UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA TRIENNALE IN INGEGNERIA BIOMEDICA

"L'USO DELLA BLOCKCHAIN IN IMAGING BIOMEDICALE"

Laureanda: Padoan Vittoria

Relatore: Prof. Veronese Mattia

Correlatrice: Dott.ssa Nordio Giovanna

ANNO ACCADEMICO 2021 – 2022

Data di laurea: 23 settembre 2022

INDICE

Indice delle figure:

Indice delle tabelle:

SOMMARIO

Gli anni che stiamo vivendo sono senz'altro lo sfondo di uno scenario che ha come protagonista il progresso tecnologico. La tecnologia blockchain è una tra le innovazioni più discusse e in risalto dei nostri giorni. La blockchain nasce da esigenze economico-finanziare portando con sé la creazione delle monete digitali, ovvero le criptovalute, usate come metodo di pagamento alternativo per transazioni online, al fine di aggirare i sistemi di controllo delle banche centrali. I suoi utilizzi si sono poi espansi nei settori più disparati come nella compravendita dei beni di seconda mano, nel voto elettorale, nel mondo accademico e scolastico, nel mercato delle energie rinnovabili e nel monitoraggio dei dati ambientali.

Risultano rilevanti le soluzioni che questa tecnologia fornisce all'ambito biomedicale, cercando di dare una valida alternativa laddove sono presenti problematiche, ad esempio nell'attuale gestione dei dati delle cartelle cliniche, nel monitoraggio remoto dei pazienti, nella ricerca clinica e nell'analisi di dati sanitari forniti da esami specifici o raccolti da sensori intelligenti. In particolare, il presente elaborato ha l'obiettivo di discutere i possibili impieghi della tecnologia blockchain nell'imaging biomedicale.

Innanzitutto, verranno descritti i principi fondamentali sui quali si fonda la blockchain ovvero come è strutturata, in che modo viene costruita e le proprietà che possono rendere interessante il suo utilizzo.

Verrà poi dato un quadro generale dell'imaging biomedico, definendo i suoi utilizzi in campo clinico e, partendo da considerazioni riguardo le nuove necessità ed esigenze di tale ambito, si andranno a discutere i possibili vantaggi, i rischi associati e le limitazioni che si riscontrano nell'applicare la tecnologia blockchain nella diagnostica per immagini facendo riferimento ad alcuni esempi che sono già stati messi in pratica.

Le caratteristiche di decentralizzazione, sicurezza e tracciabilità rendono la tecnologia blockchain una soluzione promettente in ambito di imaging biomedicale, proponendo possibili soluzioni a problemi attuali quali l'integrità dei dati, la loro condivisione e provenienza.

1. OVERVIEW SULLA TECNOLOGIA BLOCKCHAIN

1.1 La nascita della blockchain

Il settore economico-finanziario è stato il primo ad utilizzare il concetto di blockchain.

I due termini "catena" e "blocchi" fanno la loro comparsa nell'ottobre del 2008 nel white paper di Satoshi Nakamoto (un gruppo di persone o un unico individuo la cui identità rimane ancora ad oggi ignota) intitolato "*Bitcoin: A peer-to-peer electronic cash system"* [1].

Questo documento ha posto le basi matematiche per un sistema monetario elettronico innovativo, che prevede l'utilizzo di firme digitali in una rete peer-to-peer pubblica. [2]

L'esigenza di un nuovo sistema di pagamento si è sviluppata in risposta alla crisi finanziaria del 2007 con la conseguente perdita di fiducia generale che, fino a quel momento, era stata riposta nelle istituzioni bancarie. Diventa necessario dunque sovvertire l'ordinamento bancario proponendone uno decentralizzato, in cui il potere non sia più nelle mani di una sola ed unica figura centrale. È indubbiamente chiaro quest'ultimo punto dalle parole del trattato di Satoshi Nakamoto: "Il problema alla base delle valute convenzionali è dovuto alla quantità di fiducia necessaria per far funzionare il sistema. Dobbiamo fidarci del fatto che le banche non svalutino la moneta, ma purtroppo la storia è piena di momenti in cui questa fiducia non è stata rispettata. Dobbiamo fidarci del fatto che le banche conservano i nostri soldi, ma spesso sono scoppiate bolle legate al credito bancario, e solo una frazione dei soldi era effettivamente in possesso della banca. Dobbiamo riporre in questa istituzione la nostra fiducia in termini di privacy, e fidarci del fatto che i ladri d'identità non svuotino i nostri conti correnti." [1]

Il Bitcoin è una tra le implementazioni più conosciute della tecnologia blockchain, nota e ideata grazie all'esperienza di progetti che erano già stati precedentemente testati. Bitcoin è definito come moneta digitale decentralizzata, scambiata in una rete di nodi paritari, ovvero tutti con lo stesso potere decisionale all'interno della catena blockchain. In questo modo tra i nodi non esiste più un rapporto *client-server,* ma tutti contemporaneamente ricoprono il ruolo sia di *client* che di *server*. Inoltre, tramite l'utilizzo della crittografia che sta alla base di tutte le tecnologie blockchain, è stato possibile arginare il problema del *double-spending*. Avendo a che fare con contante digitale era necessario trovare un modo per garantire che denaro già speso non venisse utilizzato ulteriori volte.

L'interesse crescente sulla criptovaluta Bitcoin, e in generale sulla blockchain, sta proprio nella sua decentralizzazione assicurata dalla possibilità per ogni individuo o società di gestire valute virtuali senza la supervisione di un'autorità governativa. [3]

Successivamente a Bitcoin sono stati creati più di 1000 progetti negli ultimi anni sostenuti da enormi investimenti e coinvolgendo aziende importanti come Amazon, Google, Microsoft e altre. [4]

Esistono molteplici protocolli basati sulle tecnologie blockchain; uno di questi è Ethereum, progettato da Vitalik Buterin nel 2013. [5] L'interesse in questo network è giustificato poiché si tratta di un vero e proprio server per contratti (*smart contracts*), che permettono di portare a termine o interrompere una transazione al verificarsi di determinate circostanze e condizioni. [4] Tali smart contracts sono stati utilizzati non solo in ambito finanziario, ma anche nel settore biomedico, in quanto permettono di gestire transazioni più complesse. [6]

1.2 Definizioni di blockchain

La blockchain presenta differenti e numerosi utilizzi e, in base al contesto in cui viene inserita, è possibile concentrarsi su diverse sfaccettature, come sulla sua struttura, sulle diverse tecnologie che ne definiscono il funzionamento o sull'impatto nella società e negli ambiti in cui viene applicata.

Iniziando da una considerazione più ampia e generale, alcuni definiscono la blockchain come il "nuovo internet" o "l'internet delle transazioni", ovvero un network che permette in modo semplice e veloce di scambiare valore su internet. [7]

Da un punto di vista più specifico e strutturale, la blockchain è una rete decentralizzata che gestisce diverse tipologie di dati (denaro o informazioni), un vero e proprio libro mastro digitale e distribuito. (Figura 1) [8] Nei database decentralizzati non esiste nessuna macchina centrale che gestisce l'intero archivio, ma più macchine collaborano insieme.

In aggiunta, nella blockchain, tutti i server hanno gli stessi diritti e contengono le stesse informazioni. Ogni nodo partecipa quindi al processo di archiviazione all'interno della rete, che prende il nome di rete peer-to-peer, per raggiungere un obiettivo condiviso e comune.

In questo modo tutti gli utenti hanno la possibilità di partecipare, di verificare le informazioni, validarle e quindi consultarle. Per queste sue caratteristiche e modalità la blockchain fa parte delle *Distributed Ledger Technology*. [7] (Tabella 1)

Questo registro è formato da una sequenza di blocchi, in continua crescita, il cui ordine dipende da un algoritmo matematico chiamato "funzione di hash".

	Rete centralizzata	Rete decentralizzata
Architettura	Ha un punto centrale di errore che renderebbe non funzionante la rete.	I dati sono salvati in diversi nodi della rete (ridondanza), non c'è quindi un unico punto di possibile fallimento ma molteplici, rendendo difficile interrompere il suo funzionamento.
Autorità	È presente un'autorità centrale in cui riporre fiducia assolta.	Nessuno ha il controllo di tutta la rete e per ogni operazione ci deve essere un consenso da parte della maggior parte dei nodi.
Logica	C'è solo un unico stato del sistema, su cui concordano tutti i partecipanti.	Ci sono più versioni salvate di copie di dati perché ogni nodo può modificare la sua versione. Questo non provoca alterazioni nel funzionamento del sistema.

Tabella 1: differenza tra una rete centralizzata e decentralizzata

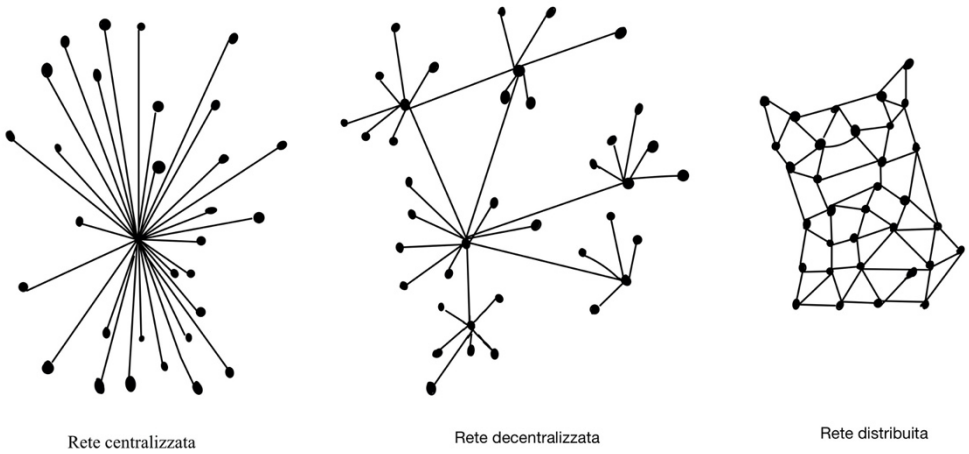

Figura 1: rappresentazione grafica di una rete centralizzata, decentralizzata e distribuita

1.2.1 Il ledger

Il ledger è un registro che raccoglie le transazioni, ovvero un libro mastro dove vengono memorizzate le operazioni effettuate.

La blockchain è definita come ledger digitale, più nello specifico appartiene alla famiglia dei Distributed Ledger, database in cui tutti i nodi sono indipendenti gli uni dagli altri. La differenza tra i ledger e i database tradizionali risiede nel fatto che, se nei primi è possibile il solo inserimento di informazioni, nei secondi si aggiunge la possibilità di modificarle ed eliminarle. I ledger risultano perciò più vincolati nelle operazioni disponibili e si distinguono sia per la loro tipologia e struttura di rete sia per il meccanismo di archiviazione. [8]

La blockchain è un particolare tipo di ledger che impiega uno schema a catena di blocchi (Figura 3) e che prevede un unico asset (criptovaluta o token) da trasferire.

Gli algoritmi di consenso su cui si basano le tecnologie blockchain (e quindi i Distributed Ledger) comportano altre differenze sostanziali con i database tradizionali; quest'ultimi eseguono più operazioni alla volta risultando anche meno dispendiosi in termini computazionali e di costi.

Dalle considerazioni analizzate ne deriva che questi tre sistemi, database, Ledger e blockchain, sono pensati per scopi e scenari diversi. (Figura 2) La preferenza di utilizzo tra uno e l'altro è determinata solamente dal tipo di problema che si sta affrontando.

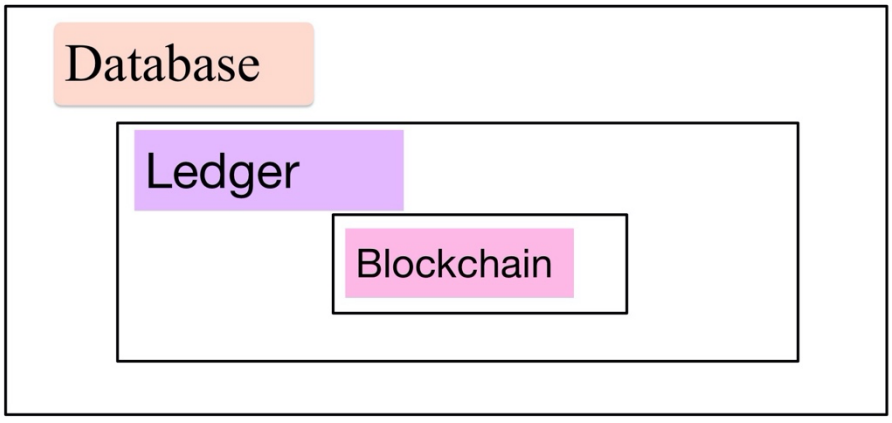

Figura 2: classificazione di database, ledger e blockchain

Nell'ambito biomedicale sono richieste alcune proprietà quali la fiducia, l'immutabilità, la sicurezza e allo stesso tempo l'eliminazione di qualsiasi dipendenza da un punto di

riferimento centrale che controlli gli accessi e le transazioni. Per questo motivo è di interesse studiare l'applicazione del sistema blockchain nel dominio biomedico.

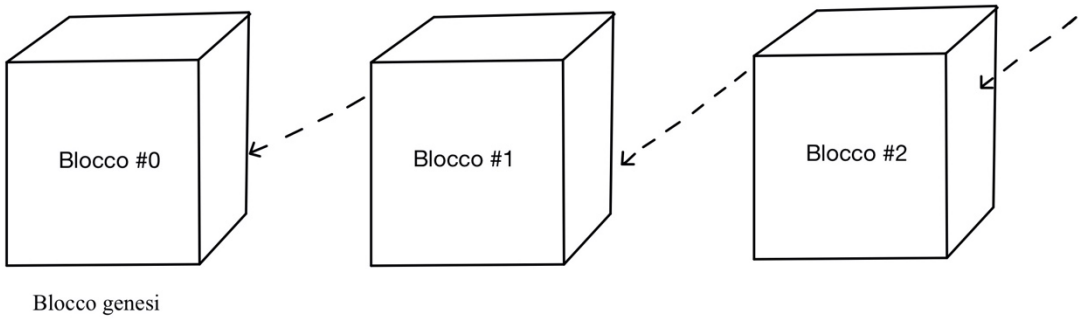

Figura 3: il ledger digitale su cui si basa la blockchain è strutturato come una catena di blocchi

1.2.2 I blocchi

La struttura fisica su cui si basa la blockchain consiste in una catena di blocchi aggiunti in modo sequenziale e tra cui si instaura un rapporto sicuro di dipendenza l'uno dall'altro in modo irreversibile. Questo concatenamento è dovuto ad una funzione matematica, chiamata *hash crittografico*, il cui funzionamento verrà spiegato successivamente. Ogni blocco è quindi dipendente dall'hash del blocco precedente, mentre il primo blocco della sequenza è chiamato "blocco genesi" e non presenta nessuna subordinazione dagli altri (Figura 4). La struttura, la dimensione dei blocchi e le informazioni contenute possono cambiare a seconda dello scopo per cui è progettata.

In generale si può schematizzare la struttura di un blocco secondo una suddivisione in due parti:

- **Block Header**, contenente:
  - Il numero del blocco, anche detto altezza del blocco
  - Il valore dell'hash del blocco precedente
  - Una rappresentazione hash dei dati del blocco
  - Il timestamp
  - La grandezza del blocco
  - Il valore di nonce, un numero manipolato dal nodo per risolvere l'hash crittografico
- **Block Data**, che comprende:
  - Un elenco di informazioni/ transazioni inclusi nel blocco

- Altri dati che variano a seconda del tipo di blockchain usata [9]

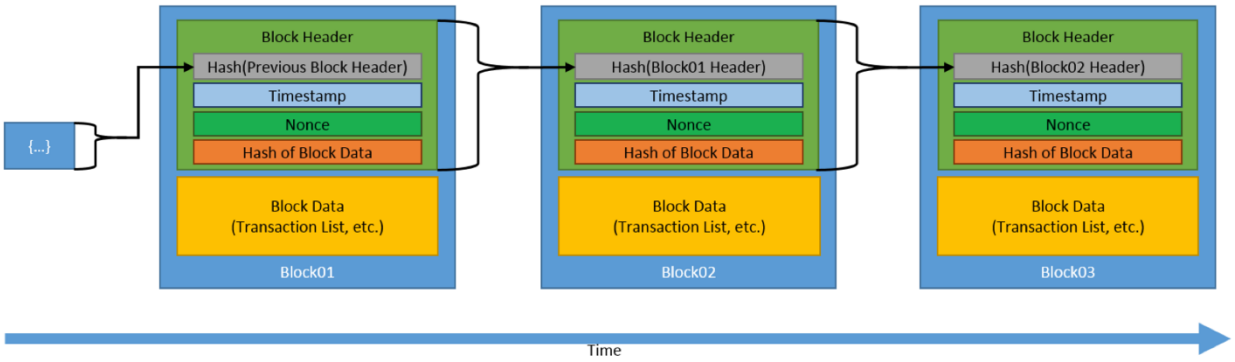

Figura 4: struttura del blocco e di una catena [9]

1.2.3 Crittografia e funzione di hash

Un sistema per essere sicuro deve garantire:

1. Privatezza dei dati; una terza entità non deve essere in grado di comprendere il significato delle informazioni salvate e/o inviate.
2. Integrità dei dati; l'eventuale alterazione dei dati da parte di una terza entità deve essere facilmente individuabile.
3. Identità dei partner; deve essere certa l'entità degli individui in gioco.
4. Non ripudiabilità dei dati; il mittente dei dati non deve poter negare di essere stato lui ad inviarli e il destinatario di averli ricevuti.

Le tecniche software utilizzate, che rispettano questi quattro punti, sono basate sulla *crittografia*.

La crittografia viene utilizzata per rendere incomprensibile un messaggio a tutti tranne che al destinatario a cui è indirizzato e al suo mittente, che ovviamente ne conosce il contenuto; il testo in chiaro, ovvero quello originale, viene trasformato in testo cifrato (o criptato). Le tecniche di crittografia si suddividono a seconda dell'algoritmo utilizzato:

- A chiave simmetrica (o segreta): questi algoritmi utilizzano la stessa chiave per cifrare e decifrare il messaggio. Questo meccanismo porta con sé diversi svantaggi e limitazioni quali l'obbligo di trasmettere la chiave tramite un canale sicuro e la proliferazione delle chiavi stesse, in quanto per motivi di sicurezza è necessario aggiornare la chiave segreta per ogni coppia di interlocutori.
- A chiave asimmetrica (o pubblica): questi algoritmi prevedono che ogni utente sia in possesso di una coppia di chiavi, ovvero una chiave segreta conosciuta solo dal proprietario e una pubblica trasmettibile anche in chiaro. Le chiavi sono in un rapporto di alter-ego, vale a dire che solo utilizzandole insieme è possibile il processo di codifica/decodifica di un messaggio. Per generare una coppia si parte dalla chiave

pubblica e tramite calcoli semplici da realizzare ma difficili da invertire, si arriva alla chiave privata. Lo svantaggio è la lentezza di questo processo, risultando circa 100 volte più lento di quello basato su chiave simmetrica.

La crittografia a chiave asimmetrica è quella maggiormente utilizzata nell'ambito blockchain e i suoi utilizzi si possono riassumere come segue:

- Le chiavi private sono impiegate per la firma digitale delle transazioni;
- Le chiavi pubbliche sono utilizzate per verificare le firme generate tramite chiavi private e per derivare gli indirizzi.

La tecnologia blockchain utilizza quindi meccanismi informatici quali funzioni di hash e firme digitali. L'hashing è una delle principali componenti e il suo funzionamento consiste nel trasformare un input (ad esempio un file o un testo) di dimensioni arbitraria, in un output con un numero di bit definito precedentemente, chiamato *digest* o *fingerprint*. Considerando m = testo in chiaro e h(m) = digest, le proprietà richieste alle funzioni di hash, che ne consolidano anche i pregi di utilizzo, sono:

1. Una funzione di hash non deve essere invertibile e deve essere resistente alle controimmagini;
   da h(m) non è possibile trovare m
   non è possibile trovare m≠m' tale che h(m)=h(m')
2. Una funzione di hash deve essere resistente alle collisioni;
   probabilità quasi nulla che a partire da m e m' (con m≠m') risulti h(m)=h(m')
3. Una funzione di hash deve essere resistente alla correlazione;
   una piccola variazione nel messaggio di partenza provoca evidenti differenze nel digest.
4. Lo stesso input è mappato sempre nello stesso output

Questo consente agli utenti di acquisire indipendentemente i dati in input e verificare tramite l'hashing se risulta lo stesso output; ogni minima modifica dell'input risulterebbe in un output completamente diverso. Così anche nella catena blockchain una minima modifica all'interno di un blocco provocherebbe un'evidente alterazione nei blocchi successivi, poiché ogni blocco contiene l'hash di quello precedente (Figura 5). Esistono diverse famiglie di funzioni di hash per la tecnologia blockchain (SHA-256, Keccak etc..) le quali vengono utilizzate al fine di creare identificatori univoci, proteggere i dati di blocco e proteggere l'intestazione del blocco. [9]

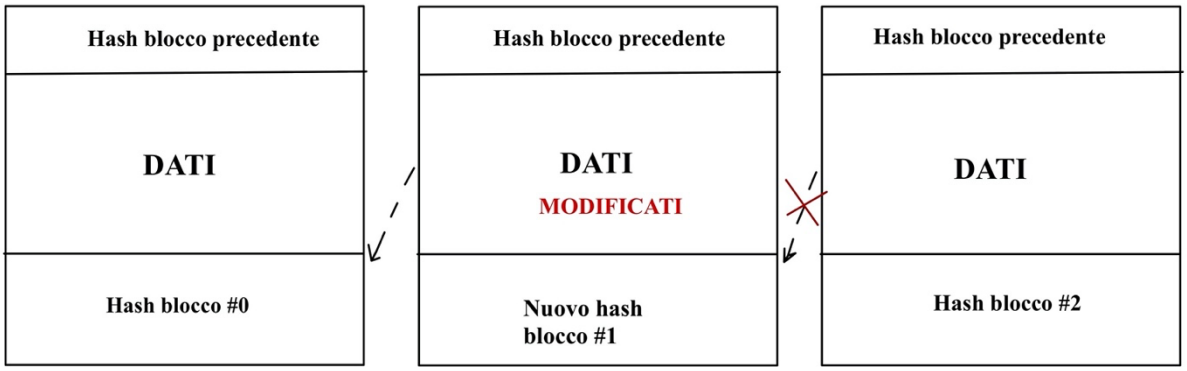

Figura 5: che cosa succede se un blocco viene modificato [5]

1.3 Principi generali di funzionamento delle tecnologie blockchain e i protocolli di consenso

Una transazione rappresenta un'interazione tra parti e può essere di vario tipo, come ad esempio una transazione monetaria, sanitaria o un certificato. I dati che la compongono sono diversi in base all'utilizzo, ma solitamente le informazioni inviate alla blockchain contengono la chiave pubblica e l'indirizzo del mittente, una firma digitale e l'input-output di transazione. [9] A prescindere dal fatto che vengano utilizzate per trasferire risorse digitali o dati è di fondamentale importanza validarle e verificarne l'autenticità.

Ogni transazione, prima di essere inserita all'interno di un blocco, deve essere confermata trovandosi dunque inizialmente solo in uno stato potenziale. Non appena la transazione entra a far parte di un blocco questa ha ottenuto 1 conferma, dopo aver creato il blocco successivo la stessa transazione ha 2 conferme e via dicendo (Figura 6). L'immutabilità viene acquisita dopo un certo numero di conferme (blocchi creati) che riceve e questa quantità dipende dal tipo di transazione considerata: in Bitcoin è consigliato attendere 6 conferme mentre in Ethereum almeno 12.

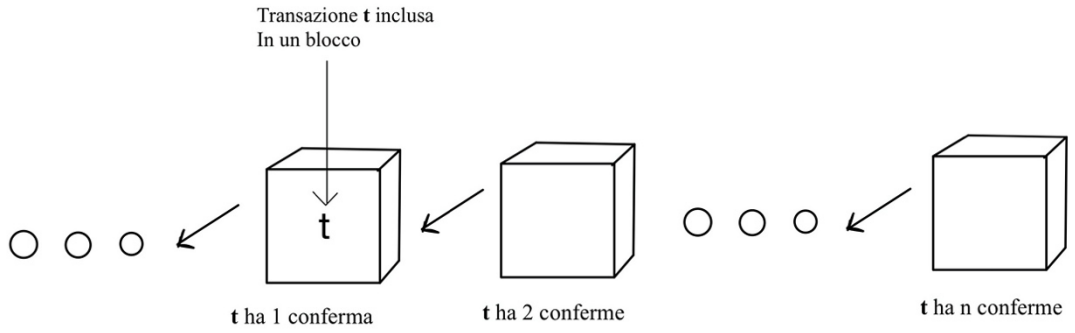

Figura 6: il numero di conferme di una transazione dipende dal numero di blocchi [8]

I modelli di consenso si pongono come garanti nel sistema blockchain per determinare quale utente possa pubblicare il blocco successivo, permettendo ai partecipanti di fidarsi senza dover contare su nessuna autorità centrale. I nodi che prendono parte al processo di accordo, chiamato *mining,* vengono denominati *miner*.
In un primo momento, in una catena blockchain viene concordato lo stato iniziale (come il blocco genesi) e, successivamente, gli utenti accettano il modello di consenso utilizzato. Ogni utente all'interno del sistema potrà poi essere in grado di verificarne l'integrità. Per poter aggiungere un nodo alla catena è necessario che tutti i nodi raggiungano un accordo univoco e distribuito; a questo scopo esistono diversi schemi di consenso ma i due più utilizzati nelle tecnologie blockchain sono il *Proof of Work* (PoW) e il *Proof of Stake* (PoS).

Protocollo Proof of Work: secondo questo modello tutti i nodi devono partecipare alla risoluzione di una sfida matematica molto difficile dal punto di vista computazionale, che consiste nel trovare un numero pseudocasuale (il *nonce*) al fine di ottenere il *digest* richiesto nella soluzione. Il primo nodo che risolve il puzzle matematico potrà pubblicare il blocco successivo, mentre tutti gli altri nodi possono verificarne la correttezza secondo un algoritmo più semplice. La sfida matematica è spesso rappresentata da una funzione di hash inversa ed è possibile arrivare al risultato finale solo tramite tentativi iterativi. La probabilità che un miner trovi la soluzione di un PoW è:

Probabilità = Hashrate del miner / hashrate del network

(Equazione 1 [8])

dove l'hashrate è definito come il numero di hash calcolati al secondo e dipende sia dalla potenza del miner sia dal tipo di hash applicato.
Dopo che la soluzione è stata verificata ed è stato raggiunto il consenso, tutti i nodi aggiornano il proprio stato della catena. Solitamente vengono previsti dei premi-ricompensa per i miner che riescono a risolvere il problema in esame, in modo da motivare i nodi a concorrere alla crescita della catena. Se da una parte si ha il vantaggio di rendere difficile la modifica della catena, dall'altra si hanno diversi svantaggi come:

- Il massiccio dispendio di energia richiesto;
- La lentezza di verifica;
- La vulnerabilità a certi tipi di attacchi.

Protocollo Proof of Stake: a differenza dello schema precedente i validatori (equivalenti dei miner nel PoW) vengono scelti a seconda del numero di token che possiedono, ovvero la quantità di commissioni acquisite definita come *stake*. Questo significa che la probabilità che

un utente della rete pubblichi un nuovo blocco dipende dal rapporto tra l'investimento fatto da un validatore e la quantità totale di transazioni all'interno della rete. Non sono previsti sforzi di calcolo complessi e questo rende l'algoritmo più veloce.
[8] [9]

	PoW	**PoS**
Chi crea il nuovo blocco	Miner, scelto casualmente in base alla potenza di calcolo	Validatore, scelto precedentemente in base allo stake
Cosa è necessario	Potenza di calcolo	Stake
Tempo per generare un blocco	Variabile (dipende dalla difficoltà dell'algoritmo)	Fissato
Equo	Si	Si
Potenza di calcolo richiesta	Elevata	Minima
Ricompensa	Commissioni e criptovalute generate insieme al blocco	Commissioni e criptovalute generate insieme al blocco

Tabella 2: i due modelli di consenso a confronto. [8]

Attraverso entrambi i modelli di consenso viene dunque modificato lo stato dell'intera catena. Questo cambiamento può portare a scenari diversi, chiamati *fork*. Le varie tipologie di *fork* sono illustrate in Figura 7.

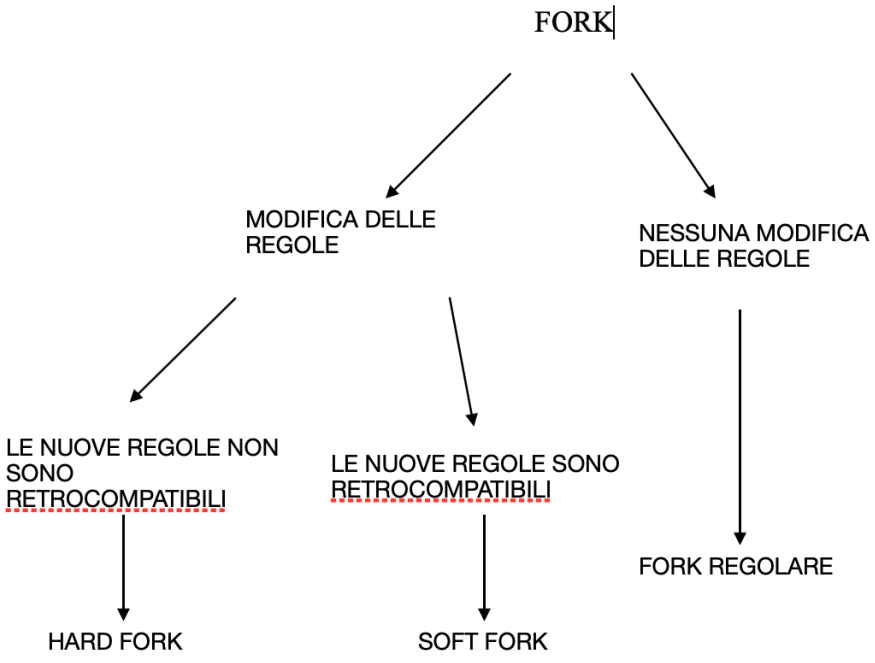

Figura 7: le diverse tipologie di fork [8]

Il processo per aggiungere un blocco alla catena si può dunque riassumere tramite la Figura 8.

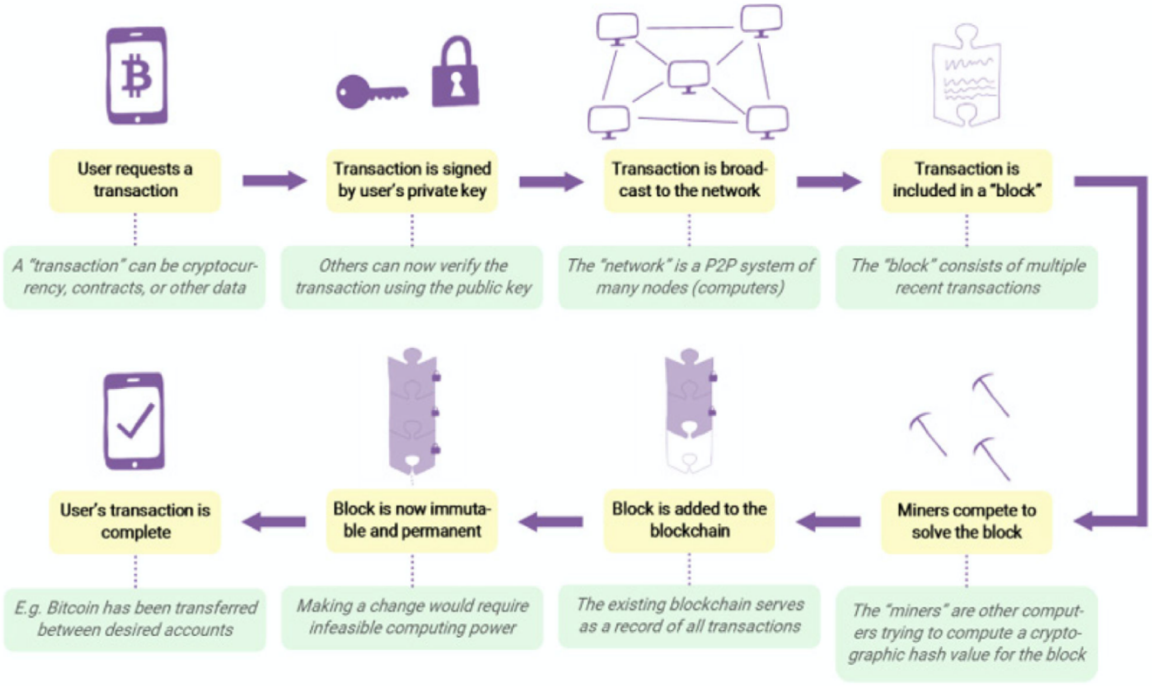

Figura 8: procedimento di aggiunta di un blocco alla catena [26]

1.4 Tipologie di blockchain

Ogni progetto può avere esigenze diverse e queste corrispondono a tipologie diverse di blockchain. In base alla gestione dell'autorità è possibile classificare la blockchain secondo tre modelli:

Pubblica	Privata	Ibrida
• Accessibile a tutti • Modello più utilizzato. • Open source: è possibile per tutti conoscere il codice alla base del funzionamento. • Esempio: criptovalute Bitcoin ed Ethereum. • Velocità ed efficienza basse. • Immutabile.	• Accesso solo ad utenti pre-autorizzati. • Parzialmente decentralizzate: esiste un controllo sugli accessi. • Il controllo è in mano ad una sola entità. • Utilizzate per applicazioni aziendali. • Alta velocità ed efficienza. • Parzialmente immutabile.	• Ha le caratteristiche della privata, ma il controllo è distribuito a tutti i partecipanti della rete. • Un buon compromesso per situazioni in cui è necessario un certo controllo su dati e sui partecipanti.

Tabella 3: confronto tra i tre diversi modelli blockchain.

1.5 Proprietà della blockchain

La blockchain è una nuova tecnologia e per questo prevede connotazioni d'avanguardia. Mettendo insieme le sue proprietà se ne possono apprezzare i vantaggi ed evidenziare alcuni dei suoi limiti:

- *Decentralizzazione*: le informazioni non sono memorizzate in un'unica posizione ma diffuse in tutto il network, tramite continui aggiornamenti dello stato della catena. Questo aspetto limita gli attacchi informatici e pone un nuovo concetto di fiducia.
- *Immutabilità:* tramite l'utilizzo della crittografia e dei protocolli di consenso, la minima modifica di un blocco comporterebbe evidenti variazioni in tutti quelli successivi. Per violare e manipolare una catena sarebbe necessario riuscire a modificare almeno il 51% dei blocchi archiviati, il che comporterebbe un grande costo computazionale.

- *Verifica delle transazioni:* questo processo è portato a termine da molti computer, riducendo il coinvolgimento umano e quindi gli eventuali errori che avrebbe portato con sé.
- *Trasparenza:* la blockchain è una tecnologia *open-source*, ovvero accessibile e consultabile da tutti, garantendo sia affidabilità sia trasparenza. La trasparenza rende disponibile la "storia" di una transazione a tutti gli utenti e preserva i dati da eventuali rischi.
- *Tracciabilità*: l'inserimento dei vari blocchi avviene con ordine e per questo è possibile tracciare una transazione facilmente esaminandone le informazioni. [8] [10]

2. PERCHE' SI PARLA DI BLOCKCHAIN NELLA GESTIONE BIOMEDICALE

2.1 La necessità di una nuova gestione di dati in ambito biomedicale

Attualmente i dati in ambito biomedicale sono gestiti principalmente da una applicazione centralizzata chiamata DDBMS che a sua volta gestisce un insieme di database distribuiti all'interno di una rete. Il DDBMS permette di aggiornare e sincronizzare la rete per ogni modifica fatta dagli utenti e sviluppa una gestione sicura per proteggere la riservatezza e l'integrità di grandi volumi di dati. Nella gestione biomedicale si ha a che fare però con un altissimo numero di dati prodotti ogni giorno, ognuno di questi di dimensioni considerevoli. La banca di dati DDBMS diventa inadeguata e presenta dei problemi nel suo utilizzo quando ha a che fare con queste specifiche, risultando lenta e macchinosa nel reperire dati, classificarli e renderli disponibili in tempi brevi a seconda della necessità. All'interno di questa banca dati è possibile modificare ciò che contenuto al suo interno e, quando ci si rapporta con informazioni sanitarie, questo aspetto deve essere limitato. I dati sanitari devono risultare integri e leggibili, evitando conseguenze legali o errori medici a causa di modifiche apportate in un secondo momento da utenti malintenzionati che sono riusciti ad eludere i sistemi di sicurezza. Gli aspetti chiave che deve assicurare una tecnologia in ambito biomedico, compreso quello dell'imaging biomedicale, sono racchiusi in sette punti:

- Mettere il paziente al centro di ogni processo;
- Raccogliere i dati in modo uniforme;
- Raccogliere una grande quantità di dati ingombranti;
- Abbattere i costi di tempo e denaro;
- Rendere la tecnologia scalabile;
- Accedere ai dati in sicurezza;
- Proteggere la privacy dei dati. [11]

La tecnologia blockchain è stata progettata per supportare le criptovalute, per questo motivo è considerata un registro di contabilità distribuita. Le sue proprietà principali, quali la decentralizzazione, la trasparenza e l'immutabilità hanno catturato l'interesse anche di operatori sanitari e biomedici in diversi settori di applicazione, monitorandone le potenzialità, i benefici e i possibili limiti di utilizzo.

Le nuove richieste di progettazione derivano dallo studio sui problemi appena accennati dell'attuale gestione biomedicale dei dati, individuando dunque la necessità di sovvertire tale sistema. L'interesse nello sviluppare e potenziare il controllo di queste informazioni proviene dalla loro importanza come risorsa per il monitoraggio della nostra salute, di eventuali terapie o per la prevenzione di possibili malattie. Non sono ancora molti i progetti blockchain in atto in tale ambito, e si prevede che questa sarà un'implementazione graduale in quanto, con il

tempo, se ne stanno valutando i costi di sforzo-beneficio in modo da trarne il maggior numero di miglioramenti possibili, evitando di scontrarsi sia con perdite economiche sia con possibili errori.

Rispetto al DDBMS, la tecnologia blockchain presenta una serie di caratteristiche che la rendono una soluzione favorevole in ambito biomedico.

A differenza di tale database, la blockchain si presenta come un registro decentralizzato, facilitando l'eventuale collaborazione tra le varie parti in gioco.

Inoltre, la blockchain assicura agli utenti che i dati inseriti rimangano immutati e integri, diversamente dal DDBMS in cui le informazioni e la loro provenienza possono essere alterate. L'origine e l'immutabilità dei dati è un aspetto importante trattandosi di dati medici.

La blockchain assicura un maggior livello di privacy e garantisce alti livelli di ridondanza di tutti i dati della catena, archiviandone una copia in ogni blocco.

La blockchain è proposta dunque come un database alternativo per informazioni biomediche, in particolare per la loro analisi, condivisione, convalida e registrazione. [12] Altre possibili applicazioni della blockchain in ambito biomedico includono :

- gli electronic medical records (EMR);
- dispositivi indossabili o impiantati (come protesi) ;
- ricerca clinica;
- catene di approvigionamento medico;
- richieste di risarcimento assicurativo.

2.2 L'attuale gestione biomedicale e i suoi limiti

L'era digitale e dei big data che stiamo vivendo ha radicalmente modificato le modalità e le esigenze di gestione, manipolazione e analisi dei dati. Secondo l'analisi svolta dall'IDC (International Data Corporation) nel 2020 è stata creata una quantità di dati pari a 64,2 Zettabytes, nel 2021 circa 79 Zb e nel 2025 è in prevista una quota di 180 Zb. [25] Tutti questi dati digitali devono essere trasmessi e processati in tempi brevi, quasi istantanei.

Nel mondo sanitario i pazienti hanno coltivato sempre maggior aspettativa di reperire informazioni in modo immediato, prospettiva che però non viene rispettata dagli attuali sistemi di archiviazione, in quanto molto lenti. I tempi per reperire questi dati è dilatato ulteriormente dal fatto che i pazienti sono utenti passivi, ovvero non coinvolti nel corso della gestione, non avendo nessuna funzione e non potendo prendere alcuna decisione in merito. La condivisione incentrata sul paziente diventa di rilevante importanza dal momento che la ricerca biomedica si sta sempre più indirizzando verso quella che viene chiamata medicina personalizzata. In vista di questo spostamento di rotta, è essenziale dare maggior peso al

coinvolgimento degli utenti, nonché pazienti, rendendoli ad esempio partecipi nelle decisioni sul processo di cura da intraprendere o su quali dati condividere con tecnici o medici.
Un'ulteriore problematica riscontrata è la frammentarietà dei servizi sanitari, che ostacola ed impedisce una giusta comunicazione tra le parti in gioco a discapito del processo di cura. Questa limitazione ha come conseguenza un ulteriore disagio per il paziente: quest'ultimo è infatti costretto a mobilitarsi con i suoi dati sanitari, fungendo da "vettore" di comunicazione tra un'azienda ospedaliera e l'altra. Pensiamo, ad esempio, ad un paziente a cui sono prescritti degli esami più specifici in strutture diverse, per indagare su un suo problema di salute. Se i risultati di un esame non vengono condivisi tra le varie strutture operanti, ma rimangono all'interno dell'istituto che li ha prescritti e/o svolti, gli enti e i professionisti che seguono il paziente non potranno mai avere una visione totale e completa sulla sua storia clinica. Questo può portare ad eventuali errori diagnostici, dilatazione dei tempi necessari e costi aggiuntivi. In America al Johns Hopkins Hospital hanno infatti dimostrato che "le decisioni mediche errate, provenienti da problemi sistemici e di coordinazione delle cure, sono al terzo posto tra le cause di morte." [11]

Un database biomedico può essere vulnerabile anche in termini di privacy, sicurezza e integrità delle informazioni contenute. I dati medici sono considerati "dati sensibili" e sono spesso nel mirino di attacchi informatici; qualora vengano alterati o corrotti, risulterebbe un problema sia di valenza medica sia di valenza legale oltre che compromettere la fiducia dei pazienti. La privacy è già regolamentata da alcuni provvedimenti, come il GDPR (General data protection regulation), ma questi riguardano maggiormente la provenienza di dove vengono originati i dati o chi li ha creati, piuttosto che offrire ai pazienti delle garanzie sul loro controllo.
Non è da sottovalutare infine il continuo rialzo del costo della sanità, messa a dura prova da una popolazione sempre più anziana che necessita di maggiore assistenza e cure sanitarie. Questa maggiore domanda viene affrontata anche con la medicina digitale, un nuovo modo di prestare soccorso e ausilio da remoto: da visite di telecardiologia alla telepsichiatra e teledermatologia.
Il monitoraggio continuo permette una diagnosi più veloce ed efficace migliorandone la qualità, abbattendo costi e risparmiando il tempo sia del medico che del paziente.
L'aspetto limitante della telemedicina è che i suoi sistemi non prevedono l'integrazione tra i dati dell'applicazione Telehealth e i sistemi utilizzati dalle organizzazioni sanitarie "fisiche". [11] [12] [13]

Considerando i problemi sopra elencati, è quindi interessante approfondire quale possa essere il ruolo della blockchain in ambito biomedico e quali opportunità tale soluzione tecnologica possa avere, in particolare nel mondo dell'imaging biomedicale.

3. BLOCKCHAIN PER L'IMAGING BIOMEDICALE

Le immagini biomediche sono quelle immagini che raffigurano l'anatomia o la fisiologia di alcune parti interne del corpo umano. Con il termine *imaging biomedicale* si indicano tutte le procedure di elaborazione delle bioimmagini ottenute tramite tecniche specifiche (tecniche radiologiche, tomografiche ed ecografiche), che consentono successivamente un controllo clinico effettuato da esperti; l'imaging acquista così un ruolo indispensabile all'interno della sanità e del processo di cura dei pazienti, in quanto la maggior parte delle malattie o di possibili traumi subiti non sono visibili ad occhio nudo. Il ruolo dell'imaging biomedicale non è solo diagnostico, ma ha diverse applicazioni:

- Programmazione del trattamento;
- Monitoraggio e controllo di una malattia;
- Valutazione dell'utilità di una terapia. [13]

Visti i molteplici utilizzi è di fondamentale importanza che i dati e gli studi di imaging vengano condivisi in modo corretto rendendoli affidabili, proteggendoli da minacce esterne e mantenendoli integri. Un insufficiente controllo di questi dati potrebbe infatti comportare diversi incidenti e rischi come la violazione della privacy degli utenti o la perdita delle stesse informazioni in essi contenute. L'inadeguatezza delle tecniche utilizzate attualmente per la condivisione e la gestione di immagini mediche è il risultato delle limitazioni che sono state presentate nella discussione sul controllo dei dati biomedici. Prime tra queste ci sono la centralità dei sistemi di controllo, lo scarso coinvolgimento dei pazienti, la frammentarietà dei servizi e i diversi formati di archiviazione. [15] [16]

3.1 Applicazioni e vantaggi dell'uso della blockchain nell'imaging biomedicale

I dati di imaging sono una risorsa preziosa per la sanità, per questo ogni giorno ne vengono raccolti e salvati in enorme quantità. Lo stato dell'arte attuale per la condivisione e gestione elettronica di immagini biomediche risulta insufficiente. Questa inefficacia deriva, prima di tutto, dai problemi riscontrati con tutti i dati medici, quali la mancanza di centralità del paziente, la mancanza di integrazione tra dati provenienti da strutture diverse e la vulnerabilità da attacchi esterni. Nel dominio di imaging si aggiunge la necessità di sviluppare dei software che includano diverse modalità di imaging e che rispettino i progressi riguardanti i dispositivi utilizzati per la creazione di immagini. Per il salvataggio delle immagini mediche è utilizzato lo standard DICOM (Digital Imaging and Comunication in Medicine) che garantisce una buona qualità delle immagini, la loro acquisizione, condivisione e recupero. Per le immagini DICOM acquisite digitalmente è utilizzato un database per l'archiviazione digitale chiamato

PACS. Esistono però molteplici software per la visualizzazione delle immagini e gli sviluppatori stanno cercando di progettarne versioni sempre più aggiornate e complete.
Il numero di immagini prodotte è sempre maggiore sia per i progressi fatti nel settore sia per la maggior richiesta da parte dei pazienti. Per i database utilizzati si aggiunge la sfida di gestire le immagini mediche che, tra gli altri dati sanitari, si distinguono per il loro grande volume. Questi database non assicurano una giusta organizzazione delle immagini digitali, non consentono a medici e a pazienti di visualizzare i dati contemporaneamente salvati in sistemi diversi e non ammettono un'integrazione ottimale e sicura tra i dati.
Per questo motivo entra in gioco una nuova soluzione, la blockchain, che porta in questo settore innumerevoli novità d'uso e vantaggi.
Nell'imaging biomedico i casi di utilizzo della tecnologia blockchain comprendono, ad esempio, la condivisione e protezione dei dati, la teleradiologia, l'intelligenza artificiale e la ricerca. L'interesse nello studio di questo ambito è giustificato da una recente analisi di startup relative all'imaging, in particolare alla radiologia, che afferma: "la tecnologia blockchain è stata identificata come il cluster in più rapida crescita." [14] Uno studio sui diversi aspetti che limitano la gestione attuale, chiarirà in che modo la blockchain risulti vantaggiosa e utile come integrazione dei sistemi correnti.

3.1.1 Lo spostamento da sistema centralizzato a decentralizzato

Uno dei più significativi cambiamenti, adottando la tecnologia blockchain, è la maggiore importanza data ai protagonisti del sistema di gestione di immagini mediche, quali i centri di imaging, i pazienti, gli operatori sanitari e biomedici. Infatti, lo svantaggio di sistemi centralizzati, largamente ancora utilizzati, è quello di avere un solo punto di errore; se viene compromesso, l'intero sistema si blocca e i dati della rete sono ad alto rischio di corruzione. La blockchain, al contrario, mette al sicuro i dati di imaging contenuti nella catena in quanto la rete ha più possibilità di rimanere funzionante. La decentralizzazione permette inoltre di dare la possibilità ai pazienti di prendere decisioni sulle loro informazioni e di condividerle con dei medici di loro scelta per eventuali consulenze, evitando di dare questo compito ad entità e parti terze; tutte le parti in gioco non hanno la necessità di rivolgersi a nessuna autorità centrale, ma hanno la possibilità, seppur separate tra loro, di tracciare un unico insieme di dati salvati nella catena blockchain. Un maggior potere implica anche una maggior responsabilizzazione degli utenti coinvolti. [15]

3.1.2. La dimensione e l'archiviazione delle immagini

Sebbene esistano già alternative digitali, come RSNA Image Share Network, le immagini mediche sono principalmente salvate e trascritte su compact disc o su DVD, lasciando la responsabilità del trasferimento e del costo di creazione di questi dischi ai pazienti stessi. Negli USA, nel 2014, il 15% delle persone interrogate hanno affermato di fare da vettore vivente per lo spostamento di un risultato radiologico e il 5% ha dovuto anche ripetere il test perché i dati di quello precedente non risultavano reperibili. [16] Il paziente si assume quindi una ulteriore e indebita responsabilità qualora le immagini venissero perse e/o danneggiate. Tramite la blockchain sarebbero evitate queste problematiche, facendo affidamento su questo database distribuito per assicurare tutte le esigenze di sicurezza necessarie.

Trattandosi di grandi quantità di informazioni aventi una dimensione di archiviazione consistente è impensabile, almeno nello stato attuale della tecnologia, salvare le immagini vere e proprie all'interno dei blocchi della catena. Risulta molto più pratico archiviare un riferimento alle immagini, ovvero un collegamento generato e rappresentato tramite le funzioni di hash su cui si basa la tecnologia blockchain; la soluzione appena presentata renderebbe possibile ovviare anche ai problemi riguardanti la bassa velocità e l'altissimo costo di salvataggio di una quantità di dati ingombrante. L'utilizzo di collegamenti ed hash crittografici si traduce nell'archiviazione dei riferimenti alle immagini "on-blockchain" e delle immagini vere e proprie "off-blockchain", utilizzando delle piattaforme di database per l'imaging già esistenti.

Tramite questa struttura, la condivisione e archiviazione tra sistemi sanitari risulta più fluida, immediata e semplice e può avvenire secondo una blockchain pubblica o una blockchain privata.

- Condivisione tramite blockchain pubblica: vengono aggiunte e visionate le immagini mediche di un individuo da qualsiasi ente pubblico o privato sanitario, senza particolari autorizzazioni.
- Condivisione tramite blockchain privata: i sistemi ospedalieri devono ottenere una autorizzazione speciale da parte del paziente per visualizzare le immagini. Il paziente crea quindi una lista modificabile di coloro a cui decide di rilasciare un permesso.

In entrambi i casi è evidente il vantaggio di sollevare il paziente dal coinvolgimento diretto nella creazione e nel trasporto dei CD contenenti le immagini mediche.

Un esempio molto rilevante è il sistema di condivisione proposto da Patel che utilizza lo schema di implementazione Ethereum. Il trasferimento di immagini avviene tramite tre transazioni a chiave pubblica e privata che definiscono:

1) La fonte dell'immagine;

2) I proprietari dell'immagine;
3) I consensi per accedervi.

In particolare, un insieme di chiavi pubbliche e private sono utilizzate per pubblicare l'immagine all'interno della catena, mentre la chiave privata detenuta dal paziente serve per accedere alle informazioni archiviate. Nello specifico, all'interno della blockchain sono memorizzati gli URL delle immagini contenute invece in DICOMWeb (database di archiviazione). La blockchain assume infine il ruolo di un vero e proprio registro di permessi, verificando che un utente richiedente sia compreso nell'elenco di autorizzazioni ad un particolare studio di imaging. In questo modo possono essere controllati gli accessi, con la garanzia aggiunta che i dati originali non possono essere modificati in forza dell'immutabilità come proprietà chiave nella gestione tramite blockchain. Le informazioni e la loro fonte risultano per questo più facilemente verificabili, riducendo il tempo e il processo di ricerche manuali ed estenuanti. [15] [16]

Il processo di gestione dei controlli sia degli accessi sia dei permessi è basato sulla crittografia. È possibile presentare gli step principali prendendo d'esempio l'utilizzo della chiave simmetrica per la crittografia della cartella clinica, in cui si trovano salvati anche i dati di imaging. Per prima cosa la cartella clinica è crittografata tramite una chiave, anch'essa successivamente crittografata con la chiave pubblica, appartenente ad una coppia di chiavi a 2048 bit.

Nel momento in cui un'entità medica ottiene il permesso del paziente di accedere alla sua cartella clinica:

1) Il record è decifrato tramite chiave privata del proprietario della cartella;
2) La chiave simmetrica è ulteriormente crittografata tramite chiave pubblica dell'utente richiedente, autorizzato dal proprietario della cartella.

Figura 9: autorizzazione di accesso

Quando invece il paziente-proprietario rimuove il permesso ad uno dei partecipanti, la procedura è la seguente:

1) La chiave simmetrica viene decifrata con la chiave privata del proprietario del record;
2) Il record viene decifrato tramite la chiave simmetrica del precedente punto;
3) Il record viene nuovamente crittografato utilizzando una nuova chiave simmetrica;
4) La nuova chiave simmetrica viene crittografata con le chiavi pubbliche degli utenti ancora autorizzanti, rimanenti quindi nella "lista" di permessi. [12]

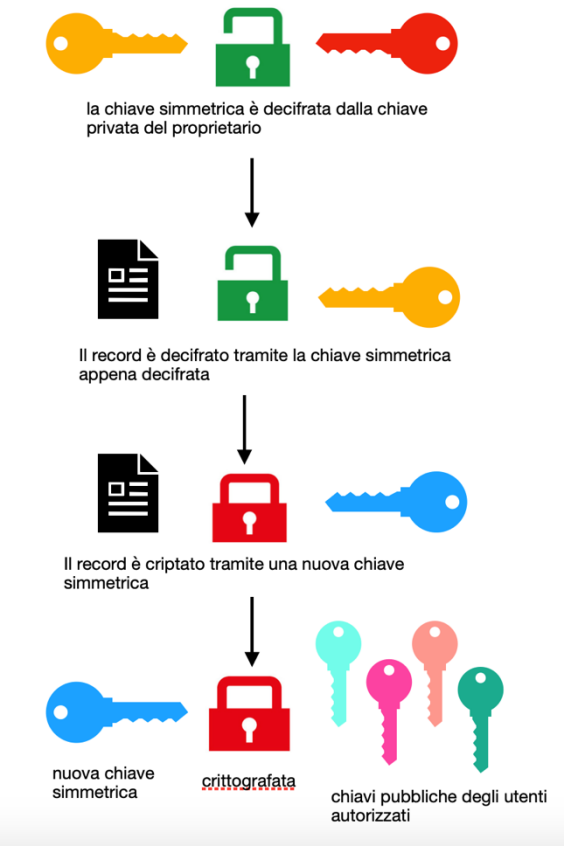

Figura 10: revoca di accesso ad un utente

Oltre al progetto proposto da Patel ne esistono diversi altri, importanti da citare, soprattutto per loro applicazione di blockchain nella gestione di big data riguardanti la salute, comprese le immagini mediche:

- Il progetto proposto dal Massachusetts Institute of Technology Media Lab e dal Beth Israel Deaconess Medical Center riguardante l'archiviazione delle cartelle cliniche elettroniche in un database locale e registrare la loro posizione di archiviazione all'interno di una blockchain consentendone accesso e autenticazione sicura.
- Un progetto che prevede la realizzazione di un'applicazione per smartphone, rivolta ai pazienti, per la gestione delle condivisioni e delle consultazioni dei loro dati sanitari, compresi i dati di imaging, tramite piattaforma blockchain.

- Altri diversi progetti che trattano l'utilizzo delle tecnologie blockchain per dati inerenti a studi clinici, assistenza sanitaria, fatturazione, approvvigionamento di farmaci ma anche di dati riguardanti pazienti diabetici e oncologici e immagini dermatologiche. [18]

3.1.3 Sicurezza e privacy

Come è emerso precedentemente, l'attuale amministrazione delle immagini è rappresentato, tra gli altri progetti, anche dall'Image Share Network (ISN) proposto dalla Radiological Society of North America (RSNA). Sebbene l'ISN abbia eliminato il bisogno del trasferimento fisico dei dati, sono emerse ulteriori preoccupazioni in particolare riguardo la centralità dell'infrastruttura e la sua vulnerabilità rispetto alla compromissione di immagini. La blockchain si assume il ruolo di garante dei diritti digitali; l'utilizzo dei dati all'interno della catena è sottoposto al controllo di un contratto intelligente e il paziente proprietario dei contenuti è automaticamente riconosciuto. Vista la natura dinamica dei dati biomedici, è essenziale assicurare la loro integrità e l'eventuale corretto recupero dei dati salvati, facilitato così dalla struttura ridondante a blocchi.
In aggiunta, l'inaffidabilità dei sistemi attuali inibisce l'interoperabilità e la condivisione sicura in vista di una collaborazione. La blockchain, al contrario, sarebbe in grado di costruire un ecosistema decentralizzato che garantisce lo scambio di dati, di cui è mantenuta una traccia sia dell'origine sia della manipolazione. [17] [19]

3.2 Blockchain e radiologia

La radiologia è uno dei rami della medicina che si occupa dell'imaging biomedicale; in particolare utilizza la tecnica di trasmissione di raggi X. La metodologia di acquisizione appena nominata prevede l'irradiamento della parte del corpo che si vuole analizzare, generando un'immagine in cui si distinguono i differenti tessuti. Quest'ultimi possiedono una diversa capacità di assorbimento dei raggi X, creando contrasto all'interno dell'immagine.
L'imaging radiografico risulta un supporto fondamentale per la diagnosi grazie alla capacità di individuare diverse strutture del corpo: dalle fratture o lesioni ossee ad alterazioni infiammatorie. I medici devono analizzare un ampio spettro di immagini per estrapolare le diverse e molteplici informazioni che contengono, in quanto hanno dimensioni considerevoli. [20]
La radiologia è una tecnologia sanitaria che richiede competenze multi-disciplinari, fisiche, ingegneristiche e cliniche e si inserisce nel contesto dei big data. Infatti, l'imaging radiologico

produce grandi quantità di dati, che a loro volta hanno dimensioni considerevoli dal punto di vista della memoria necessaria per la loro archiviazione. Questo aspetto risulta limitante per i database di attuale utilizzo, perché non possiedono ancora le caratteristiche utili per l'archiviazione di molteplici dati pesanti.

Il rapporto dell'Health Technology Assessment (H.T.A) [21] ha evidenziato le esigenze e le sfide del dominio radiologico, individuando gli elementi di criticità da sottoporre a miglioramento dell'insieme di tecnologie hardware e software, chiamate PACS, utilizzate per la gestione digitale di immagini diagnostiche. Tra queste necessità troviamo:

- aumento delle performance quantitative e qualitative dei servizi radiologici;
- impegno di un costante controllo delle procedure diagnostiche di maggiore complessità da parte degli specialisti in radiologia, in modo da garantire uniformità nelle procedure e protocolli;
- refertazione e trasmissione di esami radiologici urgenti 24 ore su 24;
- aumento dell'efficacia della teleradiologia;
- riduzione dell'utilizzo di supporti tradizionale (CD) con sostituzione di altri formati, adattandosi a questi cambi di format frequenti;
- potenziamento della formazione radiologica a distanza. [21]

Per far fronte al maggior numero possibile di queste esigenze, la blockchain è proposta come soluzione di tecnologia alternativa per il controllo delle immagini radiologiche. In futuro è dunque necessario che i radiologici si rendano conto del potenziale di questa nuova soluzione tecnologica per la gestione dei dati.

I vantaggi sono constatabili sia a livello di gestione delle attività cliniche sia a livello di ricerca radiologica. Tra questi troviamo:

- l'inserimento e l'utilizzo di numerosi dati di diversi pazienti;
- la possibilità di svolgere un'analisi quantitativa dell'immagine ottenuta;
- la possibilità di verificare i collaboratori all'interno di uno studio di imaging radiologico;
- la garanzia di utilizzare una rete informatica sicura;
- la possibilità di utilizzo della blockchain nella radiomica e nell'intelligenza artificiale.

3.2.1 Applicazione della blockchain nella ricerca radiologica

Molti aspetti all'interno della ricerca in radiologia possono essere gestiti in modo ottimale utilizzando la tecnologia blockchain.

Innanzitutto, con l'utilizzo della blockchain, i dati biomedici, quali le immagini radiologiche, possono essere archiviate in modo sicuro rispettando parametri ed esigenze di privacy ed immutabilità. La decisione su quali dati inserire ed archiviare nei blocchi è a discrezione del solo proprietario; quest'ultimo può decidere di condividere esclusivamente i dati necessari ed inerenti alla ricerca in corso a cui sta partecipando, escludendo possibili dati sensibili.

Tutto il processo di ricerca e di creazione del database come banca di dati non ha esigenza di fiducia grazie alla gestione decentralizzata, risultando un approccio nuovo, più aperto e trasparente.

Assicurando un alto livello di sicurezza e di affidabilità, i pazienti in possesso di dati utili di imaging sono più propensi a partecipare al loro caricamento e condivisione. Raccogliere e mettere insieme dati è un aspetto chiave perché più la quantità di dati disponibili è maggiore più la ricerca risulta completa, in particolare in sperimentazioni più complesse o poco comuni. La sicurezza di questo sistema favorisce inoltre maggiore collaborazione tra le squadre di ricerca, riducendo l'atteggiamento di sola competizione che porta ad una perdita sia di tempo che di denaro perché vede più enti investire forze su uno stesso aspetto. L'approccio differente risulta vantaggioso per la ricerca, che procede più velocemente e aumenta l'efficacia di diagnosi, trasmissione e performances radiologiche.

Un esempio di tale tendenza è rappresentato dalla soluzione, basata su blockchain, proposta dalla Canada's University Health Network [22]; la piattaforma UHN 2018 registra il consenso del paziente alla condivisione dei dati e successivamente trasmette ai ricercatori tutti i dettagli della transazione. Se il sistema fosse interconnesso a livello molto esteso, per assurdo globale, ogni paziente potrebbe possedere il suo "io virtuale" tramite account unico e condivisibile.

Gli studi nel dominio della radiologia hanno da sempre riscontrato problemi nel creare database che potessero ospitare immagini e dati di grandi dimensioni, in particolar modo dal momento in cui è iniziata la crescita dell'utilizzo della radiomica e dell'intelligenza artificiale (IA).

In tali applicazioni risulta significativo assicurare la ripetibilità dei metodi di ricerca. Questa facoltà per ora risulta poco possibile a causa della lentezza del funzionamento degli algoritmi controllati dall'IA. Le tecnologie blockchain riuscirebbero invece a tracciare l'intero flusso di lavoro fatto per generare gli algoritmi utilizzati nelle due discipline, assicurandone inoltre

l'immutabilità. Questo risolverebbe altresì la difficoltà, riscontrata dai radiologici, di individuare la provenienza dei dati e i risultati finali ottenuti dall'analisi delle immagini.
Le informazioni salvate nelle banche di dati sarebbero protette tramite crittografia, che assicura privacy, immutabilità risultando una specie di "cybersecurity radiologica". Verrebbero tracciate le attività dei lettori, o chiunque acceda ai vari studi, e disincentivate cattive condotte da parte di chi è coinvolto nella ricerca. I dati protetti sarebbero poi resi disponibili dalla blockchain per algoritmi di apprendimento automatico.
Il problema della sicurezza è un aspetto molto importante nella radiologia e nell'imaging biomedicale, in quanto una manomissione delle immagini potrebbe inevitabilmente alterare la loro affidabilità clinica. Grazie all'uso della blockchain, ogni minima alterazione dei dati viene immediatamente notificata.
Nel 2018, all'incontro annuale della Society for Imaging Informatics in Medicine, è stato premiato il progetto "Diagnosis Protocol-Using Blockchain to Accelerate Artificial Intelligence in Medical Imaging" [15], che ammette il caricamento di immagini biomediche in modo anonimo, da parte di pazienti, istituti e responsabili sanitari e incoraggia tale condivisione con dei "premi-ricompensa" sotto forma di token. Affidabilità e ricompense sono due parole chiave se si vuole maggior partecipazione nella condivisione dei propri dati sensibili e sanitari.

Infine, è sempre più nell'interesse comune (sia dei medici sia dei pazienti) utilizzare nuovi metodi per la diagnostica, come ad esempio la telemedicina. La teleradiologia è una delle sue applicazioni ed è adatta per essere integrata con un database distribuito e decentralizzato. Un esempio di questa messa in pratica è l'azienda MDW (Medical Diagnostic Web) che adopera tali tecnologie per condividere risultati e analisi di immagine mediche, in particolar modo per il successivo utilizzo negli algoritmi di IA. [15]
Si possono riassumere in quattro punti gli aspetti chiave dell'utilizzo della blockchain nella ricerca in ambito radiologico:

1) ogni documento è autenticato dalla blockchain;
2) gli studi che non ottengono consenso vengono soppressi;
3) il processo di collaborazione è incentivato;
4) è garantito l'anonimato dei dati caricati, proteggendo la privacy di ogni individuo. [23][24]

3.2.2 Applicazione della blockchain in ambito clinico

I vantaggi e gli utilizzi dei principi su cui si fonda la blockchain sono ampiamente utilizzati in diverse attività cliniche.

Le immagini radiologiche contenute all'interno della cartella clinica sono sottoposte a limitazioni per quanto riguarda la loro creazione e il loro trasporto, oltre che soggette a possibili danni e perdite. Decentralizzando la gestione dei dati di imaging radiologico, è possibile creare, tramite blockchain, una catena di *endpoint* per recuperare le informazioni originarie, senza l'aiuto del database centralizzato dell'ospedale.

In ogni blocco sono salvati gli indirizzi delle immagini mediche ed è possibile tenere traccia di ogni azione riguardante il loro utilizzo tramite un elenco di utenti che hanno visionato il contenuto del blocco; in questo caso la blockchain terrebbe conto di chi ha contribuito alle varie parti della EMR (cartella clinica) e in che modo. Un radiologo ne troverebbe vantaggio nel caso in cui avesse la necessità di consultare determinate sezioni della cartella clinica di uno o più pazienti perché le informazioni sarebbero già suddivise e la ricerca risulterebbe più veloce ed immediata. Il radiologo potrebbe inoltre fornire dei suggerimenti di follow-up; anche queste informazioni verrebbero archiviate e riconosciute dalla blockchain in vista di un miglioramento della qualità dell'assistenza sanitaria del paziente.

I referti radiologici hanno solitamente bisogno di più di una consulenza riguardante gli esami svolti, soprattutto quando questi sono pertinenti ad aree specifiche come quella muscolo-scheletrica, neuro-muscolare e mammaria, quando si tratta di casi insoliti, quando si combinano diverse specialità (referto svolto da radiologo e cardiologo) o diverse modalità di imaging. Se queste consulenze derivano da diversi specialisti, mettendo insieme ad esempio competenze nucleari e radiologiche e di screening mammario, i referti non vengono prodotti in maniera sincrona.

La blockchain consente di ottenere una sola relazione che raggruppa ordinatamente i vari aspetti e pareri, facilitando la consultazione diretta a chi è interessato a determinate e specifiche informazioni. È così possibile memorizzare e mantenere immutabile ogni input inserito dai diversi professionisti coinvolti nella consulenza. Oltre a riconoscere e certificare il contributo di ognuno, viene fornito un diverso livello di responsabilità ai vari contributori.

In un mondo in cui il progresso scientifico si sta indirizzando verso l'utilizzo e l'implementazione dell'intelligenza artificiale e verso resoconti in modalità ibrida, è importante differenziare gli input che provengono da uno specialista radiologo e quelli provenienti da strumenti di IA, al fine di evitare il più possibile problematiche medico-legali e legate all'etica.

Sempre per quanto riguarda problematiche medico-legali, sono da tenere conto inoltre tutti quegli errori fatti sui dati anagrafici di un paziente, collegati ai referti radiologici. Se questi sbagli fossero corretti successivamente alla firma del rapporto finale, potrebbero nascere equivoci inerenti alla sua validità. Servendosi della blockchain è invece possibile creare un registro di tutti i cambiamenti e le modifiche apportate ai dati del referto dopo che è stato firmato digitalmente, ed evitare qualsiasi implicazione e ripercussione legale. In questo modo le cartelle e i dati di imaging in esse inserite sarebbero al sicuro tramite crittografia. [23] [24]

3.3 Limiti e rischi nell'utilizzo della blockchain

L'adozione delle tecnologie blockchain presenta diversi e numerosi vantaggi nella gestione dei dati di imaging, guidando il sistema sanitario verso l'innovazione. Nonostante ciò, mostra alcune limitazioni e svantaggi d'uso. Essendo una struttura agli arbori è sottoposta a continui studi e miglioramenti, come nelle applicazioni radiologiche che mostrano ancora pochi casi studio.

Tra le difficoltà maggiori troviamo quelle che riguardano:

- La privacy e la riservatezza: sono tra gli aspetti che preoccupano di più parlando di informazioni sulla salute. Le identità dei pazienti, a cui si riferiscono i dati sanitari, vengono infatti nascoste tramite crittografia e quindi tramite le chiavi. L'obiettivo sta nell'impedire che queste chiavi vengano ricondotte ai loro possessori, associando diverse transazioni ad un'unica chiave e quindi ad un'unica identità. Una possibile soluzione sta nel creare coppie diverse di chiavi per ogni studio, in alternativa utilizzare esclusivamente blockchain private, che prevedono la condivisione e la partecipazione alla catena solo tramite una specifica autorizzazione.

  Anche coloro che ricevono i dati di imaging dai pazienti dovrebbero tenere segreta la loro identità, per evitare che le diagnosi vengano collegate ai corrispettivi utenti. Inoltre, nel caso in cui la blockchain venga "interrotta", si corre il rischio di rendere visibili le informazioni archiviate all'interno dei blocchi, specialmente se queste vengono trattate in blockchain pubbliche. Quest'oggi è molto poco probabile riuscire a decriptare un sistema del genere, ma con le evoluzioni di calcolo future potrebbe diventare un rischio sempre maggiore, aggiungendo il fatto che la blockchain è una superficie di attacco davvero estesa.
- La sicurezza: è necessario realizzare nuove ricerche per evitare la perdita o la dimenticanza delle chiavi, i dati risulterebbero così illeggibili per sempre. Se un paziente perde la sua chiave pubblica/privata oppure è in una situazione fisica di emergenza tale per cui non è in grado di utilizzarla, non ha l'accesso ai propri dati. Per

questo motivo è stata proposta l'istituzione di un organo governativo fidato che garantisca una giusta gestione delle chiavi. L'unica nota non positiva di questa soluzione è la centralità nel controllo delle chiavi.

La sicurezza è messa ulteriormente alla prova dal cosiddetto "attacco al 51%"; se un miner o un gruppo di miner ottiene il controllo di almeno il 51% della potenza di calcolo e dei blocchi della catena non verrebbe più ascoltato il meccanismo di consenso, ma verrebbe utilizzato il principio della "catena più lunga" che afferma che la catena più lunga è quella valida. Così facendo la rete è indotta a cambiare e passare alla catena che vuole l'utente malintenzionato. Per questo motivo non è possibile, almeno per ora, sostituire completamente l'uso degli attuali database con quelli progettati secondo lo schema blockchain, è possibile invece l'integrazione tra i due sistemi.

- L'ammissibilità: un altro aspetto che si collega alla sicurezza e alla riservatezza è la realizzabilità del nuovo approccio, in considerazioni delle norme vigenti come quelle contenute all'interno di alcune sezioni del Code of Federal Regulations (CFR), ad esempio la normativa sulla privacy HIPAA che riguarda le autorizzazioni per il rilascio di PHI (Protected Health Information).
- La complessità: con l'avanzare e la crescita del numero di diverse implementazioni di tecnologie blockchain, l'interoperabilità tra i vari sistemi risulterà sempre più difficile. Questo succederà sia perché verrà eliminato del tutto il contributo umano sia perché gli smart contract avranno difficoltà nel destreggiarsi tra le diverse tecnologie.
- La scalabilità e la velocità: la dotazione dei database tradizionali risulta molto più veloce rispetto all'utilizzo della blockchain. La blockchain si basa sul necessario consenso da parte di tutti i nodi della catena. Tale processo aumenta il costo computazionale delle transazioni e richiede maggiore potenza di calcolo, riuscendo ad eseguire solo un numero limitato di operazioni alla volta. Al contrario, i database di utilizzo abituale possiedono la proprietà di essere scalabili, ovvero la facoltà di adattamento nel caso i dati mutassero di mole o tipologia.

  Nelle blockchain pubbliche gli algoritmi di consenso, che ogni nodo deve cercare di risolvere per la creazione di un nuovo blocco, hanno un livello di complessità molto elevato. Usando al contrario blockchain private, i problemi matematici richiesti risultano essere molto più semplici, ma l'energia necessaria è comunque davvero elevata. Per poterla ridurre si potrebbe scegliere quanti e quali nodi possono partecipare al processo di consenso, ma il contro di questa alternativa è che verrebbe eliminata la ridondanza del sistema, punto di forza della blockchain.

- Il costo: una conseguenza del punto sopra citato è l'elevato costo di dotazione. La decentralizzazione e l'elevata energia necessaria si traducono in maggiori spese e quindi in limitazioni nell'utilizzo. Facendo un esempio, lo schema Bitcoin ha imposto una dimensione massima di ogni blocco di 1 megabyte. Da questa considerazione possiamo intuire che la maggior parte delle tecnologie blockchain pubbliche sarebbero troppo dispendiose per poterci archiviare dati così pesanti come le immagini mediche.
- Lo squilibrio economico delle transazioni: la blockchain tiene il conto di quanti studi di imaging sono messi a disposizione da ogni istituzione, valutando quindi la numerosità piuttosto che la tipologia dei dati, oscurata per privacy. A seconda del tipo di studi considerati, tipicamente, si ha un diverso indice di posta in gioco dal punto di vista economico; per fare un esempio, uno studio di imaging tomografico con emissione di positroni avrà un notevole livello di investimento rispetto ad una "semplice" radiografia. Ci sarà quindi uno squilibrio perché saranno scelte con più frequenza quelle aziende che forniscono dati che prevedono costi meno elevati, in quanto un basso costo si traduce in un maggior numero di creazioni di blocchi. Saranno sfavorite quelle aziende che, al contrario, producono pochi dati ma con costi più elevati, solo a causa della complessità delle tecnologie utilizzate.

  Questo aspetto risulta comunque essere un limite minore, poiché in generale non ci si aspetta un rifiuto nel creare blocchi.
- L'esperienza degli utenti: la blockchain comprende una serie di procedimenti che hanno alla base concetti non scontanti, poco conosciuti da tutti e per la maggior parte molto difficili da apprendere. Tra questi ci sono gli aspetti crittografici, la gestione di chiavi, la generazione di nuove chiavi, le autorizzazioni per l'accesso ai propri dati di imaging, la pubblicazione di transazioni. Tutte queste sfaccettature devono essere rese "nascoste" da un'interfaccia (come una applicazione o web app) che ne consenta l'utilizzo immediato e facilitato da parte dell'utente.

  Non solo i pazienti, ma anche gli operatori sanitari devono avere modo di utilizzare questi schemi innovativi nel miglior modo e in tempi immediati. Questo non è del tutto possibile poiché le tecnologie blockchain non trattano alcuni problemi; tramite i loro meccanismi è possibile condividere i dati ma non è garantito e studiato a fondo il loro utilizzo. Questi aspetti sono senza dubbio una sfida da affrontare. [7] [9][15] [16] [18]

Conclusione

L'applicazione blockchain nel dominio dell'imaging biomedicale è agli arbori, presentando per ora pochi casi di utilizzo e di studio. Nonostante le sfide ancora da affrontare, che non ne consentono l'applicazione su larga scala, riesce ad offrire numerosi vantaggi. Tra questi i più significativi e promettenti risultano essere l'eliminazione delle autorità centrali, lo scambio e la condivisione sicura di informazioni su studi di imaging, la garanzia di privacy per i pazienti e la possibilità di collaborazione tra i vari enti coinvolti. Per tali motivi è essenziale che gli studi sulla blockchain nel campo della diagnostica per immagini vengano continuamente approfonditi al fine di migliorarne le problematiche e rendere questa nuova tecnologia una soluzione a tutti gli effetti.

Bibliografia

[1] S. Nakamoto, «Bitcoin: A peer-to peer electronic cash system», *Decentralized Business Review,* p. 21260, 2008.

[2] M. D. Piero, «What is the Blockchain?», *Computing in Science & Engineering,* vol. 19, pp. 92-95, 2017.

[3] B. Segendorf, «What is bitcoin», *Sveri gesRiksbankEconomicReview,* pp. 2-71, 2014.

[4] C. Laneve e . M. Emiliani, «Sicurezza, attacchi e best practice nei contratti Solidity di Ethereum».

[5] V. Buterin, «Ethereum: platform review», *Opportunities and Challenges for Private and Consortium Blockchains,* 2016.

[6] M. Tondello, «Introduzione alle tecnologie blockchain e ai loro possibili usi in sanitá e nelle scienze biomediche».

[7] S. Vergine e A. Bortolotti, «Blockchain, il futuro in blocchi», *Economia Comportamentale,* 2021.

[8] G. Chiap, J. Ranalli e R. Bianchi, Blockchain. Tecnologia e applicazioni per il business, Milano: Hoepli, 2019, pp. 580-674.

[9] D. Yaga, P. Mell, N. Roby e K. Scarfone, «Blockchain technology overview», *arXiv preprint arXiv:1906.11078,* 2019.

[10] J. Golosova e A. Romanovs, «The advantages and disadvantages of the blockchain technology», in *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)*, 2018.

[11] T.-T. Kuo, H.-E. Kim e L. Ohno-Machado, «Blockchain distributed ledger technologies for biomedical and health care applications», *Journal of the American Medical Informatics Association,* vol. 24, pp. 1211-1220, 2017.

[12] «Medicalchain white paper 2.1».

[13] G. Drosatos e E. Kaldoudi, «Blockchain applications in the biomedical domain: a scoping review», *Computational and structural biotechnology journal,* vol. 17, pp. 229-240, 2019.

[14] G. Coppini, S. Diciotti e G. Valli, Bioimmagini, Pàtron editore, 2012, p. 326.

[15] M. P. McBee e C. Wilcox, «Blockchain technology: principles and applications in medical imaging», *Journal of digital imaging,* vol. 33, pp. 726-734, 2020.

[16] V. Patel, «A framework for secure and decentralized sharing of medical imaging data via blockchain consensus», *Health informatics journal,* vol. 25, pp. 1398-1411, 2019.

[17] T. Justinia, «Blockchain technologies: opportunities for solving real-world problems in healthcare and biomedical sciences», *Acta Informatica Medica,* vol. 27, p. 284, 2019.

[18] F. Verde, A. Stanzione, V. Romeo, R. Cuocolo, S. Maurea e A. Brunetti, «Could blockchain technology empower patients, improve education, and boost research in radiology departments? An open question for future applications», *Journal of digital imaging,* vol. 32, pp. 1112-1115, 2019.

[19] J. Van Rossum, «Blockchain for research», *Perspectives on a new paradigm for scholarly communication,* 2017.

[20] W. E. Brant e C. A. Helms, «Fundamentals of diagnostic radiology», 2012.

[21] M. Centonze, P. Peterlongo, E. Moser, L. Ventura, M. Recla, V. Manera, G. Guarrera, F. Fontana e C. Favaretti, «Le tecnologie», *Radiol med,* vol. 113, pp. S41-S44, 2008.

[22] D. Tapscott e A. Tapscott, «What Blockchain Could Mean for Your Health Data», *Harvard business review,* 2020.

[23] C. Campi, B. Bignotti, C. Bortolotto , A. S. Tagliafico, D. Buccicardi, F. Coppola, R. Prost, M. Rengo e L. Faggioni, «Blockchain in radiology research and clinical practice: current trends and future directions», *La radiologia medica,* pp. 1-7, 2022.

[24] E. Kotter, L. Marti-Bonmati, A. P. Brady e N. M. DeSouza, «ESR white paper: blockchain and medical imaging», *INSIGHTS INTO IMAGING,* vol. 12, 2021.

[25] Infodata, «Quanti dati sono generati ogni minuto nel 2021?», *Il sole 24 Ore,* 27 Dicembre 2021.

[26] H. S. Chen, J. T. Jarrell, K. A. Carpenter, D. S. Cohen e X. Huang, «Blockchain in healthcare: a patient-centered model», *Biomedical journal of scientific & technical research,* vol. 20, p. 15017, 2019.