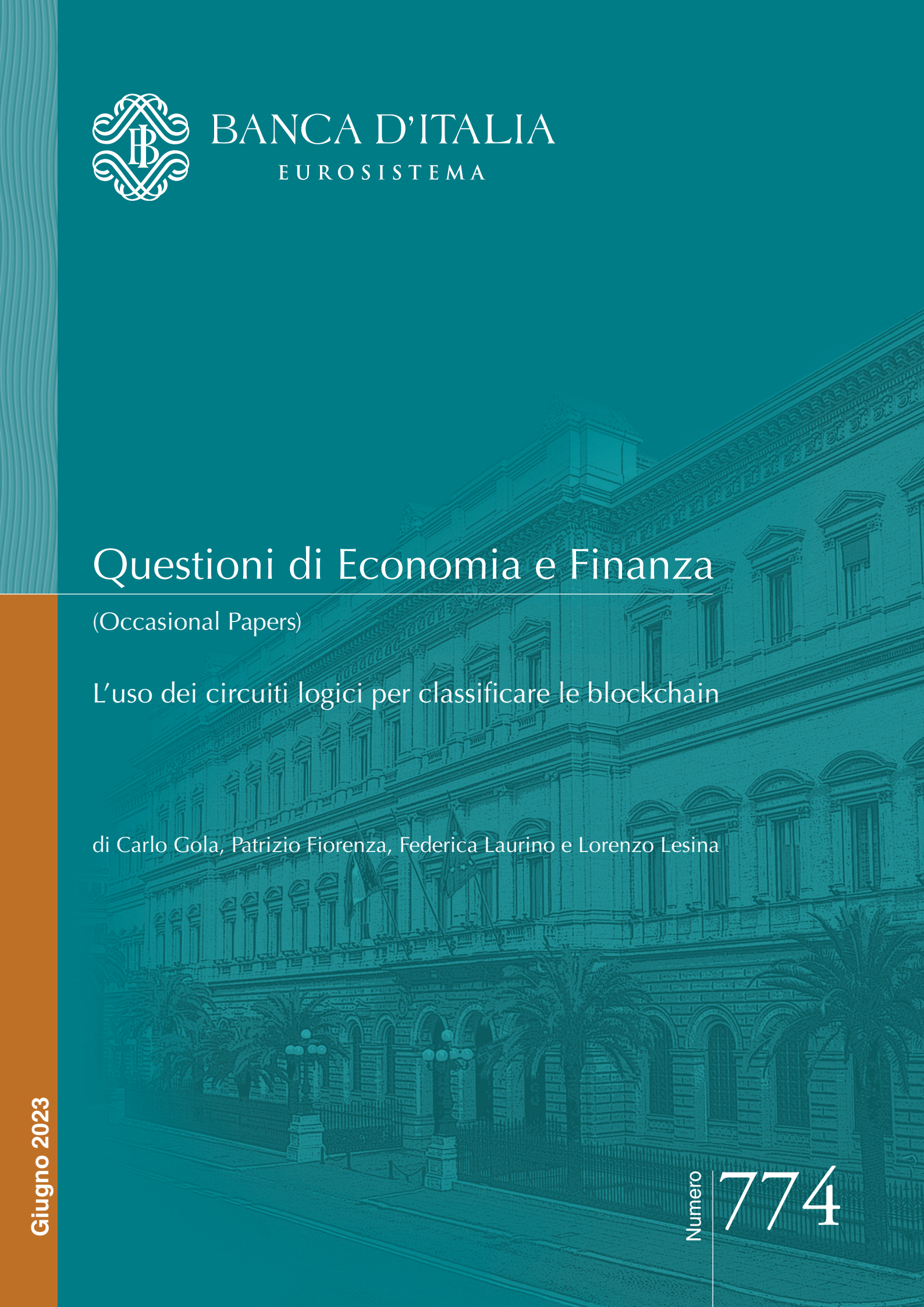
BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

L'uso dei circuiti logici per classificare le blockchain

di Carlo Gola, Patrizio Fiorenza, Federica Laurino e Lorenzo Lesina



Giugno 2023

Numero 774

BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

L'uso dei circuiti logici per classificare le blockchain

di Carlo Gola, Patrizio Fiorenza, Federica Laurino e Lorenzo Lesina

Numero 774 – 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 .

ISSN 1972-6643 (online)

Grafica a cura della Divisione Editoria e stampa della Banca d'Italia

Sommario

Il lavoro fornisce un metodo per classificare le blockchain e i sistemi informatici basati sulla *distributed ledged technology* (DLT) e facilitare il loro confronto. Le DLT, infatti, sono difficilmente comparabili, poiché adottano diverse configurazioni tecnologiche, distinte per attività svolte, caratteristiche tecniche e strutture di governo. Inoltre, alcune DLT associano a procedure organizzative automatizzate processi decisionali tradizionali, mentre altre adottano una governance interamente algoritmica. Il lavoro descrive le principali caratteristiche delle DLT: il grado di decentramento, il tipo di protocollo di consenso, il sistema di aggiornamento, la struttura di governo, la possibilità di sdoppiare il registro (*forking*). Esso utilizza la teoria dei circuiti logici (*switching circuits*) per rappresentare e confrontare visivamente DLT differenti, in base alle loro caratteristiche. La metodologia viene applicata a Ethereum e Polkadot, due DLT particolarmente complesse.

Classificazione JEL: G3, M4, D82, G14, G21, G28, M4, M15, O33.
Parole chiave: blockchain, DLT, cripto-attività, finanza decentrata, supervisione bancaria e finanziaria.
DOI: 10.32057/0.QEF.2023.0774

Indice

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

L'USO DEI CIRCUITI LOGICI PER CLASSIFICARE LE BLOCKCHAIN

di Carlo Gola, Patrizio Fiorenza*, Federica Laurino*, Lorenzo Lesina*

1 Introduzione[1]

Uno dei problemi più rilevanti nei sistemi di finanza decentrata (DeFi) che utilizzano la blockchain o le tecnologie a registro distribuito (*distributed ledger tecnhologies*, DLT) è quello di identificare le varie caratteristiche che queste strutture distribuite possono avere. Esse riguardano il grado di apertura al pubblico del protocollo informatico, la presenza o meno di una struttura di governo predefinita dall'algoritmo, il grado di interoperabilità con altre DLT, la capacità di sorreggere in modo efficiente e flessibile un insieme ampio di attività. Lo scopo di questo lavoro è quello di fornire uno strumento di immediato utilizzo per rappresentare in modo rigoroso e sintetico tali configurazioni. Il sistema permette di classificare le DLT, inclusi vari organi o sistemi collettivi di gestione e controllo operativo (sviluppatori, comitati tecnici, comitati esecutivi, ecc.) anche nelle configurazioni ibride, difficilmente riconducibili alle tradizionali due categorie, *permissionless* e *permissioned*. Esso fornisce un agile supporto all'analisi della corporate governance di una DLT[2].

Il lavoro è strutturato come segue. Vengono prima esposte in modo sintetico le principali caratteristiche di una DLT: protocollo di consenso, grado di decentramento, immutabilità, tracciabilità, scalabilità, gestione delle transazioni *on-chain* e *off-chain*, governance del protocollo nativo, interoperabilità, identificabilità degli utenti e dei nodi, aggiornabilità della blockchain e rischio di sdoppiamento (*hard fork*), efficienza ambientale (paragrafo 2). In seguito viene proposta una struttura logica per classificare le varie configurazioni di una DLT (paragrafo 3). Vengono quindi descritte attraverso questa metodologia due DLT particolarmente complesse, Ethereum e Polkadot (rispettivamente paragrafi 4 e 5). Il paragrafo 6 conclude.

2 Le principali caratteristiche di una DLT

Una buona DLT si caratterizza per i seguenti aspetti: elevato grado di decentramento (ragion d'essere di questa tecnologia); elevata efficienza (tecnologica, economica e ambientale); robustezza del sistema (integrità e resilienza agli attacchi esterni). Esistono tuttavia vari *trade-off* tra queste tre caratteristiche. In particolare, un grado molto elevato di decentramento garantisce standard di sicurezza elevati spesso a scapito dell'efficienza del sistema. Un aumento del grado di efficienza e una riduzione del grado di decentramento può indebolire la robustezza del sistema. Il mercato ha quindi sviluppato un'ampia varietà di configurazioni di DLT, difficilmente riconducibili alla semplice dicotomia *permissionless* vs. *permissioned.* Esse riflettono esigenze e funzionalità che il sistema deve

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

[1] Le opinioni espresse sono personali e non impegnano in alcun modo l'Istituzione di appartenenza. Nessun *endorsement* viene fatto alle DLT citate in questo lavoro, che sono state selezionate a scopo meramente illustrativo.

[2] Su questi aspetti e, più in generale, sulle DLT, si rimanda a: Gola, C., Cappa, V., Fiorenza, P., Laurino, F., Lesina, L., Lorizzo, F., Marcelli, G., (2023), *La governance delle blockchain e dei sistemi basati sulla tecnologia dei registri distribuiti,* Banca d'Italia, Questioni di economia e finanza (Occasional Papers), n. 773 giugno.

"sorreggere". Prima di passare alla descrizione della mappa o circuito logico in grado di rappresentare sinteticamente tali configurazioni, è utile fornire, anche solo per cenni, alcune informazioni sulle caratteristiche tecniche delle DLT[3].

Il protocollo di consenso. In primo luogo è necessario dire che nei sistemi blockchain esiste una stretta relazione tra *decentramento* e *fiducia reciproca*: un'architettura informatica di questo tipo è un sistema distribuito composto da *nodi*[4] che interagiscono tra loro secondo particolari proprietà e necessitano di accordarsi sullo stato finale di un registro pubblico (*consenso*)[5]. In modo informale, potremmo definire il decentramento come la capacità di costruire uno stato di fiducia reciproca tra soggetti che non si conoscono senza ricorrere a una controparte centrale. In tutte le circostanze nelle quali non sia possibile, o desiderabile, individuare uno o più attori che possano assumere un ruolo di "terze parti fidate" per gestire il sistema per conto dei partecipanti, le architetture blockchain offrono una valida soluzione. Esiste un'ampia varietà di protocolli di consenso (oltre alla *proof-of-work* di Nakamoto, la *proof-of stake*, la *delegated proof-of-stake*, la *pure proof-stake*, la *proof-of authority*, ecc.). Ciascuna utilizza meccanismi di incentivo e modalità di "voto" differenti.

Sistema di consenso deterministico o probabilistico. Il meccanismo di consenso del protocollo che regola la creazione e la finalizzazione delle transazioni può essere deterministico o probabilistico. In una blockchain con un sistema di consenso probabilistico, come Bitcoin, una volta che un blocco viene propagato, resta in attesa di conferma. Con l'aumentare del numero di blocchi che si aggiungono alla catena, si riduce la probabilità che tale blocco sia cambiato. In questo modo, la blockchain diventa sicura e affidabile solo col passare del tempo. In una blockchain con un sistema di consenso deterministico, la transizione è valida e definitiva quando una certa soglia di consenso tra nodi identificati è raggiunta (ad esempio due terzi dei nodi funzionanti correttamente in un dato momento). Ogni nodo della rete aggiorna il proprio registro in modo simultaneo, come avviene nei sistemi di pagamento tradizionali.

Il grado di decentramento: DLT *permissionless* e *permissioned*. Esistono due grandi categorie di DLT: le *permissionless* e le *permissioned*. Le prime sono gestite attraverso una rete di nodi senza vincoli di accesso alla gestione in scrittura e lettura del registro condiviso; le seconde, al contrario, prevedono tali restrizioni. I nodi sono anonimi o pseudo anonimi (identificabili attraverso indagini specifiche sull'indirizzo IP), numerosi e spesso paritetici. Le DLT *permissioned* sono basate su un sistema i cui nodi sono abilitati da una autorità centrale (il promotore dell'iniziativa, che può configurarsi anche in forma collettiva, come in un consorzio o una joint venture). Le DLT sono dette *pubbliche* quando l'accesso in lettura e in scrittura non è limitato a soggetti abilitati; in caso contrario si parla di DLT *private.* Sempre sotto il profilo terminologico, è da notare che generalmente si intende per blockchain il protocollo *permissionless* pubblico, introdotto da Nakamoto, che quindi è una sottoclasse dei protocolli DLT. Nella letteratura corrente i due termini sono di fatto sinonimi.

L'irreversibilità delle transazioni. Questa caratteristica discende direttamente dalla natura "*append-only*" delle blockchain, ovvero, la possibilità di aggiornare il loro stato solo aggiungendo nuove informazioni (nuovi blocchi) e mai cancellando o modificando informazioni precedentemente aggiunte (blocchi già parte della catena) a meno di dar vita ad una blockchain parallela grazie a una biforcazione (*fork*). Dato che l'unico modo di aggiornare il registro è aggiungendo nuove transazioni, una volta che una transazione viene inclusa in esso è, a tutti gli effetti, immutabile. L'immutabilità è

[3] Sulla tecnologia blockchain si veda: Yaga, D., Mell, P., Roby, N., Scarafone, K. (2018), *Blockchain Technology Overview*, National Institute of Standards and Technology, U.S. Department of Commerce, ottobre.

[4] Per nodo si intende un dispositivo o un'applicazione informatica che è parte di una rete e detiene una copia parziale (*light node*) o completa (*full node*) delle registrazioni di tutte le operazioni eseguite tramite il registro distribuito.

[5] Un protocollo di consenso di una DLT è un insieme regole matematiche e di crittografia atte a garantire un accordo tra un numero sufficiente di nodi sullo "stato" del sistema (ad esempio lo stato di aggiornamento di un registro di transazioni economiche). Il prototipo di tali sistemi è il *Nakamoto protocol*, basato sulla *proof-of-work*.

una proprietà a doppio taglio: da un lato rende difficile modificare/contraffare dati *on-chain*, rendendo le blockchain pubbliche e *permissionless*[6] delle architetture molto interessanti per la realizzazione di sistemi resistenti ad attacchi esterni, dall'altro in caso di transazioni errate (ad esempio, pagamenti effettuati verso indirizzi non corretti) è di fatto impossibile correggere gli errori senza cooperazione da parte di terzi: dato che non è possibile cancellare una transazione, l'unico modo per annullarne gli effetti è crearne una nuova uguale e contraria. Le DLT *permissioned*, avendo la possibilità di coordinare un sottoinsieme di nodi abilitati e pertanto individuabili, possono più agevolmente risolvere questo problema.

La tracciabilità e trasparenza. Questo aspetto fa riferimento alla proprietà per cui i dati registrati *on-chain* (tramite il protocollo nativo) devono essere accessibili e verificabili. Questa trasparenza, come si è visto in precedenza, è essenziale per supportare la fiducia nella sicurezza del sistema: ogni nodo è in grado, autonomamente, di ispezionare e verificare la validità di blocchi e transazioni, senza la necessità di doversi affidare a un attore terzo per farlo. Ciò comporta che è possibile ispezionare qualsiasi transazione presente su una blockchain pubblica anche per scopi di "*forensics*", analizzando le informazioni memorizzate sul registro condiviso. D'altro canto, ciò comporta anche che per preservare la privacy su una blockchain pubblica è necessaria l'adozione di tecniche specifiche e addizionali[7]. Peraltro, con il crescere della dimensione della blockchain, diventa più oneroso per un nodo il download dell'intera storia del sistema. Solo i nodi con costosi e dedicati dispositivi hardware e software (detti *full nodes*) hanno la capacità di verificare la veridicità di tutte le transazioni.

La scalabilità. Un ulteriore importante aspetto che ha portato a sviluppare configurazioni complesse delle DLT è la scalabilità. Questa è definita come la capacità del sistema di processare un numero elevato di transazioni per unità di tempo e da parte di numerosi nodi.[8] Anche in questo caso esiste un trade-off, denominato in letteratura il "trilemma" delle blockchain, poiché è difficile avere una DLT che riesca simultaneamente a garantire criteri di scalabilità, elevato decentramento e sicurezza (cfr. Tabella 1).

Gestione delle transazioni *on-chain* e *off-chain*. Dato che la scalabilità è una caratteristica necessaria per molteplici utilizzi pratici delle blockchain, soprattutto in ambienti pubblici e su larga scala, sono state proposte differenti soluzioni al problema. In prima approssimazione, esse possono essere raggruppate in due categorie: (i) soluzioni "*on-chain*" o *Layer 1* (dove il *Layer 1* è il *ledger* stesso), che comportano modifiche alla blockchain stessa, facendo un *upgrading* del *ledger* di base – ad esempio in grado di sorreggere blocchi di dimensione maggiore o algoritmi di consenso differenti rispetto a quello iniziale; (ii) soluzioni "*off-chain*", che comportano l'aggiunta di livelli di direzione al di sopra del *ledger* di base – ad esempio, le soluzioni basate su reti *Layer-2* o quelle che comportano la creazione di *side-chains*.[9]

---

[6] Nel caso delle *blockchain* private e *permissioned*, la presenza di uno o più nodi gestori della piattaforma con un ruolo sovraordinato – tecnico o di business – rende più agevole gestire queste casistiche, potendo intervenire per sanare in qualche modo gli errori.

[7] Vi sono società dedicate a questo settore, noto come "*blockchain forensics*", di cui la più nota è probabilmente Chainanalysis (www.chainanalysis.com). Il raggiungimento di obiettivi di privacy forti richiede invece l'adozione di tecniche specifiche, note anche come *Privacy Enhancing Techniques* (PETs); una descrizione approfondita di tali tecniche, focalizzata sui pagamenti digitali, può essere trovata in "*Balancing confidentiality and auditability in a distributed ledger environment*" (https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical200212.en.pdf).

[8] Per una rassegna della letteratura, si veda: Hafid, A. Senhaji, A., Samith, M. (2020), *Scaling blockchain: A comprehensive survey*, Institute of Electrical and Electronics Engeneering (IEEE), vol. 8.

[9] Per soluzione *off-chain* si intende un sistema che affianca alla *blockchain* nativa (tipicamente *permissionless*), altre *blockchain* (di solito *permissioned* e talvolta anche private) che si raccordano alla prima dopo avere svolto funzioni autonome. Ad esempio, la *blockchain* di secondo livello potrebbe validare blocchi di transazioni tramite sistemi più efficienti (meno energivori) e inserire solo in seguito il blocco di transazioni validate sulla *blockchain* nativa (di primo livello). Tuttavia, al guadagno di efficienza potrebbe corrispondere una perdita di robustezza del processo, se non ben disegnato.

Tabella 1 – Le caratteristiche di una DLT

Efficienza	*Tecnologica*: scalabilità, portata (*throughput*), capienza (*storage*), latenza (*confirmation time*), flessibilità (*upgradable, adaptable, extensible, future-proof*), interoperabilità.
	Ambientale: bassi costi fissi (costo dell'hardware e del software) e bassi costi variabili (assorbimento energetico per unità di output, ecc.)
	Economica: contendibilità del sistema (assenza barriere all'entrata)
Decentramento	*Numero dei nodi*: illimitato (*permissionless*); limitato (*permissioned*)
	Tipo di protocollo di consenso per pervenire alla fiducia reciproca *ex-post*
	Visibilità del registro condiviso e accessibilità sistema pubblico o privato
	Gestione *on-chain* e *off-chain*
	Ruolo dei nodi ed eventuali organi di coordinamento, direzione, sviluppo, controllo
	Meccanismi "enforcement": automatizzati (decentrati) v. tradizionali (accentrati)
Robustezza e integrità	*Tolleranza agli attacchi esterni* (*fault-tolerance*): monitoraggio e mitigazione dei rischi
	Irreversibilità delle transazioni; settlement deterministico o probabilistico
	Rispetto della privacy, integrità del sistema, buona struttura di governo
	Altri criteri di robustezza (ISO/TS 23635)[10]

La governance *on-chain* (algoritmica) e *off-chain*. Un aspetto particolarmente complesso e delicato riguarda la possibilità di modificare il protocollo nativo, quello utilizzato nella fase iniziale del progetto e messo in rete in modo pubblico. Tale protocollo per sua natura sarebbe immutabile (nel gergo "il codice è legge"). Nella realtà può esservi l'esigenza di modificarlo, per correggere errori (*bugs*) o per migliorare l'efficienza e la sicurezza del sistema. Vi sono due modi per fare fronte a queste esigenze: governance *on-chain*, oppure governance al di fuori del protocollo nativo, detta *off-chain* (per ulteriori dettagli, cfr. C. Gola et al., 2023).

I processi di governance *on-chain*, sono definiti come quell'insieme di regole relative al governo della DLT scritte nel protocollo nativo della DLT. Questi processi di *governance algoritmica completa* possono modificare le regole del protocollo nativo, secondo forme e modi prestabiliti (simili alle norme di revisione costituzionale). In tale ambito potrebbero ad esempio essere decise e 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 e immutabile. Le decisioni, ad esempio proposte da sviluppatori che operano in rete, vengono prese tramite referendum secondo modalità predefinite. Vi possono essere organi consuntivi, comitati, gruppi di aggregazione, ma tali organi non hanno potere sulla decisone finale.

I processi di governance *off-chain* non sono scritti direttamente sul protocollo nativo della DLT, ma interagiscono con esso dopo avere svolto funzioni organizzative o decisionali al di fuori di esso. Come nel caso precedente vi possono essere organi o comitati tecnici, ma le decisioni avvengono *off-chain*,

[10] ISO Technical specifications (2022), *Blockchain and Distributed Ledger Technologies. Guidelines for Governance*. TS/23635, febbraio.

come in una tradizionale struttura organizzativa. Conoscere questi processi decisionali, l'allocazione dei poteri e delle responsabilità, eventuali meccanismi di delega, ecc. è fondamentale. È infatti a livello *off-chain*, che si possono annidare opacità, fragilità, distorsioni (tra cui una eccessiva concentrazione dei poteri), dato che la modalità operativa non garantisce i livelli di trasparenza dei processi automatizzati *on-chain*. D'altro canto i processi *off-chain* hanno il vantaggio di potersi avvalere dei tradizionali presidi di corporate governance, tra cui l'attribuzione delle responsabilità e l'*accountability*.

L'interoperabilità. Oltre agli aspetti interni alla struttura di una data DLT (grado di apertura ai partecipanti, modalità gestionali e di controllo del protocollo, sicurezza, ecc.) un ecosistema efficiente deve avere caratteristiche tecnologiche che permettano a diverse DLT di "dialogare", di interfacciarsi, di essere "interoperative". L'interoperabilità deve riguardare sia i processi sia i dati anche provenienti da sistemi esterni (c.d. "oracoli"). Questo profilo non solo è fondamentale per evitare frammentazioni tra sistemi che dovrebbero potere interagire in modo efficiente, ma anche per mantenere elevata la contendibilità e quindi la concorrenzialità del mercato (accesso da parte di potenziali entranti anche in presenza di economie di scala o di rete).

Identificabilità dell'utente finale e dei nodi. L'identificabilità, sia dell'utente finale (colui che, ad esempio, acquista una cripto-attività), sia di chi valida le transazioni, è un aspetto che ha evidenti implicazioni nel contrasto delle attività illecite. In presenza di una DLT *permissionled* e/o di una entità centralizzata come un fornitore di servizi per cripto-attività (ad esempio un *exchanger* o un *wallet provider*) è possibile identificare gli utenti; diverso è il caso in cui si opera tramite una DLT *permissionless* secondo una modalità bilaterale (*peer-to-peer*). In questo caso l'unica informazione pubblica disponibile è l'indirizzo del *wallet* (una stringa di numeri e lettere) e solo con indagini di polizia postale è possibile tentare di identificare il proprietario delle cripto-attività. Vi sono, peraltro, sistemi algoritmici (c.d. *mixer* o *tumbler*) che rendono complessa l'associazione tra il *wallet* e il suo proprietario, o cripto-attività (come Monero), dove non è possibile collegare due transazioni, né di determinare la fonte o la destinazione dei fondi (nemmeno come indirizzo pubblico).

L'aggiornamento della blockchain e il rischio di sdoppiamento (*hard fork*). Come tutti i software, anche le blockchain richiedono un aggiornamento per aggiungere funzionalità, rimuovere errori di programmazione, ridurre le vulnerabilità. Questi aggiornamenti sono problematici in assenza di un processo decisionale accentrato. Vi sono due aspetti da considerare: quali tipi di miglioramenti sono richiesti; cosa succede in caso di disaccordo tra i nodi attivi (*full nodes*). Aggiornare una blockchain significa modificare il codice del software (la blockchain principale o protocollo nativo) preservando la storia e l'integrità del registro distribuito. Gli aggiornamenti sono di vario tipo: alcuni sono semplici correzioni di errori di programmazione e sono retro-compatibili; altri sono cambiamenti più importanti, come ad esempio la dimensione dei blocchi da validare, le commissioni ricevute dai validatori, i cambiamenti strutturali del protocollo di consenso. In un sistema open-source le proposte di cambiamento più radicali, con riflessi economici sui partecipanti, possono comportare divergenze di vedute. Nei sistemi blockchain *permissionless*, se non vi è un accordo, un gruppo di nodi può decidere di non aggiornare il software. In questo caso i contrari (spesso una minoranza) possono continuare a usare il vecchio standard e pertanto si crea una "biforcazione": se il nuovo software non è compatibile con il vecchio si verifica uno sdoppiamento della blockchain (cd. *hard fork*). Si creano quindi due network che operano in parallelo, ciascuno con i relativi "follower" (nodi, utenti finali) e con il proprio token. Il prezzo del nuovo token rifletterà il grado di apprezzamento del mercato ai due standard, premiando quello ritenuto più valido (un caso concreto è stato lo sdoppiamento di Bitcoin con Bitcoin Cash o di Ethereum con Ethereum Classic). Se la modifica è retro-compatibile e soltanto alcuni nodi devono essere aggiornati, si parla di *soft fork*. In questi casi i nodi che non aggiornano il protocollo possono continuare a partecipare alla rete, anche se potrebbero non avere accesso alle nuove funzionalità introdotte dall'aggiornamento minore. I *soft fork* non creano uno sdoppiamento della blockchain.

"*Non-forkable*" blockchain. Una blockchain "*non-forkable*" è una blockchain che non consente ai nodi di modificare le regole di consenso della rete, salvo che non vi sia un organo o una procedura che permetta di modificare la blockchain nelle forme e nei modi predefiniti. Ad esempio nel caso di Polkadot i nodi della rete hanno la caratteristica informatica di poter seguire le regole del protocollo senza che esse siano salvate sul nodo stesso. Le regole del protocollo vengono conservate direttamente sulla blockchain di Polkadot, che può essere aggiornata soltanto tramite voto *on-chain*, e poi lette dai vari nodi che sono solo in grado di "eseguire" le regole. Se le variazioni della blockchain sono retro-compatibili, la probabilità di un *hard fork* è molto più bassa.

L'efficienza ambientale. Un ultimo aspetto riguarda la scarsa efficienza energetica delle DLT basate sul meccanismo di consenso denominato *proof-of-work* (PoW).[11] Il tema è noto, e non è il caso di approfondirlo in questa sede. Il punto da rilevare è che la transizione verso sistemi tecnologici più efficienti, e quindi meno impattanti dal punto di vista ambientale (ad esempio basati su meccanismi di consenso *proof-of-stake,* oppure *proof-of-authority,* richiede un sistema governance in grado di gestire questa transizione. In alternativa, è necessario ricorrere a processi *off-chain* che a loro volta devono essere gestiti e monitorati.

3 Una mappa per individuare le attività delle DLT e la loro struttura di governo

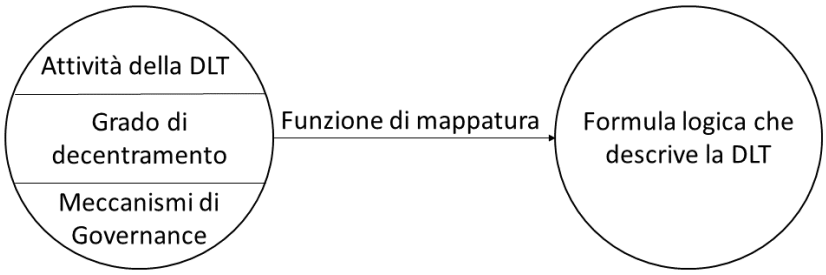
Abbiamo visto che le DLT possono avere caratteristiche tecniche molto diverse per dare risposta alle varie esigenze di scalabilità, efficienza, sicurezza e immutabilità del registro condiviso. Si è fatto riferimento a due macro-classi (*permissionless* e *permissioned*); tuttavia nella realtà esiste un ampio spettro di configurazioni, da quelle interamente decentrate e pubbliche, sia in lettura che in scrittura (come la blockchain di Bitcoin), a DLT ove alcuni nodi svolgono un ruolo privilegiato (ad esempio possono operare in qualità di validatori solo se autorizzati da altri nodi), fino a DLT dove esistono diversi organi di decisione e controllo (che possono operare *on-chain* o *off-chain*). Come vengano allocati tali poteri, quali siano le regole decisionali, in quale misura alcuni nodi siano responsabili (*accountable*) del proprio operato, è il compito di una chiara e ben disegnata struttura di governo. È rilevante sia il tipo di attività che la DLT deve svolgere, direttamente o tramite protocolli paralleli, sia il grado di decentramento della stessa. Per fare ciò è necessario individuare con chiarezza le varie tipologie di DLT, tenendo presente le diverse caratteristiche tecniche, economiche e di governance.

Di seguito si fornisce uno schema logico, che si ispira ai circuiti logici[12], in grado di identificare in modo stilizzato diverse possibili configurazioni di DLT e molte possibili strutture di governo, tramite la definizione di una funzione che, prendendo in input una serie di configurazioni (relative alle attività svolte, al grado di decentralizzazione e ai meccanismi di governance) fornisce come output una formula logica in grado di descrivere quella specifica DLT. Lo schema logico si articola come mostrato in Figura 1.

[11] Per una discussione su questi aspetti si veda: Gola, C., Sedlmeir, J. (2022), *Addressing the Sustainability of Distributed Ledger Technology*, Questioni di Economia e Finanza (Occasional Papers) 670, Bank of Italy.

[12] "Un circuito logico che contiene solo interruttori a due posizioni (quando un interruttore è chiuso passa la corrente, altrimenti no) può essere rappresentato da uno schema nel quale, vicino ad ogni interruttore, si pone una lettera che rappresenta una condizione necessaria e sufficiente perché l'interruttore conduca corrente.", cfr. Elliott Mendelson (1970), *Boolean Algebra and Switching Circuits*, McGraw Hill, capitolo 8; Elliott Mendelson (1972), *Introduzione alla logica matematica*, p. 34, ed. Bollati Borghieri;

Figura 1 – Schema logico per la mappatura delle DLT



La prima parte consiste in un tradizionale *mapping* delle attività svolte da una determinata DLT, indicate con $\{A_i\}$ (si veda Tabella 2). In linea di principio a ogni attività svolta è associato uno specifico rischio, presidiabile da un insieme di norme di autogoverno, sia interne che esterne, che dovrebbero essere rispettate per monitorare e mitigare i rischi associati al buon funzionamento della DLT.

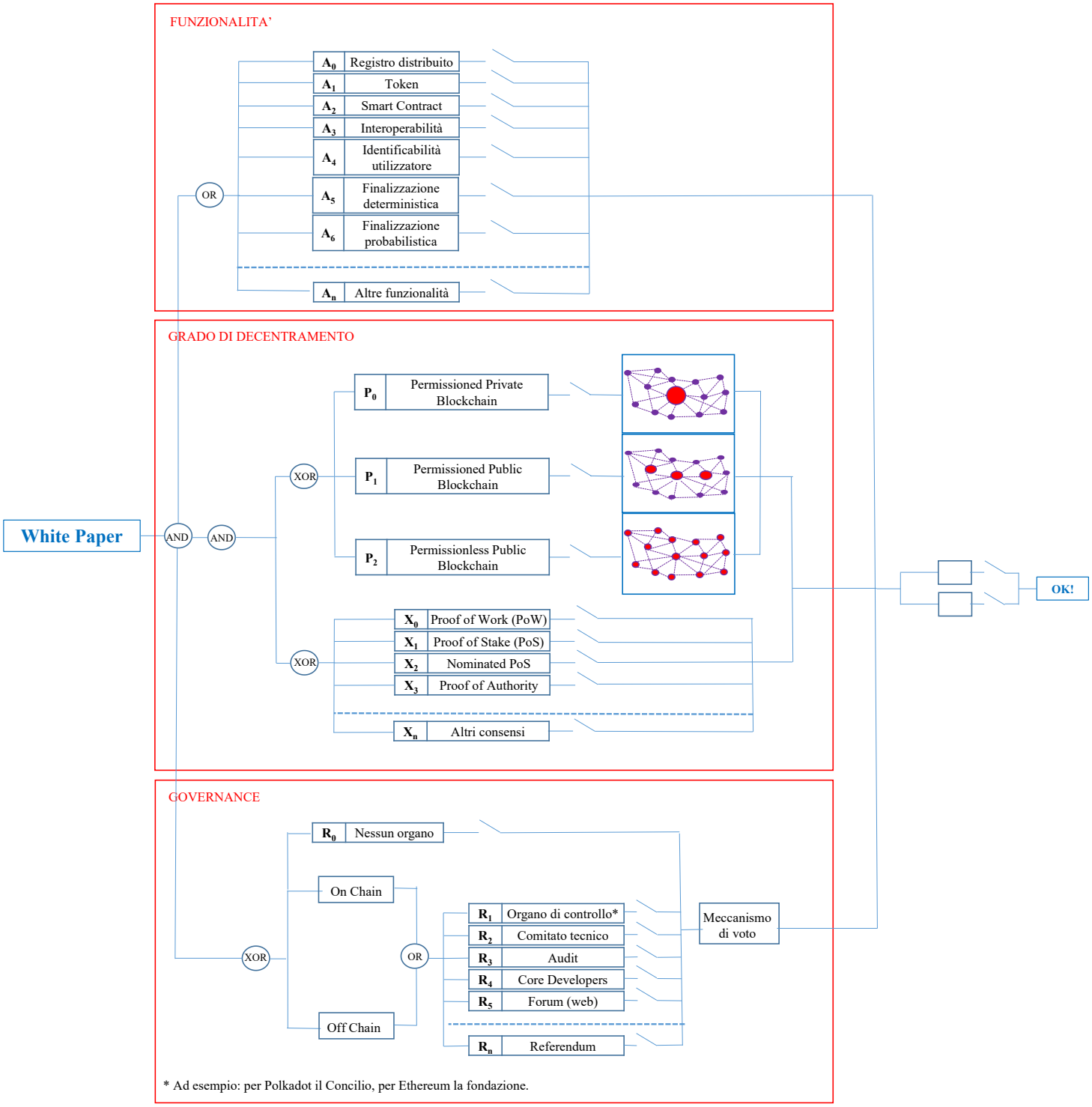
Tabella 2 - Elenco delle possibili attività svolte dalla DLT

A_0	Creazione di un registro condiviso (ad esempio per finalità di vigilanza)
A_1	Creazione di un token con certe caratteristiche (con o senza diritti incorporati)
A_2	Implementazione degli smart contracts
A_3	Interfaccia con altri sistemi (interoperabilità)
A_4	Identificabilità dell'utente finale
A_n	Altre attività

La seconda parte riguarda il grado di decentramento delle DLT. In modo semplificato possono essere individuate tre configurazioni: parzialmente accentrato, ove esiste un soggetto o un nodo con un ruolo di leadership dominante e dove soltanto soggetti autorizzati hanno accesso ai dati in lettura; sistema policentrico dove soltanto un numero limitato di nodi (ad esempio *mining pools* o DLT con organi di controllo) ha accesso ai dati in scrittura, ma dove qualsiasi soggetto ha accesso ai dati in lettura; sistema decentrato, caratterizzato da un numero alto di nodi che operano nel network senza vincoli entrata e di uscita e in un modo tendenzialmente paritetico. La prima configurazione corrisponderebbe alle DLT *permissioned* (ad esempio, Corda, IBM Blockchain, Quorum); la seconda a la terza (sia *permissionless* che *permissioned*), potrebbero essere, ad esempio, rispettivamente, Binance ed Ethereum. A ciascuna configurazione può corrispondere una diversa tipologia di meccanismo di consenso.

La *terza parte* della mappa rappresenta i meccanismi di "governo" della DLT, che chiamiamo $\{R_i\}$. Le DLT, infatti, possono avere una varietà di meccanismi di governo e controllo, attraverso gruppi abilitati di validatori, comitati tecnici, nonché sistemi *open source* di sviluppatori del protocollo che interagiscono attraverso modalità più o meno decentrate (ad esempio un referendum). I meccanismi di governo possono essere, come specificato in precedenza, sia *on-chain* che *off-chain*. Chiaramente una DLT "robusta" (il cui grado di robustezza è funzione delle attività che deve supportare) deve simultaneamente avere una buona governance e un buon presidio dei rischi che potenzialmente genera.

Figura 2- Mappa delle attività e governance delle DLT



Esempi

$(A_0 \wedge A_1 \wedge A_2 \wedge A_0) \quad (R_0)$

$(A_0 \wedge A_1 \wedge A_2 \wedge A) \quad (A_2 \wedge A_1) \quad (R_1 \wedge R_4 \wedge R) \quad ain$

$(A_0 \wedge A_1 \wedge A_3 \wedge A \wedge A) \quad (A_2 \wedge A_2) \quad (R_1 \wedge R_2 \wedge R) \quad ain$

Legenda

$\{A_i\}$

$\{R_i\}$

$\{ \ _i\}$

AND

$OR =$

OR

Quanto detto è rappresentato in Figura 2. La mappa funziona come un circuito di commutazione o logico (da notare gli "interruttori" _ _). Il circuito viene percorso da sinistra verso destra, iniziando dal *white paper* (in simboli WP), che rappresenta il documento illustrativo della DLT e dell'intero processo di governo, implicito o esplicito. Ogni DLT opera attivando alcune funzioni o "attività" $\{A_i\}$, come mostrato nella prima parte del circuito; la sua configurazione (grado di decentramento dei nodi e meccanismo di consenso) viene rappresentata nella seconda parte della mappa; infine la terza parte del circuito riguarda l'insieme di processi e regole interne $\{R_i\}$. L'intero circuito si chiude *se e solo se* si chiudono simultaneamente il circuito in alto, nel mezzo e in basso della mappa.

Vediamo, ad esempio e in modo semplificato, come la mappa riesca a rappresentare la blockchain di Bitcoin. Nella parte alta del circuito, essa attiva tre funzionalità, quella di creare un registro crittografico distribuito (attività A_0), quella di generare un token senza diritti, Bitcoin (attività A_1) e quella di finalizzazione probabilistica dei blocchi di transazioni (attività A_6). Nella parte centrale del circuito, si chiudono gli interruttori che corrispondono a una blockchain di tipo *permissionless public* (P_2) con meccanismo di consenso basato su PoW (X_0). Il circuito non prevede nessuno organo di governance (R_0). Date le sue caratteristiche, Bitcoin non risulta predisposto per gestire un processo ordinato e predefinto di *upgrading*, quindi può essere soggetto a biforcazioni ($\bar{P}$). La DLT di Bitcoin dunque è rappresentabile con la seguente formula: $(A_0 \wedge A_1 \wedge A_6) \wedge (P_2 \wedge \mathrm{X}_0) \wedge R_0 \wedge \bar{P}$.

Le DLT con funzionalità più complesse attiveranno altri percorsi con strutture di governo più articolate. Inoltre, tra i requisiti imposti dal regolatore vi potrebbe essere quello di modificabilità del protocollo nativo P. In questo caso il circuito si chiude solo in presenza di un protocollo di consenso predisposto in tal senso o in grado di ottenere lo stesso risultato durante il ciclo di vita della blockchain, secondo un processo ricorsivo o adattivo.[13] Tale proprietà richiede la presenza di un protocollo di consenso e di specifici meccanismi di governance. La recente "migrazione" di Ethereum dalla PoW alla PoS, mostra che il cambiamento del protocollo nativo è possibile, anche se detto processo è molto complesso. Un cambiamento strutturale della DLT porta necessariamente a una variazione della mappa (i simboli $\bar{P}$ e ΔP indicano questi casi). Questa metodologia potrebbe essere utilizzata nei *white paper*, permettendo un facile confronto tra DLT e la loro evoluzione temporale.

L'approccio suggerito è molto flessibile e dovrebbe essere in grado di "mappare" ogni tipo di DLT, adattando opportunamente la mappa in modo da cogliere, anche nel dettaglio, tutte le possibili configurazioni delle DLT. Infatti questa metodologia può essere usata per includere sottoinsiemi di circuiti logici aventi altre attività o funzioni. Ad esempio il circuito potrebbe includere oltre alle due macro-classi di token (con o senza diritti incorporati) altre tipologie di critpo-asset[14]; potrebbe specificare se ha una "finalità" probabilistica o deterministica; potrebbe indicare esplicitamente le tipologie di voto[15], ecc. L'uso dei circuiti logici permette di rappresentare, con un buon grado di approssimazione, ogni DLT in modo sintetico e rigoroso anche attraverso una formula algebrica (vedi Figura 2). Di seguito viene mostrata, a scopo esemplificativo, la mappatura di due DLT complesse: Ethereum e Polkadot.

[13] Su questo aspetto si rimanda a: Gola, C., et al. (2023), op cit., paragrafo 4.3.
[14] Ivi, Box 2.
[15] Ivi, Box 4.

4 Ethereum

Ethereum è un progetto informatico open source lanciato nel 2015 da un informatico russo/canadese, Vitalik Buterin, con l'obiettivo di utilizzare la tecnologia blockchain per un insieme più ampio di scopi rispetto a quelli inizialmente previsti dal protocollo di Nakamoto. L'idea è stata quella di disegnare una DLT *premissionless*, non solo pubblica (aperta sia in scrittura che in lettura), ma anche flessibile e pienamente programmabile[16]. Ethereum fornisce la base su cui impiantare programmi vincolanti per le parti sulla base di procedure predefinite (*smart contracts*).

4.1 Attività della DLT

Il protocollo Ethereum:

- detiene un registro distribuito di transazioni. Tale registro è pubblico, contiene le transazioni relative al token nativo oltre che le transazioni dei token implementati sulla piattaforma di Ethereum attraverso gli *smart contracts*;
- crea un token, chiamato Ether (in simboli ETH), che: 1) permette di partecipare alla *governance* del sistema, dando la facoltà di validare le transazioni, previo un deposito cauzionale (detto *staking*) di almeno 32 ETH; 2) può essere utilizzato per pagare le commissioni delle transazioni sulla rete ETH o per eseguire gli *smart contracts* sulla blockchain Ethereum; questi ultimi permettono agli sviluppatori di creare cripto-attività *on-chain*, ad esempio nell'ambito della finanza decentralizzata (DeFi);
- permette la creazione di entità governate da codice informatico (*Decentralized Autonomous Organizations*, DAO), sempre attraverso l'uso di *smart contracts*[17].

4.2 Grado di decentramento

Stabilire il grado di decentramento di Ethereum è attualmente piuttosto difficile, anche a causa della recente transizione del protocollo dal meccanismo di consenso PoW a quello PoS. Infatti, prima della transizione a PoS, la validazione dei blocchi della blockchain di Ethereum avveniva attraverso il *mining*. Quest'ultimo è un processo competitivo che richiede, a ciascun nodo che vuole partecipare al processo di aggiornamento del registro condiviso, l'uso di una grande quantità di energia elettrica, oltre alla necessità di utilizzare processori sempre più potenti e costosi. Peraltro, la ricerca di economie di scala o di rete ha comportato la creazione dei cosiddetti *mining pools*[18].

Tra i partecipanti al network di Ethereum è stata quindi pressante l'esigenza di promuovere una transizione verso un protocollo di consenso meno concentrato e soprattutto avente un minore impatto ambientale. Da diversi anni la comunità di Ethereum stava lavorando per realizzare questa transizione in modo sicuro, condiviso e robusto dal punto di vista della governance del sistema.

La transizione dal protocollo PoW a quello PoS. Il 15 settembre 2022, la blockchain di Ethereum è passata da un meccanismo di consenso PoW a un consenso PoS unendo Ethereum Mainnet (la blockchain principale) con la PoS Beacon Chain (una catena costruita appositamente per il passaggio

[16] A tal fine sono stati sviluppati appositi linguaggi di programmazione (Solidity e Vyper).
[17] Queste ultime due caratteristiche vengono identificate nella mappa di cui sopra con la dicitura "creazione di smart contract", infatti nel caso di Ethereum sia la creazione di nuovi token (denominati con lo standard ERC-20) sia la creazione di DAO avviene sempre per il tramite dell'attività relativa alla scrittura di Smart Contract.
[18] I *mining pools* sono gruppi di miner che mettono in comune le risorse computazionali per aumentare la probabilità di vincere le ricompense di blocco. Quando un *pool* trova con successo un blocco, i miner suddividono la ricompensa in modo imparziale tra tutti i membri del *pool*, in base alla quantità di lavoro con cui ha contribuito ogni membro.

da PoW a PoS). La fusione ha ridotto drasticamente il consumo di energia della rete Ethereum, che è stata a lungo una delle principali critiche mosse al network. L'introduzione del meccanismo di consenso PoS, secondo quanto evidenziato dagli sviluppatori del network, si inserisce all'interno di un più ampio progetto finalizzato ad aumentare l'efficienza, la sicurezza e la scalabilità della rete.

La governance di Ethereum basata su PoS. Il nuovo algoritmo PoS di Ethereum utilizza un processo che seleziona, tra i numerosi nodi attivi in rete, quelli che hanno la fortuna di essere scelti come "validatori" dei blocchi per un breve periodo di tempo. La selezione avviene tramite un processo casuale (simile ad una lotteria). A differenza del meccanismo PoW, tale algoritmo non richiede una particolare potenza di calcolo computazionale e, pertanto, limita sensibilmente il consumo energetico e impedisce la concentrazione del potere di validazione in capo a pochi nodi. Nei sistemi PoS, l'inserimento di nuovi blocchi nella blockchain viene chiamato "*forging*" anziché *mining*; i nodi che intendono partecipare al processo di *forging* devono depositare (ossia mettere in "*staking*") un minimo di 32 ETH all'interno di un indirizzo pubblico del network. Benché sia possibile depositare un quantitativo di ETH superiore all'ammontare minimo previsto, ciò non incrementa le probabilità di un nodo di venir selezionato come validatore e agire da *forger* di un blocco; tale misura è stata escogitata per mitigare fenomeni di concentrazione del processo di validazione delle transazioni in capo a pochi soggetti detentori di significative quantità di ETH.

Ogni 12 secondi un nodo con almeno 32 ETH in *stake* viene scelto casualmente per validare un blocco che in seguito trasmette al resto dei partecipanti del network apponendovi la propria "*digital signature*". Le transazioni contenute in quest'ultimo blocco vengono nuovamente verificate da un gruppo di validatori, anch'essi selezionati casualmente, deputati ad esprimere un "voto" finale sulla loro validità. I blocchi reputati corretti dalla maggioranza vengono dunque aggiunti alla blockchain, mentre gli altri vengono scartati. Poiché ogni blocco ha un proponente verificabile, eventuali comportamenti malevoli o fraudolenti assunti da questo, sono disincentivati attraverso un meccanismo sanzionatorio che può arrivare all'esclusione del validatore dal network (c.d. *slashing*) con conseguente perdita degli ETH posti in *stake*.

4.3 Governance

Pur essendo un protocollo *permissionless* pubblico, la struttura di governo di Ethereum è assai complessa. Infatti, mentre il meccanismo di consenso sopra descritto è completamente gestito *on-chain*, le principali decisioni di governance inerenti lo sviluppo e le modifiche del protocollo sono gestite *off-chain* attraverso il coinvolgimento di una pluralità di stakeholders con ruoli differenti. Il processo inizia con la pubblicazione sul web di proposte di miglioramento di Ethereum (*Ethereum improvement proposal,* EIP)[19] che possono essere formulate da ogni partecipante alla community di Ethereum[20]. Le proposte avanzate vengono poi discusse dai partecipanti della rete su forum pubblici, ma le decisioni definitive su quali EIP implementare e con che tempistiche sono prese dal team di *core developer* del network. Ciò in quanto non è stata formulata una procedura definita su come gestire le proposte controverse e le situazioni di conflitto tra i vari stakeholder interessati dall'implementazione di un determinato EIP. Di seguito vengono descritti altri aspetti relativi alla governance di Ethereum.

Ethereum Foundation. In primo luogo vi è una fondazione senza scopo di lucro, Ethereum Foundation, che di fatto sarebbe presieduta da Vitalik Buterin. La Fondazione non possiede la proprietà intellettuale del software Ethereum, né lo controlla direttamente. Lo scopo della fondazione è quello di supportare l'infrastruttura informatica nella sua manutenzione ordinaria e nei suoi

[19] Gli EIP sono standard tecnici per la predisposizione di proposte relative anche alle modifiche del protocollo come l'implementazione di nuovi processi e funzionalità.
[20] Dato l'elevato livello tecnico richiesto per inviare un'EIP ben fatta, storicamente gran parte degli autori di EIP sono stati sviluppatori di applicazioni o protocolli.

eventuali miglioramenti (*upgrading*) strutturali, a beneficio della comunità degli utenti. Appartengono alla Fondazione, oltre al fondatore, anche programmatori, società, imprenditori che possono detenere quote dei token emessi dal protocollo stesso. La maggioranza dei progetti blockchain, non solo DeFi, ma anche per altre finalità, utilizza Ethereum, che quindi si configura come una infrastruttura alla base di un intero ecosistema. La Fondazione alloca anche risorse finanziarie, denominate in ETH, attraverso procedure decisionali, non di facile individuazione, che stabiliscono quali sono i progetti più meritevoli.

Core Developers. I cambiamenti del protocollo nativo avvengono attraverso l'interazione tra la comunità degli sviluppatori, che fanno proposte di cambiamento, e un insieme ristretto degli stessi ("*core developers*", che include anche Vitalik Buterin). Il gruppo di *core devolopers*, costituito da oltre 200 membri, si riunisce mensilmente. Il processo appena descritto avviene *off-chain*, nel senso che non comporta un'automatica e vincolante integrazione delle nuove procedure nel protocollo nativo; per fare ciò, nel passato regime basato sulla PoW era necessaria la maggioranza del potere di calcolo dei *full-nodes* (nodi "validatori"). Questi ultimi devono necessariamente essere d'accordo prima, durante e dopo il processo di *upgrading* del protocollo. Qualora non vi sia un accordo si determina una duplicazione della blockchain, con conseguente creazione di un nuovo token. Con il passaggio da PoW a PoS per apportare modifiche al protocollo nativo, invece che la maggioranza del potere di calcolo è necessaria la maggioranza dei token messi a deposito (*staking*) dai validatori.

Ethereum Classic. Come menzionato sopra, in caso di disaccordo tra la comunità dei validatori (prima *miners*) su un qualche aspetto riguardante il codice di Ethereum, esiste la possibilità che la community, e di conseguenza la blockchain, si biforchi, come è già successo in passato. L'attuale blockchain di Ethereum è nata proprio da un *fork* e non contiene la storia inalterata della rete stessa, che rimane invece nella blockchain oggi nota come Ethereum Classic. Nel 2016, infatti, la fondazione Ethereum, a seguito di un hackeraggio di un progetto di terze parti (con una conseguente perdita di 50 mln di euro in controvalore ETH), ha creato una nuova versione della blockchain principale con un cambiamento di stato che ha, di fatto, riparato al danno. Una parte – minoritaria – della community dei *miners* (e degli utilizzatori) ha tuttavia deciso di ritenere illegittimo il cambiamento di stato, promulgando il concetto "*The code is law*", continuando a partecipare al network Ethereum originale ri-denominato Ethereum Classic.

Formula logica. Utilizzando la mappa descritta nel paragrafo 3, le caratteristiche della rete Ethereum possono essere riassunte con la seguente formula:

$$(A_0 \wedge A_1 \wedge A_2 \wedge A \qquad _2 \quad _1 \quad (R_1 \wedge R_4 \wedge R \qquad _{ain} \quad \bar{P}.$$

5 Polkadot[21]

Polkadot è un sistema che permetterebbe a diverse blockchain basate anche su protocolli di consenso differenti (es. PoW, PoS, PoA, sia pubbliche che private) di comunicare tra loro in un ambiente che sarebbe sicuro e affidabile[22]. Esso pertanto intenderebbe creare una infrastruttura di mercato che, a livello globale, renderebbe compatibili (interoperativi) diversi tipi di blockchain o DLT.

Il sistema Polkadot si basa su una blockchain principale, denominata Relay chain, creata dai promotori dell'iniziativa, e blockchain secondarie, denominate Parachains, che si integrano con

[21] Quanto scritto di seguito si basa in larga misura sulla documentazione ufficiale del network Polkadot https://polkadot.network/.
[22] https://wiki.polkadot.network/docs/learn-architecture

quella principale. La Relay chain è costruita per coordinare un intero ecosistema ove numerose blockchain, create da vari gruppi di sviluppatori, si collegano al sistema Polkadot.

Le Parachains collegate alla Relay chain condividono lo stesso livello di sicurezza. Se, per qualsiasi motivo, la Relay chain dovesse eliminare una transazione, o qualsiasi altro tipo di aggiornamento dei registri condivisi, anche tutte le Parachains collegate sarebbero costrette ad eliminarla. Ciò rende l'intero ecosistema Polkadot coerente nelle sue parti.

5.1 Attività della DTL

Il protocollo Polkadot:

- detiene un registro distribuito di transazioni. Tale registro è pubblico, contiene le transazioni relative alle diverse Parachains che fanno parte del protocollo e qualsiasi *full node* del sistema può candidarsi per contribuire temporaneamente alla scrittura dei blocchi del registro;
- crea un token, chiamato DOT, che: 1) permette di partecipare alla governance del sistema, dando la facoltà di candidarsi come valicatore o di votare le proposte per apportare cambiamenti al protocollo nativo; 2) può essere utilizzato come deposito cauzionale (*stake*) per potere operare nel sistema; 3) permette di aggiungere nuove Parachains al sistema;
- offre un servizio di *crowdfunding* per le Parachains che non possono permettersi uno slot all'interno del protocollo;
- fornisce un servizio di custodia (*wallet*)[23];
- permette il trasferimento di token tra diverse Parachains, tra Parachains e Relay chain e anche da blockchain esterne tramite apposite applicazioni dette *bridge*.

Il sistema Polkadot si basa su un insieme di stakeholders e organi gestionali con funzioni distinte: vi sono i "validatori"; i "nominatori" (cha supportano in modo tendenzialmente equi-distribuito i validatori); e i "collettori" (che raccolgono i blocchi provenienti dalle Parachains da inserire nel protocollo principale); i "pescatori" preposti a intercettare e sanzionare i nodi che non si comportano in modo corretto.

Vi sono inoltre organi che, in modo algoritmico, danno struttura di governo all'intero processo. Essi sono il Referendum, il Consiglio e il Comitato tecnico. Il sistema, ancora in fase di evoluzione, ambirebbe a creare un sistema equilibrato e completamente automatizzato, senza cioè la necessità di avere organi presieduti da persone o soggetti aventi un ruolo privilegiato, grazie al ruolo svolto dal referendum.

5.2 Grado di decentramento

Polkadot è una DLT *permissionless* pubblica caratterizzata da un alto livello di decentralizzazione, derivante soprattutto dall'introduzione di un protocollo chiamato *Nominated Proof of Stake* (NPoS). L'obiettivo di tale protocollo è l'elezione periodica di un numero definito di validatori, tra un numero indefinito di possibili candidati, responsabili della registrazione di nuove transazioni sulla Relay chain. Tali transazioni includono quelle relative alle diverse Parachains che fanno parte del protocollo Polkadot. Seppur simile alla tradizionale PoS, in quanto si basa sul deposito (*stake*) di token DOT a

[23] Il servizio di custodia e il software integrato per gestire i referendum sono tutti rilasciati dalla Web3 Foundation, una società che partecipa al network Polkadot implementando modifiche software che devono essere approvate tramite referendum. Si occupa anche di rilasciare informazioni dettagliate sul funzionamento dell'ecosistema.

garanzia dell'onesto operato dei validatori, presenta una sostanziale novità, che risiede nella figura dei nominatori.

***Nominated Proof of Stake* (NPoS) -** I validatori[24] sono nodi temporaneamente incaricati della produzione di blocchi sulla Relay Chain, che includono le transazioni effettuate sulle diverse Parachains, anch'esse parte del protocollo. Qualsiasi nodo che possieda l'infrastruttura tecnologica per eseguire in modo continuativo le funzioni richieste dalla Relay chain, può candidarsi come validatore. Per candidarsi i validatori bloccano una certa quantità di DOT, che gli verrà restituita al termine del proprio operato a meno di comportamenti scorretti, insieme a una ricompensa per il lavoro svolto. L'attività di un validatore dura circa 24 ore (detta "era"), dopodiché si procede a una nuova elezione.

I nominatori[25] sono dei nodi che partecipano all'elezione dei validatori supportando economicamente un insieme di candidati anch'essi tramite un deposito cauzionale (un collaterale) dato da una certa quantità di DOT. Tale deposito viene quindi ripartito tra i candidati prescelti dal nominatore e si somma al deposito di partenza dei candidati. Se i validatori prescelti dal nominatore vengono effettivamente eletti e producono almeno un blocco, una parte della ricompensa dei validatori va al nominatore, in proporzione alla quantità di DOT depositati dallo stesso. Se uno dei validatori si comporta in modo scorretto viene punito con il sequestro dei DOT depositati; lo stesso principio si applica ai nominatori che l'hanno supportato. Pertanto i nominatori sono incentivati a scegliere i candidati validatori in base alla quantità di *stake* che supporta il candidato e alle sue performance passate (indici della sua onestà) e alle commissioni richieste dal validatore.

Il sistema appena descritto è implementato da un algoritmo denominato *Phragmén sequenziale*[26], il cui obiettivo ultimo è quello di massimizzare il numero di token bloccati dai validatori, garantendo nel contempo il più elevato livello possibile di equi-distribuzione degli *stake*. Ciò garantirebbe decentralizzazione e sicurezza: la prima perché l'algoritmo di elezione garantisce che anche le minoranze (validatori che sono supportati da pochi nominatori) siano proporzionalmente rappresentate se associate a una quantità sufficiente di token; la seconda perché, con la massimizzazione del deposito minimo, ogni validatore è supportato da una quantità di DOT molto grande, dunque l'elezione di un validatore malevolo comporterebbe l'investimento di una grande quantità di DOT (che rischierebbe di essere perso).

Un ulteriore elemento che favorisce la decentralizzazione del sistema è il fatto che le ricompense ricevute dai validatori quando registrano un blocco sulla Relay Chain sono indipendenti dalla quantità di DOT posti a supporto del validatore. Ciò comporta che i nominatori dei validatori più popolari ricevano una ricompensa inferiore (perché dovrà essere ripartita tra più sostenitori) e di conseguenza sono incentivati a non votare sempre per lo stesso validatore (che comporterebbe la centralizzazione come nel caso delle *mining pools*) ma a diversificare sufficientemente i loro voti.

Il coordinamento tra Relay Chain e Parachains. Come già descritto in precedenza, il ruolo dei validatori è validare i blocchi della Relay Chain, contenenti le transazioni effettuate sulle singole Parachains. Dato che i validatori non hanno un database sincronizzato di tutte le Parachains (poiché ciò sarebbe troppo oneroso), si affidano ai nodi collettori[27] per la creazione dei blocchi delle Parachains. I validatori controllano e sono responsabili delle corrette transizioni di stato della

[24] https://wiki.polkadot.network/docs/learn-validator
[25] https://wiki.polkadot.network/docs/learn-nominator
[26] Il metodo di Phragmén è un problema di ottimizzazione complesso e, al fine di mantenere un tempo di blocco costante, Polkadot calcola il risultato off-chain e invia una transazione per proporre l'insieme dei vincitori. https://wiki.polkadot.network/docs/learn-phragmen
[27] https://wiki.polkadot.network/docs/learn-collator

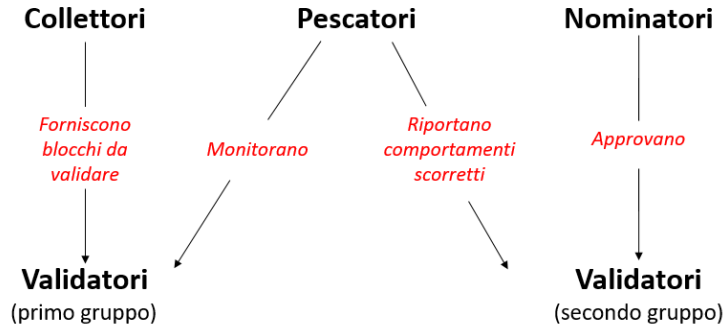
Parachain; tale attribuzione di responsabilità è assegnata casualmente e cambia ogni volta che viene creato un nuovo blocco. Più validatori sono generalmente responsabili di una stessa Parachain.

I collettori. Il sistema prevede anche la figura dei *collettori* responsabili del funzionamento dell'insieme delle varie Parachains; essi raccolgono le transazioni effettuate sulle Parachains dagli utenti e producono prove di transizione dello stato – ovvero, tramite uno specifico algoritmo, la prova che il nuovo blocco è coerente con il blocco precedente, relativamente alla stessa Parachain – per i validatori della Relay Chain. In altre parole, i collettori aggregano le transazioni delle Parachains in "candidati blocchi Parachains" e producono prove di coerenza con i blocchi validati in precedenza, in modo che i validatori della Relay Chain possano inserire i blocchi nella Relay Chain. I collettori operano come *full nodes* sia della Relay Chain che della particolare Parachain a cui sono collegati; il che significa che conservano tutte le informazioni necessarie per essere in grado di creare nuovi blocchi ed eseguire transazioni più o meno allo stesso modo dei *miners* che operano sulle blockchain basate sulla PoW. A differenza dei validatori, i collettori non sono preposti a garantire la sicurezza alla rete. Se un blocco Parachain non è valido, verrà rifiutato dai validatori.

I nodi pescatori. Rappresentano un'addizionale misura di sicurezza del sistema. Il loro ruolo è scovare validatori che hanno un comportamento scorretto. I pescatori sono nodi completi di Parachains, ma, a differenza dei validatori, svolgono un ruolo diverso rispetto alla rete Polkadot. Invece di impacchettare le transizioni di stato e produrre i successivi blocchi delle Parachains, i pescatori osservano l'intero processo e si assicurano che non siano incluse transizioni di stato non valide. Attualmente la figura del pescatore non è stata ancora resa operativa nella rete Polkadot, anche se nel design complessivo dell'infrastruttura è stata prevista.

Lo schema in Figura 3, tratto dal WhitePaper di Polkadot[28], rappresenta sinteticamente il ruolo del nominatore, validatore, collettore e pescatore.

Figura 3 – Ruoli degli attori volti a garantire il consenso e la sicurezza della rete



Creazione e finalizzazione dei blocchi della Relay Chain. Il meccanismo di consenso del protocollo Polkadot regola la creazione dei blocchi della Relay Chain e la loro finalizzazione. Quest'ultima in generale può essere di due tipi: probabilistica o deterministica. Con la finalizzazione probabilistica ogni nodo sa che un blocco è finalizzato con una certa probabilità. È il caso di Bitcoin, ove, con il passare del tempo e il crescere della catena, diminuiscono le probabilità che un blocco creato in passato possa non essere più valido (sarebbe troppo oneroso tornare indietro e cambiare la storia del sistema). Tuttavia non si è mai sicuri al 100%. Con la finalizzazione deterministica invece, una volta che un blocco viene finalizzato tale stato diventa permanente e non può più essere cambiato. Lo svantaggio in questo caso è che il processo di creazione di nuovi blocchi potrebbe diventare molto

[28] https://polkadot.network/PolkaDotPaper.pdf

lento: bisogna attendere di avere una completa finalizzazione del blocco precedente per poterne aggiungere un altro (dato che è irreversibile). In Polkadot si vogliono sfruttare i vantaggi di entrambe le tipologie di finalizzazione: dell'approccio probabilistico l'agilità e la velocità, dell'approccio deterministico il fatto che agevolerebbe le comunicazioni con blockchain al di fuori della Relay chain. Per farlo i processi di creazione e di finalizzazione dei blocchi vengono separati e sono l'uno indipendente dall'altro: il primo è denominato *Blind Assignment for Blockchain Extension* (BABE), il secondo *GHOST-based Recursive Ancestor Deriving Prefix Agreement* (GRANDPA).

Processo BABE[29]**.** Ogni "era" (periodo di validità in carica di un validatore) è divisa in "epoche", ogni epoca è divisa in più finestre temporali (*slot*); ogni *slot* corrisponde alla creazione di un blocco. All'inizio dell'epoca, ai validatori viene assegnato in maniera casuale uno *slot*. Più validatori possono operare nello stesso slot. Quando arriva il proprio turno, il validatore crea il blocco e lo aggiunge alla catena di blocchi più lunga che contiene l'ultimo blocco finalizzato con l'algoritmo GRANDPA. Si osserva che l'ultimo blocco finalizzato in molti casi non coincide con l'ultimo blocco creato: infatti ci saranno gli altri blocchi che sono stati creati nella stessa epoca ma in slot precedenti e non sono stati ancora finalizzati. Possono crearsi delle *fork* in quanto, ad esempio, possono esserci più validatori responsabili di uno stesso slot e che quindi creano allo stesso tempo blocchi diversi.

Processo GRANDPA[30]**.** Il processo GRANDPA permette ai validatori di decidere quale delle catene di blocchi create con BABE sarà finalizzata. Quando una catena raggiunge i 2/3 dei voti, allora essa e tutti i suoi blocchi non ancora finalizzati entreranno a far parte della Relay chain. Per il funzionamento del protocollo è indispensabile che il numero di validatori sia limitato; tale numero è fissato a priori. La finalizzazione si basa sull'ipotesi fondamentale che almeno 2/3 dei validatori siano onesti. In tal senso, questa DLT può essere classificata tra quelle aventi un processo di finalizzazione deterministico.

5.3 Meccanismi di governance[31]

Una volta chiariti gli elementi essenziali della DLT Polkadot, è possibile studiarne la governance. È necessario premettere il sistema di governo algoritmico è ancora in fase di sviluppo, ma in prospettiva intenderebbe poter funzionare in modo completamente automatizzato tramite l'utilizzo del solo Referendum, con l'obiettivo di evitare che un soggetto (o una coalizione di soggetti) possa controllare il network. Attualmente i principali strumenti di governance di Polkadot sono il Referendum, il Consiglio e il Comitato tecnico**.**

Referendum. Uno dei problemi più complessi delle DLT è la definizione di un sistema di governo in grado di gestire eventuali aggiornamenti o cambiamenti strutturali del protocollo informatico. In Polkadot, ogni modifica al protocollo base (la Relay chain) deve essere approvata attraverso una votazione (referendum) basata sul peso dello *stake* dei partecipanti che in questa struttura completamente pubblica può essere qualsiasi persona dotata di un computer e disposta ad acquistare attraverso una applicazione predisposta dalla DLT un certo numero di token generato dalla DLT (i DOT), ovvero i cosiddetti DOT *holders*. Ogni referendum ha sempre associata una specifica proposta di variazione di una parte del codice della Relay chain e le risposte possibili ai referendum sono sempre di tipo binario, ovvero è possibile rispondere alla proposta con un "si", con un "no", oppure con l'astensione.

I referendum possono essere attivati in diversi modi: tramite una proposta pubblica, tramite una proposta da parte del Consiglio, e tramite una proposta di "emergenza" da parte del Comitato Tecnico,

[29]https://wiki.polkadot.network/docs/learn-consensus#badass-babe-sassafras, per una trattazione più tecnica cfr. https://research.web3.foundation/en/latest/polkadot/block-production/Babe.html

[30]https://wiki.polkadot.network/docs/learn-consensus#finality-gadget-grandpa, per una trattazione dettagliata vedere anche https://github.com/w3f/consensus/blob/master/pdf/grandpa.pdf

[31] https://wiki.polkadot.network/docs/learn-governance

stante la pre-approvazione da parte del Consiglio. Ogni 30 giorni vi è un referendum (tranne per le proposte di emergenza, per le quali può essere fatta un'eccezione). La proposta da discutere viene scelta in modo alternato dalla lista delle proposte del Consiglio o dalla lista delle proposte pubbliche (viene scelta quella che ha ricevuto appoggio maggiore).

Ogni referendum ha un periodo attuazione, conteggiato come il periodo compreso tra la fine del referendum e l'attuazione delle modifiche proposte (assumendo che la proposta del referendum venga approvata).

I periodi temporali, in riferimento al referendum, si dividono in due tipologie: il ciclo di voto e il ciclo di proposta. All'interno di ogni ciclo di proposta chiunque può proporre un referendum "bloccando" un certo ammontare di token DOT; se qualche altro partecipante al network è d'accordo con la proposta depositata può aderire "bloccando" token DOT accanto a quelli bloccati dal proponente. Finito il ciclo di proposta vengono selezionati i referendum su cui votare, andando a selezionare i refendum con più token DOT bloccati su esso.

Qualsiasi utente del network che possiede dei DOT, può votare un referendum ponendo gli stessi a deposito cauzionale per un certo periodo di tempo. In particolare il peso del voto sarà determinato dalla seguente formula matematica:

$$OT \qquad *$$

In questo modo i partecipanti al network con un numero minore di DOT possono influenzare il voto di un referendum maggiormente di chi possiede maggiori DOT, bloccando i propri token per un periodo di tempo maggiore[32].

Il Consiglio. Il Consiglio è un organo composto al momento da 13 membri responsabili di una serie di funzioni di governance, eletti con intervalli di tempo regolari tra i nodi detentori di DOT.

Il Consiglio ha le seguenti funzioni: proporre referendum utili alla comunità, eliminare referendum dannosi o inutili, eleggere il comitato tecnico. Oltre a ciò, il Consiglio ha la facoltà di utilizzare i fondi di una tesoreria denominati esclusivamente in DOT, "bloccati" nella Relay chain e non accessibili in modo discrezionale (non meramente algoritmico). Il fondo è alimentato in parte dalle commissioni sulle transazioni (*fees*) e in parte dalle "sanzioni" derivanti da per comportamenti illeciti. Al fine di proporre un nuovo referendum, la maggior parte dei membri del Consiglio deve essere favorevole. Un membro del Consiglio può esercitare il diritto di veto una sola volta nel caso la proposta di referendum venda ripresentata.

A seconda della percentuale dei membri del Consiglio favorevoli alla proposta del referendum possono essere attivati diversi *schemi di conteggio*[33]; in particolare le mozioni del Consiglio che passano con una maggioranza di 3/5 (60%) – ma senza raggiungere l'unanimità – si trasformeranno in un referendum pubblico con schema di conteggio di semplice maggioranza, mentre nel caso in cui tutti i membri del Consiglio votino a favore di una mozione da trasformare in referendum verrà adottato uno schema di conteggio dove sarà matematicamente più difficile far rigettare la proposta.

---

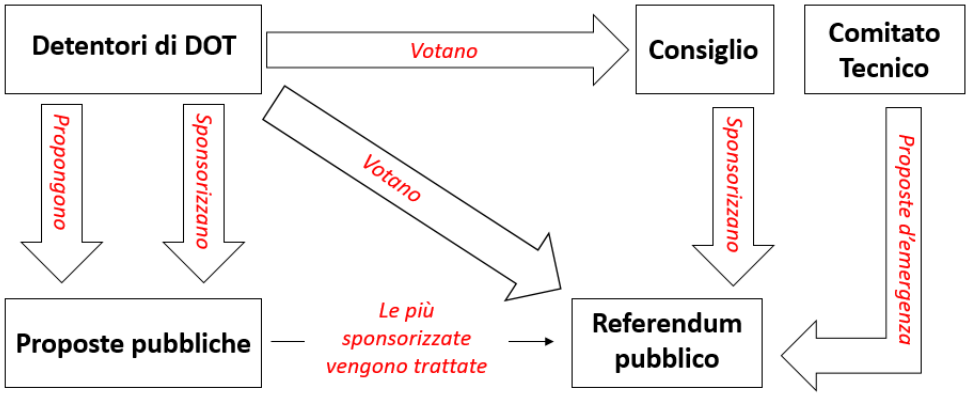
[32] Ad esempio supponiamo che Pietro voti con 10 DOT con un periodo di blocco di 6 mesi, mentre Mauro voti con 20 DOT per un periodo di blocco di 1 mese: Pietro, avendo bloccato per più tempo i token, avrà una influenza maggiore sull'esito del referendum: $Peso\ del\ voto\ di\ Pietro = 10 * 6 = 60$; $Peso\ del\ voto\ di\ Mauro = 20 * 1 = 20$.

[33] Se il referendum viene proposto dai stakeholder la mozione proposta viene approvata se si verifica la seguente condizione, denominata "positive tornout bias", $\frac{votanti\ contro}{\sqrt{\ umero\ di\ votanti}} < \frac{vot\ \ nti\ a\ \ avore}{\sqrt{\ umero\ di\ toke}}$; se il referendum viene proposto dal Concilio con unanimità la mozione proposta viene approvata se si verifica la seguente condizione, denominata "negative tornout bias", $\frac{votanti\ contro}{\sqrt{\ umero\ di\ toke}} < \frac{votanti\ a\ \ avore}{\sqrt{\ umero\ di\ votanti}}$; se il referendum viene proposto dal Concilio con un accordo di maggioranza la mozione proposta viene approvata se si verifica la seguente condizione, denominata "maggioranza semplice", $votanti\ a\ favore > votanti\ contro$.

Comitato Tecnico. Il Comitato Tecnico è composto da un insieme di membri eletti, come detto, dal Consiglio. Il suo scopo è quello di scoprire se ci sono problemi tecnici all'interno del sistema (anche a livello di sicurezza) e proporre dunque dei referendum di emergenza. Si possono candidare a farne parte tutti i team che hanno implementato con successo almeno una parte del protocollo Polkadot. Questi team possono essere aggiunti o rimossi dal Comitato con il voto di maggioranza del Consiglio. Una proposta di emergenza per passare al referendum ha bisogno dell'approvazione di almeno ¾ del Consiglio di almeno 2/3 del Comitato. Il referendum in questo caso è molto più rapido e praticamente non c'è alcun tempo di attesa tra il risultato e l'inizio dell'implementazione del cambio.

La Figura 4 mostra uno schema riassuntivo dei meccanismi di governance finora descritti, proveniente dalla documentazione ufficiale di Polkadot.

Figura 4 – Schema funzionamento della governance di Polkadot



Formula logica Utilizzando la mappa descritta nel paragrafo 3, le caratteristiche della rete Polkadot possono essere riassunte con la seguente formula:

$$(A_0 \wedge A_1 \wedge A_3 \wedge A \quad A \quad {}_2 \quad {}_2 \quad (R_1 \wedge R_2 \wedge R \quad {}_{ain} \quad \Delta P.$$

6 Conclusioni

Il lavoro fornisce una metodologia per classificare le DLT in base alle funzioni e attività svolte, alle caratteristiche tecnologiche e alla struttura di governo. Ogni configurazione può essere rappresentata in modo rigoroso e sintetico tramite una formula logica. Vengono inoltre descritte nel dettaglio due DLT *permissionless* particolarmente complesse, Ethereum e Polkadot. La prima associa al protocollo principale organi decisionali e funzionalità che operano al di fuori di esso (*off-chain*); la seconda intenderebbe sviluppare una governance algoritmica completamente (*full algorithmic governance*) iscritta nel protocollo (*on-chain*). L'analisi dei due casi studio permette di valutare come nella pratica, e in quale misura, sia possibile disegnare una architettura informatica preposta a gestire anche in modo algoritmico un registro pubblico senza vincoli di accesso in lettura e scrittura, in grado di soddisfare le seguenti caratteristiche: efficienza tecnologica (scalabilità, elevata capienza e velocità di aggiornamento, flessibilità e interoperabilità, atta a fare "dialogare" sistemi operativi anche differenti); efficienza economica e ambientale (bassi costi fissi e costi operativi); elevato grado di

decentramento e di apertura al pubblico (elevato numero di nodi con diverse funzioni); robustezza e integrità del sistema (tolleranza ad attacchi esterni e malfunzionamenti, irreversibilità, certezza e sincronia delle transazioni, buona struttura di governance).

Quest'ultima caratteristica è ottenuta tramite un insieme complesso di funzioni in larga misura automatizzate (randomizzazione dell'assegnazione dei diritti di voto, dei meccanismi di delega, della attribuzione di ruoli di controllo, di validazione e di aggregazione delle transazioni in modo da evitare concentrazione del potere); introduzione di sistemi d'incentivo o di penali (depositi cauzionali) volti a indurre comportamenti corretti e a premiare un ruolo attivo nella gestione del protocollo informatico da parte dei partecipanti al network più meritevoli.

Si ritiene che lo strumento analitico proposto, opportunamente sviluppato e arricchito, possa facilmente essere impiegato dell'attività di monitoraggio ed eventualmente di sorveglianza su queste infrastrutture informatiche e di mercato.