POLITECNICO DI TORINO

Dipartimento di Ingegneria Meccanica e Industriale

Corso di Laurea Magistrale
in Ingegneria Biomedica

Tesi di Laurea Magistrale

Applicazioni blockchain in sistemi di Telemedicina: condivisione e accesso sicuro ai dati sanitari

Relatore

Prof.ssa Monica Visintin

Candidato

Gianmarco Turchetta

Anno Accademico 2019/2020

Indice

Introduzione

Nel white-paper intitolato “Bitcoin: A Peer-to-Peer Electronic Cash System” [1], pubblicato nell’ottobre 2008 da Satoshi Nakamoto, l’autore propone un modello di transazione decentralizzato totalmente nuovo, basato su un meccanismo di consenso che elimina gli intermediari centrali, dove la blockchain rappresenta il caposaldo tecnologico di questa rivoluzione.

Per diverso tempo questa tecnologia ha suscitato l’interesse degli sviluppatori prettamente in ambito finanziario, ma negli ultimi anni la maggiore conoscenza e consapevolezza delle potenzialità della blockchain l’ha trasformata in una possibile risposta alle diverse esigenze di aziende e consumatori.

Con la blockchain l’utente connesso alla rete completa una transazione affidandosi esclusivamente al programma e al suo protocollo, non ad altri attori coinvolti, senza mediatori. Appare evidente la potenza di questa tecnologia anche in termini sociali e politici, soprattutto in una società strutturata in gran parte su modelli centralizzati.

Negli ultimi anni i sistemi decentralizzati sono stati adottati in diversi ambiti come la pubblica amministrazione, il settore agroalimentare, tra le *utilities*, dalle aziende che si occupano di logistica, dalle compagnie assicurative e in sanità. A tal proposito si sta facendo largo la possibilità di utilizzare la blockchain nei sistemi di Telemedicina, disciplina che si occupa di prelievo, gestione, scambio e conservazione di dati biomedici sfruttando tecnologie innovative.

L’applicazione della blockchain in ambiente sanitario può:

- garantire condivisione e accesso sicuro ai dati sensibili del paziente da parte di assicuratori, medici e paziente stesso;
- tenere traccia della cronologia delle prescrizioni mediche, delle somministrazioni di farmaci e della relativa assunzione di terapie;
- consentire una corretta applicazione dei protocolli terapeutici;
- garantire la corretta e sicura trasmissione di dati e informazioni durante operazioni di Telechirurgia.

La creazione di un database contenente cartelle cliniche e dati sanitari condivisibile, non modificabile e accessibile al personale medico, nel pieno rispetto della privacy del paziente: è questa la principale sfida che risiede nell'adozione di sistemi decentralizzati e della blockchain in sanità.

L'obiettivo dell'elaborato è di andare ad analizzare alcuni dei più recenti ed innovativi sistemi di Telemedicina basati sulla tecnologia blockchain, mettendo in luce i principali vantaggi e le possibili criticità derivanti da tale scelta.

1. Evoluzione del concetto di Blockchain

Facendo riferimento al "libro mastro", si può far risalire il concetto di Blockchain al 1400. Gli abitanti dell'isola di Yap, Micronesia, durante un viaggio verso l'isola di Palau, scoprirono una pietra talmente bella e particolare al punto tale da sfruttarla come moneta di scambio. Il suo valore era proporzionale alle dimensioni e alla difficoltà del processo di estrazione dal terreno, elevata al punto da poter provocare vittime. Per aggirare l'impossibilità di scambio fisico di queste pietre, dette Rai, gli abitanti crearono il "libro mastro" per tenere traccia dei loro passaggi di proprietà: ogni abitante possedeva un registro, aggiornabile a seguito di ogni transazione [2].

Dalla necessità di monitorare gli scambi senza muovere fisicamente i Rai nasce quindi il libro mastro e, di conseguenza, il concetto di blockchain, la cui effettiva introduzione e conseguente utilizzo all'interno di sistemi informatici avviene durante la coda del XX secolo. La sua evoluzione può essere riassunta in tre passaggi principali (Figura 1).

Figura 1: Evoluzione della Blockchain.

1.1 Timestamp (1991)

La prima applicazione della blockchain avviene agli albori degli anni '90 da parte di Stuart Haber e Scott Stornetta, nel tentativo di creare una marcatura temporale per i documenti digitali, il *timestamp*, che ne assicurasse l'autenticità [3]. Poter certificare la creazione e/o la modifica più recente di un documento con data e ora certe permette di superare diverse problematiche, ad esempio quelle legate ai diritti di proprietà intellettuale; ma l'uso del timestamp richiede il superamento di due questioni:

1. Occorre che i dati siano contrassegnati con l'ora esatta;
2. Il calendario non può essere modificato.

Una delle soluzioni proposte da Haber e Stornetta, definita "*naive*", consisteva nell'utilizzo di una *digital safety deposit box*: ogni volta che un client ha un file da contrassegnare con data/ora, trasmette il documento a un servizio di marcatura temporale (TSS), il quale registra

la data e l'ora in cui il documento è stato ricevuto, conservando una sua copia per custodia. Ogni volta in cui l'integrità del documento del cliente viene messa in discussione, questo viene confrontato alla copia archiviata dal TSS: se sono identici, il documento non è stato manomesso dopo la data contenuta nei registri TSS. Tale procedura soddisfa i requisiti fondamentali per la marcatura temporale di un documento digitale [4], ma presenta alcune criticità:

- **Privacy**: una terza parte potrebbe "origliare" la trasmissione del documento, al termine della quale è reso disponibile al TSS stesso. Il client deve dunque preoccuparsi della sicurezza dei documenti sotto il suo controllo diretto e di quelli sul TSS.
- **Larghezza di banda e archiviazione**: il tempo richiesto per inviare un documento per il timestamp e lo spazio di archiviazione richiesto presso il TSS dipendono dalla lunghezza del documento. Un documento di grandi dimensioni può risultare proibitivo.
- **Incompetenza:** il documento potrebbe danneggiarsi durante la trasmissione al TSS, essere contrassegnato con data e ora errate quando arriva al TSS, oppure andare del tutto perduto in qualsiasi momento mentre è memorizzato nel TSS.
- **Trust**: nulla impedisce al TSS di colludere con un client, dichiarando di aver timbrato un documento con data e ora diverse da quelle attuali.

Tenendo presenti queste criticità, Haber e Stornetta formularono un'alternativa: sottoporre il documento ad un algoritmo di hashing crittografico, che produceva un ID univoco per il documento. Anzichè trasmettere il documento x al TSS, il client invia il suo valore hash $h(x) = y$. Ai fini dell'autenticazione, la marcatura temporale y è equivalente alla marcatura temporale x. Ciò riduce notevolmente il problema della larghezza di banda e dell'archiviazione, risolvendo anche la questione privacy. A seconda degli obiettivi di progettazione, potrebbe esserci una singola funzione hash utilizzata da tutti, o più funzioni hash diverse per ciascun utente. A ciò si abbinava la firma digitale, utilizzata per identificare in modo univoco il firmatario. Controllando la firma, al client viene garantito che il TSS abbia elaborato la richiesta, che l'hash sia stato ricevuto correttamente e che l'ora inclusa sia corretta. Questo risolve il problema dell'incompetenza da parte del TSS. In Figura 2 è riportato un esempio di catena di blocchi connessi da un valore hash.

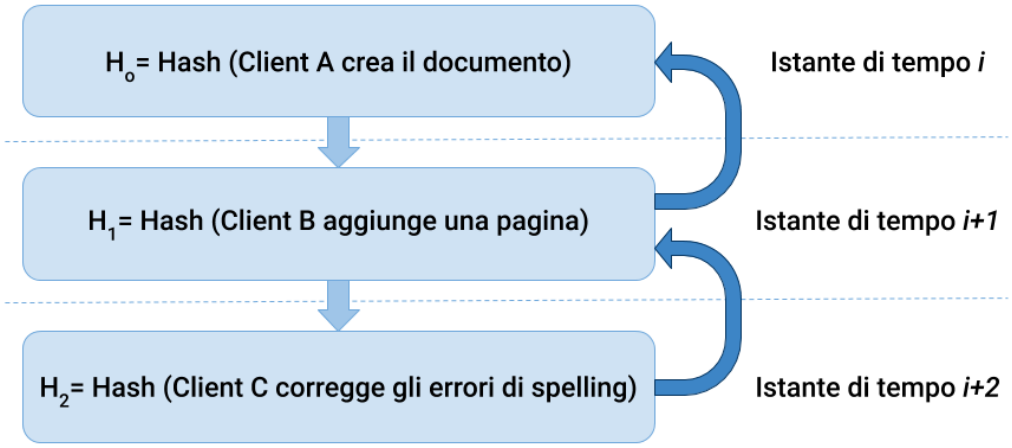

Figura 2: Un documento digitale è modificato dai client A, B e C in diversi istanti di tempo e la catena mantiene un elenco di valori di timestamp relativi agli eventi accaduti sequenzialmente. I valori di timestamp non sono modificabili e in caso di controversie ogni modifica apportata al documento può essere consultata.

1.2 Introduzione dei Merkle Tree (1992)

La struttura per la marcatura temporale di Haber e Stornetta fu integrata, grazie al contributo di Dave Bayer, con i *Merkle Tree* (Alberi di Merkle) [5], offrendo l'opportunità di raccogliere più documenti in un singolo blocco (Figura 3). Questi alberi ereditano il nome da Ralph Merkle e in essi i nodi foglia sono contrassegnati da un blocco dati, mentre i nodi non-foglia dall'hash crittografico delle etichette dei loro nodi figlio. Detti anche Alberi di hash, rappresentano una versione più generale di liste e catene hash e consentono una verifica sicura ed efficace del contenuto di grandi strutture dati.

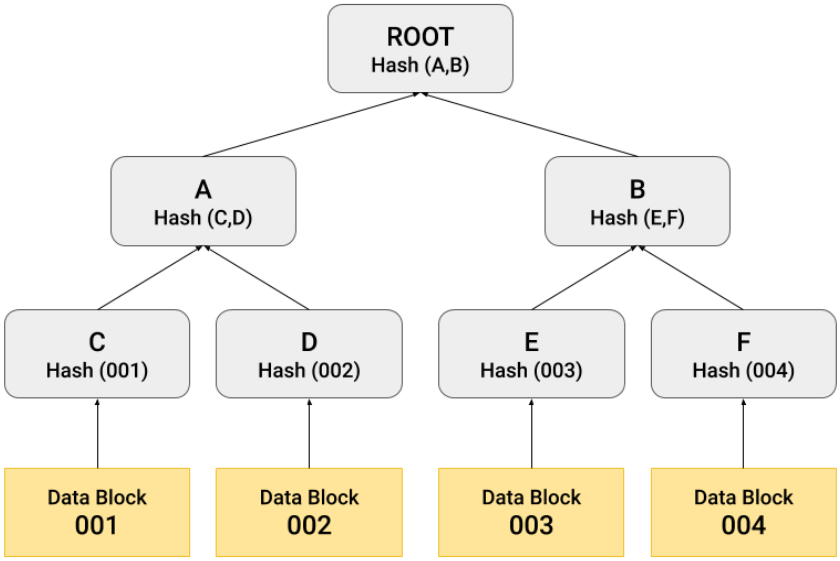

Figura 3: Esempio di albero di Merkle. I valori hash dei blocchi sono definiti "foglie", mentre i valori hash dei loro figli sono detti "nodi". Gli alberi di Merkle vengono utilizzati per rilevare incongruenze tra le repliche e per ridurre al minimo la quantità di dati.

1.3 Satoshi Nakamoto e il Bitcoin (2008)

L'applicazione più famosa e diffusa della blockchain è indubbiamente la criptovaluta Bitcoin. Nel suo white-paper [1], fu il misterioso Nakamoto ad introdurne il funzionamento, seguito dalla prima implementazione di un software Bitcoin su Sourceforge nel Gennaio 2009 [6]. Il codice di valuta del Bitcoin, sebbene non ufficiale, è *XBT*, secondo lo standard ISO-4217. Questo codice viene utilizzato da importanti organizzazioni e società in ambito finanziario come Bloomberg e XE. Proprio secondo XE, 1 Bitcoin (1 BTC) equivale a 13.723 $ ad Ottobre del 2020 (0,00076 $ al lancio) [7]. Bitcoin non è creato o regolamentato da alcun Paese, inoltre non avendo un amministratore centrale, il Bitcoin è classificato come valuta virtuale decentralizzata dal Tesoro degli Stati Uniti [8].

Il protocollo descritto da Nakamoto prevede una serie di regole in grado di garantire integrità e sicurezza dei dati durante una transazione, ridefinendo il significato di fiducia [9]. La rinuncia agli intermediari consente di snellire le sempre più complesse e inefficienti transazioni dei sistemi centralizzati [10] e di ridurre le disuguaglianze sociali, consentendo potenzialmente a chiunque di poter accedere alle transazioni finanziarie.

Con la Bitcoin blockchain (anche semplicemente Blockchain) viene superato l'ostacolo del *double-spending* (doppia spesa), tipico dello scambio di beni digitali (Figura 4).

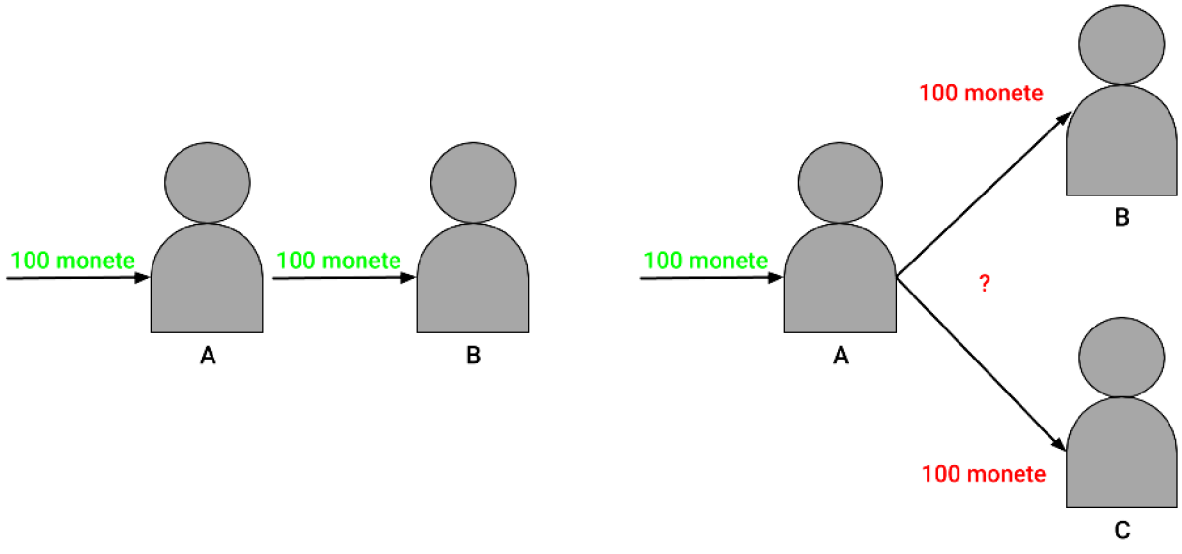

Figura 4: Il problema della doppia spesa (double-spending) in assenza di un intermediario. Supponendo che il soggetto A voglia inviare 100 monete a B, come può B (e chiunque altro utilizzi quelle monete) assicurarsi che A non abbia inviato quelle stesse 100 monete prima ad un soggetto C, senza che ci sia un intermediario (ad esempio una banca) a verificare le transazioni?

Questi beni potevano essere copiati all'infinito prima dell'avvento della Blockchain: senza un mediatore risultava impossibile verificare se una determinata spesa fosse già stata sostenuta. Se l'oggetto di uno scambio di informazioni fosse un file Excel o una PEC, il destinatario riceverebbe una copia esatta del dato trasmesso [11], mentre per il denaro è l'informazione originale ad essere trasmessa durante la transazione. L'adozione di un database distribuito consente di evitare che la stessa somma sia protagonista di più di una transazione.

1.4 Il meccanismo di consenso: dai Bizantini alla Blockchain

L'eliminazione di figure terze atte a gestire le transazioni richiede un buon livello di collaborazione tra gli attori all'interno di una rete: occorre un meccanismo di consenso efficace affinché questi siano d'accordo sull'ordine delle transazioni. Nakamoto ne ha messo a punto uno risolvendo il problema informatico dei generali bizantini [12].

Più generali bizantini, ognuno al comando di una parte dell'esercito, sono localizzati in diverse aree strategiche, in procinto di attaccare una città avversaria e possono interagire solo attraverso dei messaggeri. Occorre elaborare una strategia comune al fine di poter sferrare un attacco vincente: se la maggioranza vota per l'attacco, dovranno farlo tutti, altrimenti tutti dovranno ritirarsi. In assenza di una soluzione inequivocabile, fallirebbero sia l'assalto che la ritirata. È però possibile che tra i messaggeri ci siano dei traditori, che trasmettendo comunicazioni contrarie alla strategia dell'esercito provocheranno la sconfitta a seguito di un attacco non coordinato, o che questi siano fatti prigionieri durante la trasmissione (Figura 5).

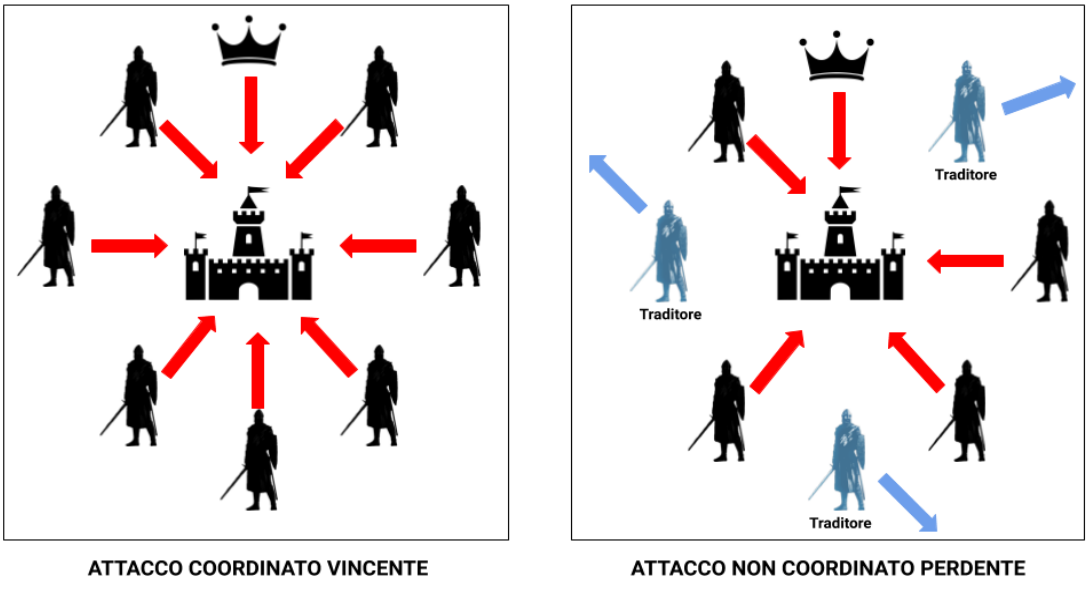

Figura 5: Illustrazione grafica del problema dei generali bizantini.

La metafora dei generali bizantini descrive le criticità di un sistema decentralizzato, nel quale manca una figura centrale a vigilare sulle transazioni tra i nodi della rete, che potrebbero anche essere fallati o corrotti. La blockchain supera questa criticità grazie al meccanismo di consenso introdotto: ogni attore della rete deve concordare sull'autenticità dell'informazione trasmessa nel corso di una transazione, in caso contrario il sistema la respinge. Le operazioni approvate, immutabili e visibili a tutti gli attori, vengono registrate nella rete, proteggendola da errori di trasmissione e tradimenti.

2. Blockchain: caratteristiche e funzionamento

La blockchain rappresenta l'Internet delle Transazioni basandosi su sette caratteristiche principali [13]:

1. Decentralizzazione
2. Trasparenza
3. Sicurezza
4. Immutabilità
5. Consenso
6. Responsabilità
7. Programmabilità

Come visto nel Capitolo 1, la blockchain introduce un nuovo concetto di fiducia, assumendo per molti anche grande valore sociale: le operazioni avvengono in modo onesto e trasparente, senza la dipendenza da un supervisore. In questo capitolo verranno analizzati gli aspetti tecnologici della blockchain pubblica di Bitcoin.

2.1 Architettura della blockchain

La tecnologia blockchain è un database pubblico decentralizzato che tiene traccia di chi possiede beni digitali e di chi effettua transazioni attraverso una rete *peer-to-peer*. Queste sono protette da crittografia e raccolte cronologicamente all'interno di blocchi di dati, a loro volta protetti e collegati. In questo modo viene creato un registro immutabile, che tiene traccia di tutte le transazioni effettuate, replicato su ogni computer che sfrutta la rete [14]. Si può considerare la blockchain come un insieme di meccanismi interconnessi che forniscono funzionalità specifiche all'infrastruttura, come illustrato in Figura 6 [15].

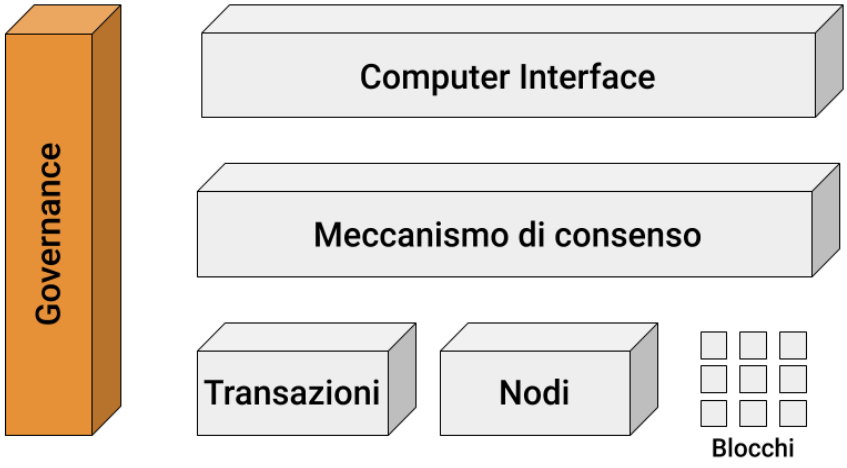

Figura 6: Architettura blockchain.

Al livello più basso di questa infrastruttura ci sono le transazioni, firmate tra i *peers*. Queste denotano un accordo tra due partecipanti, che può comportare il trasferimento di risorse fisiche o digitali. Almeno un partecipante firma questa transazione, poi divulgata ai suoi vicini. L'entità connessa alla blockchain è chiamata nodo e i nodi che verificano tutte le regole blockchain sono chiamati nodi completi (*miner*). Questi raggruppano le transazioni in blocchi e determinano se le transazioni sono valide, quindi conservate nella blockchain, e quali no.

Al livello del meccanismo di consenso, i nodi devono raggiungere un accordo su quali transazioni devono essere mantenute nella blockchain per garantire che non ci siano rami corrotti e divergenze.

La *Computer Interface* consente alle blockchain di offrire più funzionalità: una blockchain memorizza uno stato, ad esempio l'insieme di tutte le transazioni effettuate dagli utenti, mentre la Computer Interface permette di memorizzare stati complessi che vengono aggiornati dinamicamente utilizzando il calcolo distribuito.

Infine, il livello di *Governance* estende l'architettura blockchain coprendo le interazioni umane che avvengono nel mondo fisico. Seppur ben definiti, i protocolli blockchain sono influenzati da input di diversi gruppi di persone che integrano nuovi metodi, migliorano i protocolli e applicano patch al sistema. Sebbene queste parti siano necessarie per la crescita di ciascuna blockchain, costituiscono processi esterni alla catena. Pertanto, la governance della blockchain si occupa di come questi diversi attori si uniscono per produrre, mantenere o modificare gli input che compongono una blockchain.

2.2 Componenti principali della Bitcoin blockchain

Come detto, per analizzare le caratteristiche ed il funzionamento generale della tecnologia blockchain sarà presa in considerazione la più famosa: la blockchain di Bitcoin. I suoi principali elementi sono:

- Nodi;
- Transazioni;
- *Hash*;
- Blocchi;
- Registro (*Ledger*);
- Nodi completi (*Miner*).

2.2.1 Hashing

Per convertire un messaggio di una certa lunghezza in una stringa di dimensioni fisse si utilizza una funzione hash *h*, che genera valori hash (*digest*). La mappatura avviene in maniera tale da non consentire di risalire al messaggio originale partendo dalla stringa, la cui lunghezza è direttamente proporzionale al livello di sicurezza della funzione. Una funzione hash ideale dovrebbe:

1. Calcolare facilmente i valori hash, per qualsiasi dato a disposizione;
2. Produrre i medesimi digest per due o più input uguali;
3. Garantire difficoltà di previsione dei digest conoscendo i dati in ingresso;
4. Impedire di risalire alle informazioni iniziali a prescindere dalla tipologia di input;
5. Produrre valori hash molto diversi tra loro anche per input simili.

A seconda dell'algoritmo adottato varia la lunghezza dei digest. Bitcoin usa l'algoritmo SHA-256 che restituisce un output di 256 bit. Un esempio di hashing con questo algoritmo è riportato nella Figura 7. Appare chiaro come modificando anche solo leggermente la sintassi di una stessa parola ("Buongiorno") si ottengano valori hash molto diversi l'uno dall'altro.

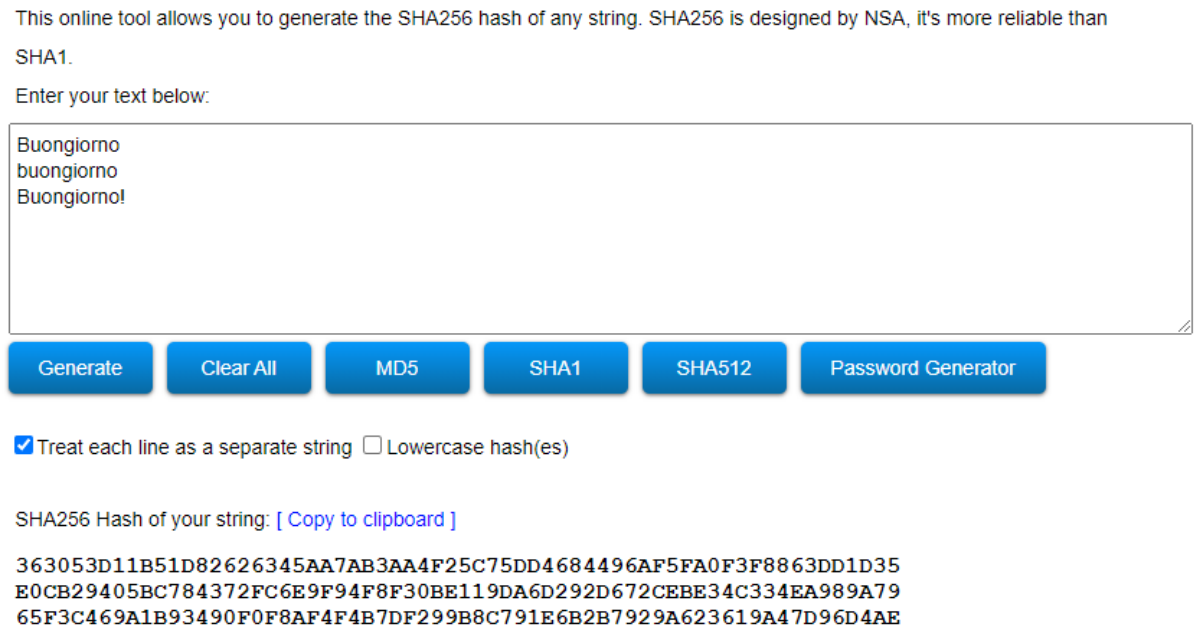

Figura 7: Valori hash ottenuti con algoritmo SHA-256 per diverse varianti dello stesso input. [Online] https://passwordsgenerator.net/sha256-hash-generator/

2.2.2 Nodi, transazioni e blocchi

La transazione è un'operazione di scambio di risorse fisiche o digitali tra utenti (nodi) connessi ad una rete peer-to-peer [16]. Al suo interno saranno contenuti gli indirizzi pubblici dei nodi coinvolti nello scambio, l'*amount* della transazione e la firma digitale del mittente (Figura 8).

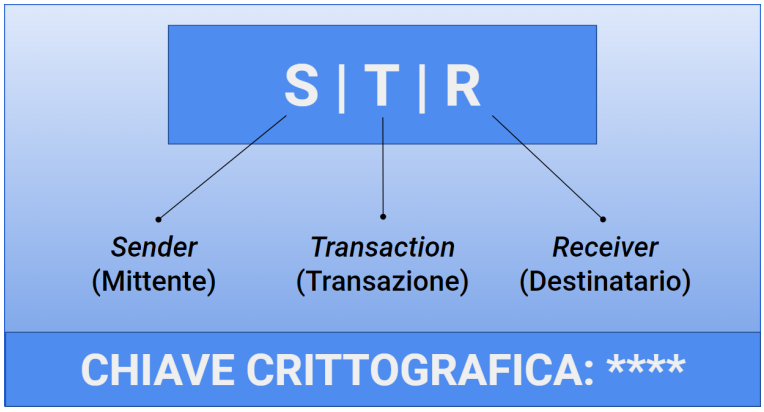

Figura 8: Principali componenti della transazione.

Le firme digitali sono utili ai nodi per dimostrare la loro identità senza rivelare la propria chiave privata. La firma è il risultato della combinazione tra la chiave privata del mittente e la funzione hash (Figura 9). Il destinatario riceve i dati crittografati insieme alla firma digitale, e sfruttando la chiave privata del mittente può decifrare i dati. La chiave pubblica è stata precedentemente condivisa tra gli utenti coinvolti o consultabile all'interno del server. L'algoritmo usato per la creazione della firma digitale è l'*Elliptic Curve Digital Signature Algorithm* (ECDSA) [17].

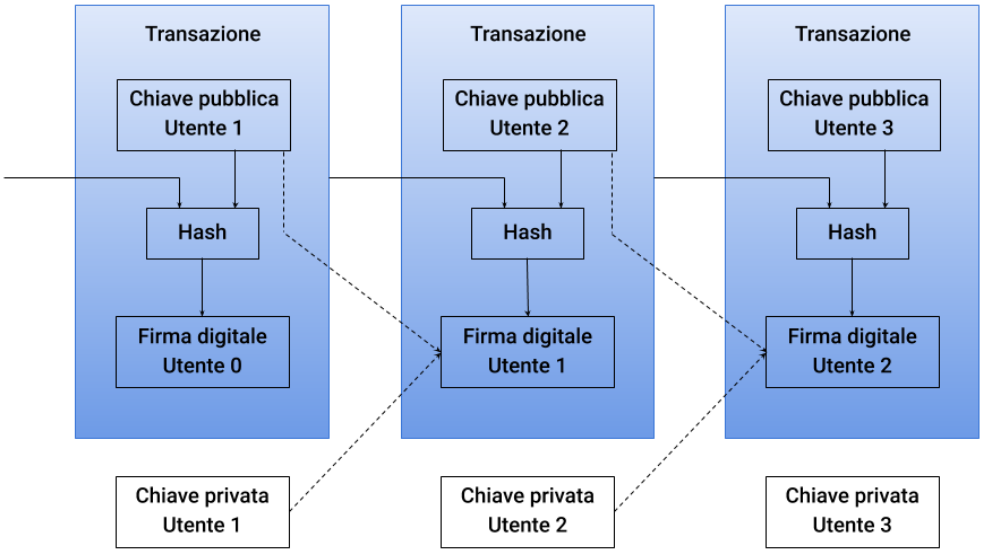

Figura 9: Uso della firma digitale nelle transazioni.

I blocchi, unità fondamentali della catena, sono caratterizzati da un insieme di transazioni, un *timestamp* che li colloca temporalmente, un valore hash posto nell'header (Figura 10) e l'hash dei blocchi precedenti, in modo tale da poter monitorare lo stato attuale della catena anche a seguito dell'aggiunta di nuovi blocchi (Figura 11).

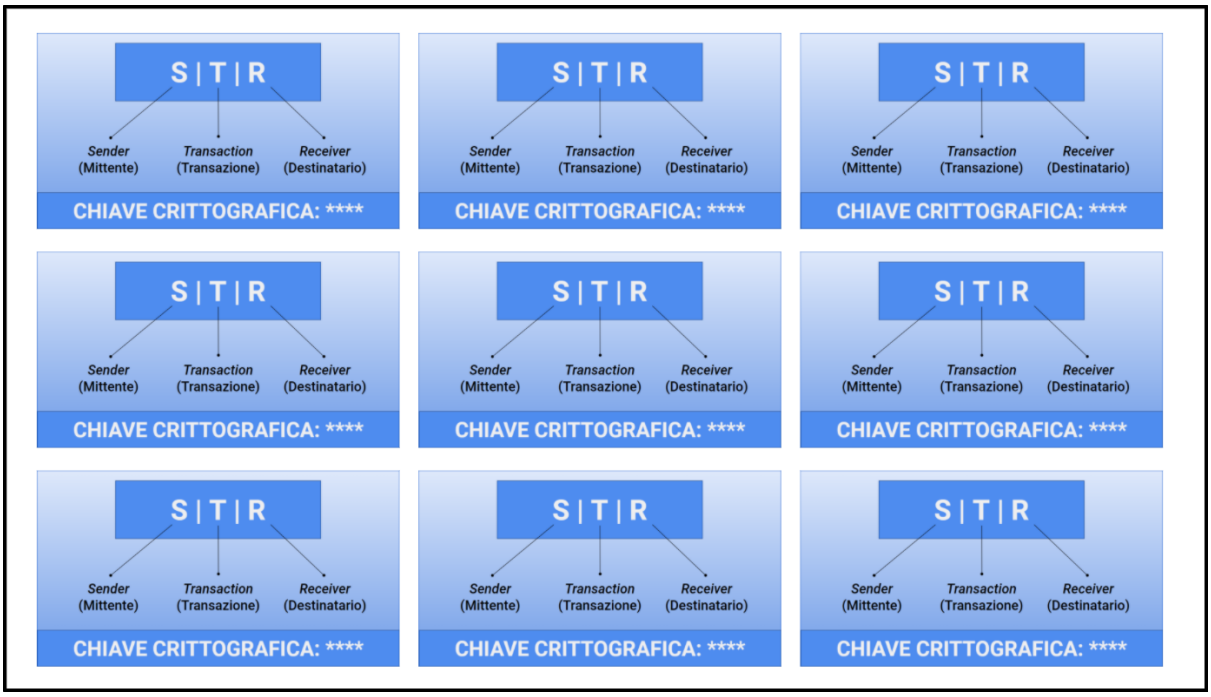

Figura 10: Struttura di un blocco contenente diverse transazioni.

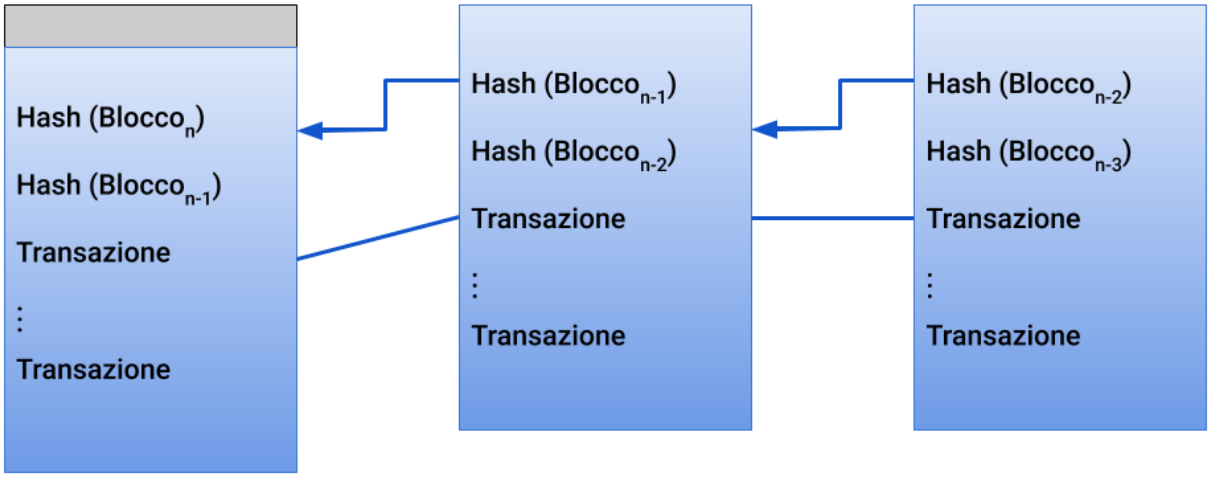

Figura 11: *Hash-chain*. Ogni blocco contiene più transazioni, un valore hash proprio e quello del blocco precedente: forma una *hash-chain* o *blockchain*. L'ordine dei blocchi è deterministico. Ogni nodo conserva una copia dell'intera blockchain, in modo da poter verificare ogni transazione.

2.2.3 Il registro (Ledger)

Esistono tre diversi tipi di network :

- **Rete centralizzata (Centralized Network):** crea un *single-point-of-failure*. Se l'intermediario centrale non è attivo o viene attaccato, l'intera rete smette di funzionare (Figura 12 A);
- **Rete Decentralizzata (Decentralized Network):** non contiene *single-point-of-failure*. Se uno dei nodi, come il nodo 1, è inattivo o è attaccato, il resto della rete può ancora funzionare normalmente (Figura 12 B);
- **Rete Distribuita (Distributed Network):** tutti i nodi possono vedere tutto ed esiste un meccanismo di timestamp distribuito (Figura 12 C).

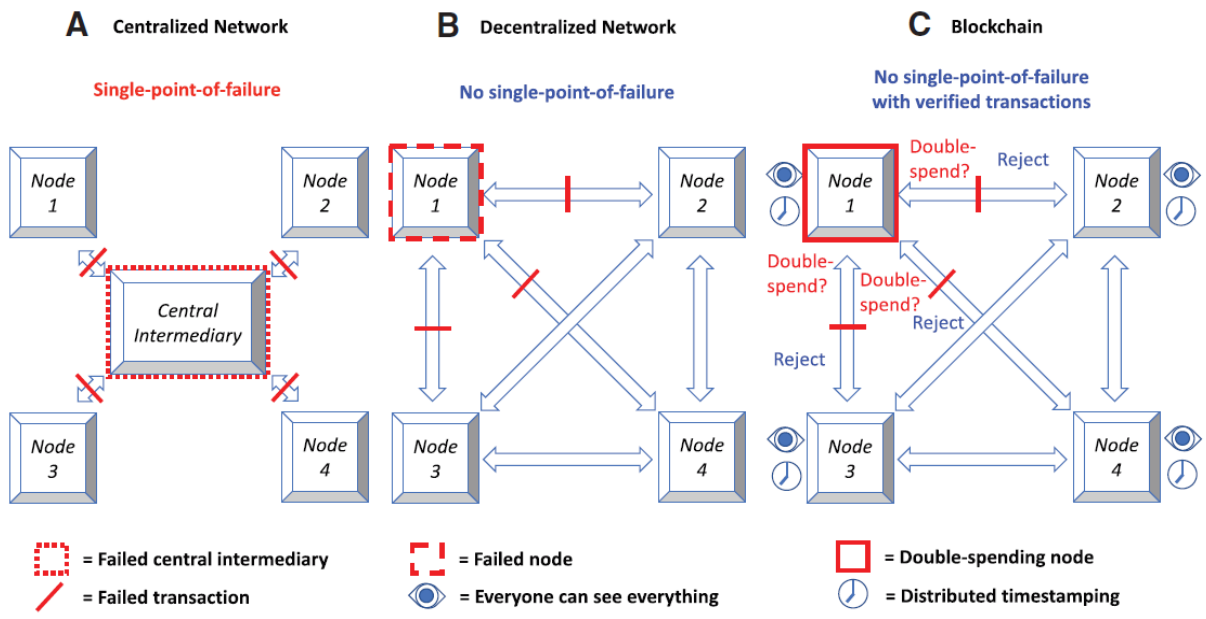

Figura 12: Confronto delle topologie di rete [18].

L'ultima configurazione è tipica della tecnologia blockchain nella quale il registro, definito anch'esso distribuito, tiene nota di tutte le transazioni avvenute all'interno della rete e offre informazioni aggiornate sullo stato attuale della catena. La configurazione distribuita è più sicura di quella centralizzata per due motivi: non esiste un punto vulnerabile centrale; la potenza di calcolo richiesta ad un hacker per modificare una transazione all'interno di un blocco, e di conseguenza in tutti i blocchi della catena, non è raggiungibile con le attuali tecnologie.

2.2.4 Proof-of-Work, Miner e token

L'algoritmo di consenso adottato dalla Bitcoin blockchain è il protocollo *Proof-of-Work* (PoW) illustrato in Figura 13.

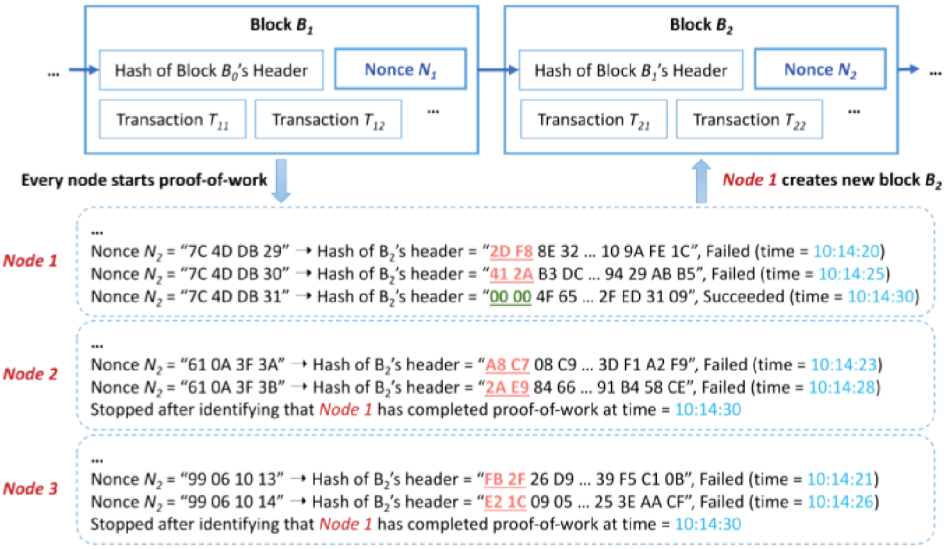

Figura 13: Meccanismo *Proof-of-Work* [18]. Uso di cifre esadecimali: 8 per i nonce, 64 per i valori hash e 4 zeri iniziali per confermare il termine del lavoro. Il Nodo 1 è il primo a completare con successo il lavoro alle 10:14:30 e crea il blocco B_2. I Nodi 2 e 3 interrompono la prova al momento della creazione del nuovo blocco.

Il *nonce*, generalmente di 32 bit, è un contatore aggiunto al blocco che funge da input della funzione hash. Per provare (*proof*) il lavoro di hashing, il nonce viene incrementato di 1 bit per ogni calcolo dell'hash (*work*) finchè il digest da 256 bit (SHA-256) non conterrà 16 bit zero iniziali (*target*).

Le transazioni non confermate vengono raccolte in un pool di memoria per ciascun nodo, mentre al primo nodo che riesce a completare la Proof-of-Work viene concessa la creazione di un nuovo blocco, la verifica delle transazioni, lo spostamento delle transazioni confermate in un nuovo blocco al fine di allungare la catena e una ricompensa (*token*).

Questo processo è detto *mining* nella Bitcoin blockchain, e i nodi coinvolti sono i *miner*. Essi sono chiamati ad affrontare dei problemi computazionali proposti dall'algoritmo, al fine di convalidare nuovi blocchi della catena a seguito della loro risoluzione. Tra i problemi troviamo [19]:

- Individuare un input partendo dal digest della funzione hash;
- Scomposizione in numeri primi;
- *Guided tour puzzle control*: ad alcuni nodi è richiesto il calcolo di una funzione di hash in caso di attacco *DoS* (*Denial of Service*).

La difficoltà del problema è proporzionale al numero di miner, alla potenza di calcolo e al carico della rete e deve essere bilanciata: se troppo elevata rallenta la creazione dei blocchi, se troppo bassa rende la rete facilmente attaccabile. La creazione di un blocco richiede mediamente 10 minuti [19]. Il problema in Bitcoin è definito *Hashcash*, e l'utente che riesce a risolverlo è ricompensato in Bitcoin (Figura 14).

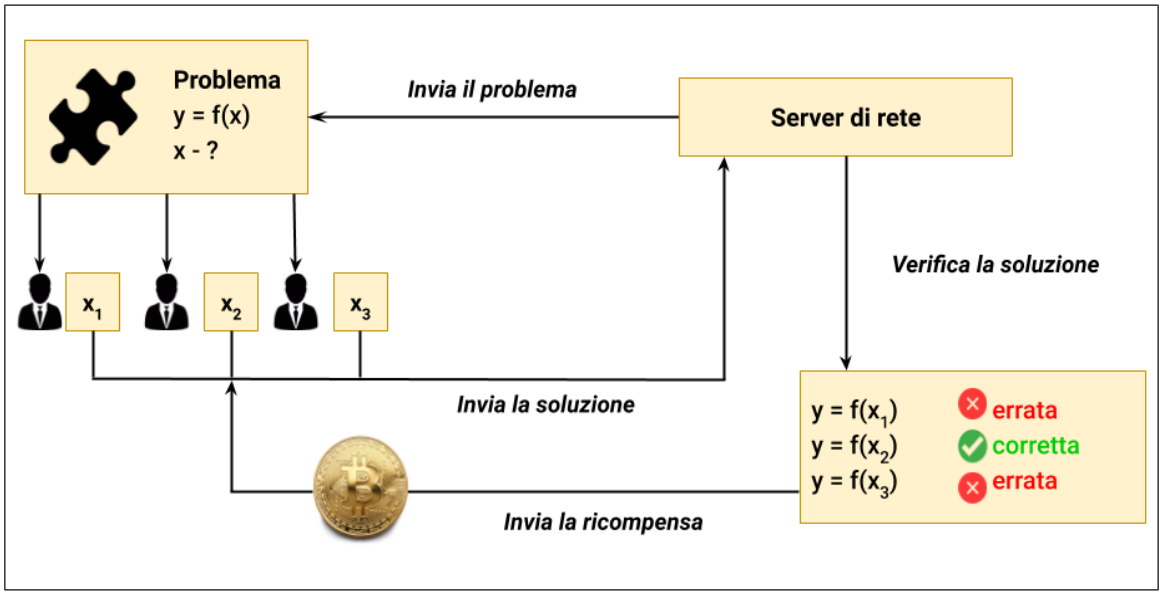

Figura 14: Esempio di funzionamento di Hashcash, nel quale il miner che fornisce la soluzione corretta al problema matematico viene ricompensato con un token.

Sulla base di quanto visto fin qui, la tecnologia blockchain può definirsi **sicura**, **trasparente**, **immutabile** e ***trustless***.

2.3 Classificazione blockchain

La blockchain Bitcoin analizzata nel precedente paragrafo è di tipo pubblico, ma negli ultimi anni si stanno diffondendo sistemi basati su blockchain privata, dove soltanto ad un numero limitato di nodi è concessa la verifica o la modifica dello stato della catena, pur non rinunciando alle caratteristiche fondamentali di autenticità e decentralizzazione. Sebbene introduca una "selezione" lontana dalla filosofia di Nakamoto, la blockchain privata ha catalizzato l'attenzione di molti settori, soprattutto quello finanziario [20]. Le tecnologie blockchain sono classificabili in:

- **Blockchain pubblica**. A nessun utente è preclusa la possibilità di partecipare alla rete come nodo e al processo di mining, mettendo a disposizione la propria quota di partecipazione. Tutti possono effettuare transazioni, validarle e accedere

pseudo-anonimamente ai contenuti del database. Totalmente decentralizzata, garantisce la sicurezza dei dati contro potenziali attacchi esterni (Figura 15).

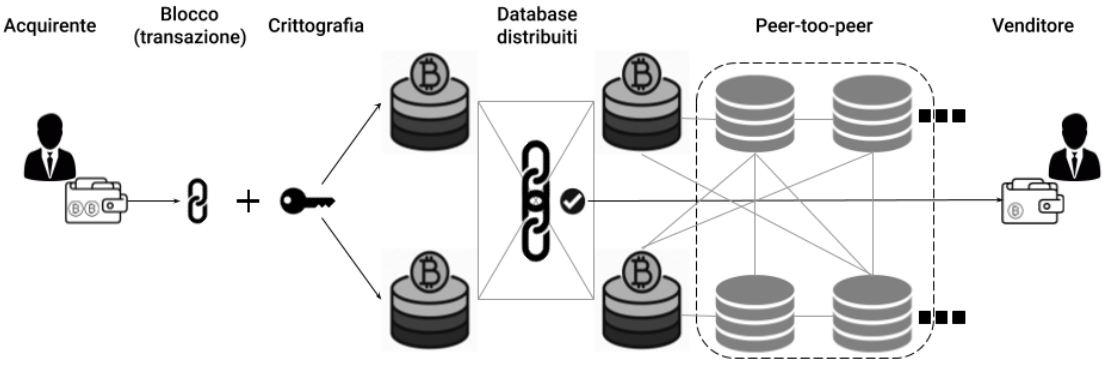

Figura 15: Blockchain pubblica. Il venditore crea un blocco o una transazione, distribuita e validata attraverso hashing crittografico. La transazione viene affidata ai miner che vengono ricompensati per il lavoro svolto. Al termine del processo, il venditore riceve la transazione [21].

- **Blockchain privata**. Mentre le operazioni di scrittura dipendono da autorizzazioni centralizzate, quelle di lettura possono essere pubbliche o assegnate a nodi selezionati.

- **Blockchain permissioned (*Consortium)***. Detta anche "decentrata", è una sintesi delle due alternative precedenti: il meccanismo di consenso è gestito da nodi predefiniti già noti (Consorzio), garantendo fiducia pregressa ed una maggiore efficienza di validazione delle transazioni, mentre le autorizzazioni di lettura possono essere rilasciate a tutti gli utenti della rete o solo ad alcuni per offrire una maggiore privacy (Figura 16).

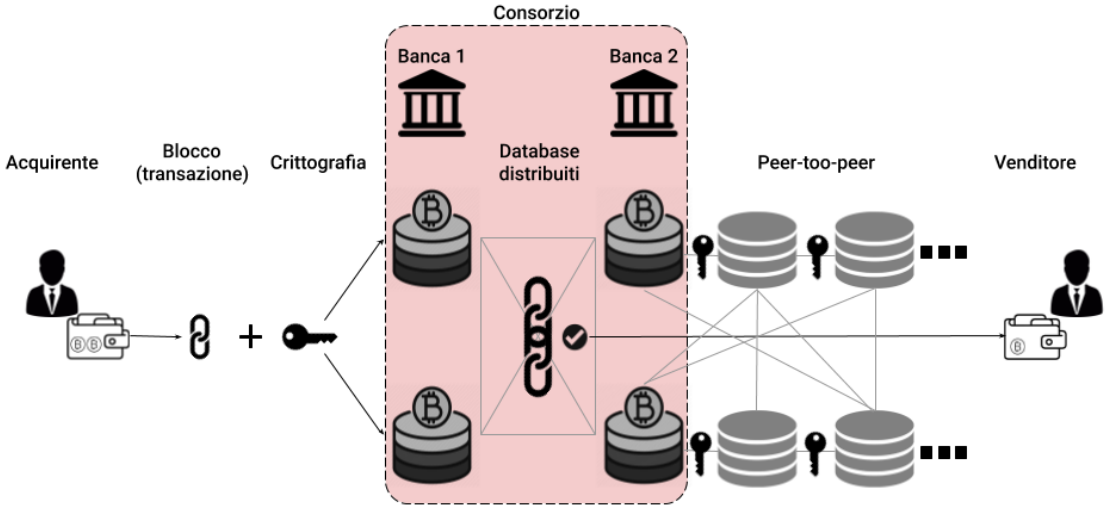

Figura 16: Blockchain permissioned. Il venditore crea un blocco o una transazione, distribuita e validata attraverso hashing crittografico. La transazione viene controllata dal Consorzio, mentre l'autorizzazione di lettura è concessa solo ad una parte della rete [21].

La Tabella 1 riassume le principali differenze tra le tipologie di blockchain appena viste.

	PUBBLICA	PRIVATA	*PERMISSIONED*
Consenso	Tutti i *miner*	Nodi selezionati	Nodi selezionati
Lettura	Pubblica	Pubblica o limitata	Pubblico o limitata
Immutabilità	Molto alta	Non definita	Non definita
Centralizzazione	No	Sì	Circoscritta
Efficienza	Bassa	Elevata	Elevata
Token	Sì	No	Dipende

Tabella 1: Confronto tra le varie tipologie di blockchain.

2.4 Ethereum e gli smart contract

I contratti intelligenti (*smart contracts*) sono stati idealizzati per la prima volta da Nick Szabo [22], ma ci sono voluti due decenni circa perché si concretizzassero. Si tratta di software auto-eseguibili all'interno della blockchain che aiutano gli utenti a portare a buon fine le transazioni senza doversi rivolgere ad un intermediario, ideali quindi per un sistema distribuito. Più che di veri e propri contratti si parla di codici *if-this-then-that* all'interno di protocolli e programmi, che leggono le clausole e le condizioni poste al momento della stipula dell'accordo e si autoesegueno al verificarsi delle condizioni. L'assenza del contributo interpretativo di un soggetto esterno fa sì che la responsabilità decisionale ricada esclusivamente sul software, garantendo oggettività di giudizio, ma può costituire una criticità durante la stesura del contratto: il codice deve essere scritto in modo tale poter prevedere ogni scenario possibile, senza commettere errori nella lettura e nell'interpretazione delle regole contenute nell'accordo. Gli smart contract possono essere quindi definiti autonomi e distribuiti. In Figura 17 è riportato un esempio di smart contract nel linguaggio *Solidity* [23].

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.4.16 <0.8.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

Figura 17: Smart contract in Solidity. È costituito da stati (‘*storedData’*) e funzioni (‘*pragma’, ‘get’, ‘set’*), mentre in cima sono indicate licenze e l’ultima versione del linguaggio. In questo specifico contratto consente a chiunque, senza specifici impedimenti, di memorizzare un numero accessibile a tutti.

Il primo utilizzo concreto degli smart contract si ha nella blockchain pubblica *Ethereum*, sviluppata a partire dal 2013 da Vitalik Buterin, nella convinzione che Bitcoin avesse bisogno di un linguaggio di scripting per creare applicazioni decentralizzate [24]. Ethereum segna il passaggio al *Distributed Computing*, in quanto paragonabile ad un grande computer condiviso, accessibile dovunque e per sempre, dalla grande potenza di calcolo; è definita anche blockchain programmabile, in quanto mette a disposizione degli utenti la possibilità di creare le proprie applicazioni decentralizzate.

Sfrutta il meccanismo di consenso *Proof-of-Stake*, nel quale l’utente blocca una parte del suo capitale come posta in gioco (*stake*) prima di partecipare al processo di *forging*, così detto in quanto i nuovi blocchi vengono letteralmente forgiati. Grazie ad una selezione pseudo-casuale basata sulla percentuale di partecipazione, l’algoritmo sceglie il nodo che dovrà validare il nuovo blocco: se possiede il 15% delle attività di blockchain, allora dovrà svolgere il 15% di forging richiesto, semplificando così la verifica e consentendo un risparmio energetico e operativo [25]. La criptovaluta della blockchain Ethereum è chiamata *Ether*, che può essere trasferita tra account o usata per compensare i costi di esecuzione degli smart contract. In più, il meccanismo Proof-of-Stake garantisce un elevato livello di sicurezza contro attacchi esterni: l’hacker dovrebbe possedere più della metà delle criptomonete per poter manomettere un blocco o aggiungerne uno non corrotto.

I contratti intelligenti adottati in Ethereum vengono generati indipendentemente, separati l'uno dall'altro, nella *Ethereum Virtual Machine* (EVM). Si tratta di un ambiente di *runtime* sicuro e protetto nel quale i programmatori possono lavorare in remoto, che consente loro di caricare aggiornamenti progressivi sulla blockchain Ethereum e che ha fatto sì che nascessero numerose applicazioni decentralizzate (*DApps*).

La Tabella 2 riassume le principali differenze tra Bitcoin ed Ethereum.

	Bitcoin	**Ethereum**
Meccanismo di consenso	*Proof-of-Work*	*Proof-of-Stake*
Algoritmo	SHA-256	Etash
Transazioni al secondo	7 tps	20 tps
Tempo creazione blocco	10 m	10-12 s
Scalabilità	No	Sì
Valuta	Bitcoin	Ether

Tabella 2: Principali differenze tra blockchain Bitcoin e Blockchain Ethereum.

La blockchain Ethereum, grazie alla rapidità di processamento delle transazioni e alla scalabilità, che consente di gestire grandi quantità di dati, viene adottata nella maggior parte dei sistemi digitali in ambito sanitario. *Patientory* e *Healthcoin* sono due sistemi che hanno anche sviluppato il proprio token: ad esempio, quando si utilizza Patientory, un medico può utilizzare un token nativo della rete (*POTY*) per poter recuperare l'anamnesi di uno specifico paziente; in Dentacoin invece il paziente riceve token con cui poter pagare le spese di cura presso una clinica odontoiatrica partner rispondendo a specifici sondaggi [26]. Alcuni dei sistemi di Telemedicina approfonditi nel Capitolo 5 (*DermoNet*, *HapiChain*, *AaYusH*) sono basati proprio su Ethereum

2.5 Privacy

La tecnologia blockchain offre grande protezione dei dati degli utenti grazie all'uso della crittografia e alla sua natura decentralizzata e distribuita che le consente di difendersi da attacchi esterni; inoltre la sua trasparenza consente agli utenti di poter tracciare tutte le transazioni all'interno della catena. Appare impossibile dunque una convivenza di questi principi con il Regolamento Generale sulla Protezione dei Dati (GDPR).

Emanato ed approvato nel Maggio 2018 dalla Commissione Europea, tale regolamento mira a tutelare il proprietario dei dati, contro una loro eventuale divulgazione non autorizzata, alterazione e/o distruzione, con l'obiettivo di uniformare le norme sulla protezione dei dati personali all'interno dell'UE. I suoi articoli cardine possono riassumersi come segue [27]:

Articolo 12: diritto al chiarimento sull'utilizzo dei propri dati da parte dell'ente e alla richiesta di risarcimento in mancanza di risposte chiare, concise e tempestive;

Articoli 13 e 14: diritto di conoscere le modalità di utilizzo dei dati personali al momento della loro raccolta/richiesta e i tempi di conservazione dei dati;

Articolo 15: diritto di accesso ai dati personali elaborati/processati dall'ente che ha ottenuto il consenso;

Articolo 16: possibilità di modificare i propri dati personali;

Articolo 17: diritto di chiedere (e ottenere) la cancellazione dei propri dati personali quando lo scopo della raccolta viene meno;

Articolo 18: possibilità di limitare il trattamento dei propri dati se inesatti oppure raccolti illegalmente o eludendo le norme giuridiche;

Articolo 19: l'ente che si occupa della raccolta dei dati deve informare anche le "terze parti" a cui è concesso l'utilizzo di eventuali modifiche o cancellazioni;

Articolo 20: l'interessato ha diritto a ricevere i propri dati personali in un formato strutturato e usato comunemente in modo che possano essere letti da una qualsiasi macchina (PC, smartphone, app, ecc.);

Articolo 21: diritto di opporsi all'utilizzo dei propri dati per profilazione o commercializzazione.

È evidente come il GDPR regolamenti soltanto sistemi centralizzati. Il *Data Protection Officer* (DPO), figura che fornisce supporto al soggetto atto al controllo e alla gestione dei dati personali, è difficile da immaginare nella blockchain, che non ammette terze parti, così come le leggi da applicare in caso di controversie. Nel contesto blockchain poi non si ha una chiara definizione di dato personale: sebbene la chiave pubblica offra pseudo-anonimato, questa non costituisce un dato personale in senso stretto. Su ogni nodo della blockchain i dati risultano "fermi", accessibili a chiunque, a prescindere dal fine per cui sono stai raccolti ed elaborati, mentre gli articoli 13, 14 e 21 del GDPR impongono una chiara illustrazione delle finalità di raccolta dei dati. Infine la possibilità di modifica e cancellazione dei dati personali, il cosiddetto "diritto all'oblio", collide con la caratteristica di immutabilità della blockchain.

Per far sì che la tecnologia blockchain possa essere sfruttata in determinati ambiti, nel caso specifico di questa Tesi in quello sanitario e delle tecnologie e-Health, occorre far coesistere i suoi principi di decentralizzazione, distribuzione ed immutabilità con il GDPR. Due possibili soluzioni potrebbero essere:

- **Stoccaggio dei dati personali all'esterno della catena**. I dati sono memorizzati all'esterno, mentre nella blockchain viene iscritto un collegamento sotto forma di hash, consentendo in caso di necessità la rimozione dei dati senza scalfire la catena [28].

- **Distruzione delle chiavi pubbliche.** Renderebbe i dati raccolti nella blockchain illeggibili. Affinché i regolatori possano accettarla come una cancellazione dei dati ai fini del GDPR, la distruzione deve avvenire in conformità con le migliori pratiche e in maniera verificabile [29].

- **Accesso ai dati limitato per i nodi.**

- **Analisi preventiva.** Sarebbe opportuno stilare un elenco di azioni, con relative conseguenze, da adottare in caso di interruzione della crittografia o di scadenza del periodo di archiviazione dei dati personali consentito dalla legge [30].

La realizzazione di un sistema informatico basato sulla blockchain che rispetti pienamente le normative vigenti sulla salvaguardia della privacy costituisce una grandissima sfida per gli sviluppatori. Il rispetto del GDPR è infatti uno dei motivi principali che ha spinto diverse aziende e istituzioni a rinunciare all'adozione di sistemi basati sulle blockchain pubbliche.

3. Blockchain e sanità

La possibilità di integrare la tecnologia blockchain nella sanità pubblica ha attirato l'attenzione dei grandi *provider* tecnologici. Il connubio blockchain-sanità ha grande potenziale, in quanto consentirebbe operazioni di autenticazione, di monitoraggio dei parametri vitali *real time* e di compilazione del diario clinico del paziente in maniera sicura, attraverso l'uso di dati immutabili e decentralizzati, protetti da crittografia.

Per rendere questo connubio efficace, la blockchain deve rispettare alcuni importanti requisiti di qualità, tenendo presente anche eventuali limiti come l'interoperabilità dei sistemi, la privacy e la scalabilità. Di seguito verranno esposti i requisiti imprescindibili per il corretto funzionamento della tecnologia blockchain in medicina, e i possibili campi applicativi.

3.1 Oltre la cryptocurrency

La natura distribuita della blockchain rende questa tecnologia camaleontica, adattabile a diversi contesti, senza limitarsi al mondo delle criptovalute. Non a caso i numerosi studi di ricerca svolti ed esposti al *World Economic Forum* (*WEF*) nel 2017 hanno evidenziato un interesse crescente nei due anni precedenti verso la blockchain da parte dei maggiori investitori, sempre alla ricerca di nuove soluzioni che garantissero maggiore efficienza e trasparenza nei processi [31]. Le caratteristiche *open source* e l'adattabilità a più settori industriali della blockchain hanno attirato sempre più programmatori, aziende ed enti governativi a sfruttare la tecnologia per rivoluzionare le proprie strutture. Con blockchain 3.0 si intendono tutte le possibili applicazioni non finanziarie della tecnologia di registro distribuito [32]. In Figura 18 sono rappresentati i principali domini applicativi della blockchain nel 2020.

Sebbene la tecnologia blockchain Bitcoin sia ampiamente riconosciuta e sia stata utilizzata per diversi scopi, questa è divenuta nota in ambito sanitario come metodo di pagamento di riscatti: i dati sanitari venivano crittografati da utenti malintenzionati e per decifrarli chiedevano alle istituzioni proprietarie dei dati un pagamento in criptovalute. I *Ransomware* (malware che limitano l'accesso al dispositivo infetto, richiedendo appunto un riscatto da pagare per rimuovere la limitazione) hanno colpito diversi sistemi sanitari, con conseguenti ingenti perdite economiche. La valuta Bitcoin viene utilizzata perché è affidabile, mentre è molto difficile rintracciare il suo destinatario. Tuttavia, la blockchain Bitcoin può essere utilizzata per aiutare i sistemi sanitari e la ricerca biomedica, e non solo per danneggiarli.

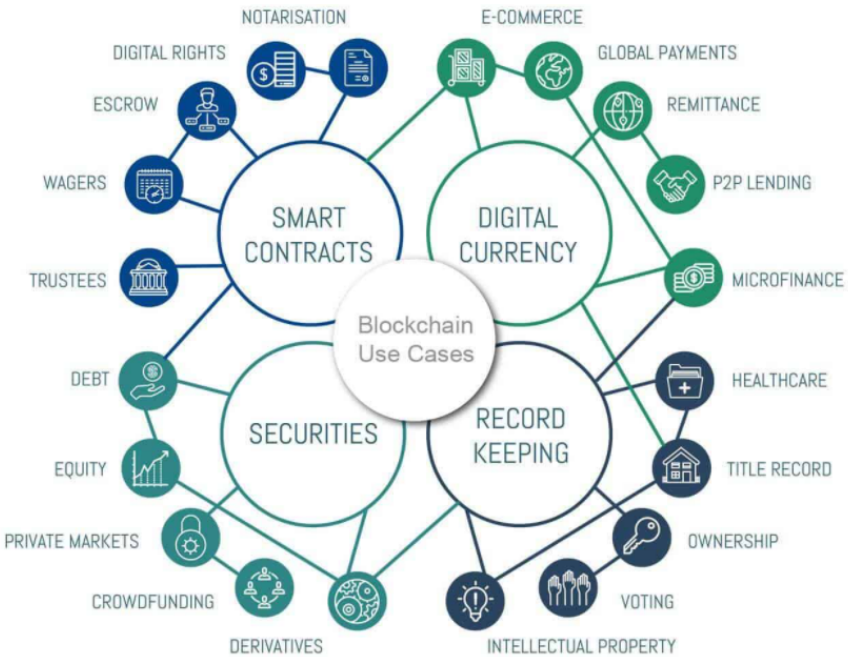

Figura 18: Principali casi d'uso della tecnologia blockchain, oltre la finanza e le criptovalute [33].

3.2 Requisiti qualitativi della blockchain in sanità

Affinché la blockchain possa essere utilizzata in maniera efficace da un software operativo in ambiente sanitario, occorre che questa rispetti cinque fondamentali requisiti di qualità:

1. **Disponibilità**
2. **Trasparenza**
3. **Sicurezza**
4. **Prestazioni**
5. **Usabilità**

3.2.1 Disponibilità

I dati medici dei pazienti, generati da diverse fonti (anche i dispositivi indossabili), possono essere raccolti direttamente all'interno di una *medical chain*, accessibile e utilizzabile dai pazienti stessi per poter consultare facilmente le proprie cartelle cliniche, anche se archiviate in posizioni distribuite (Figura 19). Essendo i dati archiviati su una rete decentralizzata, non esiste un singolo punto di attacco [34], riducendo il rischio di non accessibilità al proprio registro. I pazienti possono quindi, selettivamente e in sicurezza, condividere l'accesso ai propri dati con terze parti di cui si fidano.

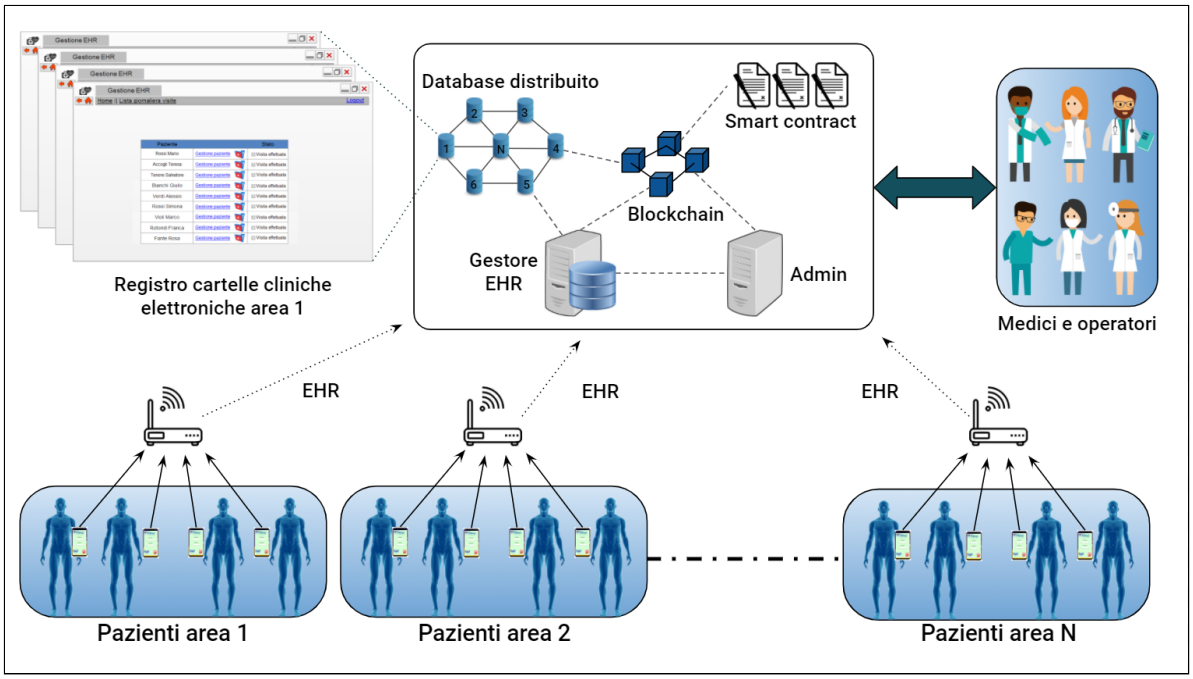

Figura 19: Sistema di gestione delle cartelle cliniche elettroniche (EHR) di pazienti localizzati in differenti aree geografiche. I dati raccolti mediante dispositivi smart consentono il continuo aggiornamento delle cartelle, processate nella blockchain pubblica basata su smart contract, e accessibili al personale medico-sanitario.

Con la tecnologia blockchain, e dal momento che non esiste un intermediario, anche gli operatori sanitari hanno accesso ai dati quasi in tempo reale: ciò consentirebbe ai ricercatori di rilevare e isolare rapidamente particolari condizioni ambientali capaci di colpire la salute pubblica, ad esempio un'epidemia.

La caratteristica di immutabilità implica anche la possibilità di accedere all'intera cronologia delle cartelle cliniche. Ciò può creare un conflitto con il GDPR che, oltre alla possibilità di accedere ai propri dati, in questo caso sanitari, garantisce agli utenti la possibilità di cancellarli da un database se lo desiderano.

3.2.2 Trasparenza

Secondo i principi della blockchain, qualunque aggiunta ai blocchi della catena dovrebbe risultare visibile ai nodi della rete (i pazienti), ed essendo i dati inseriti immutabili, risulterà semplice individuare modifiche non autorizzate.

Ad esempio nel contesto dei farmaci contraffatti, la blockchain deve essere in grado di tracciare il farmaco (Figura 20), da materia prima a prodotto finito, in un registro digitale immutabile e condiviso; rilevare i farmaci contraffatti nella *supply chain* (catena di approvvigionamento); integrarsi con le tecnologie IoT (*Internet of Things*) per automatizzare il processo; proporsi come standard tecnologico che migliori la qualità di condivisione di

informazioni tra database non correlati ma che includano diversi partecipanti alla supply chain. Questo genere di applicazione della blockchain ha il potenziale per trasformare la catena di approvvigionamento dei farmaci in un processo condiviso e trasparente, in un'architettura di *open data* affidabile che possa includere diversi partecipanti e giurisdizioni [34].

Figura 20: Blockchain per il tracciamento dei farmaci. Al momento della loro produzione, viene generato un hash contenente tutte le informazioni sui farmaci. Le informazioni vengono registrate sulla blockchain ad ogni passaggio del farmaco, facilitandone il tracciamento [35].

Un altro esempio nel quale la trasparenza assume grande rilievo è nell'ambito della formazione del personale medico. Negli anni infatti i corsi online, l'educazione basata sui social-media, ma più in generale le piattaforme digitali sono diventati capisaldi della formazione professionale, anche in medicina; ma la struttura di Internet, che ospita queste piattaforme, non permette di tracciare e verificare la fonte del materiale medico condiviso, non garantendo la legittimità del contenuto [36]. Questa mancanza di giudizio non è ammissibile in una disciplina altamente regolamentata come la medicina, perciò si può pensare di sfruttare la blockchain per tracciare i contenuti educativi, definirne la fonte e valutare il percorso formativo del personale medico, pensando di per poter creare in futuro un database contenente le identità digitali degli operatori sanitari, con possibilità di condividere e tracciare le loro credenziali.

3.2.3 Sicurezza

Le informazioni mediche sono dati sensibili. È fondamentale dunque mantenere la sicurezza e la privacy di tutti i dati medici, proteggerli dai sempre maggiori tentativi di violazione. Secondo il dipartimento della salute e dei servizi umani degli Stati Uniti d'America, nel 2015 i dati sanitari di ben 113 milioni di persone sono stati violati, principalmente da server di rete centralizzati (107 milioni) e da cartelle cliniche elettroniche (3 milioni).

La decentralizzazione della blockchain mette al sicuro i dati sanitari dei pazienti da possibili violazioni: le informazioni sono criptate, ed è assolutamente necessaria la chiave crittografica privata per potervi accedere. Questa maggiore sicurezza accresce la fiducia dei pazienti nel sistema e nella blockchain, e questi sono meno restii a partecipare al processo di condivisione dei dati, essenziale per creare un sistema sanitario più efficiente.

3.2.4 Prestazioni

La natura decentralizzata della blockchain consente di evitare la formazione di colli di bottiglia causati dalle continue richieste e risposte della rete. Con l'integrazione della blockchain con l'IoT, si può immaginare la creazione di un ciclo di feedback attivo tra medico e paziente per il monitoraggio in remoto dello stato di salute e/o della terapia seguita, aiutando a ridurre il numero di appuntamenti (Figura 21).

All'interno di una rete blockchain, la decentralizzazione, la trasparenza e il consenso implicano la memorizzazione di tutti i blocchi su ciascun nodo costituente la rete. Con il continuo aumento dei dati sanitari, la scalabilità degli stessi è un'esigenza impellente. Per esempio ad un utente, per poter partecipare alla rete Bitcoin come miner, è richiesto il download dell'intero registro, per un totale di 302,22 gigabyte nel terzo trimestre del 2020 [38], mentre il tasso di convalida delle transazioni oscilla tra 3,3 e 7 transazioni al secondo: ciò risulta in un potenziale collo di bottiglia.

Una potenziale soluzione al problema potrebbe essere la localizzazione di un'ampia raccolta di dati medici esterni alla catena in una *repository* chiamata "*data lake*". Mentre il livello blockchain impone politiche di controllo degli accessi, con tale configurazione il paziente potrebbe ancora tenere traccia di chi ha accesso ai dati personali nel data lake, perché i dati non sarebbero leggibili senza la chiave crittografica, memorizzata sull'account blockchain del paziente (Figura 22).

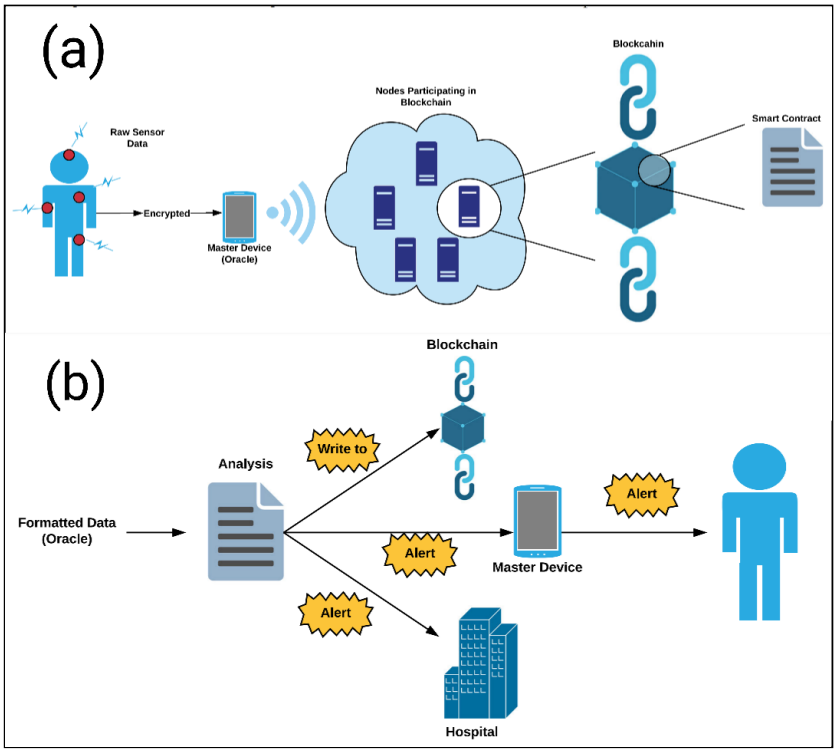

Figura 21: **(a)** Paziente monitorato a distanza da un medico è dotato di vari dispositivi per misurare alcuni parametri vitali. I dati grezzi vengono inviati a un dispositivo principale (smartphone o tablet) per l'aggregazione e la formattazione da parte dell'applicazione. Le informazioni formattate vengono poi inviate allo smart contract specifico per un confronto con i valori di soglia del paziente. **(b)** Lo smart contract valuterà quindi i dati forniti e invierà avvisi sia al paziente che all'operatore sanitario, nonché istruzioni di trattamento automatizzate per i nodi dell'attuatore, se lo si desidera [37].

Figura 22: Dopo la creazione della cartella clinica, contenente i risultati di esami diagnostici, la prescrizione, i dati del monitoraggio, i risultati di test di laboratorio e l'anagrafica di paziente e medico curante, questa viene contrassegnata da una firma digitale. I dati crittografati vengono inviati al data lake dove verranno conservati, mentre la blockchain riceve le coordinate dei dati specifici e l'identificativo del paziente [39].

3.2.5 Usabilità

Le transazioni blockchain sfruttano dei concetti di crittografia sicuramente poco familiari alla maggior parte della popolazione mondiale. Per questo motivo, in un contesto nel quale è il paziente a gestire la condivisione della propria cartella clinica, ad utilizzare le coppie di chiavi crittografiche (pubbliche e private) per le firme digitali e ad autorizzare o meno gli accessi ai propri dati sanitari, spesso si va incontro agli utenti sviluppando delle interfacce software *user-friendly*. Ma nascondere la complessità della gestione delle chiavi crittografiche dietro delle interfacce web o app mobili intuitive può costituire una potenziale minaccia alla sicurezza. Un altro limite dell'*auto-governance* del paziente può emergere nel momento in cui è impossibilitato a rispettare le autorizzazioni di accesso: potrebbe semplicemente perdere le chiavi di accesso personali o essere affetto da patologie gravi come l'Alzheimer. Inoltre, in caso di emergenza, i dati sanitari dovrebbero essere accessibili al personale medico.

3.3 Principali applicazioni blockchain in sanità

In base ai requisiti appena visti, le possibili applicazioni della blockchain in sanità, quelle su cui sono concentrati i maggiori studi, si possono così riassumere:

- **Gestione delle cartelle cliniche elettroniche**: permette gestione e condivisione dei dati sanitari sicure. Una cartella compilata con nomi e codici inequivocabili favorisce un risparmio in termini economici e di tempistiche nella ricerca e nella ricostruzione della storia clinica;

- **Reclami assicurativi**: conferisce maggiore sicurezza nella gestione dei rapporti giuridici tra paziente e strutture sanitarie, nella verifica delle transazioni di risarcimento, di finanziamento dell'assistenza sanitaria e di pre-autorizzazione, oltre a fornire modelli di pagamento alternativi;

- **Ricerca clinica e biomedica**: l'anonimizzazione sicura dei dati sensibili può spingere i pazienti a partecipare e contribuire maggiormente a studi di ricerca;

- **Creazione di un registro avanzato di dati biomedici e sanitari**: oltre che per la gestione dei dati relativi alla cura del paziente, si può pensare a registri per l'archiviazione di dati genomici, dati sull'esito dei trattamenti, sugli studi clinici, sul

consenso del paziente, sulle catene di approvvigionamento dei farmaci oppure sui biomarcatori;

- **Telemedicina**: può migliorare processi di Telemonitoraggio, Teleconsulto o Telechirurgia grazie ad una gestione dei dati sensibili che conferisce un grado di sicurezza contro gli attacchi esterni superiore, oppure stimolando i pazienti ad una maggiore partecipazione ai processi mediante sondaggi e ricompense.

L'ultima categoria sarà oggetto di studio nell'elaborato.

4. Telemedicina

La Telemedicina ricorre a tecnologie innovative per fornire servizi di assistenza sanitaria in contesti nei quali il paziente e il professionista, ma anche due professionisti, sono fisicamente distanti tra loro. Sfrutta le tecnologie di informazione e comunicazione (ICT) per consentire la condivisione sicura dei dati medici in qualsiasi forma digitale, utili per le attività di prevenzione, diagnosi, trattamento e visita. Sebbene possano paragonarsi alle prestazioni sanitarie tradizionali e pur dovendone rispettare tutti i diritti e gli obblighi, i servizi di Telemedicina non le sostituiscono totalmente, ma la loro integrazione garantisce risultati certamente superiori [40].

4.1 Benefici e campi applicativi della Telemedicina

Adottare di sistemi di Telemedicina nel sistema sanitario introduce nuove dinamiche di collaborazione tra pazienti ed operatori sanitari, contribuendo ad un miglioramento delle prestazioni offerte. Tra i giovamenti portati dall'utilizzo di servizi di Telemedicina troviamo:

- **Migliore qualità dell'assistenza**. I parametri dei soggetti particolarmente anziani o affetti da patologie croniche possono essere costantemente monitorati in remoto, consentendo loro di non dover lasciare la propria abitazione;
- **Maggiore copertura**. Sarebbe più agevole prestare assistenza sanitaria a soggetti che vivono in zone difficilmente accessibili o distanti dall'ospedale di riferimento per una particolare visita o esame diagnostico.
- **Maggiore efficacia ed efficienza**. La continua interazione fra i diversi protagonisti di un processo di assistenza sanitaria aiuta a ridurre i rischi legati ad eventuali complicazioni, il numero di ricoveri e i tempi di attesa, ottimizzando così l'uso delle risorse a disposizione.
- **Abbattimento dei costi**. L'ottimizzazione delle risorse porta come prima conseguenza una razionalizzazione dei processi socio-sanitari, consentendo un importante abbassamento delle spese.

La Telemedicina promette quindi di migliorare sensibilmente i processi di prevenzione secondaria, diagnosi, cura, riabilitazione e di monitoraggio. È possibile classificare i servizi di Telemedicina in tre principali categorie, ciascuna delle quali, a seconda del tipo di relazioni

che intercorrono tra gli attori coinvolti, possono essere erogate in differenti modalità (Tabella 3). Nello specifico si parla di:

- **Telemedicina specialistica**: insieme delle modalità di erogazione dei servizi nell'ambito di una disciplina ben precisa (la Telecardiologia o la Teledermatologia ad esempio);
- **Telesalute**: permette di responsabilizzare il paziente nei processi di prelievo e monitoraggio, sempre con il supporto del medico che interpreta i dati ricevuti da un caregiver o dal paziente stesso;
- **Tele assistenza**: grazie a sistemi di emergenza e di allarme, offre assistenza domiciliare a pazienti fragili o anziani.

<table>
<tr><th colspan="2">Classificazione</th><th>Ambito</th><th colspan="2">Paziente</th><th>Relazione</th></tr>
<tr><td rowspan="3">Telemedicina specialistica</td><td>Tele visita</td><td rowspan="3">Sanitario</td><td rowspan="3">Con patologie croniche, acute, post-acuzie</td><td>Presente attivamente</td><td>B2C, B2B2C</td></tr>
<tr><td>Teleconsulto</td><td>Assente</td><td>B2B</td></tr>
<tr><td>Tele cooperazione sanitaria</td><td>Presente real-time</td><td>B2B2C</td></tr>
<tr><td colspan="2">Telesalute</td><td>Sanitario</td><td>Con patologie croniche</td><td>Presente attivamente</td><td>B2C, B2B2C</td></tr>
<tr><td colspan="2">Tele assistenza</td><td>Socio-assistenziale</td><td colspan="2">Anziano fragile o disabile</td><td></td></tr>
</table>

Tabella 3: Classificazione dei servizi di Telemedicina. Nell'ambito delle relazioni: **B2B** - Business to Business (relazione tra medici); **B2C** - Business to Consumer (relazione tra medico e paziente); **B2B2C** - Business to Business to Consumer (relazione tra medico e paziente mediata da un operatore sanitario) [40].

4.2 Possibili criticità

Il concetto di Telemedicina è stato dunque sviluppato per fornire assistenza sanitaria in maniera più efficiente e ad un costo minore, e sta crescendo sempre di più soprattutto in termini di studi di fattibilità e prove pilota. Secondo un recente rapporto di ricerca, il mercato della Telemedicina è stato valutato a 29,6 miliardi di dollari nel 2017, e si prevede una crescita ad un tasso annuo di circa il 19% nel periodo 2017-2022 [41]. È probabile che la crescita di questo mercato sia guidata dall'aumento dell'incidenza di malattie croniche e della popolazione geriatrica, dalle iniziative governative e dalla carenza di medici, tra gli altri.

Ciò nonostante, il numero di visite di Telemedicina negli ospedali è ancora basso rispetto al numero di visite individuali: alla crescita di popolarità della Telemedicina infatti si affianca il rischio di incappare in criticità associate all'applicazione dei servizi, problemi di cui operatori sanitari, compagnie assicurative ed agenzie di regolamentazione governative devono tener conto. Queste problematiche potrebbero portare a reclami, perciò occorre tenerne conto durante la progettazione di un sistema di Telemedicina [42] [43]. Più precisamente:

- **Posizione**. Nonostante lo sviluppo tecnologico consenta oggi di stabilire corrispondenza e contatti da ogni parte del pianeta, non sono state ancora definite delle linee guida a supporto dei medici che offrono consulti e cure virtuali in tutto il mondo. Il paziente in genere riceve assistenza nel proprio Paese, secondo le leggi e le linee guida di quel Paese. Non esiste una struttura univoca a livello internazionale che consenta ai professionisti di poter assistere i propri pazienti in altre zone del mondo.

- **Interoperabilità**. Problema tipico nell'industria farmaceutica. L'interoperabilità dei servizi farmaceutici rappresenta una necessità per i fornitori di servizi sanitari, gli assicuratori e i pazienti. Problemi di riconoscimento dei pazienti e il blocco delle informazioni rientrano tra le conseguenze di una interoperabilità deficitaria.

- **Negligenza**. I casi di negligenza terapeutica sono imprevedibili, e possono ripercuotersi sulla salute del paziente o nella corrispondenza tra medico e paziente. L'utilizzo della Telemedicina può acuire questa problematica, poiché eventuali stop nell'innovazione tecnologica potrebbero portare a denunce per negligenza.

- **Standard di cura**. La diagnosi e il protocollo di cura per ciascun paziente differirà tra un professionista sanitario e l'altro. Esistono regolamentazioni sullo standard di cura da fornire al paziente, ma variano per ciascun fornitore di assistenza sanitaria.

- **Violazione dei dati**. Come già visto con i Ransomware, il rischio di violazione dei dati è elevato in ambiente informatico. Dati molto importanti e sensibili come quelli sanitari necessitano di un alto grado di protezione, per evitare che i pazienti possano cadere vittime di hacker e truffatori.

- **Diagnosi errate**. Un esame svolto con Telemedicina non è affatto simile ad uno tradizionale svolto in ospedale o in uno studio medico. Ad esempio, un paziente invia al medico una fotografia relativa ad un problema fisico, come un'eruzione cutanea.

Un'immagine distorta, di scarsa qualità o senza adeguata illuminazione potrebbe portare ad una diagnosi errata. In questi casi, il medico è responsabile.

- **Abusi e frode**. C'è una maggiore necessità per il paziente di confermare le credenziali del medico professionista, per non incorrere nel rischio di abuso virtuale. È necessario sviluppare standard e linee guida sulla Telemedicina affinché i medici possano fornire consigli ai pazienti in totale sicurezza.

4.3 Blockchain nella Telemedicina

Telemedicina e blockchain condividono l'idea comune sull'importanza di responsabilizzare il consumatore, fornendo autonomia ai pazienti nel determinare i servizi o i processi ai quali sono disposti a partecipare, e di porre maggiore enfasi su una razionalizzazione dei processi per i fornitori dei servizi sanitari.

Tra le possibili criticità della Telemedicina tradizionale menzionate nel precedente paragrafo c'è il rischio di una possibile violazione dei dati, e quindi della privacy del paziente. I sistemi centralizzati sono infatti vulnerabili agli attacchi esterni di hacker e utenti malintenzionati verso i registri contenenti dati sanitari. Per questo tra pazienti e operatori è cresciuto un sentimento di sfiducia nei confronti dei servizi di Telemedicina, portandoli a preferire molto spesso i metodi tradizionali. Con le caratteristiche immutabili e anonime della blockchain, i pazienti possono sentirsi liberi da preoccupazioni sulla privacy. L'uso della blockchain in Telemedicina contribuirà ad aumentare la fiducia dei consumatori verso sé stessi e verso i sistemi.

La Tabella 4 mostra come le differenze tra un sistema sanitario tradizionale, uno di Telemedicina centralizzato ed uno di Telemedicina basato sulla tecnologia blockchain.

	Tradizionale	Telemedicina centralizzato	Telemedicina con blockchain
Costi	Alti	Bassi	Bassi
Tempi di attesa	Elevati	Ridotti	Ridotti
Tolleranza ai guasti	Assente	Assente	Presente
Necessità visite in presenza	Sì	No	No
Origine dati	Sconosciuta	Sconosciuta	Certa
Cartelle cliniche manipolabili	Sì	Sì	No
Documentazione	Sì	Sì	No
Gestione del sistema	Centralizzata	Centralizzata	Decentralizzata
Audit trial	No	No	Sì
Sicurezza e privatezza dei dati	Complicata	Complicata	Semplice
Trasparenza	No	No	Sì
Affidabilità e integrità	Scarsa	Scarsa	Alta

Tabella 4: Principali differenze tra sistemi sanitari tradizionali e quelli che sfruttano sistemi di Telemedicina. Decentrare un sistema di Telemedicina integrandolo con la tecnologia blockchain garantirebbe maggiore tolleranza ai guasti e agli attacchi esterni, mettendo al sicuro i dati e le cartelle cliniche dei pazienti [44].

5. Sistemi di Telemedicina basati su blockchain

In questo capitolo vengono illustrati alcuni dei più recenti sistemi di Telemedicina basati sulla tecnologia blockchain. L'obiettivo principale che questi sistemi si pongono è quello di efficientare servizi già esistenti, con un'attenzione particolare rivolta ad una gestione e condivisione più sicura dei dati sensibili.

DermoNet [45], sviluppato in Italia, offre un servizio di Teledermatologia a supporto sia del paziente che può richiedere una diagnosi da casa, sia degli specialisti che possono condividere e consultare più casi clinici.

HapiChain [46], integrando un servizio di Telemonitoraggio preesistente, *Hapicare* [47], offre Teleconsulto sicuro per pazienti anziani o affetti da patologie croniche sfruttando la blockchain Ethereum e gli smart contract.

Nel 2019 *SHAREChain* [48], sfruttando gli standard *Fast Healthcare Interoperability* (FHIR) e *Cross Enterprise Document Sharing* (XDS), ha proposto un nuovo design di blockchain Consortium per la gestione sicura delle cartelle cliniche elettroniche dei pazienti.

AaYusH [49] sfrutta la connessione su rete 5G ad alta velocità e bassa latenza per garantire operazioni di Telechirurgia efficaci. Inoltre introduce un sistema di feedback per i pazienti, che recensiscono i chirurghi creando un vero e proprio ranking al quale futuri pazienti possono affidarsi nella scelta dello specialista.

Il quinto sistema approfondito introduce la tecnologia blockchain in un sistema ibrido di autenticazione biometrica basato sul riconoscimento del pattern venoso (*Finger Vein*) [50]. La tecnologia blockchain, combinata con la steganografia, mette al sicuro i dati relativi alla fisionomia venosa del paziente e li conserva poi su registri distribuiti.

Garg et al, in collaborazione con l'Alfaisal University e l'Università di Malta, hanno proposto un sistema di *contact tracing* per contenere la recente pandemia COVID-19, basato sull'utilizzo di tag per l'identificazione a radiofrequenza (RFID) e della tecnologia blockchain per la raccolta anonima dei dati [51].

La descrizione dell'architettura e del funzionamento dei sistemi sopra riportati è accompagnata da esempi di utilizzo e dall'analisi delle performance, tenendo conto dei limiti e di possibili miglioramenti.

5.1 DermoNet

Il progetto *DermoNet* è stato finanziato dalla Regione Sardegna con l'obiettivo di sviluppare un modello di organizzazione virtuale per finalità di Teledermatologia disegnando, sviluppando e validando una piattaforma software basata su tecnologia cloud, al fine di creare una rete che coinvolga pazienti, medici di famiglia, dermatologi e istituzioni sanitarie, supportando i medici durante la valutazione dei pazienti dermatologici [45]. In origine, il progetto DermoNet è stato implementato come un sistema informativo basato su cloud con risorse ridimensionate e utilizzate su Internet al fine di migliorare i servizi sanitari; successivamente si è proposto come strumento per il Teleconsulto dermatologico, in particolare nelle zone meno servite della Sardegna. Il servizio di consulenza offerto consente la diagnosi e la gestione dei pazienti con malattie della pelle da parte di medici di base o dermatologi. Ogni paziente può contattare il proprio medico di famiglia per problemi di dermatologia senza la necessità di rivolgersi fisicamente ad uno specialista, fornendo vantaggi in termini di tempo e costi. Il sistema può fornire risposte su alcune gravi malattie dermatologiche come il melanoma attraverso un'organizzazione virtuale (VO), una nuova forma di organizzazione resa possibile dall'uso dei servizi online. Infatti nelle VO i medici che lavorano in luoghi fisicamente distanti possono accedere alle stesse risorse collaborative sul web e i medici di medicina generale possono quindi avvalersi del Teleconsulto. Possono offrire soluzioni a diversi problemi dermatologici in modo tempestivo e le caratteristiche principali delle VO, come la rapida formazione della comunità e del personale coinvolto e l'assenza di impegni a lungo termine [52], rendono questo approccio utile negli ambienti sanitari in caso di emergenza, o per la diagnosi rapida della malattia. DermoNet è una piattaforma di Teledermatologia basata su blockchain: attraverso un sistema decentralizzato il paziente può accedere in autonomia ai propri dati e richiedere un consulto a uno specialista senza assistenza medica di base o ospedaliera.

5.1.1 Descrizione

Il sistema DermoNet è un prototipo preindustriale di piattaforma software collaborativa, per servizi orientati a supportare la gestione dei pazienti dermatologici e il processo di diagnosi da parte di medici e specialisti che lavorano insieme nella VO. I requisiti di interoperabilità del software, insieme ai requisiti di progettazione specifici della funzionalità dermatologica, sottolineano l'importanza di una base di conoscenza ben definita. Per gestire le informazioni,

come il recupero dei documenti utilizzando parole chiave o significato, il sistema si basa su tre diverse basi di conoscenza (*Knowledge bases*, KBs):

1. $\mathbf{KB}_{GL}$: relative alle linee guida per i dermatologi. Le linee guida contengono raccomandazioni sul comportamento clinico con l'obiettivo di aiutare i medici a scegliere l'approccio più appropriato dal punto di vista medico;
2. $\mathbf{KB}_{I}$: relative a tutte le immagini disponibili nell'Atlante dermatologico;
3. $\mathbf{KB}_{CE}$: relative alle competenze dei dermatologi che operano nei centri competenti e che forniscono servizi di Teleconsulto.

Grazie alle KB si ottengono due importanti funzionalità, ovvero la condivisione dei dati e il data linking. Il sistema software può fornire una ricerca di documenti e informazioni basata sul contenuto che funziona tenendo conto del significato dei termini di ricerca. Il portale DermoNet è raggiungibile tramite un client web ed è sviluppato in modo da essere completamente reattivo e in grado di funzionare su dispositivi mobili come tablet e smartphone. Gli utenti accedono al sistema attraverso una pagina di login con una OTP (*one-time password*), mentre il menu principale del sistema è composto da un elenco di funzionalità che dipendono dalla tipologia di utente (es. medico di base, dermatologo specialista, tutor, segretaria). Un account speciale, che fornisce l'accesso alle pagine di configurazione, è abilitato per l'amministrazione del sistema. Le voci del menu principale:

- **Componenti Staff**: apre la pagina di creazione del team. È possibile scegliere dalla lista degli utenti DermoNet filtrando per categoria, area di competenza e reparto;
- **Modello Questionario**: il medico di base può scrivere questionari personalizzati e interattivi, che sulla base delle risposte del paziente mostreranno diverse sequenze di domande;
- **Pazienti**: agli utenti accreditati, come tutor o segretaria, è fornito un modulo con cui è possibile aggiungere e modificare le informazioni sul paziente;
- **Cartella clinica**: per ogni paziente il sistema visualizza un modulo in cui sono evidenziati il nome del paziente, il medico di base, gli specialisti in dermatologia e fornisce l'elenco dei piani di trattamento e delle annotazioni terapeutiche (Figura 23);
- **Appuntamenti**;
- **Linee guida e protocolli**;
- **Reports**;

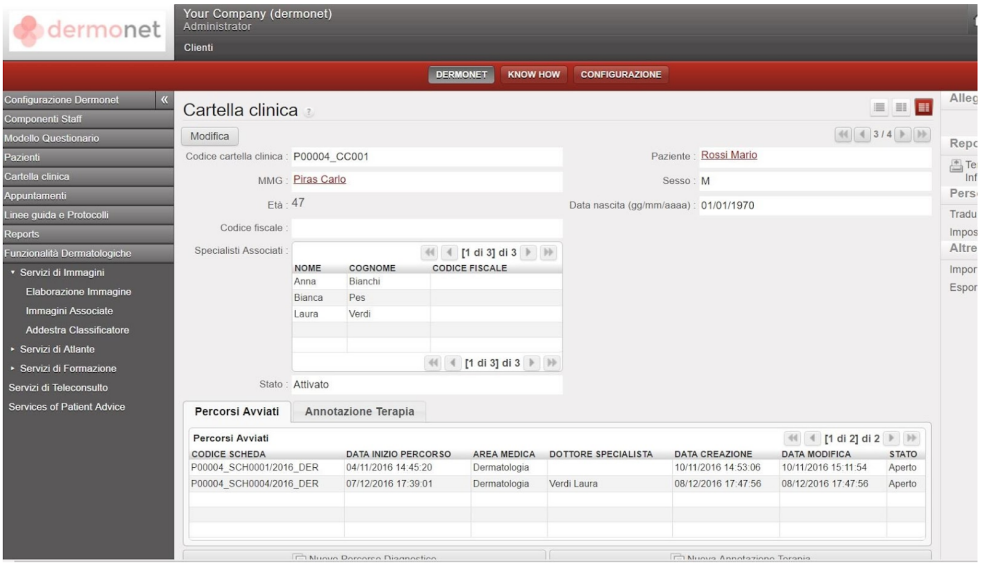

Figura 23: Cartella clinica del paziente [45].

- **Funzionalità dermatologiche**: apre la sezione dermatologica in cui sono fornite tutte le funzionalità del sistema dedicate alla Teledermatologia. Nello specifico:

  - *Servizi di immagine*. DermoNet fornisce un sistema automatico di analisi e annotazione per immagini dermatologiche, annotazione semantica di classificazione e probabilità di diagnosi sulla base delle KB_I (Figura 24).

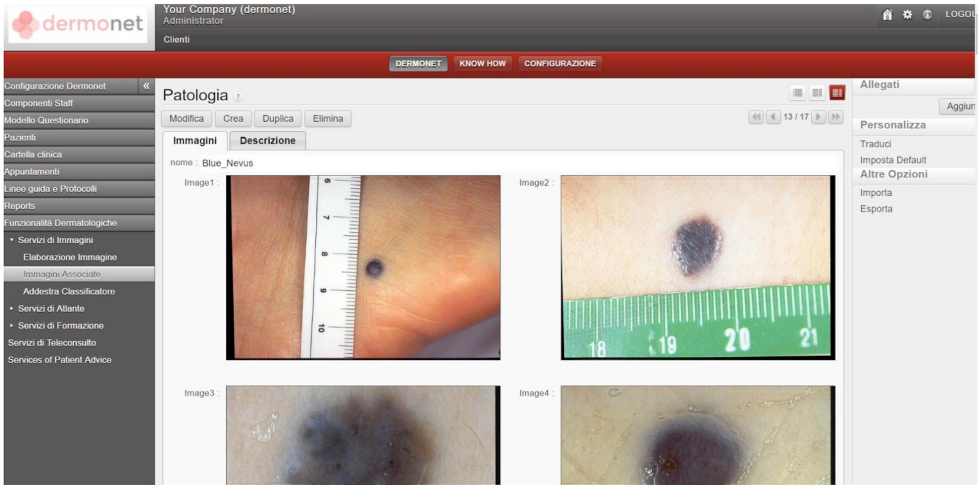

Figura 24: Immagini di disturbi della pelle [45].

  - *Servizi guida*. Consentono ai dermatologi di consultare e ricevere aggiornamenti sulla diagnosi e sulla terapia utilizzando le KB delle linee guida e contengono raccomandazioni e consigli sul comportamento clinico per aiutare i medici a scegliere l'assistenza più appropriata.

- *Servizi di Atlante*. Fornisce servizi per catalogare e condividere dati dermatologici specialistici basandosi sulle KB_I.

- *Servizi di Teleconsulto*. DermoNet fornisce un ambiente per il Teleconsulto, facilitato dalle KB_{CE}. Fornisce i dati e la terminologia necessari per evitare malintesi durante la comunicazione tra il medico di base e lo specialista.

Gli attori coinvolti nel sistema di Telemedicina DermoNet sono il paziente, che necessita di consulti dermatologici, lo specialista, che mette a disposizione la sua esperienza, e i membri della comunità medica possono accedere a dati decentralizzati per attività di ricerca come le sperimentazioni cliniche. Per interagire con il sistema è necessaria una registrazione e per ogni attore viene creato e registrato all'interno degli smart contract un identificatore (come un indirizzo blockchain). Nel sistema decentralizzato le operazioni dei partecipanti (accesso, comunicazione e autorizzazioni) sono gestite dall'intero sistema di rete tramite l'applicazione decentralizzata in esecuzione nella blockchain, che rende il paziente libero di utilizzare il sistema in modo autonomo. Ogni partecipante ha un ruolo e un tipo di accesso diverso, mentre tutte le operazioni e le comunicazioni tra gli attori e la piattaforma sono gestite dagli smart contract a seconda dei loro profili. Tutte queste operazioni sono trasparenti per l'utente che accede al sistema utilizzando un'app mobile o un'applicazione software.

Un paziente può richiedere un consulto dermatologico inviando una foto e tutti i dati di supporto per una diagnosi. Tutte le informazioni inviate al sistema, che richiede una tariffa per il pagamento del medico e della gestione del caso, vengono protette da crittografia e solo lo specialista può decifrarle. Il paziente ha il controllo sui propri dati, può accedere alla sua storia clinica e anche condividerla per motivi di ricerca.

I medici possono registrarsi al sistema pagando una tariffa e caricando le proprie credenziali come licenze mediche, titoli di studio e documenti di certificazione, verificabili da qualsiasi utente all'interno della rete membro di un comitato di verifica, che riceve un bonus per ogni voto di verifica concesso. Il sistema blockchain mostra allo specialista un elenco di pazienti; scelto un caso, può visualizzare i dati del paziente per caricare una diagnosi all'interno del sistema. Il medico riceve il pagamento non appena il paziente invia la conferma di ricezione dei dati. DermoNet presenta anche un servizio di valutazione con il quale pazienti e sistema recensiscono i medici. In Figura 25 sono riportati tre casi d'uso di DermoNet.

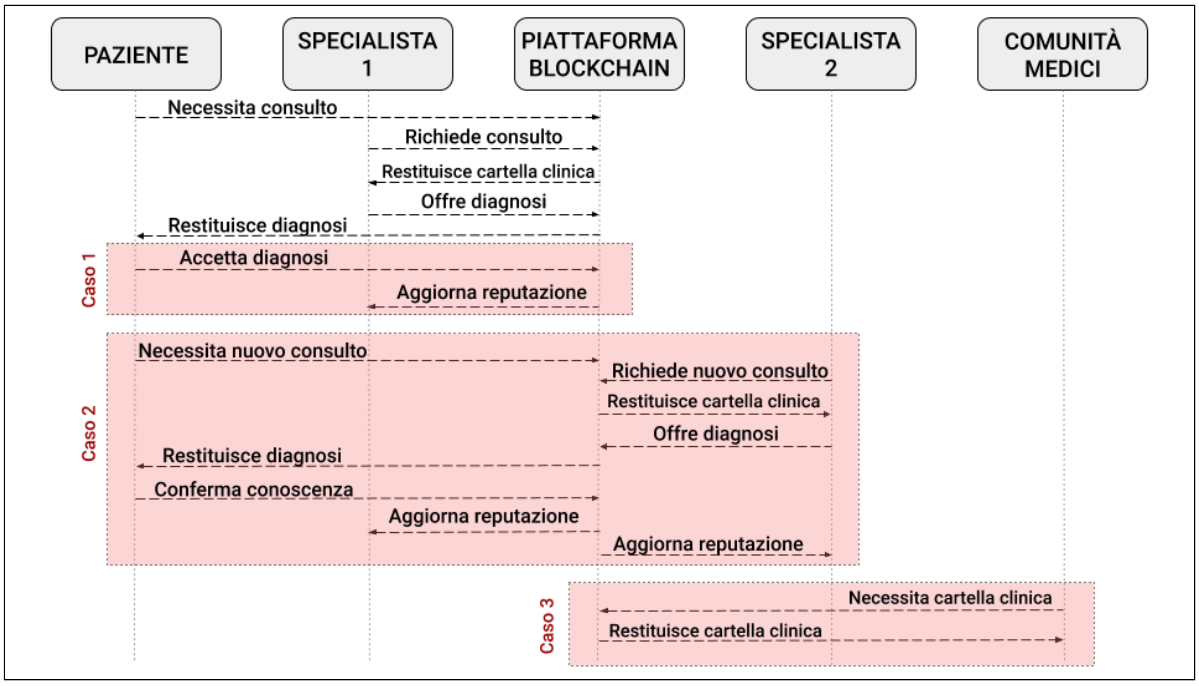

Figura 25: **(1)** Il paziente richiede un consulto e Specialista 1 fornisce la diagnosi. Quando il paziente la riceve, può accettare la risposta e valutare il medico. **(2)** Il paziente può richiedere un consulto supplementare: il sistema richiede un costo aggiuntivo e la valutazione è assegnata a Specialista 2. Supponendo che abbia una valutazione superiore rispetto a Specialista 1, al paziente viene rimborsato il primo consulto in caso di diagnosi differente e Specialista 1 non riceve alcun compenso. Se la diagnosi è la stessa, Specialista 1 riceve soldi e una buona valutazione, Specialista 2 un bonus. **(3)** Un membro della comunità medica può richiedere dati medici per condurre attività di ricerca. I dati sensibili sono protetti, ma in caso di consenso sono accessibili e condivisibili [45].

L'intero sistema è diviso in quattro livelli:

- **Livello Blockchain**. Ha il doppio ruolo di canale di comunicazione e framework. Viene adottata la blockchain Ethereum perché fornisce una piattaforma decentralizzata per le applicazioni, in cui è possibile implementare il livello DApp ed eseguire smart contract. La piattaforma e-Health utilizza la blockchain come canale di comunicazione tra le applicazioni decentralizzate. I messaggi tra le DApp sono strutturati come transazioni Ethereum. I dati blockchain sono disponibili al pubblico e, al fine di proteggere la privacy dei pazienti, ogni transazione contiene richieste o dati in forma crittografata, secondo le specifiche del livello API.
- **Livello DApp**. Insieme di applicazioni decentralizzate in esecuzione all'interno della blockchain, che gestiscono e controllano automaticamente l'intera serie di operazioni e il sistema di comunicazione, senza intermediari come i medici di base. Prendono i messaggi crittografati provenienti dal livello API gestendoli come transazioni Ethereum. Questo livello include smart contract che gestiscono le transazioni all'interno della blockchain, comprese le autorizzazioni dei dati medici e il sistema di

reputazione dei dermatologi. Inoltre, questo livello include il controllo del database decentralizzato in cui sono archiviate le cartelle cliniche (comprese le foto della pelle, ecc.).

- **Livello API**. Rappresenta i protocolli e l'elaborazione delle informazioni che consentono un flusso di informazioni sicuro e protetto tra il livello dell'interfaccia e il livello DApp. Consente l'interazione tra le interfacce *user-oriented* e i servizi di livello inferiore che diventano trasparenti per gli utenti. Include il protocollo di crittografia che gestisce e protegge l'accesso ai dati. Le informazioni per ciascuna richiesta del paziente vengono codificate utilizzando la crittografia simmetrica e quindi la stessa chiave crittografica viene utilizzata sia per cifrare che per decifrare i dati. Inoltre, il livello API fornisce le regole per la composizione dei messaggi che verranno inviati e ricevuti dagli attori nel sistema.
- **Livello interfaccia**. Livello più alto del sistema che consente l'interazione con l'utente. Include applicazioni mobili e desktop e implementa interfacce utente per ciascuna funzionalità. Le interfacce sono diverse a seconda dell'attore coinvolto, in quanto pazienti, medici e membri della comunità di ricerca hanno esigenze diverse. Le applicazioni del livello interfaccia forniscono funzionalità di login e registrazione degli utenti, tramite l'attivazione del sistema di autorizzazione nel livello DApp. Le richieste degli utenti e le informazioni mediche vengono trasmesse da e verso il sistema decentralizzato secondo le specifiche del livello API.

5.1.2 Conclusioni

L'utilizzo della blockchain fornisce un sistema decentralizzato che consente il pieno controllo dei dati del paziente con la garanzia di sicurezza, trasparenza e immutabilità che un sistema centralizzato non può garantire. Questa piattaforma può anche fornire un sistema globale di cartelle cliniche elettroniche in cui i dati saranno disponibili per scopi di ricerca, insegnamento o lavori clinici. Ogni attore coinvolto in questo sistema ha un account nella blockchain Ethereum che può essere identificato da un indirizzo. L'indirizzo è univoco per ogni utente che ha la propria coppia di chiavi private / pubbliche. Il login e l'utilizzo dei servizi sono gestiti da apposito smart contract in base al profilo dell'utente.

Grazie all'implementazione della blockchain in DermoNet le cartelle cliniche sono sempre a portata di mano, in questo modo i medici sono costantemente aggiornati sull'evoluzione del disturbo dermatologico. Ogni evento o transazione è contrassegnato da una data e una

marcatura temporale, mentre la gestione della cartella clinica avviene solo previa autenticazione mediante gli smart contract: le informazioni sul paziente e la terapia sono quindi condivise in modo sicuro. L'uso del sistema decentralizzato consente quindi un aumento della qualità delle cure offerte, unito ad un abbattimento dei costi grazie alla possibilità di condivisione immediata dei dati con altri medici o istituzioni. Questo scambio di dati è protetto crittograficamente tramite *Keyless Signature Infrastructure* (KSI), rendendo il processo di gestione uniforme e trasparente. La collaborazione tra pazienti, ricercatori e medici consente un maggior grado di scambio e confronto, portando a percorsi assistenziali specifici e personalizzati. La tecnologia blockchain risolve i problemi di archiviazione e disponibilità di immagini dermatologiche, consentendo un rapido accesso alle informazioni e un'interpretazione tempestiva degli studi di imaging dermatologico. Inoltre risolve il problema relativo al trasferimento dei dati di immagine su supporto cartaceo o ottico. Infine le prestazioni vengono memorizzate in modo permanente: è quindi possibile limitare le frodi sanitarie automatizzando l'elaborazione di ticket e fatture e riducendo così i costi amministrativi.

Sebbene i vantaggi apportati dall'implementazione della blockchain in DermoNet in termini di efficienza, costi, interoperabilità, automazione, sicurezza e integrità dei dati siano evidenti, va tenuto conto anche delle controindicazioni. L'attuale letteratura sulla blockchain non è vastissima: c'è carenza di forum o white-paper per quanto riguarda la documentazione di standard o linee guida per progettare o implementare questo tipo di sistemi, di feedback sul suo utilizzo e mancano veri e propri standard sull'integrazione con altri sistemi. Ogni transazione all'interno della blockchain deve essere verificata e convalidata, richiedendo un calcolo ad alta potenza. Infine va tenuto conto dei limiti etici e culturali: è difficile cambiare le abitudini delle persone e inoltre, a causa della burocrazia coinvolta, il settore sanitario non è ancora pronto per l'introduzione di una tecnologia così dirompente.

5.2 HapiChain

HapiChain è un framework basato sulla tecnologia blockchain pensato per migliorare la sicurezza, la scalabilità e l'abilità dei flussi di lavoro medici, realizzato dai francesi di Maidis. Sebbene sia un sistema pensato per il paziente, HapiChain è di supporto al personale sanitario consentendo di risparmiare tempo ed evitare spostamenti non necessari. In HapiChain sono stati incorporati due servizi di Telemedicina: Telemonitoraggio attraverso un software preesistente, *Hapicare*, che utilizza il ragionamento probabilistico per il coaching auto-adattivo, completato da un servizio di Teleconsulto introdotto grazie alla blockchain.

Hapicare è un sistema di monitoraggio rivolto agli anziani e ai pazienti con malattie croniche per aiutarli a condurre una vita sana in maniera autonoma. Hapicare sfrutta un ragionamento su base ontologica per integrare le letture dei segnali vitali con informazioni contestuali. Queste insieme ai dati raccolti dai sensori, vengono successivamente elaborate per effettuare le diagnosi ed individuare il trattamento più adeguato. In caso di gravi condizioni di salute è consigliato un consulto medico, inoltre Hapicare invita anziani e pazienti affetti da patologie croniche a sottoporsi a visite periodiche per verificare le condizioni di salute e lo stato del trattamento [47].

5.2.1 Descrizione

HapiChain propone un sistema di Teleconsulto integrandosi con Hapicare, includendo gli aspetti più tradizionali del consulto medico come la gestione delle prenotazioni, le misurazioni e le prescrizioni, ma ridefinendo le regole di Hapicare stesso a seconda della diagnosi. Lo schema di HapiChain comprende tre livelli principali:

1. **Livello interfaccia**, nel quale Hapicare viene sfruttato per comunicare con gli utenti, cioè medici e pazienti;
2. **Livello DApp**, che include le procedure richieste per la sicurezza e la scalabilità di HapiChain, ovvero gli smart contract e lo storage distribuito. Quest'ultimo si ottiene utilizzando *InterPlanetary File System* (IPFS);
3. **Livello blockchain**, dove viene adottata Ethereum, scelta per la semplicità e la modularità fornita nello sviluppo di applicazioni distribuite (DApps).

In Figura 26 è rappresentata una panoramica della struttura di HapiChain. Gli smart contract costituiscono il *core* di HapiChain: contengono codici Solidity per consentire l'accesso allo spazio di archiviazione e assicurare il flusso di lavoro. In HapiChain sono due i ruoli fondamentali: l'utente, che include il medico, il paziente ed il sistema Hapicare, e gli amministratori che configurano HapiChain.

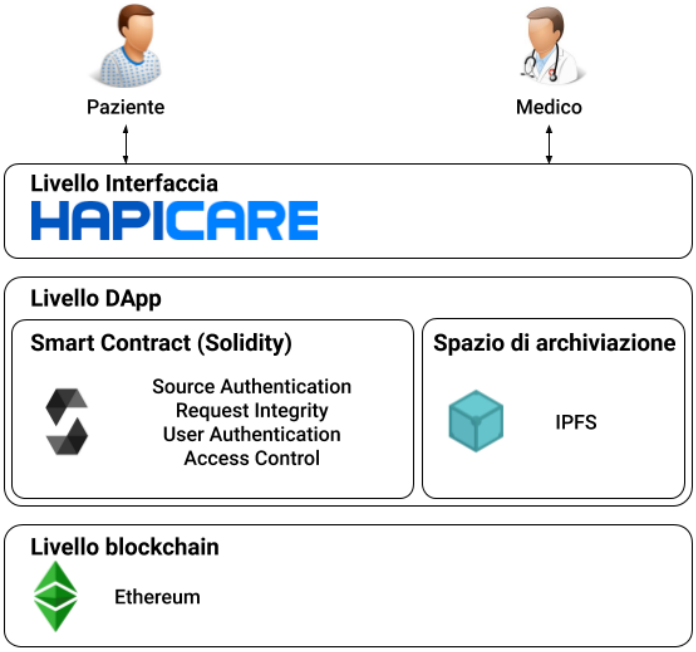

Figura 26: Rappresentazione della struttura di HapiChain [46].

Gli smart contract di HapiChain possono essere classificati nelle seguenti categorie:

- *Source Authentication*: HapiChain è progettato per essere utilizzato tramite un livello di interfaccia dedicato; quindi, al fine di evitare eventuali richieste non autorizzate, è fondamentale consentire richieste solo a sorgenti predefinite. Nella piattaforma Ethereum non è fissato un numero limite di esecuzioni, quindi, per evitare richieste da fonti non autorizzate, questo dovrebbe essere programmato esplicitamente. L'amministratore di HapiChain è l'unico soggetto in grado di autorizzare una richiesta; in questo caso viene utilizzato Hapicare a livello interfaccia, per cui HapiChain ignorerà ogni eventuale richiesta che non provenga da Hapicare.

- *Request Integrity*: HapiChain deve assicurarsi che la richiesta ricevuta sia autentica, che provenga dalla fonte autorizzata e che non sia stata manomessa (ad esempio che l'identificativo del medico o del paziente non sia stato modificato nella richiesta). Questa convalida dell'integrità si ottiene utilizzando le firme digitali. In Hapicare, i parametri della richiesta vengono sottoposti ad hashing prima della trasmissione, poi

in HapiChain il valore hash viene nuovamente calcolato e confrontato con l'hash fornito. In caso di manomissione, i valori hash non corrisponderanno e HapiChain annullerà la richiesta.

- *User Authentication*: Prima del controllo degli accessi, è fondamentale garantire l'identità dell'utente; quindi l'utente di Hapicare viene identificato e autenticato in questa serie di smart contract. Nel momento in cui un medico accede alla sua applicazione, Hapicare esegue l'autenticazione iniziale. In HapiChain, prima di elaborare le richieste del medico, la sua identità viene ricercata all'interno di una lista per assicurarsi che sia registrato al servizio. L'amministratore HapiChain può aggiornare questo elenco o delegare all'amministratore Hapicare.

- *Access Control*: Le cartelle cliniche sono le informazioni più delicate nel sistema sanitario. Pertanto, una serie di codici *Solidity* è dedicata a garantire la riservatezza e anche l'integrità delle cartelle cliniche. Il controllo degli accessi può essere personalizzato per ogni paziente, e generalmente i codici di controllo sono classificati in due sottocategorie in base all'operazione da svolgere:

    - Lettura della cartella: Hapicare utilizza costantemente una cartella clinica per la diagnosi durante il Telemonitoraggio; tuttavia, potrebbe non essere necessario accedere a tutte le cartelle. Inoltre, durante un Teleconsulto, un medico deve poter accedere all'intera documentazione clinica del paziente.
    - Modifica della cartella: ad esempio, la modifica della cartella clinica di un paziente potrebbe essere limitata al caregiver solamente ad orari stabiliti.

  Il controllo dinamico degli accessi è uno dei valori aggiunti di HapiChain. Per l'implementazione dei controlli di accesso riguardanti la lettura e la modifica di cartelle cliniche, in HapiChain viene definita una mappatura da un numero identificativo dell'entità e dall'elenco delle richieste consentite. Prima di ogni richiesta, l'entità e la richiesta vengono verificate utilizzando questa mappatura. La richiesta, nel caso più semplice, contiene il numero identificativo del paziente, il tipo di cartella clinica (monitoraggio o consultazione), il tipo di richiesta (lettura o modifica) e il periodo di accesso. Ad esempio, per il Telemonitoraggio, il sistema Hapicare può accedere solamente alle cartelle cliniche di monitoraggio di tutti i pazienti per un tempo infinito. Gli amministratori di Hapicare possono definire questi controlli di accesso.

A volte le cartelle cliniche possono raggiungere dimensioni davvero importanti, rendendo impossibile una loro archiviazione nella blockchain; per garantire una migliore scalabilità a volte può essere utile ricorrere al protocollo IPFS per l'archiviazione [53]. Inoltre per garantire la riservatezza e la privacy dei dati, questi vengono anonimizzati e crittografati prima dell'archiviazione. Una volta verificata dagli smart contract l'autorizzazione alla richiesta di "modifica", IPFS memorizzerà i nuovi dati in un nodo di archiviazione, conservando l'indirizzo per accessi futuri. A meno che Hapicare non abbia esplicitamente etichettato i nuovi dati come "monitoraggio", questi saranno di "consultazione". Il sistema Hapicare viene utilizzato come interfaccia per la comunicazione con medici e pazienti, e questo livello interagisce con gli smart contract tramite le API (*Application Programming Interfaces*) fornite.

5.2.2 Caso d'uso

Si immagini un paziente maschio di 70 anni, non fumatore, con un peso normale e un background familiare con patologie cardiovascolari, a cui sono stati diagnosticati diabete mellito di tipo 2 e malattie cardiovascolari. Assume due dosi di insulina prima di ogni pasto e utilizza Hapicare per il Telemonitoraggio: i parametri vitali (frequenza cardiaca, passi e temperatura corporea) vengono rilevati e trasmessi online grazie ad uno smartwatch, mentre i sensori ambientali forniscono informazioni su luminosità e temperatura ambientale. Utilizzando le informazioni esistenti e le azioni di rilevamento, Hapicare diagnostica al paziente una ipoglicemia, consigliando l'assunzione di carboidrati. Tuttavia, se l'ipoglicemia si presenta come una situazione ricorrente significa che l'assunzione di insulina non è adatta allo stile di vita del paziente, ma un'eventuale modifica dei dosaggi rappresenta una decisione delicata. Per questo Hapicare suggerisce al paziente un Teleconsulto.

Il medico fornisce al paziente una lista di fasce orarie per il Teleconsulto, prenotabile attraverso l'interfaccia Hapicare. Una volta unitosi alla sala d'attesa virtuale attende che il medico, il quale può vedere i pazienti in attesa con relative informazioni anagrafiche e sullo stato di salute, dia inizio alla sessione di consultazione. Nello specifico caso d'uso, il paziente (Mr Jack) ha richiesto un Teleconsulto per "Diagnosi ricorrente di ipoglicemia", ha 70 anni e la sua condizione cronica è il diabete mellito di tipo 2, diagnosticato il 02/10/2019. Queste informazioni consentono al medico di poter preparare al meglio il consulto mentre il paziente attende nella sala d'attesa virtuale (Figura 27).

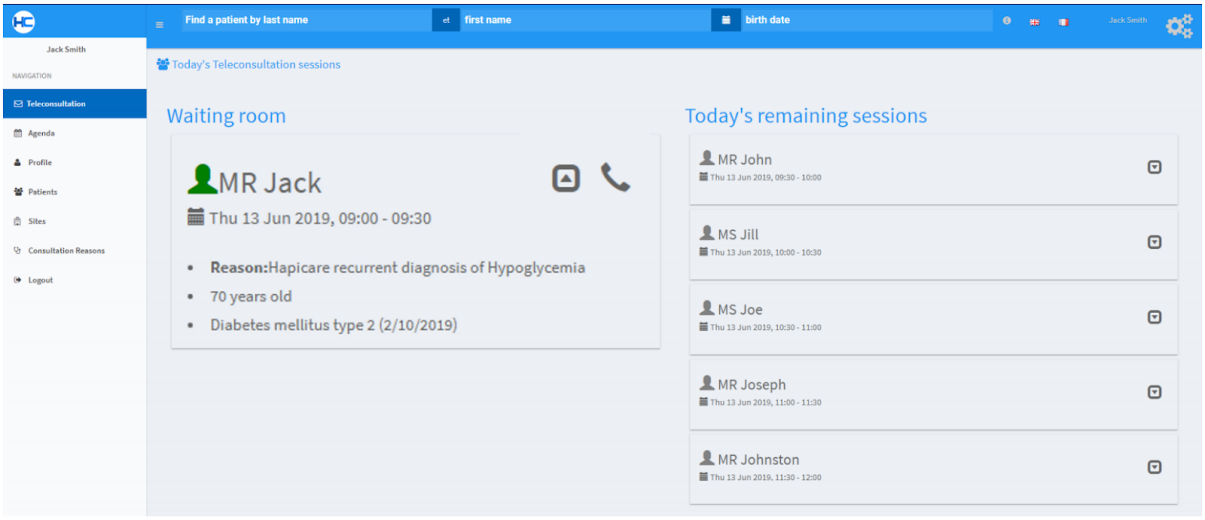

Figura 27: Interfaccia Hapicare della sala d'attesa [46].

Mentre viene stabilita la connessione tra paziente e specialista via videochiamata, quest'ultimo fa richiesta della cartella clinica tramite Hapicare, che la inoltra ad HapiChain. Gli smart contract elaborano la richiesta in modo che rispetti le seguenti condizioni:

I. la richiesta proviene da Hapicare (*Source Authentication*);

II. la firma digitale della richiesta corrisponde al valore hash calcolato (*Source Integrity*);

III. il medico è registrato in HapiChain (*User Authentication*);

IV. il medico può accedere al file richiesto nell'ora corrente (*Access Control*).

Soddisfatte queste condizioni, HapiChain consente l'accesso ed invia la cartella clinica crittografata ad Hapicare, dove verrà decodificata e mostrata al medico. Basandosi sull'analisi della cartella clinica, sul motivo della visita e su una ulteriore misurazione della glicemia real time, effettuata grazie al glucometro IoT del paziente e inoltrata ad Hapicare, il medico indaga sulla problematica (ipoglicemia ricorrente) e stabilisce, se lo ritiene necessario, una modifica della terapia seguita. Per garantire che una nuova prescrizione sia adatta al paziente, il medico riconfigura le regole di Hapicare, ad esempio per ricordargli di assumere la sua dose di insulina a digiuno per una settimana e prenotare automaticamente un nuovo appuntamento nel caso in cui la glicemia media superasse un certo valore di soglia. Al termine della sessione, la nuova cartella clinica composta dalla nuova prescrizione e da una nuova misurazione viene cifrata e archiviata utilizzando HapiChain. L'accesso alla cartella clinica per il medico viene interrotto e Hapicare continua a monitorare il paziente.

5.2.3 Conclusioni

HapiChain raccoglie in un'unica applicazione i vantaggi del Teleconsulto e della blockchain: nel caso d'uso appena visto, il medico ha modificato il dosaggio di insulina che il paziente deve assumere senza che nessuno dei due abbia dovuto lasciare la propria abitazione, comportando anche un risparmio di tempo e denaro. Inoltre anziani e soggetti affetti da patologie croniche, evitando di trascorrere molto tempo in una sala d'attesa sono messi a riparo da possibili infezioni.

La blockchain invece garantisce la riservatezza e la privacy del paziente: la cartella clinica è crittografata e limitata, accessibile solo al medico durante l'appuntamento. Gli smart contract fanno sì che le cartelle cliniche non siano manomesse. La blockchain inoltre consente elevata scalabilità ed interoperabilità grazie ad un processo di gestione dei dati trasparente e uniforme, codificato negli smart contract. Infine, essendo i report di ciascuna consultazione a prova di manomissione e archiviati in HapiChain, la gestione fiscale è trasparente e la possibilità di frodi sanitarie è ridotta al minimo.

5.3 SHAREChain

Per affrontare i problemi di affidabilità e interoperabilità nella gestione dei dati sanitari e delle cartelle cliniche, Lee et al. hanno proposto un framework di condivisione dei dati sanitari, *SHAREChain* (*Standard Healthcare-data Access with Reliability and Exchangeability*) alla Conferenza Internazionale di Bioinformatica e Biomedicina (BIBM) del 2019. Applica gli standard *Fast Healthcare Interoperability* (FHIR) e *Cross Enterprise Document Sharing* (XDS) al suo modello di dati e al metodo di trasmissione. Inoltre hanno costruito una blockchain Consortium in modo da prevenire la falsificazione dei dati archiviati e garantirne la trasparenza.

Prima di SHAREChain sono stati condotti molti studi sulla gestione e la condivisione di dati sanitari, ma molti lasciano irrisolto il problema dell'interoperabilità: i diversi formati utilizzati dalle varie strutture rendono molto complicata la condivisione di dati e cartelle. Lo studio di Yu Zhuang et al. [54], pur tenendo conto del problema, presenta dei limiti nell'applicazione di standard come *Clinical Document Architecture* (*CDA*), sviluppati prima di FIHR. Questo standard è veloce, facilita la combinazione e l'estrazione delle unità di risorse e migliora la riusabilità, un limite del metodo di condivisione basato sui documenti. Lee, Kim e Kim hanno scelto dunque di adottare il modulo FHIR Generator da loro stessi sviluppato [55].

Sebbene i vantaggi dell'utilizzo della blockchain nella gestione di dati sanitari siano ben documentati, con SHAREChain si propone una struttura di condivisione dei dati basata sugli standard, applicando FHIR e XDS. La caratteristica principale di quest'ultimo è la sua struttura registro-repository: nel primo vengono archiviati i metadati, inclusi i registri di riferimento, mentre nel secondo i dati originali. Inoltre, è stata costruita una blockchain di tipo Consortium per aumentare l'affidabilità condividendo i dati solo con istituzioni autorizzate.

5.3.1 Descrizione

Il sistema XDS su cui si basa SHAREChain (Figura 28) consta di cinque attori: sorgente di identità del paziente (*Patient Identity Source*), consumatore (*Consumer*), sorgente dati (*Data Source*), *Repository* e il registro blockchain (*Blockchain-registry*). Ogni registro blockchain delle istituzioni costituisce una rete blockchain Consortium e solo le istituzioni registrate nel consorzio possono partecipare al processo di condivisione dei dati. Tutte le transazioni che si

verificano su questa rete vengono registrate in modo trasparente e non possono essere modificate o eliminate. Nello specifico:

- ***Patient Identity Source***: gestisce gli identificatori dei pazienti e non contiene informazioni personali per minimizzare il rischio di fuga di informazioni personali. Esegue la transazione **ITI-8 (Patient Identity Feed)**. Fornisce notifiche al registro blockchain per eventuali aggiornamenti relativi all'identificazione del paziente.

- ***Consumer***: esegue due transazioni, **ITI-18 (Registry Stored Query)** e **ITI-43 (Retrieve Document Set)**. La transazione ITI-18 supporta la richiesta con l'ID di un paziente specifico al registro blockchain. Dopo che il registro ha restituito i metadati, il consumatore può eseguire la seconda transazione, ITI-43, con il repository per acquisire i dati originali.

- ***Data Source***: esegue la transazione **ITI-41 (Provide&Register Document Set)** con il repository. È responsabile dell'invio dei documenti FHIR originali e dei relativi metadati e ottiene dati grezzi attraverso un'interfaccia comune che interroga il database delle istituzioni e lo rigenera come risorsa o documento FHIR.

- ***Repository***: archivia e gestisce in modo permanente i dati originali sotto forma di FHIR. Esegue la transazione **ITI-42 (Register Document Set)** registrando i metadati ricevuti dall'origine dati nel registro. Restituisce anche i dati su richiesta del consumatore. Verifica se questo è autenticato e quindi invia i dati originali.

- ***Blockchain-registry***: memorizza i metadati che supportano la selezione e il recupero dei dati ed è indipendente dal repository in cui sono archiviati i dati originali. I metadati consentono al registro Blockchain di elaborare alcune operazioni senza la necessità di comprendere il formato o il contenuto dei dati originali.

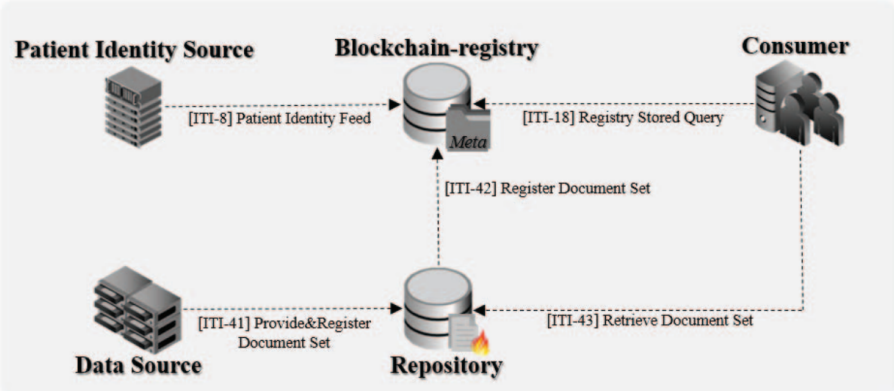

Figura 28: Schema degli attori che sfruttano i registri blockchain [48].

Uno dei concetti chiave di SHAREChain è l'implementazione del registro utilizzando la tecnologia blockchain, che garantisce l'affidabilità del sistema rendendo i dati incorruttibili. Inoltre questo sistema memorizza i valori hash dei dati nei metadati, che sono immutabili, caratteristica utile nelle attività che richiedono l'autenticità di documenti. Infine vengono registrate l'intera cronologia degli accessi, incluso il partecipante che ne fa richiesta, e l'identità utilizzata quando nell'invio di una transazione e rese pubbliche a tutti i partecipanti, riducendo la possibilità di dolo ai dati. A differenza di un tradizionale DBMS, SHAREChain utilizza un registro blockchain per sfruttare le sue caratteristiche di immutabilità, decentralizzazione e tracciabilità per condividere in modo affidabile i dati sanitari.

SHAREChain ha due funzioni principali: registrazione e *query*. Un po' come in una biblioteca nella quale si assegnano degli indici ai nuovi libri in ingresso, il registro blockchain viene utilizzato come indice dei dati sanitari. Tutti i dati in questo sistema devono prima essere registrati con metadati e avere ID univoci per essere condivisi con altre istituzioni.

In Figura 29 è rappresentato il processo di registrazione dei dati sanitari: la sorgente dati formalizza i dati grezzi per conformarsi allo standard FHIR utilizzando il generatore FHIR, quindi genera meta informazioni per questi dati con il generatore di metadati. Quando dati e metadati FHIR sono pronti, l'origine li invia al repository con la transazione ITI-41. Il repository verifica che i dati ricevuti siano conformi allo standard FHIR utilizzando il modulo *FHIR Validator* e dopo la convalida i dati FHIR vengono archiviati in una memoria persistente, mentre i metadati passano al registro Blockchain con ITI-42.

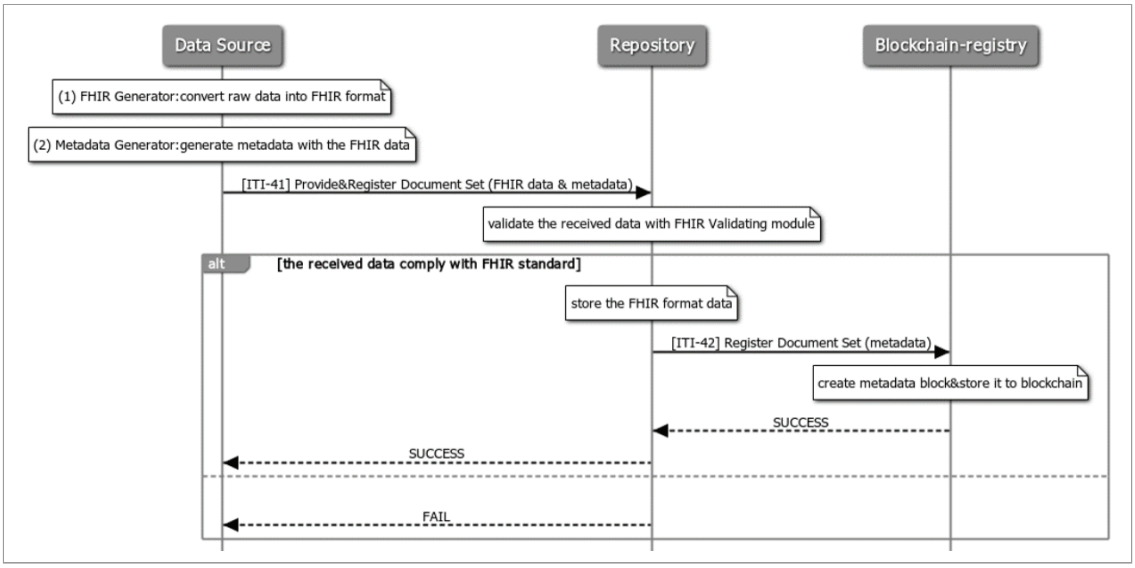

Figura 29: Processo di registrazione dei nuovi metadati nel registro blockchain [48].

Per quanto riguarda il query invece, mostrato in Figura 30, un consumatore invia query al registro Blockchain utilizzando la transazione '*Query'* memorizzata nel registro. Viene creato un blocco chiamato '*SharedHistory'* contenente sette campi di stato ('WAITING APPROVAL', 'APPROVED', 'REJECTED', 'SENT', 'RECEIVED', 'SHARED', 'ERROR') che viene aggiornato in base al processo di condivisione dei dati; in seguito il registro blockchain restituisce un elenco di metadati. Il consumatore ottiene i dati accedendo al repository e controlla il valore hash nei dati condivisi rispetto a quello dei metadati, per determinare se i dati ricevuti sono corretti.

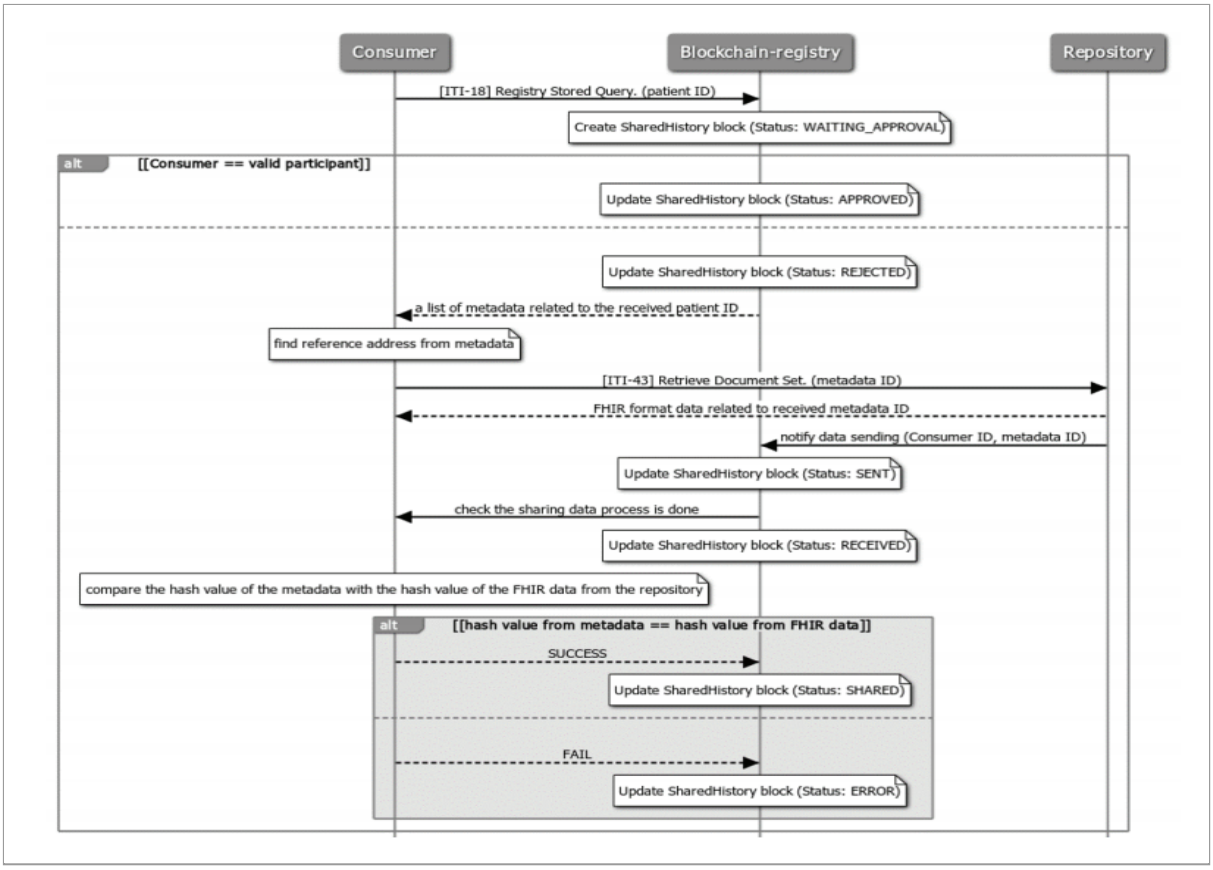

Figura 30: Il processo di query tra il consumatore ed il registro Blockchain [48].

5.3.2 Conclusioni

L'introduzione della blockchain e degli standard FHIR e XDS aiutano a garantire l'affidabilità e l'interoperabilità dei dati. La blockchain infatti gestisce i dati in modo che siano coerenti, con marcature temporali (timestamp), trasparenti e immutabili. Lo standard FHIR invece risolve i problemi di interoperabilità: mentre con CDA i dati sono relativamente statici richiedendo un lavoro specifico per ottenere le informazioni e renderle disponibili in qualsiasi altro formato, FHIR evita le trappole dello scambio basato sui documenti, che spesso richiedono un accesso separato ai dati.

Una criticità di SHAREChain sta nella mancanza di un approccio incentrato sul paziente: egli in fin dei conti è il proprietario dei dati, e se la loro raccolta viene mal eseguita, la struttura di condivisione perde significato. Gli sviluppatori, per far sì che il sistema sia più paziente-centrico, che possa trarre vantaggio dall'utilizzo di una struttura condivisa, hanno pensato di introdurre un sistema di consenso dinamico. Ad esempio con un'applicazione mobile il paziente potrebbe decidere se condividere o meno i proprio dati e tenerne traccia, confermandosi definitivamente loro proprietario.

Si può pensare di applicare SHAREChain in contesti sanitari veri: dati medici, dati di ricerca e dati pubblici possono essere raccolti in un unico posto per gettare le basi per la condivisione, possono essere aggiunte funzioni supplementari che analizzano i dati accumulati e possono essere proposte strutture per l'uso secondario dei big data sanitari, come la comprensione e il trattamento delle malattie.

5.4 AaYusH

La Telechirurgia consente ai chirurghi, in località fisicamente distanti tra loro, di collaborare per il successo delle procedure attraverso canali di comunicazione wireless (WCC). La Telechirurgia, sfruttando la rete internet tattile 5G, ha un enorme potenziale, in quanto è in grado di fornire servizi chirurgici ultra-reattivi, real time, da remoto con alta qualità e precisione, portando vantaggi importanti alla società moderna. Tuttavia, i sistemi Telechirurgia esistenti presentano problemi di sicurezza, privacy, latenza e costi di archiviazione blockchain, che ne limitano l'applicabilità nell'immediato.

Il chirurgo accede ed esamina i dati del paziente conservati in server un cloud [56], che può essere soggetto ad attacchi esterni che mettono a rischio la sicurezza e la privacy del paziente. Per garantire maggiore sicurezza dei dati, alcuni sistemi di Telechirurgia hanno adottato la tecnologia blockchain, che oltre a garantire la consistenza e l'integrità dei dati grazie ai vari meccanismi di consenso, offre altri vantaggi come la condivisione rapida dei dati, la tolleranza ai guasti, il risparmio in termini di costi, l'efficienza in termini di tempo e la tracciabilità dei dati. Inoltre la collaborazione tra più chirurghi, e la stipula degli accordi necessari tra medico, paziente e struttura sanitaria sono regolati dagli smart contract.

Negli anni sono stati presentati diversi progetti e proposte per rendere la Telechirurgia sicura ed efficiente. Nel 2015, Bonaci et al. hanno presentato un'analisi delle possibili minacce di sicurezza al robot chirurgico *Raven II* ® suggerendo delle tecniche di mitigazione, ma trascurando il problema della latenza [57]. Diversi autori hanno poi presentato delle proposte di Telechirurgia basate su connessione 5G a bassa latenza, in grado di raggiungere un ritardo di comunicazione inferiore a 1 ms: portando la latenza sotto questa soglia, aumenta la precisione dell'intervento, ma senza considerare eventuali problemi di sicurezza. Uno dei primi sistemi di Telechirurgia basato su blockchain è stato *HabiTs*, presentato da Gupta et al. [58]. Sebbene questo sistema presenti sicurezza ed affidabilità contro gli attacchi esterni, la tecnologia blockchain richiede un costo di archiviazione elevatissimo, creando un problema di scalabilità.

Per andare oltre queste limitazioni, il sistema di Telechirurgia AaYusH, progettato sempre da Gupta et al. [49], per sopperire al problema della scalabilità, sfrutta una blockchain pubblica, Ethereum, basata su smart contract scritti in Solidity con la suite Truffle, con diversi permessi e ruoli definiti per medici e pazienti (Figura 31), mentre i dati vengono raccolti in un database IPFS che offre grande capacità di archiviazione e bassa latenza. La rete sfruttata è 5G Tactical

Internet, la quale si pone come obiettivo una latenza inferiore a 1 ms con un'accuratezza del 99,999%. AaYusH inoltre presenta un sistema di feedback per i pazienti, grazie al quale possono scegliere il chirurgo in base alle valutazioni.

```
Procedure Telesurgery (E_s, E_p, E_c)
    While (True) do
        If (Entity(E) = = E_p) then
            Publish_HealthIssues (D_i,Desc)
                                ....
        End if;
        If (Entity(E) = = E_s) then
            Operate_Surgery (E_p,D_i)
                                ....
        End if;
        If (Entity(E) = = E_c) then
            Monitor_Health_Values (E_p,E_s,D_i)
                                ....
        End if;
    End While;
End Procedure;
```

Figura 31: Smart Contract Ethereum. $\mathbf{E_s}$ entità chirurgo, $\mathbf{E_p}$ entità paziente, $\mathbf{E_c}$ entità caregiver [49].

5.4.1 Descrizione

Il sistema AaYusH consiste del set di entità $\{E_p, E_s, E_c, E_a\}$: E_p è il paziente, E_s è il chirurgo, E_c è il caregiver, E_a l'autorità. E_s consiste di n chirurghi, cioè $\{S_1, S_2, S_3, \ldots, S_n\} \in E_s$, associati a m ospedali $\{H_1, H_2, H_3, \ldots, H_m\} \in H$. Qualsiasi chirurgo i-esimo S_i associato all'ospedale H può operare sul paziente $\{P_1, P_2, P_3, \ldots, P_k\} \in E_p$, soggetto ai vincoli e alle mappature, come segue:

$$\{n, m, k, i, j, a\} > 0$$

$$f_1 : S \rightarrow H(n : m), f_2 : S \rightarrow P(n : 1), f_3 : H \rightarrow P(1 : k)$$

Quindi, ci sono matrici $[SH]_{n \times m}$, $[SP]_{n \times 1}$ e $[HP]_{1 \times k}$ con le seguenti voci:

$$[SH]_{n\ x\ m} = \begin{cases} 1, & se\ S_i \in H_j,\ \forall E_s,\ H \\ 0 & altrimenti \end{cases} \quad (1)$$

$$[SP]_{n\ x\ 1} = \begin{cases} 1, & se\ S_i \in P_a,\ \forall E_s,\ E_p \\ 0 & altrimenti \end{cases} \quad (2)$$

$$[HP]_{1\ x\ k} = \begin{cases} 1, & se\ P_a \in H_j,\ \forall H,\ E_p \\ 0 & altrimenti \end{cases} \quad (3)$$

Le equazioni (1), (2) e (3) rappresentano le matrici di mappatura per le equazioni f_1, f_2 e f_3. Le entità possono comunicare utilizzando l'indirizzo del portafoglio $W = \{W_b, W_s, W_p\}$ nella blockchain. Gli indirizzi del portafoglio di un paziente, di un chirurgo e della blockchain sono costituiti dalle seguenti entità:

$$W_b = \{Send_{addr}, Nonce, T^b_{stamp}, GAS^b_{value}, M_{tree}\}$$
$$W_p = \{PK^a, PU^a, P^a_{hash}, T^a_{stamp}, GAS^a_{value}, M_{tree}\}$$
$$Ws = \{PK^i, PU^i, P^i_{hash}, T^i_{stamp}, GAS^i_{value}, M_{tree}\}$$

Pazienti e chirurghi possono comunicare spendendo una quantità specifica di criptovaluta C_{spec} tramite il canale di comunicazione wireless $C_{wireless}$. Essendo un'operazione di Telechirurgia critica, non si può scendere a compromessi con la latenza L: maggiore è la latenza, maggiori saranno le possibilità di un intervento chirurgico infruttuoso.

$$L = RTT(C_{wireless}) \tag{4}$$
$$L_{LTE-Advanced} \leq 20ms \tag{5}$$
$$L_{Tactile\_Internet} < 1ms \tag{6}$$

La funzione obiettivo di AaYusH è invece:

$$O = max\ (TS_{sec\rightarrow\{W_s, W_p, W_b\}},\ S_{accuracy}) + min\ (L) \tag{7}$$

dove $TS_{sec\rightarrow\{W_s, W_p, W_b\}}$ indica il livello di sicurezza del sistema AaYusH in termini di portafogli conservati nella blockchain Ethereum, $S_{accuracy}$ l'accuratezza del chirurgo durante l'operazione e L la latenza di andata e ritorno del canale di comunicazione.

In Figura 32 è rappresentata l'architettura del sistema AaYusH, e può essere divisa in tre livelli principali.

Al livello del chirurgo (*Surgeon Layer*) questi, a seguito della verifica, può avviare la procedura di Telechirurgia, durante la quale trasmette i comandi al robot al livello del paziente attraverso un'interfaccia e una connessione 5G. La fiducia tra gli attori coinvolti e la sincronizzazione dei comandi sono garantiti dall'esecuzione degli smart contract, e gli strumenti a disposizione del chirurgo sono: controller principale, pedaliera, manipolatore principale, dispositivi tattili, monitor video 3D, sensore di posizione, decompressore video, altoparlanti e microfono. Il chirurgo può interagire con lo smart contract tramite i client Ethereum per la richiesta e l'avvio della procedura, mentre il paziente accetta le richieste del chirurgo sulla base delle sue valutazioni. Accettata la richiesta dal paziente, il chirurgo può

avviare la procedura di Telechirurgia (‘*Sstate = Active’*) e aggiornare la cartella clinica del paziente nell’archivio IPFS. Una volta completata la procedura di (‘*Sstate = Finished’*), il paziente può valutare la prestazione del chirurgo.

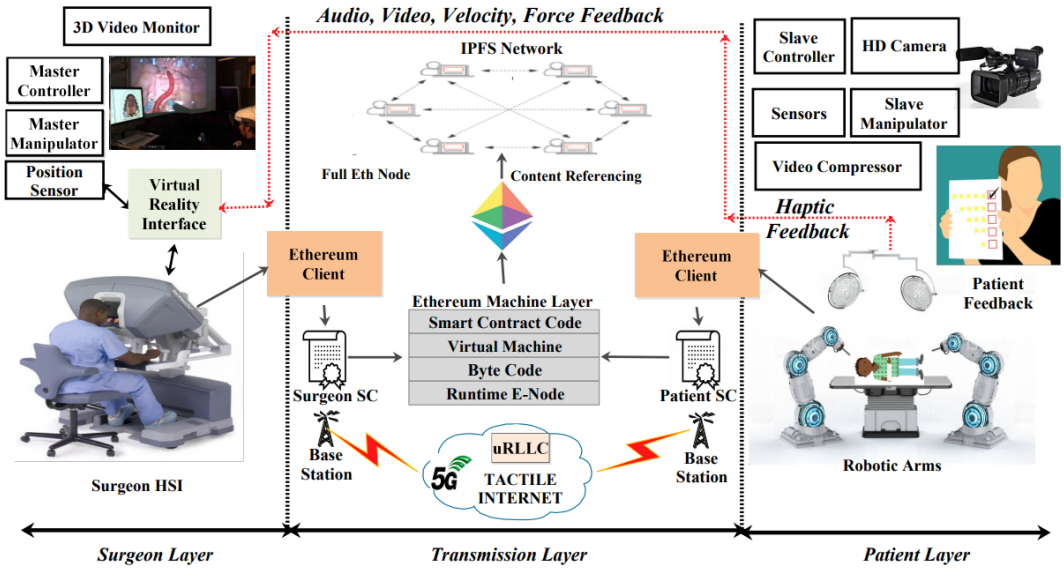

Figura 32: Architettura del sistema AaYusH [49].

Al livello della trasmissione (*Transmission Layer*) viene stabilita la connessione tra chirurgo e paziente, perciò è richiesta grande reattività ed affidabilità per trasmettere in tempo reale i comandi del chirurgo e i dati. I componenti principali di questo livello sono:

- **Smart Contract Ethereum**: in AaYusH ci sono quattro entità $\{E = E_p, E_s, E_c, E_a\}$ associate allo smart contract tramite il client Ethereum e ciascuna di esse ha un account di proprietà esterna per interagire con la Ethereum blockchain. E_a, che nel contratto rappresenta un’organizzazione sanitaria di fama mondiale, decide se approvare o meno le pratiche dei chirurghi controllando i documenti dello specialista che desidera essere autorizzato come chirurgo certificato. I requisiti per la corretta verifica del documento del chirurgo sono la Laurea in Medicina con esperienze di impiego clinico e almeno tre anni di esperienza nel proprio campo di specializzazione. Una volta accettata la documentazione, il chirurgo può praticare Telechirurgia ed essere scelto dai pazienti. I chirurghi selezionati $\{S_1, S_2, \ldots, S_n\} \in E_s$ possono avviare le procedure di Telechirurgia sul paziente $P_i \in E_p$ richiedendo la sua chiave hash IPFS per visualizzare le sue precedenti cartelle cliniche e impostare ‘*Sstate = Active’*. Ora i chirurghi possono aggiornare regolarmente la cartella del paziente nell’IPFS durante l’operazione e restituire una nuova chiave hash IPFS. Terminata la procedura (‘*Sstate=Finished’*), i pazienti possono valutare i chirurghi.

- **Protocollo IPFS**: IPFS memorizza i dati in blocchi di dimensioni fisse, che sono interconnessi tra loro e formano un Merkle Tree generalizzato del grafico aciclico diretto. Quando un file viene archiviato nell'IPFS, viene generata una chiave hash e restituita all'entità interessata. Ogni volta che abbiamo bisogno di accedere ai dati, la sua chiave hash può essere utilizzata per lo stesso tramite il gateway IPFS. In questo modo, la tracciabilità in AaYusH è utile per trovare il *loop-hole* nel sistema in caso di qualsiasi problema.

Al livello del paziente (*Patient Layer*) si trova un robot che esegue i comandi ricevuti dal chirurgo, che grazie anche ad un controller, alle telecamere, sensori e dispositivi tattili riesce ad operare in remoto. A questo livello appartengono anche i caregiver e il paziente. Come già detto, quest'ultimo ha a disposizione un sistema di feedback per poter giudicare il lavoro del chirurgo: una volta terminata la procedura il paziente risponde ad un questionario di n domande $Q = \{Q_1, Q_2, Q_3, \ldots, Q_n\}$, il sistema di feedback di AaYusH verifica il ruolo dell'entità che ha compilato il questionario, controlla che l'operazione chirurgica sia terminata e in base alle risposte calcola un valore di performance (PR_{ES}) e lo aggiorna all'interno della blockchain. Se la recensione è positiva, il PR_{ES} del chirurgo viene incrementato, viceversa si riduce secondo le equazioni 8 e 9 rispettivamente:

$$PR_{ES} \leftarrow PR_{ES} + (PR_{ES}/RC_{ES}) \tag{8}$$

$$PR_{ES} \leftarrow PR_{ES} - (PR_{ES}/RC_{ES}) \tag{9}$$

dove RC_{ES} è il numero di recensioni del chirurgo. Per valori di $PR_{ES} > 90\%$ il chirurgo è raccomandato da AaYusH, se $70\% < PR_{ES} < 90\%$ è parzialmente raccomandato, invece per PR_{Es} al di sotto della soglia del 70% AaYusH sconsiglia la scelta di quel chirurgo.

5.4.2 Valutazione delle performance

Una valutazione sull'effettiva efficacia di AaYusH come sistema di Telechirurgia può essere fornita basandosi sui due parametri su cui ci si è maggiormente concentrati:

1. **Latenza**: in Figura 33 è mostrata il paragone tra la latenza del sistema AaYusH, con connettività 5G, ed uno tradizionale su rete LTE in rapporto al numero di transazioni. In entrambi i casi i valori di latenza sono calcolati come regressione lineare dei valori calcolati, ed è evidente come siano inferiori in AaYush grazie alla connessione tattile su rete 5G che porta la latenza sotto 1 ms con un'affidabilità del 99,999%.

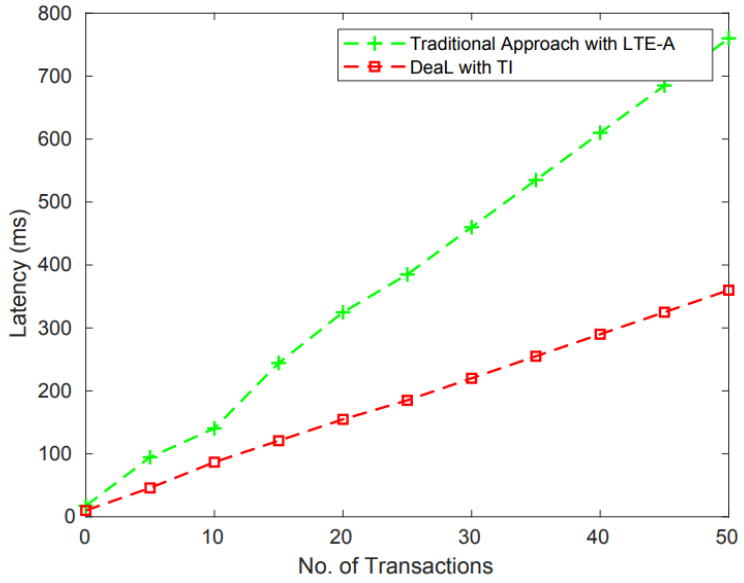

Figura 33: Valori di latenza in ms in rapporto al numero di transazioni in AaYush (rosso) e in un sistema tradizionale (verde) [49].

2. **Costo di archiviazione IPFS**: mentre i costi di archiviazione su Ethereum blockchain sono "fissi" (il costo definitivo dipende solamente dal valore della criptovaluta al momento dell'archiviazione), in AaYusH, essendo necessario solamente l'hash per archiviare nella blockchain grazie al protocollo IPFS, il costo varia in base al metodo utilizzato per il valore hash memorizzato (Figura 34).

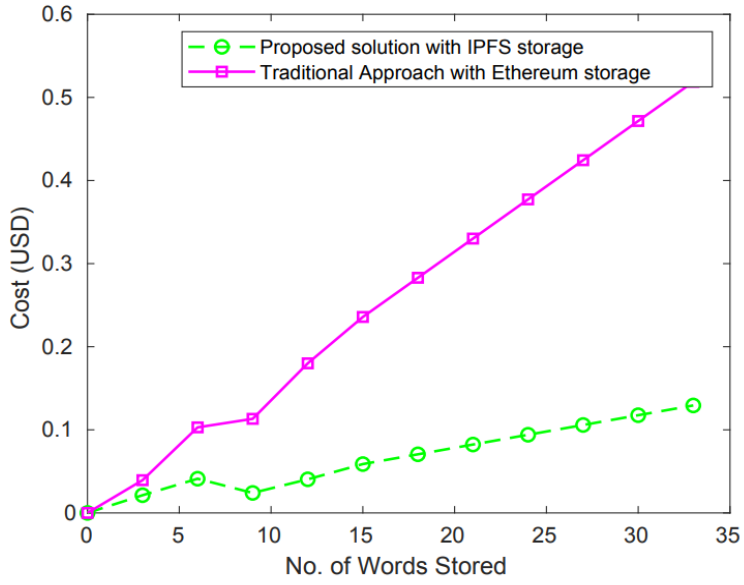

Figura 34: Comparazione dei costi di archiviazione tra la Ethereum blockchain (viola) ed i diversi scenari con il protocollo IPFS [49].

5.4.3 Conclusioni

Il sistema di Telechirurgia AaYusH, grazie all'implementazione di una blockchain pubblica, non garantisce solamente integrità e sicurezza dei dati senza dover ricorrere ad un intermediario centrale; infatti l'integrazione con il protocollo IPFS e l'utilizzo degli smart contract consentono rispettivamente un abbattimento dei costi di archiviazione ed una gestione più accurata dei ruoli e dei permessi all'interno del sistema. Infine la latenza, parametro fondamentale che nel corso di un'operazione chirurgica in remoto potrebbe costare la vita del paziente, è sensibilmente inferiore grazie alla connessione 5G.

È pensabile e auspicabile dunque l'applicazione di AaYusH su diverse piattaforme, ma sarebbero necessarie indagini più approfondite sulla scalabilità del sistema.

5.5 Autenticazione biometrica FV (Finger Vein)

I sistemi di Telemedicina richiedono un'autenticazione sicura quando utilizzano delle applicazioni, ad esempio per il Telemonitoraggio, per garantire sicurezza e protezione della privacy dei pazienti. Fra i sistemi più recenti di autenticazione biometrica troviamo la scansione venosa del dito (*Finger Vein, FV*) che offre maggiore accuratezza, velocità e sicurezza rispetto alla classica scansione delle impronte. La biometria delle vene utilizza modelli vascolari nel corpo umano, sfruttando l'unicità e la stabilità a lungo termine del pattern venoso. Inoltre le vene delle dita sono invisibili all'occhio umano trovandosi sottopelle e immuni a distorsioni o modifiche esterne. La biometria venosa è anche contactless, perciò non richiede alcun contatto fisico tra il dito e il sensore nel processo di autenticazione. In Figura 35 è mostrata l'architettura di un sistema di autenticazione biometrico FV.

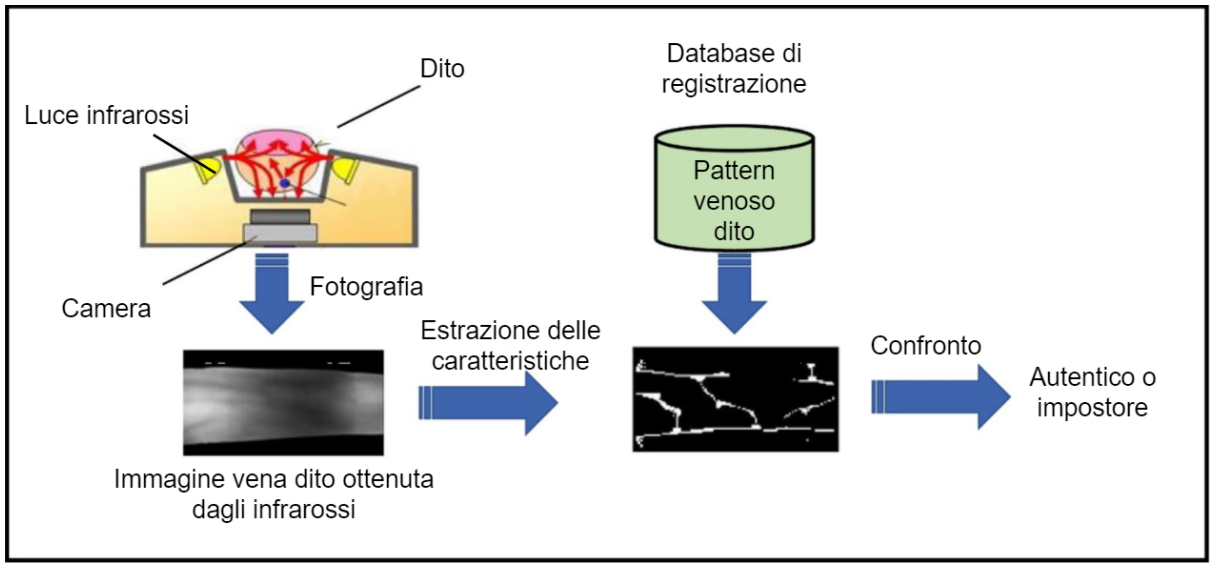

Figura 35: Architettura del sistema biometrico venoso. Il processo di verifica si articola in quattro fasi principali: acquisizione dell'immagine, pre-processing, processing e confronto [50].

Negli standard internazionali (ISO/IEC 27002, 2005), la sicurezza delle informazioni è definita come il mantenimento di riservatezza, integrità e disponibilità delle informazioni, noto anche come triangolo della CIA [59]. Questo triangolo è considerato lo standard del settore per la sicurezza informatica in base alle tre caratteristiche delle informazioni.

Moshin et al. della Universiti Pendidikan Sultan Idris, Malesia, hanno proposto un nuovo framework di verifica per l'autenticazione del paziente tra il punto di accesso (dispositivo) e il database dei nodi. Il modello di autenticazione biometrico è un ibrido risultato

dell'algoritmo di unione, che combina l'identificazione a radiofrequenza (RFID) e le caratteristiche biometriche FV per aumentare la randomizzazione e i livelli di sicurezza nella struttura del pattern. La sicurezza dei dati durante l'autenticazione è garantita da una combinazione di blockchain e steganografia, mentre la trasmissione è assicurata dalla blockchain, inclusa una tecnica di hashing per ottenere l'integrità dei dati e l'autenticità della posizione del paziente. La steganografia dell'ottimizzazione dello sciame di particelle (PSO) e le tecniche avanzate di crittografia standard (AES) vengono utilizzate per la riservatezza nel canale di trasmissione. Questa struttura può essere implementata su un'architettura di rete decentralizzata, inclusi i punti di accesso e i nodi senza un'autorità centrale.

5.5.1 Descrizione

Il processo si articola in due fasi principali. La prima è la fase di identificazione: vengono identificati i requisiti dell'operazione di verifica biometrica FV, vale a dire il set di dati e l'estrazione delle caratteristiche. Viene proposto un nuovo algoritmo di unione per combinare le caratteristiche RFID e le caratteristiche FV in un modello ibrido e casuale. La seconda fase è di sviluppo di un quadro di verifica sicuro basato sul nuovo modello biometrico definito nella prima fase. Nella seconda fase, un nuovo framework sicuro per l'autenticazione del paziente utilizza una combinazione di tecniche di crittografia, blockchain e steganografia basate sul modello di pattern ibrido, garantendo così che il sistema di verifica biometrica FV rimanga sicuro durante l'autenticazione (Figura 36).

Nell'access point le immagini FV vengono pre-processate, da queste si estraggono le caratteristiche del pattern venoso e convertite in una stringa in binario. Anche le caratteristiche RFID sono estratte ed inserite in una stringa, combinata casualmente con quella FV. Una copia del pattern ibrido implementata con un hash MD5 ed una protetta da crittografia sono inserite nello stesso blocco dati e inviate al lato nodo via blockchain.

Lato nodo, una copia criptata del pattern ibrido è già salvata nel database del nodo prima della ricezione della richiesta del dispositivo di registrazione. Il modello viene nascosto utilizzando la steganografia. Alla ricezione della richiesta del dispositivo di registrazione, l'hash nella blockchain viene verificato abbinandolo al libro mastro, utilizzato per memorizzare l'hash dei pazienti individualmente nel lato nodo. Se la corrispondenza del risultato dell'hash è vera il modello ibrido viene decifrato e altre elaborazioni continuano, altrimenti si verifica un attacco al sistema. Contemporaneamente, in background, il pattern ibrido, che esiste nel nodo tramite analisi steganografica, viene estratto e le informazioni sul

pattern ibrido criptate vengono decifrate in testo normale (binario). Viene eseguita un'operazione di divisione per separare le caratteristiche FV dalle caratteristiche RFID utilizzando l'algoritmo di unione inverso e vengono eseguite due operazioni di abbinamento tra le funzioni FV e RFID lato dispositivo di registrazione e quelle estratte dal database del nodo. Il paziente viene identificato e verificato se autorizzato o non autorizzato.

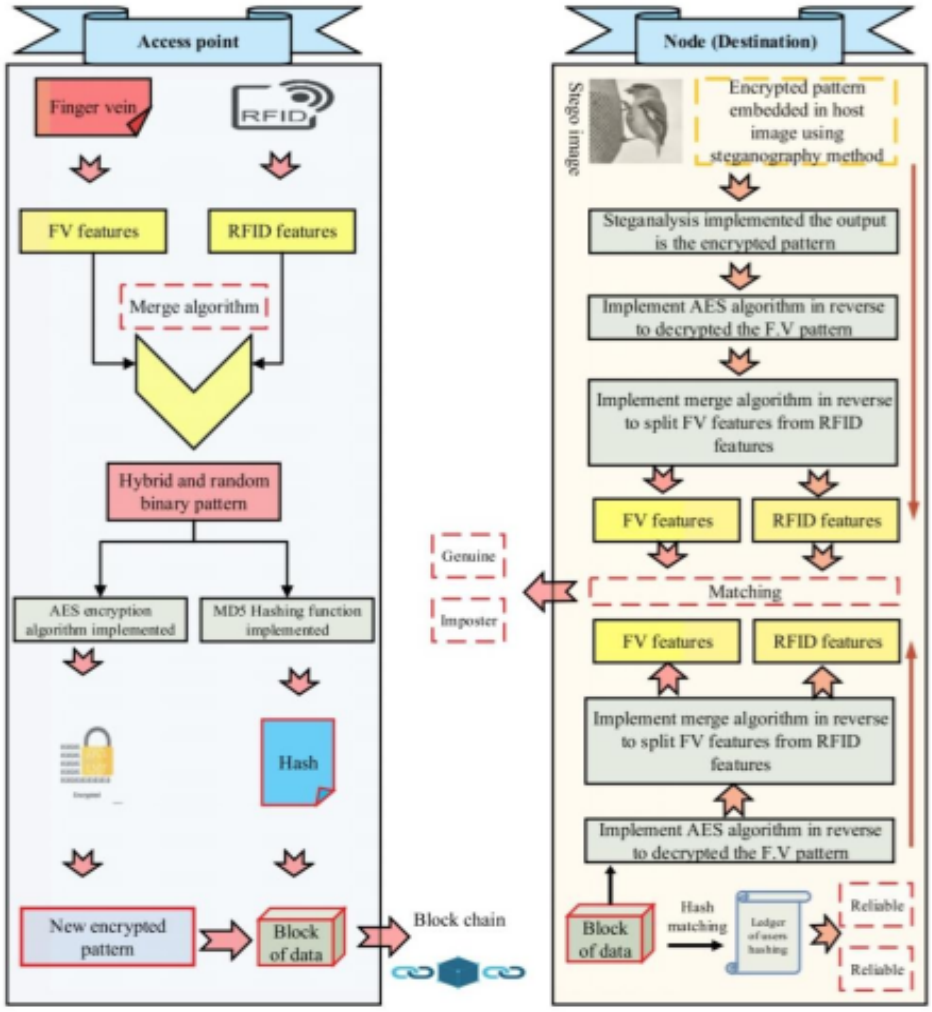

Figura 36: Framework di verifica sicura [50].

5.5.1.1 Prima fase

Nel pre-processing della prima fase occorre individuare una regione d'interesse a partire dall'immagine rilevata (ROI) e da qui, grazie a filtraggio gaussiano e all'algoritmo di segmentazione di Otsu, vengono rimossi il rumore in input e il background dell'immagine. L'estrazione delle caratteristiche FV avviene grazie ad un algoritmo basato sul metodo della massima curvatura; per le caratteristiche RFID si è utilizzato una smart card RFID ad alta frequenza che richiede una distanza tra il tag e il lettore non superiore a 30 cm, garantendo così che le informazioni contenute nel RFID non siano accessibili da una lunga distanza. Il

seriale del RFID è costituito da 38 bit (Figura 37): i primi 32 bit costituiscono un pattern binario univoco; i 2 bit successivi sono per le istruzioni di manipolazione (polo e direzione); gli ultimi 4 bit rappresentano K, la funzione caotica, e possono avere un valore che va da 8 a 15.

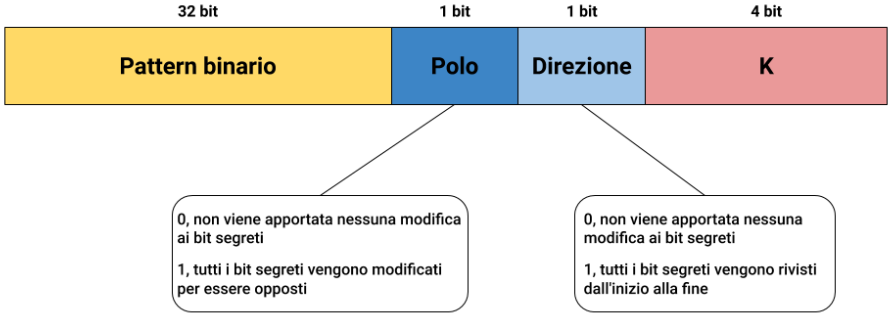

Figura 37: Formato RFID [50].

L'algoritmo di unione protegge il pattern durante la fase di registrazione, impedendo così agli aggressori di discernere quale set di dati è la stringa binaria biometrica. Questo algoritmo utilizza la stringa binaria RFID e la stringa binaria biometrica in una stringa casuale che viene estratta dal FV, e continua a funzionare correttamente quando si cambia RFID per qualsiasi motivo. L'algoritmo di unione si articola in tre passaggi: il primo è una semplice concatenazione; nel secondo verranno implementate alcune manipolazioni sui dati binari; nel terzo, una funzione caotica è implementata sui dati con le equazioni qui sotto, dove K è il grado di caos.

$$p_{n+1} = p_n + K\ sin\ (\theta_n) \tag{10}$$

$$\theta_{n+1} = \theta_n + p_{n+1} \tag{11}$$

Questa funzione caotica è chiamata mappa standard, nota anche come mappa di *Chirikov-Taylor* o mappa standard di Chirikov.

5.5.1.2 Seconda fase

Per proteggere i dati raccolti nella prima fase si utilizza l'algoritmo di crittografia a chiave simmetrica AES. Questo algoritmo può crittografare lunghi testi in chiaro con alta efficienza [60] e supporta un blocco di dati di 128 bit con una dimensione della chiave variabile di 128, 192 e 256 bit [61]. Questo algoritmo raggiunge una buona velocità nell'implementazione software e hardware e può essere utilizzato su piattaforme diverse, soprattutto su piccoli dispositivi. Il processo dell'algoritmo AES è diviso in una serie di fasi (*rounds*).

1. *Sub Bytes*: sostituzione non lineare di tutti i byte che vengono rimpiazzati secondo una specifica tabella.
2. *Shift Rows*: spostamento dei byte di un certo numero di posizioni dipendente dalla riga di appartenenza.
3. *Mix Columns*: combinazione dei byte con un'operazione lineare, i byte vengono trattati una colonna per volta.
4. *Add Round Key*: ogni byte della tabella viene combinato con la chiave di sessione, la chiave di sessione viene calcolata dal gestore delle chiavi.

L'ultimo round del processo di crittografia non contiene lo step '*Mix Columns*'. La fase di decifratura non è identica a quella di cifratura dal momento che gli step sono eseguiti in ordine inverso ('*Inverse Shift Rows'*, '*Inverse Substitute Bytes'*, '*Add Round Key'*, '*Inverse Mix Columns'*). Per aumentare la sua efficienza questo processo è stato implementato con una dimensione della chiave di 192 bit e con 12 round di iterazione. L'algoritmo viene utilizzato per crittografare i pattern FV ibridi e casuali, che sono stati prodotti nella fase 1 durante la registrazione del paziente (lato dispositivo), tuttavia l'utilizzo solo di una tecnica di crittografia non è sufficiente per ottenere un elevato livello di riservatezza.

Per soddisfare i requisiti di integrità e disponibilità secondo CIA nel canale di trasmissione, durante l'invio del pattern FV dal dispositivo di registrazione (punto di accesso) al nodo e al database del nodo, è stata utilizzata la tecnologia blockchain. Per proteggere il modello biometrico ibrido prodotto come stringa binaria unidimensionale, vengono prodotte due copie del modello. La crittografia viene implementata utilizzando l'algoritmo AES su una copia del pattern per inviare i dati al lato nodo; la funzione di hashing è implementata sull'altra copia inviando questo hash dal dispositivo di registrazione al nodo.

Per garantire una maggiore sicurezza dei dati, si affianca alla crittografia AES l'utilizzo della steganografia. La steganografia si riferisce al processo di occultamento dei messaggi in un altro mezzo, come audio, video, immagini e altre forme di comunicazione, non modificando la struttura o il layout del messaggio segreto nascondendolo all'interno di un oggetto di copertura (oggetto vettore). Quindi, l'oggetto copertina e l'oggetto stego (l'oggetto con le informazioni nascoste) sono simili. Il recupero delle informazioni senza utilizzare la steganalisi (il processo di rilevamento delle procedure di steganografia) è difficile a causa dell'invisibilità o di fattori nascosti. In molti metodi di steganografia, i dati binari sono solitamente nascosti nei bit meno significativi (LSB) del pixel dell'immagine di copertina.

Per questo studio si è scelto l'approccio steganografico del dominio spaziale, in quanto consente di incorporare dati di grande dimensione nell'immagine host introducendo minore distorsione nell'immagine stego. I bit segreti vengono dunque nascosti all'interno di una *host image*, e la determinazione della migliore posizione al suo interno per nascondere i dati avviene grazie all'algoritmo di ottimizzazione PSO. Quando si utilizza PSO nella ricerca binaria, le soluzioni proposte sono definite da particelle, che possono rappresentare un vettore booleano. Successivamente, la particella viene valutata calcolandone la velocità, mentre la sua posizione determina se la caratteristica specifica deve essere selezionata. Questa tecnica di steganografia ricerca la posizione ottimale nell'immagine host nel dominio spaziale per incorporare bit di pattern FV segreti. L'immagine risultante, che viene immagine stego, ha una buona qualità, una distorsione minima e un'elevata resistenza agli attacchi. Il metodo proposto utilizza la scansione sequenziale all'interno di quattro finestre dall'immagine host per determinare il posto migliore in cui nascondere i bit segreti FV (Figura 38).

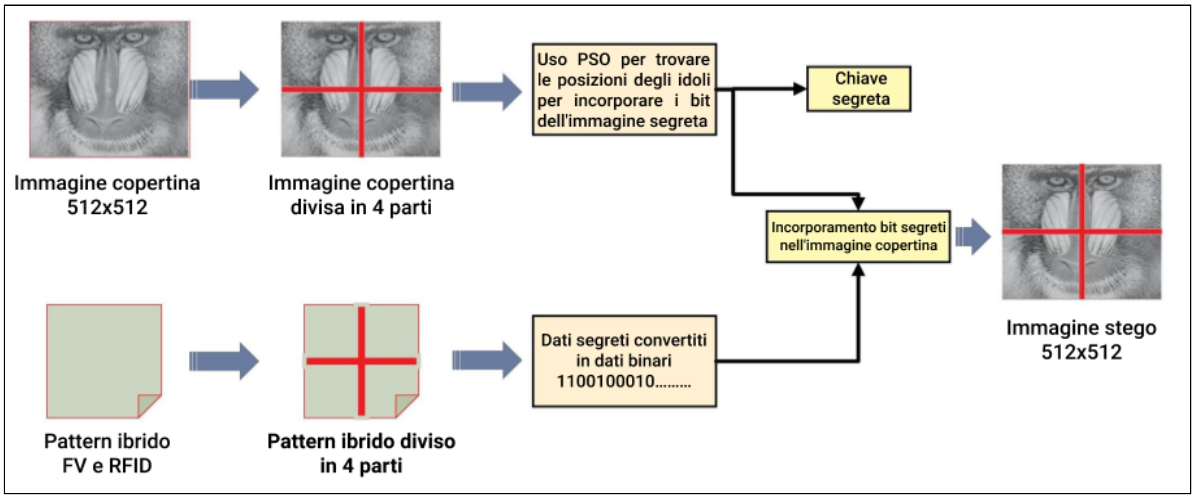

Figura 38: Diagramma del metodo di steganografia. Immagine cover e il pattern biometrico ibrido vengono divisi in 4 porzioni uguali. I dati biometrici convertiti in bit vengono nascosti nell'immagine in posizioni ben precise, individuate dall'algoritmo PSO e protette da una chiave. Il risultato finale è l'immagine stego [50].

5.5.2 Funzionamento

I dati utilizzati sono estratti dal database MMCBNU_6000, realizzato dalla Chonbuk National University in Corea del Sud. Questo set di dati contiene immagini FV di ciascuna mano e 10 immagini per ogni dito, salvate in formato BMP [62]. Nel pre-processing, dopo aver migliorato la qualità dell'immagine, cancellato il rumore ed individuata la ROI, le caratteristiche FV vengono estratte con il metodo della massima curvatura e convertite in una stringa binaria. Le caratteristiche FV sono unite a quelle RFID dei 106 pazienti del database

producendo un pattern ibrido. Il formato RFID è di 38 bit (Figura 37). L'utilizzo delle funzioni RFID presenta dei vantaggi:

- La creazione di un modello ibrido unendo un piccolo numero di funzioni RFID con le funzioni FV influenzerà la dimensione dei dati del carico utile producendo modelli flessibili e cancellabili. Inoltre, se in futuro si verificassero perdite per qualsiasi motivo, le caratteristiche FV non possono essere distinte dalle caratteristiche RFID;
- I valori dei bit polo e direzione influenzano tutti i bit del modello. Pertanto, l'utilizzo delle funzionalità RFID aggiunge un altro livello di sicurezza nella protezione del modello FV.

Dopo aver prodotto le funzionalità FV e RFID per il primo paziente, queste vengono unite casualmente grazie all'algoritmo di unione. Il modello ibrido è convertito in una stringa binaria che comprende caratteristiche FV, che hanno dimensioni diverse in base alla dimensione delle caratteristiche FV più i 34 bit della caratteristica RFID. Questo modello presenta un primo livello di protezione, in quanto costituito da funzioni FV e RFID, a cui si aggiunge la randomizzazione ottenuta dall'unione casuale delle caratteristiche.

L'hash del pattern ibrido è prodotto utilizzando la funzione MD5 durante la trasmissione dei dati tra il dispositivo di registrazione e il nodo. La dimensione dei dati hash è di 32 bit, come mostrato nella Tabella 5.

User	Hash	User	Hash
1	f4342c9a0cc03318c6e62e6ddff96145	54	a60e639b7f2b6409f319b0f480a01df9
2	1c23f956f98694f4960c8ce6f3641b93	55	d0b665b799f3b5d7ff22c173986fc603
3	1c3478e5357955a05515dc3b7aec1c4d	56	47a1a7803eb60ce716d9f3cf96cd7bab
4	c572cc57f451182c1912214c8ec3f06f	57	4443ba10f6dd7d84ba1f133b3c3799e9
...	.....	...	.....
50	0ca05608926f1de98759babb4e338feb	103	b263dff22d51e3104764583f8c410ef7
51	fe4d0c45e24b32cfe3d64e94c243963f	104	536538ec8f96fccd61971b56a5a7e31b
52	8e803ca9c175e229c7965f8ed001a80c	105	ec4a7bb1537dba515d0fbb44894e4e4f
53	e5e26899dab1aefd942131a59715666f	106	bf8385fa5234a9c42de81a2a05e25247

Tabella 5: Hash dei 106 pazienti del database dopo aver implementato la funzione MD5 sul pattern ibrido

Viene utilizzata la funzione MD5 per hash da 32 bit poiché produce dati di piccole dimensioni, indipendentemente dalla dimensione dell'input (pattern ibrido). L'uso dell'hash garantisce integrità dei dati (requisito CIA): in caso di modifica o manomissione nel payload

durante la trasmissione, questa influenzerà l'hash producendo hash diversi. Ciò rende la modifica evidente durante l'abbinamento nel registro interno del nodo, garantendo l'integrità dei dati segreti (FV del modello ibrido). Il modello ibrido viene protetto da crittografia AES e reso trasmissibile utilizzando la tecnologia blockchain. A questo punto, viene eseguita l'elaborazione sul dispositivo nel punto di accesso e il pattern cifrato, prodotto finale della prima fase, è pronto per essere inviato al lato nodo.

Il payload (pattern del paziente) inviato dal dispositivo nel punto di accesso al lato del nodo comprende un pattern ibrido e crittografato così come l'hash dei pazienti attuali e precedenti. I blocchi di dati vengono inviati dal punto di accesso al lato nodo come una catena; ogni paziente dirige il precedente in una catena, ad eccezione del primo (*genesis patient*), portando l'hash del paziente precedente. La catena può garantire l'integrità dei dati e assicura la loro disponibilità in una rete decentralizzata.

I blocchi di dati comprendono il pattern cifrato per il paziente N, l'hash del paziente N e l'hash del paziente N + 1 e vengono inviati dal dispositivo al lato nodo. L'hash del paziente N+1 viene confrontato con la copia hash del paziente, che viene archiviata nel database del nodo; tutti gli hash che raggiungono il nodo vengono archiviati nel libro mastro (Figura 29). Questo rappresenta il primo filtro utilizzato per verificare l'integrità dei dati ricevuti e l'autenticità della posizione del paziente e può essere utilizzato per memorizzare vari dati del paziente con un alto livello di protezione: un hacker infatti dovrebbe penetrare il 51% dei nodi nella rete per accedere a questo registro, ma questo processo è complicato e costoso. Se i risultati della corrispondenza hash sono veri il processo continua, altrimenti blocca e rifiuta la richiesta del paziente.

I pattern ibridi crittografati vengono archiviati nel database del nodo utilizzando tecniche di steganografia e ciascuno di essi è memorizzato in un'immagine stego. Come mostrato in Figura 36, se il risultato dell'hash matching è vero, allora viene implementata la steganalisi per estrarre il pattern cifrato dall'immagine stego. Successivamente, il modello ibrido viene decifrato utilizzando l'algoritmo AES inverso e le caratteristiche FV sono estratte con l'algoritmo di unione inverso. Infine, viene eseguito il processo di abbinamento tra le caratteristiche FV e le caratteristiche RFID estratte dal database del nodo e quelle dal lato del punto di accesso per decidere se il paziente è autentico o un impostore. L'utilizzo della steganografia migliora il livello di protezione nascondendo le informazioni segrete (pattern crittografato) in un'immagine copertina.

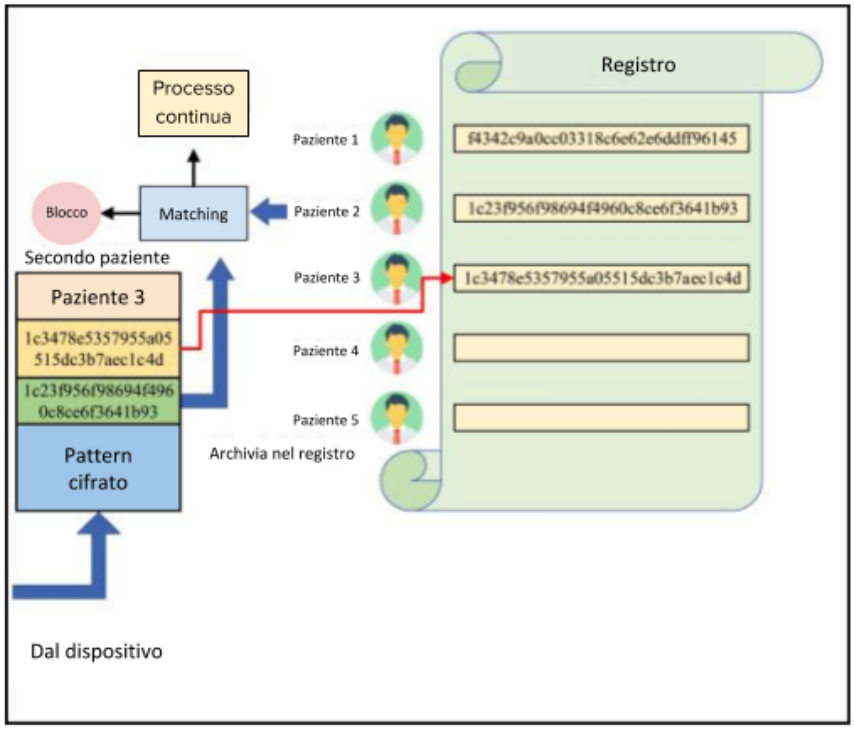

Figura 39: Processo di registrazione e risultati nel nodo [50].

5.5.3 Validazione e valutazione

Per verificare la stabilità del sistema vengono discussi due possibili scenari. Nel primo l'architettura del sistema è costituita dal dispositivo di registrazione e un solo nodo. Viene utilizzata per verificare la sicurezza del sistema contro attacchi *Spoof* e di forza bruta (*Brute-force attacks*). Nel primo caso si immagini un utente malintenzionato che riesce a falsificare il paziente mediante *phishing* e utilizzando un metodo simile per eseguire l'autenticazione biometrica sul nodo remoto. Essendo la biometria umana unica e stabile nel tempo, se un hacker riesce nel suo attacco di spoofing avrà accesso a lungo termine ai dati del paziente. L'uso della blockchain garantisce integrità dei dati e autenticità della posizione, per cui se un utente malintenzionato tenta di attaccare questo framework travestendosi da paziente autorizzato, il nodo scoprirà lo spoofing utilizzando il libro mastro a causa della provenienza esterna alla catena dei dati dell'attaccante. La catena risulta quindi indistruttibile. Per gli attacchi bruti, indovinare il pattern FV è difficile in quanto combinazione di caratteristiche FV e RFID distribuite casualmente. Nel caso in cui un utente malintenzionato possa navigare nella componente biometrica, riducendo l'ambito e supponendo che ogni componente biometrico comprenda 6 bit di chiave di sicurezza (1 bit polo, 1 bit direzione, 4 bit funzione K), questi dovrà indovinare la chiave e il valore della componente biometrica.

Utilizzando un processore da 3,4 GHz, un attacco riuscito richiede più del tempo minimo di 500 anni, indipendentemente dalla protezione che utilizza l'algoritmo AES.

Il secondo scenario invece prevede un'architettura del sistema decentralizzata (Figura 40).

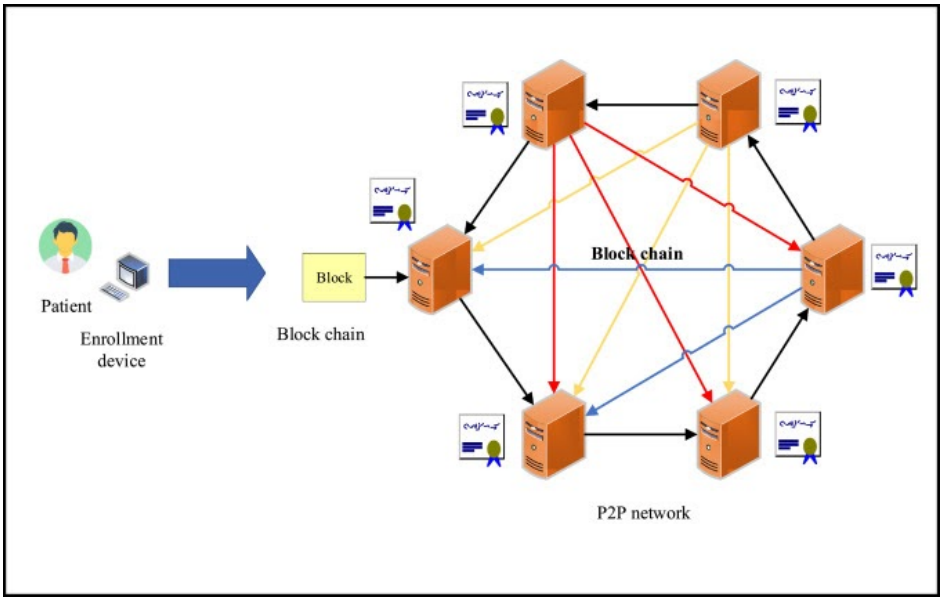

Figura 40: Verifica biometrica FV in una rete decentralizzata (secondo scenario) [50].

Questo meccanismo basato su blockchain viene utilizzato nell'autenticazione del paziente e mira ad eliminare il fallimento al nodo e ridurre le operazioni di comunicazione e verifica quando i pazienti devono acquisire servizi o ottenere simultaneamente l'accesso a più nodi. Durante l'autenticazione, il paziente invia il proprio pattern biometrico FV dal punto di accesso al nodo (destinazione) utilizzando la tecnologia blockchain, proposta con proprietà complete (come hash, libro mastro e blocco di dati). La richiesta del paziente viene inviata contemporaneamente a tutti i nodi della rete: se più del 50% verifica questa richiesta, il paziente ottiene l'accesso al servizio. Ogni nodo ha un libro mastro con cui verificare la blockchain. Se viene rilevato un errore di rete nel nodo di destinazione, la richiesta si sposterà su un altro nodo e seguirà la stessa procedura. Per quanto riguarda l'analisi della sicurezza, questo design ha la stessa resistenza contro lo spoofing e gli attacchi di forza bruta: un utente malintenzionato dovrebbe hackerare il 51% di tutti i nodi della rete per ottenere l'accesso.

Il framework proposto si concentra sul principio di corrispondenza affidabile della biometria FV e sul raggiungimento dei requisiti di sicurezza delle informazioni. Una sua limitazione è la sua incompatibilità con vecchi sistemi basati su altri standard di trasmissione: rispetto ad una blockchain pubblica, come Ethereum, utilizza una *testnet* privata, escludendo eventuali costi di interazione (come le commissioni di transazione). Pertanto, il design proposto non

sarebbe gratuito se implementato su una blockchain pubblica. La convenienza presentata da una blockchain pubblica risiede nei costi di utilizzo ragionevoli rispetto alle spese di licenza, funzionamento e manutenzione del sistema.

Un'analisi della flessibilità e dell'efficacia del sistema proposto ha mostrato come questo supporti il 100% delle specifiche (pattern ibrido e casuale; canale di trasmissione sicuro; pattern cancellabile; pattern modificabile; occultamento del pattern; applicabilità in un'architettura decentralizzata; confidenzialità; integrità; disponibilità), contro il 44,44% dei metodi di riferimento [50]. Si può pensare all'utilizzo di questo sistema di autenticazione nelle situazioni di emergenza: gli operatori sanitari dovrebbero essere in grado di accedere ai dati dell'attività del paziente anche senza che egli ricordi o fornisca una chiave di autorizzazione, oppure i pazienti dovrebbero essere in grado di accedere ai servizi sanitari da casa se necessitano un servizio di Telemedicina. Dovrebbero anche essere in grado di accedere ai sistemi utilizzando la tecnica di verifica FV integrata con blockchain, così che anche medici, pazienti e altri dipendenti possano essere autenticati nel sistema di telemedicina sfruttando un'architettura decentralizzata.

5.6 Blockchain per il contact tracing

Il COVID-19, acronimo di "Coronavirus Disease-2019", è una malattia respiratoria causata dalla sindrome respiratoria acuta grave Coronavirus-2 (SARS-CoV-2). Proprio come il virus dell'influenza, SARS-CoV-2 attacca il sistema respiratorio e causa disturbi come tosse, febbre, affaticamento e affanno, oltre alla perdita temporanea di gusto e olfatto. I primi casi di COVID-19 sono stati registrati nella città di Wuhan nel Dicembre 2019; ad inizio Novembre 2020 il COVID-19 si è diffuso in 219 Paesi, colpendo circa 50 milioni di persone e provocando più di 1 milione di vittime [63]. Sebbene alcuni studi indichino che il SARS-CoV-2 possa essere suscettibile al calore e alla luce ultravioletta (UV) [64], ad oggi non esiste un trattamento o un vaccino specifico per l'infezione; perciò l'Organizzazione Mondiale della Sanità (OMS) e i dipartimenti della salute di quasi tutti i Paesi raccomandano il distanziamento sociale e la quarantena come le migliori medicine per combattere la pandemia di COVID-19.

Per quanto riguarda il meccanismo di diffusione, l'analisi di 75.465 casi di COVID-19 in Cina ha rivelato che il virus viene trasmesso principalmente via *droplet* [65], in quanto le goccioline frutto di starnuti e colpi di tosse possono coprire fino ad 1,8 m di distanza. Sebbene le persone sintomatiche siano state identificate come la fonte primaria di trasmissione di SARS-CoV-2, esiste anche la possibilità di trasmissione attraverso soggetti asintomatici, più difficili da individuare ed isolare. Le circostanze più frequenti al seguito delle quali si verifica un contagio sono [66]:

- il contatto con un soggetto positivo a meno di 1 m di distanza per più di 15 minuti;
- l'erogazione di assistenza sanitaria a pazienti affetti da COVID-19 senza l'utilizzo di dispositivi di protezione individuale adeguati;
- la condivisione degli ambienti (casa, ufficio, trasporto) con un soggetto positivo.

Appare evidente quindi come la tracciabilità sistematica dei contatti (*contact tracing*) e l'osservanza di un autoisolamento precauzionale rappresentino delle componenti chiave nella lotta alla pandemia. Più Paesi hanno adottato misure differenti per contrastare la diffusione del virus come l'utilizzo di applicazioni mobili per i fornitori del servizio sanitario [67] o per i cittadini, l'analisi dei registri telefonici o lo sfruttamento di tecnologie hardware come smartband [68], telecamere, scanner termici e droni [69]. Tutti questi sistemi presentano possibili falle circa la gestione della privacy dei soggetti; per questo, gli autori hanno proposto un modello di sistema per il contact tracing che integra la tecnologia blockchain.

5.6.1 Descrizione

Il modello proposto da Garg et al. raccoglie le informazioni sui movimenti e i contatti in modo assolutamente anonimo, sfruttando un sistema hardware IoT. Nello specifico un trasmettitore RFID passivo, indossabile da chiunque, anche animali, senza la necessità di uno smartphone per il tracciamento anonimo. Le letture vengono prese dal lettore RFID, che può essere in un edificio o in dispositivi di alimentazione e le informazioni di prossimità acquisite vengono memorizzate nel relativo smart contract. In Figura 41 è riportata l'architettura del sistema.

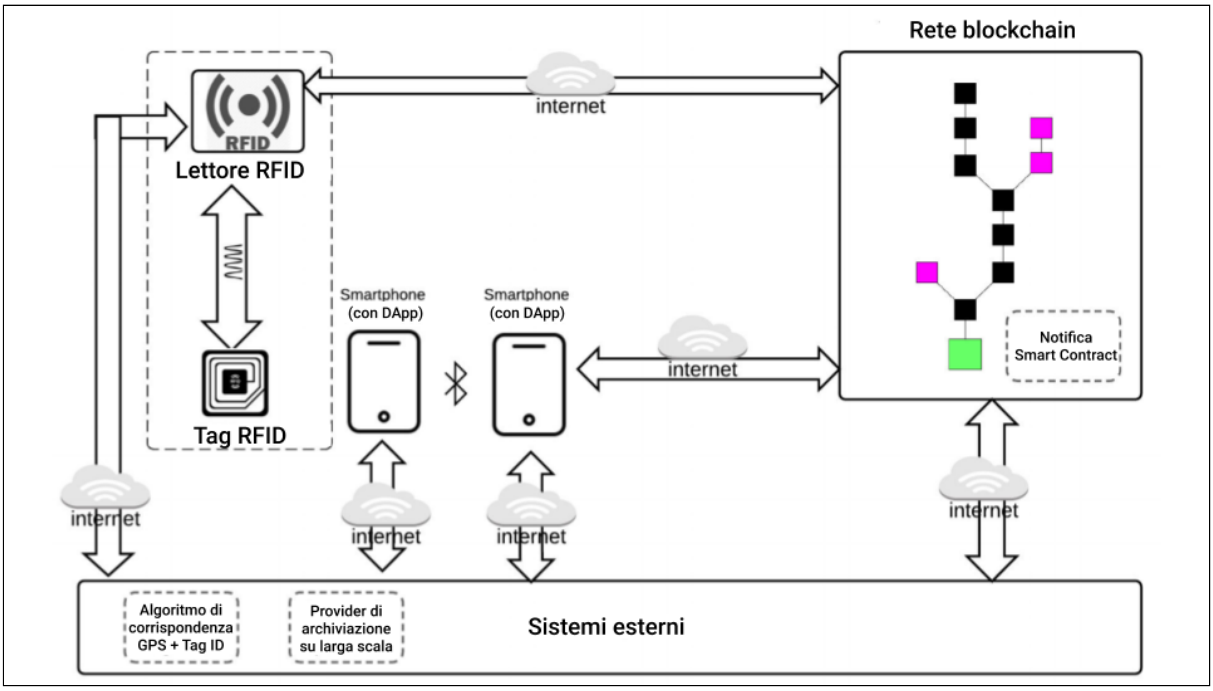

Figura 41: Architettura del sistema di contact tracing. I dati fluiscono dal tag RFID al lettore, infine alla blockchain via Internet. Sempre via Internet, i dati di prossimità raccolti dalle DApp (app mobile per i cittadini o per fornitori del servizio sanitario) vengono inviati alla blockchain. I sistemi esterni (lettore RFID, sorveglianza sanitaria, droni e telecamere) possono essere sistemi in grado di memorizzare informazioni aggiuntive per altri scopi e consentono il collegamento delle informazioni solo su richiesta. La blockchain permette di registrare i dispositivi mobili anonimamente, e le informazioni registrate possono essere usate per avvisare gli utenti in possesso di uno smartphone o di un tag RFID di un contatto con un soggetto positivo [51].

L'implementazione delle DApp per i cittadini può realizzarsi grazie ad una rete mobile a maglia, dove i dispositivi condividono le informazioni sulla posizione direttamente, senza un hub, via Bluetooth o WiFi Direct, oppure con l'acquisizione dei dati GPS, più precisi, in modo da consentire un tracciamento spazio-temporale più dettagliato. La notifica di contatto non è altro che un messaggio all'interno dell'applicazione, trasmesso con protocollo HTTP.

Il tag RFID utilizzato è passivo di sola lettura, economico e a bassa potenza, dotato di un numero di serie univoco, utilizzato come meccanismo di accesso alla catena di

aggiornamento della posizione. Il tag scambia il suo numero di serie con i dispositivi ricevitori se interrogato. Questi dispositivi, alimentati da rete elettrica o batteria, possono essere localizzati in posizioni strategiche fisse oppure su oggetti in movimento come le automobili. Le automobili stesse sono dotate di tag che possono essere letti all'ingresso di zone specifiche, ad esempio ai caselli. In questo modo si costruisce una rete efficace nella triangolazione. Durante l'interazione fra il tag e il ricevitore, questo identifica e calcola anche la distanza relativa. Le informazioni raccolte quindi sono:

- numero di serie del tag;
- data e ora;
- posizione;
- prossimità.

Chiunque sia iscritto alla blockchain ed abbia avuto un contatto con un portatore o con la sua automobile riceve una notifica con il numero seriale del tag RFID.

Il sistema adotta una blockchain pubblica basata sugli smart contract. Ne sono stati testati ed implementati tre nel *Remix Integrated Development Environment* (IDE) [70] per le operazioni di registrazione, aggiornamento e autorizzazione, mentre i contratti per l'identificazione e la notifica sono ancora in fase di test.

Al momento della registrazione (Figura 42), non vengono raccolte informazioni e sul dispositivo avviene la generazione della chiave pubblica e di quella privata. Una chiave viene registrata come chiave pubblica sulla blockchain tramite eventi per l'accesso agli smart contract, l'altra viene archiviata sul dispositivo, con possibilità di backup.

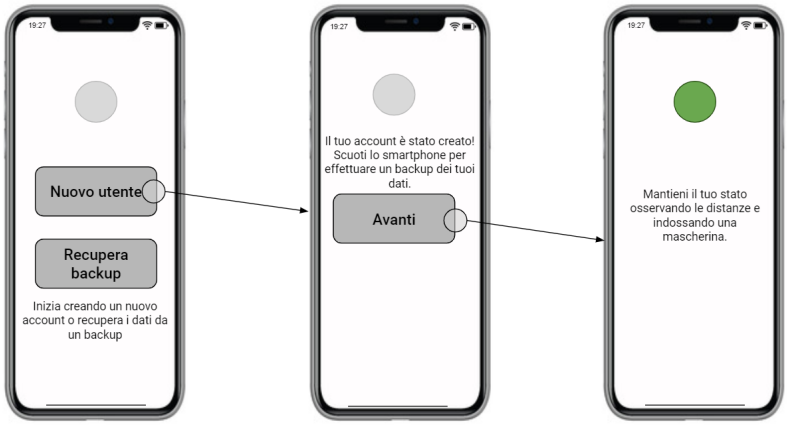

Figura 42: Processo di registrazione. Quando si seleziona la voce 'Nuovo utente', vengono generate due chiavi e una viene designata in modo casuale come chiave pubblica e contrassegnata come indirizzo dell'entità generante [51].

Lo smart contract per il processo di registrazione, scritto in linguaggio *Solidity*, viene generato direttamente nell'applicazione dell'utente oppure in un lettore RFID. L'algoritmo del contratto di autorizzazione è riportato in Figura 43.

Input: Serial number of tag or IMEI of phone
"serial_imei"; $S = \{s_1, s_2, \ldots, s_n\}$
Output: The timestamp and the hash of serial or phone
IMEI, "pub" (T, H); $H = \{h_1, h_2, \ldots, h_n\}$,
$T = \{t_1, t_2, \ldots, t_n\}$

```
1 pragma solidity 0.4.25;
2 contract registration {
    3 uint private serial_imei;
    4 bytes32 public pub;
    5 uint timestamp;
    6 event register(
        7 uint timestamp,
        8 bytes32 pub
        9 );
   10 function captureRFID(uint _s_i) public{
      11 timestamp = now;
      12 serial_imei = _s_i;
      13 pub = sha256(abi.encode(serial_imei));
      14 emit register(timestamp, pub);
      15 }
   16 function enroll() public {
      17 timestamp = now;
      18 pub = sha256(abi.encode(msg.sender));
      19 emit register(timestamp, pub);
   20 }
   21 }
```

Figura 43: Il contratto è denominato '*registration*' e la versione Solidity usata è 0.4.25 o superiore. La variabile '*pub*' può essere utilizzata come hash del tag RFID o come hash del numero IMEI di un dispositivo mobile, mentre il timestamp viene generato al richiamo dello smart contract. Le funzioni '*captureRFID ()*' caturano il numero di serie del tag RFID o dell'IMEI del telefono; la funzione '*enroll ()*' viene richiamata quando un cittadino desidera registrarsi alla blockchain [51].

Lo smart contract di aggiornamento (Figura 44) inserisce le informazioni sulla blockchain a partire dal dispositivo mobile o dal ricevitore RFID in seguito alla registrazione iniziale. Il processo di aggiornamento si ripete ogni 5 minuti e funzionerà soltanto per i dispositivi mobili partecipanti e che utilizzano le applicazioni mobili compatibili. La chiamata avviene in background, in quanto l'utente ha già fornito tutti i consensi durante la registrazione. Le informazioni sulla posizione vengono acquisite ogni 10 minuti, e il caricamento sulla blockchain ogni 20, in modo da raccogliere i dati frequentemente senza impattare eccessivamente sull'autonomia del dispositivo. L'utente viene identificato nella blockchain soltanto dalla chiave pubblica, che ricorda chi l'ha generata e le altri chiavi pubbliche con le quali è entrata in contatto. L'applicazione non traccia la posizione effettiva del dispositivo, bensì la distanza tra gli utenti che ne fanno uso. La registrazione avviene non appena la

distanza scende al di sotto dei 2 m, anche se i dispositivi fossero già connessi: le informazioni ottenute servono per definire la durata del contatto, mentre la distanza non viene memorizzata, ma utilizzata per registrare i numeri di serie.

Input: Serial number of tag $S = \{s_1, s_2, \ldots, s_n\}$ or IMEI of phone $I = \{i_1, i_2, \ldots, i_n\}$
"serial_imei";
Output: The timestamp and the hash of serial or phone IMEI, (T, H); $H = \{h_1, h_2, \ldots, h_n\}$, $T = \{t_1, t_2, \ldots, t_n\}$

```
1 pragma solidity 0.4.25;
2 contract update {
3 uint private serial_imei;
4 uint timestamp;
5 bytes32 private H;
6 bytes32 private pub;
7 event update_serial(
8 uint timestamp,
9 bytes32 pub
10 );
11 event update_imei(
12 uint timestamp,
13 bytes32 pub,
14 bytes32 H
15 );
16 function log_serial(uint_s_i)
17 public{
18 serial_imei = _s_i;
19 pub =
20 sha25(abu.encode(serial_imei));
21 timestamp = now;
22 emit update_serial(timestamp, pub);
23 }
24 function
25 log_imei(uint_s_i, uint_H)
26 public{
27 serial_imei = _s_i;
28 H = sha2(abi.encode(_H));
29 pub =
30 sha256(abi.encode(serial_imei));
31 timestamp = now;
32 emit update_imei(timestamp, H, pub);
33 }
34 }
```

Figura 44: Algoritmo smart contract '*update.sol'* per il processo di aggiornamento. In base al metodo di chiamata a seconda del dispositivo: (1) se un ricevitore RFID accede alla blockchain per conto di un tag su un animale, verrà chiamata la funzione '*log serial ()*' con il numero di serie come parametro; (2) se lo smart contract viene richiamato via Internet da un telefono, quest'ultimo richiamerà la funzione '*log_imei*' fornendo il proprio IMEI e un parametro H risultato della concatenazione di tutti i seriali Bluetooth collegati al telefono [51].

Lo smart contract per l'autorizzazione (Figura 46) è configurato per i dispositivi a disposizione delle autorità sanitarie che possono contrassegnare un utente come caso "probabile", "sospetto" o "confermato". Ogni utente presenta uno stato predefinito ('*covid_status = 0*') che può essere modificato dall'operatore sanitario, mediante l'interfaccia in Figura 45: se clicca su "positivo" il flag di '*covid_status'* verrà settato su 1, registrando tutti gli utenti che hanno avuto contatti con il soggetto come positivi. Il processo inverso avviene nel momento in cui il paziente si ristabilisce, e l'operatore lo registra come "negativo" ('*covid_status = 0'*).

Gli autori hanno implementato il modello distribuendo i tre smart contract nell'ambiente di test per la blockchain Ethereum Remix IDE, con tre indirizzi nodo su uno stesso computer. I risultati delle simulazioni hanno mostrato come le transazioni richiedano meno di 1 secondo per completarsi nell'ambiente Remix, mentre circa 25 secondi nella rete pubblica Ethereum; l'esecuzione di un contratto costa circa 1,95 $, mentre richiamarne o modificarne una funzione circa 0,34 $.

Figura 45: Interfaccia dell'applicazione per l'autorità sanitaria, che dichiara un soggetto negativo o positivo al COVID-19 in seguito agli opportuni esami [51].

Input: Covid status event log
Output: The timestamp and the hash of serial or phone IMEI, and status (T, H, CS);
$T = \{t_1, t_2, \ldots, t_n\}, H = \{h_1, h_2, \ldots, h_n\},$
$CS = \{cs_1, cs_2, \ldots, cs_n\}$

```
1 pragma solidity 0.4.25;
2 contract authorization {
    3 uint private serial_imei;
    4 uint timestamp;
    5 address pub_key;
    6 uint covid_status = 0;
    7 event update_positive(
        8 uint timestamp,
        9 address pub_key,
       10 uint covid_status
       11 );
   12 event update_negative(
       13 uint timestamp,
       14 address pub_key,
       15 uint covid_status
       16 );
   17 function log_positive(address pub_key) public{
       18 pub_key = _pub_key;
       19 covid_status = 1;
       20 timestamp = now;
       21 emit update_positive;
       22 (timestamp, pub_key, covid_status);
       23 }
   24 function log_negative(address pub_key) public{
       25 pub_key = _pub_key;
       26 covid_status = 0;
       27 timestamp = now;
       28 emit update_negative;
       29 (timestamp, pub_key, covid_status);
       30 }
31 }
```

Figura 46: Algoritmo dello smart contract '*authorization.sol'* per la modifica dello stato Covid dell'utente (se 0 negativo, se 1 positivo) [51].

5.6.2 Vantaggi e limitazioni

Il modello proposto offre evidenti miglioramenti rispetto ai sistemi di tracciamento classici, soprattutto quelli che prevedono la consultazione dei registri telefonici. Inoltre rispetto ad altri sistemi che adottano delle soluzioni hardware come smartband, i tag RFID risultano più economici e facili da implementare e non richiedono cariche continue. I lettori dei tag archiviano le informazioni protette da hash nella blockchain e da queste non si può risalire all'utente. Gli utenti che soddisfano i criteri di contatto impostati nello smart contract riceveranno una notifica sulla loro applicazione con lo stato corrente: verde se non hanno avuto contatti con soggetti positivi al COVID-19, giallo invece se c'è stato un contatto che richieda un test o un periodo di autoisolamento. Il sistema inoltre è in grado di inoltrare una

notifica sull'applicazione dell'utente se questi supera un valore soglia di potenziali contatti in una zona precisa. Il modello proposto elimina la necessità di follow-up durante il periodo di quarantena dei contatti e la notifica di prossimità viene inoltrata automaticamente dallo smart contract. L'utilizzo della blockchain e di un design decentralizzato garantiscono privacy dei dati, che non vengono gestiti da un ente governativo, e scalabilità del sistema; le dimensioni dei dati non richiedono l'utilizzo di spazi di archiviazione esterni alla catena e il costo medio di una registrazione è contenuto (0,34 $). Per migliorare l'accuratezza del tracciamento, si può combinare la metodologia vista sopra con la triangolazione delle celle, qualora gli utilizzatori del servizio fornissero accesso al registro delle telefonate.

Sebbene offra vantaggi rispetto a tecniche di tracciamento più comuni, il sistema presentato manca ancora dei contratti di identificazione e notifica ed è basato su un prototipo di smart contract che non implementa soluzioni raffinate per la sicurezza. Inoltre per poter funzionare bene richiederebbe un'installazione capillare di tag e lettori RFID, complessa soprattutto nelle aree tecnologicamente sottosviluppate.

6. Considerazioni finali

La recente diffusione a livello globale del virus SARS-CoV-2 ha evidenziato la necessità di sviluppare e consolidare forme di assistenza sanitaria solide e affidabili. In particolare, una maggiore adozione della Telemedicina potrebbe consentire una comunicazione sicura con medici e specialisti sanitari attraverso canali virtuali, riducendo il numero di potenziali contatti per i pazienti, con un conseguente calo di accessi e ricoveri nelle strutture sanitarie, già messe in ginocchio dalla diffusione del virus. Per andare oltre i limiti che caratterizzano i principali sistemi di Telemedicina esistenti, basati su design prettamente centralizzati, l'adozione della tecnologia blockchain appare uno step necessario.

Dall'analisi dei sistemi effettuata nel Capitolo 5, appare evidente come la gestione decentralizzata delle cartelle cliniche e dei dati sanitari dei pazienti garantisca loro sicurezza e privatezza, a prescindere che il servizio sia di Telemedicina specialistica (DermoNet), di Telechirurgia (AaYusH), di Telemonitoraggio (HapiChain) o di autenticazione biometrica. Nessuno dei sistemi citati però considera le potenziali incongruenze con il GDPR, che dal Maggio 2018 regolamenta la gestione dei dati sensibili da parte di enti e aziende, costituendo un potenziale ostacolo alla diffusione di questi sistemi. Dovendo attenersi al regolamento per la protezione dei dati, occorre che sviluppatori e ricercatori forniscano una definizione chiara di "dato sensibile" per gli utenti blockchain e che superino l'ostacolo della figura del DPO. L'adozione di una blockchain Consortium, come in SHAREChain, o privata rappresenta forse la soluzione ideale per i servizi di Telemedicina.

In realtà gran parte dei sistemi di Telemedicina fa uso della blockchain pubblica Ethereum e degli smart contract. Questi offrono un alto grado di automazione, ma bisogna tener conto di eventuali bug e vulnerabilità nei contratti che possono influenzare in maniera significativa il corretto funzionamento del sistema. Gli smart contract Solidity in particolare sono vulnerabili agli attacchi di rientro (*Re-entracy attacks*) [71]: subendo questo attacco, un contratto che ha privilegi esclusivi di comunicazione può alterare la cartella clinica elettronica di un paziente, oppure accedere ai fondi presenti nel portafoglio di un utente. I ricercatori hanno proposto diversi tool diagnostici per identificare le caratteristiche vulnerabili degli smart contract e aiutare gli sviluppatori a proporre contromisure adeguate [72], tuttavia le soluzioni proposte non sono adeguate per identificare tutti i tipi di vulnerabilità. È necessario adottare misure preventive per testare rigorosamente i contratti in più casi d'uso e con più tool diagnostici prima di poter procedere alla loro implementazione.

Il supporto dell'interoperabilità delle piattaforme blockchain facilita agli utenti la comunicazione tra loro senza interruzioni, senza richiedere intermediari per la traduzione e l'inoltro delle transazioni: per esempio, una piattaforma che supporti l'interoperabilità può aiutare gli operatori sanitari a utilizzare i token Bitcoin per le transazioni commerciali sulla rete blockchain di Ethereum. Tuttavia, l'architettura di piattaforme blockchain interoperabili è impegnativa a causa di vari problemi, come le differenze nei linguaggi supportati e nei protocolli di consenso delle piattaforme blockchain. Sebbene tra le piattaforme illustrate SHAREChain garantisca un ottimo grado di interoperabilità attraverso l'introduzione dello standard FHIR, la gran parte dei servizi di Telemedicina non offre un livello tale da garantire la migliore assistenza possibile per i pazienti.

I sistemi di Telemedicina richiedono uno stretto coordinamento tra gli attori che partecipano ai processi sanitari, così da mantenere un'anamnesi coerente e aggiornata del paziente e ridurre gli errori di diagnosi. Per questo si generano quantità enormi di dati, che influiscono sulle commissioni di transazione, sui tempi di attesa per l'approvazione e sui requisiti di archiviazione nel registro distribuito. Alcuni sistemi non generano grossi quantitativi di dati, ad esempio quello per il contact tracing proposto da Garg et al. non soffre di problemi di scalabilità, pur tenendo conto del fatto che gli algoritmi per gli smart contract non sono ancora definitivi. AaYusH al contrario per poter garantire massima efficienza e sicurezza necessarie in un sistema di Telechirurgia, deve rispettare tempi strettissimi nello scambio di dati e informazioni, richiedendo spazi di archiviazione importanti. Ricorrere a storage "esterni" come i data lake o proporre nuovi design di blockchain intervenendo sui meccanismi di lettura e di scrittura dei dati all'interno dei blocchi [73] costituiscono possibili soluzioni utili mitigare il problema della scalabilità, di cui programmatori e ricercatori devono sempre tenere conto.

Il GDPR, le possibili vulnerabilità degli smart contract, l'interoperabilità e la scalabilità costituiscono limiti aggirabili in sanità attraverso l'introduzione di soluzioni progettuali innovative oppure con l'adozione di una blockchain Consortium o privata anziché pubblica. I veri ostacoli che la blockchain deve oltrepassare per affermarsi nel campo della Telemedicina, e non solo, sono la scarsa conoscenza della tecnologia al grande pubblico, al paziente abituato ai metodi di erogazione tradizionale dei servizi sanitari, e nella mancanza di fiducia e coraggio da parte delle grandi imprese nel ristrutturare i propri servizi attorno a sistemi decentralizzati. Nonostante lo scorso anno sia stata registrata una crescita pari al 56% dei nuovi progetti di blockchain in tutto il mondo (Italia compresa dove i nuovi investimenti

hanno sfiorato i 30 milioni euro), gran parte delle proposte è costituita di soli annunci, principalmente rivolti al settore finanziario, alla Pubblica Amministrazione e al settore agro-alimentare [74].

Il settore sanitario, meno esplorato, gioverebbe sicuramente di maggiori investimenti in ambito blockchain. Può rappresentare infatti uno strumento determinante nella lotta contro il COVID-19, per la creazione di un grande registro di dati relativi alla pandemia, accessibile in tutto il mondo, che potrebbe dare una grossa spinta per lo sviluppo di terapie e vaccini. L'attuale contesto di grande difficoltà può rappresentare un'occasione, uno stimolo per sviluppatori, ricercatori, grandi imprese e Governi ad andare oltre i limiti sopra descritti, uniti alle problematiche di disuguaglianza digitale che affligge principalmente i Paesi sottosviluppati, ed investire concretamente nella blockchain nell'ambito della sanità e della Telemedicina.

Bibliografia

1. Nakamoto S. “Bitcoin: A peer-to-peer electronic cash system”, 2008.

2. Capaccioli G. “Come nasce la Blockchain”, 2019 [Online] https://affidaty.io/blog/it/2019/04/come-nasce-la-blockchain/ [Consultato il 2 Ottobre 2020].

3. Haber S, Stornetta W.S. “How to time-stamp a digital document”. *Journal of Cryptology*, Issue 3, 99–111, 1991.

4. Kanare H. M. “Writing the laboratory notebook”, 1985.

5. Bayer, Dave & Haber, Stuart & Stornetta, W. “Improving the Efficiency and Reliability of Digital Time-Stamping”, 1999.

6. Davis J. “The Crypto-Currency: Bitcoin and its mysterious Inventor”. *The New Yorker, 10/10/2011*[Online]https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency [Consultato il 3 Ottobre 2020].

7. CoinMarketCap. Crypto-Currency Market Capitalizations. [Online] https://coinmarketcap.com/ [Consultato il 28 Ottobre 2020].

8. Calvery JS. “Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury”, 2013.

9. Gupta V. “A Brief History of Blockchain”, 2017. [Online] https://hbr.org/2017/02/a-brief-history-of-blockchain [Consultato il 4 Ottobre 2020].

10. Seffinga J, Lyons L, Bachmann A. “The Blockchain (R)evolution - The Swiss Perspective”, *Deloitte*, 2017.

11. MacIver K. “I-CIO”, 2016. [Online]https://www.i-cio.com/big-thinkers/don-tapscott/item/from-the-internet-of-information-to-the-internet-of-value [Consultato il 4 Ottobre 2020].

12. Lamport, Leslie & Shostak, Robert & Pease, Marshall. “The Byzantine Generals Problem”, 2002.

13. Bellini M. “Blockchain: cos’è, come funziona e gli ambiti applicativi in Italia”, 2017. [Online]https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/ [Consultato il 5 Ottobre 2020].

14. Warburg B. “How the blockchain will radically transform the economy”, 2016.

15. Casino F, Thomas K. Dasaklis, Constantinos Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues”, *Telematics and Informatics*, Volume 36, 2019, Pages 55-81, 2019.

16. Ølnes S, Ubacht J, Janssen M. “Blockchain in government: Benefits and implications of distributed ledger technology for information sharing”, *Government Information Quarterly*, Volume 34, Issue 3, Pages 355-364, 2017.

17. Lake J. “Understanding cryptography’s role in blockchains”, 2019. [Online] https://www.comparitech.com/crypto/cryptography-blockchain/ [Consultato il 6 Ottobre 2020].

18. Kuo T-T, Kim H-E, Ohno-Machado L. “Blockchain distributed ledger technologies for biomedical and health care applications”, *J Am Med Inform Assoc*. 24 (6): 1211-1220, 2017.

19. Tar A. “Proof-of-Work, Explained”, 2018. [Online] https://cointelegraph.com/explained/proof-of-work-explained [Consultato il 6 Ottobre 2020].

20. Buterin V. “On Public and Private Blockchains”, *Ethereum Blog*, 2015.

21. Valsecchi V. “La classificazione delle Blockchain: pubbliche e private”, 2019. [Online] https://www.spindox.it/it/blog/la-classificazione-delle-blockchain/ [Consultato il 10 Ottobre 2020].

22. Szabo N. “Smart Contracts: Building Blocks for Digital Markets”, *Extropy*, Issue 16, 1996.

23. Solidity Documentation, 2017. [Online] https://solidity.readthedocs.io/en/develop/ [Consultato il 12 Ottobre 2020].

24. Binance Academy. “History of Blockchain”, 2020. [Online] https://academy.binance.com/it/articles/history-of-blockchain [Consultato il 12 Ottobre 2020].

25. Hasse F, von Perfall A, Hillebrand T, Smole E, Lay L, Charlet M. “Blockchain - an opportunity for energy producers and consumers?”, *PwC*, 2016.

26. Bennett B. “Using Telehealth as a Model for Blockchain HIT Adoption”, *Telehealth and Medicine Today*, 2 (4), 2018.

27. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.[Online]https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016R0679 [Consultato il 16 Ottobre 2020].

28. Del Fungo M. “Blockchain e GDPR”, 2019. [Online] https://www.smart4ius.eu/blockchain-e-gdpr/ [Consultato il 18 Ottobre 2020].

29. McMullen G. “Blockchain & Law in 2017: Finally friends or still foes?”, 2017. [Online] https://medium.com/ipdb-blog/blockchain-and-law-in-2017-f535cb0e06c4 [Consultato il 19 Ottobre 2020].

30. Rujtes A. “Blockchain and GDPR: better safe than sorry”, 2018. [Online] https://www.linkedin.com/pulse/blockchain-gdpr-better-safe-than-sorry-arne-rutjes/?trk=v-feed [Consultato il 20 Ottobre 2020].

31. Tapscott D, Tapscott A. “Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World”, 2016

32. Swan M. “Blockchain: Blueprint for a new economy”, 2015.

33. Zammit J. “Blockchain Use Cases In Business”, University of Malta, 2018.

34. Ivan D. “Moving Toward a Blockchain-Based Method for the Secure Storage of Patient Records”, *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, 2016.

35. Petre A. “Blockchain uses in healthcare”, 2017. [Online]https://www.linkedin.com/pulse/blockchain-use-cases-healthcare-anca-petre [Consultato il 21 Ottobre 2020].

36. Funk E, Riddell J, Ankel F, Cabrera D. “Blockchain Technology: A Data Framework to Improve Validity, Trust, and Accountability of Information Exchange in Health Professions Education”, *Acad Med.* 93(12), 2018.

37. Griggs K, Ossipova O, Kohlios C, Baccarini A, Howson E, Hayajneh T. “Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. Journal of medical systems”, *Journal of Medical Systems,* 42, 2018.

38. https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/ [Consultato il 28 Ottobre 2020].

39. Linn L, Koo M. “Blockchain for health data and its potential use in health IT and Healthcare related research”. https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf

40. Ministero della Salute. “Telemedicina, Linee di indirizzo nazionali”. http://www.salute.gov.it/imgs/C_17_pubblicazioni_2129_allegato.pdf

41. “Research and Markets, Global Telemedicine Market Outlook 2022 Report”, 2020. [Online]https://www.researchandmarkets.com/reports/3766749/global-telemedicine-marketoutlook-2022 [Consultato il 24 Ottobre 2020].

42. Sarhan F. “Telemedicine in healthcare 1: Exploring its uses, benefits, and disadvantages”, *Nursing times*, 105, 10-3, 2009.

43. Hjelm N. M. “Benefits and drawbacks of telemedicine”, *J Telemed Telecare*, 11 (2): 60-70, 2005.

44. Ahmad R, Salah K, Jayaraman R, Yaqoob I, Ellahham S, Omar M. “The Role of Blockchain Technology in Telehealth and Telemedicine”, 2020.

45. Mannaro K, Baralla G, Pinna A, Ibba S. “A Blockchain Approach Applied to a Teledermatology Platform in the Sardinian Region (Italy)”, 2018

46. Kordestani H, Barkaoui K, Zahran W. “HapiChain: A Blockchain-based Framework for Patient-Centric Telemedicine”, *IEEE 8th International Conference on Serious Games and Applications for Health (SeGAH)*, Vancouver, BC, Canada, 2020, pp. 1-6.

47. Kordestani H, Mojarad R, Chibani A, Osmani A, Amirat Y, Barkaoui K, Zahran W. “Hapicare: A Healthcare Monitoring System with Self-adaptive Coaching Using Probabilistic Reasoning”, *IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, Abu Dhabi, United Arab Emirates, 2019, pp. 1-8.

48. Li A-R, Kim M-G, Kim I-K. “SHAREChain: Healthcare data sharing framework using Blockchain-registry and FHIR”, *IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, San Diego, CA, USA, 2019, pp. 1087-1090.

49. Gupta R, Shukla A, Tanwar S. “AaYusH: A Smart Contract-based Telesurgery System for Healthcare 4.0”, *IEEE International Conference on Communications Workshops (ICC Workshops)*, Dublin, Ireland, 2020, pp. 1-6.

50. Mohsin A.H, Zaidan A.A, Zaidan B.B, Albahri O.S, Albahri A.S, Alsalem M.A, Mohammed K.I. “Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication”, *Computer Standards & Interfaces*, Volume 66, 2019.

51. Garg L, Chukwu E, Nasser N, Chakraborty C, Garg G. “Anonymity Preserving IoT-Based COVID-19 and Other Infectious Disease Contact Tracing Model”, *IEEE Access*, vol. 8, pp. 159402-159414, 2020.

52. Mahmud H. “Modeling Virtual Organization for Home Healthcare Using UML”, *International Journal of Computer Sciences and Engineering*, Issue 4, pp. 22-31, 2016.

53. Benet J. “IPFS - Content Addressed, Versioned, P2P File System”, 2014.

54. Zhuang Y, Sheets L, Shae Z, Tsai J, Shyu C. “Applying Blockchain Technology for Health Information Exchange and Persistent Monitoring for Clinical Trials”, *AMIA Annu Symp Proc,* 1167-1175, 2018.

55. Kim M. G, Lee A. R, Kim I. K. “CHDC: Common Hospital Data Connector for Exchanging Medical Information”, *41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, Berlin, Germany, 2019, pp. 3478-3481.

56. Hathaliya J. J, Tanwar S, Tyagi S, Kumar N. “Securing electronics healthcare records in healthcare 4.0: A biometric-based approach”, *Computers & Electrical Engineering,* Volume 76, 2019, pp. 398-410.

57. Bonaci T, Herron J, Yusuf T, Yan J, Kohno T, Chizeck H. J. “To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots”, arXiv Preprint arXiv:1504.04339, 2015.

58. Gupta R, Tanwar S, Tyagi S, Kumar N, Obaidat M. S, Sadoun B. “Habits: Blockchain-based telesurgery framework for healthcare 4.0”, *International Conference on Computer, Information and Telecommunication Systems (CITS)*, Beijing, China, 2019, pp. 1-5.

59. von Solms R, van Niekerk J. “From Information security to cyber security”, *Computers & Security*, Volume 38, Pages 97-102, 2013.

60. Mathur N, Bansode R. “AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection”. *Procedia Computer Science*, 79, 1036-1043, 2016.

61. Kundi D.S, Aziz A, Ikram N. “A high performance ST-Box based unified AES encryption/decryption architecture on FPGA”, *Microprocessors and Microsystems*, Volume 41, Pages 37-46, 2016.

62. Lu Y, Xie S.J, Yoon S, Wang Z, Park D.S. “An available database for the research of finger vein recognition”, *6th International Congress on Image and Signal Processing (CISP)*, Hangzhou, pp. 410-415, 2013.

63. [Online] https://www.worldometers.info/coronavirus/ [Consultato il 9 Novembre 2020].

64. Cascella M, Rajnik M, Cuomo A, Dulebohn S.C, Di Napoli R. “Features, evaluation and treatment coronavirus (COVID-19)”, [Updated 2020 Oct 4]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2020 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK554776/

65. WHO. “Modes of Transmission of Virus Causing COVID-19: Implications for IPC Precaution Recommendations”, 2020.

66. WHO. “Considerations for Quarantine of Individuals in the Context of Containment for Coronavirus Disease (COVID-19)”, 2020.

67. WHO. “Report of the WHO-China Joint Mission on Coronavirus Disease 2019 (COVID-19)”, 2020.

68. Vaas L. “Location-Tracking Wristbands Required on All Incoming Travelers to Hong Kong”, 2020. [Online] https://nakedsecurity.sophos.com/2020/03/20/location-tracking-wristbands-required-on-all-incoming-travelers-to-hong-kong/ [Consultato il 30 Ottobre].

69. UniSA Working on ‘Pandemic Drone’ to Detect Coronavirus, 2020. [Online] https://www.unisa.edu.au/Media-Centre/Releases/2020/unisa-working-on-pandemic-drone-to-detect-coronavirus/ [Consultato il 2 Novembre 2020].

70. [Online]https://remix.ethereum.org/#optimize=false&evmVersion=null&version=soljson-v0.6.6+commit.6c089d02.js [Consultato il 4 Novembre 2020]

71. Shahda W. “Protect Your Solidity Smart Contracts From Reentrancy Attacks”, 2019 [Online]https://medium.com/coinmonks/protect-your-solidity-smart-contracts-from-reentrancy-attacks-9972c3af7c21 [Consultato il 4 Novembre 2020].

72. Hu Y.-C, Lee T.-T, Chatzopoulos D, Hui P. “Analyzing smart contract interactions and contract level state consensus”, *Concurrency and Computation: Practice and Experience*, 32 (12), 2019.

73. Mazlan A. A, Daud S. M, Sam S. M, Abas H, Rasid S. Z. A, Yusof M. F. “Scalability Challenges in Healthcare Blockchain System - A Systematic Review”, *IEEE Access*, vol. 8, pp. 23663-23673, 2020.

74. [Online]https://www.osservatori.net/it/ricerche/comunicati-stampa/cresce-la-blockchain-488-progetti-nel-mondo-plus56-nel-2019-e-grandi-opportunita-per-litalia [Consultato il 15 Ottobre 2020].

Ringraziamenti

Al termine di questo lavoro di Tesi, trovo doveroso ringraziare tutte le persone che mi hanno accompagnato lungo il percorso universitario, contribuendo al raggiungimento di questo importante traguardo.

In primis ringrazio la Prof.ssa Monica Visintin. La grande stima che nutro verso di Lei non è soltanto figlia della profonda conoscenza e della competenza provate negli anni, sin dai tempi del corso di Analisi dei Segnali, ma soprattutto della sensibilità e umanità dimostrate nei miei confronti in un momento particolare della mia carriera.

Ringrazio la mia famiglia, esempio costante di forza e caparbietà, per avermi appoggiato in ogni circostanza, moralmente ed economicamente, per i consigli e per le critiche che mi hanno fatto crescere, rendendomi la persona che sono. Nonostante ci fossero centinaia di chilometri a separarci, so di avervi avuti sempre al mio fianco.

Grazie ad Annarosa, che con pazienza e amore ha saputo sostenermi ed incoraggiarmi in ogni tappa di questo viaggio, soprattutto in quelle più difficili, senza mai smettere di credere nelle mie capacità. Senza di te non ce l'avrei fatta.

Un ringraziamento speciale a Giuseppe, Francesco, Francesco, Stefano, Marco, Martina e Nicolò per aver reso indimenticabili questi anni torinesi e per avermi fatto sentire come a casa. Vespucci sarà per sempre la mia seconda famiglia.

Ringrazio i miei amici, che seppur distanti e impegnati, hanno saputo consigliarmi e sostenermi in ogni scelta.

Infine Torino, città culla di storia e di cultura, accogliente e stimolante, mi hai cresciuto professionalmente e caratterialmente. Ti ho conosciuto da ragazzino, ti saluto da adulto. Grazie.