

KIZUNA V1

Prefazione

Il nostro sistema sanitario attuale affronta molte sfide, tra cui la sicurezza e la privacy dei dati sanitari degli utenti. La condivisione dei dati sanitari tra i fornitori di cure primarie e specialistiche può essere problematica a causa dei rischi di violazioni della privacy e di perdita di dati. Inoltre, le restrizioni normative e le politiche di sicurezza spesso impediscono una condivisione efficace dei dati.

Per anni strutture sanitarie, medici e pazienti di tutto il mondo si sono affidati a sistemi centralizzati che, per quanto (nella maggior parte dei casi) siano semplici da utilizzare, si rivelano sempre più deboli dal punto di vista della sicurezza dei dati.

Obiettivo

Ho sempre creduto che la tecnologia e in particolare l'informatica, che oggi attraversa un periodo roseo e pieno di innovazioni, debbano essere improntate unicamente al miglioramento delle condizioni di vita dell'umanità, alla facilitazione del lavoro e alla creazione di un mondo migliore.

Per questo, la domanda che mi sono posto è stata la seguente: **il sistema sanitario mondiale, che oggi si basa per la stragrande maggioranza su sistemi centralizzati, può essere migliorato utilizzando al meglio le tecnologie che ci offre la nostra epoca?**

L'obiettivo che mi sono prefissato è stato quindi quello di creare una piattaforma decentralizzata che consenta la condivisione sicura dei dati sanitari degli utenti e che sia progettata per essere altamente sicura, privata e conforme alle normative sulle protezioni dei dati.

Come fare? Attraverso l'utilizzo di una **Blockchain**.

La Blockchain

La blockchain è un **registro digitale condiviso e immutabile** che registra le transazioni in modo trasparente e sicuro. Funziona come un grande libro mastro, distribuito su una rete di computer chiamati nodi, senza una singola autorità centrale che lo controlli. Ogni transazione viene registrata in blocchi di dati collegati tra loro in modo crittografico, creando una catena di informazioni che può essere verificata da tutti i partecipanti. La blockchain offre **trasparenza, sicurezza e decentralizzazione**, eliminando la necessità di intermediari e aprendo nuove possibilità di innovazione e collaborazione.

Perché la decentralizzazione?

La decentralizzazione delle blockchain offre numerosi vantaggi rispetto a un database tradizionale centralizzato. Uno dei principali vantaggi è la sicurezza migliorata. In un database tradizionale, i dati sono generalmente archiviati in un unico punto, rendendoli vulnerabili agli attacchi informatici e alle frodi. Al contrario, una blockchain decentralizzata distribuisce i dati su una rete di nodi, rendendo estremamente difficile per gli hacker alterare o compromettere le informazioni. Inoltre, grazie all'utilizzo di algoritmi crittografici avanzati e al consenso distribuito, le transazioni all'interno di una blockchain sono sicure e immutabili.

Un altro vantaggio della decentralizzazione delle blockchain è la trasparenza. Nei database tradizionali, spesso non è chiaro come i dati vengano gestiti e modificati nel tempo. Con una blockchain, invece, tutte le transazioni vengono registrate in modo permanente e verificabile sulla catena dei blocchi. Ciò significa che ogni partecipante alla rete può accedere a un registro condiviso delle transazioni, promuovendo la trasparenza e la responsabilità.

La decentralizzazione delle blockchain offre anche una maggiore resistenza al fallimento. Nei database centralizzati, se il sistema centrale fallisce o viene compromesso, l'intero sistema può collassare. Al contrario, una blockchain decentralizzata distribuisce le informazioni su molti nodi, garantendo che il sistema rimanga operativo anche se alcuni nodi falliscono o vengono attaccati. Questa resilienza contribuisce a mantenere i servizi basati su blockchain affidabili e disponibili.

Inoltre, la decentralizzazione delle blockchain elimina la necessità di una terza parte fiduciaria. Nei database tradizionali, spesso è richiesta la fiducia in un'entità centralizzata per verificare e validare le transazioni. Con una blockchain, il consenso distribuito consente agli utenti di confermare autonomamente le transazioni senza affidarsi a intermediari. Ciò riduce i costi e gli oneri amministrativi associati alla gestione di una terza parte fiduciaria.

Infine, la decentralizzazione delle blockchain favorisce **l'interoperabilità** e l'accesso equo. Poiché le blockchain sono basate su standard aperti e protocolli condivisi, diversi sistemi blockchain possono interagire tra loro senza restrizioni. Questo crea un ambiente in cui le informazioni e i servizi possono fluire liberamente tra diverse applicazioni, consentendo una maggiore collaborazione e innovazione.

Complessivamente, la decentralizzazione delle blockchain offre vantaggi significativi rispetto a un database tradizionale centralizzato, tra cui una maggiore sicurezza, trasparenza, resistenza al fallimento, eliminazione di terze parti fiduciarie e maggiore interoperabilità. Questi benefici hanno reso le blockchain una tecnologia promettente per una vasta gamma di settori e applicazioni, aprendo nuove possibilità per l'efficienza, l'affidabilità e la democratizzazione dei servizi digitali.

Quale Blockchain scegliere

Dopo mesi di studio la mia scelta è ricaduta su **Ethereum**.

Perché?

Innanzitutto, Ethereum è nota per il suo supporto ai contratti intelligenti. I contratti intelligenti sono programmi autonomi che si eseguono sulla blockchain e consentono di stabilire regole e accordi autonomi, senza la necessità di intermediari. Questa funzionalità di Ethereum offre un'enorme flessibilità per la creazione di **DApp** (Applicazioni decentralizzate) che richiedono la gestione automatica di transazioni e la validazione delle regole del gioco.

Inoltre, essa ha una vasta comunità di sviluppatori e utenti attivi, il che significa che ci sono molti strumenti, risorse e librerie disponibili per semplificare lo sviluppo di applicazioni decentralizzate.

Un altro motivo per scegliere Ethereum è la sua interoperabilità. Il supporto a numerosi standard per la creazione di contratti intelligenti, che consentono alle DApp di interagire sia tra loro sia con altri servizi basati su Ethereum, apre le porte alla creazione di ecosistemi interconnessi, dove le applicazioni possono scambiarsi token e dati in modo efficiente.

Inoltre, Ethereum ha un meccanismo di consenso chiamato Proof of Stake (PoS) che è stato progettato per migliorare l'efficienza energetica e ridurre i costi di transazione rispetto al tradizionale Proof of Work (PoW). Ciò significa che le applicazioni su Ethereum possono beneficiare di tempi di conferma più rapidi e costi di transazione più bassi.

Infine, Ethereum ha dimostrato di essere una piattaforma affidabile e stabile nel tempo. È stato in funzione dal 2015 e ha gestito una vasta gamma di DApp e transazioni su scala globale.

Come funziona

Registrazione dei dati

Gli utenti saranno in grado di caricare i propri dati sanitari sulla piattaforma, dove saranno conservati in modo sicuro e privato. Da questo momento in poi, l'utente sarà il solo e unico *owner* (proprietario) dei dati.

I fornitori di cure primarie e specialistiche autorizzati potranno accedere a questi dati solo se autorizzati dagli utenti stessi, tramite la creazione di un contratto smart sulla blockchain. Ciò significa che gli utenti avranno il controllo completo sui propri dati e potranno revocarne l'accesso in qualsiasi momento.

Registrazione di eventi

La piattaforma sarà in grado di gestire diversi tipi di eventi:

- Eventi generati dall'utente, come ad esempio la richiesta di un consiglio da parte di un fornitore di cure primarie e/o specialistiche, l'invio di dati previa richiesta da parte di uno dei medici autorizzati, oppure la prenotazione di una visita di qualsiasi tipologia.
- Eventi generati dai fornitori di cure, come ad esempio la conferma di una prenotazione, l'invio di un report riguardante una visita o un intervento chirurgico, la richiesta di dati per lo svolgimento di analisi, l'invio di una prescrizione medica, ecc.

I dati gestiti durante gli eventi saranno ovviamente trattati come dati personali del paziente e quindi saranno accessibili esclusivamente al personale medico autorizzato precedentemente.

Condivisione dei dati

Previo autorizzazione da parte dell'utente, la piattaforma potrà consentire la condivisione dei propri dati tra diverse tipologie di fornitori di cure. Questa è ovviamente una feature non obbligatoria, ma che potrebbe semplificare le diagnosi in moltissimi casi.

Prendiamo in esempio il caso della diagnosi di una patologia poco comune. In queste situazioni, diversi medici da tutto il mondo potranno contribuire alla cura e fornire la loro esperienza direttamente dal loro dispositivo, collaborando in tempo reale con i fornitori di cure fidati dell'utente.

Analisi dei dati

In caso di autorizzazione da parte dell'utente, la piattaforma potrà anche consentire la raccolta di dati al puro fine di analizzarli e controllare l'andamento generale di determinati bacini d'utenza. È opportuno ricordare che i dati saranno sempre e solo analizzati da personale autorizzato e trattati in forma completamente sicura. Questo potrà aiutare i fornitori di cure a studiare in modo più preciso l'andamento delle patologie degli utenti ai quali sono collegati o di precise zone geografiche.

Transazioni

La piattaforma utilizzerà la crittografia end-to-end per garantire la sicurezza dei dati durante il trasferimento e il salvataggio. Inoltre, tutte le transazioni saranno registrate sulla blockchain, creando una tracciabilità completa e garantendo che tutte le parti coinvolte siano a conoscenza della provenienza e della storia di tutti i dati.

Vantaggi

Riassumendo, i principali vantaggi derivanti dall'utilizzo di questa piattaforma saranno i seguenti:

- Maggiore sicurezza e privacy per i dati sanitari degli utenti
- Una piattaforma altamente conforme alle normative sulle protezioni dei dati
- Accesso immediato ai dati sanitari da parte dei fornitori di cure primarie e specialistici autorizzati
- Controllo completo degli utenti sui propri dati, con la possibilità di revocare l'accesso in qualsiasi momento
- Tracciabilità completa e sicurezza elevata grazie alla tecnologia blockchain

Requisiti e costi

Gli account sulle blockchain funzionano in maniera leggermente diversa rispetto ai sistemi "tradizionali" ai quali siamo abituati. Per poter creare un account c'è bisogno di un *wallet*, letteralmente un portafoglio digitale, che genererà automaticamente un indirizzo hash che corrisponderà alla nostra persona.

Questo è un esempio: **0d680149400a9ed662d3b2d49e878664efd1b853**.

La creazione di questo hash è completamente gratuita e le procedure variano a seconda del provider che si sceglierà, ma sono tutte molto semplici. Alcuni esempi di wallet provider sono MetaMask o Coinbase.

Perché l'utilizzo di un portafoglio digitale?

Le transazioni su blockchain hanno un costo, che normalmente si basa su diversi fattori:

- La potenza computazionale utilizzata per poter eseguire la richiesta di un utente
- L'attuale quantità di richieste da dover eseguire nello stesso lasso di tempo
- L'attuale valore di un *Ether*, ovvero la valuta principale sulla quale si basa Ethereum e che sarà la valuta attraverso la quale andranno pagate le transazioni

È facile intuire come il costo per ogni singola transazione dipenda dal giorno della settimana o addirittura dal momento della giornata in cui la si esegue.

Tuttavia, dopo vari calcoli effettuati durante alcune simulazioni, posso affermare che nel caso della piattaforma sopra descritta il costo delle transazioni non sarà superiore a qualche centesimo, con un picco massimo raggiungibile di 1-2\$.

È importante specificare anche che solo le transazioni in **scrittura** hanno un costo. In altre parole, recuperare dei dati dalla blockchain sarà sempre gratuito e le uniche azioni ad avere un costo saranno l'inserimento e/o l'upload di dati.

Questo si traduce in costi assolutamente sostenibili e in molti casi addirittura inferiori a quelli normalmente affrontati per una visita specialistica o un normale check-up di routine.

Conclusioni

Questa piattaforma decentralizzata per la condivisione sicura dei dati sanitari rappresenta un grande passo avanti per il settore sanitario. Offre una soluzione altamente sicura e privata per la condivisione dei dati sanitari degli utenti, creando un ambiente in cui gli utenti hanno il controllo completo sui propri dati e i fornitori di cure primarie e specialistiche autorizzati possono accedere a informazioni critiche in modo rapido e sicuro.

Così nasce **Kizuna**.

Fonti

- <https://iopscience.iop.org/article/10.1088/1742-6596/1267/1/012014/meta>
- <https://www.mdpi.com/2227-9032/7/2/56>

