



BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

La governance delle blockchain e dei sistemi
basati sulla tecnologia dei registri distribuiti

di Carlo Gola, Valentina Cappa, Patrizio Fiorenza, Paolo Granata,
Federica Laurino, Lorenzo Lesina, Francesco Lorizzo e Gabriele Marcelli

Giugno 2023

Numero

773



BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

La governance delle blockchain e dei sistemi
basati sulla tecnologia dei registri distribuiti

di Carlo Gola, Valentina Cappa, Patrizio Fiorenza, Paolo Granata,
Federica Laurino, Lorenzo Lesina, Francesco Lorizzo e Gabriele Marcelli

Numero 773 – Giugno 2023

La serie Questioni di economia e finanza ha la finalità di presentare studi e documentazione su aspetti rilevanti per i compiti istituzionali della Banca d'Italia e dell'Eurosistema. Le Questioni di economia e finanza si affiancano ai Temi di discussione volti a fornire contributi originali per la ricerca economica.

La serie comprende lavori realizzati all'interno della Banca, talvolta in collaborazione con l'Eurosistema o con altre Istituzioni. I lavori pubblicati riflettono esclusivamente le opinioni degli autori, senza impegnare la responsabilità delle Istituzioni di appartenenza.

La serie è disponibile online sul sito www.bancaditalia.it.

LA GOVERNANCE DELLE BLOCKCHAIN E DEI SISTEMI BASATI SULLA TECNOLOGIA DEI REGISTRI DISTRIBUITI

di Carlo Gola, Valentina Cappa*, Patrizio Fiorenza*, Paolo Granata*,
Federica Laurino*, Lorenzo Lesina*, Francesco Lorizzo** e Gabriele Marcelli**

Sommario

Il lavoro affronta il tema della governance dei sistemi basati sulla tecnologia dei registri distribuiti (*distributed ledger technology*, DLT). Questa tecnologia consente di creare un archivio elettronico condiviso e accessibile via internet, in cui sono memorizzate le informazioni in modo sicuro e irreversibile. L'aggiornamento e la gestione del registro avvengono senza ricorrere a un ente terzo fiduciario. L'assenza di strutture organizzative e di governance tradizionali rende complessa la gestione delle DLT. Il lavoro fornisce gli strumenti per comprendere la tecnologia DLT e analizza la governance, sia per le DLT aperte (*permissionless*), sia per quelle ad accesso limitato (*permissioned*). Vengono suggeriti diversi approcci per l'applicazione di regole di governo, anche in presenza di DLT con una governance interamente algoritmica (*full algorithmic governance*). Si mostra che la creazione di strumenti, detti governance tokens, aventi diritti amministrativi e patrimoniali incorporati, favorisce i processi gestionali e di controllo delle DLT. Infine si descrive la struttura di governance di due DLT: Ethereum e Polkadot.

Classificazione JEL: G3, M4, D82, G14, G21, G28, M4, M15, O33.

Parole chiave: blockchain, DLT, corporate governance, governance algoritmica, governance token, cripto-attività, finanza decentralata, supervisione bancaria e finanziaria.

DOI: 10.32057/0.QEF.2023.0773

Indice

1	Introduzione.....	5
2	Cenni sui principi di corporate governance.....	8
2.1	Sui fondamenti di una struttura organizzativa e di governo.....	8
2.2	Una definizione di corporate governance per registri distribuiti.....	10
2.3	Proprietà e controllo.....	10
3	Governance collettiva e algoritmica.....	11
3.1	La blockchain come sistema per costruire la fiducia reciproca.....	12
3.2	I protocolli di consenso e i diritti di voto.....	14
3.3	Governance <i>off-chain</i> e <i>on-chain</i> (algoritmica).....	16
4	Quando è necessario l'intervento del regolatore.....	18
4.1	La trasparenza e il ruolo del <i>white paper</i>	19
4.2	Requisiti di governance in funzione delle attività svolte.....	20
4.3	Sul problema dell' <i>entry point</i>	20
4.4	Sui limiti di un sistema di governo decentrato.....	23
5	Conclusioni.....	24
	Appendice.....	26
	Bibliografia.....	30

* Servizio Supervisione Intermediari Finanziari, Dipartimento Vigilanza Bancaria e Finanziaria, Banca d'Italia.

** Servizio Pianificazione Informatica, Dipartimento Informatica, Banca d'Italia.

1 Introduzione¹

La blockchain è una tecnologia che consente di creare un archivio elettronico condiviso e accessibile via internet, in cui sono memorizzate in modo sicuro e irreversibile le informazioni inserite liberamente dai partecipanti al network. L'aggiornamento del registro – con riguardo, ad esempio, alle informazioni relative a transazioni economiche – avviene in modo decentrato, senza ricorrere a un ente terzo fiduciario, come nei sistemi tradizionali. Il lavoro analizza la governance delle blockchain e più in generale dei registri crittografici distribuiti (*distributed ledger technology* - DLT), sia di tipo *permissionless*, che *permissioned* (cfr. Box 1).

Gli organismi internazionali (FMI (2023), FSB (2022)) raccomandano per l'ecosistema cripto appropriate strutture di governo e di controlli interni, in grado di assicurare un'efficace e prudente gestione dei rischi². Tale obiettivo è più agevolmente conseguibile per le DLT *permissioned*, dove i partecipanti possono operare solo se autorizzati e con ruoli ben definiti, rispetto a quelle *permissionless*, ove il rispetto di regole di governance può essere problematico. Il lavoro analizza l'argomento e fornisce alcune proposte di policy.

Negli ultimi anni i regolatori bancari e finanziari hanno posto grande attenzione alla tematica delle cripto-attività, anche in relazione al fatto che la DLT permette di negoziare e trasferire la titolarità di strumenti o prodotti finanziari tradizionali. Nel 2022 la Commissione europea ha emanato un pacchetto legislativo sulla finanza digitale (il c.d. *Digital Finance Package*) che mira a fornire una cornice normativa anche per queste tecnologie e a regolarne le sperimentazioni. Di recente il comitato di Basilea, impegnato a definire criteri di trattamento prudenziale per le banche che intendono detenere cripto-attività, ha deciso di valutare se le DLT *permissionless* possano essere considerate affidabili come quelle *permissioned* dal punto di vista della governance³. La problematica è rilevante anche perché la base su cui si appoggia la maggior parte delle iniziative di finanza decentrata (DeFi) è la DLT *permissionless* Ethereum.

* Servizio Supervisione Intermediari Finanziari, Dipartimento Vigilanza Bancaria e Finanziaria, Banca d'Italia.

** Servizio Pianificazione Informatica, Dipartimento Informatica, Banca d'Italia.

¹ Le opinioni espresse sono personali e non impegnano in alcun modo l'Istituzione di appartenenza. Eventuali errori o imprecisioni sono attribuibili esclusivamente agli autori. Essi ringraziano: Paolo Angelini, Fabio Bernasconi, Luigi Cannari, Roberto Parmeggiani, Andrea Pilati, Giuseppe Siani, Zorana Milicevic, per gli utili commenti. Un ringraziamento particolare va a Marco Bevilacqua, Oscar Borgogno, Marina La Fratta e Carlo Lanfranchi per i preziosi suggerimenti. Nessun *endorsement* viene fatto sui casi di DLT citati a scopo illustrativo.

² In particolare, l'FSB (2022) ha osservato che: "Authorities should have the appropriate powers and tools, and adequate resources, to regulate, supervise, and oversee crypto-asset activities and markets, including crypto-asset issuers and service providers, as appropriate", Raccomandazione 1.

³ Cfr. BCBS (2022), p. 4.

La tematica è stata oggetto della recente *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*, ove si osserva che «[...] la tecnologia “lega” le componenti oggettive (strumenti, infrastrutture tecniche e organizzative) e soggettive (le diverse tipologie di operatori coinvolti) degli ecosistemi in nuovi prodotti e servizi, espressione “sintetica” di ciascun contributo. Tale rilevanza della componente tecnologica e degli stessi fornitori di tecnologia realizza una sorta di “governance algoritmica” che scardina gli schemi di governo tradizionali e della quale è necessario tenere conto»⁴.

Box 1 – DLT: tecnologia, accessibilità, governance

Sotto il profilo tecnologico, le DLT sono particolari architetture informatiche caratterizzate come sistemi distribuiti composti da una rete di nodi elaborativi che cooperano tra loro per raggiungere uno stato comune, sotto forma di registro condiviso; gli aggiornamenti allo stato del registro avvengono grazie ai c.d. “algoritmi di consenso”, che definiscono le regole che i nodi devono rispettare per effettuare tali aggiornamenti. Le blockchain costituiscono uno specifico sottoinsieme delle DLT, dotate di due ulteriori proprietà: (a) il loro registro è strutturato sotto forma di blocchi di transazioni (che costituiscono le unità elementari di aggiornamento dello stato del registro) e; (b) i blocchi sono concatenati tra di loro grazie all'utilizzo di particolari funzioni crittografiche, che rendono possibile aggiornare il registro solamenteaggiungendo dati alla fine, senza poter modificare blocchi precedenti.

In questo lavoro utilizzeremo la definizione di DLT di recente adottata dal regolamento europeo 2022/858 (*DLT Pilot regime*) che recita quanto segue: “una DLT è una tecnologia che consente il funzionamento e l'uso dei registri distribuiti” ove per registro distribuito si intende “archivio di informazioni in cui sono registrate le operazioni e che è condiviso da una serie di nodi di rete DLT ed è sincronizzato tra di essi, mediante l'utilizzo di un meccanismo di consenso”.

Le DLT vengono solitamente classificate in base ai profili di lettura e scrittura. In base ai profili di lettura, e quindi alla possibilità di accedervi per consultare le informazioni contenute nel registro, le DLT sono classificate in pubbliche e private (questo secondo caso prevede che solo alcuni nodi autorizzati possano accedervi). In base ai profili di scrittura, invece, le DLT sono comunemente distinte tra *permissionless* e *permissioned* in accordo alla modalità di partecipazione al meccanismo di consenso (nelle *permissioned*, solo alcuni dei nodi sono autorizzati a partecipare al meccanismo di consenso che permette l'aggiornamento dello stato del registro).

La governance che potremmo definire “ordinaria” del registro avviene, come sopra descritto, attraverso automatismi codificati nel protocollo di consenso, che definisce le regole per il suo aggiornamento. Qualora si debbano invece andare a effettuare dei cambiamenti strutturali a tali regole (upgrading di aspetti rilevanti del software), si pone invece il problema di come tali modifiche, che potremmo definire “straordinarie”, possano essere governate.

Analizzare la struttura di governo delle DLT *permissioned* è più agevole, dato che vi si applicano processi di coordinamento esplicito tra i gestori, in linea con quanto avviene ad esempio nelle tradizionali strutture societarie. Più complessa è invece l'analisi della struttura di governo delle DLT *permissionless*, in cui alcuni processi possono essere regolati, a vario livello, dalla governance algoritmica, detta anche “*on-chain*”. La governance *on-chain* si distingue da quella “*off-chain*” in quanto automatizza le funzioni di governo.

Il bilanciamento tra processi governati *on-chain* e *off-chain* è una peculiarità della specifica blockchain; in questo lavoro, per esemplificare le differenze tra i due approcci, vengono analizzate due piattaforme che adottano modelli piuttosto diversi tra loro: Ethereum e Polkadot. Ethereum affianca al protocollo informatico nativo (quello principale, di inizio progetto) processi decisionali in capo a persone fisiche o giuridiche individuabili. Ad esse sono demandate decisioni “straordinarie” relative al funzionamento della DLT. La blockchain Polkadot, invece, ambisce a introdurre nel protocollo stesso tutti i processi organizzativi e decisionali. Questa modalità può essere classificata come “interamente *on-chain*” o anche governance algoritmica completa (*full algorithmic governance*). Anch'essa prevede organi, comitati tecnici, meccanismi di voto, ma l'*enforcement* è automatizzato. La governance algoritmica completa prevede quindi l'inclusione di meta-regole atte a rivedere, secondo modalità predefinite, anche le regole “costituzionali” del protocollo stesso. La governance algoritmica (sia parziale che completa) è associata all'emissione di *governance token* che

⁴ Cfr. Banca d'Italia (2022), p. 7.

forniscono diritti di voto, amministrativi e talvolta anche patrimoniali a soggetti che partecipano alla gestione della DLT.

Vi sono vantaggi e svantaggi in ambedue gli approcci: solo per citare i principali, i processi *off-chain* sono soggetti a opacità, azzardo morale, conflitto di interessi dei partecipanti; i secondi (*on-chain*) sono trasparenti e verificabili, ma necessariamente più rigidi e “incompleti”, nel senso che non sono in grado – per definizione – di includere processi decisionali non individuabili ex ante. Inoltre, le decisioni assunte da sistemi di governance algoritmica potrebbero essere fonte di effetti automatizzati indesiderabili e potenzialmente non controllabili. L’approccio *on-chain* deve peraltro ancora mostrare di essere in grado di risolvere alcuni problemi come la correzione ex post di transazioni inserite in modo errato o di dare risposta all’esigenza di avere un chiaro fondamento giuridico incluso il foro competente ove risolvere eventuali contenziosi.

Prima di procedere è necessario fare alcune precisazioni: il perimetro della nostra analisi riguarda esclusivamente i processi di governo relativi al funzionamento delle DLT, escludendo quindi quelli che riguardano i servizi offerti da terzi a supporto delle cripto-attività, come ad esempio le piattaforme di scambio di cripto-attività o la custodia di tali attività. Parimenti non sono trattati nel lavoro gli aspetti, peraltro assai rilevanti, relativi ai fondamenti giuridici di queste infrastrutture tecnologiche decentralizzate⁵. Un tentativo in tal senso è stato condotto per le organizzazioni autonome decentralizzate (c.d. DAO) da Brummer e Seria (2022) ove si cerca di individuare un “contenitore legale” (*legal wrapper*) tra le forme giuridiche esistenti negli Stati Uniti, siano esse società di capitali, anche a responsabilità limitata, società cooperative senza scopo di lucro, fondazioni, fiduciarie, partnership, joint ventures, e financo associazioni senza personalità giuridica, come i *social clubs*. Nessuna delle categorie citate pare accogliere in modo soddisfacente queste forme organizzative e probabilmente sarà necessario introdurre una nuova categoria. A tale riguardo, come dovrebbe emergere chiaramente nel corso della nostra trattazione, sarà necessario porre particolare attenzione al ruolo della randomizzazione e dei governance token. Il primo aspetto si sostanzia nell’assegnazione casuale dei diritti amministrativi, di controllo e di delega; un dispositivo utilizzato per evitare la concentrazione dei poteri e garantire (o cercare di garantire) a soggetti “atomistici” una forma implicita di coordinamento; il secondo aspetto attiene alla necessità di allineare gli incentivi verso uno scopo condiviso attraverso l’uso di rappresentazioni digitali di diritti aventi valore di mercato, trasferibili e negoziabili. Molti problemi rimangono aperti, quali la natura di questi diritti e le modalità attraverso le quali essi possano essere rappresentati e protetti. Infine teniamo a sottolineare che il lavoro non fornisce un’analisi dei rischi relativi alla gestione e controllo di questa tecnologia, ma unicamente un quadro concettuale preliminare per tali ulteriori sviluppi.

Il lavoro è strutturato nel modo seguente: dopo avere descritto gli elementi essenziali della corporate governance tradizionale (paragrafo 2), si confrontano tali aspetti con le caratteristiche di governo implicite o esplicite delle DLT, sia *permissionless* che *permissioned* (paragrafo 3). In seguito si discute il tema dell’intervento del regolatore (quando intervenire, come calibrare l’intervento, come fare *enforcement* a fronte di diversi sistemi di DLT) (paragrafo 4). Il paragrafo 5 fornisce alcune considerazioni conclusive. In Appendice vengono descritti i sistemi di governo di due DLT *permissionless* che utilizzano processi di governance sia *on-chain* sia *off-chain*, Ethereum e Polkadot.

⁵ Su questi aspetti, si vedano: Garrido *et al.* (2022); O. Borgogno (2022); UK Jurisdiction Taskforce (2019); The Law Society (2020), specie il capitolo 8, “*Blockchain Consortia*”. Per un inquadramento nelle categorie generali del diritto civile e nel diritto finanziario italiano, con particolare riferimento alle cripto-attività, si veda C. Lanfranchi (2019).

2 Cenni sui principi di corporate governance

La corporate governance è un sistema di regole riguardanti i diritti, i processi organizzativi e i meccanismi di controllo degli organi gestionali e di direzione, per salvaguardare gli interessi degli *stakeholders* e conseguire gli obiettivi strategici dell'impresa. Essa dovrebbe allineare gli incentivi, stabilire responsabilità, monitorare i processi e determinare una serie di valori attraverso una cultura di impresa. Storicamente, si sono affermati diversi modelli di governo: più prescrittivi nell'Europa continentale; basati su principi generali e sull'autogoverno, nei paesi di *common law*. La materia spesso si è evoluta a seguito di importanti crisi societarie. L'approccio basato su principi generali presenta il vantaggio che meglio si adatta alle circostanze, inclusi gli sviluppi tecnologici. Nel Regno Unito l'intera materia è stata sistematizzata nel Rapporto Cadbury del 1992, poi confluito nel *Combined Code on Corporate Governance*, aggiornato periodicamente dal *Financial Reporting Council*⁶. In Europa, la Commissione ha svolto un ruolo importante per creare un quadro di riferimento applicabile in paesi con tradizioni e strutture normative differenti⁷. In ambito bancario e finanziario detti principi sono stati declinati ponendo particolare enfasi sui profili di sana e prudente gestione, sul ruolo degli organi di controllo, monitoraggio e mitigazione dei rischi⁸.

A livello internazionale, l'OCSE ha sviluppato principi divenuti un punto di riferimento sull'argomento. Lo scopo è stato quello di “favorire gli investimenti di lungo periodo, la stabilità finanziaria, l'integrità e, da ultimo, la crescita e l'inclusività di una economia”⁹. Ciò avviene “attraverso un ambiente economico basato sulla fiducia, la trasparenza e la responsabilità”. L'OCSE sottolinea che un framework di corporate governance “tipicamente include elementi relativi alla legislazione, la regolamentazione, i sistemi di autoregolamentazione (*self-regulatory arrangements*), gli impegni volontari (*voluntary commitments*), le pratiche d'affari derivanti da circostanze specifiche, da fattori storici o dalle tradizioni dei vari paesi”; ciò che rileva – sottolinea l'OCSE – è il risultato finale (“*functional equivalence principle*”)¹⁰. Aspetti di governance sono presenti anche nella recente regolamentazione europea che permette, in via sperimentale, di emettere e negoziare titoli tramite la DLT¹¹.

2.1 Sui fondamenti di una struttura organizzativa e di governo

Da un punto di vista formale, una struttura di governo è un sistema organizzativo in grado di pervenire a decisioni in base a una regola di scelta collettiva (uno statuto, un codice condiviso, un protocollo) e a decisioni formulate sulle informazioni accessibili in un dato momento da parte degli agenti

⁶ Cfr. N. G. Maw *et al.* (1994); J.H. Farrar e B.M. Hannigan (1998),

⁷ Commissione Europea, “Libro Verde. Il quadro dell'Unione europea in materia di governo societario”, Bruxelles, 5 aprile 2012. Cfr. anche: Commissione Europea, Piano d'azione: diritto europeo delle società e governo societario- una disciplina giuridica moderna a favore di azionisti più impegnati e società sostenibili. COM(2012) 740 final. Strasburgo, 12 dicembre 2012.

⁸ In particolare, cfr. EBA (2021); BCBS (2015). Per l'Italia, cfr. Circolare Banca d'Italia (285/2013 e successivi aggiornamenti (Disposizioni di vigilanza per le banche), Parte Prima, Titolo IV, Governo societario, controlli interni e gestione dei rischi, p. 274-472.

⁹ Cfr. OECD (2015), p. 9.

¹⁰ Cfr. OECD (2017), p. 11.

¹¹ Di recente la Commissione Europea ha emanato un regolamento pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito (regolamento *DLT Pilot Regime*). I responsabili della DLT (banche, intermediari finanziari, gestori di mercato, altri operatori) dovranno rispettare i tradizionali requisiti organizzativi, di governance, di protezione degli investitori, requisiti KYC/AML. Analogamente il regolamento sul mercato delle crypto-attività (*MiCA Regulation*) stabilisce regole il cui *enforcement* passerebbe attraverso un soggetto vigilato (ad esempio il prestatore di servizi in crypto-attività (*cripto-asset service provider* - CASP)).

economici. Come sottolineato da Kennet Arrow (1974)¹², poiché la trasmissione di informazione è costosa in termini di risorse, in linea di principio è più efficiente trasmettere tutte le informazioni a un unico centro, piuttosto che distribuirla a tutti gli agenti. Arrow nota inoltre che l'alternativa più radicale all'autorità centrale è il "consenso". Egli osserva che il consenso spontaneo sarebbe efficiente in un'organizzazione i cui membri hanno interessi e informazioni identiche. Tuttavia, se le informazioni non sono facilmente e perfettamente distribuite, gli incentivi potrebbero divergere. Ad esempio, alcuni agenti potrebbero essere inclini a seguire comportamenti scorretti a scapito di altri se tali comportamenti (o il risultato degli stessi) non sono completamente osservabili; una problematica nota come *principal-agent problem*¹³. Inoltre, se i costi transazionali sono eccessivi, i contratti incompleti o la razionalità è limitata, le scelte allocative potrebbero essere inefficienti (O.D. Hart (1995); O. Williamson (1999)). A livello di singola iniziativa imprenditoriale, nel corso degli anni, anche tramite interventi normativi, sono stati introdotti dispositivi, organi e procedure atte a risolvere o a limitare tali problematiche attraverso funzioni di controllo, gestione dei rischi, esercizio dei poteri, delle responsabilità e dei conflitti di interesse, per dati flussi informativi e meccanismi di incentivo.

Al crescere della complessità o delle funzioni aumentano i costi di coordinamento sotto forma di flussi informativi all'interno della struttura o delle relazioni tra gli agenti (contrattuali o comportamentali, anche sotto forma di contratti impliciti). L'organizzazione permette di sfruttare economie di scala o di scopo; essa risponde all'esigenza di rendere efficiente il processo riducendo - per definizione - il livello di decentramento. Internalizzare i processi produttivi permette anche di ridurre i rischi di comportamenti malevoli da parte di soggetti esterni, dato che i controlli interni entro una struttura organizzativa sono più facili, e la presenza di interessi condivisi più probabile. Tuttavia, oltre a una certa soglia, il guadagno di efficienza tende a ridursi se all'interno del sistema organizzativo prevalgono meccanismi distorsivi o si possono ottenere aumenti di efficienza esternalizzando determinate funzioni o creando configurazioni di gruppo (P. Milgrom, J. Roberts, (1992)). Esistono quindi vari *trade-off* che giustificano una struttura organizzativa e d'impresa più o meno complessa (più o meno decentrata) per minimizzare i costi produttivi e transazionali che derivano da informazione imperfetta, contratti incompleti e comportamenti opportunistici.

A livello operativo si tratta di disegnare una struttura organizzativa che vincoli il processo decisionale in base a determinati criteri per individuare e preservare la soluzione migliore per l'insieme collettivo degli agenti (*stakeholders*) "in conformità con l'interesse pubblico su base sostenibile"¹⁴. Se sono possibili forme di coordinamento (ad esempio di tipo gerarchico) tra gli agenti economici (o gruppi di agenti economici), la struttura di governo prevede organi con funzioni distinte (distribuzione dei poteri, delle responsabilità, dei meccanismi di controllo)¹⁵. Da notare che la proprietà (quota di capitale o diritti di voto) non comporta necessariamente il controllo diretto dell'iniziativa (potere gestionale); ciò avviene di solito tramite un meccanismo di delega ai direttori (esecutivi e indipendenti) e richiede una quota sufficientemente elevata (ad esempio il 50% +1) dei voti o la capacità di creare delle coalizioni di voto atte a raggiungere il *quorum* richiesto per approvare determinate decisioni. Pertanto, all'interno dell'impresa, la struttura organizzativa si basa su meccanismi più o meno stringenti di fiducia reciproca, di delega, di circolarità delle informazioni. Una struttura di governo equilibrata, basata sul controllo e bilanciamento (*check and balance*) tra vari

¹² Cfr. K. Arrow (1974), pp. 49-50.

¹³ Per una rassegna della letteratura sull'argomento cfr. K. Arrow (1986). Si veda inoltre: Jensen, M. C.; Murphy, K. J. (1990).

¹⁴ Cfr. BCBS (2015), p.3.

¹⁵ I principali organi sono: un organo direttivo, preposto a valutare e proporre le scelte strategiche da adottare; un organo decisionale che si esprime attraverso un sistema di voto; un organo gestionale, preposto a realizzare nel miglior modo possibile le decisioni adottate; uno o più organi di monitoraggio e controllo indipendenti chiamati a vigilare sul rispetto delle regole di governo stabilite dallo statuto o dettate da una autorità esterna per evitare conflitti di interesse o comportamenti scorretti.

organi diventa pertanto essenziale. Essa deve tenere sotto controllo sia i processi interni, sia di quelli esternalizzati (in outsourcing o distribuiti nel network), se rilevanti.

2.2 Una definizione di corporate governance per registri distribuiti

Le tradizionali categorie della corporate governance e dei processi organizzativi si attagliano solo in parte alla problematica oggetto di questo lavoro. Il governo dei registri distribuiti presenta infatti caratteristiche del tutto inedite, simili a quelle osservabili nei sistemi di governance collettiva, come quelli “spontanei” di creazione e gestione di *software open source* (Markus, L. M. (2007))¹⁶. Alcuni autori hanno pertanto definito la governance delle blockchain nel modo seguente: “mezzo per conseguire la direzione, il controllo e il coordinamento degli *stakeholders* entro il contesto di un dato progetto di blockchain nel quale essi danno un contributo congiunto”¹⁷ (van Pelt *et al.* 2020, p. 21).

Mentre nell’attuale versione della maggior parte delle DLT vi sono processi automatizzati associati a forme di coordinamento di tipo tradizionale, alcuni progetti ambiscono a sviluppare DLT in cui i processi di governo siano totalmente automatizzati (quali ad esempio Polkadot). Occorre notare tuttavia che, a prescindere dal grado di decentramento, la governance di entrambe le tipologie di DLT richiede la presenza di organi (comitati direttivi, organi tecnici e decisionali) e strumenti (token con diritti di voto variamente configurati) non solo per pervenire a forme decisionali ordinate e rispettose dei diritti impliciti dei partecipanti, ma anche per garantire l’efficienza del sistema (scalabilità per sostenere volumi rilevanti di transazioni in tempi contenuti, sicurezza, flessibilità rispetto ai cambiamenti).

2.3 Proprietà e controllo

È opportuno segnalare che nelle tradizionali linee guida di corporate governance in ambito bancario e finanziario, (ad esempio BCBS (2015); EBA (2021); ECB (2021a, 2021b)) il tema della relazione tra proprietà e controllo (diritti di voto, rapporto tra azionisti e management, ecc.) non viene di solito considerato¹⁸. L’attenzione è posta sui meccanismi di gestione, sul ruolo e l’indipendenza degli organi, sui processi di monitoraggio e mitigazione dei rischi, ecc. Tuttavia, anche i primi aspetti sono rilevanti in una analisi dei criteri di governo di una DLT, poiché sono strettamente connessi con i meccanismi di raggiungimento del consenso distribuito. Si deve quindi porre attenzione anche al processo di creazione dei token, se incorporano particolari diritti nella gestione della DLT, e se sono possibili coalizioni di voto o forme di concentrazione¹⁹ nell’esercizio di tali diritti (cfr. Box 2 e paragrafo 3.3). Questi aspetti potrebbero configurare la forma giuridica di società di fatto, esponendo i partecipanti a diversi rischi, in primo luogo all’eventuale responsabilità nei confronti delle obbligazioni sociali. Tale responsabilità sarebbe *illimitata*, pertanto i partecipanti risponderebbero non solo nei limiti della “quota” conferita, ma anche con il proprio patrimonio personale. Su questi aspetti permane una grande incertezza ed essi richiederebbero un’analisi specifica partendo dai fondamenti giuridici e dalle soluzioni proposte dal diritto commerciale (O. Borgogno (2022)). Una ricognizione esaustiva sconfinerebbe in temi relativi alla natura giuridica di queste organizzazioni

¹⁶ Vengono definiti *open source* i software per i quali viene reso liberamente disponibile il codice sorgente originale.

¹⁷ La definizione presenta alcune affinità con quella di *Decentralized Autonomous Organizations* (DAOs), dove le funzioni manageriali e operative sono codificate *on-chain* nelle DLT sotto forma di *smart contracts*. Cfr. Hassan, S., De Filippi, P. (2021); Santana, C., Albareda, L. (2022).

¹⁸ Le regole relative agli assetti proprietari degli intermediari sono disciplinate nell’ambito delle normative nazionali dei singoli paesi membri al di fuori delle linee guida di corporate governance. In Italia la disciplina è contenuta nel TUB e nel TUF, e nei provvedimenti della Banca d’Italia che regolano l’iter autorizzativo di accesso al mercato. Ai partecipanti al capitale oltre al rispetto dei requisiti di onorabilità, correttezza, competenza professionale, è richiesto di dimostrare che il loro ingresso nel capitale non pregiudichi la capacità dell’intermediario di rispettare nel medio-lungo periodo i requisiti prudenziali e regolamentari.

¹⁹ Su questi aspetti si vedano: Schär, F., Nadler, M. (2022); Sultanik, E. *et al.*, (2022).

decentrate. Alcuni aspetti verranno nondimeno analizzati in questa sede sotto un profilo tecnologico: ruolo dei nodi, ruolo degli sviluppatori coinvolti attraverso diversi meccanismi di incentivo, ruolo di vari comitati consultivi o tecnici presenti in alcune DLT. L'intento è quello di fornire elementi utili per una futura riflessione sui profili giuridici e regolamentari di queste strutture.

Box 2 – Sui vari tipi di token

In questo lavoro usiamo il termine token per indicare una qualsiasi rappresentazione di valore (anche creata dalla DLT stessa), trasferibile tramite questa tecnologia. La maggior parte dei token sono negoziabili tramite una piattaforma di scambio. Tre sono gli aspetti da tenere in considerazione: natura economica del token e sua funzione prevalente (mezzo di scambio, riserva di valore, scommessa sul suo valore futuro); caratteristica finanziaria (liquidità, volatilità, negoziabilità); natura legale (capacità di rappresentare diritti, promesse, vincoli contrattuali). Se usiamo come trainante quest'ultima categoria, è possibile ricondurre i token a due macro-classi, a seconda che essi incorporino o meno dei diritti in capo al possessore²⁰.

La prima macro-classe include token senza diritti (reali o finanziari) incorporati, fatta eccezione del possesso del token stesso; essi non sono rappresentazioni di valore con un attivo e un passivo che si elidono per consolidamento; non attribuiscono alcun diritto in capo all'utilizzatore; non hanno spendibilità generalizzata o potere liberatorio garantito per legge, come la moneta. Questa classe di token include i c.d. *unbacked crypto assets* (senza una riserva di attività a sostegno) e i token "algoritmici" creati tramite altri token senza diritti incorporati.

La seconda macro-classe include i token che incorporano diritti. Essi sono: i) moneta elettronica "tokenizzata" (ove per "tokenizzata" si intende trasferibile tramite DLT); ii) moneta di banca centrale "tokenizzata"; iii) strumenti e prodotti finanziari "tokenizzati"; iv) *non-fungible token*, NFT: token univoci, rappresentanti diritti di proprietà su beni quali opere d'arte o essi stessi opere d'arte digitali; v) *utility token*: token volti esclusivamente a garantire il diritto di accesso a un bene o servizio fornito della DLT; alcuni utility token non sono trasferibili e quindi non sono negoziabili; vi) *governance token*, creati dal protocollo tramite *smart contract* e assegnati a coloro (ad esempio sviluppatori) che forniscono una prestazione atta a migliorare il protocollo; essi attribuiscono al possessore un diritto specifico alla gestione attuale o futura del protocollo (simile a un diritto amministrativo e/o patrimoniale). I governance token possono essere assegnati attraverso diverse modalità, anche tramite estrazione casuale, e possono attribuire diversi tipi di diritto di voto (cfr. il Box 4 e l'Appendice sui casi studio Ethereum e Polkadot).

3 Governance collettiva e algoritmica

In questo paragrafo si cerca di delineare un "ponte" tra la struttura di governo tradizionale prima descritta e una struttura organizzativa decentrata. Una buona governance (anche implicita, che scaturisce da un sistema che si organizza in modo spontaneo) dovrebbe individuare in modo chiaro il ruolo e le modalità operative di tutti i soggetti che operano nel *network*, garantire la trasparenza, regolare i meccanismi di incentivo contenendo comportamenti opportunistici o malevoli, evitare concentrazioni di potere che possano impedire una corretta dialettica interna; soprattutto dovrebbe dirimere in modo ordinato eventuali conflitti tra i partecipanti. Essa dovrebbe essere in grado di recepire le norme di legge delle giurisdizioni dove opera la DLT. Il punto fondamentale - che si cercherà di mettere in luce in seguito - è la distinzione tra funzioni di governo collettivo della DLT operate tra soggetti organizzati in *network* e il c.d. "governo algoritmico", che automatizza determinate funzioni. Il primo aspetto attiene prevalentemente all'allocazione dei poteri e delle responsabilità; il secondo riguarda l'*enforcement* dei meccanismi di governo che si realizza tramite una procedura informatica. L'intento dei sostenitori dell'approccio basato su una governance algoritmica completa sarebbe quello di pervenire a un sistema di governo interamente automatizzato; nella realtà, anche nelle forme più avanzate (come nel caso di Polkadot, qui presentato) pare difficile ottenere in modo completo questo risultato, come avviene peraltro per ogni forma contrattuale,

²⁰ Su questi aspetti e sul conseguente trattamento contabile cfr. C. Gola e A. Caponera (2019). Sul ruolo dei governance token, cfr. IOSCO (2022).

necessariamente “incompleta” rispetto ad accadimenti originariamente non previsti dalle parti (*contingent claim*).

3.1 La blockchain come sistema per costruire la fiducia reciproca

Nelle DLT *permissionless*, e in particolare in quelle basate su meccanismi di consenso “*Proof-of-Work*” (cfr. *infra*), si configura un sistema di governo sui generis che scaturisce non tanto da meccanismi di delega e di verifica del rispetto di regole tradizionali, quanto da automatismi e da meccanismi economici endogeni che conducono al raggiungimento di un consenso fra attori che non comunicano direttamente tra loro, senza necessità pregresse di una fiducia reciproca tra gli *stakeholders*.

Questo processo può essere modellato come un equilibrio dinamico (equilibrio di Nash), rappresentabile matematicamente come un processo stocastico che “domina” altri possibili comportamenti tra agenti che non comunicano tra di loro²¹. L’equilibrio trae origine dal “protocollo di consenso” che permette ai vari *stakeholders*, intesi come agenti razionali che massimizzano la propria utilità, di conseguire uno scopo comune.

In ambito informatico, la problematica del raggiungimento del consenso tra diversi attori si era posta tradizionalmente nei termini di stabilire come raggiungere uno “stato” di sincronizzazione (un “consenso”) tra un numero discreto di sistemi autonomi (detti nodi), con un certo grado di tolleranza²². Si trattava di stabilire sotto quali condizioni il sistema potesse operare correttamente pur in presenza di un certo numero di nodi aventi comportamenti anomali (non funzionanti o derivanti da comportamenti malevoli). È stato dimostrato che vi sono soglie critiche di tolleranza (ad esempio 2/3 dei nodi operanti correttamente in un dato momento) al di sopra delle quali il sistema continua a funzionare correttamente nel suo complesso²³.

Una delle novità introdotte dalla blockchain di Bitcoin, grazie al meccanismo di consenso noto come *Proof-of-Work*²⁴, è stata quella di dimostrare che è possibile pervenire – sebbene in forma probabilistica – a un risultato sostanzialmente analogo (i.e. raggiungimento del consenso su un registro condiviso) anche in un sistema aperto *peer-to-peer* senza richiedere una comunicazione esplicita tra partecipanti identificati a priori²⁵. Infatti, nelle DLT che adottano meccanismi di consenso *Proof-of-Work*, il processo di raggiungimento del consenso viene configurato come una competizione per la risoluzione di un problema crittografico ad elevato costo computazionale; ad esso corrisponde un elevato dispendio energetico e di conseguenza economico: in tal modo, comportamenti scorretti vengono disincentivati poiché risulterebbero insostenibili.

Se interpretiamo il funzionamento di questo modello di raggiungimento del consenso in termini di processo per la risoluzione dei problemi di governo prima descritti, potremmo affermare che esso “collassa” funzioni attestata su più livelli operativi (manageriali e di controllo) su un unico processo, quello di raggiungimento del consenso sullo stato del registro condiviso.

²¹ Cfr. Paul Apivat: <https://paulapivat.medium.com/economics-games-and-proof-of-work-842d820f198c>.

²² La questione è nota in letteratura come “Problema dei Generali Bizantini” e i sistemi che, sotto specifiche condizioni, esibiscono tolleranza a comportamenti anomali da parte di un sottoinsieme dei nodi, sono definiti “Byzantine Fault Tolerant” (BFT) (*infra*).

²³ Cfr. Lamport, L., *et al.* (1982).

²⁴ Tale meccanismo è noto anche come “protocollo di Nakamoto”, dallo pseudonimo con cui venne pubblicato il documento *white paper* in cui viene descritto per la prima volta Bitcoin: <https://bitcoin.org/bitcoin.pdf>.

²⁵ Si definisce *peer-to-peer* un sistema informatico distribuito in cui tutti i nodi svolgono le stesse funzioni in modo paritetico. Questo sistema si contrappone alle architetture del tipo *client-server*, in cui alcuni nodi assumono un ruolo di erogatori del servizio (i *server*) e altri quello di utilizzatori (i *client*). Quest’ultimo modello è quello più diffuso nella realizzazione delle applicazioni informatiche distribuite, mentre il primo è storicamente noto per il suo utilizzo in piattaforme per la condivisione e lo scambio di dati.

L'obiettivo di cooperazione non coordinata tra nodi che non sono preventivamente identificati viene quindi ottenuto tramite un incentivo economico assegnato ai nodi partecipanti attivamente al processo (i c.d. *miner*), che ha come esito quello di creare nuovi token assegnati ai nodi che vincono la competizione per la risoluzione del sopracitato problema crittografico. In Bitcoin, inoltre, il numero complessivo di token generabili tramite questo processo è limitato ex ante dal protocollo stesso: i token sono quindi percepiti come oggetti aventi valore di mercato, anche in ragione della loro offerta limitata. Il sistema di incentivo si basa quindi interamente sull'assunto che il token abbia un valore connesso alla sua scarsità e che continui ad averlo in futuro. La loro sorte, pertanto, è potenzialmente precaria ed è connessa esclusivamente al fatto che il token di riferimento continui ad essere ritenuto un bene meritevole di valore anche economico da un numero sufficiente di individui.

Questo sistema, basato sull'imposizione di un costo computazionale, disincentiva i comportamenti scorretti, rendendo estremamente costoso a eventuali partecipanti malevoli di moltiplicare artificiosamente il proprio ruolo nel processo di aggiornamento del registro condiviso. Infatti, in assenza di una entità centrale che verifica l'identità del partecipante al network, sarebbe possibile generare a basso costo un numero elevato di identità digitali solo apparentemente differenti, acquisendo per questa via un livello di controllo sproporzionato sulla rete. In questo modo una coalizione di nodi riconducibili ad un medesimo soggetto o gruppo di soggetti potrebbe controllare l'intero sistema (c.d. *sybil attack*). L'inserimento di un costo per la partecipazione al meccanismo di consenso riduce invece drasticamente questa possibilità. Al contrario, i protocolli di consenso *Proof-of-Work* sono disegnati in modo tale da "allineare gli incentivi" tra i nodi, nel senso che è più vantaggioso comportarsi correttamente piuttosto che tentare di compromettere l'integrità della rete.

L'equilibrio intertemporale tra i nodi risulta così raggiunto per qualsiasi valore di mercato del token, dato che i protocolli *Proof-of-Work* modificano in modo adattivo la difficoltà del problema crittografico in funzione dei tempi di soluzione dello stesso, e quindi il relativo costo computazionale per risolverlo. Un aumento del prezzo dei token determina infatti l'ingresso nel mercato di nuovi *miner*, una creazione più rapida di token e quindi (per costruzione dell'algoritmo) un aumento della complessità²⁶. Tutto ciò, come si è detto, rende molto difficile l'esecuzione di attacchi volti a tentare di modificare transazioni già effettuate o a impedire la conferma di nuove transazioni²⁷.

Box 3 – I meccanismi di incentivo

I due principali meccanismi di incentivo per i partecipanti alle DLT *permissionless* (come la blockchain di bitcoin) sono i token generati dal protocollo stesso e le commissioni (*fees*) pagate, sempre sotto forma di token, dagli utenti finali per eseguire le transazioni. L'utente può aumentare detta commissione per rendere più veloce il processo di validazione della propria transazione, creando una competizione fra utenti in funzione del prezzo che essi sono disposti a corrispondere per vederla finalizzata in tempi brevi. Quando si raggiunge il limite massimo di token previsto dal protocollo (nel caso di bitcoin, 21 milioni) il sistema verrebbe incentivato solo dalle commissioni.

Per quanto riguarda le DLT *permissioned*, caratterizzate da un insieme identificabile e limitato di nodi partecipanti attivamente al meccanismo di consenso (e.g. con ruolo di validazione delle transazioni), gli schemi di incentivo potrebbero in linea di principio essere disegnati liberamente, anche usando i tradizionali sistemi di remunerazione, in funzione dello "sforzo" profuso. In generale, i sistemi di incentivo dipendono dalla tipologia del protocollo di consenso utilizzata e dai connessi meccanismi di voto e di controllo della blockchain. Ad esempio, la creazione di token con diritti di voto (*governance token*) ha introdotto una nuova tipologia di incentivo – descritta più avanti, anche in relazione ai casi di studio presentati.

²⁶ Come osservato nel *white paper* di Bitcoin: "To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases", cfr. Nakamoto (2008), p. 3.

²⁷ Diverso è invece il problema di conseguire tale risultato tramite coalizioni (*mining pools*) che coordinano un numero elevato di nodi e sono create per sfruttare le economie di scala in presenza di elevati costi di entrata (processori sempre più costosi per risolvere in tempi ragionevoli il puzzle crittografico).

3.2 I protocolli di consenso e i diritti di voto

Si è visto in precedenza che la creazione di un token attraverso il protocollo basato sulla *Proof-of-Work* è un elemento fondamentale non solo per remunerare l'attività dei *miners*, ma anche per "allineare gli incentivi" e creare fiducia reciproca. Tuttavia, non tutte le DLT operano con meccanismi di consenso di tipo *Proof-of-Work*: esistono altre tipologie di algoritmi, adottate per ragioni di efficienza e di riduzione dell'impatto ambientale²⁸.

Nel seguito descriviamo brevemente tre classi di protocolli di consenso alternativi, essendo aspetti che hanno implicazioni anche sul governo della DLT: *Proof-of-Stake* (PoS), *Pure Proof-of-Stake* (PPoS), e *Proof-of-Authority*²⁹.

Proof-of-stake (PoS) – Gli algoritmi di consenso che ricadono in questa categoria si basano sul presupposto che, per poter aggiornare il registro, i nodi devono poter dimostrare di possedere un certo "interesse in gioco" (*skin-in-the-game*). Questo interesse, o *stake*, è solitamente costituito dal possesso di una certa quantità di token che vengono immobilizzati nel protocollo, come una sorta di deposito cauzionale. Da un lato, lo *stake* costituisce il presupposto per poter essere candidabili a svolgere il ruolo di validatori, ovvero di creatori di nuovi blocchi della blockchain (con modalità che variano da algoritmo ad algoritmo); dall'altro, esso costituisce il "capitale di rischio" che incentiva il nodo-validatore a comportarsi correttamente (ad esempio evitando che uno stesso token venga speso due volte (*double spending*)), e a farsi parte attiva nella gestione della DLT (ad esempio per evitare disconnessioni dalla rete o blocchi del servizio). Se il nodo si comporta in modo non conforme a quanto stabilito dal protocollo viene penalizzato con la perdita di parte del proprio deposito. Pertanto, se nei meccanismi PoW la garanzia di comportamento corretto deriva dalla dimostrazione di aver compiuto del lavoro, nel caso dei meccanismi PoS tale garanzia deriva ad un meccanismo di collateralizzazione.

Pure proof-of-stake (PPoS) – Si tratta di una variante dei meccanismi PoS, adottata dalla blockchain Algorand³⁰, che presenta interessanti caratteristiche addizionali, ad esempio in termini di garanzia di finalità delle transazioni (è sostanzialmente, sebbene non formalmente³¹, *forkless*) e che, secondo quanto asserito dai promotori del progetto, è in grado di risolvere il cosiddetto "trilemma" delle blockchain³². A questo algoritmo di consenso possono partecipare potenzialmente tutti gli utenti della blockchain, senza creare distinzioni per ruolo dei nodi. L'influenza esercitata da ogni nodo nella scelta del nuovo blocco della catena è proporzionale al numero di token posseduti (*stake*). Tra tutti i nodi, per ogni singolo blocco di transazioni da validare, vengono scelti in modo casuale e segreto il nodo con il ruolo di proponente di un nuovo blocco (nodo *leader*) e i nodi con diritti di voto sulla proposta fatta (nodi afferenti al *committee*). Tutti i nodi *online* della blockchain hanno la possibilità

²⁸ Su questi aspetti si rimanda a: C. Gola e J. Sedlmeir (2022); M. Javarone, *et al.* (2022).

²⁹ Per la descrizione di altri protocolli di consenso, e relative implicazioni di policy, cfr. Bains, P. (2022)

³⁰ Cfr. Chen, J., Micali, S. (2019).

³¹ La probabilità di *fork* è pari a 10^{-18} ovvero, sostanzialmente nulla. In tal caso, sebbene formalmente il meccanismo di consenso sia probabilistico, nella sostanza e a tutti gli effetti pratici può essere considerato di tipo deterministico.

³² Il c.d. "trilemma" asserisce che è impossibile per una *blockchain* conseguire contemporaneamente tre obiettivi: sicurezza, scalabilità e decentralizzazione; il termine è stato introdotto da V. Buterin, uno dei creatori della *blockchain* Ethereum. Ad esempio, gli algoritmi PoW soffrono di solito di problemi di scalabilità *on chain*. Al converso, *blockchain* basate su algoritmi di consenso PoS tradizionali, che scalano meglio degli algoritmi PoW, soffrono di problematiche di sicurezza (attacchi "*nothing at stake*" e "*long range*", che si sostanziano in tentativi di riscrittura dell'intera *blockchain* o di parte di essa); questi problemi sono mitigati attraverso complessi meccanismi di "punizione" degli utenti scorretti. Infine, tecnologie DLT descritte come "*Enterprise*", di solito di tipo *permissioned*, garantiscono il raggiungimento degli obiettivi di sicurezza e, entro certi limiti, di scalabilità, ma lo fanno a scapito della decentralizzazione. Infatti, è comune in queste tecnologie l'introduzione di nodi con ruoli speciali di coordinamento/validazione e che di fatto costituiscono delle "*trusted third parties*".

di essere scelti per assumere i ruoli di leader e di *committee*, tuttavia la probabilità di essere scelti e il peso del proprio voto sono direttamente proporzionali allo *stake* di ciascuno. Il sistema rimane sicuro purché la maggioranza dei token restino in mano a utenti “onesti”, che giocano secondo le regole stabilite dalla blockchain.

Proof-of-Authority (PoA) – Gli algoritmi che ricadono in questa categoria presuppongono l’esistenza di nodi speciali che assumono un ruolo di coordinamento (e.g. assumono il ruolo di “notai”), svolgendo di fatto il ruolo di *trusted third parties*. Questi nodi validano le transazioni inserite grazie a meccanismi di firma crittografica. Questa categoria di algoritmi presenta due importanti caratteristiche: (a) il consenso raggiunto tra i nodi è di tipo “deterministico”, anche in termini formali, e non “probabilistico” – una volta raggiunto il consenso su un nodo/transazione, esso è “finale” e non è necessario attendere che siano consolidati ulteriori blocchi per poterla considerare non più modificabile; (b) il consenso si basa su risultati classici della teoria dei sistemi distribuiti e offre parziali garanzie di tolleranza a guasti di tipo Bizantino (Byzantine Fault Tolerance - BFT)³³. Gli algoritmi di tipo PoA sono di fatto utilizzabili solo in modalità ristretta (*permissioned*), poiché la possibilità di identificare tali nodi diventa un prerequisito essenziale. Inoltre, a differenza di algoritmi come il PoS e il PoW, i sistemi basati sulla PoA presentano problemi di scalabilità al crescere del numero di nodi validatori (questo poiché, in generale, il numero di messaggi che i nodi validatori devono scambiarsi per poter raggiungere il consenso cresce con il numero dei validatori).

Box 4 – Sui diritti di voto e i meccanismi partecipativi

Vi sono vari meccanismi di assegnazione dei token ai nodi che partecipano alla gestione della blockchain, anche in funzione delle attività svolte. I meccanismi di voto possono servire sia per il funzionamento ordinario della DLT (e.g. validazione delle transazioni e aggiornamento del registro condiviso), sia per svolgere attività “straordinarie” (e.g. cambiamento dei parametri tecnici del protocollo nativo o addirittura del sistema di consenso). Per tale secondo specifico fine, sono stati introdotti in alcune DLT particolari tipologie di token (c.d. *governance token* o *voting right token*).

La logica sottostante ad alcuni sistemi di voto delle DLT è quella di limitare la concentrazione, non solo nella fase di lancio del progetto ma anche nel tempo, e di rafforzare gli incentivi - sia tramite una ricompensa, sia attraverso un meccanismo partecipativo (*skin-in-the-game*). Ciò viene fatto attraverso vari espedienti, ad esempio l’assegnazione casuale dei diritti di voto (randomizzazione)³⁴. Infatti, una eccessiva concentrazione di diritti di voto³⁵ non solo ha evidenti implicazioni di governance, ma ha anche un effetto negativo sulla sicurezza del sistema. Un altro problema rilevato è la presenza di un elevato numero di possessori di diritti di voto che non votano nelle decisioni da prendere per gestire cambiamenti del protocollo. Essi sono l’equivalente degli azionisti “assenteisti” o passivi nelle società di capitale. Sono stati sviluppati meccanismi di delega temporanei assegnati tramite processi casuali. È altresì necessario mantenere nel tempo il coinvolgimento del soggetto che partecipa al sistema. Ciò avviene tramite depositi cauzionali, premi sotto forma di token, che agiscono come incentivo a fornire contributi intellettuali o economici, “premi fedeltà” e penali a fronte di comportamenti scorretti.

Si elencano alcuni possibili approcci ai sistemi di voto:

- “Una CPU un voto”: il potere decisionale è connesso al possesso di hardware con elevata potenza computazionale; su questo principio si basa l’algoritmo di PoW (*mining*);
- “Un token un voto”: è il caso ad esempio della PoS, dove il potere decisionale è connesso al numero di token posseduti e posti in deposito. In alcuni sistemi il voto può essere ripetuto (*multy-round voting*) o “a tempo” (*coin aging*);
- “Una testa un voto”: tutti i partecipanti hanno il diritto di voto (possibile solo nelle *permissioned*);
- “Lotteria pura”: il diritto di voto è distribuito in modo casuale a un numero definito di partecipanti senza vincoli;

³³ I sistemi informatici distribuiti *Crash Fault Tolerant* (CFT) sono in grado di continuare a funzionare anche se parte dei nodi che li compongono cessa di rispondere, a causa di un guasto o di problemi di rete. I sistemi *Byzantine Fault Tolerant* (BFT), oltre ad essere CFT, possono continuare a funzionare correttamente anche se un sottoinsieme dei nodi si comporta in modo scorretto (il che può verificarsi sia per un malfunzionamento, sia in conseguenza di un attacco informatico, sia per ricerca deliberata di un proprio interesse da parte di un nodo a discapito degli altri). Nel caso delle *blockchains*/DLT la CFT normalmente non è considerata sufficiente e si ricorre a meccanismi di consenso BFT.

³⁴ È stato osservato che l’uso della assegnazione casuale dei diritti di voto trova una interessante analogia in alcune soluzioni adottate nella teoria delle scelte sociali per aggregare le preferenze, di recente rivitalizzate dalla *computational social choice*, cfr. D. Grossi (2022).

³⁵ Per alcuni dati sulla concentrazione del possesso di *governance token*, cfr. FSB (2023), tabella 1, p. 13.

- “**Lotteria solo per i nodi attivi**”: come la lotteria pura ma il diritto può essere conferito solo a chi partecipa in modo attivo alla gestione della DLT (es. sviluppatori);
- “**Lotteria con delega**”: il diritto di voto è conferito in modo casuale ai partecipanti, i quali possono a loro volta delegare un numero limitato di altri nodi con particolari competenze. Nel tempo, il delegato guadagna una reputazione.

3.3 Governance *off-chain* e *on-chain* (algoritmica)

In questo paragrafo mostreremo come alcune regole della DLT sono incorporate nel codice nativo (*on-chain*) e, per questa via, limitano i problemi delle asimmetrie informative (*principal-agent problem*) attraverso sistemi automatizzati, mentre altre funzioni o processi si realizzano al di fuori del protocollo nativo (*off-chain*) e talvolta si affidano a tradizionali presidi di corporate governance, come comitati tecnici o organi di coordinamento tra i partecipanti.

Il quadro d’insieme è ulteriormente complicato dall’esistenza di approcci multilivello, in cui in alcune DLT (blockchain di secondo livello o “*Layer 2*”, *sidechains*) è possibile una “esternalizzazione” di alcuni processi, essi stessi automatizzati, ma spesso basati su sistemi di governo/consenso differenti³⁶. Approfondiremo brevemente questi aspetti, limitando la nostra analisi alle DLT *permissionless*, poiché quelle *permissioned* sono governabili tramite i tradizionali sistemi societari di gestione e controllo³⁷.

La maggior parte delle DLT *permissionless*, come Bitcoin o Ethereum, non prevedono ex ante dei processi codificati per consentire un loro aggiornamento (upgrading). Pertanto, quando emerge l’esigenza di migliorarne la sicurezza o l’efficienza, devono affrontare un processo decisionale che, in assenza di un sistema di governo strutturato, può essere lungo e complesso. Questo processo, non essendo predisposto dal protocollo nativo, è realizzato *off-chain*³⁸(cfr. Box 5). Se si raggiunge un accordo, e quindi la maggioranza dei nodi aggiorna il proprio software alla nuova versione proposta del protocollo, l’aggiornamento diviene *de facto* la nuova versione del protocollo nativo. Se una parte della comunità non concorda con la proposta e di conseguenza decide di non aggiornare la versione del software utilizzato come *client*, si determina uno sdoppiamento (*hard fork*) del protocollo (cfr. Box 5) e del registro condiviso, che da quel momento in poi seguirà evoluzioni distinte per ciascuno dei “rami” creatisi con la biforcazione³⁹. Se invece la modifica introdotta è retro-compatibile, si parla di *soft fork*: in tal caso i nodi che non aggiornano il protocollo possono continuare a partecipare alla rete, anche se potrebbero non avere accesso alle nuove funzionalità introdotte dall’aggiornamento⁴⁰.

Box 5 – Processi *on-chain*, *off-chain* e misti

Processi di governance *on-chain* – Sono definiti come quei processi di governo scritti nel protocollo nativo della DLT. Questi processi, che si potrebbero definire di *governance algoritmica completa*, possono modificare le regole del protocollo nativo, secondo forme e modi prestabiliti. In questo ambito potrebbero, ad esempio, essere decise, e

³⁶ Si tratta di funzionalità che possono essere anche diverse da quelle gestite nel protocollo base, come ad esempio *layers* che gestiscono *smart contracts* per svolgere attività di scambio dei token, di prestito di cripto-attività, o altro. Di fatto questi sistemi esternalizzano la validazione delle transazioni, eseguendole sul livello 2 e registrandole sul livello 1. Semplificando, si può dire che le funzioni di livello 2 “ereditano” caratteristiche di sicurezza del livello 1 sottostante. Per una descrizione di queste ulteriori articolazioni o “strati” (*layers*) delle DLT cfr. Schär, F. (2021) e IOSCO (2022).

³⁷ Negli ultimi anni sono stati prodotti numerosi contributi sulla governance delle DLT. Si vedano, ad esempio: Accenture (2019); Allen, D. W. E., Berg, C. (2020); ASTRI (2016), Hofman, D., *et al.* (2021); Liu, Y., *et al.* (2022); Naudts, E., *et al.* (2022); van Pelt, R. *et al.* (2020); Wang S. *et al.* (2019).

³⁸ Cfr. Ehram, F. (2017).

³⁹ Costituiscono esempi di “*hard fork*” quelli verificatisi in ambito Bitcoin con la creazione della blockchain “Bitcoin Cash”, oppure in ambito Ethereum con la creazione delle blockchain “Ethereum Classic” e, più recentemente, “Ethereum PoW”.

⁴⁰ Costituiscono esempi di *soft fork* gli *upgrade* al protocollo Bitcoin noti come “*SegWit*” e “*Taproot*”, che pur introducendo novità nel protocollo - ad esempio in termini di caratteristiche di scalabilità o tecnologie crittografiche di firma - non hanno prodotto con la loro introduzione una biforcazione del registro condiviso.

direttamente iscritte nel protocollo, regole relative ai meccanismi di voto, alle dimensioni dei blocchi o delle transazioni, alle modalità di interfaccia (API/RPC). Il processo decisionale è predefinito nei modi e nei tempi operativi direttamente nel codice sorgente del protocollo. È possibile introdurre diversi meccanismi che guidano il processo o che aggregano le preferenze dei partecipanti al network, nonché vincoli non modificabili di natura tecnica (ad esempio il linguaggio del codice base) o politica (come le norme sostanziali non modificabili di uno statuto). Vi possono essere organi consultivi, comitati, gruppi di aggregazione spontanei, ma le decisioni finali avvengono tramite referendum aperto ai partecipanti al network, secondo modalità predefinite e non alterabili, stabilite dalla blockchain. È opportuno osservare che, sulla base delle nostre conoscenze, ancora non è stata sviluppata una DLT con una governance interamente *on-chain*. Vi sono tuttavia progetti in fase avanzata di sviluppo che si stanno muovendo per eliminare qualsiasi fase *off-chain*, cercando di sviluppare una governance algoritmica completa.

Processi di governance *off-chain* e misti – Questi processi non sono scritti direttamente nel protocollo nativo della DLT, ma prevedono che le funzioni organizzative o decisionali siano svolte all'esterno. Come nel caso precedente vi possono essere organi o comitati tecnici ma le decisioni avvengono *off-chain*, attraverso una tradizionale struttura organizzativa. Conoscere questi processi decisionali, l'allocazione dei poteri e delle responsabilità, eventuali meccanismi di delega, ecc. è fondamentale per valutare la governance di una DLT. È infatti a livello *off-chain*, che si possono annidare opacità, fragilità, distorsioni (come una eccessiva concentrazione dei poteri), dato che questa modalità operativa non garantisce i livelli di trasparenza dei processi *on-chain*, interamente automatizzati. Si tratta naturalmente di una "trasparenza" che dipende dalla capacità tecnica e materiale di verificare e comprendere tali contenuti pubblicamente accessibili. I processi *off-chain*, se chiaramente definiti e strutturati, hanno il vantaggio di potersi avvalere dei tradizionali presidi di corporate governance, tra cui l'attribuzione delle responsabilità e l'*accountability*. Nella realtà, allo stato attuale, la maggior parte delle DLT ha una configurazione mista, con alcuni processi interamente automatizzati nella blockchain e altri che avvengono al di fuori di essa, attraverso forme di coordinamento tra i partecipanti al network più o meno formalizzate. Dei due casi studio descritti in Appendice, Ethereum ha una forte componente *off-chain*, mentre Polkadot opera prevalentemente *on-chain*⁴¹.

Le procedure *off-chain* comportano vari meccanismi decisionali e di coordinamento, sia formali (attraverso strutture decisionali e di controllo predisposte dai fondatori dell'iniziativa), sia informali (ad esempio tramite *blog*, *social network*, o altri *fora* costituiti tra i partecipanti al network)⁴². Questi processi decisionali possono essere lunghi e dare luogo a risultati non ottimali; spesso sono aperti alla comunità, ma le decisioni finali possono essere prese in modo opaco o verticistico. La minaccia di una biforcazione (*hard-fork*) stabilisce una certa disciplina che spinge i membri del network a trovare una soluzione meno traumatica. Infatti, quando questi eventi si verificano, si creano incertezza *ex ante* e costi transazionali e di adattamento *ex post*.

Dal punto di vista della corporate governance le implicazioni delle diverse tipologie di aggiornamenti sono evidenti. Nei casi in cui le modifiche da apportare abbiano impatti di modesta entità, traducendosi in un *soft fork*, è più facile che un consenso possa essere trovato tra gli utenti. Al contrario, in caso di cambiamenti radicali, con un potenziale forte impatto economico che comporta la perdita di valore del "capitale installato" (ad es. dispositivi hardware utilizzati per partecipare alla DLT) oppure che richiede nuovi investimenti, raggiungere un consenso sull'aggiornamento può essere problematico. Il problema risulta ancora più rilevante in caso di modifiche conseguenti all'individuazione di vulnerabilità di carattere informatico, che richiederebbero invece tempi di intervento rapidi.

Per superare i limiti dei sistemi di governance sopra descritti è possibile individuare due strade: a) la comunità potrebbe organizzarsi con funzioni di governo più strutturate ed equilibrate, rispettando i tradizionali criteri di separatezza dei ruoli per evitare conflitti di interesse, azzardo morale, concentrazione dei poteri; b) espandere ulteriormente il campo della governance algoritmica *on-chain*, inserendo nel protocollo ulteriori automatismi decisionali che stabiliscano un sistema di

⁴¹ Per una posizione a favore dell'approccio misto con una forte componente *off-chain* si vedano i *post* del fondatore di Ethereum, V. Buterin (2017, 2021).

⁴² Ad esempio per il BIP per Bitcoin o il EIP per Ethereum (https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals e <https://ethereum.org/en/eips/>).

autogoverno, incluse regole “endogene” che consentano di modificare il protocollo nativo (c.d. *upgradable* blockchain – cfr. M. Ciampi, *et al.* 2020).

Alcune DLT stanno seguendo questa seconda strada (e.g. Polkadot, Tezos, Internet Computer (ICP)), anche se per ora sono ancora in una forma ibrida tra i due modelli. Il dibattito è peraltro aperto e vede da un lato i sostenitori di un modello interamente *on-chain*, basato unicamente su una governance algoritmica che include la capacità di effettuare l’upgrading della blockchain; dall’altro, permangono dubbi su questa scelta da parte di coloro che sottolineano l’emergere di numerose complessità e trade-off non risolvibili in modo soddisfacente⁴³.

Le strutture di governance pienamente *on-chain* di solito seguono un processo decisionale prestabilito secondo un percorso sequenziale inscritto nell’algoritmo. Ad esempio: i) sottomissione delle proposte di cambiamento; ii) accettazione provvisoria delle stesse; iii) creazione di una blockchain parallela per testare le proposte; iv) inserimento delle proposte una volta superata la fase di sperimentazione; v) assegnazione di premi (sotto forma di token) al soggetto (o i soggetti) che partecipano al sistema. Onde evitare concentrazione dei poteri, il sistema di solito prevede limiti a quest’ultimo passaggio. Lo stesso percorso viene svolto anche nelle DLT che operano *off-chain*, ma con una differenza fondamentale: se la governance è interamente algoritmica tutto il processo avviene direttamente *on-chain* in modo predefinito, trasparente e vincolante *ex ante* (e, in quanto tale, facilmente accessibile a un *auditor* esterno). Come tutte le regole “costituzionali”, esse dovrebbero non solo indicare attraverso quali procedure e meccanismi di voto sia possibile modificare il protocollo nativo, ma anche porre vincoli a tali cambiamenti per non snaturare lo stesso. Ad esempio, una DLT potrebbe prevedere regole di governance tali da consentire il passaggio da un protocollo basato sulla *Proof-of-Work* ad uno basato sulla *Proof-of-Stake*, ma garantendo al contempo il rispetto di requisiti di partecipazione stabiliti *ex ante*.

4 Quando è necessario l’intervento del regolatore

In linea generale il regolatore dovrebbe rispettare il principio della *neutralità tecnologica* per non interferire negli autonomi sviluppi del mercato (OCSE 2022). Sappiamo tuttavia che l’azione del regolatore è giustificata dalla necessità di favorire una allocazione efficiente delle risorse specie nei casi in cui il mercato non sia in grado di raggiungere questa condizione in modo spontaneo, attraverso la libera concorrenza tra agenti economici. La situazione di efficienza è rispettata se non vi sono “fallimenti di mercato”⁴⁴. Questi si possono manifestare sia nelle DLT *permissioned* - di fatto inquadrabili nei sistemi di governo tradizionali - sia in quelle *permissionless*, anch’esse non scevre da problemi di corporate governance, ad esempio a causa della concentrazione dei diritti di voto. L’intervento del regolatore dovrebbe essere calibrato in funzione dei rischi potenzialmente non mitigati dalle dinamiche spontanee del mercato. Le regole dovrebbero essere applicate secondo modalità non tradizionali, nella consapevolezza che permangono intrinseche difficoltà nel fare ciò in

⁴³ Cfr.: Buterin (2017, 2021).

⁴⁴ Questi possono derivare da: i) *asimmetrie informative* (che possono favorire situazioni di azzardo morale o di comportamenti opportunistici o scorretti, ad esempio di alcuni soggetti (gli “agenti”) nei confronti del promotore dell’iniziativa (il “principale”); ii) *sfruttamento di posizioni dominanti*, anche attraverso eccessiva concentrazione, barriere all’entrata, scarsa interoperabilità o altri aspetti che limitano la contendibilità del mercato, come ad esempio – nel nostro contesto - la presenza di pochi *mining pools*; iii) *creazione di esternalità negative* (sotto forma di contagio finanziario, di impatto ambientale negativo, di lesione di alcuni diritti). Vanno inoltre considerati *profili non riconducibili al principio di efficienza allocativa e produttiva*, come, ad esempio la tutela della privacy, l’inclusività o la necessità di tutelare le persone e la società nel suo complesso da rischi “inaccettabili” dal punto di vista etico (aspetto considerato, ad esempio, nella proposta di regolamento europeo sull’intelligenza artificiale (Artificial Intelligence Act)).

un ambito decentrato. Vediamo dunque questi aspetti, incluso il ruolo della trasparenza attraverso il documento illustrativo (*white paper*) che accompagna ogni progetto DLT. Questo aspetto è importante, specie in un contesto nel quale è necessario informare il mercato delle caratteristiche e delle criticità di questa tecnologia.

4.1 La trasparenza e il ruolo del *white paper*

L'analisi degli standard che dovrebbero essere rispettati per una buona gestione della DLT non rientra tra gli scopi di questo lavoro. Ci limitiamo a richiamare i profili che il promotore dell'iniziativa dovrebbe illustrare nel *white paper* (WP) in fase di lancio del progetto⁴⁵.

Il WP dovrebbe in primo luogo descrivere le finalità della DLT, la strategia di fondo, la sua sostenibilità economica e, in modo non tecnico, gli aspetti principali del “protocollo di consenso” da cui dipendono la creazione dei token, il ruolo dei nodi, i meccanismi di incentivo, il sistema di voto.

Più in dettaglio, il WP dovrebbe indicare se la DLT è di tipo *permissionless* o *permissioned*, pubblica o privata; se intende seguire un approccio tendenzialmente paritetico (egualitario) o “capitalistico”, dove i soggetti che detengono un maggiore numero di token hanno la possibilità di decidere sulle scelte strategiche della DLT. Il WP dovrebbe indicare se gli stakeholders possono operare in modo collettivo o individuale (tramite organi, comitati, coalizioni, sia *on-chain* che *off-chain*). Se la DLT “crea” dei token, il WP dovrebbe distinguere se essi contengono dei diritti, ad esempio diritti di accesso alla “gestione straordinaria” della blockchain (variazioni dei parametri del protocollo nativo o del suo funzionamento), oppure solo a diritti di gestione “ordinaria” (validazione delle transazioni, aggiornamenti retro-compatibili); dovrebbe chiarire come i token sono assegnati ai partecipanti, ad esempio in modo casuale, in funzione del potere di calcolo (CPU) impiegato, in funzione di un *commitment* (deposito cauzionale) o di un contributo attivo nella scrittura del protocollo informatico. Se la DLT prefigura una società di fatto tra un numero identificabile di partecipanti, essa dovrebbe chiarire la natura sociale e la giurisdizione di appartenenza, per dare certezza giuridica all'iniziativa e tutelare gli stakeholders. In questo caso, come indicato dai principi OCSE (2015, 2017), devono essere analiticamente affrontati i tre aspetti fondamentali della corporate governance: struttura e concentrazione della proprietà e controllo; strumenti di controllo; esercizio del controllo.

Circa gli aspetti tecnici, il WP potrebbe tenere conto dei criteri di governance per le DLT di recente messi a punto dall'Organizzazione internazionale per la standardizzazione (ISO)⁴⁶. Questi dovrebbero essere integrati adattando le linee guida del Comitato di Basilea in materia di governance delle Banche (BCBS 2015). In particolare dovrebbero essere coperti in modo analitico i seguenti aspetti⁴⁷:

- 1) Protocollo di consenso utilizzato e implicazioni di governance: ISO P3;
- 2) Stakeholders (*nodes*; *full nodes*): identificazione, concentrazione: OCSE-1; ISO-P1; BCBS-2 e 3;
- 3) Upgrading del protocollo nativo (*on-chain* e *off-chain*) e la risoluzione dei conflitti (senza *hard forking*);
- 4) Tipi di token generati e scambiati (con o senza diritti amministrativi o patrimoniali incorporati);
- 5) Esercizio del controllo tramite partecipazione a organi ed esercizio del voto sia *on-chain* sia *off-chain*;
- 6) Gestione della DLT, sia *on-chain* sia *off-chain*: ISO P2; BCBS-4 e 5;
- 7) Trasparenza e grado di apertura (DLT pubbliche e private): ISO-P4; BCBS-12;
- 8) Meccanismi di incentivo (assegnazione dei token, commissioni (*fees*), penali): ISO-P5; BCBS 10;
- 9) Gestione dei rischi, privacy e integrità della DLT: ISO P7 e P8; BCBS- 6, 7, 8;
- 10) Funzioni di *compliance* e di *auditing* (espliciti o tramite disciplina di mercato): BCBS- 9, 10, 13.

⁴⁵ Si fa qui riferimento al documento che di solito associa il lancio di una DLT, come il ben noto WP di Nakamoto (2008).

⁴⁶ Cfr. ISO (2022).

⁴⁷ A latere di ciascun aspetto da considerare si indica il numero del principio utilizzabile.

4.2 Requisiti di governance in funzione delle attività svolte

Una componente fondamentale di una buona governance riguarda l'individuazione, il monitoraggio e la gestione dei rischi. Ciò dipende dal suo utilizzo. Occorre infatti osservare che la DLT può essere usata per un'ampia varietà di funzioni. In ambito bancario e finanziario, dalla gestione di un archivio condiviso, alla creazione e distribuzione di un token *unbacked* (senza diritti incorporati), al trasferimento di asset digitali tradizionali, sino a un vero e proprio sistema di pagamento. A ciascuna di queste funzioni corrisponde un diverso insieme di eventi rischiosi e di impatti negativi sul sistema. È quindi necessario stabilire una relazione funzionale (un *mapping*) tra attività svolte tramite una DLT, i rischi che essa può generare e i relativi impatti. Proponiamo qui uno schema logico, facilmente sviluppabile adottando i consueti strumenti di monitoraggio e gestione del rischio.

Tabella 1- Attività sorrette dalla DLT e relativi rischi: uno schema logico⁴⁸

A1	Creazione di un registro condiviso (ad esempio per finalità di vigilanza)	R1
A2	Creazione di un token senza diritti incorporati (tipo bitcoin)	R2
A3	Creazione di un token con diritti incorporati (es NFT)	R3
A4	Attività di scambio e custodia di cripto-attività	R4
A5	Gestione di uno schema operativo per lo scambio e il regolamento di uno strumento finanziario	R5
A6	Attività di trasferimento di moneta elettronica "tokenizzata"	R6
A7	Attività di intermediazione basata su strumenti "tokenizzati" (collaterale, prestiti, derivati, ecc.)	R7
An	Altre attività	Rn

Attraverso questo *mapping* il regolatore potrebbe imporre regole via via più stringenti in funzione dell'impatto di tali rischi. I requisiti richiesti potrebbero riguardare semplici vincoli di robustezza informatica, rispetto dei criteri di privacy, rispetto delle norme antiriciclaggio e contrasto al finanziamento del terrorismo (AML/CFT), sino a regole più pervasive, ad esempio per protocolli DLT che sorreggono uno *stablecoin* con funzioni monetarie. La tabella 1 mostra un *mapping* tra date attività A1, A2, ...An, e i corrispondenti rischi R1, R2, ...Rn che sarebbero generati dal malfunzionamento della DLT. Non rientra nello scopo di questo lavoro l'analisi dei processi volti a individuare e monitorare e mitigare i rischi delle DLT. Il nostro obiettivo è mostrare come questi processi possano essere incardinati in una opportuna struttura di governance.

4.3 Sul problema dell'*entry point*

Una volta individuati i requisiti di governance che una DLT dovrebbe rispettare, il quesito da porsi è il seguente: come è possibile per il regolatore far applicare questi requisiti a una struttura decentrata o parzialmente decentrata come una DLT? Mentre nelle DLT *permissioned* è possibile porre in essere una interazione tra un sottoinsieme di soggetti (persone fisiche o giuridiche) e il regolatore, tale interazione non è possibile nelle consuete modalità se si è di fronte a un insieme indefinito e anonimo o pseudo-anonimo di agenti (nodi) che "governano" in modo collettivo la blockchain, come avviene nelle DLT *permissionless*. In questi casi la letteratura sull'argomento sembra fare affidamento a forme di *enforcement* indirette⁴⁹. Quest'ultime si sostanziano in un processo iterativo tra l'oggetto osservabile (la blockchain) e il soggetto (o i soggetti) che devono valutare se la DLT è rispettosa di

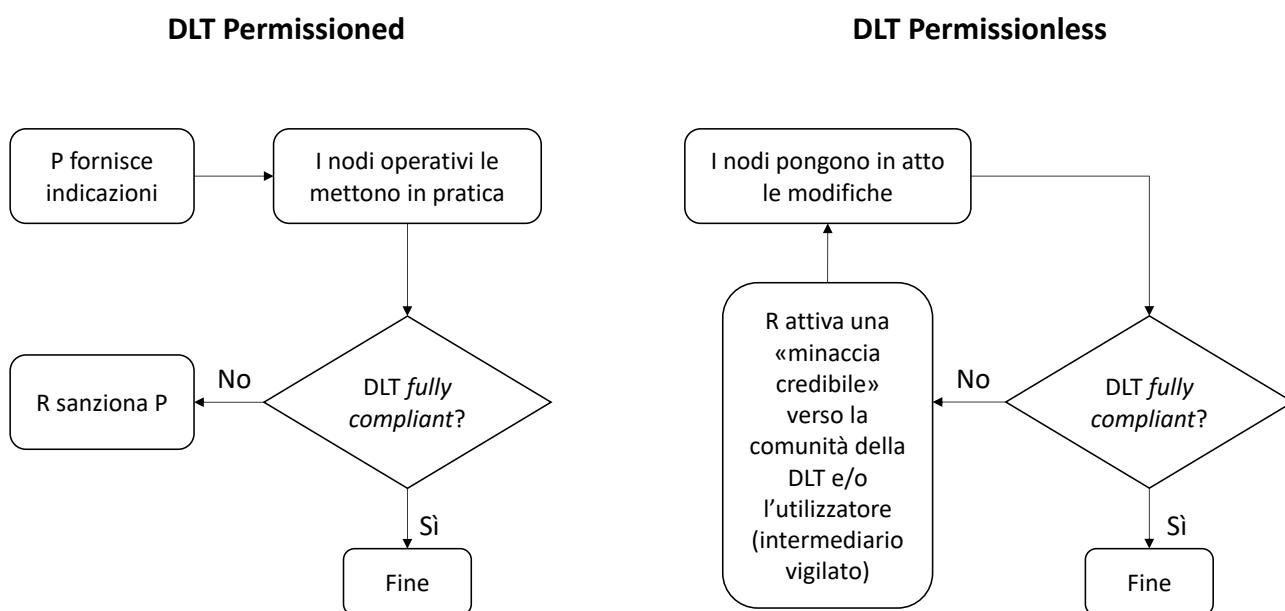
⁴⁸ Per un elenco dei casi d'uso e una loro frequenza cfr.: Deloitte (2021), p. 18.

⁴⁹ Si vedano, ad esempio, Y. Liu *et al.* (2022); ISO (2022).

determinati principi o regole. Nel seguire questo approccio si potrebbe fare riferimento al *functional equivalence principle* (OCSE, 2017), che mira a valutare il risultato finale di un processo di governance, ove la sostanza prevale sulla forma. Vediamo più in dettaglio questi aspetti.

DLT permissioned - La Figura 1 rappresenta in modo stilizzato le due situazioni: nell’approccio tradizionale (applicabile alle DLT *permissioned*) il promotore dell’iniziativa (che chiamiamo **P** e che potrebbe essere rappresentato anche da un gruppo di soci di un consorzio) fornisce una serie di indicazioni di natura strategica a un insieme di agenti (o nodi operativi) che, secondo modalità più o meno gerarchiche, assolvono a determinate funzioni (ad esempio fanno proposte per migliorare la sicurezza del sistema) e sono responsabili dell’iniziativa. Tali funzioni o processi, una volta incorporati nella DLT, sono osservabili dal regolatore, da un auditor di un organismo di autoregolamentazione del mercato o dall’utilizzatore della DLT (ad esempio un responsabile della banca delegato al monitoraggio). Chiamiamo questi soggetti **R**. Se la DLT non rispetta determinate regole o principi, R può agire su P se non è *fully compliant*.

Figura 1- L'enforcement di regole di governo



Le regole di governance da rispettare dovrebbero essere calibrate in base al *mapping* prima descritto basato sul tipo di attività svolta. In caso di mancato rispetto dei principi di governo richiesti per una DLT usata per una determinata attività (ad esempio per trasferire obbligazioni “tokenizzate”), R può agire attraverso una “sorveglianza diretta” sulla DLT che in tal modo verrebbe assimilata a un’infrastruttura informatica di mercato (come avviene in altri ambiti, ad esempio quello dei sistemi di pagamento). R potrebbe stabilire che una certa infrastruttura non può essere usata per svolgere determinate funzioni.

DLT permissionless - Passiamo ora a descrivere le modalità di attuazione di una buona governance per una DLT *permissionless*. In questo caso, in assenza di un soggetto chiaramente identificabile, l’unica via che sembrerebbe percorribile è quella di un’azione indiretta, volta a far conseguire alla DLT uno “stato” coerente con i criteri ritenuti soddisfacenti da R. In questo caso R potrà agire sugli utilizzatori della DLT scoraggiandone l’utilizzo se quest’ultima non rispetta determinati criteri.

Il miglioramento, solo progressivo e tendenziale, verso caratteristiche accettabili per il regolatore avverrebbe attraverso il processo illustrato a destra nella Figura 1. Si tratta di un approccio coerente con il modo di operare tipico dei sistemi *open source* e di molte DLT *permissionless* (si veda in Appendice il caso Ethereum). Peraltro, questo processo non pare distante da ciò che nel diritto viene definita “regolazione partecipata” (sebbene questa in un contesto tradizionale avvenga in modo strutturato, tramite procedure di consultazione). L’azione collettiva degli agenti partecipanti al network dovrebbe porre in essere i dovuti correttivi, se coerenti con i benefici economici della maggioranza. Il processo permetterebbe in linea di principio di adattarsi anche in caso di un eventuale cambiamento delle regole e delle attività supportate dalla DLT.

In questo processo diventa decisiva la possibilità, da parte di R, di porre in essere “minacce credibili”⁵⁰ atte a incentivare gli utilizzatori della DLT a rispettare gli standard desiderabili. Una minaccia è *credibile* se il regolatore mostra di avere le competenze per valutare la corretta applicazione, anche se indiretta, delle regole imposte a quella classe di DLT ed è in grado di mostrare che dispone di strumenti di *enforcement* indiretto. La semplice minaccia potrebbe indurre i partecipanti al network, anche senza un coordinamento esplicito, a convergere verso una soluzione coerente con le regole di R, nell’interesse di tutti gli stakeholder. È verosimile pensare che la minaccia di una “migrazione” da parte di molti utilizzatori verso una DLT più rigorosa delle regole possa indurre la comunità che collettivamente gestisce detta DLT verso protocolli che applicano gli standard desiderati. Ad esempio, è stata proprio la pressione della comunità internazionale sugli effetti ambientali negativi della PoW a indurre la transizione ecologica di Ethereum, anche a costo di rilevanti “costi di aggiustamento”.

La tabella 2 mostra le interfacce (*l’entry point*) per applicare le regole di governance, sia in modo diretto, sia in modo indiretto (tramite intermediari vigilati o altri soggetti). Se il singolo intermediario o un gruppo di intermediari vigilati (ad esempio in forma di consorzio) sono essi stessi i gestori della DLT e questa è di forma *permissioned*, allora è possibile agire in forma diretta (colonna A e B)⁵¹. Qualora gli intermediari si avvalgano di servizi di terzi identificabili (colonna C), le autorità competenti potrebbero disporre di taluni poteri di vigilanza. La Banca d’Italia, ad esempio, in base al Testo Unico Bancario⁵², dispone di poteri di vigilanza informativa e ispettiva, nonché di limitati poteri sanzionatori e di intervento sui fornitori che prestano le attività esternalizzate per intermediari vigilati dovendo questi ultimi rispettare criteri di sana e prudente gestione⁵³. La nuova normativa europea sulla resilienza operativa digitale (*digital operational resilience act*, DORA) rafforza il presidio nei confronti dei fornitori degli intermediari vigilati, introducendo sia requisiti specifici in materia di rischi ICT inclusi quelli di terza parte, sia un regime di sorveglianza diretto nei confronti parti terze ICT con valenza critica.

Non esiste allo stato attuale una modalità di *enforcement* per le DLT *permissionless*, anche se l’approccio di sorveglianza mista (individuale e consortile) potrebbe essere applicato alle DLT *permissionless* con una componente *off-chain* rilevante (colonna D)⁵⁴. Circa le DLT *permissionless*

⁵⁰ Per questo concetto, tipico della teoria dei giochi, cfr. il classico contributo di C. Schelling (1960), capitolo 8.

⁵¹ Cfr. CPMI-IOSCO (2022) con riferimento agli stablecoins. Sulla gestione di una DLT per una infrastruttura di mercato, cfr. E. Naudts *et al.* (2022), pp. 11-13.

⁵² Cfr. anche orientamenti EBA (2019); ESMA (2021).

⁵³ Nel caso di banche, gruppi bancari e intermediari finanziari, tali poteri sono esercitati su tutti i soggetti con i quali gli intermediari vigilati hanno un accordo di esternalizzazione, mentre nel caso di SIM, gestori, intermediari che prestano servizi di investimento, IP e IMEL, solo sui providers i cui servizi vengono qualificati come “funzioni essenziali o importanti”.

⁵⁴ Da notare che di recente la Commissione Europea, nella proposta di regolamento sull’uso e accesso equo dei dati (*Data Act Regulation*), dopo avere definito gli *smart contract*, ne regola i requisiti (robustezza, bloccabilità, *auditability*, ecc.); questi requisiti, nella proposta della Commissione, dovrebbero essere rispettati o dal fornitore delle applicazioni che usano

con una governance interamente algoritmica (*on-chain*) l'unica strada percorribile sarebbe quella prima descritta di *enforcement* indiretto (colonna E). Si tratta, naturalmente, di un *enforcement* tendenziale e di lungo periodo. Rimane inevaso il problema giuridico delle possibilità di reazione, eventualmente in termini di tutela reale, del soggetto che si ritenga pregiudicato dal funzionamento del protocollo; un aspetto, come sottolineato in premessa, che esula dallo scopo di questo lavoro.

Tabella 2 – Entità, forme di corporate governance e possibili “entry point”

	DLT permissioned			DLT permissionless	
	A - Singolo intermediario	B - Infrastruttura di mercato (MFI)	C- Terze parti ITC	D – Off-chain	E – On-chain
Corporate governance	Tradizionale	Tradizionale (in base a schemi e a regole condivise)	Tradizionale	Mista (algoritmica + organi decisionali e di controllo)	Algoritmica completa
Entry point	singola entità	Singola entità/gruppo di imprese	via indiretta	via indiretta	via indiretta tramite disciplina di mercato
Normative o linee guida rilevanti	OCSE (2015) BCBS (2015) DORA (2022) DLT Pilot (2022) MiCAR (2023)	OCSE (2015) CPMI-IOSCO (2022) ECB (2021a) ECB 2021b)	OCSE (2015) DORA (2022) DLT Pilot (2022) se “sistemica” MiCAR (2023)	OCSE (2015)	OCSE (2015)

4.4 Sui limiti di un sistema di governo decentrato

Come accennato in precedenza, la tecnologia blockchain si sta evolvendo per migliorare l'efficienza e la flessibilità d'uso. Per fare ciò essa sta introducendo forme di governo più strutturate, sebbene ancora in fase preliminare. Sono state seguite due strade, ancora molto discusse tra gli addetti ai lavori⁵⁵: la prima (seguita da Ethereum) consiste nell'adottare elementi della tradizionale corporate governance sviluppati tramite organi o funzioni esterne al protocollo elettronico (*off-chain*); la seconda (seguita da Polkadot), più ambiziosa, intenderebbe sviluppare una governance algoritmica completa. Questa include meta-regole atte a rivedere, secondo modalità predefinite, anche le regole “costituzionali” del protocollo, cercando di eliminare la necessità di strutture di governo esterne. Vi sono tuttavia tre aspetti che limitano questo approccio. Il primo attiene all'impossibilità di modificare il codice nativo secondo modalità incompatibili con le regole che il codice (la “costituzione”) stabilisce come non modificabili. Come tutti i contratti, essi possono essere incompleti in caso di circostanze non previste ex ante. Il secondo aspetto riguarda situazioni che richiedono flessibilità o una difficile interpretazione, associata, ad esempio, a un criterio di ragionevolezza di non facile definizione. Il terzo aspetto sarebbe la difficoltà ad avere un sistema puramente automatizzato che preservi in ogni circostanza i meccanismi di incentivo evitando le biforcazioni. Queste possono creare *triggers* o automatismi con effetti sistemici difficilmente controllabili. Se l'impatto di tali eventi, anche se rari, fosse particolarmente elevato in considerazione dell'attività svolta da una determinata

gli *smart contract* o, in sua assenza, dalla persona (nella nostra interpretazione un nodo di una DLT) la cui attività commerciale, imprenditoriale o professionale comporti l'implementazione di *smart contract* per altri soggetti nel contesto di un accordo di messa a disposizione dei dati. (*Data Act*, art. 30).

⁵⁵ Si vedano gli interventi di V. Buterin (2017, 2021).

DLT, un approccio precauzionale basato anche su forme di governo tradizionale, sarebbe preferibile. Allo stato attuale della tecnologia appare quindi opportuno affidare infrastrutture di mercato complesse solo a DLT sorrette da presidi di governo storicamente affermati e a lungo sperimentati. Questi sarebbero in grado di porre in essere i noti sistemi di individuazione, monitoraggio, mitigazione dei rischi.

5 Conclusioni

Dal lavoro emerge quanto segue: le DLT che si affidano prevalentemente a processi *on-chain* riducono le asimmetrie informative migliorando per questa via le problematiche di tipo principale-agente, con difficoltà, tuttavia, ad adottare i tradizionali presidi di corporate governance. Le DLT basate prevalentemente su processi *off-chain* sono più esposte alle criticità di tipo principale-agente, ma ad esse si possono applicare i tradizionali presidi per mitigare i rischi e migliorare i processi di governo. Nel mondo delle DLT si sta osservando un fenomeno simile a quello che ha interessato l'evoluzione dei sistemi *open source* all'inizio degli anni 2000: da strutture di governo "spontanee", volte a sviluppare e migliorare i *software* in modo aperto e condiviso, si è passati a forme più strutturate, indispensabili per favorire le decisioni collettive e superare eventuali conflitti tra i partecipanti (P.B. De Laat, 2007). Vi è una crescente consapevolezza di questi problemi, e si stanno sperimentando soluzioni differenti. Alcune DLT (come Ethereum) si stanno muovendo verso forme ibride, che affiancano a forme di governance algoritmica, strutture esterne di corporate governance più tradizionali; altre (come Polkadot) ambiscono a incorporare interamente questi processi nel protocollo informatico. I fautori dell'approccio basato su una governance algoritmica completa (*full algorithmic governance*) intendono declinare nel modo più coerente l'idea di realizzare una struttura aperta, egualitaria e organizzata in network. In ambedue i modelli, per evitare una eccessiva concentrazione dei poteri e dei ruoli è stato usato l'espedito della randomizzazione dell'assegnazione dei ruoli gestionali e dei diritti di voto (modalità peraltro ampiamente esplorata anche dalla teoria delle scelte sociali).

Quale sia l'esito di questi sviluppi è difficile a dirsi, ma è certo – come nel campo dell'intelligenza artificiale – che questa tecnologia apre nuovi e ineludibili scenari sul modo di operare del sistema economico.

Gli approcci all'enforcement delle regole - Sulla base dell'analisi svolta il lavoro suggerisce, per ciascun tipo di DLT⁵⁶, diversi approcci per fare rispettare le regole di corporate governance ritenute più opportune. Con particolare riferimento ai processi *on-chain*, non esistendo una diretta interfaccia per un ente regolatore o per un *auditor* esterno per eseguire l'attività di *enforcement* (c.d. problema dell'*entry point*), si può agire per via indiretta, attraverso due canali che si rinforzano mutualmente:

- i) tramite la disciplina di mercato, attraverso l'interazione con la comunità attiva in tali sistemi; si tratta di una modalità tipica di molte strutture *open source*, il cui modo di operare è descritto nel dettaglio anche attraverso due casi studio (Ethereum e Polkadot). L'azione collettiva degli agenti partecipanti al network e i meccanismi d'incentivo endogeni potrebbero indurre a migliorare la governance del sistema;
- ii) imponendo ai soggetti attivi in settori regolamentati che utilizzano una DLT di affidarsi solo a sistemi in grado di rispettare criteri di governo ritenuti soddisfacenti. Tali criteri sarebbero calibrati in funzione delle attività supportate da una data DLT (da un semplice

⁵⁶ Una metodologia per descrivere e confrontare in modo rigoroso e sintetico le DLT con diverse configurazioni tecnologiche, funzionali e di governance è fornita nel lavoro Gola, C., Fiorenza, P., Laurino, F., Lesina, L. (2023)

registro condiviso per la raccolta di informazioni, sino al supporto di uno strumento finanziario emesso in forma digitale o di una moneta elettronica “tokenizzata”). Il lavoro illustra l’applicazione di un criterio flessibile, basato su regole di governo in funzione dell’impatto generato da eventuali eventi negativi.

Ciò che emerge dal lavoro è che le DLT basate su un sistema decisionale decentrato, anche interamente automatizzato, necessitano di una chiara, ben bilanciata e robusta struttura di governo se intendono rispettare requisiti di efficienza, scalabilità, flessibilità e sicurezza. Nel perseguire questo bilanciamento, è sicuramente d’ausilio la consolidata esperienza data dagli sviluppi della corporate governance, delle categorie del diritto e della teoria economica, che da tempo hanno affrontato numerosi aspetti utili anche in questo contesto. D’altro canto, il salto di paradigma introdotto da questa tecnologia impone di rivedere alcune categorie consolidate delle discipline sopra citate. Appare inoltre necessario che gli attori economici tradizionali, inclusi i *policy makers*, abbiano un’approfondita conoscenza di questi sviluppi tecnologici. Essi dovrebbero intervenire, in deroga al principio di neutralità tecnologica, se la tecnologia è fonte di un “fallimento di mercato”.

APPENDICE

Due casi studio: Ethereum e Polkadot⁵⁷

Nel corso del testo sono state citate più volte le DLT Ethereum e Polkadot. I motivi per cui sono state selezionate queste due DLT sono i seguenti:

- Ethereum è la seconda rete più diffusa a livello globale⁵⁸ dopo Bitcoin, ed è stata selezionata anche perché il suo modello di governance prevede un bilanciamento tra processi *on-chain* e *off-chain*, come numerose altre blockchain;
- Polkadot rappresenta un esempio di blockchain che si pone l'obiettivo di avere una governance completamente algoritmica.

A - Ethereum

Ethereum è un progetto informatico *open source* lanciato nel 2015, con l'obiettivo di creare una DLT *permissionless* pubblica (aperta sia in scrittura che in lettura) pienamente programmabile⁵⁹. Ethereum è stata progettata come un “sistema di calcolo distribuito”, e non esclusivamente come sistema di pagamento decentralizzato; essa è stata disegnata sin dall'inizio per consentire l'esecuzione di software in modalità decentralizzata (*smart contract*).

Sino al 2022, Ethereum ha utilizzato un meccanismo di consenso *Proof-of-Work*; tuttavia, per contenere l'elevato costo computazionale e quindi energetico/ambientale, nonché per migliorare le performance del protocollo ed abbassare il costo delle commissioni (*fees*), vi è stata di recente la transizione verso un più ecologico ed efficiente protocollo di tipo *Proof-of-Stake* (PoS)⁶⁰.

La pianificazione e l'esecuzione di tale transizione in Ethereum – denominata “*the merge*” – è stata gestita *off-chain*, in analogia con i processi che in Ethereum regolano lo sviluppo e l'applicazione di modifiche al codice della DLT.

Il passaggio al nuovo sistema di consenso ha richiesto un lungo processo di preparazione; era infatti necessario garantire la robustezza della PoW ma ottenere un sistema più flessibile ed efficiente. Il sistema utilizzato è stata una combinazione tra l'introduzione di un deposito cauzionale (*skin-in-the-game*) e l'assegnazione casuale sia dei token (*rewards*) sia dei nodi con poteri di voto. Il *mining* è stato sostituito con il *forging*, il processo di creazione dei blocchi della PoS.

È stato in primo luogo imposto ai nodi che intendono partecipare alla creazione dei blocchi di transazioni di “immobilizzare” nel protocollo stesso un minimo di 32 Ether (ETH) (circa 53 mila auro

⁵⁷ Per una analisi più approfondita di queste due DLT, si rimanda a: Gola, C. *et al.* (2023).

⁵⁸ Per statistiche aggiornate si può, ad esempio, fare riferimento a <https://coinmarketcap.com/>

⁵⁹ A tal fine, è stato realizzato un modello di macchina virtuale distribuita fra tutti i nodi partecipanti alla rete, denominata “Ethereum Virtual Machine” (EVM); per poter sviluppare codice per tale macchina virtuale, sono stati sviluppati appositi linguaggi di programmazione (Solidity e Vyper). Tra i membri più rappresentativi del gruppo di sviluppatori che ha ideato Ethereum, un ruolo preminente è ricoperto da Vitalik Buterin, che è tutt'ora uno dei principali leader nell'evoluzione di Ethereum, e da Gavin Wood, che ha ideato il linguaggio di programmazione Solidity, e che in seguito ha promosso lo sviluppo della *blockchain* Polkadot.

⁶⁰ Il processo di upgrade, piuttosto articolato, ha richiesto vari anni per risolvere problemi tecnologici e, soprattutto, per trovare un accordo tra la maggioranza dei partecipanti al network. Esso ha previsto prima la realizzazione di una rete separata, denominata “Beacon Chain”, con un meccanismo di consenso PoS; successivamente, la rete principale di Ethereum (“mainnet”) è stata unificata con la Beacon Chain. L'unificazione delle due reti ha consentito, in termini molto semplificati, di riprendere lo stato della prima e il meccanismo di consenso della seconda.

al prezzo di metà maggio 2023) a garanzia del corretto svolgimento del loro compito di validatori. Benché sia possibile depositare un quantitativo di ETH superiore all'ammontare minimo previsto, ciò non incrementa le probabilità di un nodo di essere selezionato come validatore ma solo la sua eventuale ricompensa. I validatori infatti sono scelti utilizzando un processo casuale ("randomizzato"), che contiene i fenomeni di concentrazione in capo a pochi soggetti. Ogni 12 secondi si elegge un validatore per la creazione di un nuovo blocco. Le transazioni contenute in quest'ultimo sono ulteriormente verificate da un gruppo di validatori, anch'essi selezionati casualmente, deputati ad esprimere un "voto" finale sulla loro validità. I blocchi ritenuti corretti dalla maggioranza dei validatori vengono dunque aggiunti alla blockchain, mentre gli altri blocchi vengono scartati.

L'aggiornamento di Ethereum ha richiesto diverse interazioni tra gli *stakeholders*. Il punto di partenza è stata la proposta formale di modifica (detta *ethereum improvement proposal* - EIP⁶¹) che può essere formulata e pubblicata sul web da qualsiasi membro della community di Ethereum⁶². Prima di pubblicare formalmente l'EIP, vi è stata una discussione sul forum della *community*⁶³, per escludere proposte deboli o già esplorate in passato. Superata la fase di *peer review*, la proposta è stata formalizzata e vagliata dalla *community* (inclusi sviluppatori). La versione finale dell'EIP è stata riesaminata dagli sviluppatori del protocollo - i c.d. "*Core Developers*" - e, dopo una fase di verifica, inserita in un programma di aggiornamento della rete Ethereum. Questo modello di governance presenta il limite di prevedere processi lunghi e dall'esito incerto con il rischio di una biforcazione della blockchain. In effetti ciò è accaduto anche con il "*merge*", quando una minoranza di nodi ha mantenuto il modello basato sulla *Proof-of-Work*, creando il network minoritario "*EthereumPoW*".

Anche se il fondatore dell'iniziativa, Vitalik Buterin, rimane una figura carismatica, vi è una rilevante differenza rispetto a quanto si osserva nei progetti *open source* tradizionali, dove spesso il fondatore dell'iniziativa continua ad avere un sostanziale potere di veto sulle proposte di cambiamento che emergono dalla comunità.

B - Polkadot

Polkadot è un protocollo la cui caratteristica è quella di facilitare l'interoperabilità tra blockchain attraverso la condivisione dello stesso meccanismo di sicurezza. Esso ambisce inoltre a sviluppare una struttura di governo interamente algoritmica, aperta e democratica, dove i processi decisionali, i meccanismi di voto e di *enforcement* sono eseguiti *on-chain*.

Polkadot permetterebbe a blockchain con caratteristiche differenti (ad esempio basate su PoW, PoS, PoA, *permissionless*, *permissioned*) di comunicare tra loro grazie alla connessione con una blockchain centrale, detta *Relay chain*. L'obiettivo è quello di creare a livello globale un ecosistema dove ogni progetto basato sulla DLT possa interfacciarsi in modo sicuro e affidabile grazie al ruolo centrale della *Relay chain*. Per evitare una eccessiva concentrazione del potere, pur garantendo opportuni organi di direzione e controllo, sono state introdotte varie soluzioni, tra cui l'assegnazione distinta di diritti di voto per la gestione "ordinaria" e "straordinaria" della DLT. Nel seguito descriviamo le linee essenziali del progetto, peraltro ancora in fase di sviluppo.

Il meccanismo di consenso della *Relay chain* è interamente *on-chain*. Esso prevede un processo di elezione dei nodi validatori, responsabili della creazione dei blocchi, denominato *Nominated Proof of Stake* (NPoS). Si tratta di un algoritmo di consenso di tipo *Proof-of-Stake*, in quanto i potenziali candidati alla carica di nodo validatore devono bloccare una certa quantità di token nativi della

⁶¹Gli EIP sono standard tecnici per la predisposizione di proposte inerenti anche le modifiche del protocollo come l'implementazione di nuovi processi e funzionalità.

⁶²Alla community appartengono tutti i detentori di ETH. Dato però l'elevato livello tecnico richiesto per inviare un'EIP ben fatta, di solito gran parte degli autori di EIP sono sviluppatori di applicazioni o protocolli.

⁶³ Ethereum Magicians Forum, <https://ethereum-magicians.org/>

blockchain Polkadot, denominati DOT, che verrà loro restituita al termine del proprio operato a meno di comportamenti scorretti, insieme ad una ricompensa per il lavoro svolto. A differenza di quanto avviene in Ethereum, oltre ai nodi candidati validatori, ci sono anche i cosiddetti nodi “nominatori”, che partecipano all’elezione dei validatori supportando economicamente un insieme di candidati tramite un deposito cauzionale di una certa quantità di DOT.

Se i validatori prescelti dal nominatore vengono effettivamente eletti e producono almeno un blocco, una parte della ricompensa dei validatori viene retrocessa ai nominatori. I validatori sono eletti in base al loro *stake* (funzione della quantità e del tempo di immobilizzazione dei token) tramite un algoritmo che garantisce la proporzionale rappresentazione delle minoranze (ovvero dei validatori sostenuti da un numero minore di nominatori), purché supportate da una quantità sufficiente di DOT, e restano in carica per un periodo definito di tempo. Questo algoritmo (oneroso dal punto di vista computazionale) è eseguito in una blockchain esterna a quella principale, per non rallentare il processo di creazione dei blocchi. La presenza dei nominatori garantisce maggiore sicurezza e una più equa distribuzione dei diritti di voto decentrati nella comunità dei partecipanti.

Dal punto di vista della governance, una significativa innovazione introdotta da Polkadot rispetto ad altre blockchain come Ethereum è la gestione delle modifiche al protocollo grazie a meccanismi *on-chain*. Le modifiche al protocollo Polkadot possono essere proposte da un qualsiasi utente possessore di DOT o da uno dei due organi di governance, il Consiglio e il Comitato Tecnico (cfr. *infra*).

Le modifiche sono votate tramite un meccanismo di referendum direttamente *on-chain*. I referendum avvengono ogni 30 giorni circa e ognuno di essi è associato ad una singola proposta. Tutti i possessori di DOT possono esercitare il proprio diritto di voto ponendo in *stake* i propri DOT per un determinato periodo di tempo al fine di: i) supportare in una fase pre-referendum, una o più proposte; solo la proposta con supporto maggiore diventa oggetto del referendum⁶⁴; ii) partecipare al referendum. Il peso del voto dipende dalla quantità di DOT posta in deposito e dal tempo per cui si decide di bloccarli; ciò fornisce la possibilità anche ai nodi che possiedono pochi DOT di aumentare il peso del loro voto, incrementando il tempo di “blocco”. E’ possibile esprimere il proprio voto anche non ponendo nulla in *stake*, ma in questo caso il voto ha un peso molto basso. Un nodo può anche decidere di delegare il potere di voto a un altro nodo e in questo caso il deposito del nodo delegante si somma a quello del nodo delegato.

Come accennato in precedenza, Polkadot prevede due organi di governance. Il Consiglio è un organo composto da 13 utenti possessori di DOT che restano in carica per un periodo di tempo prestabilito (13-26 settimane)⁶⁵ e nasce con lo scopo di fare le veci dei nodi “passivi”, che non partecipano attivamente alle decisioni di governance. Il Consiglio ha il potere di proporre referendum utili alla comunità, eleggere il comitato tecnico e di cancellare un referendum se i 2/3 dei membri sono d’accordo. Quando i membri del Consiglio partecipano a un referendum con oggetto le proposte da essi stessi formulate, i loro voti sono considerati per-membro e non sulla base dei DOT posti in *stake*; ciò permette di evitare che i membri possano avere il controllo sull’approvazione di tali proposte nei casi di referendum con bassa affluenza.

Il Comitato Tecnico ha invece il compito di individuare eventuali problemi tecnici all’interno del sistema (ad es. a livello di sicurezza) e proporre dunque dei referendum di emergenza per correggerli. Si possono candidare a farne parte tutti i gruppi che hanno implementato con successo almeno una parte del protocollo Polkadot e tali gruppi possono essere aggiunti o rimossi dal Comitato con il voto di maggioranza del Consiglio⁶⁶. Una proposta di emergenza, per poter passare poi alla fase di

⁶⁴ Scelta, in modo alternato, tra la proposta pubblica e la proposta del Consiglio più supportata.

⁶⁵ Qualsiasi nodo detentore di DOT può candidarsi ad essere membro del Consiglio e l’elezione si svolge allo stesso modo di quella dei validatori, dunque si svolge *on-chain* e sono gli utenti a votare.

⁶⁶ In questo caso quindi l’elezione non è propriamente democratica. Tuttavia il Comitato Tecnico ha uno scopo ben preciso e dei poteri molto limitati.

referendum, ha bisogno dell'approvazione di almeno 3/4 del Consiglio o di almeno 2/3 del Comitato. Il Comitato Tecnico ha inoltre il potere di cancellare un referendum in caso di unanimità.

Attualmente la comunità degli sviluppatori di Polkadot sta pianificando il lancio di un referendum su una nuova proposta di governance che mira a ridurre il grado di centralizzazione nel sistema di governo dovuto alla presenza del Consiglio e del Comitato Tecnico. In sostituzione del Consiglio, si prevede di fornire la possibilità ai nodi che intendono essere "passivi" nelle decisioni di governance di delegare il proprio potere di voto a molteplici entità – mentre attualmente è possibile conferire la propria delega solo ad un'unico soggetto terzo – differenziando il delegato in base all'importanza del referendum (c.d. *Multirole Delegation*). Inoltre, i referendum potranno essere cancellati se la rete di nodi voterà in favore dell'eliminazione. Il Comitato Tecnico sarà sostituito dalla *Fellowship*, che rappresenterà l'organo di coordinamento tecnico del protocollo, e che prevedrà condizioni di accesso meno limitanti per gli sviluppatori che vorranno farne parte, allargando così la platea di potenziali partecipanti. Ad ogni membro della *Fellowship* sarà assegnato un livello di competenza che influirà sul peso del suo voto. Non sono state definite, tuttavia, le modalità secondo cui verranno assegnati i livelli, tenendo conto che l'assegnazione dovrà essere fatta in modo tale che la *Fellowship*, o piccoli gruppi di sviluppatori, non abbiano un potere di voto che permetta di avere il controllo su tutta la rete.

Bibliografia

- Accenture (2019), *Governing DLT Networks. Distributed Ledger Technology Governance for Permissioned Networks*.
- Allen, D. W. E., Berg, C. (2020), *Blockchain Governance: what we can learn from the Economics of Corporate governance*, The JBBA, Volume 3, Issue 1.
- Arrow, K. J. (1974), *The limits of the organization*, W.W. Norton and Company NY - London.
- Arrow, K. J. (1986), *Agency and the market*, in: K. J. Arrow e M.D. Intrilligator (a cura di), *Handbook of Mathematical Economics*, Volume 3, Chapter 23, pp. 1183-1195.
- ASTRI (2016), *Whitepaper on Distributed Ledger Technology*, Hong Kong Applied Science and Technology Research Institute and Hong Kong Monetary Authority.
- Bains, P. (2022), *Blockchain Consensus Mechanisms: A Primer for Supervisors*, *Fintech Notes*, n. 3, International Monetary Fund.
- Banca d'Italia (2022), *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*, Roma.
- BCBS (2015), *Guidelines - Corporate governance principles for banks*.
- BCBS (2022), *Prudential treatment of cryptoasset exposures*.
- Borgogno, O. (2022), *Marking decentralized autonomous organizations (DAOs) fit for a legal life: mind the gap*, Banca d'Italia, *Questioni di Economia e Finanza*, n. 718.
- Brummer, C.J., Seira, R. (2022), *Legal Wrappers and DAOs*, disponibile su:
SSRN: <https://ssrn.com/abstract=4123737> or <http://dx.doi.org/10.2139/ssrn.4123737>.
- Buterin, V. (2017), *Notes on Blockchain Governance*, <https://vitalik.ca>
- Buterin, V. (2021), *Moving beyond coin voting governance*, <https://vitalik.ca>
- Chen, J., Micali, S. (2019): “*Algorand: A secure and efficient distributed ledger*”, *Theor. Comput. Sci.* 777
- Ciampi, M., Karayannidis, N., Kiayias, A., e Zindros, D. (2020), *Updatable blockchain*, *Computer Security - ESORICS 2020, Lecture Notes in Computer Science*, vol. 12309, Springer-Verlag, pp. 590-609.
- CPMI – IOSCO (2022), *Application of the Principles for Financial Market Infrastructures to stablecoins arrangements*.
- De Laat, P. B. (2007), *Governance of open source software: State of the Art*, *Journal of Management and Governance* 11(2):165-177.
- Deloitte (2021), *Global Blockchain Survey*.
- EBA (2019), *Orientamenti in materia di esternalizzazione*.
- EBA (2021), *Guidelines on internal governance*.
- ECB (2021a), *Eurosystem assessment methodology for electronic payment instruments, schemes and arrangements*.

ECB (2021b), *Response to the public consultation on the European oversight framework package for electronic payment instruments, schemes and arrangements*.

ESMA (2021), *Orientamenti in materia di esternalizzazione a fornitori di servizi cloud*.

EU Commission (2020), *DORA*, Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014

EU Commission (2022), *Data Act.*, Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data. Brussels, 23.2.2022 COM(2022) 68 final 2022/0047 (COD).

EU Commission (2022), *DLT Pilot regime*, Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology (EU) 2022/858 PE/88/2021/REV/2.

EU Commission (2022), *MiCA*, Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937.

Ehram, F. (2017), *Blockchain Governance: Programming Our Future*, Mimeo.

Farrar, J. H., Hannigan, B. M. (1998), *Farrar's Company Law*, Butterworth, London, fourth edition.

FMI (2023), *Elements of Effective Policies for Crypto Assets*, gennaio.

FSB (2022), *Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets Consultative document*, ottobre.

FSB (2023), *The financial stability risks of decentralised finance*, febbraio.

Garrido, J., Liu, Y., Sommer, J., Viancha, S. (2022), *Keeping Pace with Change: Fintech and the Evolution of Commercial Law*, IMF Fintech Notes 2022/01.

Gola, C., Caponera, A. (2019), *Policy issues on crypto-assets*, LIUC Papers in Economics, Cattaneo University.

Gola, C., Fiorenza, P., Laurino, F., Lesina, L. (2023), *L'uso dei circuiti logici per classificare le blockchain*, Questioni di Economia e Finanza (Occasional Papers), n. 774, Banca d'Italia.

Gola, C., Sedlmeir, J. (2022), *Addressing the Sustainability of Distributed Ledger Technology*, Questioni di Economia e Finanza (Occasional Papers), n. 670, Banca d'Italia.

Grossi, D. (2022), *Social Choice Around the Block: On the Computational Social Choice of Blockchain*, Cornell University.

Hart, O. D. (1995), *Firms, Contracts, and Financial Structure*, Clarendon Press, Oxford.

Hassan, S., De Filippi, P. (2021), *Decentralized Autonomous Organization*, Internet Policy Review, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 2, pp. 1-10.

- Hofman, D., DuPont, Q., Walch, A. e Beschastnikh, I. (2021), *Blockchain Governance: De Facto (x)or Designed?*, in Lemieux, V.L., Feng, C. (eds.), *Building Decentralized Trust*, Chapter 2.
- IOSCO (2022), *IOSCO Decentralized Finance Report*, marzo.
- ISO – Technical specifications (2022), *Blockchain and Distributed Ledger Technologies, Guidelines for Governance*, TS/23635, febbraio.
- Javarone, M., Di Antonio, G. Vinci, Pietronero, L. e Gola, C. (2022), *Evolutionary Dynamics of Sustainable Blockchain*, Royal Society Open Science, Proceedings.
- Jensen, M. J., Murphy, K.J. (1990), *Performance Pay and Top-Management Incentives*. Journal of Political Economy, Vol. 98, pp. 225-264.
- Lamport, L., Shostak, R., e Pease, M. (1982), *The Byzantine Generals Problem*, ACM Transactions on Programming Languages and Systems, 4:3, pp. 382-401.
- Lanfranchi, C. (2019), *Profili giuridici delle valute virtuali*, Ciberspazio e Diritto, volume 20, n, 62.
- Liu, Y., Lu, Q., Yu, G., Paik, H-Y., Zhu, L. (2022), *Defining Blockchain Governance Principles: A Comprehensive Framework*, University of New South Wales, Australia.
- Markus, L. M. (2007), *The governance of free/open source software projects: monolithic, multidimensional, or configurational?*, Journal of Manage Governance, 11:151–163.
- Maw, N.G., Lord Lane of Horsell, Craig-Cooper, M. (1994), *Maw on Corporate governance*, Dartmouth Publishing Company, Brookfield, Vermont, USA.
- Milgrom, P., Roberts, J. (1992), *Economics, Organization and Management*, Prentice Hall, Inc. New Jersey, USA.
- Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, white paper.
- Naudts, E., Aerts, T., Franken, L. Pieterse A. (2022), *Governance in systems based on distributed ledger technology (DLT): A comparative study*, AFM.
- OCSE (2015), *G20/OECD Principles of Corporate governance*, OECD Publishing, Parigi.
- OCSE (2017), *Methodology for Assessing the Implementation of the G20/OECD Principles of Corporate governance*, OECD Report to the G20 Finance Ministers and Central Bank Governors, Parigi.
- OCSE (2022), *Why Decentralised Finance (DeFi) Matters and the Policy Implications*, Parigi.
- Santana, C., Albareda, L. (2022), *Blockchain and the emergence of Decentralized Autonomous Organizations (DAOs): An integrative model and research agenda*, Technological Forecasting & Social Change, 182, 121806.
- Schär, F. (2021), *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*, Federal Reserve Bank of St. Louis Review, 103(2), pp. 153-74.
- Schär, F., Nadler, M. (2022), *Decentralized Finance, Centralized Ownership? An Iterative Mapping Process to Measure Protocol Token Distribution*, Journal of Blockchain Research, Vol. 1, pp. 29–36.
- Schelling, T. C. (1960), *The strategy of conflict*, Harvard University, Cambridge, Massachusetts, USA.

Sultanik, E., Remie, A., Manzano, F., Brunson, T., Moelius, S., Kilmer, E., Myers, M., Amir, T., Schriener, S. (2022), *Are Blockchain Decentralized? Unintended Centralities in Distributed Ledgers*, Trail of Bits.

The Law Society (2020), *Blockchain: Legal & Regulatory Guidance*, Tech London Advocates, *Blockchain Legal and Regulatory*.

UK Jurisdiction Taskforce (2019), *Legal statement on crypto-assets and smart contracts*, The LawTech Delivery Panel.

van Pelt, R., Jansen, S., Baars, D., e Overbeek, S. (2020), *Defining Blockchain Governance: A Framework for Analysis and Comparison*, *Information Systems Management*, 38:1, 21-41.

Wang, S., Ding, W., Li, J. Yuan, Y., Ouyang, L, e Wang Fei-Yue, (2019), *Decentralized Autonomous Organizations: Concept, Model, and Applications*, *IEEE Transactions on Computational Social Systems*, Vol. 6, n. 5.

Williamson, O. (1999), *The Mechanism of Governance*, Oxford University Press.