra inoltre che, al contrario di quanto comunemente si crede, prima dell'uso del denaro gli scambi avvenivano principalmente attraverso dei pagherò bilaterali piuttosto che tramite il baratto.

[4] Queste funzioni della moneta sono state oggetto di studi approfonditi nella letteratura in materia. Ecco alcuni dei principali esempi: Kiyotaki e Wright (1989) mostrano come la moneta, quando è usata come mezzo di scambio, possa rappresentare un miglioramento rispetto al baratto. Kocherlakota (1996) dimostra che, quando non è possibile tenere un registro esatto per transazioni e impegni, la moneta migliora i risultati fungendo da "memoria". Samuelson (1958) illustra, tramite un modello a generazioni sovrapposte, che la moneta può aumentare l'efficienza quando è usata come riserva di valore. Doepke e Schneider (2017) mostrano come l'utilizzo di un'unità di conto comune migliori i risultati e spiegano perché la moneta pubblica sia allo stesso tempo unità di conto e mezzo di scambio.

[5] Esempi di beni usati come moneta merce sono le conchiglie in Africa, le fave di cacao nella civiltà azteca e i *wampum* (cinture di perline) nelle colonie del Nord America. Anche in questi casi, questi meccanismi coesistevano certamente con relazioni di credito. Cfr., per esempio, Melitz (1974) per un'analisi più approfondita.

[6] Riguardo all'evoluzione delle lettere di credito e al ruolo chiave che hanno avuto nello sviluppo dei sistemi monetari in generale, e nel credito al commercio in particolare, cfr. de Roover (1948, 1953). Per una storia e un'analisi dettagliate, cfr. Kindleberger (1984) per un approccio generale e Santarosa (2015) sull'importanza dell'introduzione dell'obbligazione solidale.

[7] La moneta pubblica garantita da una materia prima, come il gold standard o sistema aureo, fu un altro tentativo di stabilire un equilibrio. Se in tempi normali garantisce stabilità, in periodi di tensioni finanziarie ed economiche i suoi vincoli tendono a limitare la capacità della banca centrale di assicurare elasticità nell'offerta di moneta. In circostanze estreme, questi vincoli spesso sono stati semplicemente eliminati, passando all'inconvertibilità. Per esempio, con il sistema aureo, la funzione di convertibilità in oro poteva essere vista come un vincolo alla capacità dello Stato di emettere moneta in eccesso e deprezzare la valuta. Il vincolo era credibile proprio perché la materia prima ha un valore di mercato per usi non monetari, cioè non come mezzo di pagamento. Ciò permetteva di evitare che lo Stato tenesse i detentori della moneta ostaggio dei suoi poteri di monopolio. Cfr. Giannini (2011) per ulteriori analisi.

[8] Per uno studio recente, che include un'analisi degli incentivi per svalutare la moneta, cfr. Schnabel e Shin (2018).

[9] Cfr. Van Dillen (1964), Roberds e Velde (2014) e Bindseil (2018). Riguardo al legame con le banche centrali, cfr. Ugolini (2017); Bindseil (2018) e Schnabel e Shin (2018).

[10] Inoltre, le banche centrali hanno solitamente avuto la flessibilità di agire come prestatore di ultima istanza. La recente Grande Crisi Finanziaria ha ricordato ancora una volta la fragilità e allo stesso tempo l'adattabilità degli assetti monetari odierni, anche nelle economie più avanzate. Se la crisi ha messo a nudo le lacune del quadro regolamentare vigente, l'attenzione data alla vigilanza bancaria e alla regolamentazione nel periodo che è seguito evidenzia come gli assetti istituzionali possano evolvere per mantenere la fiducia nella moneta all'interno del quadro generale del sistema su due livelli.

[11] Cfr. Carstens (2018a). Anche Giannini (2011) sottolinea l'importanza degli assetti istituzionali che assicurano l'offerta di moneta: "L'evoluzione delle istituzioni monetarie sembra essere soprattutto il frutto di un dialogo continuo tra la sfera economica e politica, in cui entrambe cercano a turno di creare innovazioni monetarie [...] e di salvaguardare l'interesse comune contro gli abusi derivanti dagli interessi di parte."

[12] Oggigiorno le banche centrali supervisionano i sistemi di pagamento e forniscono ingenti quantità di credito infragiornaliero per garantire proprio questo risultato, in particolare nei sistemi di pagamento all'ingrosso. A seconda delle specificità degli assetti, questo credito può anche essere concesso overnight o a scadenze più lunghe. Per una descrizione più approfondita degli assetti, delle procedure operative e di altre questioni, cfr. BRI (1994) e Borio (1997).

[13] Cfr. Bech e Garratt (2017) e CPIM-CM (2018) per un'analisi dettagliata.

[14] Come con le banconote e altri token fisici, ogni transazione è verificata in riferimento all'oggetto del pagamento, ovvero l'iscrizione rispettiva nel ledger. Ciò costituisce una differenza rispetto ad altre forme di denaro elettronico, in cui la verifica si basa sull'identità del detentore del conto. Di conseguenza, le criptovalute sono moneta digitale basata su token.

[15] Tra le criptovalute attualmente esistenti e quelle in via di elaborazione che usano un modello con autorizzazione con nodi fidati selezionati, ricordiamo la moneta che verrà emessa dalla fondazione SAGA, il Ripple e l'Utility Settlement Coin.

[16] Usiamo "Bitcoin" per indicare il protocollo e la rete di utenti e miner della criptovaluta e "bitcoin" per l'unità monetaria.

[17] Tra gli esempi, vi sono Ethereum, Litecoin e Namecoin.

[18] Auer (2018) presenta una descrizione dettagliata degli elementi tecnologici del Bitcoin e di altre criptovalute basate sulla blockchain, come le firme digitali, l'hashing e il concatenamento crittografico di blocchi. Cfr. anche Berentsen e Schär (2018).

[19] Tecnicamente, ciò avviene tramite l'uso di funzioni crittografiche di hash, come SHA-256 nel Bitcoin. Queste funzioni sono caratterizzate dal fatto che i risultati sono imprevedibili, e un risultato specifico può quindi essere generato solo tramite tentativi ed errori.

[20] Affinché una criptovaluta senza autorizzazione possa funzionare in un contesto dove la fiducia è del tutto assente, tutti i miner e gli utenti devono conservare una copia aggiornata dell'intero ledger. Tuttavia, nella pratica, molti utenti si fidano delle informazioni fornite da altri. Alcuni utenti verificano solo la sintesi delle informazioni del ledger mediante un processo chiamato "simplified payment verification" (verifica dei pagamenti semplificata). Inoltre, in forte contrasto con l'idea originaria alla base del Bitcoin, un numero ancora più ragguardevole di utenti può accedere ai propri fondi solo tramite un sito internet di un soggetto terzo. In questi casi, solo questo soggetto terzo ha il controllo delle posizioni in criptovaluta dei suoi clienti.

[21] Nakamoto (2009), p. 8.

[22] Ciò viene ottenuto tramite un'autocalibrazione del proof-of-work, che aumenta il livello richiesto di difficoltà matematica fino al punto in cui la potenza computazionale congiunta di tutti i miner è sufficiente soltanto per aggiornare il ledger alla velocità prestabilita dal protocollo.

[23] Cfr. Carstens (2018a).

[24] Il problema della congestione potrebbe essere risolto permettendo un aumento della dimensione dei blocchi, ma ciò potrebbe avere conseguenze ancora più gravi. Tralasciando i block reward, un certo livello di congestione è necessario per indurre gli utenti a pagare per le transazioni: se il sistema operasse al di sotto della soglia, tutte le transazioni sarebbero elaborate e quindi gli utenti razionali non pagherebbero quasi nessuna commissione. I miner non riceverebbero nessun beneficio dall'aggiornamento delle transazioni e l'equilibrio rischierebbe di crollare. Cfr. in particolare Hubermann et al. (2017) e Easley et al.(2017), nonché Abadi eBrunnermeier (2018).

[25] In termini tecnici, l'interazione tra gli utenti è tra sostituti strategici, non tra complementi strategici. Le criptovalute sono quindi più un gioco di congestione che di coordinamento.

[26] La natura probabilistica della definitività potrebbe creare rischi aggregati in particolare se le criptovalute fossero usate per pagamenti all'ingrosso, in cui i fondi tendono a essere reinvestiti senza indugio. Di fatto, ciò creerebbe una dimensione completamente nuova di rischio aggregato, dato che le esposizioni sarebbero connesse tra loro attraverso la probabilità di non definitività di tutta la storia delle transazioni.

[27] Le proposte di soluzioni non mancano, ma la maggior parte di esse non è ancora stata sperimentata nella pratica. Da un lato, i futuri protocolli di criptovalute potrebbero abbandonare i costosi processi di proof-of-work per rimpiazzarli con processi di "proof-of-stake", che si basano sull'idea di realizzare la credibilità dimostrando il possesso di posizioni in criptovalute piuttosto che effettuando un costoso lavoro computazionale. Le soluzioni proposte per il problema della scalabilità includono il Lightning Network, che fondamentalmente sposta le piccole transazioni fuori dalla blockchain principale e in

un ambiente separato prefinanziato. Vi sono anche nuove criptovalute, come la IOTA, che intendono sostituire la blockchain con un ledger e una struttura di verifica più complessi.

[28] Cfr. Juskalian (2018).

[29] Cfr. Carstens (2018a,b).

[30] Neanche i funzionari pubblici sono immuni al fascino delle criptovalute: due agenti governativi statunitensi sono stati accusati del furto di bitcoin confiscati in occasione della chiusura di Silk Road.

[31] Per esempio, la maggior parte dei pagamenti in bitcoin effettuati tramite uno smartphone sono probabilmente elaborati indirettamente da soggetti terzi, dato che l'attuale dimensione della blockchain supera la capacità di memoria della maggior parte degli smartphone. Reuters (2017) e Moore e Christin (2013) elencano alcuni dei casi in cui questi soggetti terzi si sono rivelati fraudolenti o hanno subito attacchi da parte di hacker. Per un'analisi degli usi illeciti delle criptovalute, cfr. Fanusie e Robinson (2018) e Foley et al. (2018).

[32] Cfr. Ministri finanziari e Governatori delle banche centrali del G20 (2018).

[33] Clayton (2017), analizzando la regolamentazione delle ICO rispetto alle OPI dalla prospettiva degli Stati Uniti, afferma che un "cambiamento della struttura dell'offerta di titoli non cambia la questione fondamentale, e cioè che quando vi è un'offerta di titoli devono essere seguite le nostre leggi sui valori mobiliari". FINMA (2018) ha stabilito un quadro regolamentare in Svizzera che classifica le ICO in base all'uso finale dei token emessi: come pagamenti, come attività o come utility token.

[34] Tecnicamente, per far funzionare le criptovalute basate su un protocollo è sufficiente che almeno un paese permetta l'accesso. Le difficoltà che le autorità hanno riscontrato per chiudere siti web di download illegali come Napster o The Pirate Bay e protocolli di download come BitTorrent sottolineano i problemi relativi all'esecuzione delle norme.

[35] La Financial Action Task Force (2015) afferma che è fondamentale che vi sia coerenza nel trattamento di prodotti e servizi simili a seconda della loro funzione e del loro profilo di rischio nelle varie giurisdizioni, al fine di migliorare l'efficacia degli standard internazionali antiriciclaggio.

[36] Una complicazione è data dal fatto che i pagamenti sono regolamentati da un insieme di autorità e di norme con obiettivi molto diversi, come il controllo del sistema dei pagamenti, la vigilanza prudenziale, la protezione dei consumatori e la lotta contro il finanziamento del terrorismo e il riciclaggio di denaro. Per esempio, le istituzioni con sede negli Stati Uniti devono osservare anche le norme della legge sulla segretezza bancaria (Bank Secrecy Act), dell'USA PATRIOT Act e dell'Office of Foreign Assets Control. Un'altra complicazione riguarda l'applicabilità della legislazione esistente ai nuovi strumenti. Ad esempio, nell'Unione europea, la definizione giuridica di moneta elettronica include l'obbligo che i saldi rappresentino un credito nei confronti dell'emittente. Dato che le criptovalute non rappresentano nessun credito, non possono essere considerate moneta elettronica e di conseguenza, per esclusione, non sono coperte dalla relativa legislazione.

[37] Vi sono molte applicazioni tecniche potenziali di CBDC basate su token. Potrebbero essere basati su una DLT con caratteristiche analoghe alle criptovalute, con la differenza che la banca centrale, e non il protocollo, avrebbe il controllo sugli importi emessi e garantirebbe il valore del token.

[38] CPIM-CM (2018).

Riferimenti bibliografici

Abadi, J. e M. Brunnermeier (2018): "Blockchain economics", Princeton University, mimeo, maggio.

Auer, R. (2018): "The mechanics of decentralised trust in Bitcoin and the blockchain" *BIS Working Papers*, di prossima pubblicazione.

Autorità federale di vigilanza sui mercati finanziari (FINMA) (2018): *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, 16 febbraio.

Banca dei regolamenti internazionali (1994): *64ª Relazione annuale*, giugno.

Bech, M. e R. Garratt (2017): "Criptovalute delle banche centrali", *Rassegna trimestrale BRI*, settembre 2017.

Berentsen, A. e F. Schär (2018): "A short introduction to the world of cryptocurrencies", Federal Reserve Bank of St. Louis, *Review*, vol. 100, n. 1.

Bindsell, U. (2018): "Pre-1800 central bank operations and the origins of central banking", Universität Mannheim, mimeo.

Borio, C. (1997): "The implementation of monetary policy in industrial countries: a survey", *BIS Economic Papers*, n. 47, luglio.

Carstens, A. (2018a): "Money in the digital age: what role for central banks?", discorso presso la House of Finance, Goethe-Universität, Francoforte sul Meno, 6 febbraio.

——— (2018b): "Central Banks and cryptocurrencies: guarding trust in a digital age", dichiarazioni rilasciate presso la Brookings Institution, Washington DC, 17 aprile.

——— (2018c): "Technology is no substitute for trust", *Börsen-Zeitung*, 23 maggio.

Catalini, C., J. Boslego e K. Zhang (2018): "Technological opportunity, bubbles and innovation: the dynamics of initial coin offerings", *MIT Working Papers*, di prossima pubblicazione.

Clayton, J. (2017): "Statement on cryptocurrencies and initial coin offerings", www.sec.gov/news/public-statement/statement-clayton-2017-12-11, 11 dicembre.

Comitato per i pagamenti e le infrastrutture di mercato e Comitato sui mercati (2018): *Central bank digital currencies*, marzo.

De Roover, R. (1948): *Money, banking and credit in mediaeval Bruges: Italian merchant bankers Lombards and money changers, a study in the origins of banking*, Mediaeval Academy of America.

——— (1953): *L'évolution de la lettre de change: XIVe-XVIIIe siècle*, Armand Colin.

Doepke, M. e M. Schneider (2017): "Money as a unit of account", *Econometrica*, vol. 85, n. 5, pagg. 1537-1574.

Easley, D., M. O'Hara e S. Basu (2017): "From mining to markets: The evolution of Bitcoin transaction fees", papers.ssrn.com/sol3/papers.cfm?abstract_id=3055380.

Fanusie, Y. e T. Robinson (2018): "Bitcoin laundering: an analysis of illicit flows into digital currency services", memorandum del Center on Sanctions & Illicit Finance, gennaio.

Financial Action Task Force (2015): *Guidance for a risk-based approach to virtual currencies*, giugno.

Foley, S., J. R. Karlsen, e T. J. Putniņš (2018): "Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies?", dx.doi.org/10.2139/ssrn.3102645.

Giannini, C. (2011): *The age of central banks*, Edward Elgar.

Graeber, D. (2011): *Debt: the First 5,000 Years*, Melville House. [trad. it., *Debito: i primi 5000 anni*, Il Saggiatore, 2012]

Huberman, G., J. Leshno e C. Moellemi (2017): "Monopoly without a monopolist: an economic analysis of the Bitcoin payment system", *Columbia Business School Research Papers*, n. 17-92.

Juskalian, R. (2018): "Inside the Jordan refugee camp that runs on blockchain", *MIT Technology Review*, edizione online, 12 aprile.

Kindleberger, C. (1984): *A financial history of western Europe*, Allen & Unwin. [trad. it., *Storia della finanza nell'Europa occidentale*, Laterza-Cariplo 1987]

Kiyotaki, N. e R. Wright (1989): "On money as a medium of exchange", *Journal of Political Economy*, vol. 97, n. 4, pagg. 927-954.

Kocherlakota, N. (1996): "Money is memory", *Journal of Economic Theory*, vol. 81, n. 2, pagg. 232-251.

Melitz, J. (1974): *Primitive and modern money: an interdisciplinary approach*, Addison-Wesley.

Ministri finanziari e Governatori delle banche centrali del G20 (2018). Comunicato del vertice di Buenos Aires, 19-20 marzo.

Moore, T. e N. Christin (2013): "Beware the middleman: empirical analysis of Bitcoin-exchange risk", in A.-R. Sadeghi (a cura di), *Lecture Notes in Computer Science*, vol. 7859.

Nakamoto, S. (2009): "Bitcoin: a peer-to-peer electronic cash system", libro bianco.

Reuters (2017): "Cryptocurrency exchanges are increasingly roiled by hackings and chaos", 29 settembre.

Roberds, W. e F. Velde (2014): "Early public banks", *Federal Reserve Bank of Chicago Working Papers*, n. 2014-03.

Samuelson, P. (1958): "An exact consumption-loan model of interest with or without the social contrivance of money", *Journal of Political Economy*, vol. 66, n. 6, pagg. 467-482.

Santarosa, V. (2015): "Financing long-distance trade: the joint liability rule and bills of exchange in eighteenth-century France", *The Journal of Economic History*, vol. 75, n. 3, pagg. 690-719.

Schnabel, I. e H. S. Shin (2018): "Money and trust: lessons from the 1620s for money in the digital age", *BIS Working Papers*, n. 698, febbraio.

Ugolini, S. (2017): *The evolution of central banking: theory and history*, Palgrave-Macmillan.

Van Dillen, J. G. (1964): *History of the principal public banks*, Frank Cass & Co LTD.