Capitolo I
Struttura, funzione e disciplina generale degli NFT

1. Le origini culturali della blockchain

La blockchain ha una data ufficiale d'inizio: il 31 ottobre del 2008 è apparso su una mailing dedicata alla crittografia [1] il whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System" [2], firmato con il solo pseudonimo Satoshi Nakamoto [3], che descrive il funzionamento della blockchain dei bitcoin, la quale sarebbe stata realizzata di lì a poco [4]. Tuttavia, il sistema culturale e simbolico del mon-

[1] Il nome della mailing list è Metzdowd ed è visionabile al seguente URL: https://www.metzdowd.com/mailman/listinfo/cryptography.

[2] Il whitepaper è tuttora disponibile on-line al seguente URL: https://bitcoin.org/bitcoin.pdf.

[3] L'identità di Satoshi Nakamoto non è tuttora nota, né è chiaro se si tratti di una persona o di un gruppo organizzato. Due dati, tuttavia, possono essere affermati con relativa certezza: primo, al di là di chi si celi dietro lo pseudonimo di Satoshi Nakamoto, è certo che la blockchain è nata sulla base dello sviluppo storico e culturale descritto nel presente paragrafo; in secondo luogo, chi ha creato la blockchain ha anche fatto un "ottimo affare" in quanto ha conservato per sé elevati quantitativi di bitcoin che, apprezzandosi nel tempo, lo/li hanno reso/i estremamente ricco/i: secondo alcune stime avrebbe/ro, infatti, almeno tuttora un milione di bitcoin.

[4] La prima transazione di Bitcoin è avvenuta alcuni mesi dopo la pubblicazione del whitepaper, cioè il 9 gennaio 2009 ed è stata annunciata con una email indirizzata alla mailing list Metzdowd indicata *supra* in nota 1. Il testo di tale email è

do cripto, e conseguentemente degli NFT che in tale ecosistema "hanno vita", non è nato dal nulla ma è il portato di uno sviluppo almeno decennale nell'ambito della tecnologia, del diritto e delle dottrine politiche statunitensi.

Le origini culturali della blockchain possono essere fatte risalire al movimento Cypherpunk sviluppatosi negli Stati Uniti nel 1992. Si tratta di un movimento composto da circa un migliaio di partecipanti, molti dei quali poi diventeranno figure di spicco del movimento cripto [5], che coniuga la filosofica americana *libertarian* con l'uso della crittografia a fini di protezione dall'intromissione dei governi nelle vite delle persone.

Il movimento *libertarian*, sviluppatosi essenzialmente negli Stati Uniti, è un'evoluzione del liberalismo classico, rispetto al quale si contraddistingue per l'attenzione data all'importanza di tutelare l'individuo dall'interferenza dello Stato nella sfera privata [6]: inter-

---

disponibile al seguente URL: https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html. In tale occasione, Nakamoto ha reso pubblico la versione 0.1 del software dei bitcoin su SourceForge e ha anche ufficialmente lanciato il network, definendo così il blocco "genesis" (cioè il blocco numero "0" o blocco di genesi) che aveva una ricompensa per i *miners* di 50 bitcoin. Nella transazione del blocco "0", Nakamoto ha inserito la seguente frase «the Times 03/Jan/2009 Chancellor on brink of second bailout for banks» tratta da un titolo del giornale del Regno Unito The Time di quel giorno, cioè il 9 gennaio 2009: l'inserimento di tale frase nel blocco genesis dei bitcoin è sempre stato interpretato come un accenno al fatto che il sistema delle criptovalute è stato realizzato per superare il sistema della moneta tradizionale il cui fallimento è stato palesato dalla crisi bancaria del 2008.

[5] Per esempio: Nick Szabo, per cui si veda *infra* in questo stesso paragrafo; Marc Andreessen, uno dei fondatori di Andreessen Horowitz (nota come "A16Z"), la società di venture capital che ha effettuato, nel corso degli anni, i maggiori investimenti nel mondo cripto.

[6] Il massimo teorico del movimento *libertarian* può essere considerato Robert Nozick. In *Anarchy, State, and Utopia*, uno dei testi base del movimento *libertarian*, Nozick, per esempio, scrive: «our main conclusions about the state are that a minimal state, limited, to the narrow functions of protection against force, theft, fraud, enforcement of contracts, and so on, is justified, but any more extensive state will violate persons' rights not to be forced to do certain things, and is unjustified; and that the minimal state is inspiring as well as right», *Anarchy, State, and Utopia*, p. ix, New York, Basic Books, 1974.

ferenza sia dalla pretesa impositiva del fisco ma anche (e soprattutto) dai sistemi di monitoraggio e controllo sulle comunicazioni e la vita privata delle persone [7].

Il gruppo dei Cypherpunks, a sua volta, declina la filosofia *libertarian* essenzialmente sul versante tecnologico [8]: all'epoca si era ancora agli albori di internet, ma era già chiaro che i governi o le grandi corporation hanno un forte interesse ad accedere ai, e monitorare i, dati digitali generati dagli individui per profilarli e controllarli; pertanto, i Cypherpunks iniziano essenzialmente a discutere, in modo spontaneo, di come utilizzare la crittografia per difendere la "privacy" degli individui.

Sotto il profilo più marcatamente storico [9], il gruppo dei Cypherpunks si è formato nel 1992, a seguito delle riunioni che Eric Hughes, Timothy C. May e John Gilmore hanno iniziato a tenere con regolarità nella sede della società Cygnus Solutions di proprietà di Gilmore, presso la baia di San Francisco, e si è successivamente sviluppato in una mailing list con diverse centinaia di iscritti [10]. Il nome

---

[7] Si tratta essenzialmente delle intercettazioni considerando che, all'epoca, la prima industria informatica si stava sviluppando e già erano stati creati i primi rudimentali sistemi di monitoraggio sui flussi di dati digitali.

[8] Si veda, in questo senso, M. Raskin, *The Law and Legality of Smart Contract*, in *Geo L. Tech. 1 Review*, 2017, p. 305, il quale scrive «as with many new technologies, behind bitcoin stood a political ideology skeptical of centralized power and supportive of capitalism and free markets. Although he never identified himself as such, many describe the creator of bitcoin, Satoshi Nakamoto, as a libertarian. Certainly many of the early adopters of bitcoin were self-described libertarians. Szabo has been called libertarian and his writings emphasize alternatives to the state's enforcement of rights. Traditionally, states have been defined as monopoly holders of force with a power to tax. Among the most radical visions for smart contracts is that the technology will subject the provision of justice to market forces and break the state's monopoly over the court system. This is an idea that has been discussed by many libertarians, including Robert Nozick, Murray Rothbard, and David Friedman».

[9] Si veda in proposito J. Bartlett, *Cypherpunks Write Code*, in www.americanscientist.org, disponibile al seguente URL: https://www.americanscientist.org/article/cypherpunks-write-code.

[10] La mailing list aveva raggiunto i 700 iscritti nel 1994 e circa 2000 iscritti nel 1997. Ufficialmente la mailing list è ancora attiva e può essere raggiunta al se-

deriva dalla contrazione tra la parola "*cypher*" (cioè "cifrario" [11] in inglese) e "punks".

Nel manifesto dei Cypherpunks redatto da Hughes nel 1993 si legge che: «privacy in an open society requires anonymous transaction systems […] an anonymous system empowers individuals to reveal their identity when desired and only when desired» e che «privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy» e, infine, «we cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak. To try to prevent their speech is to fight against the realities of information. Information does not just want to be free, it longs to be free» [12].

Sotto il profilo più marcatamente giuridico, Nick Szabo, uno dei partecipanti originari al movimento Cypherpunk, in un breve articolo scritto su un blog nel 1994 [13], introduce per la prima volta il concetto di smart contract [14] che è definito da Szabo: «a computerized transaction protocol that executes the terms of a contract» [15].

---

guente URL: https://lists.cpunks.org/pipermail/cypherpunks/ dove è anche visionabile l'intero archivio delle email inviate fin dalla creazione di tale mailing list.

[11] In crittografia, il cifrario è un algoritmo utilizzabile per cifrare o decrittare dei dati.

[12] Il manifesto Cypherpunks è accessibile al seguente URL: https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt.

[13] L'articolo è intitolato *Smart Contracts* ed è consultabile al seguente URL https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. Il tema degli smart contracts è stato successivamente ripreso e approfondito da Szabo in due articoli del 1997: *The Idea of Smart Contracts*, disponibile al seguente URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html e *Formalizing and Securing Relationships on Public Networks*, disponibile al seguente URL: http://myinstantid.com/szabo.pdf.

[14] Sugli smart contract, si veda *infra*, in questo capitolo, par. 5.

[15] N. Szabo, in *Smart Contracts*, cit.

Il termine "smart contract" ha, poi, avuto una particolare fortuna nel mondo cripto, in quanto designa il tipo di software che sovraintende alle transazioni informatiche nella rete Ethereum, ma è opportuno specificare, fin da ora, che tale tipologia di software non corrisponde all'idea di smart contract elaborata da Szabo: Vitalik Buterin, uno dei creatori di Ethereum, agli albori della creazione di Ethereum, ha semplicemente preso in prestito l'espressione coniata da Szabo per dare un nome a quelli che, poi, appunto sarebbero stati conosciuti come gli "smart contract" [16], vale a dire il software utilizzato all'interno della rete di Ethereum.

La nozione di smart contract elaborata da Szabo ha, in effetti, un significato più generale e diverso, al tempo stesso, rispetto alla nozione di smart contract ormai diventata di uso comune nel mondo cripto, in quanto si riferisce alla possibilità di utilizzare la crittografia e altre tecnologie innovative (per l'epoca) allo scopo di «to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries» [17] ma anche di realizzare «related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs» [18].

---

[16] Tra l'altro è noto come Buterin si sia in seguito pentito di tale scelta. Si veda, per esempio, S. Orlando, *Profili definitori degli "smart contracts"*, in R. Clarizia (a cura di), *Internet, Contratto e Persona, Quale futuro?*, Pisa, Pacini, 2021, p. 43, il quale riporta che: «di fronte ai dubbi e agli equivoci indotti dal sostantivo "contract", Buterin, nell'ottobre 2018 su twitter dichiarava di essersi pentito di aver utilizzato questa espressione: "To be clear, at this point I quite regret adopting the term "smart contracts". I should have called them something more boring and technical, perhaps something like "persistent scripts"». Ed è riportato che uno degli sviluppatori di Ethereum avrebbe definito gli smart contracts come "stored procedures". Nella edizione in lingua inglese del Libro bianco di Ethereum (non perfettamente coincidente con quella in lingua italiana) gli smart contracts sono definiti semplicemente come "a piece of code implementing arbitrary rules (smart contracts)».

[17] N. Szabo, in *Smart Contracts*, cit.

[18] *Ibid.*

Lo scopo di minimizzare "trusted intermediaries", come Szabo stesso dice nell'articolo citato, è latamente connesso alla filosofia del gruppo dei Cypherpunks di utilizzare la crittografia per difendere la privacy degli individui dall'interferenza dei governi e delle big corporations.

L'idea di smart contract elaborata da Szabo contiene in sé l'idea dell'autoeseguibilità di tali contratti (ed è in effetti una diretta conseguenza del fatto di eliminare gli intermediari), sia nel senso che il contratto non richiede che le parti dello stesso lo eseguano (che adempiano, in altri termini) [19] così come che è eliminata, alla radice, la necessità di ricorrere all'esecuzione forzata sulla base di un provvedimento giudiziale nel caso d'inadempimento [20].

I valori rivendicati dal movimento dei Cypherpunk e l'idea alla

---

[19] Nell'ambito del mondo cripto e della dottrina che si è occupata degli smart contract si fa anche frequentemente riferimento all'espressione "*code is law*": si tratta di una locuzione derivata dal titolo del primo capitolo di un noto libro di Lawrence Lessig intitolato *Code and Other Laws of Cyberspace*, 1999, New York, USA, Basic Books,; il testo, come altri scritti di Lessig è liberamente scaricabile dal sito https://lessig.org/ sotto licenza CC. L'idea base sviluppata da Lessig nel testo citato è che: «in real space we recognize how laws regulate – through constitutions, statutes, and other legal codes. In cyberspace we must understand how code regulates – how the software and hardware that make cyberspace what it is regulate cyberspace as it is. As William Mitchell puts it, this code is cyberspace's law», p. 6. In senso analogo al principio del *code is law* di Lessig, si veda J.R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, in *Texas Law Review*, 3, febbraio 1998, p. 553 ss. Nell'ambito della dottrina italiana si veda M. Maugeri, *Smart Contract e Disciplina dei Contratti*, Bologna, Il Mulino, 2021, pp. 51-52, secondo cui il filone dottrinale in base al quale «gli Smart Contracts non necessiterebbero del diritto perché rappresenterebbero essi stessi un'alternativa al diritto dei contratti, che sarebbe, pertanto, destinato a scomparire» riprenderebbe in sostanza l'idea di Lessig del "Code is Law".

[20] Si veda, in tal senso, M. Raskin, *The Law and Legality of Smart Contract*, cit., p. 320: «by decreasing the costs of mediation, self-enforcement, and arbitration, Szabo saw smart contracts as representing a fundamental shift in the world away from paper and towards digital systems, like the banking backed by computers and digital databases. This shift was not to take place immediately, however, as Szabo recognized the value of the long history».

base degli smart contract (nel senso di Szabo) sono tuttora gli elementi fondanti del mondo cripto e, quindi, degli NFT[21]: l'uso della tecnologia, in particolare della crittografia, per eliminare nelle transazioni (digitali) tra individui la presenza di intermediari che addebitano costi non necessari e violano la privacy[22] delle persone a beneficio dei governi o delle grandi corporation; la rivendicazione dell'anonimato quale garanzia del diritto alla privacy delle persone[23], cioè la possibilità di operare nelle blockchain con identità digitali (in pratica i wallet)[24] totalmente anonimi[25]; il valore della decentralizzazione da intendersi come autogestione degli individui senza l'intermediazione di strutture sovraordinate gerarchicamente, i cui rapporti, anche sotto il profilo giuridico, sono garantiti sulla base delle regole (informatiche) contenute negli smart contract.

---

[21] L'affermazione contenuta in tale paragrafo va riferita solamente alle blockchain *permissionless* e non a quelle *permissioned* o private; sulla distinzione tra queste due tipologie di blockchain si veda *infra*, in questo capitolo, par. 3.

[22] Il concetto di privacy qui utilizzato va inteso nel senso che il movimento Cypherpunk dà a tale nozione: cioè il diritto delle persone di proteggere la loro riservatezza dal controllo esercitato dai governi e dalle big corporation. Nel mondo cripto quando si parla di "privacy" in genere ci si riferisce a tale nozione, la quale non coincide propriamente con il diritto alla riservatezza del diritto civile e del regolamento UE 2016/679 (noto come "GDPR").

[23] Sulle "tensioni" tra il carattere anonimo dei wallet e la normativa antiriciclaggio si veda *infra*, cap. IV, par. 9.

[24] Sui wallet si veda *infra*, in questo stesso capitolo, par. 5.

[25] Si legga, per esempio, il seguente brano tratto dal blog personale di Vitalik Buterin del 31 ottobre 2021: «many national governments around the world are showing themselves to be inefficient and slow-moving in response to long-running problems and rapid changes in people's underlying needs. In short, many national governments are missing live players. Even worse, many of the outside-the-box political ideas that are being considered or implemented for national governance today are honestly quite terrifying. Do you want the USA to be taken over by a clone of WW2-era Portuguese dictator Antonio Salazar, or perhaps an "American Caesar", to beat down the evil scourge of American leftism? For every idea that can be reasonably described as freedom-expanding or democratic, there are ten that are just different forms of centralized control and walls and universal surveillance», Crypto Cities, in www.vitalik.ca, 31 ottobre 2021 disponibile al seguente URL: https://vitalik.ca/general/2021/10/31/cities.html.

Per quanto riguarda gli NFT, vale la pena precisare che i CryptoPunks[26], una delle prime e tuttora più importanti collezioni di NFT, sono stati progettati con un evidente richiamo simbolico-culturale ai Cypherpunk.

2. Il funzionamento tecnico della blockchain

La blockchain, in primissima definizione, è un registro digitale distribuito, realizzato attraverso un network di computer (definiti tecnicamente nodi), che validano le informazioni inserite nel registro attraverso un peculiare meccanismo che ne garantisce l'inalterabilità e, cioè, essenzialmente il *proof of work* o il *proof of stake*[27].

Una blockchain, in italiano "catena di blocchi", è appunto una catena di blocchi di dati digitali[28] registrati in un libro mastro decentralizzato (il libro mastro è, pertanto, la blockchain stessa) in ordine cronologico e validati attraverso un sistema di crittografia basato sulla funzione di hash[29]. Ciascun blocco contiene l'hash

---

[26] La collezione dei CryptoPunks su Opensea è visionabile al seguente URL: https://opensea.io/collection/cryptopunks.

[27] Sulla differenza tra *proof of work* e *proof of stake* si veda *infra* in questo stesso paragrafo.

[28] Si parla frequentemente di "*transactions*", o "transazioni" secondo la traduzione italiana, soprattutto nell'ambito delle criptovalute.

[29] La funzione di hash (dal verbo inglese "*to hash*" che significa sminuzzare o pasticciare e designa, altresì, una polpetta fatta di avanzi di carne e verdure) è una funzione matematica che permette di produrre una stringa (sequenza di caratteri) di lunghezza fissa partendo da qualunque altra stringa di caratteri. Ogni minima modifica della stringa originaria produrrà una diversa stringa in uscita. La caratteristica fondamentale di queste funzioni è la loro difficile invertibilità: dato un valore di hash, è molto difficile risalire alla stringa originaria che l'ha generata. Esistono numerosi algoritmi che permettono di realizzare funzioni di hash, alcuni dei quali implicano l'uso di crittografia come quelli che sono alla base dei protocolli che sovrintendono al funzionamento delle criptovalute. Le funzioni crittografiche di hash, a differenza di quelle convenzionali, devono rispettare tre proprietà: 1) resistenza alle collisioni (deve essere computazionalmente intrattabile trovare una coppia di input distinti che producono lo stesso hash come output); 2) resistenza

crittografico del blocco precedente, un *timestamp* (cioè una marca temporale), e i dati della transazione, i quali generalmente sono rappresentati da un albero di Merkle, nel quale i nodi di dati sono rappresentati da "foglie" [30]. La marca temporale prova che la transazione era realmente esistente quando nel blocco è stato inserito il suo hash. Poiché ogni blocco contiene l'hash del blocco precedente, si forma una catena di tali blocchi, ciascuno dei quali contiene gli hash dei blocchi precedenti.

I blocchi di dati non sono contenuti in un singolo computer o server centralizzato ma ogni blocco di dati è validato in una rete di computer, ognuno dei quali è definito "*node*", o "nodo" in italiano: ciascun blocco è validato in tutti i nodi che compongono la rete blockchain e, pertanto, il dato è registrato simultaneamente in tutti i nodi, che sono distribuiti a livello mondiale.

A livello teorico, una blockchain può essere costituita anche da tre computer posizionati nella stessa stanza, ma, in pratica quando

---

alla preimmagine (deve essere computazionalmente intrattabile "invertire" la funzione di hash, vale a dire trovare l'input partendo da un dato output); 3) resistenza alla seconda preimmagine (deve essere computazionalmente intrattabile trovare un secondo input in collisione con un input specifico) sia le funzioni di hash convenzionali che quelle crittografiche produrranno sempre un output della stessa dimensione: questa proprietà deterministica significa che, fino a quando l'input non cambia, l'algoritmo di hashing continuerà a produrre lo stesso output (noto come *digest* o hash).

[30] Un albero di Merkle (dal nome di Ralph Merkle, il matematico che lo scoprì negli anni '80) è un sistema utilizzato per verificare in modo efficiente e rapido grandi quantità di dati in poco tempo. Nel caso in cui si voglia scaricare, per esempio, un file di grandi dimensioni cifrato con una funzione di hash (si veda nota precedente 29), risulterebbe eccessivamente lungo e complicato verificare il corrispondente hash del file scaricato con quello del file originario (al fine di evitare il download di un file contraffatto, che magari installi un virus nel computer). Gli alberi di Merkle scompongono, pertanto, un file in singoli frammenti ma presentano anche un "Merkle root", cioè la radice di Merkle, anch'essa cifrata con la funzione di hash: pertanto, tornando all'esempio precedente, sarà sufficiente confrontare la Merkle root del file scaricato con quella del file originario per verificare che il file scaricato sia realmente il file che si voleva scaricare all'origine e senza necessità di procedere alla verifica di ogni singolo file incluso nel pacchetto, ottenendo pertanto un notevole risparmio di tempo.

si parla di "blockchain" ci si riferisce alle catene a blocchi costituite da migliaia di nodi: la rete Bitcoin, per esempio, è formata da 15.794 nodi [31] mentre la rete Ethereum è attualmente formata da 5.756 nodi [32].

Ogni blocco viene validato dai cosiddetti *miners* [33], utilizzando degli specifici protocolli, in genere consistenti nella soluzione di un problema computazionale, i principali dei quali sono il sistema del *proof of work* e quello del *proof of stake* [34]. Quando un blocco di dati è validato esso è registrato, in ordine cronologico, in tutti i blocchi della catena e informaticamente saldato a tutti i blocchi precedenti: ciò significa che per modificare un'informazione contenuta in un blocco, la si deve poter modificare in tutti i blocchi della catena, un'operazione tendenzialmente impossibile [35] da cui deriva una delle caratteristiche fondamentali delle blockchain, vale a dire l'inalterabilità [36].

I protocolli utilizzati dai *miners* per validare i vari blocchi sono detti protocolli di consenso, cioè un meccanismo che permette a diversi utenti, o computer, di coordinarsi in un contesto distribuito. Una delle caratteristiche maggiormente peculiari delle blockchain è

---

[31] I dati sono tratti da https://bitnodes.io/ dove sono anche presenti le statistiche suddivise per i vari paesi.

[32] I dati sono tratti da https://ethernodes.org/ dove sono anche presenti le statistiche suddivise per i vari paesi.

[33] Sui *miners* si veda *infra* in questo stesso paragrafo.

[34] Sulla differenza tra *proof of work* e *proof of stake* si veda *infra* in questo stesso paragrafo.

[35] In effetti, da un punto di vista strettamente tecnico, le blockchain non sono completamente inalterabili. Le blockchain sono, infatti, comunque, soggette al cosiddetto 51% *attack*, cioè al caso in cui un agente terzo s'impossessi del 51% dei nodi con la conseguenza di poter impedire la registrazione di nuovi blocchi o anche, in alcuni casi, di annullare le transazioni già registrate nelle blockchain. Da questo punto di vista, maggiori sono i nodi che compongono le blockchain e più resistente è la blockchain a un 51% *attack*. Si sono verificati, per esempio, casi di 51% *attack* contro Monacoin, Bitcoin Gold o ZenCash.

[36] Si veda *infra*, in questo stesso paragrafo, per un approfondimento su questo aspetto.

che le procedure di validazione dei blocchi sono decentralizzate [37]: sono i vari *miners* a validare nuovi blocchi sulla base delle regole contenute nei protocolli informatici che sono alla base della blockchain stessa e non un unico soggetto che, in maniera centralizzata, decide quali dati possano essere inseriti in un registro, come avviene, per esempio, in Italia, con la Conservatoria dei registri immobiliari, dove è il Conservatore a decidere, in modo centralizzato, se trascrivere o meno un atto di compravendita o iscrivere un'ipoteca su un dato immobile [38].

Il protocollo che è stato creato per primo quando è stata realizzata la blockchain dei bitcoin, e che ancora oggi ne regolamenta il funzionamento, è il *proof of work* [39]: tale meccanismo di consenso si basa su una sorta di gara tra i *miners* in quanto il primo che risolve il problema computazionale e lo presenta ai nodi della rete che lo accettano, validandolo, riceve come ricompensa delle criptovalute stesse del sistema (dei bitcoin, per esempio).

L'attività dei *miners* è, quindi, una vera e propria attività d'impresa che richiede elevati investimenti [40], a fronte dei quali si viene ripagati con delle criptovalute native della blockchain di riferimento. La "gara tra i *miners*" su cui si basa il protocollo del *proof of work* ha sollevato un vivace dibattito relativamente agli effetti negativi per il cambio climatico che si producono a seguito del con-

---

[37] Sulla decentralizzazione si veda il paragrafo successivo.

[38] Naturalmente anche il Conservatore sottostà alle regole poste del Codice civile sulla trascrizione degli atti, ma l'interpretazione di tali regole (e, quindi, in ultima analisi, la decisione su cosa trascrivere) è demandata al Conservatore stesso, fermo restando la possibilità di presentare un reclamo all'autorità giudiziaria nel caso in cui il Conservatore trascriva o iscriva un atto con riserva.

[39] Se, sotto il profilo teorico, la differenza tra il modello *proof of work* e quello *proof of stake* è chiara, nella pratica, si danno diversi modelli ibridi e soluzioni tecnologiche innovative le quali, sebbene costruite a partire dai due modelli di base citati, hanno, poi, realizzato dei protocolli di consenso altamente complessi.

[40] Gli investimenti, in particolare, consisteranno in costi d'impianto, cioè la disponibilità di data center e centri di calcolo che contengano apparecchiature informatiche in grado di sviluppare elevate potenze di calcolo e costi variabili, consistenti essenzialmente nell'energia necessaria al funzionamento delle apparecchiature informatiche.

sumo di energia utilizzata dai vari centri di calcolo che competono per risolvere il problema computazionale [41]. L'idea che il sistema di validazione del *proof of work* sia particolarmente energivoro è fortemente avversata dalla comunità cripto, anche sulla base di studi che evidenziano il bassissimo livello di consumo energetico di blockchain come quella dei bitcoin rispetto ad altre industrie [42].

Il secondo protocollo maggiormente diffuso è il cosiddetto *proof of stake*, in base al quale i *miners* per validare un blocco devono mettere "*in staking*", cioè vincolare a garanzia, delle criptovalute, con il rischio di perderle qualora il blocco non sia, poi, validato dalla rete: maggiore è la quantità di criptomoneta che un validatore sarà in grado di mettere *in staking* e maggiori saranno le possibilità che potrà vincere la gara e ottenere la ricompensa [43].

Il *proof of stake* non solleva i problemi ambientali che solleva il *proof of work* in quanto non si verifica la gara tra i *miners* per risolvere il problema computazionale [44] e, conseguentemente, non c'è "spreco di energia", ma è meno sicuro in quanto un attacco informatico può essere realizzato facilmente nel caso di elevate disponibilità di criptovalute da mettere *in staking*, soprattutto nel caso delle blockchain a bassa capitalizzazione.

A settembre 2022, la blockchain Ethereum, essenzialmente a fi-

---

[41] Indipendentemente dalla veridicità o meno della problematica ambientale del *proof of work*, è sicuramente vero che tale protocollo rimane quello maggiormente affidabile sotto il profilo della sicurezza informatica e, coerentemente, la blockchain dei bitcoin rimane quella più resiliente dal punto di vista della cybersecurity. Va, peraltro, notato che il regolamento UE 2023/1114, noto come MiCA, su cui si veda *infra*, cap. IV, contiene norme specificamente volte a limitare l'uso di risorse energetiche.

[42] Uno di tali studi è accessibile al seguente URL: https://bitcoinmagazine.com/business/bitcoin-energy-use-compare-industry.

[43] Si noti che anche il protocollo *proof of work*, in realtà, richiede la disponibilità di elevate quantità di capitali finanziari: come visto alla nota 40 precedente, i *miners* del *proof of work* devono affrontare elevati investimenti in costi d'impianto e in costi fissi.

[44] In effetti, nel *proof of stake* si verifica una gara tra pochissimi soggetti come conseguenza della barriera all'entrata costituita dalla disponibilità di risorse finanziarie necessarie per effettuare lo *staking*.

ni di maggiore sostenibilità ambientale, ha abbandonato il *proof of work* ed è passata al protocollo *proof of stake* [45].

Un principio fondamentale della blockchain è che leggere dei dati in blockchain non costa, mentre si paga ogni volta che si scrive nel registro delle blockchain: trasferire criptovalute, creare un NFT, acquistare un NFT, effettuare il *deployment* di uno smart contract sono tutti esempi di azioni che richiedono di pagare un costo nella moneta propria della blockchain detta *gas fee* [46].

Una distinzione importante nell'ambito delle blockchain è quella tra le catene a blocchi pubbliche e quelle private.

Le blockchain sono dette pubbliche o *permissionless* [47] (letteralmente senza il permesso), quando ciascun soggetto può partecipare alla rete stessa e ciascuno può liberamente prendere parte alla validazione dei blocchi attraverso il meccanismo di consenso in uso nella blockchain stessa. Le blockchain *permissionless* sono reti o community dove nessuno ha il potere di controllare in modo discrezionale l'entrata o l'uscita dalla rete stessa (o le procedure di funzionamento) e, una volta soddisfatte le condizioni previste dal protocollo informatico della blockchain, l'accesso alla rete non può essere negato.

Le blockchain private, o *permissioned*, sono, invece, catene a blocchi centralizzate nel senso che è presente un'autorità che decide, centralmente e discrezionalmente, chi possa essere parte della rete: per esempio, le blockchain create dalle imprese che

---

[45] Si tratta del cosiddetto "The Merge", avvenuto il 15 settembre 2022 e che ha ridotto il consumo di energia della rete Ethereum del 99,99%. Per maggiori informazioni si consulti il comunicato ufficiale di Ethereum disponibile al seguente URL: https://ethereum.org/en/roadmap/merge/.

[46] Le *gas fees* sono il costo che si paga in quanto ogni singola transazione (che andrà a far parte di un blocco specifico) deve essere aggiunta dai *miners* alla catena a blocchi attraverso il *proof of work* o il *proof of stake*. Le *gas fees* sono, in altri termini, il costo che si paga all'infrastruttura che compone la blockchain per registrare nuove transazioni (in pratica ai *miners* per la loro attività di validazione).

[47] "*Permissionless*" significa letteralmente senza permesso ma, in senso figurato, tale attributo rimanda al concetto di decentralizzazione.

operano nel settore delle grandi infrastrutture per la gestione delle proprie *supply chain* sono tipicamente private, in quanto è l'EPC a decidere, centralmente, quali soggetti potranno farne parte (in quanto sub-fornitori) e quali non possano accedere alla catena a blocchi.

Le maggiori blockchain diffuse a livello internazionale come la catena a blocchi Bitcoin o Ethereum sono blockchain *permissionless*: in effetti, il mondo cripto, che in pieno bull market aveva abbondantemente superato il trilione di capitalizzazione di asset digitali[48] ma, anche nel bear market, è attestato nella pur sempre rispettabile somma di 900 miliardi di dollari di capitalizzazione[49] è costituito al 99,5% da blockchain *permissionless*, mentre il fenomeno delle blockchain private è praticamente ininfluente in termini d'importanza di mercato. Inoltre, non essendo le blockchain *permissioned* decentralizzate, non possono essere ascritte, almeno sotto il profilo "culturale", alla linea di sviluppo che dai Cypherpunks ha portato alla blockchain di Bitcoin e di Ethereum: le blockchain *permissioned* implementano formalmente il sistema tecnologico delle catene a blocchi ma, privandolo del carattere della decentralizzazione, lo rendono una mera variante tecnologica di un classico database centralizzato.

Nell'ambito delle blockchain è anche importante distinguere tra *layer 1* e *layer 2*[50]. Il *layer* 1, nell'ambito delle grandi blockchain *permissionless*, è la rete principale, la cosiddetta *mainnet*[51] cioè le blockchain di livello 1. Le *layer 2* delle blockchain sono, invece, delle catene a blocchi secondarie ma collegate alla *mainnet* principale (cioè al *layer 1*), le quali sono nate per risolvere il problema di

---

[48] In particolare, il livello più alto di capitalizzazione dei *crypto assets* si è avuta il 13 novembre 2021 con un valore di 2,82 trilioni di dollari americani. Fonte: https://coinmarketcap.com/charts/.

[49] Alla data del 11 novembre 2023 il livello di capitalizzazione dei *crypto assets* si attesta a 1,42 trilioni di dollari americani Fonte: https://coinmarketcap.com/charts/.

[50] Le blockchain *layer* 2 sono anche dette *sidechains*.

[51] In inglese, "*main net*" cioè "rete principale".

"*scalability*" [52] delle blockchain, cioè della capacità del sistema di gestire quantitativi sempre più crescenti di utenti e transazioni.

In linea di principio, sarebbe sempre possibile aumentare le dimensioni di ogni singolo blocco ma ciò richiederebbe computers (cioè nodi) di enormi dimensioni e questo creerebbe una barriera all'ingresso per l'aggiunta di nuovi nodi a ogni singola blockchain. La soluzione a tale problema è appunto la creazione di uno o più *layer 2*: in ciascuno di questi *layer 2*, infatti, gli input di migliaia di utenti sono "impacchettati" (o "*roll up*" in inglese) e registrati come un'unica transazione nel *layer 1* che ne verifica la validità [53].

Ci sono, in genere, due sistemi di impacchettamento e validazione dei dati dal *layer 2* al layer 1: l'*optimistic roll up* e il *validity roll up*. L'*optimistic roll up*, come il nome stesso suggerisce, si basa su un principio di ottimismo: il sistema parte dall'idea che la transazione registrata sul *layer 2* sia corretta e, pertanto, procede immediatamente a introdurla nella catena a blocchi del *layer* 1 senza averla previamente verificata.

Il sistema basato sul *validity roll up*, invece, impacchetta le transazioni in un unico blocco e le posta nel *layer 1* ma, poi, richiede una prova di validità che "dimostri" al *layer 1* che tutte le transazioni nel pacchetto sono corrette e che, quindi, non devono essere rieseguite.

Il *validity roll up* è, altresì, detto *zero knowledge*, che è una particolare tecnica di validazione, la quale permette di verificare determinati presupposti senza comunicare ulteriori informazioni a chi effet-

---

[52] Il problema della "*scalability*" delle blockchain si riferisce al fatto che, con la crescita delle community e degli asset digitali su una data blockchain (in altre parole, del traffico sulla catena a blocchi), il sistema è a rischio d'ingolfamento per una sproporzione tra il traffico in esso attivo e le capacità della infrastruttura di base di poterlo gestire. Pertanto, si intende "scalabilità" nel senso della capacità del sistema di crescere, mantenendo inalterati i livelli di efficienza dello stesso.

[53] La tecnica dell'impacchettamento permette anche di ridurre il costo delle *gas fees*. Le *gas fees* in Polygon, per esempio, il più noto *layer* 2 di Ethereum, sono estremamente più basse di quelle di Ethereum.

tua la verifica, cioè preservando la confidenzialità delle informazioni (appunto a conoscenza zero, o "*zero knowledge*" in inglese)[54].

3. I caratteri strutturali delle blockchain *permissionless*

Appare utile nel presente paragrafo elencare i caratteri strutturali delle blockchain *permissionless* in quanto si tratta di elementi che caratterizzano, per osmosi, anche gli NFT[55] e che è importante tenere presente per poter avere una comprensione effettiva dei non-fungible token. Tali caratteristiche sono: 1) la certezza relativamente alla registrazione dei dati; 2) l'immodificabilità dei dati registrati in blockchain; 3) la decentralizzazione del sistema delle blockchain; 4) la deterritorializzazione nel senso di un sistema non inquadrabile *by default* in un particolare territorio o Stato nazionale; 5) i protocolli informatici e crittografici come base della "fiducia di sistema"; 6) la tokenizzazione o tokenomics come meccanismo economico di base per la regolamentazione del sistema; 7) l'anonimato delle identità digitali operanti nelle blockchain.

La prima caratteristica delle blockchain è quella della certezza con riferimento al fatto che i dati sono stati registrati in essa. Se, per esempio, può essere relativamente facile contraffare un registro cartaceo notarile o un database informatico centralizzato, è, invece, estremamente complicato, hackerare e contraffare migliaia di computer che costituiscono i nodi di una blockchain[56]. L'elevato livel-

[54] Il concetto di *zero knowledge* è fondamentale per l'infrastruttura delle blockchain ed è sempre più usato nell'ambito delle soluzioni tecnologiche relative all'identità digitale (inclusa la cosiddetta "*decentralized identity*"). Si veda, l'articolo di Vitalik Buterin, *The different types of ZK-EVMs*, in www.vitalik.ca, 4 agosto 2022 disponibile al seguente URL: https://vitalik.ca/general/2022/08/04/zkevm.html.

[55] Alcuni degli elementi qui descritti saranno, in realtà esaminati approfonditamente nei paragrafi successivi del presente capitolo ma, per ragioni di organizzazione sistemica del capitolo e per offrire al lettore una visione d'insieme fin dall'inizio, sono stati qui riassunti.

[56] Si veda *supra*, nota 35.

lo di certezza di una blockchain dipende, tuttavia, dalle dimensioni della blockchain stessa: se la certezza è massima per le blockchain di maggiori dimensioni, come quella di Bitcoin, Ethereum, Solana o Cardano, il discorso cambia nel caso delle blockchain formate da pochi nodi (s'immagini una blockchain formata da cinque nodi, come pure è perfettamente possibile) che, in genere, coincidono con le blockchain private.

La certezza dei dati registrati in una blockchain, quindi, non è una caratteristica assoluta ma va valutata in funzione delle dimensioni della blockchain stessa, vale a dire del numero di nodi che la compongono [57].

Inoltre, e soprattutto, va rimarcato che la certezza è limitata al fatto che una determinata serie di dati siano stati immessi in una data blockchain, in una certa data e da un certo indirizzo presente sulla blockchain stessa, ma nulla prova in relazione alla verità di quanto è stato registrato nella blockchain [58]. Pertanto, se in una blockchain si inseriscono informazioni false (per esempio, si registra l'informazione che Tizio il 15 giugno 2023 era a Roma, mentre invece si trovava a Milano), tali rimangono e non "diventano vere" perché sono state inserite in una blockchain. L'unico effetto dell'inserimento in blockchain in casi simili a quelli appena citati è solamente quello di avere la certezza che determinate informazioni siano state registrate da un certo indirizzo e in una certa data, ma tali informazioni, se erano false all'origine, lo rimarranno anche dopo l'inserimento in blockchain [59].

"Certo", peraltro, non significa nemmeno lecito, né costitutivo di diritti: proprio il meccanismo della decentralizzazione [60] delle blockchain impedisce che, *by default*, siano effettuati dei controlli da qualcuno sulla liceità delle informazioni che si regi-

---

[57] In sostanza, la certezza delle blockchain corrisponde alla sicurezza della catena a blocchi rispetto a eventuali attacchi esterni. Si veda anche *supra*, nota 35.

[58] Si veda *infra*, in questo capitolo, par. 4, per quanto riguarda il valore giuridico dei dati registrati in blockchain nell'ordinamento italiano.

[59] Il concetto è noto in informatica con l'acronimo GIGO: *garbage in, garbage out*.

[60] Sul concetto di decentralizzazione si veda *infra* in questo medesimo paragrafo.

strano in blockchain; da questo punto di vista la blockchain è meno affidabile, per esempio, dello strumento della dichiarazione a un pubblico ufficiale nella quale si possono inserire dichiarazioni false ma non illecite (poiché il pubblico ufficiale non le riceverebbe).

Inoltre, e soprattutto, la nozione di "certezza" riferita alle blockchain non coincide nemmeno con il concetto di certificazione: ciò è di particolare rilevanza per gli NFT, in quanto è ricorrente l'affermazione che gli NFT costituiscano il certificato di autenticità del file-artwork incorporato nel NFT stesso, ma l'unica tipologia di certificazione riscontrabile nelle blockchain è che un determinato NFT, dal punto di vista delle regole interne delle blockchain, appartiene a un determinato wallet (in gergo è stato "mintato" da quel wallet in un dato momento), ciò, però, nulla ha a che vedere con il concetto di titolarità dei diritti di proprietà intellettuale sul file linkato a tale NFT. Se qualcuno, infatti, per esempio, scaricasse in modo illecito un file immagine e lo usasse per creare un NFT (cioè lo usasse come file immagine da linkare al token non fungibile), allora, dal punto di vista della blockchain, quell'NFT "appartiene" al wallet di quella persona ma, dal punto di vista dell'ordinamento giuridico, si è trattato di una violazione del soggetto che detiene i diritti di proprietà intellettuale su quell'immagine e tali diritti di proprietà non vengono sicuramente meno per effetto dell'inserimento in blockchain.

La seconda caratteristica delle blockchain è l'immodificabilità: una volta che un blocco è stato registrato nel registro distribuito, le informazioni in esso contenute non sono modificabili a meno di cambiare tutte gli altri blocchi che formano la catena: un'operazione difficilmente realizzabile (almeno nel caso delle blockchain formate da molteplici nodi) [61].

Va precisato, tuttavia, che "immodificabile" non significa (almeno non necessariamente) irrevocabile con riferimento a un token, in quanto, da un punto di vista tecnico, è perfettamente possibile creare degli smart contract che generino dei token che, a date

[61] Si veda *supra*, in questo stesso paragrafo e, inoltre, nota 35.

condizioni, sono revocabili [62]. In tal caso, va operata una distinzione: l'immodificabilità è una caratteristica del codice sorgente dello smart contract validato attraverso i protocolli di consenso e registrato nella blockchain, mentre la revocabilità del token dipende dalle regole di funzionamento contenute nello smart contract stesso [63].

Il terzo elemento caratteristico della blockchain è la decentralizzazione [64]. La caratteristica della decentralizzazione, da un punto di vista strettamente tecnico, può essere intesa in almeno due accezioni: in un primo senso, i dati inseriti in blockchain sono decentralizzati nel senso che risiedono nell'insieme dei computer, dei nodi cioè, che compongono la rete e non in un database centralizzato; in una seconda accezione, le blockchain sono decentralizzate con riferimento al fatto che ciascuno può registrare dei dati in blockchain purché rispetti i protocolli informatici che costituiscono l'insieme di regole su cui si basa la blockchain stessa e, quindi, che tali dati siano correttamente validati dal sistema attraverso il sistema del *proof of work* o del *proof of stake*.

In senso più ampio e meno tecnico, tuttavia, la decentralizzazione indica un sistema connotato dalla mancanza di una forma di governo autoritativo e gerarchico il quale è sostituito da rapporti (tendenzialmente) orizzontali tra i membri del sistema e il cui funzionamento si basa sull'osservanza di regole oggettive e l'applicazione di protocolli informatici.

Il contraltare negativo della decentralizzazione è che, in caso di controversia [65] o di incidenti [66], non ci sia alcuna autorità superiore

---

[62] Da un punto di vista tecnico il token viene distrutto o "*burned*".

[63] La revocabilità deve essere, quindi, prevista originariamente dallo smart contract. In assenza di un'espressa funzione che permetta di "distruggere" dei token, essi saranno irrevocabili. Sugli smart contract si veda *infra*, in questo capitolo, par. 5.

[64] Dal punto di vista delle community che compongono l'ecosistema cripto, la decentralizzazione ha trovato espressione nelle cosiddette *decentralized autonomous organizations* o DAO.

[65] Si pensi a una lite giudiziaria sulla proprietà di un NFT.

[66] Per esempio, la perdita della chiave privata per accedere al wallet.

cui si possa ricorrere per risolvere la questione: sono noti, per esempio, i casi di smarrimento della chiave privata di un wallet con perdita definitiva e irreversibile di tutti i *crypto assets* in esso presenti, per la semplice ragione che non esiste alcun autorità sovraordinata in grado di ri-generare una nuova chiave privata come, invece, potrebbe fare una banca nel caso di smarrimento della password di accesso all'home banking.

Un'ulteriore caratteristica della blockchain è la deterritorializzazione: anche nelle blockchain formate da pochi nodi situati all'interno di un unico paese il dato inserito in blockchain non risiede in un unico luogo (come avviene per esempio nei database centralizzati) ma è presente simultaneamente in tutti i nodi che formano la blockchain; nel caso delle maggiori blockchain come Ethereum, quindi, il dato digitale è registrato contemporaneamente in tutti i nodi sparsi praticamente in tutto il mondo [67], in un superamento ideale dei confini politici degli Stati-nazione.

Un'ulteriore caratteristica delle blockchain è che il collante che tiene insieme l'intero sistema è la "fiducia" nei protocolli informatici e nella crittografia che costituiscono le basi fondative, da un punto di vista tecnologico, dei sistemi stessi [68]. In questo senso, il concetto di sistema è riferito non tanto al meccanismo informatico delle catene a blocchi quanto alla comunità di persone (sviluppatori, investitori, utenti, etc.) che operano e interagiscono in esse: in altri termini, chi opera nel mondo cripto, e in particolare nelle maggiori blockchain *permissionless*, si affida in effetti alla validità e al funzionamento dei protocolli informatici che regolano la blockchain e non all'operato degli organi di vertice del sistema (che, peraltro, in quanto decentralizzato, non esistono).

Un altro elemento caratteristico della blockchain è la cosiddetta

---

[67] La deterritorializzazione delle blockchain implica la difficoltà di adattare a tali contesti sistemi di compliance che presuppongono un soggetto "centralizzato" responsabile di eventuali violazioni della normativa applicabile: nel caso del regolamento europeo sulla privacy 2016/679, noto come GDPR, è altamente problematico identificare chi sia nell'ambito delle blockchain il "*controller*" *ex* art. 24 del regolamento stesso. Si veda, in proposito, *infra*, cap. III, par. 6.

[68] Su questo punto si veda *supra*, par. 1, in questo capitolo.