Il Mulino - Rivisteweb

Danilo Bruschi, Davide Rusconi, Matteo Zoia

La diversificazione delle tecnologie blockchain

(doi: 10.4478/106697)

Osservatorio del diritto civile e commerciale (ISSN 2281-2628)
Fascicolo Speciale, settembre 2022

Ente di afferenza:
()

Copyright © by Società editrice il Mulino, Bologna. Tutti i diritti sono riservati.
Per altre informazioni si veda https://www.rivisteweb.it

Licenza d'uso

Questo articolo è reso disponibile con licenza CC BY NC ND. Per altre informazioni si veda https://www.rivisteweb.it/

La diversificazione delle tecnologie *blockchain*

Danilo M. Bruschi, Davide Rusconi e Matteo Zoia

Blockchain Technologies State of the Art and Evolution: An Overview

The blockchain technology has received in various professional contexts and on media a big emphasis, but it still is an on-progress technology. To be properly exploited, the blockchain technology requires a big effort by the research community to overcome some "technical" criticalities. It also requires time to be assimilated and understood in all its aspects in to be effectively deployed in different application contexts. In the following we will briefly describe several issues which characterize the most famous current implementations as well as the main characteristics of the new ones.

Keywords: Blockchain, Bitcoin, Ethereum, Smart Contract, Consensus Algorithm, Cryptocurrencies.

1. Introduzione

I nostri sistemi economici, legali e politici sono tutti basati su contratti, transazioni e scritture di varia natura e sulla loro rispettiva trascrizione in atti di diversa rilevanza. Questi atti raccontano i diversi eventi che caratterizzano l'evolversi delle nostre società a partire da quelli legati alla vita di ogni singolo cittadino sino alla più complessa organizzazione internazionale. Sono questi atti che governano le interazioni e le scelte tra nazioni, organizzazioni, comunità e individui.

Nel corso di questo ultimo decennio questi strumenti così critici per il funzionamento della nostra società e le burocrazie formate per gestirli si sono dimostrati inadeguati in tempi e modi alla trasformazione che le tecnologie digitali stanno imponendo all'economia e alla società. Nella società digitale in cui le tecnologie hanno annullato i tempi di comunicazione e rivoluzionato le modalità di scambio e acquisizione delle informazioni diventa difficile per cittadini e enti di varia natura il doversi adeguare a procedure e meccanismi ancora molto spesso basati sullo scambio di supporti cartacei. Spesso al centro di questi meccanismi esistono organismi centrali che esercitano la loro riconosciuta funzione di controllo e autorizzazione ma al tempo stesso risultano un freno all'efficientamento e all'economicità dei processi.

 ISSN 2281-2628 © Società editrice il Mulino

La tecnologia *blockchain* potrebbe diventare uno degli strumenti per la soluzione di questi problemi. Questa tecnologia la cui applicazione più significativa è stata sinora la creazione del mercato delle monete virtuali, consente la creazione di un libro mastro digitale in cui possono essere registrate transazioni di varia natura in modo permanente, e verificabile da chiunque ne sia interessato. Non solo, i dati contenuti in una *blockchain* sono protetti da manomissione e, aspetto molto importante, i dati inseriti nella *blockchain* sono validati collettivamente. Fatto estremamente importante e spesso trascurato, tutto quanto sinora detto rimane vero fintantoché la comunità di riferimento della *blockchain* ha una prevalenza di componenti onesta, qualora questo requisito dovesse venire meno molti degli algoritmi che provvedono al funzionamento di una *blockchain* possono essere sovvertiti.

In una *blockchain* la correttezza delle informazioni registrate è costantemente verificata e confermata almeno dalla maggioranza dei nodi eliminando la necessità di un intermediario affidabile, come ad esempio una istituzione pubblica o finanziaria.

In un mondo governato da *blockchain* gli utenti sono rappresentati da pseudonimi, e più in dettaglio da una coppia di chiavi pubbliche e private. Ogni attività che coinvolge almeno due parti nel contesto di applicazione della *blockchain*, una richiesta ad una pubblica amministrazione, un contratto, un pagamento, un acquisto, ecc., è una possibile transazione, che deve essere sottoscritta con la firma digitale delle parti coinvolte, al fine di garantirne l'integrità e la non ripudiabilità. La rete provvederà poi alla convalida e archiviazione di queste transazioni. In questo contesto le intermediazioni non sono più necessarie e individui e organizzazioni possono liberamente interagire lasciando traccia indelebile del loro operato. Questo è l'immenso potenziale della *blockchain*.

Stiamo però parlando di una tecnologia che nonostante l'enfasi ricevuta in diversi contesti professionali e sui media presenta ancora diverse criticità come avremo modo di illustrare. Soprattutto, per poter essere correttamente sfruttata richiede diversi sforzi da parte del mondo della ricerca per superare alcune criticità «tecniche» e dall'altra di essere assimilata e compresa in tutti i suoi aspetti per poter essere efficacemente impiegata nei diversi contesti applicativi.

Nell'ambito di questo contributo dopo aver delineato le principali caratteristica di una *blockchain*, ne illustreremo le sue criticità ed i suoi diversi stadi evolutivi.

2. Che cos'è una *blockchain*

La Figura 1 rappresenta schematicamente una *blockchain*, il cui nome deriva dalla particolare struttura dati con cui è organizzato questo registro digita-

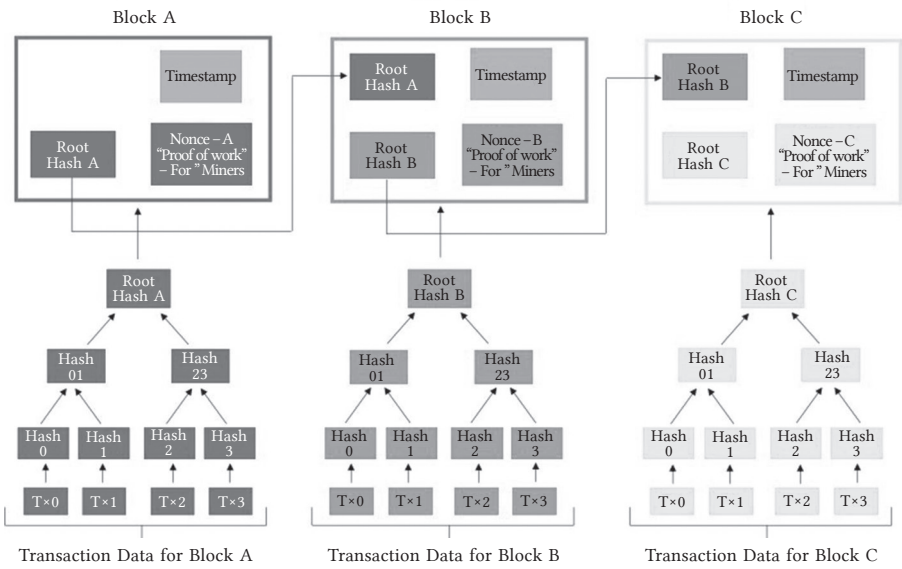

FIG. 1. Rappresentazione schematica di una *blockchain*.

Fonte: cowellclarke.com.au.

le, cioè una catena di blocchi, ciascuno dei quali «legato» indelebilmente ai blocchi aggiunti in precedenza. All'interno di ciascun blocco vi è contenuta dell'informazione, generalmente costituita da un certo numero di transazioni, le quali hanno scopi e una struttura ben definita. L'intero registro è memorizzato in uno o più file e/o database ed ogni operazione effettuata, tipicamente l'aggiunta di un nuovo blocco, viene replicata tra tutti gli utenti interessati al mantenimento del registro digitale. Questi utenti possono essere assimilati ai nodi di una rete che eseguono un determinato protocollo mirato alla gestione della *blockchain*.

Questo protocollo prevede che una parte di questi nodi, chiamati *miner*, possano essere incaricati della verifica della correttezza delle transazioni contenute all'interno di un blocco ed eventualmente allo svolgimento di altre operazioni necessarie a garantire l'omogeneità del contenuto della *blockchain* tra tutti i nodi della rete, proprietà questa che viene garantita attraverso un protocollo di consenso che descriveremo in seguito.

Come abbiamo detto una *blockchain* è una catena di blocchi ciascuno dei quali contiene delle transazioni, vediamo di definire più precisamente questi termini.

2.1. Transazioni

Le transazioni rappresentano l'elemento base di ciascuna *blockchain* e sono la rappresentazione digitale di un qualunque atto tra parti (ordine di merce, pagamento di merce, acquisto di cose/oggetti, passaggio di proprietà, ecc.). I nodi della *blockchain* sono tenuti a mantenere in locale (sul proprio pc) una copia dell'intero registro per poter garantire l'integrità ed il corretto funzionamento della *blockchain*. Questo requisito fondamentale costringe i nodi della *blockchain* al consumo di enormi quantità di memoria (per esempio, i dati della *blockchain* di bitcoin hanno superato i 500 gigabyte).

Ciascuna transazione, una volta proposta alla rete, viene archiviata in una lista ordinata da cui sarà successivamente «ripescata» dai *miner* che procederanno con la verifica della sua correttezza e a seguito di esito positivo, al suo inserimento in un nuovo blocco che sarà successivamente aggiunto alla catena. Solo quando questa operazione sarà stata effettuata la transazione sarà considerata valida.

2.2. Blocchi

Un blocco è il contenitore di un numero limitato di transazioni (di solito qualche centinaio), la cui dimensione viene definita dal protocollo; maggiore è la capienza del blocco, maggiori saranno le informazioni che sarà possibile inserire e di conseguenza validare nel breve periodo. Vi è un ampio dibattito in corso (https://www.coindesk.com/learn/2015/08/21/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/) per stabilire il corretto dimensionamento di un blocco che dipende da diversi fattori caratterizzanti la *blockchain*, ad esempio bitcoin prevede che un blocco abbia una dimensione massima di 1 megabyte.

Ciascun blocco è composto da due elementi: una prima struttura, contenente tutti i metadati necessari alla validazione del blocco stesso, ed una seconda struttura, contenente le transazioni da importare nella catena. Un blocco è creato da un *miner* che dopo aver selezionato le transazioni da introdurvi (rispettando comunque l'ordine cronologico) e averne verificato la correttezza provvede ad avviare l'operazione di consenso e quindi a distribuire il blocco a tutti i nodi.

2.3. Consenso

Caratteristica fondamentale della *blockchain* è l'assenza di un organismo centralizzato che possa governare e autorizzi le diverse transazioni che avvengono nel sistema, e contemporaneamente garantire che ogni transazione sia approvata collegialmente. Affinché questo possa accadere è necessario che tutti i nodi abbiano la conoscenza completa di ciò che è avvenuto e sta avvenendo nel sistema. Più formalmente parlando: tutti i nodi devono condividere lo stesso stato globale del sistema. Sfortunatamente questa non è un'operazione facile quando si opera in una rete come Internet. Come infatti tutti hanno avuto modo di sperimentare la rete «può perdere» dei messaggi, o non funzionare propriamente per alcuni periodi. In questi casi alcuni nodi della *blockchain* potrebbero perdere transazioni o blocchi, perdendo di fatto l'allineamento con il resto del sistema. Ad esempio, un nodo A che non ha ricevuto la transazione in cui il nodo B ha speso 10 Btc per l'acquisto di un'automobile, potrebbe successivamente accettare da B la stessa valuta per l'acquisto di un altro servizio. Per evitare il verificarsi di questa evenienza si ricorre ad eseguire periodicamente un opportuno algoritmo di *consenso* il cui scopo è proprio quello di allineare tutti i nodi allo stesso livello di conoscenza. L'algoritmo di consenso è una delle principali caratteristiche che differenzia tra loro le diverse tecnologie di *blockchain*. In Figura 2 sono riportati alcuni tra gli algoritmi più utilizzati attualmente. A titolo esemplificativo descriviamo brevemente le due strategie più usate per lo svolgimento di questo algoritmo rimandando a (https://www.bitstamp.net/learn/security/what-are-*blockchain*-consensus-rules/) per maggiori approfondimenti.

Teoricamente tutti i nodi di una *blockchain* potrebbero creare un blocco e proporlo al resto della rete per il suo inserimento nella *blockchain*. In questo modo però potrebbero essere troppe le diverse proposte su cui dover decidere ed aumenterebbe la possibilità per nodi disonesti di poter facilmente influenzare il comportamento dell'intera rete. Per ridurre questa entropia sono stati introdotti dei meccanismi che consentono di ridurre considerevolmente il numero di nodi che possono elaborare delle proposte e contemporaneamente scoraggiare i nodi disonesti dal farlo.

Uno di questi meccanismi è noto come *Proof of Work* (PoW), e prevede che un nodo possa proporre il suo blocco solo dopo avere risolto un criptopuzzle. La soluzione di questo criptopuzzle richiede però l'impiego di potenze di calcolo estremamente elevate (e quindi significativi investimenti) e quindi è alla portata solo di pochi utenti (i *miner* appunto). Il *miner* che per primo risolve il criptopuzzle lo diffonde a tutti i nodi della rete che avviano il processo di accettazione. Se la maggioranza dei nodi accetta la proposta il blocco viene aggiunto alla *blockchain*. Terminata questa fase il *miner* che ha

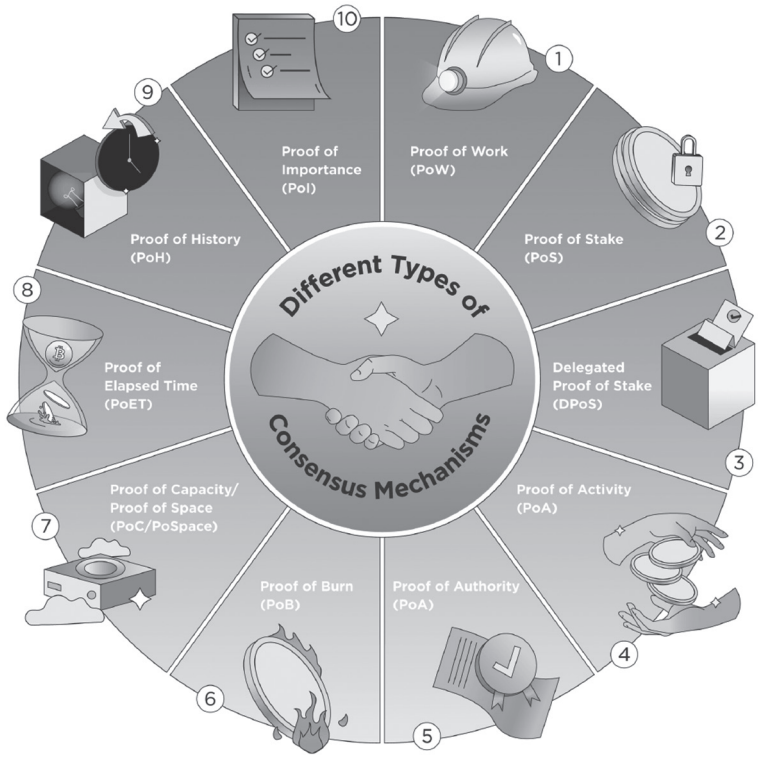

Fig. 2. Differenti tipologie di consenso.

Fonte: crypto.com.

provveduto a validare il blocco riceva un compenso in Bitcoin, il cui ammontare è prestabilito dal protocollo stesso.

In alternativa a PoW, incomincia a prendere piedi un altro meccanismo di consenso noto come *Proof of Stake* (PoS). In un sistema basato su PoS i *validator* sostituiscono i *miner*. Esiste un processo che seleziona tra i nodi della rete quelli che hanno maggiori credenziali (*stake*). Tra questi ne viene scelto uno casualmente. Una volta che un nodo viene selezionato come *validator* del blocco successivo, dovrà controllare se le transazioni in esso contenute sono valide, firmare il blocco e aggiungerlo alla *blockchain*. A differenza dei sistemi PoW, in cui il lavoro dei *miners* viene premiato con la creazione di nuova moneta, nei sistemi *Proof of Stake* la ricompensa per i *validators* consiste in una *fee* trattenuta sulla transazione validata. Prima di poter ritirare la propria quota depositata e riscuotere la propria ricompensa, il network veri-

fica l'operato del *validator*, controllando che non siano stati aggiunti blocchi fraudolenti. PoS è meno decentralizzato rispetto a PoW, ma migliora significativamente la scalabilità ed efficienza del consenso.

3. Uno sguardo alle prestazioni

Nonostante negli ultimi anni si sia registrato un crescente interesse da parte dell'opinione pubblica alle *blockchain*, si continua a respirare aria di incertezza ogniqualvolta emerge un nuovo progetto che ne promette l'impiego. Questo perché sussistono alcuni problemi intrinseci della *blockchain* che ne rendono ancora oggi problematica la sua applicazione. Questi problemi sono principalmente legati alle prestazioni che *blockchain* è in grado di fornire, prestazioni che sono solitamente espresse attraverso diversi parametri, questi i principali:

- Tolleranza ai guasti: indica il numero massimo di nodi difettosi/disonesti che il protocollo di consenso può tollerare.
- Produttività: indica il numero di transazioni che il protocollo può elaborare in un secondo.
- Scalabilità: si riferisce alla capacità di poter aumentare il numero di utenti della *blockchain* senza degradarne le prestazioni.
- Latenza: si riferisce al tempo che intercorre tra quando viene proposta una transazione fino alla sua validazione.
- Consumo energetico: indica la quantità di energia consumata per il funzionamento della *blockchain*.

Tra questi parametri due occupano un posto preponderante quando si valuta l'applicabilità di una soluzione *blockchain*: il consumo energetico, che in questa fase storica sta diventando un fattore molto critico e la produttività (*throughput*). Vediamoli più in dettaglio.

3.1. Il consumo energetico di una *blockchain*

A titolo di esempio riassumiamo nella Figura 3 i consumi energetici necessari per il mantenimento della *blockchain* di Bitcoin, che però in qualche modo sono indicativi dei consumi di una *blockchain* il cui meccanismo di consenso e basato sul PoW.

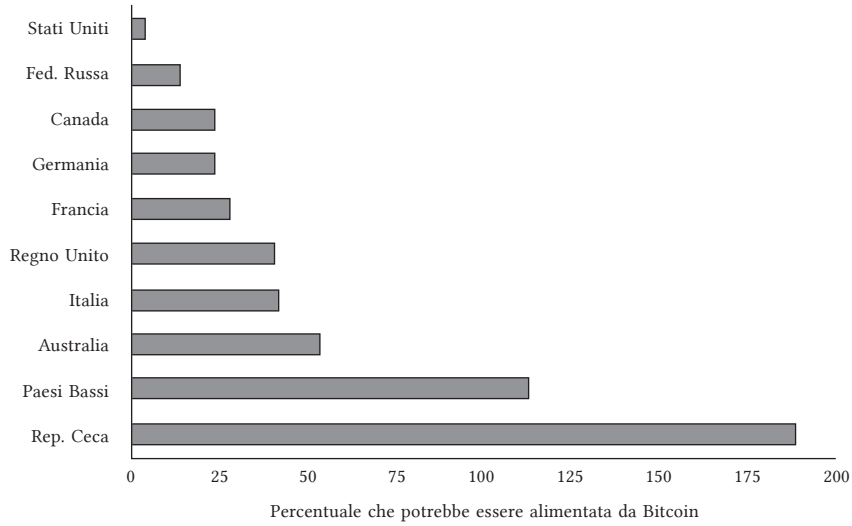

Fig. 3. Consumi energetici necessari per il mantenimento della *blockchain* di Bitcoin in alcuni paesi.

Secondo il sito https://digiconomist.net/bitcoin-energy-consumption il mantenimento della *blockchain* Bitcoin richiede il consumo di circa 140 terawatt/anno, cioè il 25% dell'energia consumata in Germania in un intero anno, poco meno del 50% dell'energia consumata in Italia e molto più dell'energia necessaria a far funzionare l'Olanda. Secondo dati pubblicati sempre dalla stessa fonte l'impatto in termini di CO2 prodotta in un anno si aggirerebbe intorno ai 74 milioni di tonnellate cioè quanto la Nuova Zelanda. Problematico anche il fronte dei rifiuti: gli scarti elettronici dovuti all'usura degli apparati usati per eseguire il PoW è di 36.980 tonnellate, equiparabili a quelli prodotti in un intero anno dall'Olanda.

3.2. Produttività

Tra i punti qualificanti di una *blockchain* va considerata la sua possibilità di poter gestire un numero significativo di transazioni al secondo (tps), infatti se si vuole che la *blockchain* possa trovare applicazione in settori significativi dell'economia globale quali ad esempio quello energetico, è necessario che il sistema sia in grado di gestire milioni di transazioni fisiche e finanziarie al giorno.

A questo riguardo è opportuno considerare il fatto che Bitcoin è in grado di «reggere» una media di circa 7 transazioni al secondo (tps), cioè

Tab. 1. Confronto prestazionale tra diverse *blockchain*.

Blockchain Name	Consensus Protocol	Transaction per Second (TPS)	Transaction Confirmation Time (TCT)	Supply Chain Suitability
Bitcoin (BTC) [21]	PoW	3-7	25 min	Expensive, low bandwidth (TPS), high TCT.
Ethereum (ETH) [22]	PoW	15-20	2 min	Expensive with viable, for commerciai deployment TCT
Ripple (XRP) [23]	RCPA	1.500	4 s	High bandwidth, low cost and high TCT
Bitcoin Cash (BCH) [24]	PoW	60	60 min	Expensive and not suitable for real-time
Litecoin (LTC) [25]	PoW	56	30 min	Expensive, not well suited for real-time
EOS(EOS) [26]	DPoS [27]	millions	6 min	lnexpensive, high throughput, low TCT
Cardano (ADA) [28]	PoS	5-7	3-5 min	lnexpensive, moderate throughput, low TCT
Stellar (XLM) [29]	PoS	.1000	2-5s	lnexpensive, high throughput, low TCT
NEO (NEO) [30]	DBFT	10.000	15-20 s	lnexpensive, high throughput, low TCT
Monero (XMR) [31]	DAG (Tangle)	4	30 min	lnexpensive, low TPS, low TCT
Tether (USDT) [32]	Various consensus mechanisms	Ethereum-based token	15-30 s	lnexpensive with moderate TPS and low TCT
NEM (XEM) [33]	PoI	4.000	1-2 min	lnexpensive with moderate TPS and low TCT

Fonte: Litke, Anagnostopoulos, Varvarigou, *Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment*, in *Logistics*, 2019, 3(1), https://doi.org/10.3390/logistics3010005.

circa 600.000 transazioni al giorno mentre Ethereum (un'altra tecnologia di *blockchain* oggi in espansione) ha un limite superiore di circa 20 tps. Questi dati non sono a oggi paragonabili a quelle ottenibili con le piattaforme centralizzate come ad esempio PayPal (450 tps) e Visa (56.000 tps). Nella tabella 1 sono riportati i valori di produttività e di latenza di alcune tra le più diffuse

blockchain, valori che come emerge da una lettura di tale tabella sono determinati dall'algoritmo di consenso utilizzato.

4. Le diverse tipologie di *blockchain*

A partire dal 2008 la tecnologia *blockchain*, grazie alla sua implementazione nel sistema di criptovaluta Bitcoin, ha esibito le sue potenzialità ed è diventata oggetto di diversi studi e applicazioni in diversi ambiti. Contemporaneamente però ha anche esibito le sue debolezze, che hanno indotto molti sviluppatori a rivedere alcuni dei suoi presupposti di funzionamento al fine di individuare soluzioni che potessero operare nell'ecosistema di implementazione. Sono quindi nate soluzioni di *blockchain* con obiettivi più modesti ma praticamente applicabili. Ad oggi sono state individuate tre diverse tipologie di *blockchain*: pubblica, privata e *permissioned*.

Una *blockchain pubblica* prevede che non esistano dei vincoli o autorizzazioni per poter accedere alla rete, eseguire transazioni o partecipare alle attività di verifica e validazione. Chiunque può quindi operare sulla *blockchain*, aumentando di fatto il rischio di potenziali attacchi alla rete. Per contro, va sottolineato che la stabilità e la sicurezza di una *blockchain* pubblica aumentano al crescere dei nodi che compongono la rete con particolare riferimento ai *miner*, da questo segue la scelta di assegnare loro una ricompensa, incentivandoli ad una collaborazione continuativa e coordinata.

In una *blockchain privata* invece, i permessi di accesso in lettura e scrittura sono limitati e controllati da un'autorità centrale, l'unica ad avere i privilegi per effettuare operazioni di certificazione e validazione delle transazioni. Per quanto sacrifichino gran parte della logica decentralizzata, le soluzioni private hanno ottenuto un discreto successo nei modelli di business tradizionali, dove la privacy e la gestione dei dati sono di vitale importanza e devono rimanere sotto il controllo dell'organizzazione. In questo modello i nodi non necessitano di alcun incentivo economico per il corretto mantenimento dello stato di integrità della catena, abbassando di fatto i costi di utilizzo per l'utente e aumentando l'efficienza nella gestione delle transazioni.

Le *blockchain permissioned* mantengono invece un'impostazione ibrida tra le pubbliche e private: l'accesso alla rete è consentito al pubblico ma sono imposti dei limiti nelle attività di validazione, governate esclusivamente da un'autorità centrale o da un collettivo di nodi delegati. Anche in questa soluzione, come in quella privata, i nodi non necessitano, in tutto o in parte, di incentivi.

5. Le diverse generazioni di *blockchain*

Come evidenziato nelle sezioni precedenti l'attuale tecnologia *blockchain*, e ci riferiamo a *blockchain* pubbliche, non è ancora pronta per un'adozione generale e presenta diverse carenze. Queste carenze ovviamente si riflettono anche sulle applicazioni che dovrebbero utilizzare questa tecnologia (*blockchain enabled*) e sono da individuare come il fattore che oggi maggiormente frena l'adozione di questa tecnologia. Ci sono intense attività di ricerca in corso per migliorare l'intero sistema *blockchain*, attività che si stanno concentrando sull'individuazione di algoritmi più efficienti per: la gestione e memorizzazione delle transazioni, per l'effettuazione del consenso e per uno sfruttamento migliore della banda di rete. La continua ricerca di soluzioni continuamente migliorative sta dando vita a generazioni di *blockchain* e a oggi si riconoscono abbastanza universalmente tre generazioni di *blockchain* le cui principali caratteristiche sono descritte qui di seguito.

5.1. Prima generazione

La tecnologia *blockchain* di prima generazione è indissolubilmente legata alla cryptovaluta bitcoin e la sua descrizione è contenuta nell'articolo fondazionale di Bitcoin (https://bitcoin.org/bitcoin.pdf). In questo articolo, infatti, l'autore (Satoshi Nakamoto) oltre a descrivere l'ecosistema sottostante la criptovaluta descrive con un certo dettaglio la sottostante *blockchain* basata su PoW. Bitcoin è il primo vero caso d'uso della tecnologia *blockchain* e il suo scopo è la realizzazione di un sistema di trasferimento elettronico di denaro che possa consentire agli utenti di scambiare denaro senza l'intervento di una banca (sia del settore privato che governativo). Il sistema permette ai propri utenti di trasferire fondi in modo anonimo utilizzando opportune applicazioni chiamate «wallet (portafogli)» e di accedere al libro mastro transazionale.

Il buon funzionamento di bitcoin ha incoraggiato ricercatori e investitori e replicare il modello in altre piattaforme di trading di criptovaluta. Le *blockchain* di prima generazione sono quindi caratterizzate da un consenso basato su PoW che ha dimostrato nei fatti di garantire sicurezza (fatta eccezione per alcuni casi di attacco informatico che però hanno inciso minimamente sull'intero sistema), correttezza e stabilità. Per contro come abbiamo già avuto modo di commentare questo meccanismo di consenso è caratterizzato da una produttività molto bassa e da un consumo energetico assolutamente non sostenibile.

5.2. Seconda generazione

La II generazione di *blockchain* nasce dalla constatazione delle limitazioni di Bitcoin sia prestazionali che di funzionalità. In particolare, Bitcoin consente solo di inviare, ricevere e scambiare criptovaluta. Cioè consente solo l'esecuzione di transazioni che potremmo definire «elementari» quali l'acquisto e la vendita di merce/servizi, ad esempio Bitcoin non consente di esprimere condizioni e termini all'interno delle transazioni. Praticamente parlando, una transazione del tipo: «Pagherò a Bob l'importo XX in criptovaluta solo quando il mio ordine mi sarà stato consegnato» non può essere espressa in Bitcoin. Per far fronte a queste limitazioni nel 2013 è stata proposta una nuova *blockchain* di nome Ethereum (https://ethereum.org/). Nella sua versione originale Ethereum prevedeva l'adozione di un algoritmo di consenso di tipo PoW, recentemente riconvertito in uno di tipo PoS. Due sono gli aspetti innovativi introdotti da Ethereum:

- il concetto di *smart contract*. Si tratta di una forma particolare di transazione scritta attraverso un opportuno linguaggio di programmazione. Questi programmi sono tipicamente utilizzati per automatizzare l'esecuzione di un accordo tra parti affinché tutti i partecipanti possano confermarne il risultato, oppure per automatizzare dei flussi di lavoro o eseguire delle azioni specifiche al verificarsi di determinate condizioni.
- Un ecosistema digitale per lo sviluppo di nuovi progetti di criptovaluta. Ethereum fornisce cioè una piattaforma che può essere utilizzata per codificare ed eseguire app decentralizzate (dApps) che possono essere eseguite su una qualunque piattaforma Ethereum, allo stesso modo con cui una app scaricata dal Play Store può essere eseguita su un qualunque sistema Android.

5.3. Terza generazione

Le *blockchain* di terza generazione, che include piattaforme come Algorand, Cosmos, Tron e Cardano, sono caratterizzate principalmente da un significativo miglioramento prestazionale oltre che dall'introduzioni di altre importanti caratteristiche, più precisamente:

- *Scalabilità*: la *blockchain* è in grado di elaborare un numero crescente di transazioni proporzionalmente alla crescita di domanda da parte degli utenti. La scalabilità si riflette anche su un'ottimizzazione della larghezza di banda per consentire il trasferimento di un maggior numero possibile di transazioni nell'unità di tempo, ed in questo caso sono state introdotte tecniche per la compressione dei dati.

• *Interoperabilità*: consente agli utenti di interagire non solo con un tipo di valuta, ma con più valute su varie *blockchain*. Inoltre, l'interoperabilità con le entità bancarie centralizzate è altrettanto importante per garantire legittimità e convenienza d'uso. Quando due utenti utilizzano una stessa piattaforma *blockchain*, come Bitcoin, lo scambio di dati e valore in digitale è un processo «semplice». Tuttavia, le stesse transazioni non sono possibili quando le parti utilizzano piattaforme *blockchain* diverse. Questa limitazione riduce significativamente la possibilità di scambi digitali tra attori diversi, questo perché le diverse entità che usano tecnologia *blockchain* usano reti diverse. Un'azienda A che volesse trasferire un certo ammontare di Bitcoin ad un'azienda B che usa Ethereum non può farlo. L'interoperabilità tra i sistemi dovrebbe consentire di superare questi problemi. Si tratta ovviamente di un tema particolarmente complesso da affrontare e che richiederà diversi anni per poter essere risolto. Nel frattempo, le *blockchain* di terza generazione stanno incominciando ad affrontarlo ed a proporre soluzioni parziali, cioè a consentire di comunicare tra loro ad un numero ristretto di altre *blockchain*. Esempi in questo senso sono costituita dagli ecosistemi COSMOS e Chainlink (https://chain.link/) che si basano sul protocollo Inter-*Blockchain* Communication (IBC) e consentono il trasferimento di dati tra diverse *blockchain* senza intaccare la loro sovranità.

• *Sostenibilità*: un altro cambiamento significativo che le *blockchain* di terza generazione, hanno introdotto è il definitivo abbandono dell'algoritmo di consenso PoW a favore del modello *Proof-of-Stake* (PoS). In questo modo si procede con l'eliminazione di dispositivi informatici altamente complessi utilizzati per la soluzione dei cryptopuzzle e l'enorme consumo di energia necessario per creare nuovi blocchi. Questo è il motivo per cui molte delle recenti *blockchain* sono definite «*blockchain* verdi».

Al fine di fornire alcuni parametri oggettivi su cui valutare lo stato evolutivo delle *blockchain* a partire dalla *blockchain* di bitcoin riportiamo alcuni parametri prestazionale di uno tra le *blockchain* proposte più recentemente sul mercato delle criptovalute. Si tratta di Algorand una *blockchain* proposta nel 2017 che mira ad essere una *blockchain* molto veloce ad emissioni zero. Algorand riesce a gestire fino a 6000 transazioni al secondo, un numero notevole soprattutto se comparato a tecnologie centralizzate largamente utilizzate nel contesto attuale come PayPal. Anche il tempo di latenza è estremamente ridotto e si attesta intorno ai cinque secondi. Questi risultati sono una diretta conseguenza del protocollo di consenso adottato chiamato *Pure Proof-of-Stake*. Il protocollo di consenso adottato da Algorand non porta benefici solamente prestazionali, ma riduce notevolmente anche il consumo energetico, si stima che Algorand consumi circa 0,0000008 kWh/txn, una quantità irrisoria specie se comparata a Bitcoin (930 kWh/txn) o ad Ethereum (70 kWh/txn).

6. Conclusioni

Il presente contributo costituisce una rassegna introduttiva sullo stato dell'arte nel settore delle tecnologie *blockchain*. Dopo una breve esposizione delle principali peculiarità di tale tecnologia abbiamo delineato alcune delle principali criticità legate ad un suo impiego massivo. Abbiamo altresì delineato le principali direttrici su cui si sta muovendo la ricerca per rimuovere le suddette limitazioni ed aggiungere ulteriori caratteristiche che possano rendere la tecnologia fruibile nei più diversi contesti applicativi.

Danilo M. Bruschi
Dipartimento di Informatica «G. degli Antoni»
Università degli Studi di Milano
Via Celoria 18, 20133 Milano
danilo.bruschi@unimi.it
Orcid: 0000-0002-5905-5976

Davide Rusconi
Dipartimento di Informatica «G. degli Antoni»
Università degli Studi di Milano
Via Celoria 18, 20133 Milano
davide.rusconi@unimi.it
Orcid: 0009-0009-3648-7416

Matteo Zoia
Dipartimento di Informatica «G. degli Antoni»
Università degli Studi di Milano
Via Celoria 18, 20133 Milano
matteo.zoia@unimi.it
Orcid 0009-0006-2722-7178