POLITECNICO DI TORINO

Corso di Laurea in
Ingegneria Informatica

Tesi di Laurea Magistrale

# Tecnologia Blockchain per la consegna di farmaci a domicilio


**Relatore:**
Prof. Fabrizio Lamberti

**Correlatrice:**
Ing. Valentina Gatteschi

**Candidato:**
Marco Boscardin

**Tutore Aziendale:**
Francesco Mocci (Consoft Sistemi)



Dicembre 2019

# Ringraziamenti

Vorrei, innanzitutto, esprimere la mia riconoscenza verso i miei genitori, mio fratello e la mia famiglia per il sostegno profuso in questi intensi anni di Politecnico; è stato fondamentale per raggiungere questo traguardo. Ringrazio i miei amici e tutte le persone che hanno condiviso con me i momenti gioiosi e i momenti difficili. Ringrazio ACMOS per avermi fatto sentire parte di una comunità d'intenti, per avermi educato alla cittadinanza attiva e per aver avermi dimostrato che il mondo può essere cambiato in meglio, un passo alla volta, e che ne vale la pena. L'ultimo ringraziamento, ma non meno importante, va all'AUC e ai miei fratelli in Goliardia. Il tentativo di riassumere in poche parole gli ultimi due anni sarebbe velleitario, quindi dico solamente che è stata una "valvola di sfogo" creativa e un importante punto di riferimento per la mia crescita personale. E di questo sono grato, AUC tucc'un!

# Sommario

L'obiettivo principale di questa tesi, svolta presso Consoft Sistemi, era quello di studiare l'utilizzo della Blockchain (tecnologia basata su un registro distribuito e immutabile di transazioni ordinate nel tempo, eseguite dai nodi di una rete, che modificano o trasferiscono asset) in ambito sanitario e, quindi, di realizzare un Proof of Concept di una soluzione innovativa, basata su tecnologia Hyperledger, per la consegna a domicilio di farmaci con ricetta. Attualmente, l'ambito affrontato presenta numerose problematiche tra cui la mancanza di controllo e possesso da parte dei pazienti dei propri dati sanitari, l'insicurezza, la frammentazione della storia clinica, la mancanza di fiducia, la scarsa aderenza alle terapie, l'abuso di medicine legali e, infine, con particolare riferimento al tema affrontato, il rispetto della privacy nella consegna a domicilio di farmaci. La soluzione progettata prevede l'impiego di un'applicazione web che si interfaccia con la Blockchain, con i sistemi esterni (per la gestione delle ricette elettroniche ed i pagamenti) e con le web app utilizzate dagli utenti (clienti, fattorini e farmacisti) attraverso servizi REST; le app dei clienti e dei fattorini a loro volta si interfacciano con lucchetti intelligenti. La fase realizzativa del Proof of Concept si è concentrata sul modello della Business Network (con particolare enfasi su regole di accesso e logica delle transazioni), sulle web app e sulle API REST.

# Indice

# Elenco delle tabelle

# Elenco delle figure

# Capitolo 1

# Introduzione

Lo scopo primario di questa tesi, svolta presso Consoft Sistemi, era quello di studiare l'utilizzo della Blockchain in ambito sanitario e, quindi, di realizzare un Proof of Concept di una soluzione innovativa, basata sulla Blockchain Hyperledger Fabric e sul framework Hyperledger Composer, applicata alla consegna a domicilio di farmaci con ricetta. Si è scelto di approfondire l'applicazione della tecnologia Blockchain all'ambito sanitario perchè presenta grandi opportunità (solo in parte esplorate), sia dal punto di vista informatico sia dal punto di vista dell'impatto sociale. Da un lato la Blockchain è considerata una rivoluzione al pari di Internet e il suo utilizzo si sta diffondendo in molti settori. Dall'altro, la sanità e il suo indotto sono di primaria importanza per la società e l'economia, anche se non sempre sono adeguati alle necessità, a causa di annose questioni che peggiorano i servizi forniti ai pazienti (ad esempio la cattiva gestione dei dati sanitari e della privacy). Tuttavia, al loro interno esistono i casi d'uso (come le consegne a domicilio di farmaci con ricetta) e le condizioni ideali affinché la Blockchain possa esprimere tutto il suo potenziale e apportare i benefici sperati.

In questo capitolo introduttivo verrà dunque presentato il Gruppo Consoft (di cui Consoft Sistemi fa parte), verranno poi descritti brevemente la tecnologia Blockchain, Hyperledger Fabric e Hyperledger Composer, in terzo luogo verranno elencate le principali problematiche della sanità attuale e le possibili soluzioni basate sulla Blockchain e infine verrà proposto il Proof of Concept.

## 1.1 Presentazione del Gruppo Consoft

Il Gruppo Consoft [1] è un insieme di aziende italiane presente sul mercato ICT dal 1986 con sedi a Milano, Torino, Genova, Roma e Tunisi. Oltre alla capogruppo Consoft Sistemi sono attive altre società: CS InIT, specializzata nello scouting e distribuzione di soluzioni software, Consoft Consulting, focalizzata sulla PA, Consoft

Sistemi MEA e C&A Soft Consulting, finalizzate all'espansione dell'offerta della capogruppo nel Nord Africa e nel Medio Oriente.

Il Gruppo Consoft ha suddiviso la propria offerta in aree tematiche: finanza, assicurazioni, industria, telecomunicazioni, utilities, automotive, pubblica amministrazione e media (solo per citarne alcuni). Il filo conduttore è la Digital Transformation e l'implementazione di soluzioni "end to end" per i propri clienti attraverso attività di consulenza, formazione, realizzazione di soluzioni integrate ed erogazione di servizi in insourcing e outsourcing.

Consoft Sistemi è parte del CDA del Cluster Tecnologie per le Smart Cities & Communities Lombardia, è membro di Assolombarda e Assintel (tramite CS InIT) ed è attiva nei progetti di innovazione proposti dagli Enti. Ha fatto parte dell'Osservatorio Internet of things e Osservatorio Big Data del MIP, è membro IOTitaly. Consoft Sistemi come partner tecnologico collabora attivamente a progetti di ricerca sia regionali che nazionali ed europei con l'obiettivo di studiare e realizzare soluzioni che arricchiscano il mercato con ulteriori componenti ICT sviluppati a partire dalla realtà progettuale proposta, basati pertanto su un'esperienza che ne abbia già stimato il grado di fattibilità e sostenibilità economica. Le attività di R&D, inoltre, permettono di creare ulteriori contatti tra aziende, centri di ricerca, università e operatori di settore per costruire un'offerta di servizi più competitivi e completi, consentendo l'utilizzo sinergico di risorse nell'ottica di un complessivo aumento di efficienza ed efficacia. Tra le aree di specializzazione tecnologica annovera DevOps, Testing, Analytics & Big Data, Cyber Security e Internet of Things. Infine, è da sottolineare che Consoft abbia ottenuto la certificazione ISO 27001 e possiede un sistema di gestione qualità certificato UNI EN ISO 9001:2008.

Concludendo la presentazione, è da sottolineare che l'innovazione sociale, declinata in questo caso nel miglioramento della sanità e della qualità della vita, sia uno dei temi centrali nella visione di Consoft ed è appunto in questo ambito che si colloca questa tesi [1].

## 1.2 Blockchain, Hyperledger Fabric e Hyperledger Composer

La Blockchain è un registro condiviso, sincronizzato e immutabile di transazioni ordinate nel tempo, eseguite dai nodi di una rete, che definiscono il passaggio di proprietà di risorse (asset) o la loro modifica. Prima di essere inserite definitivamente nel registro, le transazioni vengono verificate dalla rete stessa senza ricorrere a terze parti fidate. La criptografia è determinante in questa fase e in quella successiva di mantenimento dell'integrità del registro. Le transazioni tracciate e le relative informazioni possono essere consultate in modo trasparente. Queste proprietà, unite alla digitalizzazione dei dati e all'automazione delle procedure, contribuiscono a

migliorare (in determinate circostanze) i sistemi in cui tale tecnologia viene adottata, in termini di efficienza, sicurezza e fiducia degli utenti. Bisogna tuttavia sottolineare che la Blockchain non sia una panacea, non migliora ogni sistema in cui viene inserito. Infatti, essa apporta un contributo positivo qualora si verifichino quattro condizioni [2]:

1) Esistano delle informazioni in un repository condiviso e centralizzato che vengano accedute e modificate da diverse entità con interessi contrapposti attraverso transazioni.

2) Tali entità necessitino di sapere con certezza se le transazioni siano valide o non valide.

3) Le terze parti non siano ritenute sufficientemente fidate o efficienti tanto da affidare loro le dovute verifiche.

4) Sia necessaria una maggiore sicurezza per garantire l'integrità e il corretto funzionamento del sistema.

Tali condizioni, come si vedrà nel capitolo relativo allo stato dell'arte, sono presenti nell'ambito sanitario. Le strutture sanitarie, ad esempio, conservano i dati sanitari dei pazienti all'interno di database centralizzati che vengono continuamente aggiornati e/o acceduti dagli operatori sanitari (medici, infermieri, ecc.), dai ricercatori, dai pazienti e da altre categorie di persone. Trattandosi di dati sensibili e necessari per la qualità delle cure, per gli studi clinici e per la prevenzione, è indispensabile che i dati siano corretti e che le operazioni eseguite su di essi siano validabili e tracciabili. Tuttavia, sovente la fiducia nel sistema e in coloro che dovrebbero controllare è poca a causa dei scandali, degli attacchi informatici e delle frodi che periodicamente salgono alla ribalta della cronaca. Tutto ciò porta a concludere che il paradigma Blockchain possa migliorare il sistema sanitario.

In questa tesi è stato approfondito in particolare l'utilizzo di Hyperledger Fabric, una Blockchain privata e permissioned, nata nel 2017, che presenta caratteristiche innovative come un nuovo ciclo delle transazioni (da order-execute a execute-order-validate), i "channel" e la possibilità di utilizzare linguaggi di programmazione general-purpose. Inoltre è stato utilizzato il framework Hyperledger Composer, che facilita e velocizza la realizzazione di applicazioni Blockchain e la loro installazione in Hyperledger Fabric, per creare il modello che sta alla base delle consegne di farmaci del Proof of Concept e i componenti del sistema.

## 1.3 Problematiche della sanità attuale e soluzioni Blockchain

Attualmente, l'ambito affrontato presenta numerose problematiche tra cui: la mancanza di controllo e possesso da parte dei pazienti dei propri dati sanitari, la difficoltà a consultarli, a ottenerli e a condividerli, l'insicurezza (ad esempio, esiste il rischio di furti o manomissioni di documenti), la frammentazione della storia clinica del paziente tra tutte le strutture sanitarie che lo hanno visitato e curato, la mancanza di fiducia nel fornire i propri dati (ad esempio per scopi di ricerca), nell'acquistare farmaci e vaccini e, in generale, nella sanità. Ad esse si aggiungono l'uso prevalete di documenti in formato cartaceo, le inefficienze in termini di tempo, denaro e personale, le frodi e la corruzione, i controlli approssimativi, la bassa qualità dei prodotti farmaceutici e dei dispositivi medici, la scarsa aderenza alle terapie da parte dei pazienti, la carenza di scorte, l'abuso di medicine legali e, infine, con particolare riferimento al tema affrontato, il rispetto della privacy nella consegna a domicilio di farmaci. Queste sono alcune delle questioni che possono essere risolte, in toto o in parte, sfruttando le proprietà della tecnologia Blockchain. Per analizzare queste problematiche e descrivere le soluzioni teoriche e i progetti concreti basati sul nuovo paradigma Blockchain, nella prima parte della tesi sono state definite cinque aree di studio e applicazione:

1) Gestione dei dati sanitari
2) Monitoraggio della salute
3) Studi clinici
4) Tracciabilità dei medicinali, dei vaccini e dei dispositivi medici
5) Piattaforma per prescrizioni e consegna di farmaci a domicilio

## 1.4 Proof of concept: Blockchain applicata alla consegna di farmaci

Sulla base dell'analisi effettuata, è stato identificato l'ambito della consegna a domicilio di farmaci con ricetta, in cui la Blockchain non è ancora stata utilizzata, ma si ritiene che la sua applicazione apporterebbe notevoli benefici; con questo intento è stato realizzato un Proof of Concept. Lo scenario senza Blockchain prevede che un cliente effettui un ordine e il relativo pagamento, che il fattorino successivamente ritiri la ricetta cartacea dal cliente, si rechi quindi da un farmacista o da un fornitore, mostri la ricetta, ritiri i farmaci e, infine, che li consegni al cliente. Questo scenario implica diversi svantaggi tra cui poca fiducia dei malati nell'affidare ai

fattorini le loro ricette o la consegna dei farmaci (per timore che venga persa la ricetta, per timore di manipolazioni/furti di medicinali, di ritardi, ecc.), la mancanza di privacy (perché il fattorino può leggere la ricetta cartacea o vedere le medicine che consegna), inefficienza (alcuni passaggi sono evitabili o migliorabili), mancanza di tracciabilità e monitoraggio delle transazioni, possibili truffe, manomissioni dei dati o dei prodotti.

Per risolvere questi problemi è stata progettata e implementata una soluzione innovativa, basata su Hyperledger Fabric e Hyperledger Composer. La prima è stata scelta essenzialmente perché è una blockchain privata e permissioned: questo vuol dire che i participant non sono anonimi, ma hanno una identità certificata, vuol dire che i dati sensibili salvati nella Blockchain sono leggibili, modificabili e condivisibili solo dai legittimi proprietari e che esistono tipologie di partecipanti differenti a cui si possono concedere permessi di accesso differenti. Il secondo è stato scelto perché semplifica e velocizza la modellazione di Business Network e lo sviluppo di applicazioni Blockchain per Hyperledger Fabric.

Inoltre, le ricette cartacee sono state sostituite con quelle elettroniche e sono stati aggiunti dei lucchetti intelligenti per chiudere i pacchi anonimi (ovvero che non permettono di conoscere ciò che è al suo interno) contenenti i farmaci. I pacchi vengono chiusi al momento dell'erogazione per poi essere riaperti solamente alla conclusione della consegna dal cliente tramite un codice cifrato inviato dal farmacista. È rilevante notare che l'asset del modello della Business Network (la rete formata da tutti i partecipanti) sia l'ordine del cliente (al cui interno vi è il codice NRE, ovvero il Numero di Ricetta Elettronica, insieme ad altri dati); il cliente, in quanto creatore, è anche il proprietario dell'asset.

Il sistema progettato è costituito da una Blockchain, da un'applicazione web che si interfaccia con la Blockchain, con i sistemi esterni (i sistemi di pagamento e il sistema che contiene il database delle ricette elettroniche) e con le web app utilizzate dagli utenti (clienti, fattorini e farmacisti) attraverso i REST web service. Le web app dei clienti e dei fattorini a loro volta si interfacciano con i lucchetti intelligenti. È da rimarcare che all'interno della Blockchain non vi siano le ricette elettroniche, ma solo il codice NRE, insieme ad alcune altre informazioni degli ordini; questo determina una minore complessità del sistema e una maggiore scalabilità, dovuta alle dimensioni inferiori degli asset (lo spazio di memorizzazione è una questione potenzialmente critica, data la natura ridondante della Blockchain). Complessivamente, i vantaggi portati da Blockchain, ricette elettroniche e lucchetto intelligente dovrebbero determinare un aumento della fiducia dei clienti, un minore rischio di truffe e manomissioni, maggiore privacy, sicurezza ed efficienza.

## 1.5 Struttura della tesi

Il capitolo successivo, ovvero il secondo, descriverà nella prima parte più nel dettaglio la tecnologia Blockchain, in particolare i suoi elementi base, il suo protocollo, le

sue proprietà e i concetti più importanti (come il consenso, gli smart contract, ecc.). Nella seconda parte verranno affrontati Hyperledger Fabric, con relativi concetti e proprietà, e nell'ultima Hyperledger Composer.

Il terzo capitolo racconterà le aree di studio e di applicazione presentate in precedenza, le problematiche, le teoriche soluzioni Blockchain, le proprietà fornite e i progetti concreti considerati più rilevanti, cercando quindi di dare una panoramica complessiva dello stato dell'arte.

Il quarto capitolo è destinato all'introduzione del Proof of Concept, vale a dire l'applicazione di Hyperledger Fabric alla consegna di farmaci con ricetta a domicilio. Per questo motivo nella prima parte verranno descritti i concetti base dell'attuale processo attraverso cui il paziente acquisisce i farmaci e di quello futuro ipotizzato dalla soluzione, la consegna a domicilio di farmaci e le problematiche con e senza il suo utilizzo. Nella seconda parte verrà presentato l'approccio proposto per risolvere o mitigare tali questioni e, infine, verranno analizzati i relativi vantaggi.

Il quinto capitolo è finalizzato alla progettazione del Proof of Concept. In primo luogo, verrà preso in considerazione il contesto in cui il sistema è chiamato ad operare e le interfacce utilizzate dagli attori per comunicare col sistema. In secondo luogo, verranno elencati i requisiti funzionali e non funzionali. In terzo luogo, si descriveranno i casi d'uso e i relativi scenari. In ultimo luogo, verranno spiegati i vocaboli chiave attraverso un glossario e definiti i componenti costitutivi del sistema.

Il sesto capitolo verterà sull'implementazione del Proof of Concept. Si andranno ad approfondire i suoi obiettivi, il modello della Business Network più ulteriori concetti riguardanti il sistema, il sistema visto come macchina di Moore, l'ambiente di sviluppo, lo scenario principale di successo, i test eseguiti e, infine, i prototipi dell'interfaccia utente.

Il capitolo conclusivo, il settimo, trarrà le conclusioni riguardanti la tesi svolta e i risultati raggiunti. Da ultimo, traccerà le linee dei possibili sviluppi futuri.

# Capitolo 2

# Tecnologia Blockchain

Nella prima parte del capitolo verrà trattata dal punto di vista teorico la tecnologia Blockchain, descrivendo le proprietà che fornisce e i concetti più importanti. Nella seconda parte ci si concentrerà su una Blockchain in particolare, ovvero Hyperledger Fabric, e su Hyperledger Composer, un framework supportato da una serie di strumenti di sviluppo che facilita e velocizza la realizzazione di applicazioni Blockchain e la loro installazione in Hyperledger Fabric.

## 2.1 Blockchain

Il 31 ottobre 2008 Satoshi Nakamoto, un anonimo inventore, pubblicò il documento “Bitcoin: A Peer-to-Peer Electronic Cash System” [3] col quale spiegò il funzionamento del protocollo Bitcoin e della corrispondente criptovaluta. Nel nucleo concettuale di questo sistema di pagamento elettronico, basato sulla criptografia e priva di terze parti fidate, vi è la tecnologia Blockchain.

Definita alcuni anni fa "the trust machine" (la macchina della fiducia) da The Economist [4], questo "meccanismo" ha come fine quello di creare fiducia dove non c’è fiducia [5]. Infatti, nella società attuale vi è una crescente sfiducia nell’altro, a partire dai propri pari fino ai tecnici e a chi ricopre un ruolo di controllo, che porta a sentire la necessità di un sistema sicuro, fidato e relativamente semplice da utilizzare, in modo tale da non dover avere entità esterne che controllino o esperti che eseguano operazioni al proprio posto. E la Blockchain è sistema fidato perché costituita da codice che è regolatore e legge [6] applicata ex ante (dato che ogni transazione per concretizzarsi deve essere convalidata attraverso algoritmi di consenso [7]). Per questo e altri motivi, che verranno analizzati in seguito, la Blockchain viene considerata la terza rivoluzione dopo Internet e l’Internet of Things (IoT).

### 2.1.1 Elementi base

Di seguito sono elencati i componenti che, assemblati insieme, costituiscono lo scheletro della tecnologia Blockchain [8]:

- **Nodo**: costituisce la rete insieme ad altri partecipanti.
- **Asset**: rappresenta il bene posseduto dal partecipante, il valore che può essere scambiato o modificato.
- **Transazione**: operazione eseguita all'interno della Blockchain; può essere un passaggio di proprietà di asset tra due partecipanti, la modifica di asset, ecc. È necessario prima di tutto controllare la sua validità basandosi sulle informazioni che contiene e su quelle possedute dai partecipanti che sono chiamati a verificare, poi accettarla o meno e infine archiviarla.
- **Hash**: la funzione di hash è uno strumento matematico che prende in input un messaggio alfanumerico di una qualsiasi dimensione e produce in output una stringa di lunghezza fissa, chiamata digest. Viene utilizzata, nel caso specifico della Blockchain, ad esempio per identificare univocamente i blocchi di transazioni o per controllare un'eventuale modifica degli stessi. Aspetto molto importate è l'impossibilità di invertire la funzione, cioè impedire che malintenzionati eseguano i calcoli inversi per ottenere il testo originale.
- **Blocco**: insieme di transazioni raggruppate insieme e identificate da un digest presente nell'header che contiene il "riassunto" del blocco corrente e dell'header di quello precedente. In questo modo si crea una catena di blocchi collegati; da qui il nome block chain (catena di blocchi).
- **Ledger**: database distribuito tra diversi computer, prende il nome dai libri mastri utilizzati da secoli per annotare tutte le entrate e uscite di un'attività economica. Viene visto dagli utenti come un registro globale e pubblico, in cui vengono segnate tutte le transazioni in maniera immutabile, sequenziale e trasparente. È costituito da una catena di blocchi tra loro legati ed identificati da funzioni di hash.
- **Timestamp**: anche detto marca temporale, associa ad un documento digitale una data e un'ora univoche e immutabili; viene utilizzato per definire l'ordine in cui sono state eseguite le transazioni, in modo tale che si possano scoprire eventuali manomissioni, e quando sono state registrate.

### 2.1.2 Descrizione

La Blockchain permette a un insieme di entità (persone fisiche, gruppi di persone, organizzazioni e altro ancora) collegate tra di loro all'interno di una rete di

scambiarsi o modificare risorse, anche dette asset (denaro, azioni finanziarie, dati sanitari, contratti, voti, brani musicali, ecc.) senza la necessità di una terza parte fidata (banche, governo, aziende, persone con ruoli di controllo, ecc.) che verifichi l'autorizzazione all'esecuzione della transazione, i suoi partecipanti e la validità della stessa. Questa verifica viene effettuata dai nodi della rete: essi sono dei dispositivi elettronici, ad esempio computer, utilizzati dalle entità, in grado di scambiarsi dati e di svolgere precise funzioni. Tutti i nodi possiedono le stesse informazioni, perché tutti possiedono una copia del ledger (in italiano, libro mastro), ovvero un database distribuito con tutta la storia pregressa delle transazioni eseguite. Il processo decisionale consiste nella creazione di un consenso attraverso l'uso di appositi algoritmi. Qualora la maggioranza dei nodi approvasse la transazione (dopo aver effettuato i dovuti controlli), essa potrebbe essere inserita in un blocco insieme ad altre transazioni approvate, a sua volta aggiunto alla catena di blocchi che costituiscono il ledger. Nell'header del blocco verrebbe scritto un digest (stringa alfanumerica di lunghezza fissa) ottenuto applicando una funzione di hash (algoritmo criptografico non invertibile che fa corrispondere un messaggio di lunghezza arbitraria ad una stringa di lunghezza fissa [8]) sulle transazioni contenute nel blocco stesso, un digest ottenuto applicando una funzione di hash sull'header del blocco precedente e, infine, un timestamp (marcatore temporale) [9]. Dopo questa fase la transazione non potrebbe più essere rimossa o modificata e la sua storia potrebbe essere ricreata in qualsiasi momento. Gli algoritmi di consenso impediscono in pratica di manomettere il ledger distribuito a proprio favore, perché sarebbe necessario controllare la maggioranza della rete. Inoltre, tutti possono potenzialmente avere accesso allo stato attuale e alla storia passata della Blockchain avendo così un elevato grado di trasparenza [8]. Nella figura 2.1 si può vedere schematicamente il funzionamento del protocollo.

### 2.1.3 Proprietà

Di seguito vengono riportate le principali proprietà che caratterizzano la tecnologia Blockchain:

- **Tracciabilità**: tutte le transazioni e le relative informazioni (come mittenti e destinatari) sono registrate definitivamente nella Blockchain e chiunque può controllare la storia pregressa.
- **Trasparenza**: tutti i dati salvati sul ledger sono consultabili da chiunque.
- **Decentralizzazione**: non esiste un ente centrale col compito di controllare il sistema e custodire le informazioni, ma la responsabilità è assegnata equamente a tutti i partecipanti.
- **Sicurezza**: proprietà complessa che si compone di molteplici elementi (tra cui immutabilità, integrità, sequenzialità, disponibilità, ecc.).

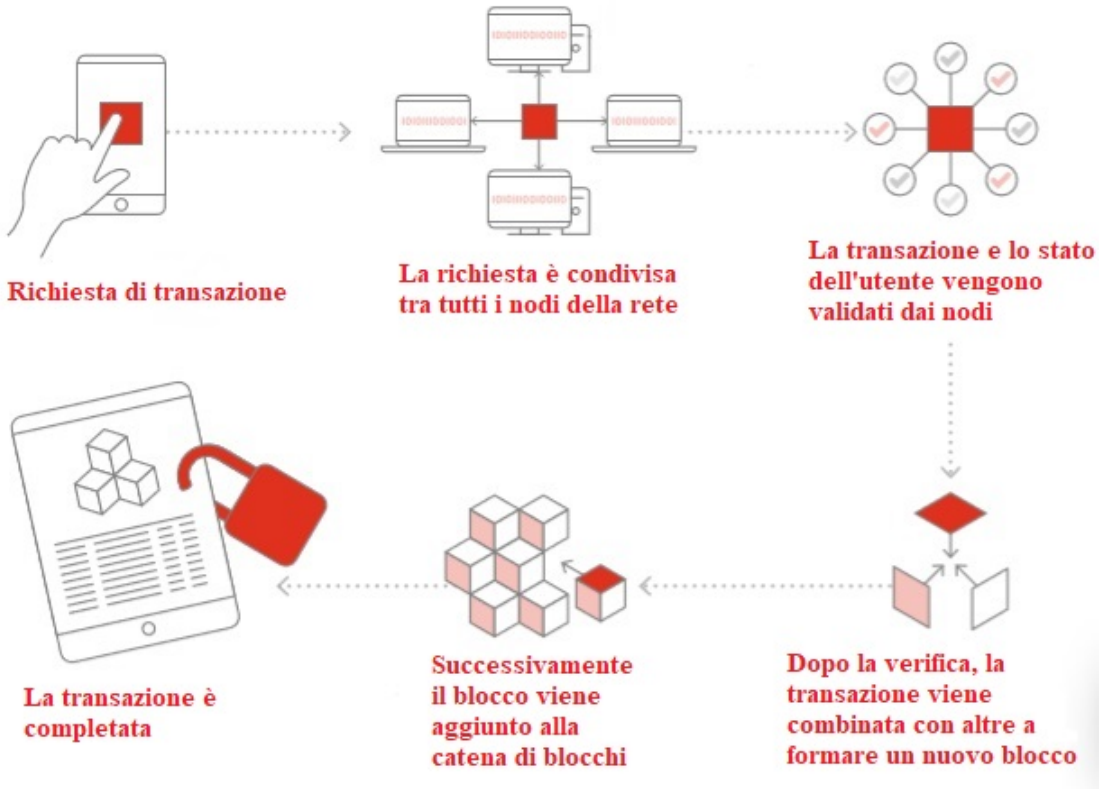



**Figura 2.1:** protocollo Blockchain (modificata a partire da [10]).

- **Immutabilità e integrità**: permettono il rilevamento di tentativi di modifica del ledger basandosi sui digest salvati nei blocchi, quindi le transazioni sono cristallizzate all'istante in cui sono state inserite.

- **Sequenzialità**: impedisce che venga invertito l'ordine temporale di due o più operazioni, grazie anche al timestamp.

- **Disponibilità**: attitudine di un'entità o di un sistema a fornire un servizio ad un utente in un determinato istante di tempo; è garantita dagli algoritmi di consenso (che impediscono ad esempio il Denial of Service) e dal fatto che il sistema sia distribuito.

- **Correttezza**: garantita dagli algoritmi di consenso, che impediscono l'aggiunta di blocchi inesatti.

- **Ridondanza**: ogni nodo possiede una copia locale del ledger, quindi è intrinsecamente immune a perdite di dati accidentali o intenzionali.

- **Efficienza**: permette minori costi e risparmi di tempo attraverso la disintermediazione delle operazioni, l'automazione, la semplificazione dal lato utente e altre caratteristiche del sistema.

### 2.1.4 Consenso

In un sistema distribuito non esiste un'istituzione centralizzata che verifichi e autorizzi (o meno) le transazioni e il loro salvataggio definitivo nel ledger. Le decisioni devono essere prese collettivamente, da pari a pari, dopo una fase iniziale di elaborazione delle informazioni; concluso il processo si arriva al consenso, cioè ad un verdetto accettato da tutti (che si traduce nella registrazione delle transazioni in tutte le copie locali dalla Blockchain). Inoltre, bisogna fare in modo che sia impossibile per uno o più nodi malevoli (comunque meno della metà dei complessivi) portare il sistema ad inserire dati errati; anzi, possibilmente deve essere conveniente concorrere alla corretta validazione. Vi sono vari algoritmi utilizzati per raggiungere il consenso [8, 11, 12], qui di seguito verranno elencati i principali:

1) Il **Practical Byzantine Fault Tolerance** (PBFT), uno dei primi ad essere delineati, si costituisce di due fasi. La fase iniziale coinvolge i singoli nodi, i quali ricevono la transazione da verificare e in base alla loro copia locale della Blockchain calcolano l'esito (accettazione o rifiuto), che verrà comunicato a tutti gli altri nodi. La fase conclusiva elabora i risultati individuali per arrivare ad un esito collettivo. Questo algoritmo richiede uno sforzo computazionale inferiore rispetto ai metodi successivi, ma pregiudica l'anonimato nella rete.

2) Il **Proof of Work** (PoW), utilizzato da Bitcoin ed Ethereum, ha come obiettivo quello di evitare verifiche sulle transazioni volontariamente (ad esempio, attacchi Denial of Service) o involontariamente (ad esempio, errori di computazione) sbagliate da parte dei nodi preposti. Per raggiungere questo obiettivo i creatori dell'algoritmo hanno supposto che un ipotetico malintenzionato non sia disposto a compiere uno sforzo computazionale ed energetico rilevante per calcolare la risposta ad una sfida (in inglese, challenge) da inviare prima di poter aggiungere alla Blockchain il blocco di transazioni controllate; inoltre, il numero di nodi scelti per la verifica (chiamati miner) riduce al minimo il rischio di errori di calcolo. Questi nodi, dopo aver controllato una serie di transazioni, devono trovare un digest che abbia una forma prestabilita (spesso deve iniziare con un certo numero di zeri). Per ottenere il digest devono calcolare un hash utilizzando l'header con al suo interno un nonce (un numero casuale utilizzato una sola volta nell'algoritmo [13]). Se il risultato ottenuto non è quello sperato si incrementa il nonce e si riesegue il calcolo, attuando una strategia "prova e sbaglia" (in inglese, "trial and error"), ovvero a forza bruta. I miner sono in competizione tra loro, perché solo il primo a trovare il digest giusto ha il diritto di aggiungere il blocco alla Blockchain e a essere premiato con delle

criptomonete. Gli altri nodi della rete ricevono il nuovo blocco, lo verificano e infine lo aggiungono alla loro copia locale del ledger. La complessità di calcolo viene modulata in modo tale da mantenere il numero medio di blocchi creati costante nel tempo. Il processo attraverso cui si risolve la sfida criptografica viene chiamato mining. In ultima analisi, il Proof of Work consente una facile ed ampia partecipazione alla rete, perché non è richiesto che tutti partecipino a tutte le verifiche e i requisiti minimi per partecipare sono pochi (ad esempio i nodi possono rimanere anonimi).

3) Il **Proof of Stake** (PoS) ha una strategia simile, ma coloro che devono concorrere alla creazione del consenso sono ristretti principalmente ai partecipanti con un forte interesse nella Blockchain, vale a dire coloro che posseggono più criptomonete o che le detengono da più tempo. Il calcolo del digest è sostituito con il calcolo di una firma digitale che dimostra la proprietà del proprio interesse (in inglese, stake). Il validatore (colui che deve annunciare il responso e produrre un nuovo blocco) viene scelto a partire da un gruppo di partecipanti con probabilità direttamente proporzionale al proprio interesse. Per essere inseriti nel gruppo dei potenziali validatori è necessario possedere delle criptomonete ed eseguire una specifica transazione che le blocchi all'interno di un deposito. Come in Bitcoin anche in questo caso il lavoro del validatore viene premiato con nuove criptomonete. Questo algoritmo è molto meno dispendioso computazionalmente e richiede meno tempo (al contrario del mining), anche se c'è il rischio di accentrare il potere decisionale ad una cerchia di pochi componenti; ciò può essere evitato inserendo dei parametri che consentono potenzialmente anche ai partecipanti alla rete con poco interesse di essere scelti, anche se con probabilità basse. Infine, un eventuale malintenzionato potrebbe aggiungere un blocco errato solamente nel caso in cui possegga il 51% delle criptomonete.

4) Il **Delegated Proof of Stake** (DPoS) è quasi uguale al PoS, ma i singoli nodi possono decidere di farsi rappresentare da delegati; così facendo si raggruppano gli interessi dei singoli a formare delle entità più grosse con maggiore possibilità di essere scelte. Questo algoritmo contrasta il potere dei grandi possessori di interesse e permette al sistema di lavorare più velocemente rispetto al PoS classico.

I sistemi che non utilizzano PoW sono spesso chiamati "virtual mining system" perché non effettuano l'attività di mining.

### 2.1.5 Smart contract

Con l'avvento Ethereum è stato introdotto il concetto di smart contract legato alla tecnologia Blockchain. Da punto di vista informatico è un pezzo di codice

che viene concordato dai contraenti definendone il comportamento e definendo i parametri. In seguito, viene inserito nel ledger rendendolo immutabile. Infine, in base a determinate condizioni o eventi interni o esterni alla Blockchain lo smart contract verrà attivato ed eseguirà una serie azioni precedentemente scritte; tutto questo in automatico. Ovviamente le transazioni prima di essere effettuate verranno verificate dal sistema.

### 2.1.6 Pubblica vs privata, permissionless vs permissioned e consortium

La differenza sostanziale tra Blockchain pubblica e privata è il fatto che chiunque possa accedere liberamente, oppure no, ad essa e se gli utenti della rete debbano identificarsi o possano mantenere l'anonimato.

L'ulteriore distinzione permissioned/permissionless aggiunge delle possibili restrizioni alle Blockchain: limita i partecipanti che possono contribuire al consenso dello stato del sistema, che possono compiere determinate azioni, che hanno i diritti per convalidare le transazioni o per accedere a certe informazioni nel ledger oppure che possono creare gli smart contract. Nelle Blockchain permissioned la verifica delle transazioni viene eseguito dalla governance, cioè dall'autorità che ha creato la Blockchain e che ha definito le autorizzazioni e le regole del sistema; in quelle permissionless viene fatto dai partecipanti. Per le questioni sopra elencate solitamente le imprese che vogliono implementare una soluzione Blockchain si orientano verso la tipologia permissioned. Del resto le Blockchain pubbliche e permissionless si possono comparare a Internet, mentre quelle private e permissioned alle intranet all'interno delle aziende. Infine, il consortium si va a collocare in mezzo a tutte le soluzioni elencate in precedenza: invece di consentire ad ogni entità di verificare le transazioni o di consentirlo solo ad una società, si scelgono alcuni nodi, creando un consiglio di persone o di organizzazioni note e fidate [14, 15].

## 2.2 Hyperledger Fabric

Hyperledger è un progetto open source nato alla fine del 2015 e portato avanti dalla fondazione Linux insieme ad un gruppo di imprese legate all'informatica, all'elettronica e alla finanza per portare sviluppare soluzioni Blockchain a livello industriale. Si suddivide in diverse piattaforme, tra cui Fabric. Nelle prossime righe e nei prossimi paragrafi verrà spiegata la sua struttura, le sue funzionalità e le sue caratteristiche, confrontandola con altre piattaforme e sottolineandone le differenze.

Hyperledger Fabric è una Blockchain privata e permissioned, implementata in Go, con un'architettura modulare e configurabile. È la prima piattaforma a ledger distribuito che permette l'utilizzo di linguaggi di programmazione general-purpose

come Java, Node.js e Go per scrivere smart contract. Questo perché il ciclo di vita delle transazioni è stato rivoluzionato: da un modello order-execute ad uno execute-order-validate. Gli smart contract vengono eseguiti da ogni peer della rete all'interno di contenitori Docker. Infine, ulteriori importanti differenze sono la possibilità di scegliere tra più di un protocollo di consenso e il fatto che essi non richiedano l'utilizzo di criptovalute (caratteristica presente anche in altre Blockchain private e permissioned, aumenta la velocità di esecuzione, mentre riduce possibili rischi o attacchi) [16, 17].

### 2.2.1 Peer, endorser, orderer e client

Un aspetto interessante è l'assegnazione di ruoli e compiti specifici ai nodi. Essi sono le entità di comunicazione nella Blockchain. Un nodo è solo una funzione logica, nel senso che più nodi di tipi diversi possono operare sullo stesso server fisico. Ciò che conta è come i nodi siano raggruppati in "domini di fiducia" e associati a entità logiche che li controllano. Esistono quattro tipi di nodi [18]:

- **Peer**: mantiene il ledger e lo aggiorna ogniqualvolta riceve le nuove transazioni ordinate dagli orderer.
- **Endorser**: è un tipo specifico di peer approva (oppure no) le transazioni controllando se soddisfano le condizioni necessarie e sufficienti (ad esempio la presenza delle firme richieste).
- **Orderer**: fornisce un canale di comunicazione a client e peer tramite il quale i messaggi contenenti transazioni possono essere diffusi. Per quanto riguarda il consenso, i canali assicurano che tutti i peer connessi ricevano esattamente gli stessi messaggi con lo stesso ordine logico.
- **Client**: agisce per conto dell'utente finale, crea e invoca le transazioni, oltre a comunicare con i peer e gli orderer.

### 2.2.2 Channel

Un channel (canale) Hyperledger Fabric è una sottorete (in inglese, subnet) privata di comunicazione tra due o più membri specifici della rete (in inglese, network), allo scopo di condurre transazioni confidenziali. Un channel è definito dai membri (organizzazioni che contengono insiemi di peer), dagli anchor peer e dai leader peer (uno per ogni membro), dal legder condiviso (di fatto il channel rappresenta una Blockchain condivisa tra nodi di quel channel), dalle applicazioni che utilizzano gli smart contract e dai nodi del servizio di ordering. Gli anchor peer permettono ai peer di diverse organizzazioni di comunicare tra loro facendo da "ponte", mentre il leader peer comunica col servizio di ordering per conto del proprio membro. Ogni transazione sulla rete viene eseguita in un channel, in cui ciascun attore

dell'operazione deve essere autenticato e autorizzato ad effettuare transazioni su quel channel. Ad ogni peer che si aggiunge ad un channel viene fornita un'identità da un membership services provider (MSP), che gli permette di essere identificato dagli altri peer e dal servizio di ordering [16].

Nella figura 2.2 è illustrata una rete di esempio con tre organizzazioni Org1, Org2 e Org3, ognuna delle quali possiede un peer Peer0, e un'organizzazione con un nodo Orderer. La rete ha due channel, ChannelAll, che unisce Org1, Org2 e Org3, e Channel12, che unisce Org1 e Org2 [19].

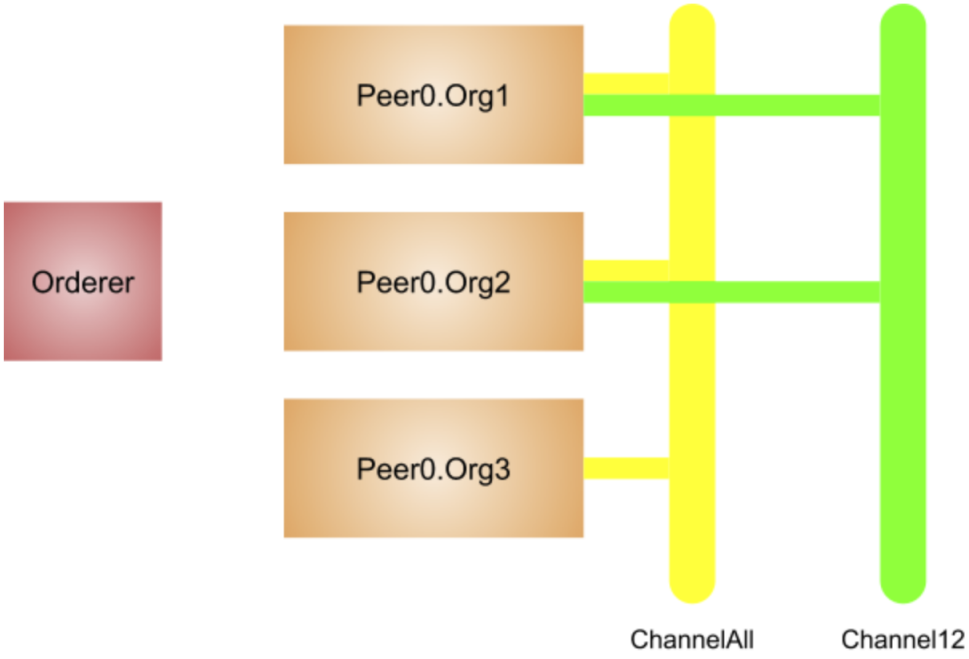



**Figura 2.2:** rete multi-channel in Hyperledger Fabric (tratta da [19]).

### 2.2.3 Asset

Gli asset possono andare dal concreto (immobiliare e hardware) all'astratto (contratti e proprietà intellettuale). Hyperledger Fabric fornisce la possibilità di modificarli utilizzando le transazioni e i corrispondenti smart contract. L'asset è rappresentato concettualmente come una coppia chiave-valore e concretamente in forma binaria e/o JSON, con le modifiche di stato registrate come transazioni su un registro del channel [16].

### 2.2.4 Smart contract e Chaincode

Generalmente, lo smart contract è la logica della transazione che controlla il ciclo di vita di un oggetto contenuto del world state. In base alle istruzioni che sono state scritte dentro al suo codice un'applicazione client può invocarlo per accedere o modificare, se si hanno i permessi, le coppie chiave-valore presenti nel world state. In Hyperledger Fabric, durante la fase di sviluppo, lo smart contract viene impacchettato insieme ad altri in un chaicode, che successivamente verrà installato sui peer della rete della Blockchain e istanziato in uno o più channel. Da quel momento tutti gli smart contract definiti in quel chaincode saranno disponibili per tutte le applicazioni. Per questo motivo spesso i termini smart contract e chaincode vengono utilizzati con sinonimi [16].

### 2.2.5 Ledger

Il ledger è il registro, sequenziale e resistente alle manomissioni, di tutte le transizioni di stato. Le transizioni di stato sono il risultato di invocazioni di transazioni effettuate dai nodi coinvolti. Ogni transazione inserita nel ledger viene rappresentata come un insieme di coppie chiave-valore dell'asset, più l'azione seguita (crea, leggi, aggiorna o elimina). Esiste un ledger per ogni channel; ogni peer mantiene una copia del ledger per ogni channel di cui è membro. Il ledger è costituito da una chain (catena) che contiene blocchi di transazioni immutabili e ordinate temporalmente (cioè la storia passata del sistema), nonché da uno state database per mantenere lo stato corrente. I dati dello stato corrente rappresentano i valori più recenti di tutte le chiavi nel channel; per questo a volte viene indicato come world state (stato mondiale). Le chiamate chaincode eseguono transazioni basandosi sullo stato corrente, quindi memorizzarlo in un database migliora le prestazioni rispetto al solo utilizzo della chain. In Hyperledger Fabric vengono usati due tipi di database: LevelDB e CouchDB. LevelDB è il database di stato predefinito incorporato nel processo che coinvolge i peer e permette la memorizzazione dei dati del chaincode come coppie chiave-valore. CouchDB è un database di stato esterno e opzionale che fornisce un supporto ulteriore per le query quando i dati del codice chaincode sono modellati come JSON [16].

### 2.2.6 Ciclo di vita delle transazioni

Come è stato detto in precedenza, il ciclo di vita delle transazioni in Hyperledger Fabric è stato modificato e migliorato rispetto altre Blockchain. Il vecchio modello prevedeva una prima fase, chiamata Order, in cui le transazioni erano aggiunte al ledger in un determinato ordine e poi inviate a tutti i peer; nella seconda e ultima fase, chiamata Execute, le transazioni erano eseguite sequenzialmente (ad esempio usando gli smart contract) in tutti i peer. Questo comportava, in primo luogo, che le transazioni dovessero essere eseguite deterministicamente, affinché non vi fossero

incongruenze di risultato tra i peer, e, in secondo luogo, l'impossibilità di utilizzare linguaggi general-purpose per gli smart contract. Il nuovo modello prevede una prima fase, chiamata Execute, in cui le transazioni sono eseguite tramite chaincode in un qualsiasi ordine, possibilmente anche in parallelo; nella seconda fase, chiamata Order, dopo che un numero sufficiente di nodi ha approvato i risultati della transazione, essa viene aggiunta al ledger dandole un ordine, e inviata a tutti i peer; nell'ultima fase, chiamata Validate, ogni peer valida e applica le transazioni del ledger in sequenza, controllando se una transazione successiva è stata invalidata da una precedente [16]. Andando più nel dettaglio, il flusso delle transazioni segue questi passi:

1) L'utente di un'applicazione che vuole compiere la transazione deve essersi registrato presso una certificate authority (CA) e aver ricevuto il materiale criptografico necessario ad autenticarsi, il channel deve essere stato configurato e attivato, il chaincode deve essere stato installato sui peer e sul channel e le sue endorsement policy devono specificare i nodi designati ad essere endorser (figura 2.3).


**Figura 2.3:** transazione di esempio (modificata a partire da [16]).

2) Il client dell'utente sfrutta una delle API disponibili (Node, Java o Python) dell'SDK (Software Development Kit) supportato per generare una proposta di transazione. La proposta è una richiesta di invocazione di una funzione del chaincode in modo che i dati possano essere letti e/o scritti nel ledger. L'SDK impacchetta la proposta di transazione nell'opportuno formato (protocollo buffer su gRPC) e prende le credenziali criptografiche dell'utente per firmarla in maniera univoca (figura 2.4).

3) Gli endorser verificano che la proposta di transazione sia sintatticamente corretta, che non sia già stata presentata in passato (protezione da attacchi di tipo replay), che la firma sia valida (usando il MSP) e che il mittente sia autorizzato a compiere quella determinata operazione in quel channel. Se la verifica non ha riscontrato problemi, gli endorser approvano l'operazione ed eseguono la funzione sul database dello stato attuale e inviano all'SDK, e alla relativa applicazione, la risposta alla proposta con i risultati e la loro firma. In questa fase il ledger non viene aggiornato (figura 2.5).

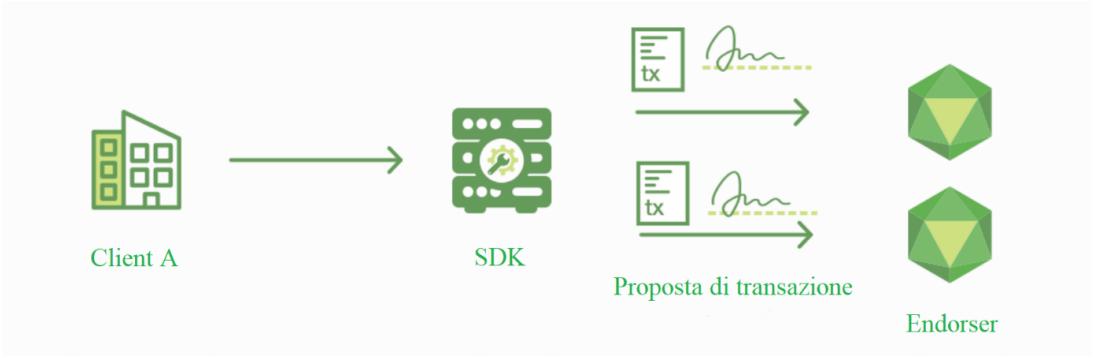



**Figura 2.4:** il client A inizia una transazione (modificata a partire da [16]).

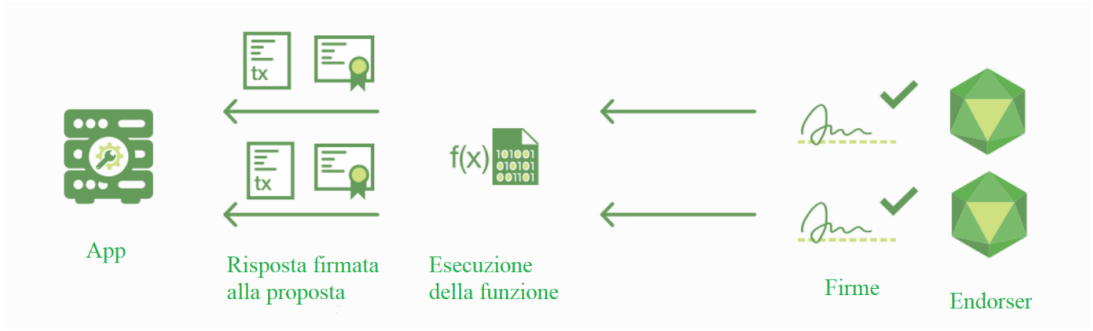



**Figura 2.5:** verifica ed esecuzione da parte degli endorser (modificata a partire da [16]).

4) Il client verifica le firme degli endorser e compara le varie risposte per accertarsi che siamo identiche (figura 2.6). Nel caso in cui il chaincode abbia solamente interrogato il ledger per ottenere un'informazione, il flusso si conclude in questo passaggio. Nel caso in cui il chaincode voglia aggiornare il ledger, il flusso continua coinvolgendo il servizio di ordering.

5) Se le firme sono corrette e le risposte sono tutte uguali, l'applicazione può inviare in broadcast al servizio di ordering un messaggio contenente la proposta di transazione, la relativa risposta e le informazioni finora raccolte. Il servizio di ordering riceve messaggi da tutti i channel della rete e li ordina cronologicamente in base ai channel ID. Infine, vengono creati blocchi di transazioni per ogni channel (figura 2.7).

6) I blocchi di transazioni di uno specifico channel vengono consegnati ai relativi peer. Le transazioni all'interno del blocco vengono convalidate per garantire che l'endorsement policy sia soddisfatta e che non siano state apportate modifiche allo stato del ledger nel periodo di tempo trascorso dall'esecuzione della transazione fino a quel momento. Le transazioni nel blocco sono contrassegnate come valide o non valide (figura 2.8).


**Figura 2.6:** verifica delle risposte (modificata a partire da [16]).


**Figura 2.7:** servizio di ordering (modificata a partire da [16]).

7) Ogni peer aggiunge il blocco alla catena del channel e, per ciascuna transazione valida, le relative modifiche al database dello stato corrente. Infine, vengono emessi due eventi destinati all'applicazione: uno per notificare che la transazione è stata immutabilmente aggiunta alla catena e un altro per notificare se la transazione è stata convalidata o invalidata (figura 2.9).

Per concludere questo paragrafo, sono da sottolineare quattro questioni importanti riguardanti il modello Execute-Order-Validate. In primo luogo, la separazione tra l'esecuzione della transazione (Execute) e l'effettivo aggiornamento del ledger (Validate). In secondo luogo, il fatto che i peer possano assumere ruoli e compiti diversi nel processo di raggiungimento del consenso: ad esempio, la fase di esecuzione del chaincode può essere svolta anche solo da alcuni e non da tutti (come invece capita per la validazione), in base alle policy di endorsement. Queste policy specificano, tra le altre cose, chi può eseguire determinate transazioni; è possibile quindi impedire ai non autorizzati la visione e l'esecuzione di specifici smart contract. In terzo luogo, l'aumento considerevole del volume di transazioni eseguite dovuto all'esecuzione in parallelo. Da ultimo, l'esplicito assenso per quanto riguarda l'esito delle transazioni prima dell'inserimento nel ledger permette a Fabric di usare chaincode non deterministico, quindi di utilizzare i linguaggi general-purpose [16, 17].

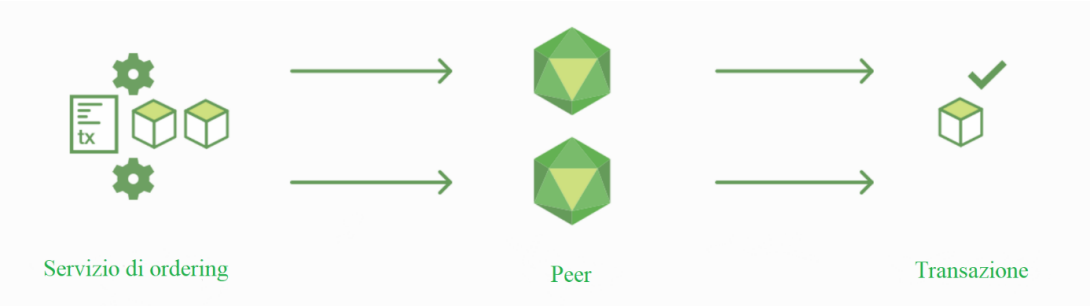



**Figura 2.8:** validazione della transazione (modificata a partire da [16]).

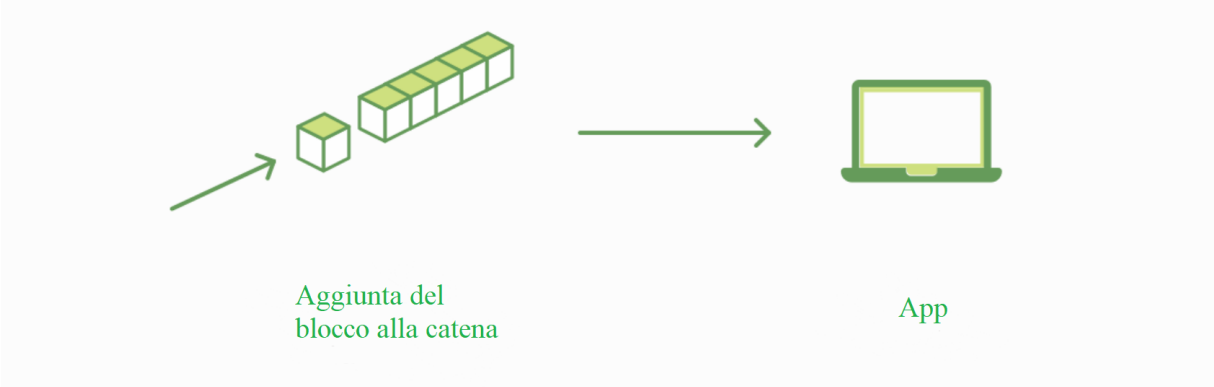



**Figura 2.9:** aggiornamento ledger (modificata a partire da [16]).

### 2.2.7 Consenso

Come già detto in precedenza, il consenso è definito come la verifica da parte dei peer della correttezza di un insieme di transazioni inserite all'interno di un blocco da aggiungere al ledger; esso viene raggiunto, in ultima analisi, quando l'ordine e i risultati delle transazioni di un blocco hanno soddisfatto i criteri delle policy.

L'ordine delle transazioni è delegato a un componente modulare, chiamato servizio di ordering, che ha il compito di gestire il consenso; esso è disgiunto logicamente dai nodi che eseguono le transazioni (gli endorser) e che mantengono il ledger (i peer). Poiché il consenso è modulare, le sue implementazioni possono essere molteplici. Questa architettura modulare consente alla piattaforma di contare su toolkit ben consolidati per l'ordering CFT (Crash Fault-Tolerant) o BFT (Byzantine Fault-Tolerant). CFT significa che l'ordering viene eseguito correttamente anche in presenza di alcuni crash o arresti arbitrari del sistema; BFT include il concetto di CFT, ma lo estende al caso di errori causati intenzionalmente da malintenzionati. Attualmente in Fabric sono disponibili due diverse implementazioni del servizio di ordering di tipo CFT. Il primo è Raft che si basa su una libreria Etcd del protocollo Raft (Etcd è un archivio distribuito e affidabile di dati salvati sotto forma di coppie

chiave-valore). Il secondo è Kafka che internamente utilizza Zookeeper. Raft e Kafka seguono entrambi un modello "leader-follower", in cui un nodo leader viene eletto (in ogni channel) e le sue decisioni vengono replicate dai suoi follower. I servizi di ordinazione di Raft sono più facili da configurare e gestire rispetto ai servizi di ordinazione basati su Kafka; in più Kafka e Zookeeper non sono progettati per essere utilizzati in reti estese. Tuttavia, è bene sottolineare che questi servizi non si escludono a vicenda: una rete Fabric può disporre di più servizi finalizzati ad ordinare temporalmente le transazioni che supportano diverse applicazioni o requisiti applicativi [16].

### 2.2.8 Identità e Membership Service Provider

I diversi attori di una rete Hyperledger Fabric possono essere peer, applicazioni client, amministratori, ecc., solo per citarne alcuni. Ognuno di questi attori ha un'identità digitale incapsulata in un certificato digitale X.509. Queste identità sono importanti perché in base ad esse si concedono, oppure no, le autorizzazioni sulle risorse, sulle operazioni e sull'accesso alle informazioni. Affinché un'identità sia verificabile, deve provenire da un'autorità attendibile: il Membership Service Provider (MSP) è il modo in cui questo viene realizzato in Fabric. In particolare, un MSP è un componente che definisce le regole che governano le identità valide per questa organizzazione. L'implementazione MSP predefinita in Fabric utilizza i certificati X.509, rilasciati da una Certificate Authority (CA), come identità, adottando il modello gerarchico tradizionale della Public Key Infrastructure (PKI). Da un lato, una PKI fornisce vari tipi di identità verificabili; dall'altro, un MSP determina quali di quelle sia un membro fidato (in inglese, trusted member) di una specifica sotto-rete. Più concretamente, il componente MSP astrae tutti i meccanismi e i protocolli di criptografia dietro l'emissione e la convalida dei certificati e l'autenticazione dell'utente. Un MSP può definire la propria nozione di identità e le regole con cui tali identità sono governate (convalida dell'identità) e autenticate (generazione e verifica delle firme). Una rete Hyperledger Fabric può essere governata da uno o più MSP. Ciò fornisce modularità alle operazioni di membership (appartenenza) e l'interoperabilità tra i suoi diversi standard e architetture [16].

### 2.2.9 Proprietà

Oltre alle proprietà base della tecnologia Blockchain, Fabric ne possiede altre qui elencate [16]:

- **Autenticazione**: I partecipanti hanno un'identità certificata tramite certificato che può essere eventualmente verificata.
- **Autorizzazione**: la rete è permissioned, quindi le operazioni che si possono eseguire e i dati a cui si può accedere sono vincolati alle autorizzazioni che si

posseggono; il controllo d'accesso è dinamico, vale a dire che possono cambiare i permessi, ad esempio, qualora il proprietario dei dati decidesse di condividerli con qualcun altro.

- **Efficienza**: oltre agli aspetti già sottolineati per la Blockchain, nel caso di Fabric il nuovo ciclo di vita permette un aumento del volume delle transazioni e una maggiore flessibilità. Ad esso si aggiunge il consenso privo di mining che incrementa la velocità di registrazione delle transazioni, aggiunto ad una maggiore scalabilità.

- **Riservatezza**: la piattaforma si serve dei channel, un concetto nuovo nell'ambiente Blockchain, utilizzato per ridurre la visibilità di sottoinsiemi di transazioni e dati a determinate organizzazioni o peer.

## 2.3 Hyperledger Composer

Hyperledger Composer è un framework costruito con JavaScript che supporta la Blockchain Hyperledger Fabric; è fornito di tool (tra i quali si ricordano Node.js, npm, CLI e gli editor più utilizzati) che semplificano e velocizzano lo sviluppo e il testing di smart contract e applicazioni Blockchain. Inoltre consente di modellare le reti aziendali (Business Network) e integrare i sistemi e i dati esistenti con le applicazioni Blockchain. Per creare un'astrazione di una Business Network esiste un linguaggio specifico per la modellazione e un set di API per definire e utilizzare rapidamente applicazioni che consentono ai partecipanti (participant) di inviare transazioni (transaction) che scambiano risorse (asset), oltre a diverse altre operazioni.

Nella figura 2.10 si può vedere lo schema riassuntivo delle parti che compongono la Business Network Definition (BND), vale a dire il modello completo della Business Network: il Model File (contenente le definizioni degli asset, dei participant, delle transaction e degli event), lo Script File (contenente le funzioni delle transazioni), l'Access Control (contenente le regole del controllo di accesso) e il Query File (contenente le definizioni delle query per interrogare la Blockchain). Il BND viene poi archiviato all'interno del Business Network Archive (BNA), un archivio pronto per essere inserito in un ledger distribuito, in locale oppure online.

Composer può essere utilizzato in vari modi: attraverso un'interfaccia da browser, chiamata Hyperledger Composer Playground (disponibile online senza necessità di installazione o con un'installazione in locale che permette di creare e testare offline le Business Network), oppure installando la versione da sviluppatore che sfrutta al massimo le sue caratteristiche [20].

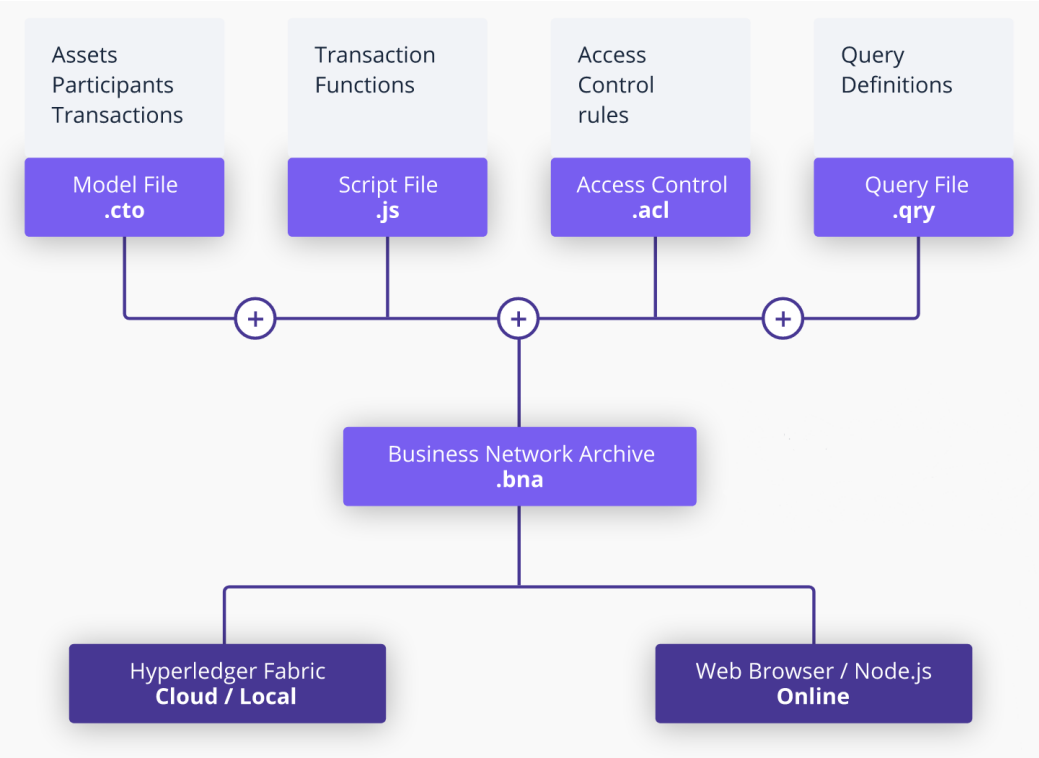



**Figura 2.10:** schema della Business Network Definition (modificata a partire da [20]).

### 2.3.1 Business Network Definition

Di seguito sono descritti i concetti che costituiscono la Business Network Definition (BND), modello che è alla base di Composer [20]:

1) Il **Business Network Model** definisce la struttura e le relazioni tra gli elementi del modello. Essi si suddividono in:

   - **Asset**: sono beni tangibili o intangibili, servizi o proprietà e sono salvate negli appositi registri. Gli asset devono avere un identificatore univoco (oltre ad altre proprietà che si possono definire all'occorrenza) e possono essere correlati ad altri asset o participant.
   - **Participant**: sono i membri di una Business Network (BN); possono possedere asset e effettuare transazioni. Come per gli asset, anche i participant devono avere un identificatore univoco e possono avere delle proprietà qualora richiesto.
   - **Transaction**: sono il meccanismo attraverso cui i partecipanti interagiscono con gli asset scambiandoseli, creandoli, modificandoli o eliminandoli.

- **Event**: sono definiti come gli asset e i participant, dopodiché possono essere emessi dal processore delle transaction function per notificare ai sistemi esterni che qualcosa di importante è avvenuto all'interno del ledger.

2) Le **Transaction Function** implementano in JavaScript il comportamento delle transazioni.

3) L'**Access Control** contiene una serie di regole di controllo dell'accesso che definiscono i diritti dei diversi partecipanti nella Business Network ad accedere agli asset o ad eseguire determinate transazioni oppure ad avere specifici privilegi.

4) Le **Query** vengono utilizzate per restituire dati sul World State, cioè sullo stato corrente della Blockchain. Sono definite all'interno di una Business Network e possono includere parametri variabili per un'agevole personalizzazione. Le query vengono inviate attraverso l'utilizzo delle API di Hyperledger Composer.

### 2.3.2 Blockchain State Storage

Tutte le transazioni eseguite in una Business Network sono memorizzate sul ledger e lo stato corrente degli asset e dei partecipanti è memorizzato nel database di stato. La Blockchain distribuisce il ledger e il database di stato tra un insieme di peer e garantisce che i loro aggiornamenti siano coerenti tra tutti i peer utilizzando un algoritmo di consenso [20]. La memorizzazione delle informazioni è quindi concettualmente uguale a quella di Hyperledger Fabric, tranne per il fatto che il termine ledger in Composer viene usato per indicare la chain in Fabric e per la presenza di registri che suddividono le informazioni sul database di stato in categorie (asset, participant, transaction e identità).

### 2.3.3 Business Network card

Le BN card sono composte da un'identità (identity), un connection profile (profilo di connessione) e dei metadati che talvolta contengono il nome della BN a cui connettersi. Le Business Network card semplificano il processo di connessione ad una BN ed estendono il concetto di identità all'infuori della BN in un wallet (portafoglio) con diverse identità, ognuna associata ad una BN e ad un profilo di connessione.

Un'identità è un certificato digitale e una chiave privata. Le identità vengono utilizzate per effettuare transazioni su una BN e devono essere associate a un partecipante di tale BN. Così facendo una singola identità consente all'utente di quella BN card di effettuare transazioni su una specifica BN attraverso quel partecipante.

I connection profile vengono utilizzati per definire il sistema a cui connettersi; concretamente è un documento JSON. Questi profili sono di solito forniti dall'amministratore del sistema a cui si riferiscono e dovrebbero essere utilizzati per creare BN card al fine di essere in grado di connettersi a quel sistema [20].

### 2.3.4 Architettura delle soluzioni Composer

Hyperledger Composer consente di creare rapidamente soluzioni "full-stack", vale a dire soluzioni che comprendono la logica del business (che "gira" sulla Blockchain), le API REST che espongono questa logica alle applicazioni web e/o mobili, oltre all'integrazione della Blockchain con i sistemi aziendali esistenti. Nella figura 2.11 è possibile vedere più nel dettaglio i componenti che costituiscono il framework [20]:

- **Yeoman**: è un framework che genera codice e, in particolare, crea gli scheletri delle applicazioni web Angular, delle applicazioni Node.js e della Business Network.
- **Angular**: è una piattaforma attraverso cui è possibile realizzare applicazioni web che vengono eseguite completamente nei browser.
- **Server REST**: converte il modello di una BN in una serie di API REST che possono essere utilizzate dalle applicazioni web, fornisce al momento dell'esecuzione l'implementazione delle operazioni di creazione, lettura, aggiornamento ed eliminazione degli asset e dei participant e permette di richiedere il processamento o il recupero di transazioni.
- **CLI**: (Command Line Interface) viene adoperata per inserire e gestire le definizioni delle Business Network.
- **SDK**: è un insieme di API Node.js che consente di creare applicazioni per gestire e interagire con le BN distribuite.
- **Web Playground**: è un'interfaccia utente Web per definire e testare le BN.
- **Runtime**: sono i diversi sistemi che permettono di eseguire la Business Network.

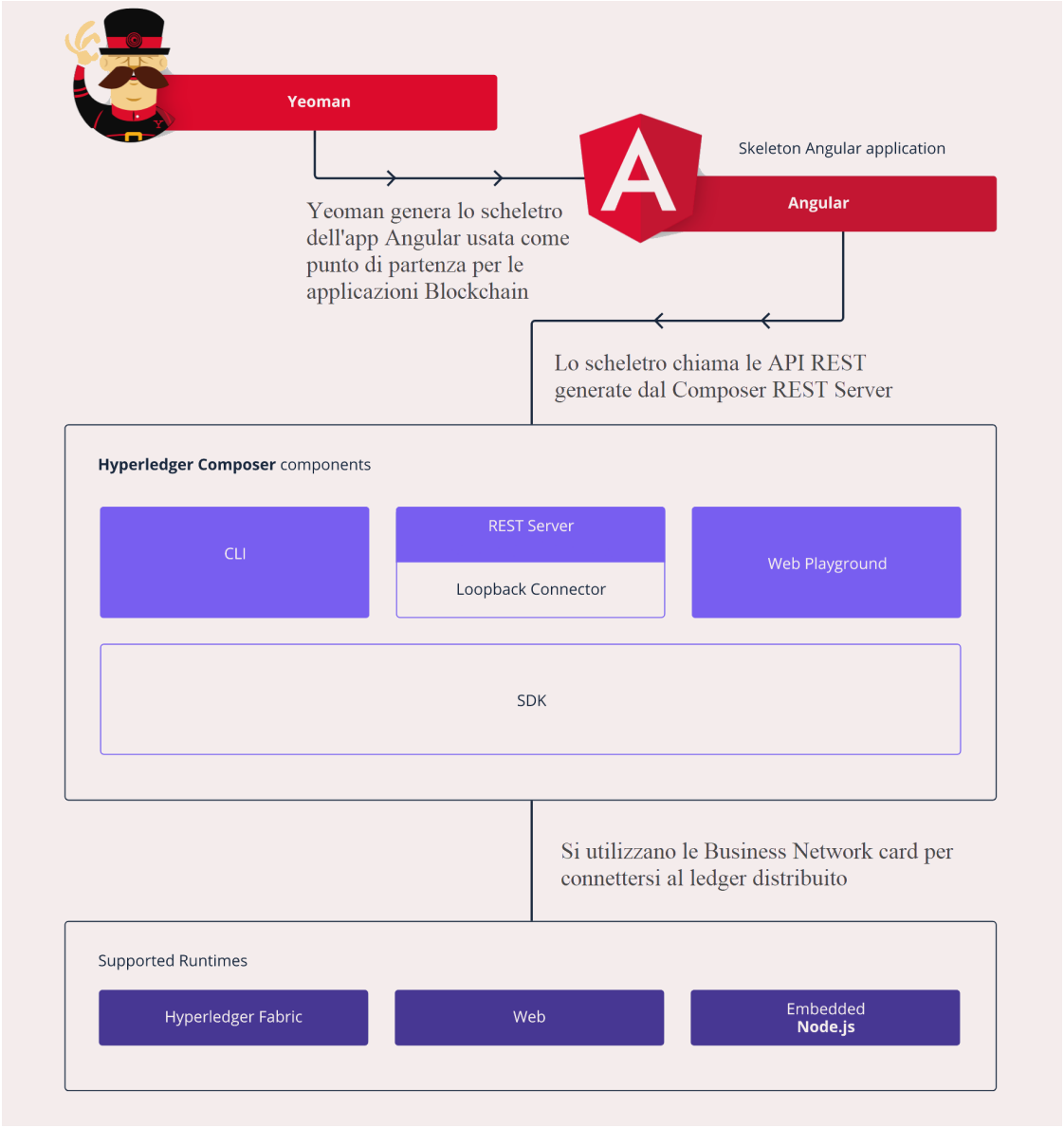



**Figura 2.11:** architettura Hyperledger Composer (modificata a partire da [20]).

# Capitolo 3

# Stato dell'arte

La tecnologia Blockchain, dopo essere nata come infrastruttura per la creazione e lo scambio di criptovalute (prima tra tutte Bitcoin [3]) e quindi aver avuto come contesto applicativo l'economia e la finanza (si può prendere anche come esempio BitPesa [21, 22], una piattaforma che ha come fine quello di agevolare il trasferimento di denaro da e per l'Africa oppure Nebeus [21, 23], una crypto piattaforma che vuole fornire servizi bancari e finanziari a persone che sono escluse dalle banche tradizionali), è stata sperimentata anche in altri ambiti: nelle filiere alimentari per la tracciabilità dei prodotti (ad esempio Carrefour, Nestlé e IBM hanno iniziato una collaborazione per implementare una Blockchain che tracci il cibo lungo tutta la filiera, dal produttore al consumatore [24]), per il contrasto della contraffazione e per il controllo della qualità (come ad esempio Thomas Crown Art smART un sistema basato su Blockchain che fornisce una Proof of Provenance (PoP) immutabile delle opere d'arte [25]), nella mobilità (con la missione di rendere i servizi di mobilità più efficienti, convenienti, ecologici, sicuri e meno congestionati, come si propone il consorzio MOBI [26]), nel sistema di voto elettronico [27], nella distribuzione dell'energia tra pari all'interno di comunità energetiche [28], nella governance per debellare corruzione, inefficienze e concentrazione di potere [29], nell'ambito assicurativo [30, 9, 31], nella gestione della proprietà intellettuale [73], solo per fare alcuni esempi [33].

Questa tesi in particolare si concentra sull'applicazione di Blockchain nell'ambito della sanità; in particolare, nelle prossime sezioni verranno illustrate le attuali principali aree di studio e di applicazione, le problematiche, le teoriche soluzioni Blockchain, le proprietà fornite e i progetti concreti considerati più rilevanti.

## 3.1 Gestione dei dati sanitari

Nell'attuale regolamento generale sulla protezione dei dati dell'Unione Europea, ovvero il GDPR (General Data Protection Regulation), all'articolo 4 punto 15) è

scritto che i dati sanitari sono "dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute". La gestione di questi dati attualmente presenta diverse problematiche (riportate nella sezione sottostante) che però possono essere risolte, o quanto meno limitate, utilizzando la tecnologia Blockchain. Per questo motivo sarà analizzata una sua applicazione teorica con le relative proprietà e successivamente verranno descritti i progetti attualmente realizzati o in procinto di esserlo.

### 3.1.1 Problematiche

Vi sono varie questioni irrisolte legate ai dati sanitari gestiti dalle strutture mediche:

- La mancanza di controllo e possesso da parte dei pazienti sulle proprie informazioni (esiti degli esami, prescrizioni mediche, anamnesi, attività diagnostico-terapeutiche, ecc.).
- La difficoltà a consultarle, a ottenerle ed eventualmente a condividerle in maniera comoda con persone di fiducia come i propri parenti.
- I problemi di sicurezza (ad esempio i furti di documenti sensibili).
- La frammentazione della storia clinica del paziente tra tutte le strutture sanitarie che lo hanno visitato e curato. Questo impedisce di vedere nel complesso la situazione della persona, limita le potenzialità di utilizzo degli algoritmi alla base dei Big Data (che richiedono grandi moli di dati) e porta sovente a rifare esami già effettuati, oltre a compiere anamnesi e diagnosi approssimative.
- La mancanza di fiducia nel fornire i propri dati per scopi di ricerca.
- Un rapporto tra medico curante e paziente migliorabile da una comunicazione al passo con i tempi e da una maggiore condivisione di informazioni.
- Il formato cartaceo dei documenti, con i relativi problemi di spazio fisico di archiviazione, la mancanza di backup e le difficoltà di accesso, non ancora completamente sostituito da quello digitale.
- Un enorme spreco di tempo, denaro e personale che pesa su un sistema sanitario a continuo rischio collasso.

### 3.1.2 Soluzione Blockchain e relativi vantaggi

In generale, una possibile soluzione alle problematiche sopra elencate sarebbe quella di creare un sistema Blockchain per l'acquisizione, il salvataggio e la condivisione dei dati sanitari che metta al centro il paziente e le sue esigenze[34]. Innanzitutto,

gli stakeholder (pazienti, dottori, ricercatori, ospedali, aziende, università, parenti, Stato, assicurazioni, ecc.) dovrebbero fornire la loro identità. Solo successivamente, potrebbero accedere e interagire col sistema attraverso un'interfaccia (app o browser) inserendo, visionando, condividendo e scaricando le informazioni sanitarie. In particolare, esse sarebbero criptate, firmate digitalmente e memorizzate all'interno di database gestiti da alcuni stakeholder come gli ospedali, i dottori, le università, i centri di ricerca, ecc. o all'interno di un unico data lake. Nella Blockchain, invece, dovrebbero essere presenti delle liste di metadati che puntino alla posizione effettiva dei dati nei database; ogni lista si dovrebbe riferire a un paziente[35]. Utilizzando queste liste il sistema potrebbe fornire e visualizzare nelle interfacce grafiche tutti i dati deframmentati del paziente, o parte di essi.

I vantaggi di questa soluzione sarebbero molteplici: il paziente tornerebbe ad avere piena autorità sui propri dati, sarebbe in grado di vederli deframmentati in modo agevole, in formato digitale e non più cartaceo, potrebbe condividerli selettivamente (ad esempio con i parenti o con i ricercatori), il sistema sarebbe sicuro (utilizzando la criptografia in trasmissione e in memorizzazione) e immune a manomissioni (per la parte che compete alla Blockchain, per i database dipende dalla loro implementazione). Inoltre, il sistema non sarebbe centralizzato e non sarebbero presenti terze parti addette al controllo del suo corretto funzionamento, perché completamente automatizzato attraverso smart contract. L'automazione, il controllo dei partecipanti alla rete e dei loro accessi alle risorse, il rispetto della privacy, immutabilità dei metadati salvati nella Blockchain, la sicurezza e le altre caratteristiche tipiche della Blockchain aumenterebbero la fiducia del paziente nel sistema. I dati non sarebbero salvati nella Blockchain, ma nei database, perché l'eccessiva ridondanza e la probabile enorme mole di informazioni porterebbe il sistema alla saturazione, compromettendo la possibilità di scalare a livello nazionale o mondiale. Complessivamente tutte queste caratteristiche porterebbero ad un incremento dell'efficienza dei processi che utilizzerebbero i documenti sanitari.

### 3.1.3 Proprietà della soluzione

Di seguito vengono riportate le proprietà della soluzione Blockchain descritta nella sezione precedente:

1) **Integrità**: proteggere le informazioni da modifiche o cancellazioni involontarie oppure effettuate volontariamente e con cattive intenzioni da terze parti.

2) **Immutabilità**: impedire modifiche nel tempo dei documenti.

3) **Riservatezza**: impedire ai partecipanti o ad entità (persone o macchine) di leggere i dati.

4) **Autenticazione**: fornire un certificato o comunque un'identità verificabile prima di poter accedere al sistema.

5) **Autorizzazione**: avere partecipanti con ruoli diversi che comportano autorizzazioni (di creazione, di accesso, di esecuzione, ecc.) differenti.

6) **Disponibilità**: avere le informazioni sempre consultabili.

7) **Scalabilità**: mantenere le stesse prestazioni e la stessa efficienza nonostante l'aumento o la diminuzione delle dimensioni del sistema.

8) **Sequenzialità**: rilevare e impedire la modifica della sequenza temporale delle operazioni.

9) **Non ripudio**: associare azioni o cambiamenti ad un unico e specifico individuo (l'autore).

### 3.1.4 Progetti emblematici

Nella sezione precedente è stata presentata una soluzione Blockchain teorica, mentre di seguito verranno riportati dei progetti concreti:

- **RecordsKeeper**: è una piattaforma basata sulla tecnologia Multichain (utilizzata per creare e installare Blockchain con funzionalità aggiuntive di privacy e controllo [36]) che fornisce un sistema decentralizzato disponibile a livello globale per la gestione di qualsiasi tipo di dato (quindi potenzialmente anche quelli sanitari). Offre diverse soluzioni per l'archiviazione (tramite database NoSQL) e la messa in sicurezza dei dati strutturati di organizzazioni e singoli individui. Il RecordsKeeper sfrutta i vantaggi della rete Blockchain per creare un ecosistema con trasferimento sicuro dei dati, autorizzazione all'accesso, oltre che integrità ed autenticità. Tutti i record possono essere inseriti nel formato coppia chiave-valore con un piccolo costo di commissione in token XRK (la criptovaluta alla base di RecordsKeeper) per ogni transazione e gli stessi dati possono essere successivamente recuperati utilizzando la stessa chiave o l'ID della transazione in maniera gratuita per tutta la vita. La Blockchain di RecordsKeeper, infatti, è una Blockchain pubblica con mining; essendo pubblica è possibile per chiunque verificare l'autenticità, integrità e immutabilità dei record salvati. In sintesi il sistema segue queste fasi (vedere figura 3.1):

  1) Il generico utente acquisisce i token XRK e li mette nel proprio wallet (portafoglio) XRK.
  2) L'utente inserisce il record nel sistema (quest'azione causa il salvataggio di metadati firmati nel ledger della Blockchain), che viene criptato e memorizzato in un database esterno alla Blockchain.
  3) I miner confermano la transazione aggiungendo un nuovo blocco.

4) Vengono ripagati per il loro lavoro con una ricompensa in criptomonete.

5) L'utente può condividere il record con altri user usando la chiave del record o l'ID della transazione per identificarla; essi possono verificare l'autenticità e l'integrità del dato in qualsiasi momento nel futuro tramite.

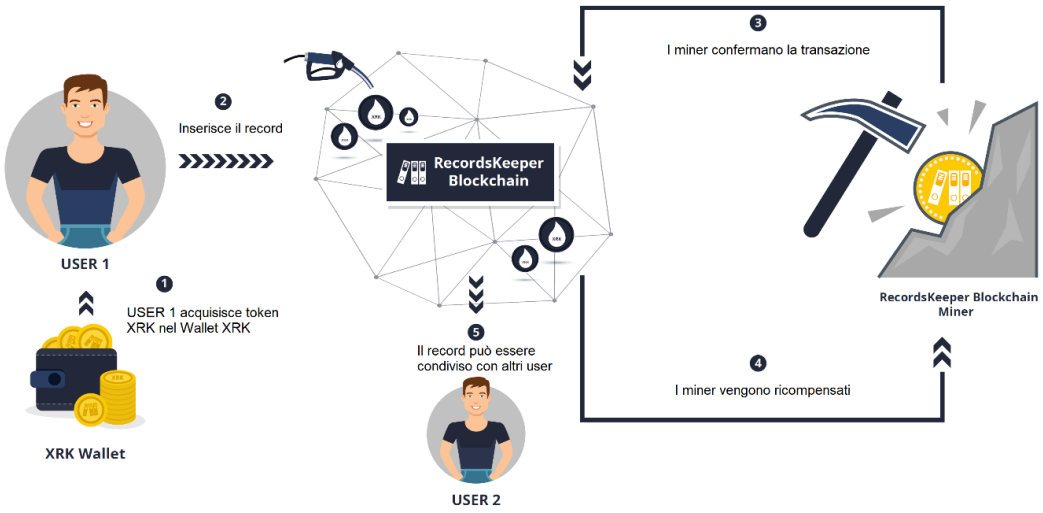



**Figura 3.1:** schema di funzionamento di RecordsKeeper e XRK (modificata a partire da [37]).

RecordsKeeper offre una serie di librerie e API open-source per pubblicare i record nel sistema utilizzabili all'interno di siti web, di servizi di backend, di app per smartphone e tablet, di applicazioni desktop, i server, ecc. [37].

- **MedRec**: è un sistema che fornisce al paziente una visione della storia medica completa, trasparente e facilmente accessibile. Si tratta di un sistema di accesso e validazione distribuito che utilizza la Blockchain Ethereum per sostituire gli intermediari solitamente presenti nei sistemi centralizzati. Medrec non "memorizza" direttamente il record, piuttosto codifica i metadati che consentono l'accesso sicuro ai record da parte dei pazienti, unificando l'accesso ai dati tra diversi provider. Effettua di fatto una deframmentazione che permette al paziente di vedere tutti i propri dati in un "luogo" solo (account personale sul sito web), ordinati per data di inserimento nel sistema o di creazione e suddivisi in categorie (ad esempio, esami del sangue, vaccinazioni, visite, ecc.). I metadati contengono informazioni sulla proprietà, l'autorizzazione e l'integrità dei dati richiesti.

MedRec utilizza tre tipi di smart contract per regolare il funzionamento del sistema: il registrar contract per mappare i partecipanti (pazienti, provider e assicuratori) con la loro identità Ethereum (equivalente ad una chiave pubblica), il patient-provider relationship contract per collegare due nodi del sistema, dove uno dei due memorizza e gestisce i dati sanitari dell'altro, e infine il summary contract che riassume le relazioni dello specifico paziente con gli altri partecipanti. L'accettazione, il rifiuto o la cancellazione delle relazioni sono controllati dal paziente, dando pieno controllo su quali record della loro storia desiderano riconoscere.

Quando il paziente richiede l'accesso ad uno specifico record, viene controllata la sua identità e le sue autorizzazioni; se l'esito è positivo, il sistema esegue una query sul database locale del nodo e restituisce il risultato al client [38].

- **Solve.Care**: è una piattaforma con svariati obiettivi tra cui la riduzione della frammentazione delle informazioni sanitarie, dei costi burocratici, degli sprechi di tempo, delle frodi e degli intermediari, a cui vanno aggiunti l'aumento della fiducia della sanità e miglioramento nell'accesso alle cure. Per raggiungerli è stata creata un'app che fornisce una serie di servizi agli stakeholder, ma soprattutto è stato implementato un sistema basato sulla tecnologia Blockchain per decentralizzare e automatizzare tutta una serie di processi amministrativi molto onerosi da gestire. Ad esempio, l'autorità di controllo e decisionale viene delegata al paziente e al provider (senza quindi terze parti fidate), i pagamenti vengono effettuati attraverso delle criptomonete (velocizzando il ciclo di pagamento delle prestazioni sanitarie) e le relazioni (paziente e dottore, paziente e assicuratore, paziente e parente, ecc.) che intercorrono tra due stakeholder vengono definite e incapsulate attraverso gli smart contract. Il sistema inserisce nel ledger distribuito solamente i log degli eventi che hanno luogo tra i diversi partecipanti, notificandoli poi ai nodi interessati; i dati relativi agli eventi (ad esempio, la prescrizione medica, le note del medico, i risultati delle analisi, ecc.) vengono mantenuti all'infuori della Blockchain (e solo per la durata autorizzata), assicurando la loro trasmissione sicura (con proprietà di riservatezza e autenticazione) tramite doppia cifratura [39, 40]. I vantaggi per gli stakeholder coinvolti si possono riassumere come segue:

  1) Ai **singoli individui** e alle **famiglie** il sistema permette di fissare appuntamenti, condividere documenti, confrontare i prezzi, massimizzare gli sconti, gestire le prescrizioni, visualizzare le informazioni sull'assistenza personalizzata, effettuare pagamenti precisi.
  2) Ai **dottori** e in generale ai **fornitori di assistenza sanitaria** il sistema permette di ridurre gli oneri amministrativi, migliorare le cure e di essere a disposizione per l'effettivo assegnamento delle cure. Pubblica la loro

disponibilità, verifica la copertura sanitaria e la possibilità dei pazienti di dedurre i costi, accede in maniera accurata e appropriata ai record, gestisce il consenso informato, rilascia le prescrizioni e permette il coordinamento tra specialisti, laboratori e terapisti.

3) Agli **assicuratori** il sistema permette di migliorare drasticamente le relazioni con i fornitori di assistenza sanitaria e le tempistiche dei pagamenti (più precisi e puntuali). Automatizza e semplifica la gestione dei vari casi. Riduce radicalmente il carico amministrativo e la sua complessità. Contribuisce attivamente a migliorare il benessere del cliente, premiando le eventuali prestazioni eccellenti dell'operatore sanitario e promuovendo comportamenti più sani.
4) Alle **istituzioni regionali e statali** il sistema permette di concentrarsi maggiormente sui bisogni della popolazione e meno sulla gestione dei fornitori e dei sistemi IT.

Solve.Care è composta da diversi componenti:

1) **Care.Wallet** è progettato come app Blockchain per aiutare i fornitori e i pazienti a comunicare e gestire l'erogazione dell'assistenza. Care.Wallet ospita Care.Card e Care.Coin che danno al utente il pieno controllo sulle informazioni e sulle azioni. Care.Wallet e Care.Card si sincronizzano automaticamente con altri wallet, con conseguente coordinamento in tempo reale tra tutte le parti interessate.
2) **Care.Card** sono applicazioni appositamente progettate che possono essere collegate, sovrapposte e sincronizzate (vedere figura 3.2).
3) **Care.Marketplace** è lo store in cui si possono ottenere le Care.Card.
4) **Care.Coin** è una moneta digitale di pagamento intelligente che attribuisce accountability, trasparenza, proof of service/autorizzazione e protezione da attacchi replay alle transazioni sanitarie. Questa criptomoneta è progettata per effettuare pagamenti per servizi sanitari verificabili tra membri di una rete amministrativa di assistenza. Il suo valore non varia ed è sostenuto da risorse della valuta a cui è collegato. Care.Coin non può essere scambiato sui cripto-exchange e non vi è un limite alla sua creazione.
5) **CAN token** è un token a valore variabile che cambia nel prezzo in base alla domanda e può essere scambiato liberamente. Viene utilizzato dai clienti per pagare i servizi forniti da Solve.Care, ma non può essere utilizzato come valuta di pagamento tra i membri della rete. Il numero di token che si possono generare è limitato.
6) **Care.Protocol** è utilizzato per connettere e sincronizzare wallet, card e coin tra stakeholder per coordinare le cure e automatizzare le transazioni.

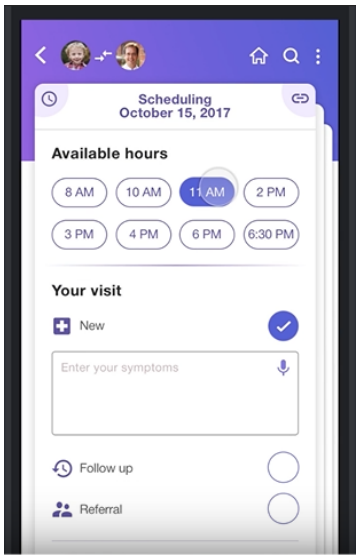



**Figura 3.2:** Care.Card per prenotare una visita in un determinato orario presso un dottore (tratta da [39]).

7) **Care.Vault** è un modulo di Care.Protocol per organizzare i dati all'interno della piattaforma e dai sistemi esterni.

## 3.2 Monitoraggio della salute

Il monitoraggio della salute personale attraverso i wearable (dispositivi indossabili) e la tele-assistenza tramite l'IoT (Internet of Things), oltre che un'eventuale elaborazione dei dati raccolti tramite l'AI (Artificial Intelligence), è quanto mai attuale. In un mondo iperconnesso e tecnologicamente avanzato in cui la popolazione sta invecchiando, il costo del welfare è in costante aumento e l'assistenza ai pazienti si sta spostando dagli ospedali e dalle cliniche verso le abitazioni per ridurre i costi e sgravare le strutture. Curare gli ammalati o controllare che seguano le terapie richiede l'uso massiccio di apparecchiature di diagnostica remote ovvero apparecchiature wearable connesse a Internet che, attraverso sensori, possano ottenere e trasmettere dati su avvenimenti che li riguardano o sulla loro condizione (in maniera continua). Vigilare sui pazienti sovente vuol dire anche verificare che essi seguano le terapie prescritte (e quindi le tempistiche di assunzione, la frequenza e il dosaggio). Le apparecchiature dovrebbero essere in grado di misurare i valori vitali (la pressione del sangue, la frequenza cardiaca, la temperatura del corpo, ecc.), iniettare insulina, esercitare una stimolazione tramite calore, vibrazione o scarica elettrica, emettere un segnale che attiri l'attenzione degli infermieri e, infine, connettersi da remoto ad un centro di assistenza dove degli specialisti possano esaminare le informazioni inviate e reagire adeguatamente [41].

Un altro settore che richiede il monitoraggio della salute è quello dello sport; per molti aspetti simile all'ambito dell'assistenza ai malati, si differenzia nella collocazione spaziale, perché lo sport non si svolge solo al chiuso, ma anche all'esterno delle abitazioni. Questo aggiunge complessità alle questioni poste in precedenza, perché il luogo in cui deve operare il sistema di monitoraggio può variare parecchio per quanto riguarda i parametri ambientali (posizione, temperature, pressione, umidità, ecc.).

L'apporto che può dare la tecnologia Blockchain a questo ambito verrà descritta nelle prossime sezioni. Prima di tutto verranno elencate le problematiche, poi verrà illustrata la soluzione teorica e i relativi vantaggi, in terzo luogo verranno elencate le proprietà della soluzione ed infine verranno esposti i progetti più emblematici.

### 3.2.1 Problematiche

Di seguito vengono riportate le principali problematiche relative al monitoraggio della salute:

- Invecchiamento della popolazione.
- Costo del welfare in aumento.
- Necessità di un maggiore monitoraggio a livello sportivo.
- Non aderenza alle terapie.
- Necessità di maggiore assistenza domestica.
- Mala sanità.
- Furto o alterazione di dati sanitari.

### 3.2.2 Soluzione Blockchain e relativi vantaggi

La soluzione teorica potrebbe prevedere il continuo salvataggio dei parametri vitali registrati dai sensori wearable che monitorano il paziente o l'atleta all'interno del ledger. Il ledger sarebbe distribuito tra tutti i nodi della rete. Gli utenti di questo servizio sarebbero dunque coloro che sono monitorati (i pazienti e gli atleti) e coloro che monitorano (medici, allenatori, addetti all'antidoping, famigliari, ecc.). Questo permetterebbe di reagire tempestivamente o addirittura prevenire l'insorgere di complicanze in automatico (usando gli smart contract, l'intelligenza artificiale e gli attuatori wearable), di combattere l'uso di doping e la mala sanità, di aumentare le prestazioni degli atleti, di migliorare l'aderenza alle terapie, di ridurre sensibilmente il furto o alterazione di dati sanitari e di ridurre l'ospedalizzazione dei pazienti. Inoltre la persona monitorata potrebbe avere il totale controllo dei suoi dati e potrebbe fornirli con maggiore serenità, ad esempio, ai ricercatori. Globalmente

le strutture sanitarie verrebbero sgravate da costi e carichi di lavoro, la salute di pazienti e atleti ne beneficerebbe e la fiducia nel sistema aumenterebbe.

### 3.2.3 Proprietà della soluzione

In tutto questo il concetto di Blockchain entra in gioco perché fornisce una serie di caratteristiche addizionali alle applicazioni che possono essere realizzate, vale a dire:

1) **Tracciabilità**: deve permettere di sapere quando, perché e chi o cosa provoca eventi o effettua misurazioni.

2) **Integrità**: eventuali manomissioni di dati inseriti nel ledger devono essere rilevate.

3) **Decentralizzazione**: non è necessaria un'autorità terza di controllo della correttezza delle transazioni e delle informazioni, ma è il sistema ad avere l'incarico (ciò porta un risparmio di tempo e risorse).

4) **Automazione**: gli smart contract reagiscono in automatico quando i sensori rilevano che il paziente ha una crisi (infarto, epilessia, ecc.) iniettando medicinali appositi e registrando l'evento e la medicina somministrata; successivamente inviano una notifica a parenti, dottori e soccorsi. Un altro esempio può essere in ambito sportivo con il rilevamento periodico dei parametri vitali.

5) **Non ripudio**: nel caso di controverse su misurazioni o cure errate, l'autore delle azioni non può negare la paternità delle stesse.

6) **Sequenzialità**: deve rilevare o impedire che venga invertito l'ordine temporale di due o più operazioni grazie anche al timestamp. Questa proprietà deve sottintendere l'utilizzo di una Blockchain con tempi di verifica rapidi, per ovviare ad eventuali problemi dovuti ai tempi lunghi di elaborazione (si pensi alla necessità di somministrare quanto prima un farmaco salvavita).

7) **Riservatezza**: deve essere impedito ai partecipanti alla rete (persone o macchine) di leggere i dati se non autorizzati.

Tutte queste proprietà aumentano la fiducia del paziente e ciò favorisce la condivisione delle informazioni con parenti, medici, aziende di assistenza sanitaria e istituti di ricerca.

### 3.2.4 Progetti emblematici

L'elenco sottostante riporta alcuni dei progetti più rilevanti per quel che riguarda il monitoraggio della salute:

- **CoMEHeRe**: è un progetto dell'università di Surrey attualmente in corso di completamento che ha come obiettivo l'utilizzo in sinergia di biosensori wearable, IoT, AI e tecnologia Blockchain per incentivare la raccolta di grandi volumi di dati sanitari biometrici e il loro utilizzo nella ricerca, ottimizzando assistenza sanitaria preventiva, contribuendo a realizzare un sistema sanitario più efficiente e a migliorare le condizioni di salute della popolazione. CoMEHeRe ha già implementato un'infrastruttura di raccolta dati attraverso più di 100 studenti universitari durante una sessione esami. Sono state sviluppate nuove tecniche di AI per il deep learning per analizzare questi dati e trarre conclusioni tra i dati del biosensore e gli eventi di stress acuto (come gli esami) con la capacità di dedurli con un'accuratezza superiore al 70% [42].

  Il motivo per cui si vuole utilizzare la tecnologia Blockchain va ricercato nel fatto che attualmente nella rete di servizi del settore sanitario gli utenti finali non hanno veramente il controllo dei loro dati, ma devono fidarsi di diverse entità terze per quel che riguarda la privacy e la memorizzazione; tali dati oltretutto sono sparpagliati in diversi server e codificati in modi differenti. Queste problematiche possono essere risolte utilizzando un ledger pubblicamente accessibile, non modificabile, distribuito e ridondante (anche se non elimina interamente la presenza di un'entità centrale fidata). Per quel che riguarda i dati, essi possono essere criptati in maniera tale che solo il proprietario sia in grado di decriptarli e condividerli.

  Andando più in profondità, è stato realizzato un Proof of Concept che sfrutta la Blockchain per registrare (in inglese logging) in maniera attendibile gli eventi riguardanti i dati sanitari. Questi log sono creati tramite l'esecuzione di codice (attendibile, non modificabile e verificabile da tutti i utenti) sulla Blockchain; dopo la loro creazione questi record non sono più modificabili o eliminabili. Esistono due tipi di attori nel sistema: le istituzioni che usano il sistema come fonte di dati utili alle loro ricerche e i partecipanti che partecipano alle ricerche e che creano tali dati. Dal punto di vista architetturale, il sistema è composto da un server centralizzato e fidato che gestisce il database in cui sono conservati i dati sanitari e la Blockchain pubblica Ethereum che crea i log dei dati. La logica del sistema risiede nei seguenti quattro smart contract: IdManager (mantiene le identità digitali degli utenti che si sono registrati), ResearchManager (mantiene i dettagli delle ricerche pubblicate e la lista degli aderenti alle ricerche), KSI (Keyless Signature Infrastructure, mantiene i dati relativi le informazioni sanitarie inserite nel database insieme ai relativi hash come prova anti-manomissione) e DataManager (mantiene le autorizzazioni a memorizzare e a ottenere i dati, oltre ad essere il vero smart contract che registra le operazioni di memorizzazione e accesso).

  In futuro i ricercatori hanno intenzione di aggiungere i dottori come attori, dato che realisticamente sono loro che dovrebbero inserire i dati nel sistema,

successivamente vogliono creare un'app mobile per interagire col sistema e, infine, risolvere il problema che si verrebbe a creare nel caso in cui venisse persa una chiave privata (il che comporterebbe l'impossibilità di accedere alla propria storia clinica) [43].

- **SciCoins**: sta creando applicazioni decentralizzate basate su algoritmi di consenso, riassunti col termine Proof of Change, per wearable (ad esempio SciRyng, un dispositivo indossabile con sistema di allarme) che utilizzano la tecnologia Blockchain e gli smart contract. Questi smart contract vengono eseguiti sui nodi di una rete all'interno di una piattaforma permissioned chiamata SciVM. I token SciCoins sono criptomonete usate nel sistema. I dispositivi indossabili sono equipaggiati con biosensori in grado di raccogliere informazioni in tempo reale (ad esempio dati biometrici e biochimici). In seguito, dopo aver aggregato e analizzato i dati, gli smart contract sono in grado di arrivare ad una diagnosi accurata e ad una soluzione che tenga conto delle raccomandazioni dei dottori e della storia clinica del paziente. In caso di pericolo grave un sistema di allarme è abilitato ad avvertire i servizi sanitari di emergenza [44].

## 3.3 Studi clinici

Uno studio clinico (clinical trial o trial clinico) è una ricerca finalizzata a trovare le risposte a precise domande su nuove terapie, nuovi farmaci o nuove modalità di utilizzo di trattamenti noti e autorizzati. Ci sono due tipologie di studi differenti: sperimentali e osservazionali. Negli studi sperimentali intervengono direttamente coloro che svolgono l'attività di ricerca, ad esempio con la somministrazione di medicinali, od operando sul paziente, con successiva analisi degli effetti. Gli studi osservazionali consistono nell'osservazione delle persone nell'usuale pratica clinica e i risultati ottenuti vengono raccolti dai ricercatori. Tutti gli studi vengono svolti sulla base di un protocollo che descrive le finalità dello studio e viene esaminato dai comitati etici preposti.

Soffermandosi sui trial clinici sperimentali, generalmente si suddividono in 4 fasi: durante la fase I, alcune decine di volontari sani vengono utilizzati per testare la sicurezza del farmaco e il dosaggio da somministrare. La fase II, che può durare fino a due anni, comprende spesso trattamenti in cieco, ovvero procedure in cui un gruppo di pazienti riceve il farmaco sperimentale, mentre un altro gruppo di pazienti riceve un placebo (una sostanza inerte) per valutarne obiettivamente l'efficacia [45]. Nella fase III, un numero più elevato di pazienti (spesso migliaia) viene testato per verificare ulteriormente l'efficacia del farmaco e valutare i possibili effetti collaterali. Infine, gli studi della fase IV, chiamati anche "attività di sorveglianza post-marketing", provano a confrontare il farmaco commercializzato con le alternative presenti in quel momento sul mercato [46].

Le persone intenzionate a partecipare ad uno studio clinico prima di iniziare le sperimentazioni vengono informate di tutto ciò a cui vanno incontro attraverso il consenso informato. Questo procedimento permette al potenziale aderente al trial clinico di capire le informazioni più importanti, affinché possa scegliere coscientemente se parteciparvi oppure no. È da sottolineare che l'azione informativa rivolta ai partecipanti non si interrompe durante lo studio, ma al contrario perdura in maniera continua in tutte le fasi. I ricercatori prima di iniziare lo studio consegnano il documento di informativa che contiene dettagli come le finalità, la durata, i procedimenti, i rischi e gli ipotetici benefici. Il paziente, per sancire la volontà di partecipare allo studio, deve firmare i fogli del consenso informato. In qualsiasi momento dello studio esso può decidere di abbandonarlo; questo comporta la revoca del consenso informato.

I trial vengono eseguiti da ricercatori in istituti di ricerca, ospedali, cliniche o ambulatori e vengono sovvenzionati da vari enti pubblici o privati oppure da singole persone (tra cui aziende farmaceutiche, fondazioni, agenzie governative, dottori, ecc.) [45]. Le autorità con il compito di controllare la correttezza dei protocolli e in generale la ricerca sulla salute e i farmaci sono, ad esempio, la World Health Organization (WHO) dell'ONU, la Food and Drug Administration (agenzia statunitense per la sicurezza alimentare e dei farmaci, abbreviato FDA), l'EMA (European Medicines Agency, l'autorità europea per la sicurezza dei farmaci) e l'Agenzia Italiana del Farmaco (AIFA).

### 3.3.1 Problematiche

Di seguito vengono riportate le principali problematiche relative agli studi clinici:

- La mancanza di fiducia dei potenziali partecipanti agli studi clinici, causata dalla poca chiarezza e trasparenza che talvolta si riscontra nel consenso informato e nella documentazione (mancanza di consenso scritto e/o firmato, moduli non approvati o non validi, mancato consenso a un protocollo rivisto, approvazione inesistente dei comitati istituzionali alle modifiche del protocollo, ecc.), dalle frodi nelle procedure, nei controlli inefficienti di enti terzi e dal conflitto di interesse che in alcuni Stati viene a crearsi quando le aziende farmaceutiche finanziano o sponsorizzano i trial clinici oppure le autorità preposte alla verifica degli stessi. Questa mancanza di fiducia porta a difficoltà e ritardi nel reclutare persone per le ricerche.

- Le sperimentazioni cliniche sono inefficienti per quanto riguarda i finanziamenti, i pagamenti e risorse, aumentando il costo dei nuovi medicinali.

- I problemi di sicurezza (ad esempio i furti di dati sensibili).

- Il rischio di manomissioni che possono intaccare la validità degli studi e a conseguenti pericoli per la salute pubblica.

- La frammentazione delle informazioni impedisce di vedere nel complesso il consenso informato e gli studi, limitando le potenzialità di utilizzo degli algoritmi alla base dei Big Data e del Machine Learning (che richiedono grandi moli di dati).
- La mancanza di automazione nei processi porta ad allungare i tempi dell'ingresso nel mercato dei nuovi farmaci o di nuove terapie.
- Scarsa qualità dei dati, dovuta a informazioni incomplete o incoerenti oppure alla perdita degli stessi.

### 3.3.2 Soluzione Blockchain e relativi vantaggi

Un modo per combattere la crescente sfiducia, le inefficienze, l'insicurezza e la mancanza di organizzazione sarebbe quello di passare a una tecnologia con ledger decentralizzato e immutabile come quella Blockchain. Il decentramento della rete, l'assenza di terze parti che controllino il corretto funzionamento del sistema e il salvataggio dei moduli del consenso informato dei partecipanti, insieme con i dati e/o i metadati dei trail, su un ledger immutabile impedirebbero ai produttori farmaceutici di monopolizzare il processo, impedirebbe le manomissioni e limiterebbe i procedimenti fraudolenti [46]. Inoltre, il decentramento intrinsecamente fornirebbe ridondanza, la quale diminuirebbe enormemente la possibile perdita di dati. Grazie a questa soluzione gli stakeholder (partecipanti agli studi, ricercatori, aziende farmaceutiche, autorità, ecc.) sarebbero in grado di vedere tutte le informazioni deframmentate in modo agevole, grafico e in formato digitale, si potrebbero tracciare tutte le operazioni eseguite sulla Blockchain, si aumenterebbe il grado di sicurezza e privacy, tutto potrebbe essere automatizzato attraverso smart contract e gli eventuali compensi per la partecipazione potrebbero essere effettuati tramite criptovalute. Complessivamente tutte queste caratteristiche porterebbero ad un incremento dell'efficienza delle procedure legate agli studi clinici.

### 3.3.3 Progetti emblematici

L'elenco sottostante riporta alcuni dei progetti più rilevanti inerenti agli studi clinici:

- **DocChain**: è uno strumento di raccolta del consenso informato attraverso Blockchain nell'ambito degli studi clinici [47]. È il risultato del lavoro di ricerca preliminare sull'argomento da parte di un team francese composto da Benchoufi, Porcher e Ravaud. Il suo obiettivo è appunto quello di implementare un processo che consenta la raccolta del consenso informato dei pazienti; la raccolta coinvolge anche le revisioni dei protocolli, l'archiviazione e il tracciamento del consenso in modo sicuro, non falsificabile e verificabile da chiunque,

consentendo la condivisione di queste informazioni in tempo reale [48]. Il team ha identificato nel prototipo progettato tutti i partecipanti con un ID e fornito loro una chiave privata da usare per la firma digitale dei documenti, ha associato ad ogni fase del consenso di ogni persona un timestamp e poi l'ha inserita nella Blockchain in modo immutabile attraverso la criptografia, come mostrato nella Figura 3.3.

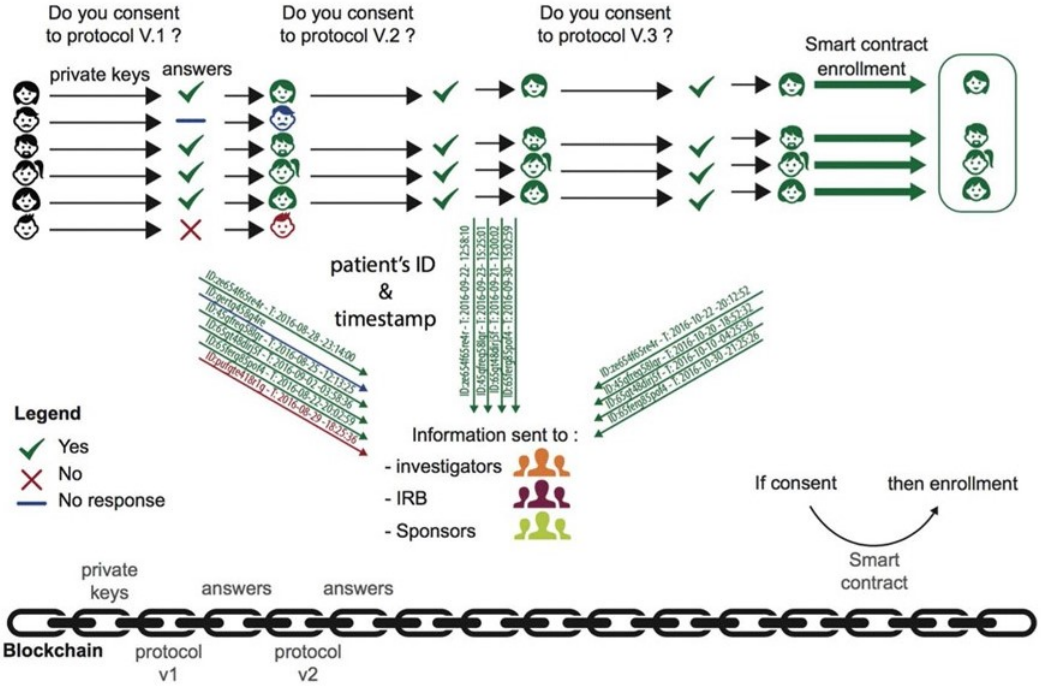



**Figura 3.3:** flusso della raccolta del consenso informato correlato alla Blockchain (tratta da [48]).

Alla fine del flusso del procedimento si ottiene un documento unico, tracciabile e incorruttibile (vale a dire che non può essere modificato o distrutto). Solo se sono state ottenute tutte le firme necessarie la persona viene registrata nel trial clinico [46].

Andando più nello specifico la release di DocChain consiste in 2 parti: il front-end Web Service e il Blockchain agent. Il front-end Web Service è dedicato ai partecipanti agli studi clinici e ai ricercatori. I partecipanti possono dare o rifiutare il consenso in maniera trasparente ad ogni fase dello studio a cui partecipano (ogni fase ha un protocollo di versione specifico). I ricercatori possono tracciare e ricevere la risposta data da ogni partecipante per ogni fase del trial. Il Blockchain agent invia le transazioni relative alle interazioni dei pazienti con il modulo del consenso informato alla rete Bitcoin. Il team ha

scelto la Blockchain Bitcoin invece che Ethereum per via della funzione "multi-sig" di Bitcoin che consente più firme su una singola transazione (attualmente questa funzione esiste anche in Ethereum, è possibile quindi che nella fase iniziale del progetto non fosse ancora stata introdotta) [46]. Ogni istanza di queste interazioni è legata alle versioni del protocollo, anch'esse tracciate sulla Blockchain [47].

Gli sforzi di Benchoufi, Porcher e Ravaud sono un esempio di come la Blockchain possa essere applicata nel settore sanitario per semplificare i passaggi del consenso informato e limitare le pratiche fraudolente, ripristinando così la fiducia dei consumatori e dei pazienti nel mercato e nella ricerca [46].

- **ClinTex**: è un'azienda con sede nel Regno Unito che fornisce soluzioni per l'industria farmaceutica, attraverso un ecosistema decentralizzato che utilizza smart contract per gestire in automatico studi clinici per nuovi farmaci. Di questo ecosistema fa parte una permissioned consortium Blockchain basata sulla rete Ethereum, che tra le sue caratteristiche ha i bassi costi di transazione. Gli obiettivi sono molteplici: da un più generico abbassamento dei costi per i nuovi medicinali e un aumento della velocità di avanzamento delle sperimentazioni, all'utilizzo del Machine Learning e delle analisi predittive per la loro gestione (prevenendo le cause di ritardo), allo sfruttamento dell'interoperabilità dei dati attraverso la tecnologia Blockchain per creare un sistema che promuova la collaborazione tra le diverse aziende farmaceutiche, fino all'impiego dei ledger distribuiti per garantire un tracciamento immutabile delle azioni compiute nei trial [49].

È da evidenziare la collaborazione con Chainlink (un'azienda che ha come scopo quello di fornire un canale sicuro e affidabile per accedere e verificare eventi esterni alle Blockchain, vale a dire un oracolo che le connetta ai dati del mondo reale o a database esterni) per accedere ai dati provenienti da sistemi farmaceutici esterni, come i moduli clinici elettronici, per calcolare i pagamenti che dovrebbero essere corrisposti a investigatori e venditori [50].

## 3.4 Tracciabilità dei medicinali, dei vaccini e dei dispositivi medici

Il ciclo di vita dei prodotti medici (medicali, vaccini e dispositivi medici) presenta diverse fasi: studi clinici, progettazione, produzione, distribuzione, vendita, utilizzo; in ogni fase operano uno o più stakeholder che spesso hanno obiettivi in contrasto tra loro[51]. Questo può portare ad un abbassamento della qualità del prodotto finale, dovuto a svariate problematiche (contraffazione, bassi standard, errate procedure, ecc.) che verranno descritte successivamente. Per porvi rimedio negli ultimi anni è stata proposta come una delle possibili soluzioni la tecnologia Blockchain, la quale

porterebbe svariati benefici (tra cui una maggiore e più sicura tracciabilità). Per meglio illustrare tale applicazione alla fine di questa sezione verrà riportato un progetto che utilizza la Blockchain per tracciare i prodotti medici.

### 3.4.1 Problematiche

L'elenco sottostante riporta alcuni dei progetti più rilevanti inerenti alla tracciabilità dei medicinali, dei vaccini e dei dispositivi medici:

- Frodi e corruzione nella produzione, della distribuzione e nella vendita di farmaci e vaccini che hanno portato a scandali in diversi Paesi del mondo.
- Controlli approssimativi e non efficaci sulle aziende farmaceutiche.
- Mancanza di sufficienti verifiche sulla filiera dei farmaci e dei vaccini (in inglese, drug and vaccines supply chain), oltre che dei dispositivi medici, e sugli stakeholder coinvolti (produttori, trasportatori, depositari, distributori intermedi e punti di dispensazione al paziente come farmacie, parafarmacie, ASL e ospedali [52]).
- Inefficiente distribuzione dei medicinali e dei vaccini.
- Bassa qualità dei prodotti.
- Dispositivi medici difettosi.
- Difficoltà nel trovare i colpevoli di scandali nella sanità, nella filiera del farmaco e nelle aziende farmaceutiche.
- Furto di documenti sensibili.
- Alterazione o contraffazione di farmaci.
- Vendita di medicinali scaduti.
- Logistica complessa e non efficiente.
- Conservazione errata di prodotti farmaceutici a temperature più elevate del necessario, rendendoli inutili o, peggio ancora, dannosi [53].
- Spionaggio industriale (furto di dati importanti per le aziende farmaceutiche).
- Scarsità di informazioni dei prodotti che i consumatori comprano.
- Poca fiducia del paziente, o in generale del cittadino, nei confronti dei medicinali e nei vaccini e nella sanità.

### 3.4.2 Soluzione Blockchain e relativi vantaggi

Ciò che potrebbe attenuare, o addirittura eliminare, le problematiche messe in luce nella sezione precedente sarebbe l'avvalersi di strumenti e di tecnologie che permettano di tracciare, monitorare e mantenere al sicuro (da un punto di vista informatico) la produzione dei farmaci e dei vaccini, la loro distribuzione e le informazioni che li riguardano, oltre al fornire un sistema che metta al centro il cittadino e il suo benessere. Tutto questo potrebbe essere ottenuto attraverso l'utilizzo della tecnologia Blockchain che presenta diverse proprietà utili, tra le quali la tracciabilità delle operazioni svolte, l'immutabilità dei dati inseriti, l'assenza di terze parti che controllino la correttezza delle informazioni immesse, il fatto che il sistema sia distribuito, la possibilità di verificare l'identità e le autorizzazioni dei partecipanti alla rete, il timestamping, la riservatezza dei dati, la possibilità di accedere in maniera comoda e ovunque alle informazioni, l'automazione attraverso gli smart contract, solo per citarne alcune, che servono a risolvere le questioni sollevate in precedenza. È possibile vedere nella figura 3.4 un esempio di tracciabilità attraverso l'utilizzo della Blockchain in una drug supply chain con le principali operazioni eseguite dagli stakeholder.

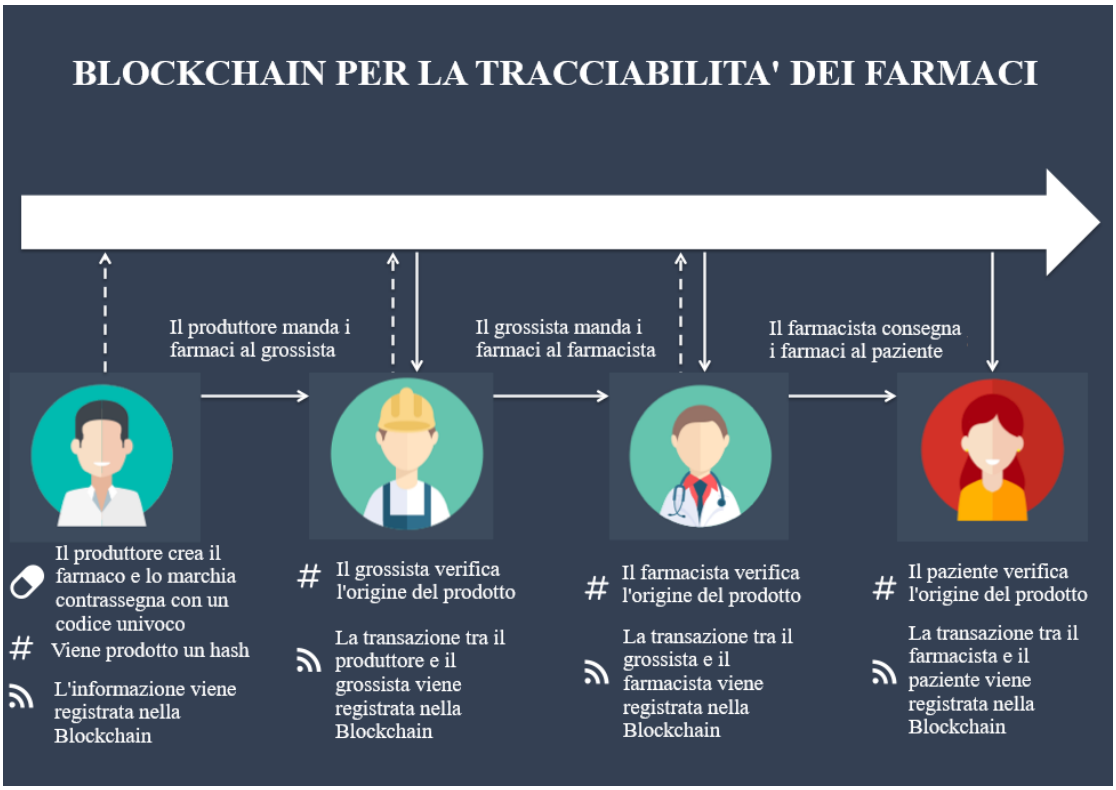



**Figura 3.4:** Blockchain per tracciare la filiera del farmaco (modificata a partire da [54]).

### 3.4.3 Progetto emblematico

Il progetto che si vuole portare come esempio è VeChain, realizzato dall'omonima azienda, che fornisce una piattaforma Blockchain pubblica "as-a-service" (concetto tale per cui l'hardware e il software sono centralizzati e sono forniti da altri come servizio e i clienti tipicamente vi accedono tramite Internet col browser), integrata all'IoT, che fa da ecosistema affidabile e distribuito per le attività commerciali più disparate (compresi i beni di lusso, l'agricoltura, la logistica, il cibo, i farmaci, ecc.). In particolare, VeChain vuole consentire un flusso di informazioni trasparente e immutabile, una maggiore sicurezza e un aumento della fiducia nella sanità (per medito delle proprietà della Blockchain) da parte dei pazienti [55].

Soffermandosi sull'ambito sanitario, VeChain permette di tracciare l'intera filiera dei farmaci, dei vaccini e della strumentazione medica, proteggendo i relativi dati. Tutto ciò è possibile grazie a dispositivi IoT (dotati di sensori altamente sensibili) che registrano e trasmettono i dati rilevanti durante l'intero ciclo di vita del prodotto ad esso collegato, dalla creazione fino all'utente finale. Nello specifico questi dispositivi sono smart chip possono essere implementati come chip NFC, tracker RFID o codici QR. VeChain ha rilasciato un'immagine di un'implementazione concreta, con dimensioni 41 mm x 55 mm x 9 mm (figura 3.5) [53, 55].


**Figura 3.5:** dispositivo VeChain (tratta da [56]).

Le informazioni sono fornite dagli attori in gioco, da ogni processo e da ogni luogo coinvolto: dalla produzione, agli impianti di stoccaggio, passando per la distribuzione della catena del freddo (cold chain distribution), fino ai punti di dispensazione come farmacie e ospedali e persino nella fase di utilizzo. Questi dati sono tutti registrati sulla Blockchain VeChainThor, eliminando così tutti i potenziali rischi nel processo e garantendo che i record dei prodotti medici siano immutabili e permanenti. Più precisamente, con la soluzione VeChain si avranno backtracking,

informazioni approfondite, veritiere e al sicuro da manomissioni o furti, responsabilità precise in caso di problemi, richiamo mirato dei prodotti difettosi o dannosi, maggiore efficienza e coordinazione nella "macchina" della produzione e della distribuzione, un aumento della qualità dei prodotti, sollecitazioni rapide e automatiche in caso di potenziali rischi, una maggiore fiducia del consumatore, solo per elencare alcuni vantaggi. Gli utenti finali saranno in grado di scansionare un codice identificativo univoco per recuperare la cronologia completa del prodotto che stanno ricevendo [53].

## 3.5 Piattaforme per prescrizioni e consegne di farmaci a domicilio

In questa sezione verranno in primo luogo spiegati alcuni dei problemi che tuttora affliggono la sanità, in secondo luogo verrà riportato un approccio improntato sulla tecnologia Blockchain e infine verranno descritti alcuni progetti che hanno implementato soluzioni concrete.

### 3.5.1 Problematiche

- I trattamenti sanitari non seguiti correttamente dai pazienti. Ci sono svariate ragioni che spiegano perché i pazienti non seguano il loro trattamento correttamente. Può capitare che si fermino non appena si sentono meglio, che il loro trattamento sia troppo complesso o il paziente non sia invogliato adeguatamente [57].

- La carenza di scorte, un problema comune nelle farmacie che la maggior parte dei pazienti ha già affrontato. Anche se può essere risolto in pochi giorni o ore, il 25% delle volte i pazienti non tornano a prendere le loro medicine. In effetti, il paziente o dimentica di tornare o semplicemente acquista il prodotto in un'altra farmacia che lo ha in magazzino. Ciò porta a tre importanti questioni: in primo luogo, il paziente potrebbe non ricevere mai il suo trattamento. In secondo luogo, se il paziente decide di acquistare il farmaco in un'altra farmacia, è probabile che la farmacia originale non venga mai informata, ciò porta alla perdita dei dati dei clienti. Infine, la farmacia invia denaro per ordinare un prodotto che non è in magazzino e che resterà nello scaffale se i pazienti non torneranno più a prenderlo [57].

- L'abuso di medicine legali, prescritte da medici e comprate in farmacia. Gli antidolorifici, insieme ai sonniferi e ai farmaci per l'ansia, sono tra le sostanze legali più abusate; gli oppiacei causano migliaia di morti per overdose ogni anno. La dipendenza può spingere le persone a commettere frodi nell'ambito delle prescrizioni: i truffatori possono tentare di ottenere prescrizioni lecite

(usandole però illecitamente) o fare in modo che le farmacie eroghino medicine usando prescrizioni false. Il sistema attuale per prescrivere i farmaci presenta diverse debolezze e falle. Le prescrizioni sono scritte a mano su carta da prescrizione, che spesso contiene caratteristiche di sicurezza scadenti, e consegnate a mano dal paziente alle farmacie. Questo crea un ambiente in cui le prescrizioni possono essere facilmente falsificate, copiate o alterate [58].

- Il furto di sostanze subito dai produttori, dalla catena di approvvigionamento e dai punti di dispensazione al paziente.

- La produzione illegale di farmaci contraffatti.

### 3.5.2 Soluzione Blockchain e relativi vantaggi

Una soluzione che risolva i problemi relativi agli abusi e alle azioni illecite legate ai farmaci sarebbe quella di garantire che la medicina giusta raggiunga solo la persona a cui è destinata. Per fare ciò sarebbe necessario un sistema che tracci tutto il ciclo di vita delle prescrizioni e le operazioni necessarie ai pazienti per ottenere i medicinali che devono assumere. E qui entra in gioco la tecnologia Blockchain: con le sue caratteristiche di sicurezza, trasparenza, tracciabilità delle operazioni, immutabilità delle informazioni impedisce azioni malintenzionate e incoraggia le parti interessate della filiera farmaceutica a garantire la qualità e l'autenticità dei prodotti che inviano e ricevono. Dato che la Blockchain rende consultabili e verificabili le transazioni, sarebbe facile per le parti interessate individuare i problemi ed agire di conseguenza (punendo i responsabili di truffe o manomissioni e ripristinando la correttezza del sistema). Sarebbe più facile contenere l'uso e l'abuso improprio di farmaci da parte delle persone ed evitare l'immissione sul mercato di sostanze illegali, legali ma rubate o prodotte senza autorizzazione [58].

Un'altra soluzione che risolva i problemi relativi alle terapie che i pazienti dovrebbero seguire potrebbe essere composta da due parti: porre rimedio all'inconveniente della mancanza delle medicine in farmacia che può portare disagi e riluttanze al paziente e fornire un incentivo alla persona affinché continui e segua correttamente le cure. La prima parte può essere implementata con un sistema che si faccia carico di consegnare i farmaci a casa del paziente (ad esempio, tramite droni [59]), mentre la seconda parte può essere attuata dando degli incentivi allettanti ogniqualvolta la medicina viene assunta. Il tutto sfruttando la Blockchain e le sue caratteristiche per gestire i dati e metterli eventualmente a disposizione di enti terzi (col consenso del proprietario delle informazioni).

### 3.5.3 Progetti emblematici

- **BlockMedx**: è una startup che sta lavorando su una piattaforma per prescrizioni mediche end-to-end utilizzando la Blockchain Ethereum. La piattaforma utilizza token crittografici per facilitare le transazioni. Le prescrizioni trasmesse, salvate o utilizzate dagli stakeholder (dottori, pazienti, farmacisti, ecc.) tramite la piattaforma possono essere verificate insieme con i dettagli del medico e del paziente. I medici saranno in grado di esplorare l'insieme delle ricette dei propri pazienti in ordine cronologico e persino di revocarle qualora lo ritenessero necessario (ad esempio, nel caso in cui i farmaci sortissero effetti collaterali). Sarà possibile salvare nella Blockchain la transazione che certifica l'utilizzo delle prescrizioni legittime da parte delle farmacie. Le prescrizioni non verranno più essere alterate e l'identità delle parti interessate nel sistema potrà essere verificata rigorosamente [58].

- **ScriptDrop**: è una startup basata su Blockchain che potrebbe aver trovato un modo per affrontare il fatto che i pazienti non seguano correttamente i trattamenti. ScriptDrop sta costruendo un approccio ecosistemico agendo su vari punti dolenti. In primo luogo, si parte dal presupposto che nessun paziente dovrebbe mai lasciare la farmacia senza la certezza di avere i farmaci con sé o di riceverli a casa. Per evitare l'abbandono delle prescrizioni, ScriptDrop ha implementato un sistema di consegna come descritto nella figura 3.6.

  Se una farmacia esaurisce un prodotto, esso verrà automaticamente consegnato a casa del paziente. In secondo luogo, una volta consegnato il trattamento, ScriptDrop si assicura che il paziente prenda la medicina attraverso i promemoria dei farmaci. Il sistema è lineare e non è necessario che il paziente fornisca alcuna informazione. ScriptDrop raccoglie tutti i dati dai farmacisti e dai medici che hanno interagito con il paziente in precedenza attraverso un sistema di integrazione diretta. Il sistema potrebbe essere completo così, ma il team di ScriptDrop ha osservato che dopo un po' molti pazienti hanno interrotto comunque il trattamento, poiché non c'è stato nessun incentivo a fare diversamente. È qui che entra in gioco la Blockchain.

  Uno dei principali problemi affrontati nel sistema sanitario è che le comunità mediche o farmaceutiche non hanno abbastanza informazioni sull'effettivo comportamento del paziente una volta che lui o lei è a casa. Questa mancanza di dati porta a trattamenti inappropriati che vengono seguiti in maniera approssimativa. La soluzione di ScriptDrop incentiva i pazienti a interagire con la piattaforma di promemoria dei farmaci attraverso sistemi basati sulla ricompensa. Infatti, i pazienti vincono i token ScriptDrop che possono utilizzare per pagare le farmacie convenzionate con la startup. Con le informazioni relative al momento in cui il farmaco è stato dato, le interazioni quotidiane

del paziente con i promemoria dei farmaci e la data di rinnovo della prescrizione, ScriptDrop è in grado di tracciare l'andamento effettivo dei trattamenti, costruendo i profili dei pazienti. Questi profili, caricati sulla Blockchain, sono una fonte unica di dati che possono essere condivisi, con il consenso del paziente, con i gruppi di medici e farmacisti che seguono il paziente, oltre che eventualmente con i ricercatori e le aziende farmaceutiche [57]. Nell'ambito della conservazione dei dati raccolti la tecnologia Blockchain fornisce un supporto fondamentale per mantenerli integri e al sicuro e per tracciare le azioni eseguite, automatizzando i processi e mantenendo alta la fiducia del paziente nel sistema. In figura 2.7 viene schematizzato il sistema ScriptDrop e il passaggio di informazioni tra i diversi stakeholder.

Poiché il profilo è condiviso tra i fornitori di assistenza sanitaria del paziente, essi sono facilitati nell'azione di controllo e supporto alla cura, perché dispongono di maggiori informazioni sul comportamento del paziente (e quasi in tempo reale); possono quindi dedicarsi maggiormente a istruire e discutere con i pazienti che mostrano scarso impegno nel seguire la terapia al fine di spronarli, aiutarli e convincerli. La Blockchain e il meccanismo della ricompensa utilizzati da ScriptDrop funzionano col Proof of Act. Quando i pazienti interagiscono con l'app e seguono correttamente il trattamento, i token vengono sbloccati. Inoltre, poiché le transazioni si originano obbligatoriamente a partire dalla farmacia, è molto difficile per i pazienti manomettere il sistema [57]. Tutto questo porta ad avere un numero maggiore di pazienti che seguono correttamente le cure, aumentando lo stato di salute della popolazione, diminuendo il costo dell'assistenza sanitaria, diminuendo gli sprechi e aumentando l'efficienza del sistema sanitario.

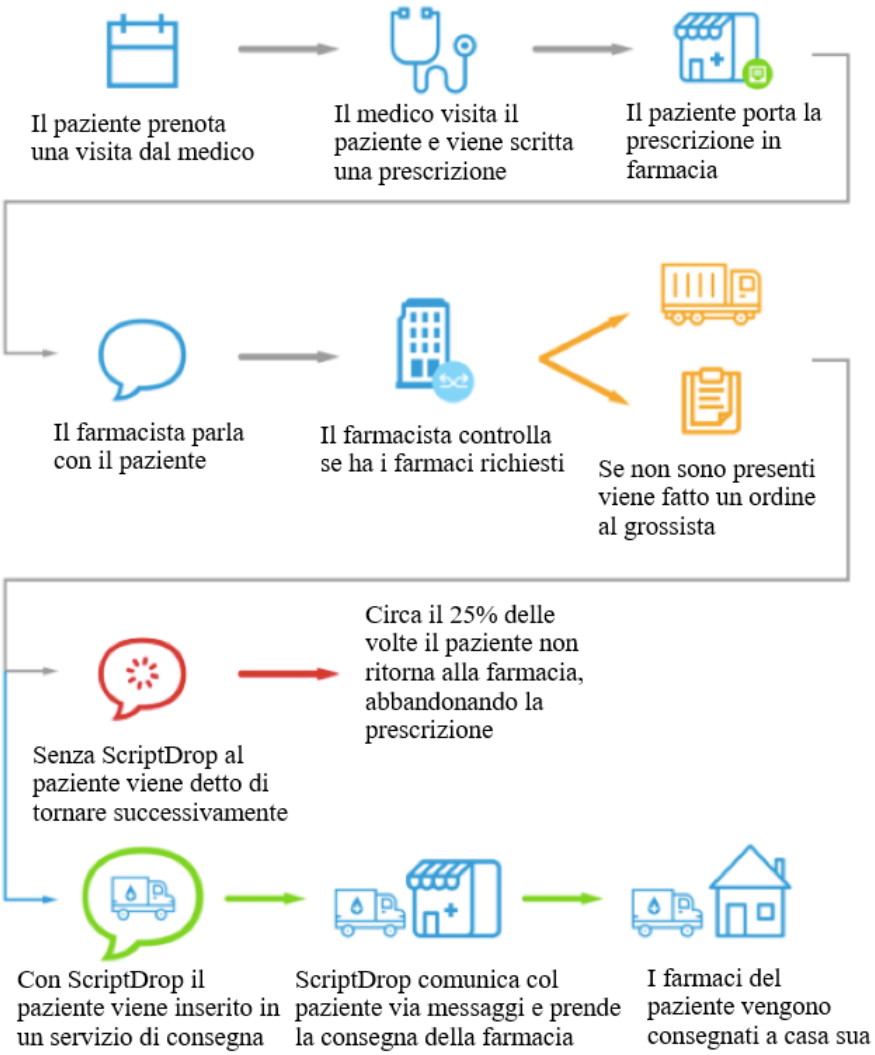



**Figura 3.6:** sistema di consegna di ScriptDrop (modificata a partire da [57]).

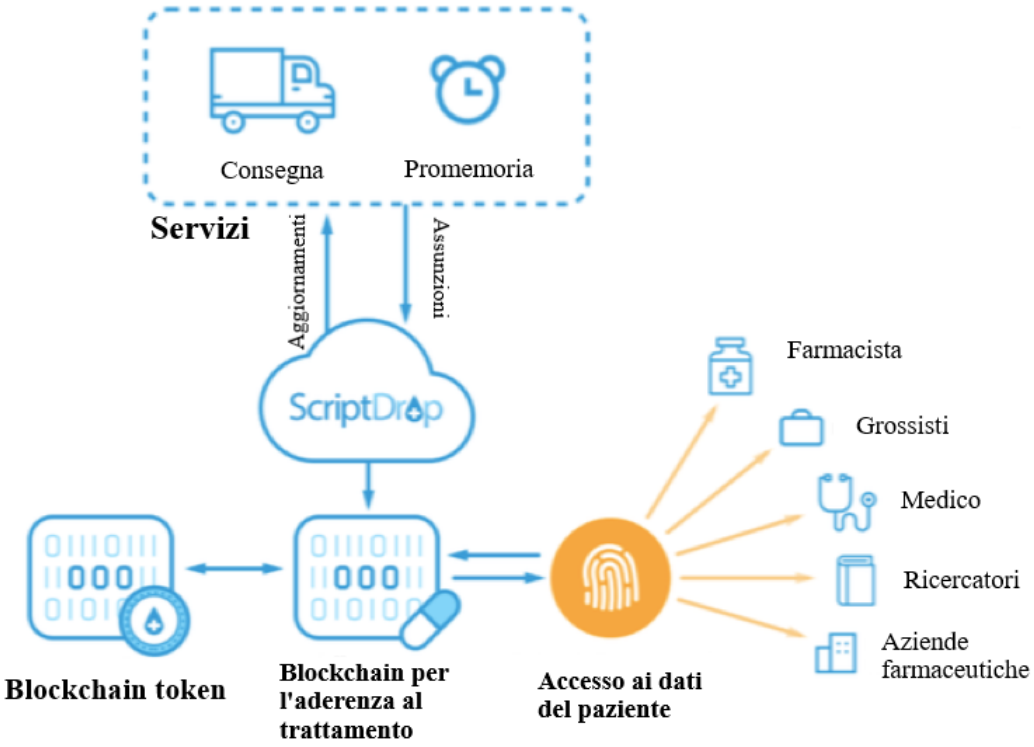



**Figura 3.7:** il sistema ScriptDrop e la trasmissione di dati (modificata a partire da [57]).

# Capitolo 4

# Proof of Concept: Blockchain nella consegna di farmaci

Il Proof of Concept proposto vuole dimostrare la fattibilità di una soluzione innovativa volta a migliorare la consegna a domicilio di farmaci (in inglese, drug delivery); più precisamente ci si focalizzerà sui farmaci con ricetta. Tale soluzione comprende l'utilizzo della tecnologia Blockchain (e in particolare di Hyperledger Fabric), delle ricette contenute nelle cartelle elettroniche e di un lucchetto intelligente.

Il capitolo seguente è suddiviso in due parti: descrizione generale e approccio proposto. Nella prima parte vengono descritti i concetti base (presenti nell'attuale processo attraverso cui il paziente acquisisce i farmaci oppure in quello futuro ipotizzato dalla soluzione), la consegna a domicilio di farmaci e le problematiche con e senza il suo utilizzo. Nella seconda parte prima viene proposto un approccio a tali questioni che sfrutti principalmente Hyperledger Fabric e poi vengono analizzati i relativi vantaggi.

## 4.1 Descrizione generale

In questa sezione vengono fornite informazioni dettagliate sui tipi di medicine esistenti, sulle ricette (cartacee e digitali) e sulle cartelle elettroniche che le contengono. Viene inoltre spiegato il funzionamento teorico e generale del lucchetto intelligente. Infine viene effettuata una panoramica sulla consegna a domicilio di farmaci e sulle problematiche senza e con il suo utilizzo.

### 4.1.1 Tipologie di farmaci

Secondo il Sistema Sanitario Nazionale (SSN) i farmaci si possono suddividere in 5 categorie [60]:

1) **Farmaci non soggetti a prescrizione medica**: sono quei farmaci che non hanno effetti collaterali gravi, sono di libera vendita e non serve la ricetta del medico.

2) **Farmaci soggetti a prescrizione medica**: hanno effetti collaterali potenzialmente gravi, per cui prevedono la prescrizione di un medico. L'unico luogo in cui si possono acquistare sono le farmacie.

3) **Farmaci soggetti a prescrizione medica limitativa**: possono essere utilizzati o prescritti solo in determinati ambienti, come in ospedali o centri specialistici. Sono i medicinali utilizzati da un determinato specialista per una particolare terapia.

4) **Farmaci soggetti a prescrizione medica rinnovabile**: essendo il loro uso continuativo dannoso per l'organismo, sono dei farmaci prescritti periodicamente.

5) **Farmaci soggetti a prescrizione medica speciale**: in questa categoria rientrano le sostanze psicotrope e degli stupefacenti, che possono comportare una dipendenza da farmaco.

Un altro tipo di classificazione dei medicinali ha come discriminante il tipo di ricetta o il fatto che possa essere reperito in farmacia o solo in ospedale [60]:

1) **Classe A:** sono tutti i farmaci forniti dal SSN, ritirabili in farmacia mostrando la ricetta rossa, dei quali si pagherà solo il ticket.

2) **Classe C:** completamente a carico del paziente con ricetta bianca, esclusi casi specifici.

3) **Classe H**: farmaci utilizzati soprattutto in ospedale.

### 4.1.2 Ricetta cartacea

La ricetta cartacea è un foglio sul quale il dottore scrive le terapie che il paziente deve seguire, le visite a cui sottoporsi e/o i farmaci da assumere [61]. Le ricette si possono suddividere in base al colore: rossa, nel caso di prescrizioni di medicinali, esami o visite specialistiche a carico del SSN in maniera totale o parziale (nei confronti dei quali i pazienti hanno solo l'onere di contribuire attraverso il pagamento del ticket), oppure bianca, nel caso in cui i farmaci o le prestazioni sanitarie siano

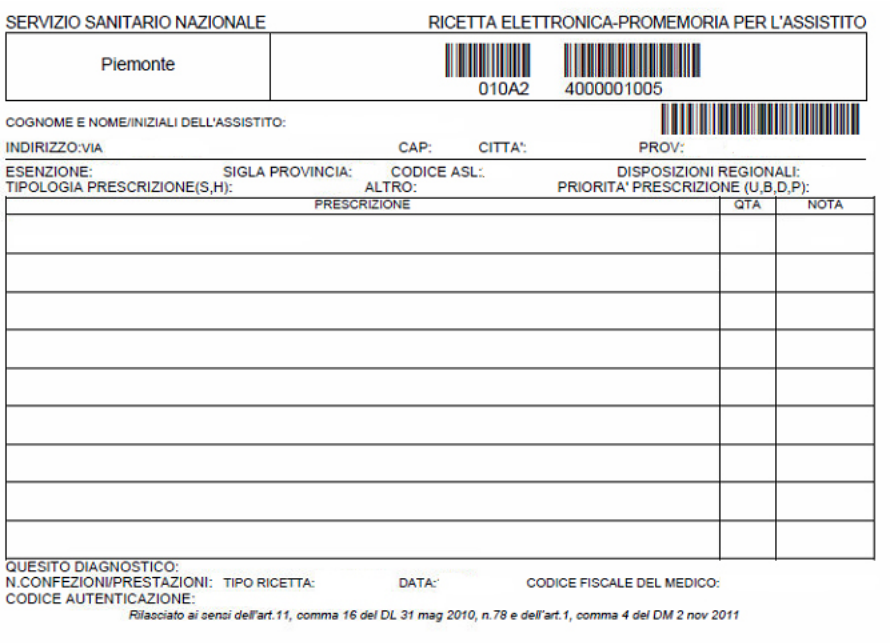
non prescrivibili e dunque a carico del malato. È possibile un'ulteriore classificazione secondo la possibilità (o meno) di riutilizzo: ripetibile, se la ripetibilità della vendita di farmaci è consentita, oppure non ripetibile, altrimenti.

### 4.1.3 Ricetta elettronica

Negli ultimi anni è entrata in vigore una nuova tipologia di ricetta, quella elettronica (in Piemonte la fase pilota è attiva dal 2014). Un processo che ha coinvolto farmacisti, medici, ASL, Regioni, Agenzia delle Entrate, INPS, Guardia di Finanze e altri soggetti, con la realizzazione ad opera di SOGEI (Società Generale d'Informatica), società di ITC del Ministero dell'Economia e delle Finanze (MEF) [62]. Essa permette di centralizzare i dati, di digitalizzare le informazioni sanitarie e di dematerializzare (eliminando il formato cartaceo) i documenti necessari per accedere a determinati servizi assistenziali [61].

La procedura classica per ottenere dei farmaci soggetti a prescrizione medica era quella di rivolgersi ad un medico, il quale compilava a mano una ricetta (bianca o rossa) con le informazioni proprie, del paziente e dei medicinali da prescrivere. Dopo di che il paziente si recava in farmacia e, presentando la ricetta cartacea al farmacista, poteva ottenere i farmaci.

La nuova procedura prevedere che i medici non ricevano più blocchi di ricette cartacee dalle ASL, ma una serie di numeri progressivi delle ricette elettroniche (NRE) prodotti dal sistema centrale gestito da SOGEI. Il medico per prescrivere un medicinale o una visita specialistica, si può connettere tramite il proprio computer (e in futuro anche con tablet o smartphone) al sistema di riferimento e, dopo essersi identificato, compilare la ricetta on line utilizzando uno degli NRE a lui assegnati e il codice fiscale dell'assistito. Il sistema controllerà il numero, il codice fiscale e tutte le informazioni di esenzione (per reddito e/o per patologia). Successivamente, il medico completerà la procedura con la prescrizione del farmaco, generando così la ricetta elettronica sul server di SOGEI. Infine, il medico consegnerà all'assistito un "promemoria" cartaceo (a regime non verrà più fornito, rendendo la procedura completamente priva di carta) che riporta NRE, codice fiscale, eventuali esenzioni e la prescrizione. Il promemoria garantisce al malato la possibilità di ottenere il farmaco anche in caso di assenza di linea o in presenza di qualsiasi altro inconveniente legato all'accesso al server [62]. In figura 4.1 è riportato un fac-simile del promemoria. In farmacia il farmacista accede alla ricetta elettronica attraverso NRE e codice fiscale del paziente ed eroga il prodotto. Come ultima operazione invia al server di SOGEI i dati relativi all'erogazione (prezzo, quantità, sconti, ticket, ecc.) e i codici che individuano la singola confezione: (codice AIC e codice "targatura", cioè il codice seriale identificativo della singola scatola). Il funzionamento delle ricette dematerializzate che prescrivono le visite specialistiche e le analisi da effettuare nei laboratori è analogo.


SERVIZIO SANITARIO NAZIONALE — RICETTA ELETTRONICA-PROMEMORIA PER L'ASSISTITO

Piemonte — 010A2 — 4000001005

COGNOME E NOME/INIZIALI DELL'ASSISTITO:

INDIRIZZO:VIA — CAP: — CITTA': — PROV:

ESENZIONE: — SIGLA PROVINCIA: — CODICE ASL:. — DISPOSIZIONI REGIONALI:

TIPOLOGIA PRESCRIZIONE(S,H): — ALTRO: — PRIORITA' PRESCRIZIONE (U,B,D,P):

| PRESCRIZIONE | QTA | NOTA |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

QUESITO DIAGNOSTICO:

N.CONFEZIONI/PRESTAZIONI: — TIPO RICETTA: — DATA:' — CODICE FISCALE DEL MEDICO:

CODICE AUTENTICAZIONE:

*Rilasciato ai sensi dell'art.11, comma 16 del DL 31 mag 2010, n.78 e dell'art.1, comma 4 del DM 2 nov 2011*

**Figura 4.1:** promemoria della ricetta elettronica [63].

Oltre alle caratteristiche positive già elencate, il sistema a regime permetterà un risparmio di carta, tempo e burocrazia, un miglioramento nel monitoraggio della spesa e delle prescrizioni in tempo reale, una verifica accurata dell'appropriatezza delle prescrizioni, dei percorsi terapeutici e della correttezza dei dati anagrafici dell'assistito, senza contare lo snellimento delle procedure di prenotazione, che in tutte le modalità possibili (telefonicamente, on line o allo sportello) richiederà al paziente di fornire soltanto codice fiscale e NRE [63].

### 4.1.4 Cartella elettronica

In linea con la filosofia della ricetta elettronica, anche la cartella clinica ha subito il processo di trasformazione dal formato cartaceo a quello digitale (con diverse caratteristiche e informazioni aggiuntive). La cartella clinica elettronica è una raccolta online di dati clinici del paziente (informazioni personali, anamnesi, terapie, esami diagnostici, prescrizioni mediche, ecc.) a disposizione dei pazienti e del sistema sanitario.

Gli obiettivi sono sempre gli stessi della ricetta dematerializzata: avere tutti i dati e la storia sanitaria del malato in un unico posto, facilmente accessibile ovunque e in qualsiasi momento, evitare l'uso della carta, scongiurare il rischio di non perdere documenti importanti, accorciare le tempistiche della burocrazia, eliminare le spese accessorie inutili e rendere così il SSN più efficiente per i cittadini. Da non trascurare le funzionalità che vengono fornite dall'informatica, vale a dire la

possibilità di fare ricerche rapide attraverso parole chiave, la possibilità di realizzare statistiche e analisi sui dati a disposizione e la possibilità di condividere, aggiornare e la visualizzazione le informazioni su molteplici dispositivi e luoghi (ospedali, cliniche, farmacie, ecc. e in generale ovunque il paziente possa utilizzare un dispositivo elettronico).

La Commissione Europea ha definito delle linee guida che i singoli Stati dovranno rispettare e garantire dal momento che adotteranno la cartella clinica digitale nel proprio SSN, in particolare [64]:

- Utilizzare i dati sensibili sulla salute degli assistiti solo per scopi ad essa legati rispettando la loro privacy.
- Assecondare la decisione autonoma del paziente su come e dove i dati devono essere usati.
- Possibilità di ogni paziente di accedere al suo fascicolo, mentre per gli operatori sanitari sarà necessario un sistema di autenticazione che identifichi anche il ruolo ricoperto.
- Accesso alla cartella clinica digitale permesso solo dagli operatori sanitari coinvolti in quel momento nella cura del malato.
- Utilizzare i dati sanitari solo per ricerche scientifiche e statistiche.
- Adozione di sistemi di sicurezza per garantire l'accesso solo alle persone autorizzate.
- Garantire la trasparenza tramite notifiche e informative.

### 4.1.5 Lucchetto intelligente

Negli ultimi anni il trend degli acquisti online (e le relative consegne a casa) è in continuo aumento. Tuttavia non sempre si riesce ad essere presenti in casa quando arrivano i pacchi o a delegare qualcuno a ritirarli; in più si aggiunge il rischio di furto nel caso in cui il fattorino li lasci sull'uscio o in un contenitore. Una delle soluzioni più interessanti è l'utilizzo di un lucchetto intelligente (smart padlock) che protegga la cassetta in cui il fattorino posa il pacco, apribile solo dal destinatario tramite un codice a barre. Un esempio concreto è BoxLock [65] (attualmente utilizzabile solo negli Stati Uniti). Questo lucchetto, visibile in figura 4.2, può scannerizzare codici a barre premendo un pulsante: il codice rilevato viene utilizzato per controllare che il destinatario sia quello corretto e che si riferisca ad una consegna ancora da effettuare (evitando usi fraudolenti di codici a barre fasulli o già utilizzati). Se è corretto, BoxLock si apre e invia una notifica all'app (attraverso WiFi o bluetooth). Infine, il proprietario o altre persone autorizzate possono aprirlo tramite app o specifico barcode. Via app è possibile tracciare le spedizioni accedendo con gli account dei principali corrieri statunitensi (UPS, USPS, FedEx e Amazon).

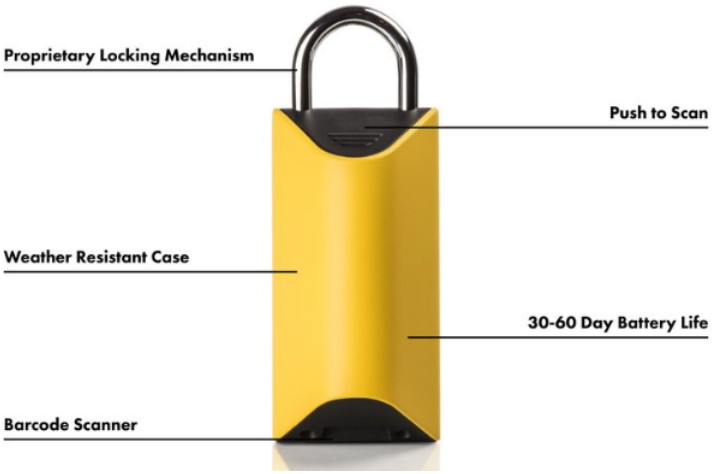



**Figura 4.2:** lucchetto BoxLock (tratta da [65]).

### 4.1.6 Consegna a domicilio di farmaci

Ultimamente i servizi di home delivery stanno modificando il modo in cui i consumatori ottengono i prodotti che comprano: non devono più andare fino al negozio, magazzino, ristorante, pizzeria, ecc. per acquistarli, ma possono semplicemente richiederli tramite smartphone, computer o tablet e pagarli con carte di pagamento, Paypal o contanti restando comodamente a casa loro.

I medicinali non sono esclusi da queste dinamiche, per ovvi motivi: per procurarseli si devono compiere una serie di attività time-consuming che molti mal sopportano o che proprio non sono in grado di compiere per impegni (ad esempio il lavoro) o impedimenti vari (ad esempio problemi di salute che non permettono di uscire di casa). Anche il semplice acquisto di farmaci non soggetti a prescrizione medica può rivelarsi impegnativo e stressante: arrivare fino alla farmacia in macchina (dovendo trovare parcheggio) o con un altro mezzo, fare la coda (impiegando mediamente dai 5 ai 10 minuti [66]), per poi magari scoprire che il farmaco non è presente in magazzino, andare in un'altra farmacia e, infine, tornare a casa. La questione si complica se in più serve una prescrizione: questo implica dover fare la coda dal medico (e secondo una stima del Ministero della Salute i tempi medi di attesa in uno studio medico variano tra i 90 e i 180 minuti [67]); nel caso peggiore la ricetta deve essere rinnovata periodicamente.

È in questo contesto che la consegna a domicilio di farmaci (drug delivery) risulta essere una buona soluzione che consente al malato di risparmiare tempo, fatica, stress e soldi (senza contare i benefici per l'ambiente e la comunità, dato che si avrebbe una riduzione del traffico e dell'inquinamento). Prendendo il caso specifico di una startup nata in Piemonte e attualmente presente in alcune città del nord e centro Italia, vale a dire Pharmercure [68], nell'ipotesi di medicinali senza ricetta,

si cerca sul sito, si effettua l'ordine fornendo tutte le informazioni necessarie e successivamente un fattorino consegnerà i prodotti all'indirizzo prescelto. Nell'ipotesi invece di farmaci con ricetta, il fattorino andrà prima a ritirare la ricetta dal cliente e poi ritornerà con i prodotti richiesti.

Un altro player di questo settore è PillPack [69], startup creata negli Stati Uniti che consegna i farmaci bypassando le farmacie. Il suo obiettivo è fornire un servizio ai malati cronici (nella maggior parte dei casi sottoposti a terapie che comprendono l'assunzione diverse medicine) che faciliti l'aderenza alle cure (cioè assunzione corretta e nel momento giusto dei farmaci), riduca il rischio di interruzione delle assunzioni causata dalla fine delle dosi e dalla necessità di rinnovare ricetta ed elimini tutte le attività tediose, ma necessarie a procurarsi i medicinali (andare in farmacia, trovare parcheggio, fare la coda, ecc.) che sono solo fonte di stress e uno spreco di tempo e soldi. Concretamente, dopo essersi registrati e aver comunicato la terapia e le relative medicine, ogni mese PillPack si occupa di acquistarle e ordinarle in base al giorno e all'ora; dopo questa fase viene spedito a casa un dispenser, in figura 4.3, con un opportuno numero di blister multi-farmaco e le tempistiche dell'assunzione stampate su ogni blister.


**Figura 4.3:** dispenser e blister (tratta da [69]).

### 4.1.7 Problematiche

All'interno dei procedimenti attraverso cui un malato ottiene i farmaci di cui necessita esistono svariate problematiche legate al formato cartaceo e all'utilizzo o meno delle consegne a domicilio. Con le ricette in formato cartaceo sono possibili truffe da parte del medico o del paziente, un uso improprio delle ricette o una difficile comprensione della prescrizione e non si sfruttano le potenzialità del formato digitale (tutte le informazioni consultabili in un unico posto, ridotto rischio di perdere le ricette, ricerche facilitate, analisi e statistiche). I procedimenti in cui non si fa uso della consegna a domicilio sono generalmente inefficienti: i malati perdono tempo e soldi (in code, traffico, benzina, ecc.), rischiano di non essere aderenti alle terapie e aumentano lo stress quotidiano. Se è vero che le consegne a domicilio portano molti vantaggi, è anche vero che vengono a crearsi nuovi possibili svantaggi: mancanza di privacy (perché il fattorino può leggere la ricetta cartacea o vedere le medicine che consegna), inefficienza (si fa magari un viaggio a vuoto per prendere la prescrizione dal cliente, come avviene per Pharmecure), mancanza di tracciabilità e monitoraggio delle transazioni, poca fiducia dei malati nell'affidare ai fattorini le loro ricette o la consegna dei farmaci (per timore che venga persa la ricetta, per timore di manipolazioni/furti di medicinali, di ritardi, ecc.), procedimenti migliorabili, solo per citarne alcuni.

## 4.2 Approccio proposto

A partire dalle problematiche messe in luce nella sezione precedente, riguardanti il processo attraverso cui il malato ottiene i medicinali che gli occorrono, verrà ora proposta una soluzione migliorativa che sfrutti le potenzialità della consegna a domicilio di farmaci, della Blockchain Hyperledger Fabric, delle ricette elettroniche e di un lucchetto intelligente. La soluzione si focalizzerà su pazienti che devono assumere farmaci con ricetta. Infine verranno esplicitati i vantaggi della soluzione.

### 4.2.1 Soluzione

La soluzione (figura 4.4) prevede che il paziente vada dal dottore e che esso (dopo averlo visitato) prescriva una ricetta elettronica con uno o più farmaci (che viene inserita nella cartella elettronica del paziente nel database di SOGEI, esterno al sistema).

A questo punto il paziente (divenuto cliente del servizio di consegne a domicilio di farmaci con ricetta, avendo già provveduto a registrarsi nel sistema fornendo un certificato digitale, firmato con chiave privata, contenente le sue informazioni personali, tra cui il codice fiscale, e la chiave pubblica) richiede i farmaci ad una farmacia o ad un'azienda che fornisce un servizio analogo, ad esempio PillPack, specificando i codici NRE corrispondenti alle ricette elettroniche da utilizzare. Il

farmacista (o il fornitore) controlla di averli in magazzino, attraverso un proprio sistema informatico, e verifica l'erogabilità dei farmaci (ovvero: se, in base alle ricette, quei farmaci possono essere venduti a quel cliente). Se il cliente non può comprare quei farmaci, l'operazione di acquisto termina con un messaggio di errore; se sono presenti e possono essere erogati, richiede il pagamento, altrimenti attende che lo siano. Il cliente paga l'ordine (che intanto è stato salvato nella Blockchain con i relativi dati) con un sistema di pagamento e autorizza uno specifico fattorino (o chi ha lo stesso compito, ovvero quello di ritirare i farmaci, ad esempio un parente) al ritiro. Il farmacista (o il fornitore) verificherà il pagamento e, nel caso in cui sia stato correttamente effettuato, verrà inviata una notifica di "richiesta di consegna" al fattorino designato.

Il fattorino andrà presso la farmacia o l'azienda e comunicherà il proprio identificativo e quello dell'ordine. Il farmacista (o il fornitore) verificherà che sia autorizzato consultando la Blockchain, ricaverà la ricetta e tutte le informazioni del cliente (compreso il codice fiscale) attraverso il sistema delle ricette elettroniche; con questi dati sarà in grado di soddisfare l'ordine consegnando un pacco anonimo (ovvero che non permette di conoscere ciò che è al suo interno) contenente i farmaci al fattorino e segnando come "erogato" lo stato dell'ordine. Il contenitore utilizzato dal fattorino per trasportare il pacco può essere chiuso con un lucchetto intelligente, simile a quello usato da BoxLock, al momento della presa in carico. Verrà riaperto solo dal destinatario (o da suoi delegati) al momento della consegna con un codice alfanumerico, un barcode o un QR code generato dalla decifratura tramite chiave privata di una stringa (specifica per quell'ordine) criptata utilizzando la chiave pubblica e inviata al cliente dal farmacista o dal fornitore.

Se la ricetta è ripetibile, questa sequenza di operazioni può essere ripetuta ciclicamente per un tempo indefinito (eccezion fatta per la visita medica che viene svolta una sola volta). Se non è ripetibile, il medico può valutare se lasciare invariata, modificare o eliminare la ricetta dal sistema delle ricette elettroniche. Da notare che la Blockchain contiene i dati forniti dagli utenti al momento della registrazione, gli ordini e i codici NRE delle ricette elettroniche. Tutti coloro che interagiscono col sistema (clienti, fattorini, farmacisti e fornitori), oltre ad essersi registrati, devono aver effettuato l'accesso. Gli stati dell'ordine sono: creato, richiesto, da pagare, pagato, autorizzato, pronto alla consegna, erogato e consegnato.

### 4.2.2 Vantaggi

I vantaggi della soluzione proposta rispetto al procedimento "classico" (vale a dire il malato che si procura autonomamente il medicinale) sono molteplici e derivano dall'utilizzo combinato della consegna a domicilio di farmaci, ricette/cartelle elettroniche, lucchetto intelligente e, soprattutto, tecnologia Blockchain (in particolare Hyperledger Fabric per le sue caratteristiche):

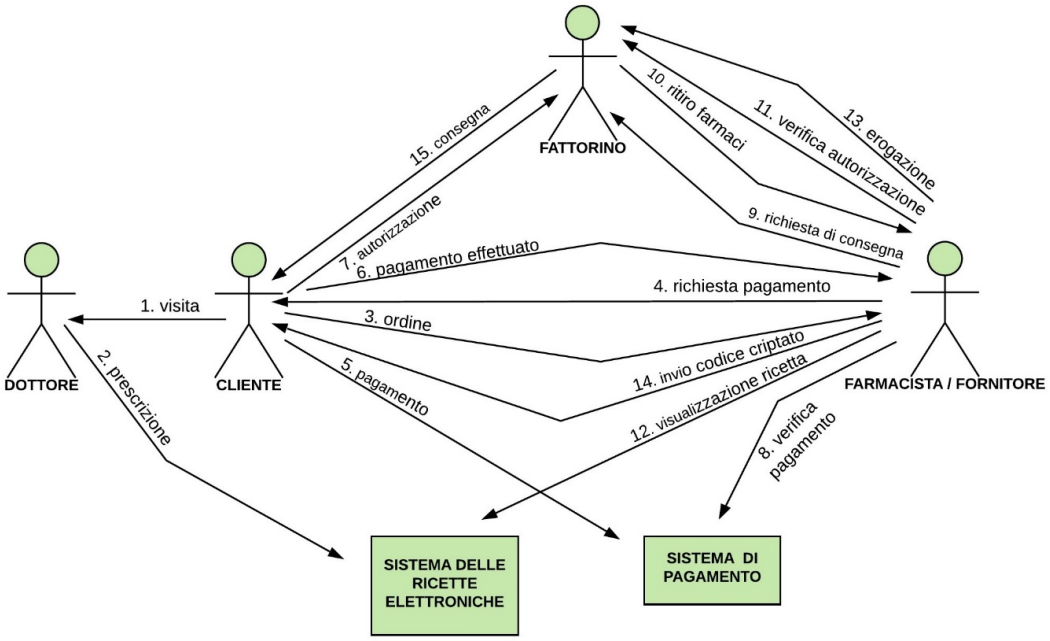



**Figura 4.4:** schema della soluzione.

- **Blockchain**: uno dei problemi maggiori della consegna a domicilio di farmaci (e dell'home delivery in generale) è la mancanza di fiducia in coloro che portano il prodotto dal luogo di produzione o vendita al cliente finale, vale a dire i fattorini. Andando più nel dettaglio il sistema attuale presenta potenziali rischi di privacy, truffa, furto o manomissione del prodotto trasportato (solo per citare alcune questioni). Hyperledger Fabric è una Blockchain privata e permissioned; questo vuol dire che i participant non sono anonimi, ma hanno una identità certificata (proprietà di autenticazione), e possono eseguire solo determinate azioni e transazioni (proprietà di autorizzazione); il controllo d'accesso è dinamico, vale a dire che i permessi possono cambiare, ad esempio, qualora il proprietario dei dati decidesse di condividerli con qualcun altro. La Blockchain presenta, inoltre, altre proprietà che contribuiscono ad aumentare la fiducia dei fruitori nel servizio: la tracciabilità delle operazioni, l'integrità dei dati, il fatto che non siano necessarie terze parti fidate perché le informazioni sono distribuite e ridondanti e il controllo della correttezza delle transazioni è decentralizzato, l'automazione di determinate operazioni attraverso gli smart contract, la sequenzialità temporale delle transazioni, per citarne alcune. Un altro vantaggio è la scalabilità del sistema data dalle ridotte dimensioni degli asset (i dati relativi agli ordini) e dal fatto che Hyperledger Fabric sia dotata di un nuovo ciclo di vita e di un consenso senza mining.

- **Consegna a domicilio di farmaci**: assicura al cliente un risparmio in termini di tempo e denaro, evita la preoccupazione del parcheggio, favorisce una diminuzione del traffico e inquinamento, riduce le code in farmacia e lo stress. Aiuta, infine, le persone impossibilitate a muoversi a rifornirsi dei medicinali.
- **Ricette e cartelle elettroniche**: avere un database esterno al sistema in cui sono presenti le ricette in formato digitale evita ai fattorini di dover andare a casa dei clienti a ritirare la ricetta cartacea (risparmiando così tempo, fatica e soldi), aumenta la fiducia nel servizio da parte dei malati perché non devono più fornire la ricetta cartacea ai fattorini (con il rischio di perderla o con timori per la privacy) e permette la centralizzazione dei dati, un risparmio di carta, tempo e burocrazia, un miglioramento nel monitoraggio della spesa e delle prescrizioni in tempo reale, una verifica accurata dell'appropriatezza delle prescrizioni, dei percorsi terapeutici e della correttezza dei dati anagrafici dell'assistito, senza contare lo snellimento delle code in farmacia e dal dottore.
- **Lucchetto intelligente**: garantisce che il fattorino (o qualsiasi altra persona potenzialmente malintenzionata) non abbia aperto il pacco.

# Capitolo 5

# Progettazione del Proof of Concept

A partire dalla descrizione della soluzione proposta, in questo capitolo verranno analizzate le caratteristiche e i comportamenti che il sistema deve avere per essere conforme alle aspettative. In primo luogo, verrà preso in considerazione il contesto in cui il sistema è chiamato ad operare e le interfacce utilizzate dagli attori (entità esterne al sistema: possono essere utenti umani oppure altri sistemi) per comunicare col sistema. In secondo luogo, verranno elencati i requisiti funzionali e non funzionali. In terzo luogo, si descriveranno i casi d'uso e i relativi scenari. Infine, verranno definiti i concetti chiave attraverso un glossario e i componenti costitutivi del sistema.

## 5.1 Contesto

Gli attori che interagiscono col sistema (come si vede della figura 5.1, rappresentante il diagramma di contesto) sono: i clienti che necessitano di farmaci, il sistema con cui i clienti pagano i farmaci e il servizio, i farmacisti che erogano le medicine, i fattorini che le ritirano e le consegnano, i fornitori di farmaci e servizi, il sistema in cui sono salvate le ricette elettroniche. Essi vengono suddivisi in due categorie: gli utenti (attori umani), ovvero i clienti, i fattorini, i farmacisti e i fornitori, e i sistemi esterni (attori non umani), ovvero il sistema di pagamento e il sistema delle ricette elettroniche.

Nella tabella 5.1 sono elencate le interfacce fisiche e logiche utilizzate dagli attori per dialogare col sistema della consegna a domicilio di farmaci con Blockchain. Andando più nel dettaglio delle interfacce logiche e delle operazioni che dovrebbero consentire:

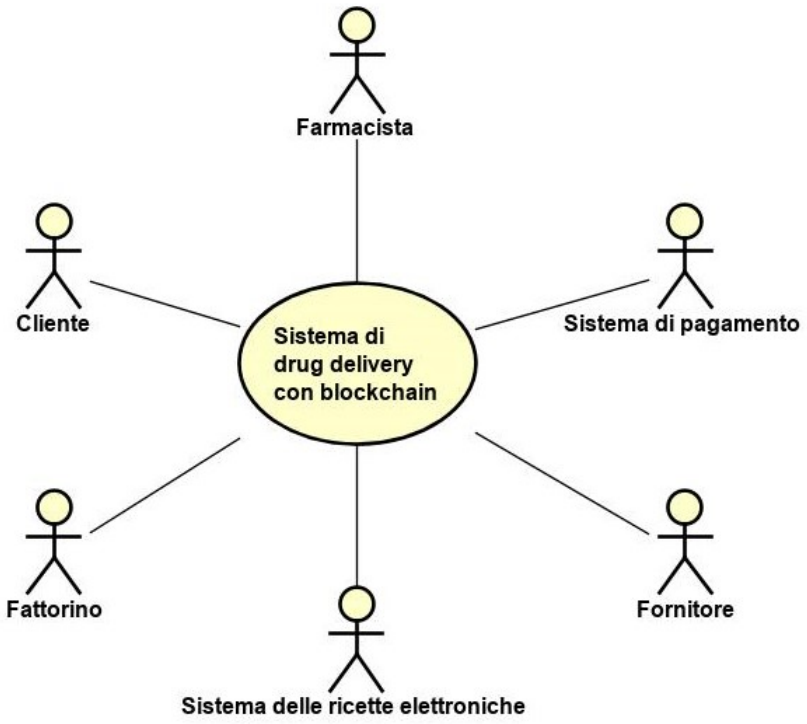



**Figura 5.1:** diagramma di contesto.

- **Cliente**: registrarsi sul sistema, accedere al sistema, vedere le ricette elettroniche attualmente prescritte, ordinare uno o più farmaci, dare le informazioni necessarie alla spedizione, autorizzare uno specifico fattorino (o chi ha lo stesso compito, ovvero quello di ritirare i farmaci, ad esempio un parente) a ritirare il pacco, pagare l'ordine, vedere il tracking dei pacchi e, infine, uscire dal sistema (operazioni eseguite dall'utente tramite interfaccia grafica); aprire il lucchetto (operazione eseguita dall'utente scrivendo un codice o mostrando un barcode/QR code da lui stesso generato a partire da un codice inviato dal farmacista al relativo lettore).

- **Sistema di pagamento**: effettuare un pagamento (operazione eseguita tramite funzioni, scambio di dati in formato XML/JSON, protocolli SOAP/REST, ecc.).

- **Fattorino**: registrarsi sul sistema, accedere al sistema, vedere gli ordini, vedere le relative informazioni (ad esempio l'indirizzo della destinazione), associare il pacco al lucchetto, concludere la consegna e, infine, uscire dal sistema (operazioni eseguite dall'utente tramite interfaccia grafica); aprire il lucchetto (operazione eseguita dall'utente scrivendo un codice o mostrando un barcode/QR

**Tabella 5.1:** interfacce fisiche e logiche tra gli attori e il sistema.

| Attori | Interfacce fisiche | Interfacce logiche |
|---|---|---|
| Cliente | Connessione internet sicura e smartphone/tablet, lettore barcode/QR code | Interfaccia grafica, barcode/QR code |
| Sistema di pagamento | Connessione internet sicura | Web Service |
| Fattorino | Connessione internet sicura e smartphone/tablet, lettore barcode/QR code | Interfaccia grafica, barcode/QR code |
| Farmacista | Connessione internet sicura e PC | Interfaccia grafica |
| Fornitore | Connessione internet sicura e PC | Interfaccia grafica |
| Sistema delle ricette elettroniche | Connessione internet sicura | Web Service |

code fornito dal farmacista al relativo lettore).

- **Farmacista**: registrarsi sul sistema, accedere al sistema, verificare se il fattorino sia autorizzato a ritirare quel farmaco per quello specifico cliente e se il pagamento sia stato effettuato, confermare l'erogazione dei prodotti, ricevere la conferma dell'invio del codice necessario ad aprire il lucchetto, uscire dal sistema (operazioni eseguite dall'utente tramite interfaccia grafica).
- **Fornitore**: stesse interfacce logiche (operazioni eseguite dall'utente tramite interfaccia grafica), ma con meno informazioni riguardanti il cliente.
- **Sistema delle ricette elettroniche**: ottenere i dati relativi alla ricetta elettronica e al paziente in base al codice NRE (operazione eseguita tramite funzioni, scambio di dati in formato XML/JSON, protocolli SOAP/REST, ecc.).

## 5.2 Requisiti funzionali e non funzionali

I requisiti funzionali, ovvero i servizi o i comportamenti che il sistema dovrebbe fornire o avere, sono elencati di seguito:

1. Registrazione (sul sistema)
2. Accesso (al sistema)
3. Ordinazione dei farmaci
   (a) Visualizzazione delle ricette elettroniche prescritte
   (b) Ricerca di un farmaco tra quelli prescritti
   (c) Visualizzazione dei dettagli della singola ricetta
   (d) Selezione di un farmaco
   (e) Inserimento dei dati utili alla spedizione (destinazione, farmacia o fornitore, ecc.)
   (f) Inserimento delle informazioni personali
   (g) Autorizzazione dello specifico fattorino a ritirare il pacco
   (h) Pagamento dell'ordine (carta di pagamento, Paypal, ecc.)
4. Controllo delle spedizioni
   (a) Visualizzazione delle spedizioni
   (b) Ricerca di una spedizione
   (c) Visualizzazione dei dettagli della singola spedizione
5. Gestione del lucchetto
   (a) Apertura del lucchetto
   (b) Chiusura del lucchetto
6. Consegna di un ordine
   (a) Visualizzazione gli ordini
   (b) Ricerca di un ordine
   (c) Visualizzazione dei dettagli (ad esempio il codice NRE) del singolo ordine
   (d) Associazione del pacco al lucchetto
   (e) Conferma di avvenuta consegna
7. Erogazione dei farmaci
   (a) Verifica dell'autorizzazione
   (b) Verifica del pagamento

   (c) Acquisizione dei dati relativi alla ricetta e al cliente in base al codice NRE
   (d) Conferma dell'erogazione dei prodotti
   (e) Invio del codice necessario ad aprire il lucchetto

8. Uscita (dal sistema)

I requisiti non funzionali, ovvero i vincoli a cui è soggetto il sistema, sono elencati di seguito:

1. **Sicurezza**: requisito generico che include l'autenticazione degli utenti e dei dati, l'autorizzazione all'esecuzione di determinate operazioni, la riservatezza, l'integrità delle informazioni, il monitoraggio del sistema e la disponibilità del servizio (solo per citare alcuni dei requisiti più specifici).

2. **Riservatezza**: solo i proprietari dei dati sensibili e gli attori esplicitamente autorizzati possono vederli e/o modificarli; questo implica il fatto che le informazioni riservate trasmesse da e verso il sistema, o salvate al suo interno, debbano essere cifrate nella maniera più opportuna.

3. **Tracciabilità**: ogni transazione od operazione deve essere registrata, insieme all'autore, all'istante in cui è stata eseguita.

4. **Integrità**: i dati devono essere protetti da modifiche, cancellazioni o aggiunte accidentali o volontarie effettuate da terze parti; o meglio, tali azioni devono poter essere rilevate e i dati alterati devono essere ripristinati allo stato precedente.

5. **Verificabilità**: requisito legato alla tracciabilità, le affermazioni degli utenti devono essere verificabili attraverso il sistema.

6. **Scalabilità**: il sistema deve, ad esempio, essere in grado di gestire la crescita degli utenti e dei relativi dati.

7. **Backup**: evitare la perdita di dati salvando più copie nel sistema.

8. **Efficienza**: riduzione di passaggi, costi e tempi rispetto alla soluzione precedente a quella proposta, ogni operazione elementare che non richiede l'intervento di un attore (come avviene, invece, per i pagamenti) deve essere eseguita in tempi accettabili (ad esempio, 0.5 secondi), aumento della disintermediazione e dell'automazione delle procedure.

9. **Usabilità**: l'esperienza dell'utente nell'usufruire del servizio deve essere facile e soddisfacente; questo vuol dire che l'interfaccia grafica deve essere user-friendly, il tempo di apprendimento necessario ad avere padronanza del servizio deve essere breve, le operazioni base che servono per il raggiungimento

un obiettivo devono essere poche, semplici e standard, infine, il sistema deve limitare il numero dei potenziali errori dell'utente e dare la possibilità di rimediare.

10. **Disponibilità**: il rapporto tra il tempo in cui il servizio è utilizzabile dagli utenti e il tempo totale deve essere accettabile.

11. **Costo**: il sistema deve essere sostenibile economicamente per tutti gli stakeholder.

12. **Volume**: la dimensione dei dati non deve essere eccessiva rispetto all'unità di memoria in cui sono salvati o alle operazioni che devono essere eseguito su di essi.

13. **Conformità**: il sistema deve essere conforme alle leggi e alle norme vigenti (ad esempio il GDPR, ovvero il regolamento europeo sulla protezione dei dati personali).

## 5.3 Casi d'uso

Nella figura 5.2 vengono riportati i casi d'uso più rilevanti, gli attori coinvolti e le relazioni che intercorrono tra i casi d'uso e gli attori. I casi d'uso presi in considerazioni sono: l'acquisto dei farmaci da parte dei clienti, la consegna dei medicinali da parte dei fattorini e, infine, l'erogazione dei farmaci effettuata dai farmacisti o dai fornitori. Essi verranno analizzati più nel dettaglio nelle sotto-sezioni successive.

### 5.3.1 Caso d'uso: acquista farmaci

**Descrizione**: in questo caso d'uso un cliente vuole acquistare uno o più farmaci. Richiederà, quindi, al sistema di vedere la lista delle sue ricette prescritte, il quale le recupererà a sua volta dal sistema delle ricette elettroniche. Dopo di che il cliente potrà leggere i dettagli di una specifica ricetta (farmaci, dosaggio, dottore, ecc.) ed eventualmente selezionare i farmaci (e il numero di confezioni) che vuole acquistare oppure tornare alla lista precedente. Dopo aver terminato la fase di selezione, il cliente dovrà inserire le informazioni personali (se non sono già state salvate nel sistema) e di spedizione (farmacia/magazzino prescelta per l'erogazione, destinazione, ecc.). In risposta alla richiesta di ordine verrà verificato se i farmaci sono tutti disponibili nella farmacia o nel magazzino scelto e se il farmacista possa effettivamente erogare quei farmaci in base alle ricette del cliente; in caso affermativo, verrà chiesto il pagamento corrispondente. Il passo successivo, dopo aver effettuato il versamento attraverso il sistema di pagamento selezionato, sarà l'autorizzazione al ritiro nei confronti del fattorino. A questo punto il cliente potrà monitorare la spedizione fino alla consegna. Infine, il lucchetto che chiude

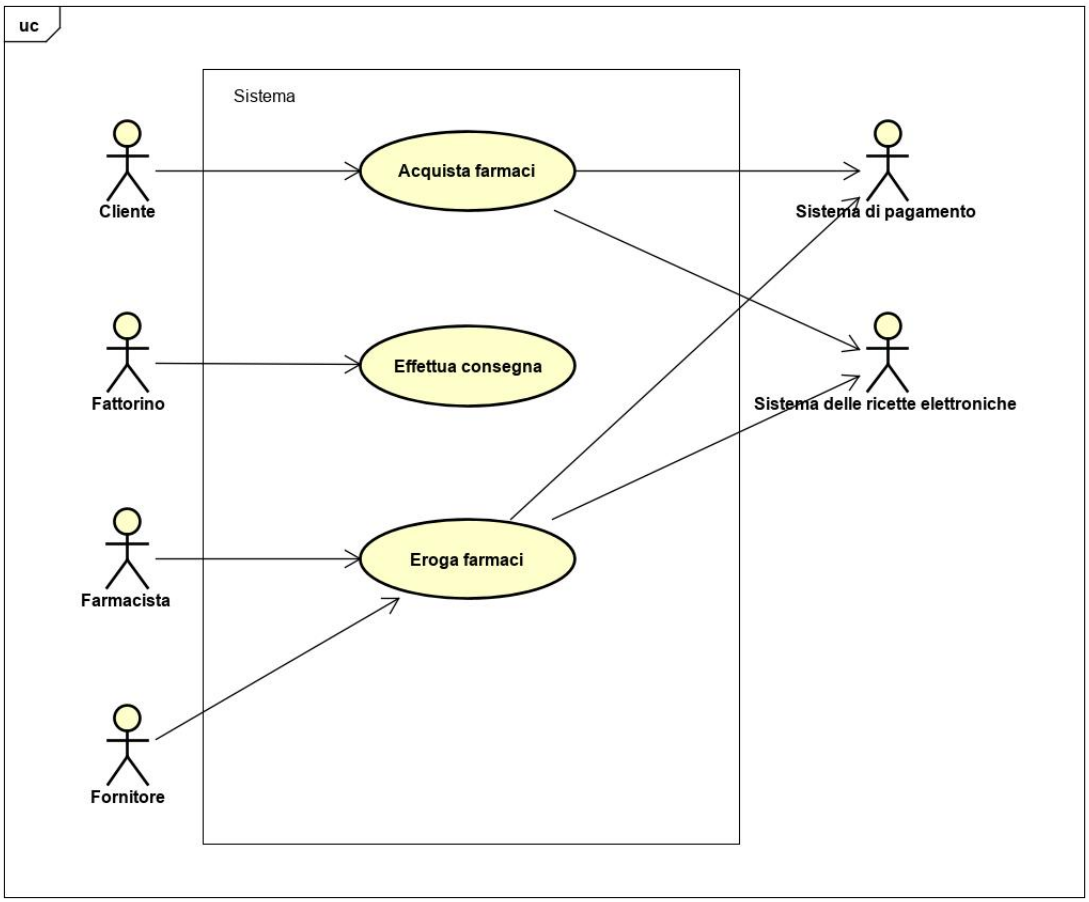



**Figura 5.2:** diagramma dei casi d'uso del sistema.

il pacco potrà essere aperto dal cliente (o da suoi delegati) utilizzando il codice alfanumerico/QR code/barcode ottenuto dalla decifrazione del codice mandato dal farmacista/fornitore, certificando così di essere il legittimo destinatario.
**Diagramma del caso d'uso**: vedere figura 5.3
**Livello**: sommario
**Attore primario**: cliente
**Attori secondari**:

- Sistema delle ricette elettroniche
- Farmacista
- Fornitore
- Sistema di pagamento

**Precondizioni**:

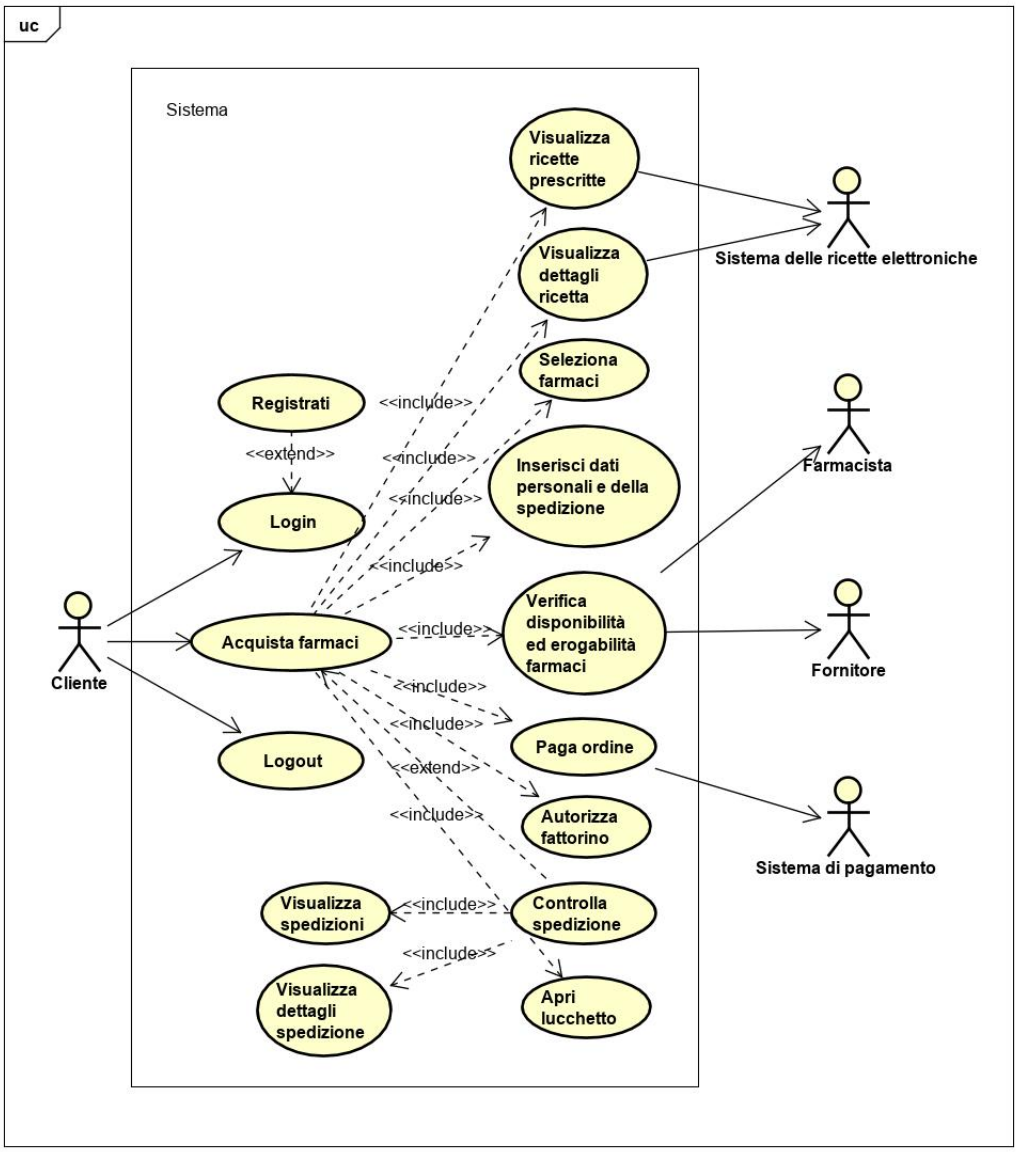



**Figura 5.3:** diagramma del caso d'uso "acquista farmaci".

- Il cliente deve essere stato visitato da un dottore
- Il dottore deve avergli prescritto una ricetta
- Tale ricetta deve essere salvata nel sistema delle ricette elettroniche
- Il cliente deve essersi registrato sul sistema
- Il cliente deve aver effettuato il login

**Postcondizioni**:

- **Garanzie minime**: il sistema ha registrato la richiesta di ordine (composta dalla lista dei codici NRE, dalla lista dei farmaci, il numero delle confezioni, le informazioni personali, quelle della spedizione e quelle del farmacista/fornitore, ecc.); quando il cliente completerà l'acquisto, autorizzando uno specifico fattorino al ritiro e pagando l'ordine, le fasi di erogazione e consegna potranno iniziare.
- **Garanzie massime**: il sistema deve aver ricevuto la conferma di avvenuto pagamento e il cliente deve aver ricevuto i farmaci che ha acquistato.

**Trigger**: il cliente accede al sistema per acquistare uno o più farmaci
**Scenario principale di successo**:

1. Il cliente va nella sezione "ricette prescritte"
2. Il sistema fornisce l'elenco delle ricette prescritte del cliente recuperandolo dal sistema di ricette elettroniche
3. Il cliente seleziona una ricetta di suo interesse
4. Il sistema presenta i dettagli della ricetta
5. Il cliente seleziona i farmaci di suo interesse e le relative quantità oppure torna all'elenco
6. Il cliente conclude la fase di selezione dei farmaci
7. Il cliente inserisce i dati personali e di spedizione
8. Il sistema verifica la disponibilità di tutti i farmaci nella farmacia o nel magazzino scelto e verifica il fatto che il farmacista possa effettivamente erogare quei farmaci in base alle ricette del cliente
9. Il farmacista/fornitore richiede il pagamento dell'ordine
10. Il cliente paga l'ordine attraverso un sistema di pagamento
11. Il cliente autorizza uno specifico fattorino al ritiro dei farmaci
12. Il cliente va nella sezione "spedizioni"
13. Il sistema fornisce l'elenco delle spedizioni in corso del cliente
14. Il cliente seleziona una spedizione di suo interesse
15. Il sistema presenta i dettagli della spedizione
16. Il cliente torna all'elenco

17. Il cliente apre il lucchetto che chiude il pacco del fattorino con all'interno i farmaci

Nota: i passi 3-5 e 14-16 possono essere ripetuti un numero indefinito di volte dal cliente.

**Diagramma di sequenza dello scenario principale di successo**: vedere figura 5.4

### 5.3.2 Caso d'uso: effettua consegna

**Descrizione**: in questo caso d'uso un fattorino vuole effettuare una consegna di farmaci. Dopo aver ricevuto una richiesta di consegna, richiederà al sistema di vedere la lista degli ordini pendenti a lui assegnati. Il fattorino potrà leggere i dettagli di uno specifico ordine selezionandolo e, al momento del ritiro presso una farmacia o un magazzino, comunicare le informazioni necessarie (codici NRE, numero di confezioni, ecc., oltre che il proprio identificativo). Dopo che il farmacista o il fornitore avranno eseguito le necessarie verifiche, il fattorino potrà mettere i farmaci all'interno di un pacco chiuso da un lucchetto e associarlo a quello specifico ordine. Infine il fattorino porterà al legittimo destinatario (l'unico in grado di aprire il lucchetto con un codice alfanumerico/QR code/barcode) e concluderà la consegna.
**Diagramma**: vedere figura 5.5
**Livello**: sommario
**Attore primario**: fattorino
**Precondizioni**:

- Il fattorino deve essersi registrato sul sistema
- Il fattorino deve aver effettuato il login

**Postcondizioni**:

- **Garanzie minime**: il fattorino deve aver preso in carico la consegna dei farmaci e aver fatto un tentativo di consegna
- **Garanzie massime**: il fattorino ha consegnato i farmaci al legittimo destinatario

**Trigger**: il fattorino riceve una notifica di richiesta di consegna
**Scenario principale di successo**:

1. Il fattorino va nella sezione "ordini"
2. Il sistema fornisce l'elenco degli ordini a lui assegnati

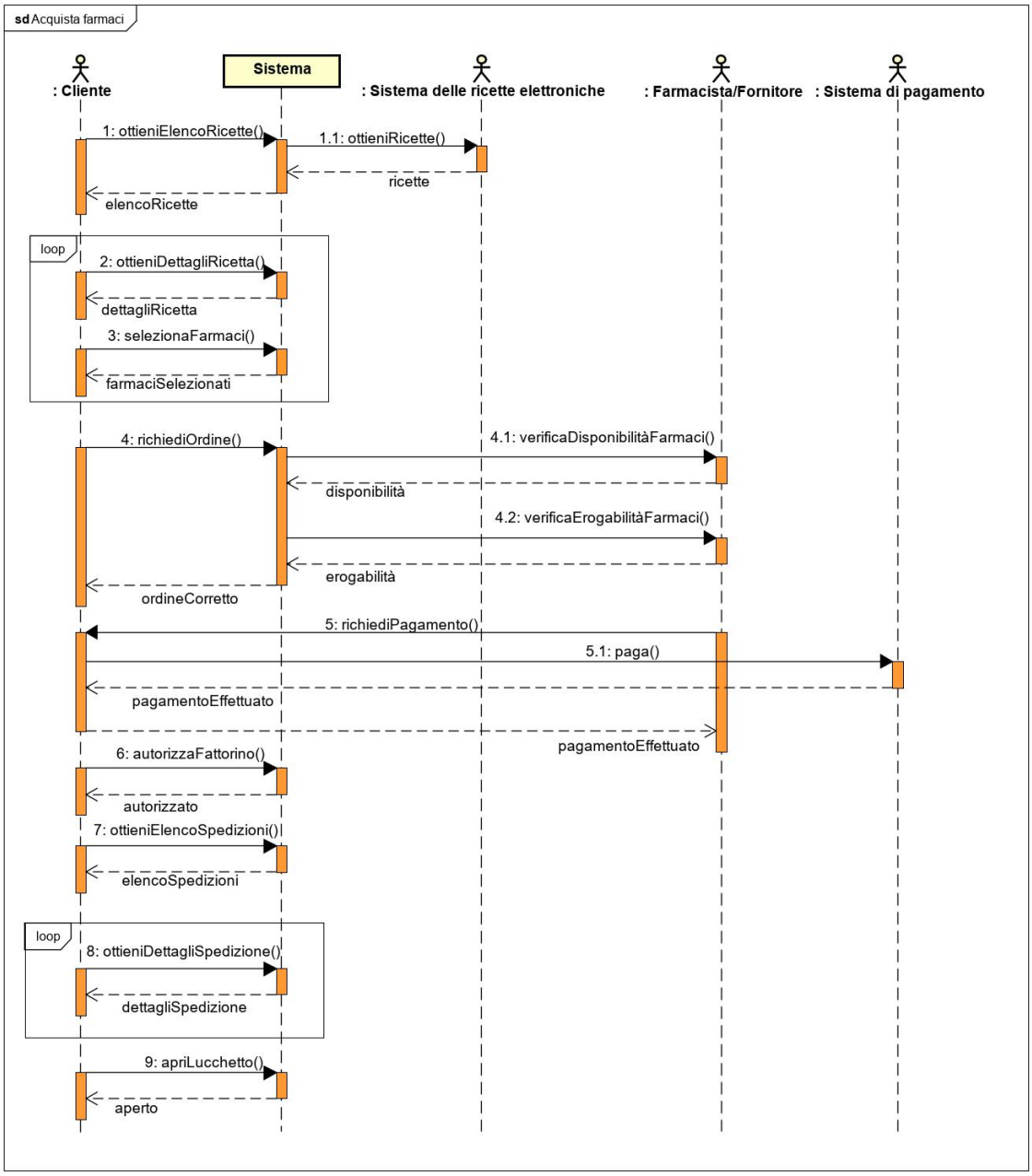



**Figura 5.4:** diagramma di sequenza dello scenario principale del caso d'uso "acquista farmaci".

3. Il fattorino seleziona un ordine di suo interesse

4. Il sistema presenta i dettagli dell'ordine

5. Il fattorino comunica al farmacista o al fornitore le informazioni necessarie al

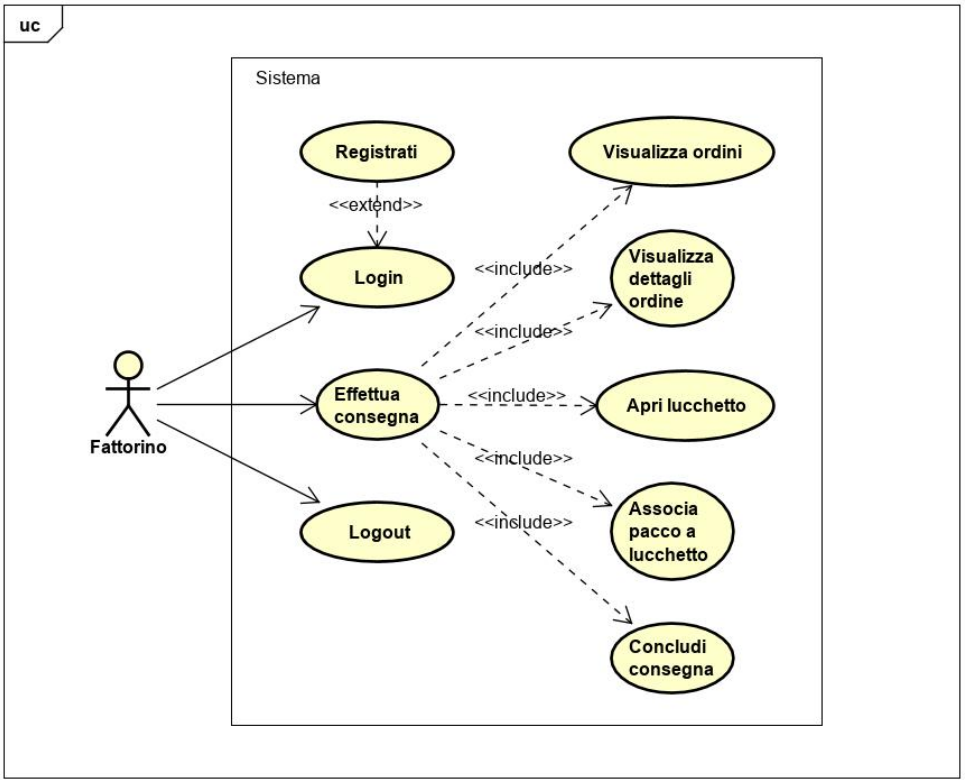



**Figura 5.5:** diagramma del caso d'uso "effettua consegna".

ritiro

6. Il fattorino mette i farmaci all'interno di un pacco chiuso da un lucchetto intelligente
7. Il fattorino associa il lucchetto all'ordine (e quindi al destinatario)
8. Il fattorino porta i farmaci al legittimo destinatario concludendo la consegna

Nota: i passi 3-4 possono essere ripetuti un numero indefinito di volte dal fattorino.

**Diagramma di sequenza dello scenario principale di successo**: vedere figura 5.6

### 5.3.3 Caso d'uso: eroga farmaci

**Descrizione**: in questo caso d'uso un cliente vuole acquistare dei farmaci presso un farmacista/fornitore, per cui effettua la richiesta di ordine. Il farmacista/fornitore verifica la disponibilità e l'erogabilità dei farmaci richiesti in base alle informazioni

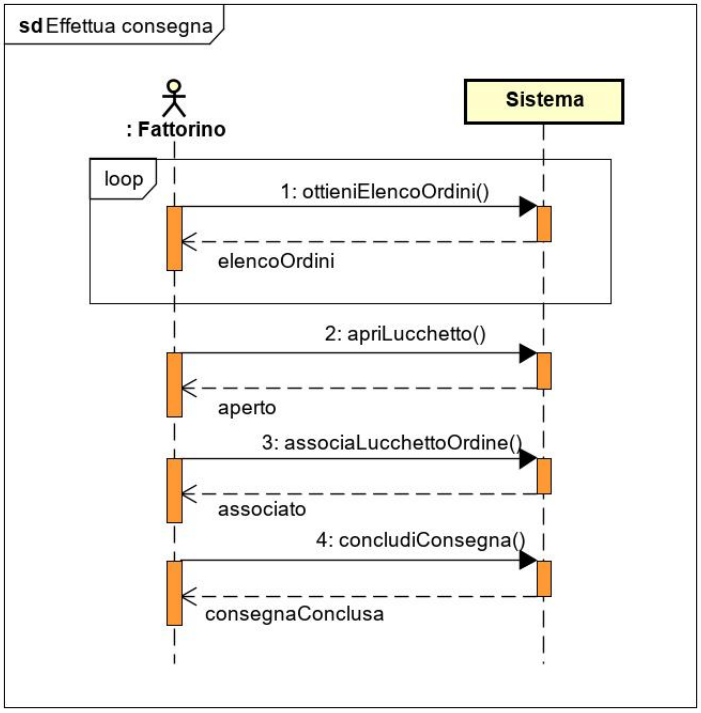



**Figura 5.6:** diagramma di sequenza dello scenario principale del caso d'uso "effettua consegna".

dell'ordine (codici NRE, numero di confezioni, ecc.) attraverso il proprio sistema informatico e attraverso il sistema di ricette elettroniche; in caso affermativo richiederà il pagamento al cliente. Dopo che il farmacista/fornitore ha verificato l'avvenuto pagamento l'ordine è pronto per la consegna, quindi il fattorino designato dal cliente riceverà una notifica. Esso andrà presso la farmacia o il magazzino e fornirà il suo identificativo e le informazioni dell'ordine necessarie al ritiro (codici NRE, numero di confezioni, ecc.). Il farmacista/fornitore verificherà che il fattorino sia autorizzato e potrà vedere i dettagli delle ricette e del cliente. Se tutto è corretto, il farmacista/fornitore darà un contenitore anonimo al fattorino (al cui interno vi sono i farmaci) e invierà al cliente un codice criptato necessario all'apertura del lucchetto intelligente. L'erogazione si concluderà segnando come "erogato" l'ordine.
**Diagramma**: vedere figura 5.7
**Livello**: sommario
**Attore primario**: farmacista o fornitore
**Attori secondari**:

1. Sistema di pagamento

2. Sistema delle ricette elettroniche

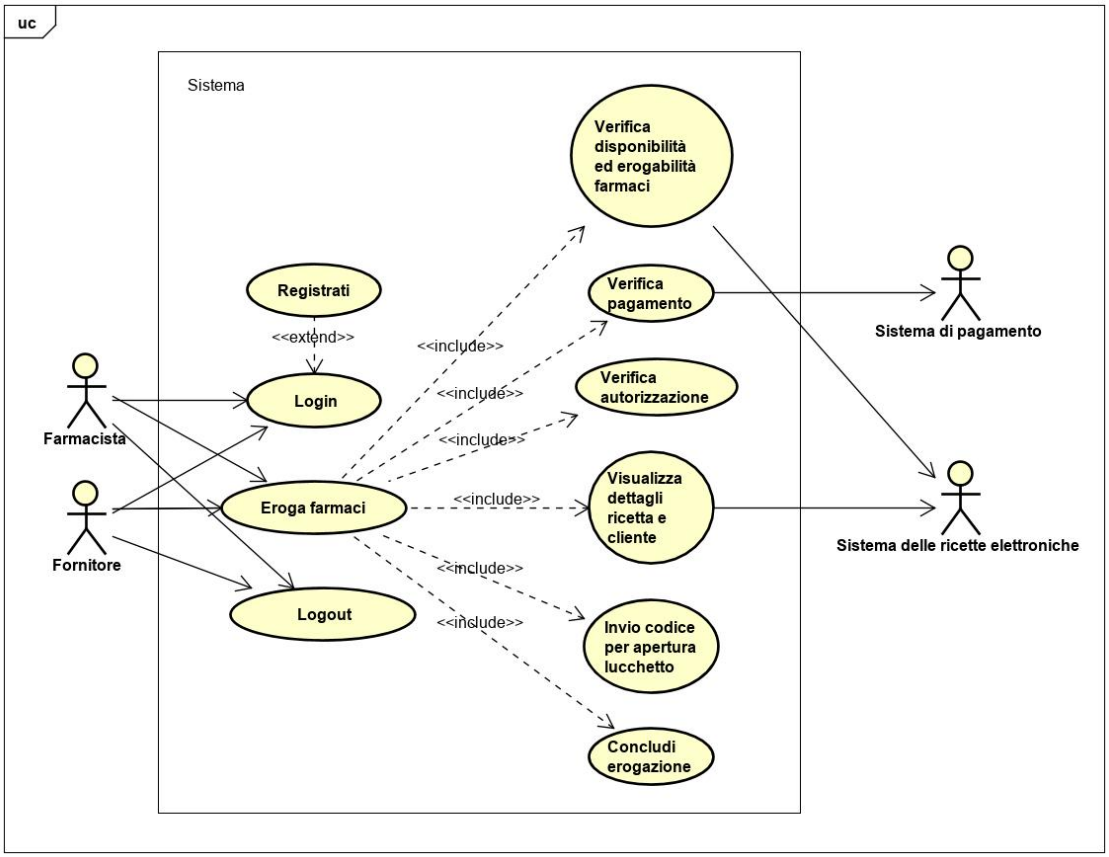



**Figura 5.7:** diagramma del caso d'uso "eroga farmaci".

**Precondizioni**:

- Il farmacista/fornitore deve essersi registrato sul sistema
- Il farmacista/fornitore deve aver effettuato il login

**Postcondizioni**:

- **Garanzie minime**: il farmacista/fornitore deve aver effettuato le verifiche necessarie all'erogazione dei farmaci, vale a dire disponibilità ed erogabilità dei farmaci, l'avvenuto pagamento dei farmaci e l'autorizzazione del fattorino al ritiro.
- **Garanzie massime**: il farmacista/fornitore ha erogato i farmaci

**Trigger**: il cliente effettua la richiesta di ordine
**Scenario principale di successo**:

1. Il farmacista/fornitore va nella sezione “ordini”
2. Il sistema fornisce l’elenco degli ordini
3. Il farmacista/fornitore seleziona un ordine di suo interesse
4. Il sistema presenta i dettagli dell’ordine, delle ricette e del cliente
5. Il farmacista/fornitore verifica l’erogabilità dei farmaci
6. Il farmacista/fornitore verifica la disponibilità dei farmaci
7. Il farmacista/fornitore richiede il pagamento dell’ordine
8. Il cliente paga attraverso il sistema di pagamento
9. Il farmacista/fornitore verifica l’avvenuto pagamento
10. Il fattorino riceve la richiesta di consegna
11. Il fattorino si presenta presso la farmacia/magazzino per effettuare il ritiro dei farmaci fornendo il proprio identificativo e le informazioni relative all’ordine
12. Il farmacista/fornitore seleziona l’ordine
13. Il sistema presenta i dettagli dell’ordine, delle ricette e del cliente
14. Il farmacista/fornitore verifica l’autorizzazione
15. Il farmacista/fornitore consegna un contenitore anonimo al fattorino
16. Il farmacista/fornitore invia al cliente un codice criptato necessario all’apertura del lucchetto intelligente
17. Lo stato dell’ordine diventa “erogato”

**Diagramma di sequenza dello scenario principale di successo**: vedere figura 5.8

## 5.4 Glossario

Nell’elenco successivo vengono definiti i concetti chiave (riportati anche in figura 5.9) riguardanti il sistema di consegna a domicilio di farmaci finora analizzato:

- **Account**: area riservata ad uno specifico utente, a cui si accede tramite una procedura di autenticazione (login), in cui si possono visualizzare le informazioni accessibili dal sistema o memorizzate al suo interno (come ad esempio quelle del profilo personale, la cronologia delle operazioni eseguite, le proprie ricette se si è fatto accesso come cliente, le consegne da effettuare per i fattorini e così via), utilizzare strumenti e effettuare operazioni (in base al proprio ruolo all'interno del sistema).

- **Cliente**: utente che vuole acquistare e ricevere a domicilio dei farmaci (in linea teorica il cliente e il paziente dovrebbero essere la stessa persona).

- **Consegna**: trasporto da parte del fattorino dei farmaci acquistati dal cliente alla sua destinazione finale.

- **Corriere**: azienda che effettua consegne di pacchi; i fattorini lavorano per un corriere.

- **Dottore**: medico che visita il paziente e gli prescrive le ricette elettroniche inserendole nel sistema di ricette elettroniche.

- **Farmacia**: luogo in cui vengono venduti al dettaglio i medicinali dal farmacista.

- **Farmacista**: colui che lavora in una farmacia e che consegna i farmaci al fattorino per la consegna.

- **Farmaco**: sostanza, medicina (o prodotto medicinale), prescritta da un medico ad un paziente attraverso ricetta, che agisce sull'organismo umano provocando modificazioni funzionali, utili o dannose, mediante un'azione chimica o fisica; ogni confezione è identificata da un codice seriale e ogni farmaco (e relativi formati) è identificato da un codice AIC.

- **Fornitore**: colui che svolge un ruolo simile a quello del farmacista (vale a dire erogare farmaci), ma lavora in un magazzino e fornisce dei servizi supplementari (packaging, riordino dei farmaci, aggiunta di informazioni e altri servizi, come offre l'azienda PillPack).

- **Fattorino**: colui che effettua le consegne

- **Lucchetto intelligente**: lucchetto (simile a quello fornito dall'azienda BoxLock), identificato nel sistema con un ID, che chiude i pacchi utilizzati per le consegne; viene aperto tramite un codice.

- **Magazzino**: luogo in cui vengono conservate grandi quantità di farmaci che possono essere venduti all'ingrosso alle farmacie o al dettaglio attraverso consegne a domicilio; vi lavora il fornitore.

- **Ordine d'acquisto**: è un contratto digitale stipulato tra il cliente e il venditore di farmaci e/o servizi (sistema, fattorino, farmacista, fornitore, ecc.), in cui vengono specificati i dettagli dell'acquisto (quali farmaci e/o servizi sono stati acquistati, i dati del cliente e del venditore, quali sono i termini di consegna e spedizione, l'importo pagato, i termini di pagamento, numero e data del documento, ecc.); è identificato nel sistema con un ID.
- **Pacco**: contenitore identificato nel sistema con un ID, che racchiude i farmaci del cliente, chiuso da un lucchetto intelligente utilizzato dal fattorino per effettuare la consegna.
- **Pagamento**: trasferimento digitale di soldi tramite un sistema di pagamento in cambio di farmaci e/o servizi forniti al cliente da altri attori.
- **Paziente**: malato a cui un dottore ha prescritto una ricetta in seguito ad una visita medica (in linea teorica il paziente e il cliente dovrebbero essere la stessa persona).
- **Ricetta elettronica**: ricetta in formato digitale identificata da un codice NRE e salvata all'interno del sistema delle ricette elettroniche.
- **Sistema delle ricette elettroniche**: sistema esterno gestito da SOGEI in cui sono salvate le ricette elettroniche prescritte dai dottori ai pazienti.
- **Sistema di pagamento**: sistema esterno attraverso cui si effettuano i pagamenti (carte di pagamento, Paypal, ecc.).
- **Sistema esterno**: attore non umano che interagisce col sistema (sistema di pagamento o sistema delle ricette elettroniche).
- **Spedizione**: invio dei farmaci dal luogo in cui sono conservati i farmaci al momento dell'acquisto (presso una farmacia o presso un magazzino) alla destinazione specificata dal cliente; può richiedere più passaggi e l'impiego di più corrieri e fattorini.
- **Utente**: attore umano che utilizza il sistema (cliente, fattorino, farmacista o fornitore); è identificato nel sistema con un ID.

## 5.5 Componenti hardware e software del sistema

I componenti hardware che costituiscono il sistema sono i dispositivi elettronici (PC, smartphone e/o tablet) e i server. Si ipotizza che i PC vengano usati dai farmacisti e dai fornitori, mentre gli smartphone e i tablet vengano utilizzati dai clienti e dai fattorini. All'interno dei dispositivi elettronici girano le applicazioni

client (app mobile e Web App) attraverso cui gli utenti accedono al servizio, mentre nei server sono presenti l'applicazione web e la Blockchain che gestiscono i servizi e tutti i relativi dati (registrazioni, ordini, ecc.). Il sistema presenta dunque un'architettura client-server, in cui i server forniscono dei Web Service ai client tramite API REST. Come si vede in figura 5.10 i sistemi di pagamento, il sistema delle ricette elettroniche e i lucchetti sono esterni al sistema. Anche i sistemi esterni espongono Web Service che il sistema utilizza.

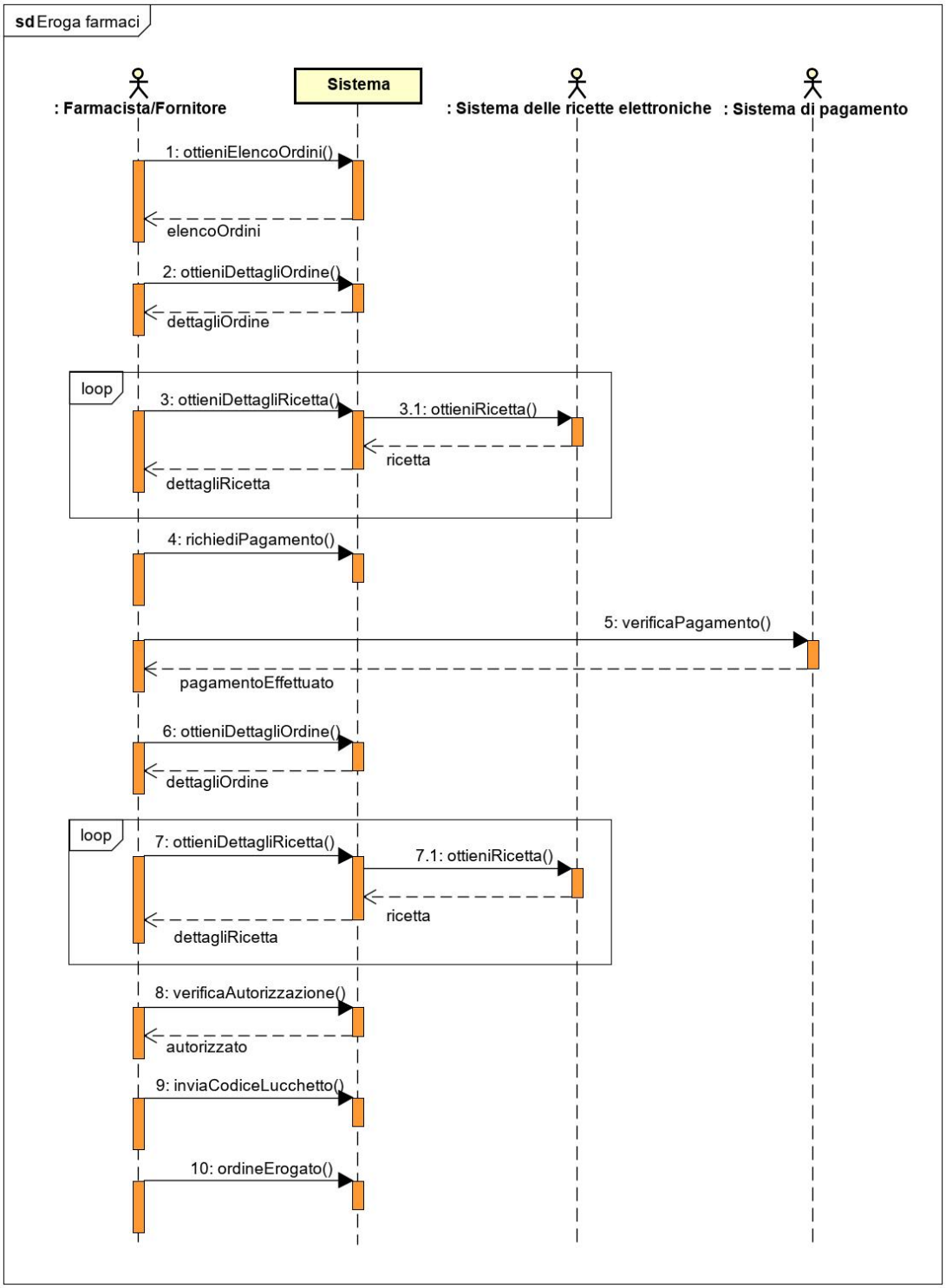



**Figura 5.8:** diagramma di sequenza del caso d'uso "eroga farmaci".

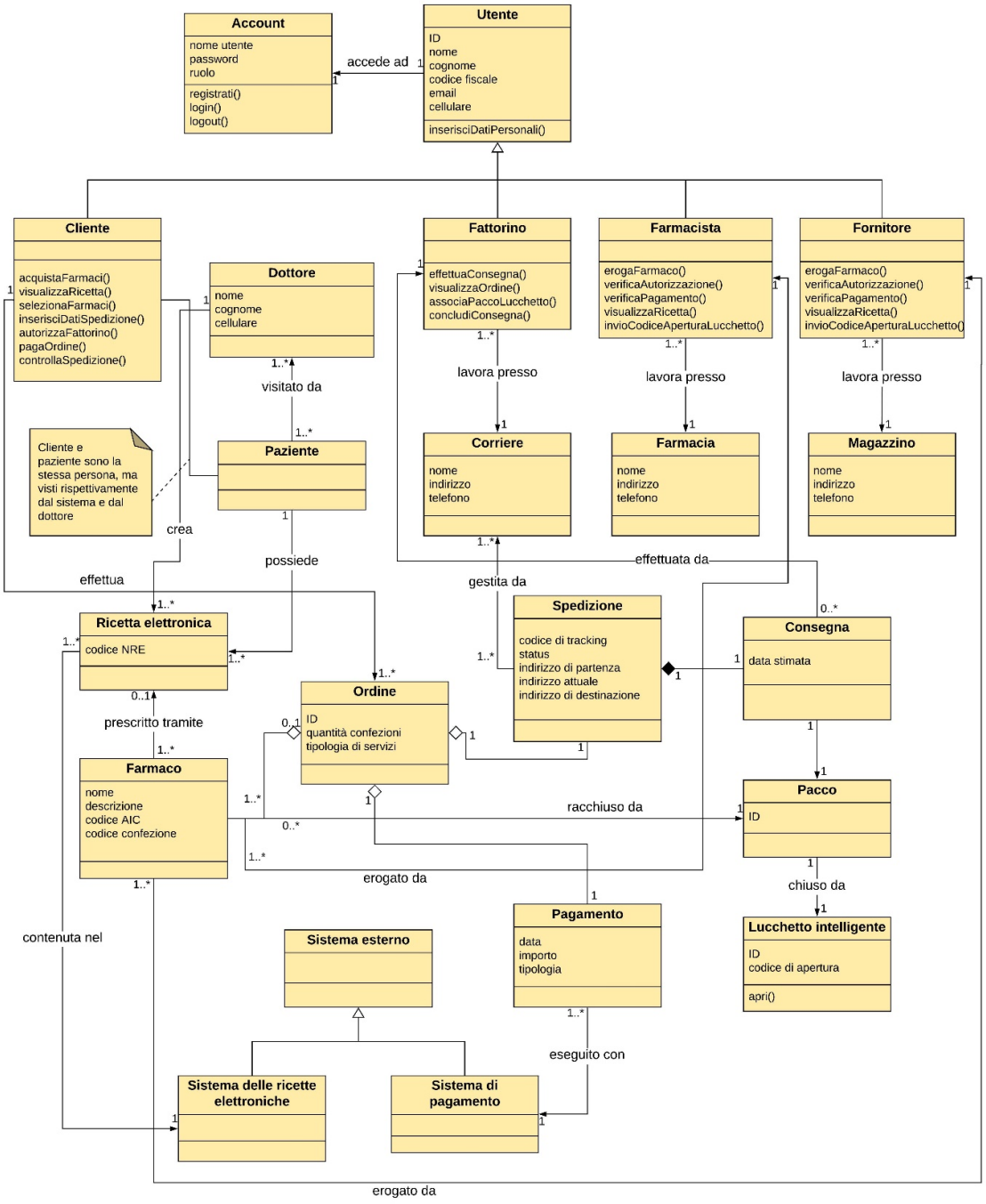



**Figura 5.9:** diagramma dei concetti chiave del sistema.

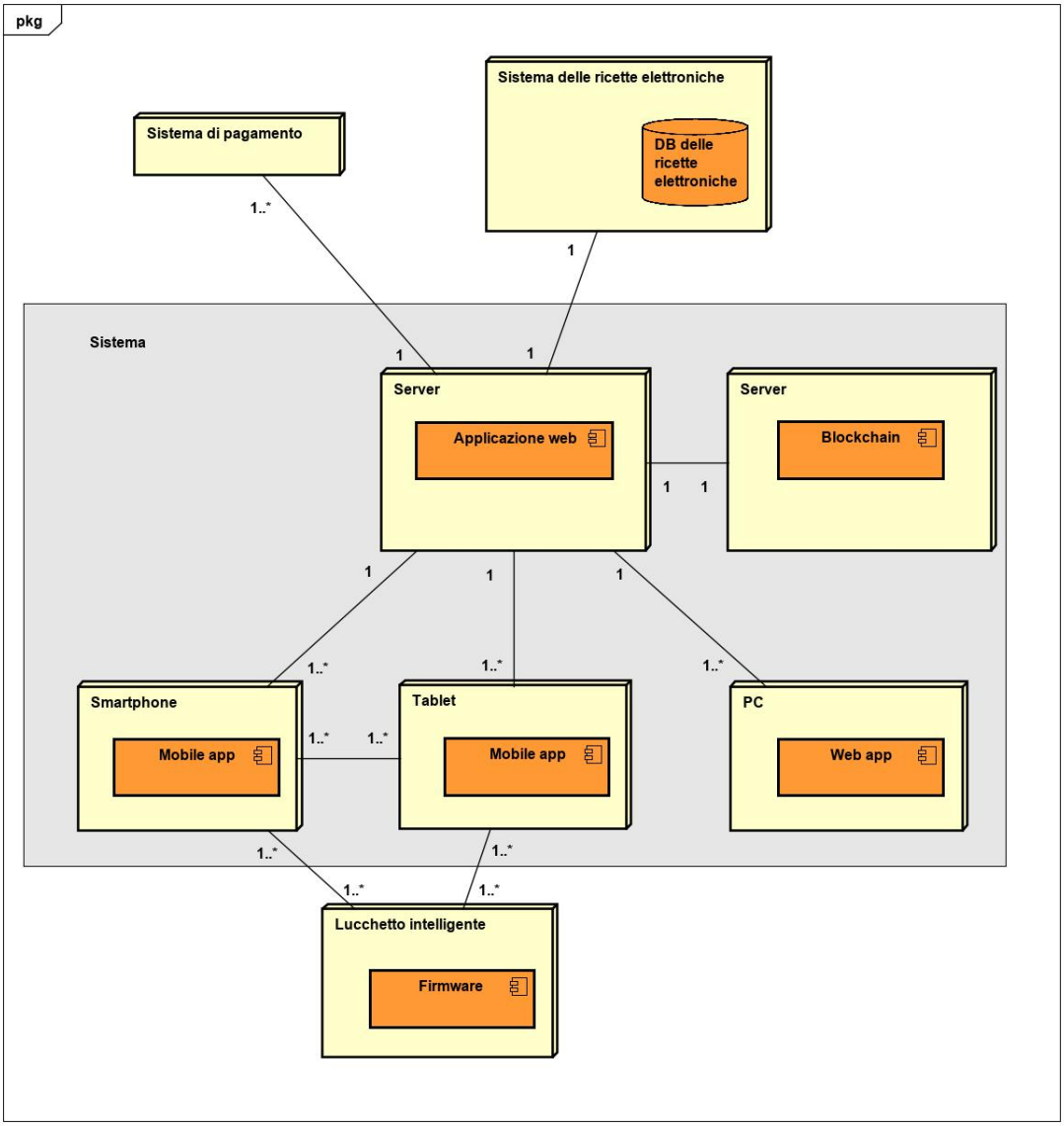



**Figura 5.10:** diagramma di deployment.

# Capitolo 6

# Realizzazione del Proof of Concept

In questo capitolo si descriverà una possibile realizzazione del Proof of Concept, con particolare attenzione per la Blockchain Hyperledger Fabric e per il framework Hyperledger Composer. Nel software implementato sono stati tralasciati alcuni aspetti non essenziali, come la memorizzazione di alcune informazioni secondarie, la visualizzazione delle ricette elettroniche da parte dei clienti, o la presenza di un fornitore di farmaci (è trascurabile perché interagirebbe col sistema nella stessa maniera di un farmacista).

Come anticipato nella precedente sezione "Componenti hardware e software del sistema", l'architettura dell'ipotetico sistema (vedere figura 6.10 del capitolo precedente) è client-server con due server, uno che fornisce i Web Service REST e un altro per la Blockchain in cui è caricata la Business Network Definition (il modello della BN), e un numero indefinito di client (Web App). Quando il sistema è operativo, generalmente si susseguono gli stessi passaggi concettuali: l'utente interagisce con il client, il client effettua una richiesta HTTP (fornendo i dati eventualmente passati dall'utente), il server REST la riceve e la inoltra al server Fabric; questo la elabora e invia la risposta che, infine, viene restituita, seguendo il percorso inverso, al client. Nella maggior parte dei test eseguiti il numero di client è stato limitato a tre (utilizzati da un ipotetico cliente, un ipotetico fattorino e da un ipotetico farmacista).

Dunque, nelle prossime sezioni si approfondiranno l'obiettivo principale e i sottobiettivi del Proof of Concept, il modello della Business Network, ulteriori concetti riguardanti il sistema, il sistema visto come macchina di Moore, l'ambiente di sviluppo, lo scenario principale di successo, i test eseguiti e infine i prototipi dell'interfaccia utente.

## 6.1 Obiettivo principale e sottobiettivi

L'obiettivo principale di questo Proof of Concept è quello di dimostrare che attraverso utilizzo di Hyperledger Fabric sia possibile ovviare alla mancanza di fiducia dei clienti delle consegne a domicilio di farmaci nei confronti dei fattorini, alla scarsa privacy, all'assenza di tracciabilità, alle potenziali truffe e manomissioni dei dati o dei prodotti (solo per citare alcune problematiche), aumentando l'automazione e l'efficienza rispetto al sistema "tradizionale". Per raggiungere questo obiettivo il Proof of Concept deve fare in modo che:

1. I fattorini non sappiano quello che trasportano (e neanche il codice NRE, ma unicamente l'ID del ordine, il cliente e il farmacista);
2. I fattorini non possano modificare gli ordini (a parte lo stato, se autorizzati);
3. Solo il fattorino autorizzato possa ritirare il pacco;
4. I fattorini non possano andare a ritirare i farmaci dello stesso ordine più volte;
5. I fattorini ritirino solo quello che c'è scritto nell'ordine;
6. I participant (cliente, fattorino, farmacista, cioè 3 casi differenti) possano eseguire solo le loro transazioni;
7. I participant non possano eseguire transaction spettanti all'amministrazione della Business Network, vale a dire (elenco delle principali):
   (a) Eliminare un participant;
   (b) Rimuovere un asset;
   (c) Aggiungere un participant;
   (d) Rimuovere un participant;
   (e) Rilasciare una nuova identità a un participant;
   (f) Revocare un'identità;
   (g) Avviare la Business Network;
   (h) Resettare la Business Network;
   (i) Settare il livello di log;
8. I participant possano effettuare le operazioni CRU sulle loro informazioni, mentre su quelle degli altri non possano operare;
9. Solo i clienti possano creare gli ordini;
10. Il cliente proprietario dell'asset possa effettuare le operazioni CRU su di esso;

11. I participant possano effettuare operazioni RU sugli asset altrui solo se autorizzati, in particolare:
    (a) Il fattorino autorizzato possa conoscere l'ID dell'ordine, del cliente e del farmacista;
    (b) Il fattorino autorizzato possa modificare il campo "stato";
    (c) Il farmacista possa vedere tutte le informazioni;
    (d) Il farmacista possa aggiungere dati nei campi "importo" e "codiceAperturaLucchetto";
    (e) Il farmacista possa modificare il campo "stato";
12. I participant vedano solo le transaction che sono state eseguite da loro oppure quelle in cui sono stati coinvolti;
13. I fattorini non possano alterare/sottrarre il contenuto del pacco;
14. Solo il destinatario o i delegati possano aprire il pacco;
15. L'amministratore non possa eseguire e vedere transaction spettanti ai participant;
16. L'amministratore non possa operare sugli ordini;
17. Le notifiche non contengano informazioni sensibili;
18. Le transaction, dopo essere state eseguite, non siano modificabili (e di conseguenza il timestamp);

I sottobiettivi sopracitati sono stati raggiunti principalmente attraverso la definizione delle access control rule (che verranno descritte nel modello della Business Network), poi con la scelta delle informazioni da inserire negli asset (ad esempio specificando il fattorino scelto per la consegna dei farmaci all'interno dell'ordine si impedisce il ritiro non autorizzato) e infine con i controlli effettuati all'interno delle funzioni corrispondenti alle transaction eseguite (ad esempio controllando che lo stato corrente sia corretto, impedendo così l'esecuzione multipla di una transaction per il medesimo ordine).

## 6.2 Modello della Business Network

Per realizzare la parte di sistema inerente alla Blockchain Hyperledger Fabric, utilizzando il framework Hyperledger Composer, si è definito innanzitutto il modello della Business Network da implementare (in figura 6.1 è riportato il diagramma di classe). Gli elementi che lo compongono sono presenti nell'elenco successivo:

- **Asset**: ordine
- **Participant**: cliente, fattorino e farmacista
- **Transaction**:

  1) AutorizzazioneFarmacista
  2) RichiestaPagamento
  3) ConfermaPagamento
  4) AutorizzazioneFattorino
  5) RichiestaConsegna
  6) Erogazione
  7) Consegna
  8) InfoParzialiOrdine
  9) StoricoTransazioniFattorino

  Nota: queste transaction vanno aggiunte a quelle già presenti di default.

- **Event**:

  1) FarmacistaAutorizzato
  2) PagamentoRichiesto
  3) PagamentoConfermato
  4) FattorinoAutorizzato
  5) ConsegnaRichiesta
  6) OrdineErogato
  7) OrdineConsegnato
  8) InfoParzialiOrdineLette

  Nota: gli event vengono emessi in seguito all'esecuzione delle transaction.

- **Access control rule**:

  1) Ogni participant può leggere e aggiornare le proprie informazioni
  2) Ogni cliente può creare, leggere e aggiornare un proprio ordine
  3) L'amministratore non può operare sugli ordini
  4) Il cliente può leggere tutte le transazioni che ha eseguito o in cui è stato coinvolto, a patto che esso sia il proprietario dell'ordine specificato

5) Il fattorino può leggere tutte le transazioni che ha eseguito o in cui è stato coinvolto (vale a dire "autorizzazioneFattorino", "richiestaConsegna", "Consegna", "infoParzialiOrdine" e "storicoTransazioniFattorino"), a patto che esso sia autorizzato ad operare sull'ordine specificato
6) Il farmacista può leggere tutte le transazioni che ha eseguito o in cui è stato coinvolto (vale a dire tutte tranne quelle di tipo "Consegna", "infoParzialiOrdine" e "storicoTransazioniFattorino"), a patto che esso sia autorizzato ad operare sull'ordine specificato
7) Il cliente può eseguire le transazioni di tipo "autorizzazioneFarmacista", "confermaPagamento" o "autorizzazioneFattorino", a patto che esso sia il proprietario dell'ordine specificato
8) Il fattorino può eseguire le transazioni di tipo "Consegna", "infoParzialiOrdine" o "storicoTransazioniFattorino", a patto che esso sia autorizzato ad operare sull'ordine specificato
9) Il farmacista può eseguire le transazioni di tipo "richiestaPagamento", "richiestaConsegna" o "erogazione", a patto che esso sia autorizzato ad operare sull'ordine specificato
10) Il fattorino può leggere e modificare lo stato dell'ordine specificato, attraverso l'esecuzione della transaction di tipo "consegna", e leggere l'ID dell'ordine, del cliente e del farmacista, attraverso l'esecuzione della transaction di tipo "infoParzialiOrdine", a patto che sia autorizzato
11) Il farmacista può potenzialmente leggere e aggiornare tutte le informazioni relative all'ordine specificato (in realtà le informazioni su cui agisce sono minori e sono determinate dalle transazioni che può eseguire: può leggere tutto, aggiungere dati nei campi "importo" e "codiceAperturaLucchetto" e modificare il campo "stato"), a patto che sia autorizzato
12) Ogni participant può vedere le transazioni, presenti dell'historian registry, che ha eseguito
13) Ogni cliente può vedere le transazioni, presenti dell'historian registry, che coinvolgono i propri ordini
14) Ogni fattorino può vedere le transazioni, presenti dell'historian registry, in cui è coinvolto (perché autorizzato), vale a dire di tipo "autorizzazioneFattorino", "richiestaConsegna", "consegna", "infoParzialiOrdine" o "storicoTransazioniFattorino"
15) Ogni farmacista può vedere le transazioni, presenti dell'historian registry, in cui è coinvolto (perché autorizzato), vale a dire tutte tranne quelle di tipo "Consegna", "infoParzialiOrdine" e "storicoTransazioniFattorino"
16) Il fattorino può leggere l'ordine specificato attraverso la transazione "storicoTransazioniFattorino"

17) L'admin può vedere solo le transazioni, presenti dell'historian registry
18) L'admin può accedere alle risorse utente
19) L'admin può accedere alle risorse di sistema
20) Nessun participant può revocare un'identità
21) Nessun participant può avviare la Business Network
22) Nessun participant può resettare la Business Network
23) Nessun participant può settare il livello di log
24) Nessun participant può accedere allo storico delle transazioni
25) Tutti i participant possono accedere alle risorse di sistema

Nota: le access control rule vengono applicate dall'alto verso il basso, quindi sono scritte dalla più specifica alla più generica.

Gli ordini sono caratterizzati dall'ID (che li identifica all'interno del sistema), dallo stato dell'ordine, dal codice NRE della ricetta utilizzata, opzionalmente dal codice di apertura del lucchetto criptato, dall'id del cliente che ha richiesto l'ordine, opzionalmente dall'id del farmacista, opzionalmente dall'id del fattorino autorizzato ad effettuare la consegna e opzionalmente dall'importo da pagare per i farmaci acquistati. I clienti, i fattorini e i farmacisti sono caratterizzati dall'ID (che li identifica all'interno del sistema).

Nella tabella 6.1 per ogni transaction, sono riportati il nome, le proprietà (l'equivalente dei parametri delle funzioni), chi esegue la transaction e lo stato dell'ordine conseguente all'esecuzione. AddAsset è stata inserita nella tabella nonostante sia una transaction predefinita perché viene utilizzata dai clienti per creare gli ordini, per cui per estensione fa parte del modello. Le transaction InfoParzialiOrdine e StoricoTransazioniFattorino possono essere eseguite dal generico fattorino dopo che lo stesso è stato autorizzato ad operare sull'ordine oggetto delle due transaction; la loro esecuzione non provoca un cambio di stato dell'ordine. Nella tabella 6.2 viene descritta ogni transazione.

Nella tabella 6.3, per ogni event, sono riportati il nome, le proprietà e la transaction che lo emette.

## 6.3 Ulteriori concetti

Oltre al modello della Business Network della Blockchain Hyperledger Fabric, il sistema è caratterizzato da altri concetti che concorrono alla soluzione proposta e che aumentano la fiducia da parte dei clienti:

- **Business network card**: sono composte da un'identità, un certificato digitale e un connection profile (profilo di connessione).

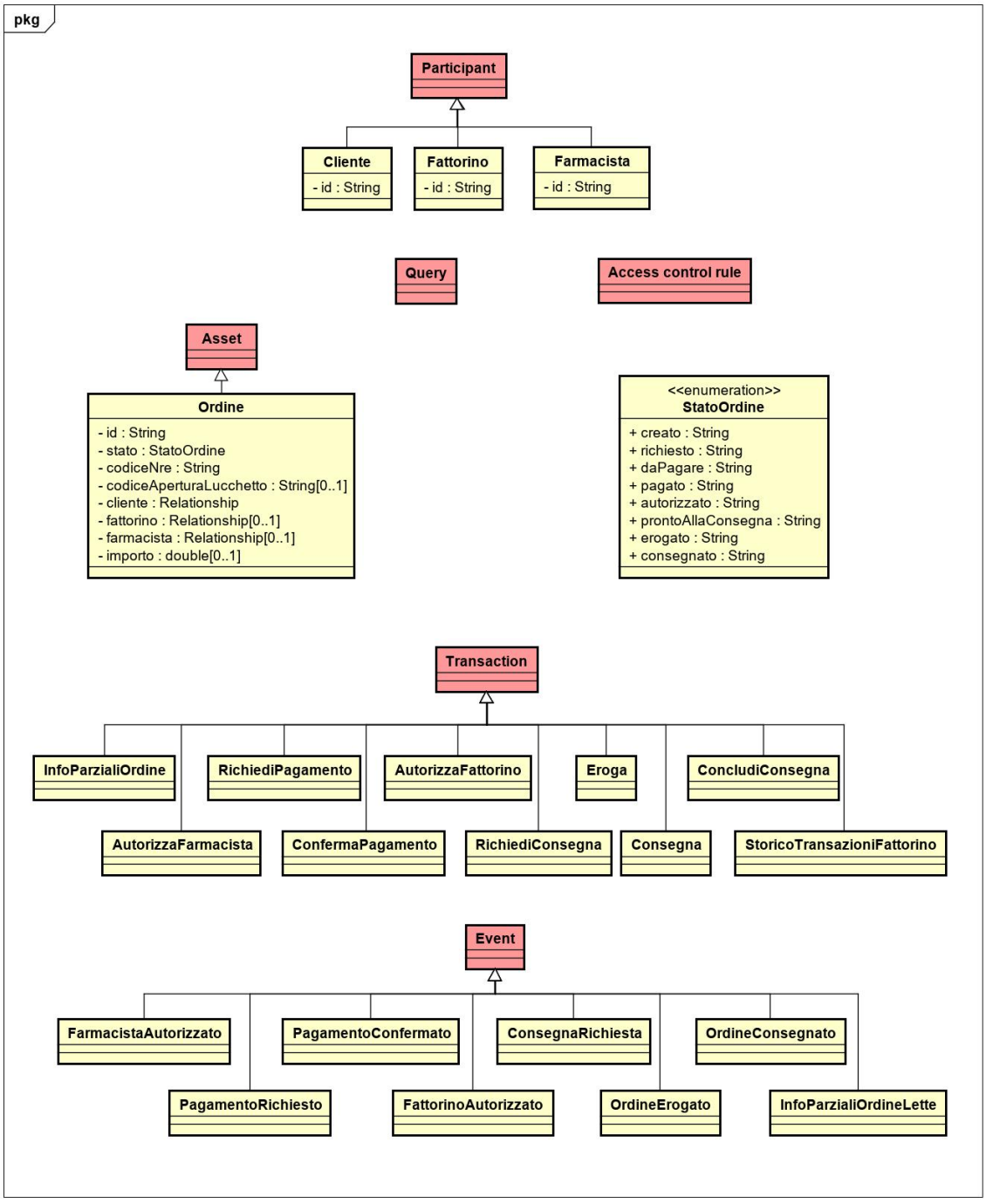



**Figura 6.1:** diagramma di classe del modello della Business Network.

- **Identità e chiave pubblica/privata**: ogni utente deve avere un certificato digitale X.509, contenente diverse informazioni tra cui i dati personali, la chiave

**Tabella 6.1:** dettagli delle transaction del modello della Business Network.

| **Transaction** | **Proprietà** | **Esecutore** | **Stato dell'ordine** |
|---|---|---|---|
| AddAsset | Id, stato, codiceNRE, cliente | Cliente | Creato |
| AutorizzazioneFarmacista | Ordine, farmacista | Cliente | Richiesto |
| RichiestaPagamento | Ordine, importo | Farmacista | DaPagare |
| ConfermaPagamento | Ordine | Cliente | Pagato |
| AutorizzazioneFattorino | Ordine, fattorino, farmacista | Cliente | Autorizzato |
| RichiestaConsegna | Ordine | Farmacista | ProntoAllaConsegna |
| Erogazione | Ordine, fattorino, codiceApertura-Lucchetto | Farmacista | Erogato |
| Consegna | Ordine | Fattorino | Consegnato |
| InfoParzialiOrdine | Ordine | Fattorino | - |
| StoricoTransazioniFattorino | Ordine | Fattorino | - |

pubblica e la Certificate Authority che assicura la corrispondenza tra chiave pubblica e l'identità. Il concetto di identità è fondamentale perché in base ad esso si concedono, oppure no, le autorizzazioni sulle risorse, sulle operazioni e sull'accesso alle informazioni (ad esempio quando un cliente autorizza un fattorino al ritiro dei farmaci), si può risalire all'autore di condotte disoneste o le si possono prevenire (ad esempio se i farmaci sono stati alterati) e si può verificare se un utente si finge qualcun altro (ad esempio al momento del ritiro dei farmaci in farmacia). La chiave pubblica di un determinato cliente che ha richiesto un ordine viene utilizzata dal farmacista autorizzato per criptare il codice di apertura del lucchetto che chiude il pacco contenente i farmaci, in modo tale che sia solamente il destinatario ad aprirlo (decifrando il codice attraverso la chiave privata).

- **Connection profile**: vengono utilizzati per definire il sistema a cui connettersi.

- **Consenso**: algoritmo attraverso cui i peer della Blockchain verificano, ed eventualmente approvano, una determinata transaction; ciò fa sì che non sia necessaria una terza parte fidata.
- **Chaincode**: termine usato in Hyperledger Fabric per definire lo smart contract, esso permette di automatizzare ed ottimizzare una serie di operazioni e processi che altrimenti sarebbero manuali.
- **Ledger e state database**: dopo che le transaction sono state approvate vengono inserite nel ledger distribuito tra i vari peer, mentre lo stato corrente degli asset e dei participant è all'interno dello state database. I meccanismi già descritti in precedenza (funzioni di hash, digest, timestamp, ecc.) garantiscono la tracciabilità, l'immutabilità, l'integrità e la sequenzialità delle operazioni eseguite dai participant.
- **Web Service REST**: a partire dal modello si possono creare le REST API per effettuare operazioni sulla Blockchain.
- **Lucchetto intelligente**: verrebbe utilizzato al momento del ritiro dei farmaci da parte del fattorino. In particolare esso inserirebbe all'interno di un pacco identificato da un codice ID i farmaci e poi lo chiuderebbe con il lucchetto. Dopo questa operazione il fattorino assocerebbe il pacco al lucchetto (e di conseguenza al relativo ordine). Infine, nella fase di consegna il destinatario aprirebbe il lucchetto usando un codice a barre o un QR code che rappresenta il codice generato dalla decriptazione del codice cifrato inviato dal farmacista al cliente. Per fare tutto ciò il lucchetto intelligente dovrebbe avere quanto meno avere un codice identificativo, un lettore di codici a barre o QR code e una batteria (un esempio concreto è il lucchetto BoxLock).

## 6.4 Modello del sistema realizzato: macchina di Moore

Il sistema può essere interpretato come una macchina di Moore ovvero un automa a stati finiti con le seguenti caratteristiche:

- Dinamico
- Tempo invariante
- Non lineare
- A stati discreti e finiti
- Con un'evoluzione dipendente dal susseguirsi di un insieme finito di eventi

- Deterministico
- A tempo continuo
- Con uscite ricavate in funzione dei soli stati correnti

Tale macchina può essere definita attraverso sei elementi:

$$M = M\,(S,\ S_0,\ I,\ U,\ f,\ g)\,, \text{ dove}$$

- $S$ è l'insieme finito di **stati** dell'ordine: {creato ($s_0$), richiesto ($s_1$), daPagare ($s_2$), pagato ($s_3$), autorizzato ($s_4$), prontoAllaConsegna ($s_5$), erogato ($s_6$), consegnato ($s_7$)};
- $S_0$ è lo **stato iniziale** appartenente a $S$;
- $I$ è l'insieme finito degli **ingressi**, vale a dire le seguenti transaction eseguite dai participant: {addAsset ($i_0$), autorizzazioneFarmacista ($i_1$), richiestaPagamento ($i_2$), confermaPagamento ($i_3$), autorizzazioneFattorino ($i_4$), richiestaConsegna ($i_5$), erogazione ($i_6$), consegna ($i_7$)};
- $U$ è l'insieme finito di **uscite**, vale a dire i seguenti event emessi come conseguenza dell'esecuzione delle transaction: {farmacistaAutorizzato ($u_1$), pagamentoRichiesto ($u_2$), pagamentoConfermato ($u_3$), fattorinoAutorizzato ($u_4$), consegnaRichiesta ($u_5$), ordineErogato ($u_6$), ordineConsegnato ($u_7$)};
- $f\ : (S \times I)\ \rightarrow\ S$ è la **funzione di transizione** che mappa uno stato e un ingresso con lo stato successivo;
- $g\ : (S \rightarrow\ U)$ è la **funzione di trasformazione** che mappa ciascuno stato con il corrispondente output.

Graficamente questa specifica macchina di Moore può essere rappresentata come un diagramma di stato (figura 6.2), che assume anche la struttura di un grafo aciclico orientato (in inglese Directed Acyclic Graph, DAG).

## 6.5 Ambiente di sviluppo

Il sistema è stato implementato all'interno di una macchina virtuale **VisualBox** con sistema operativo **Ubuntu**, mentre la macchina reale utilizzata ha come sistema operativo **Windows**. Gli strumenti adoperati sono:

- **Visual Studio Code** con estensione **Hyperledger Composer** (per scrivere la Business Network definition);

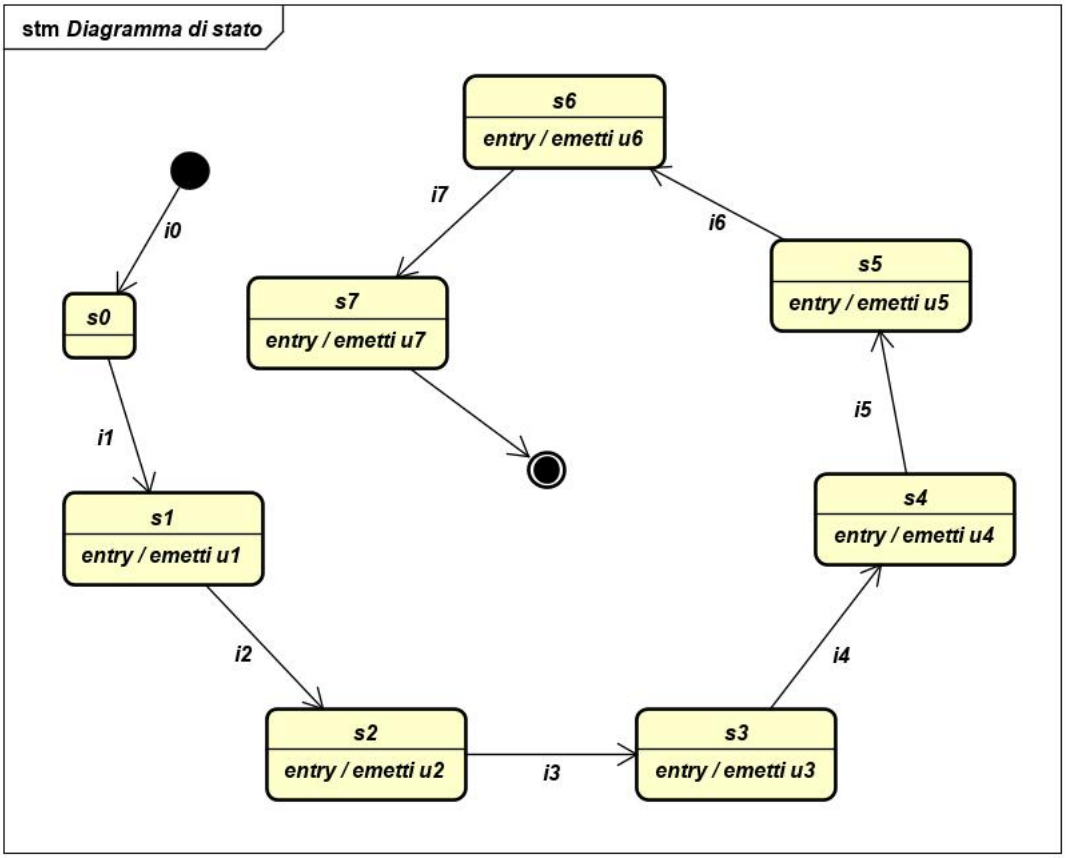



**Figura 6.2:** diagramma di stato della macchina di Moore che modella il sistema; in seguito all'esecuzione di una transaction il sistema cambia stato causando l'emissione un event.

- **Git** (software di controllo di versione distribuito);
- **Node.js** (runtime per l'esecuzione di codice JavaScript lato server);
- **Npm** (sistema di gestione di pacchetti);
- **Docker Engine** e **Docker Compose** (simile a VirtualBox, ma al posto delle macchine virtuali vi sono i container che contengono parti di sistemi operativi);
- **Python** (o meglio, l'interprete del linguaggio di programmazione Python);
- **Yeoman** (software per la generazione di applicazioni);
- **Angular** (Web App per interagire con la Business Network);
- **LoopBack** (piattaforma per la creazione di API e microservizi in Node.js);

- **Swagger** (framework utilizzato per progettare, creare, documentare e consumare Web Service REST);
- **Composer-cli** (interfacce a linea di comando essenziali per sviluppare con Composer);
- **Composer-rest-server** (runtime su cui caricare la REST API);
- **Generator-hyperledger-composer** (utility per generare un'applicazione Composer);
- **Composer-playground** (Web App per interagire con la Business Network);
- **Hyperledger Fabric** (runtime su cui caricare la Business Network).

## 6.6 Scenario principale di successo

Per testare adeguatamente il sistema (figura 6.3) è stato definito uno scenario principale di successo con relative premesse e poi è stato simulato il suo funzionamento in diverse condizioni.

**Premesse**:

1) Attori: un cliente, un farmacista e un fattorino;
2) La Business Network definition è stata installata sul server Fabric dall'amministratore ed è stato creato un amministratore per la BN;
3) È stata creata la REST API;
4) L'amministratore della BN ha creato un participant per tipologia di attore e ha rilasciato altrettante identità sotto forma di Business Network card (che vengono utilizzate per connettersi alla BN e identificarsi attraverso un certificato);
5) Gli attori si sono collegati alla Business Network fornendo le loro card.

**Scenario principale di successo**:

1) Il cliente crea un ordine contenente il codice NRE di una ricetta elettronica;
2) Il cliente richiede i farmaci di quella ricetta ad un farmacista e lo autorizza a vedere/modificare alcuni campi dell'ordine;
3) Il farmacista elabora la richiesta e manda l'importo da pagare;
4) Il cliente paga e conferma il pagamento;

5) Il cliente autorizza un fattorino a prelevare i farmaci;

6) Il farmacista, dopo aver verificato il pagamento, richiede al fattorino di prelevare il pacco contenente i farmaci;

7) Il farmacista, all'arrivo del fattorino, controlla il suo identificativo, visualizza l'ordine, consegna il pacco e aggiunge all'ordine il codice cifrato per l'apertura del lucchetto intelligente;

8) Il fattorino porta il pacco a destinazione;

9) Il cliente (o un suo delegato) apre il lucchetto con il codice decifrato;

10) Il fattorino conferma la conclusione della consegna.

## 6.7 Test effettuati

I test effettuati sono consistiti nella simulazione dello scenario principale di successo e degli scenari alternativi contenenti azioni non consentite o errori. La finalità dei test è stata quella di verificare che il sistema realizzato raggiungesse gli obiettivi del Proof of Concept elencati in precedenza. Per questo motivo i test si sono focalizzati essenzialmente sulle regole di accesso, nucleo fondamentale del sistema insieme alla logica delle transazioni, tenendo un livello di granularità pari alla singola operazione CRUD (Create, Read, Update, Delete) e al singolo campo degli asset. Infatti, per essere aderenti agli obiettivi, sono stati privatizzati i dati all'interno degli asset e sono state definite alcune transazioni utilizzabili solo da specifiche tipologie di participant (e solo previa autorizzazione del proprietario dell'asset) che potessero agire sui singoli campi. Ad esempio è stato verificato che un fattorino potesse vedere solo i campi di un ordine di cui aveva l'autorizzazione alla lettura o che potesse aggiornare lo stato dell'ordine oppure è stato verificato il fatto che un cliente potesse vedere lo storico delle proprie transazioni e di quelle che hanno riguardato il proprio ordine. I test sono stati eseguiti periodicamente alla fine di ogni fase di implementazione per verificare che il codice scritto corrispondesse alle aspettative, aumentando di volta in volta la complessità del sistema. Di seguito sono riportati i gruppi di test effettuati in diversi scenari:

1) Simulazioni con client Playground online per verificare la correttezza della Business Network definition con access rule generiche;

2) Simulazioni con client Playground online per verificare la correttezza della Business Network definition con access rule specifiche;

3) Simulazioni con server Fabric, server REST e client Angular con access rule generiche;

4) Simulazioni con un server Fabric, un server REST e un client Playground locale per ogni attore con access rule specifiche.

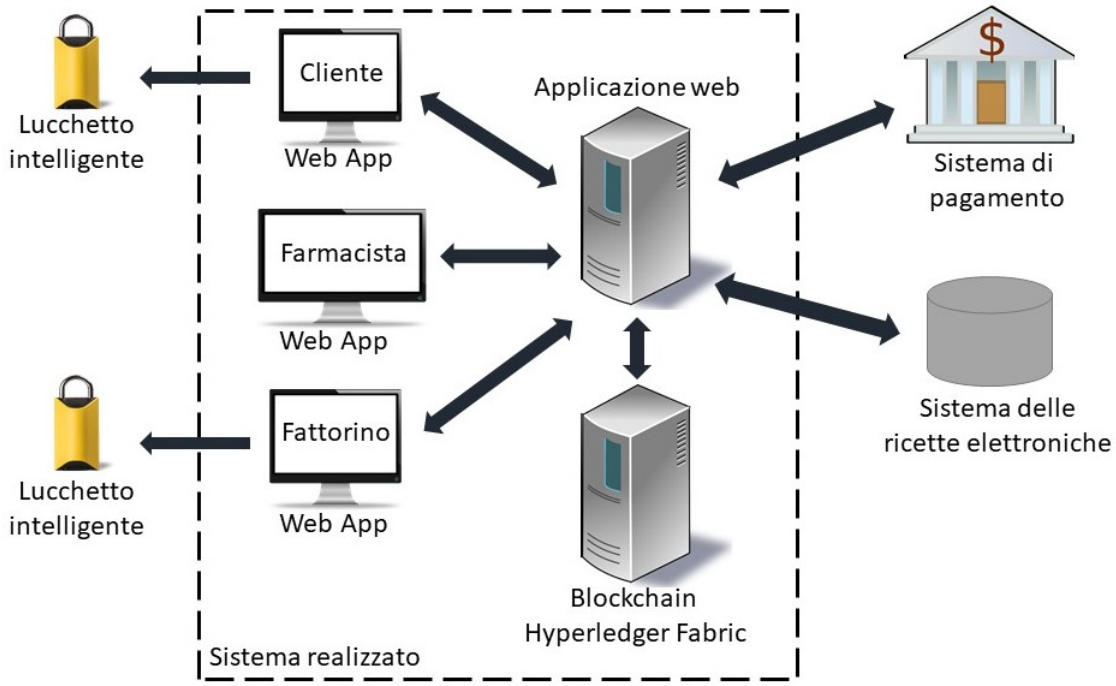



**Figura 6.3:** architettura del sistema.

## 6.8 Prototipi di interfaccia utente

Di seguito verranno riportati i principali prototipi dell'interfaccia utente della Web App. Alcune pagine sono in comune tra tutti gli attori, altre sono specifiche. Tutte le pagine sono all'interno di un browser e sono identificate da una URL presente nella barra degli indirizzi.

### 6.8.1 Login

In figura 6.4 è riportata la pagina di login con il form da compilare per accedere, se si è già registrati, altrimenti è possibile registrarsi seguendo l'apposito link. In alto è presente il logo e il nome della Web App.


**Figura 6.4:** pagina di login del prototipo dell'interfaccia utente.

### 6.8.2 Registrazione cliente

In figura 6.5 è riportata la pagina di registrazione con il form da completare. Da notarsi il radio button per specificare la registrazione come cliente. In alto è presente il logo e il nome della Web App.

### 6.8.3 Registrazione fattorino

In figura 6.6 è riportata la pagina di registrazione con il form da completare. Da notarsi il radio button per specificare la registrazione come fattorino. Ciò comporta il fatto che si debba specificare il corriere per cui si lavora. In alto è presente il logo e il nome della Web App.

### 6.8.4 Registrazione farmacista

In figura 6.7 è riportata la pagina di registrazione con il form da completare. Da notarsi il radio button per specificare la registrazione come farmacista. Ciò comporta il fatto che si debba specificare la farmacia per cui si lavora. In alto è presente il logo e il nome della Web App.

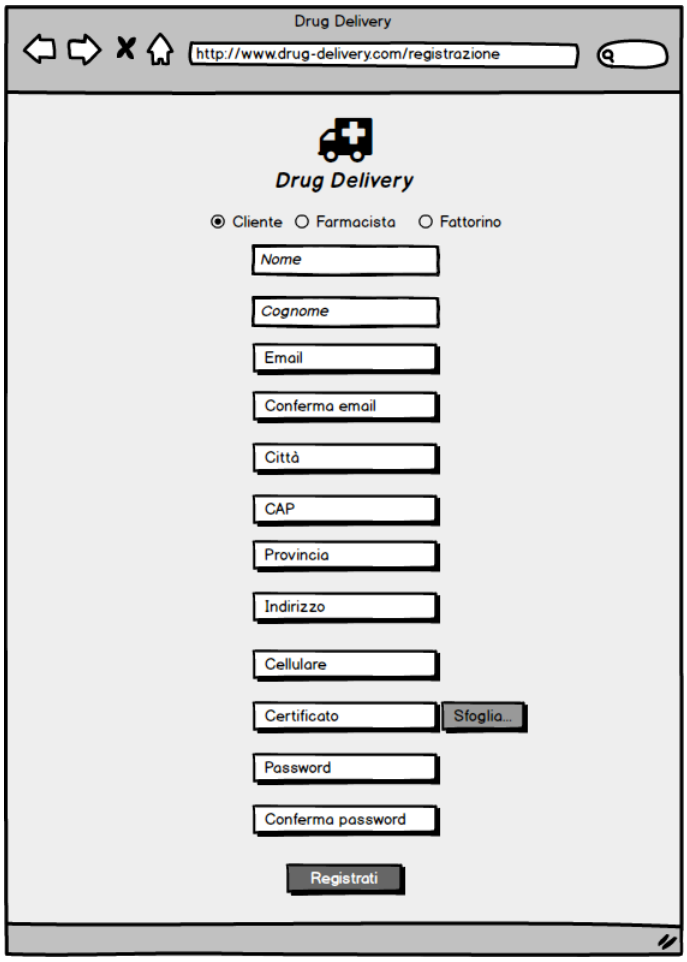



**Figura 6.5:** pagina di registrazione di un cliente.

### 6.8.5 Home cliente

In figura 6.8 è riportata la pagina home di un cliente. In alto a sinistra è presente il profilo con cui si è fatto l'accesso, con l'immagine di profilo a fianco del nome. In alto al centro è presente il logo e il nome della Web App. In alto a destra ci sono il bottone delle notifiche e quello di logout. Infine, al centro è presente un menù orizzontale per la navigazione che contiene le sezioni specifiche per i clienti e sotto l'immagine della home.

### 6.8.6 Home fattorino

In figura 6.9 è riportata la pagina di home di un fattorino. In alto a sinistra è presente il profilo con cui si è fatto l'accesso, con l'immagine di profilo a fianco del nome. In alto al centro è presente il logo e il nome della Web App. In alto a destra ci sono il bottone delle notifiche e quello di logout. Infine, al centro è presente un

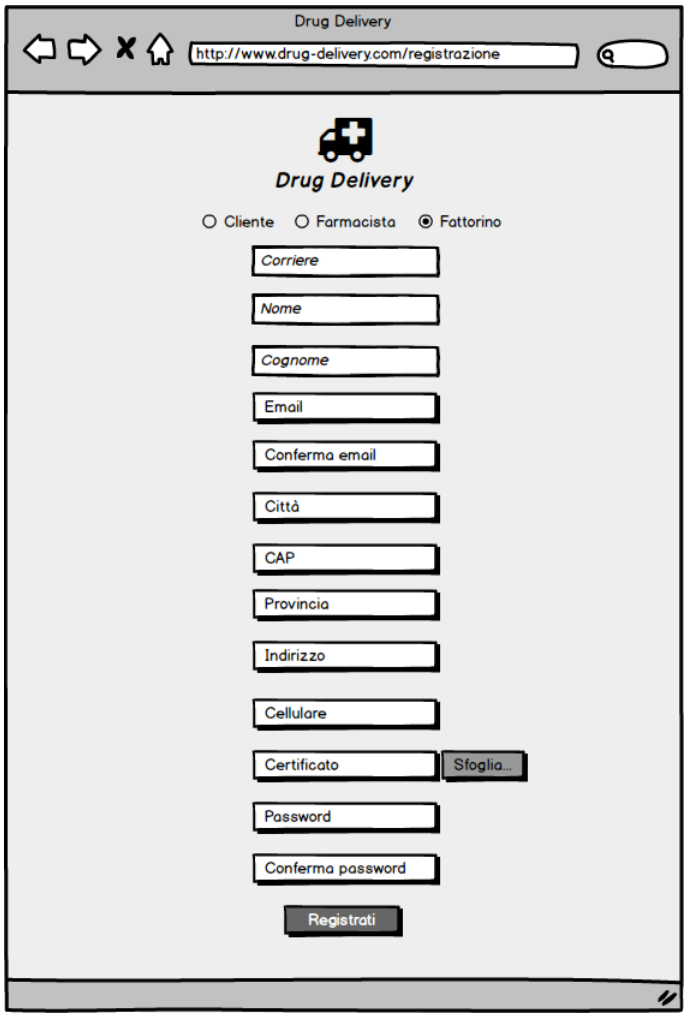



**Figura 6.6:** pagina di registrazione di un fattorino.

menù orizzontale per la navigazione che contiene le sezioni specifiche per i fattorini e sotto l'immagine della home.

### 6.8.7 Home farmacista

In figura 6.10 è riportata la pagina della home di un farmacista. In alto a sinistra è presente il profilo con cui si è fatto l'accesso, con l'immagine di profilo a fianco del nome. In alto al centro è presente il logo e il nome della Web App. In alto a destra ci sono il bottone delle notifiche e quello di logout. Infine, al centro è presente un menù orizzontale per la navigazione che contiene le sezioni specifiche per i farmacisti e sotto l'immagine della home.

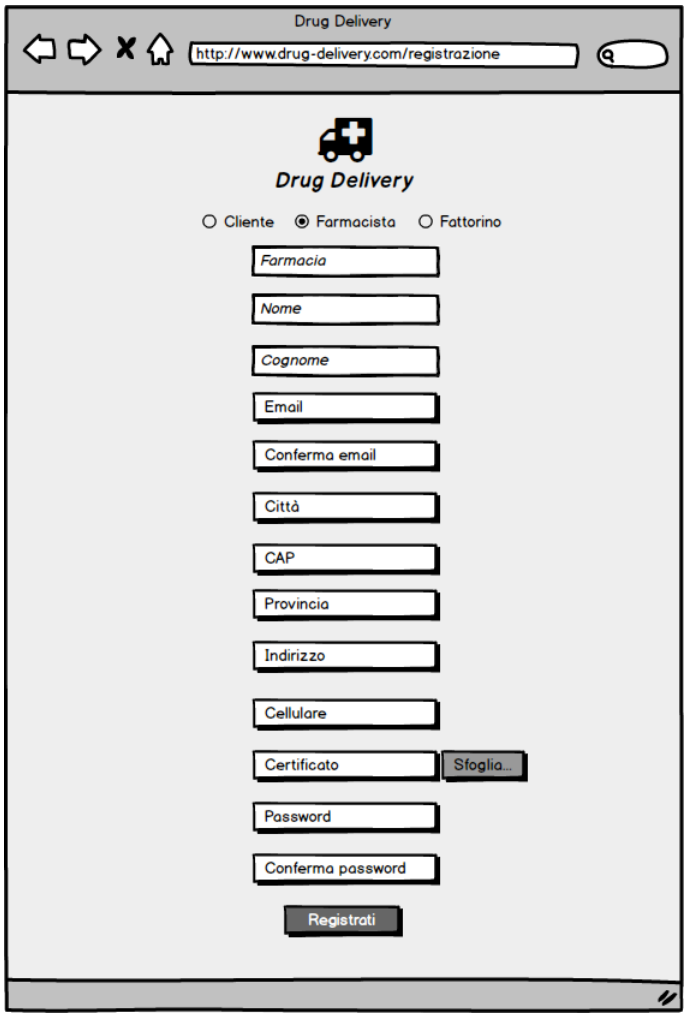



**Figura 6.7:** pagina di registrazione di un farmacista.

### 6.8.8 Ordini cliente

In figura 6.11 è riportata la pagina degli ordini di un cliente. Al centro è presente una tabella specifica per i clienti con i dati relativi agli ordini, sopra c'è un tasto per creare nuovi ordini, mentre di fianco agli ordini ci sono eventualmente dei tasti per eseguire delle operazioni (a seconda dello stato corrente dell'ordine).

### 6.8.9 Ordini fattorino

In figura 6.12 è riportata la pagina degli ordini presi in carico da un fattorino. Al centro è presente una tabella specifica per i fattorini con i dati relativi agli ordini, di fianco agli ordini ci sono eventualmente dei tasti per eseguire delle operazioni (a seconda dello stato corrente dell'ordine).


**Figura 6.8:** pagina home di un cliente.

### 6.8.10 Ordini farmacista

In figura 6.13 è riportata la pagina degli ordini presi in carico da un farmacista. Al centro è presente una tabella specifica per i farmacisti con i dati relativi agli ordini, di fianco agli ordini ci sono eventualmente dei tasti per eseguire delle operazioni (a seconda dello stato corrente dell'ordine).

### 6.8.11 Storico cliente

In figura 6.14 è riportata la pagina dello storico di un cliente (ma lo storico dei fattorini e dei farmacisti è identico della struttura, cambia solo nei contenuti visualizzabili).


**Figura 6.9:** pagina home di un fattorino.


**Figura 6.10:** pagina home di un farmacista.

**Tabella 6.2:** descrizione delle transaction del modello della Business Network.

| **Transaction** | **Descrizione** |
|---|---|
| AddAsset | Il cliente crea l'ordine sotto forma di asset inizializzandolo con le proprietà della transaction. |
| AutorizzazioneFarmacista | Il cliente richiede il farmaci presenti nella ricetta elettronica identificata con il codice NRE e autorizza il farmacista a vedere l'ordine, a modificare il campo "stato" e aggiungere dati nei campi "importo" e "codiceAperturaLucchetto". |
| RichiestaPagamento | Il farmacista verifica di avere i farmaci e di poterli erogare al cliente. In caso affermativo, aggiunge nel campo "importo" la cifra da pagare e richiede il pagamento modificando il campo "stato". |
| ConfermaPagamento | Il cliente paga attraverso un sistema di pagamento e modifica il campo "stato". |
| Autorizzazione Fattorino | Il cliente inizializza il campo "fattorino", comunica qual è il farmacista autorizzato all'erogazione, autorizza il fattorino a vedere i campi "id", "cliente" e "farmacista" e a modificare i campo "stato". |
| RichiestaConsegna | Il farmacista verifica il pagamento e, nel caso in cui sia stato correttamente effettuato, modica il campo "stato", richiedendo così al fattorino di andare a ritirare i farmaci. |
| Erogazione | Il fattorino si reca presso la farmacia e comunica il proprio identificativo e quello dell'ordine. Il farmacista verifica che sia autorizzato consultando la Blockchain, ricava tutte le informazioni del cliente e dell'ordine attraverso la Blockchain e visualizza la ricetta attraverso il sistema delle ricette elettroniche. Con questi dati soddisfa l'ordine consegnando un pacco anonimo (ovvero che non permette di conoscere ciò che è al suo interno), contenente i farmaci al fattorino. Successivamente scrive nel campo "codiceAperturaLucchetto" un codice criptato per permettere al cliente di aprire il lucchetto intelligente. E infine segna come "erogato" lo stato dell'ordine. |
| Consegna | Il fattorino, dopo aver portato i farmaci a destinazione, modifica il campo "stato". |
| InfoParzialiOrdine | Il fattorino visualizza i campi "id", "cliente" e "farmacista" dell'ordine specificato. |
| StoricoTransazioniFattorino | Il fattorino visualizza le transaction che ha eseguito o in cui è coinvolto all'interno dello storico. |

**Tabella 6.3:** dettagli degli event.

| Event | Proprietà | Transaction |
|---|---|---|
| FarmacistaAutorizzato | idOrdine, idCliente, idFarmacista | AutorizzazioneFarmacista |
| PagamentoRichiesto | idOrdine, idCliente | RichiestaPagamento |
| PagamentoConfermato | idOrdine, idCliente | ConfermaPagamento |
| FattorinoAutorizzato | idOrdine, idCliente, idFattorino, idFarmacista | AutorizzazioneFattorino |
| ConsegnaRichiesta | idOrdine, idCliente | RichiestaConsegna |
| OrdineErogato | idOrdine, idCliente, idFattorino | Erogazione |
| OrdineConsegnato | idOrdine, idCliente | Consegna |
| InfoParzialiOrdineLette | idOrdine, idCliente, idFarmacista | InfoParzialiOrdine |

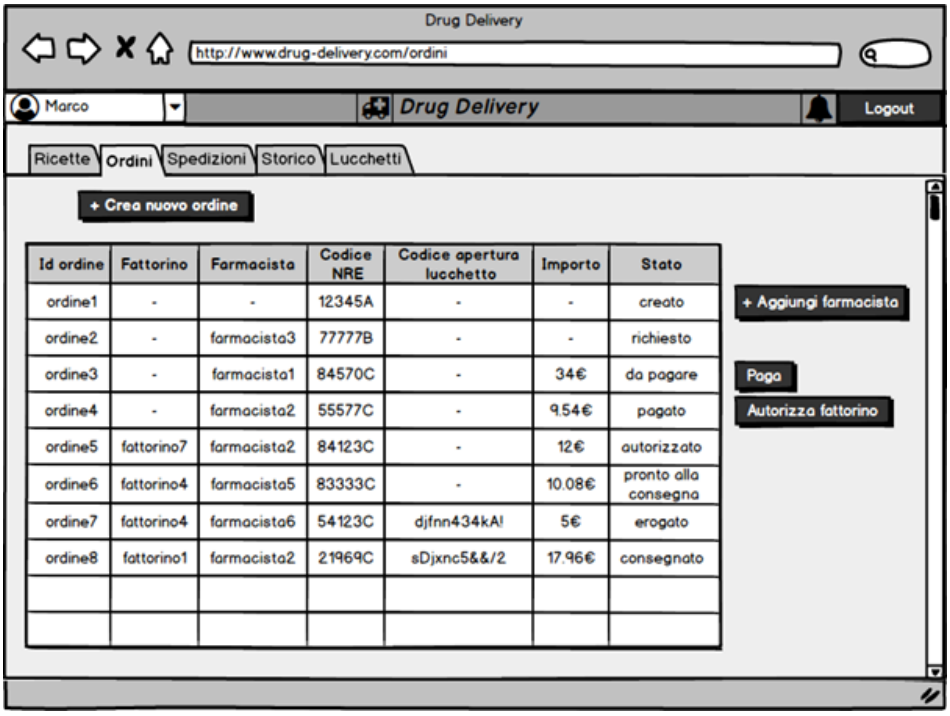



**Figura 6.11:** pagina degli ordini di un cliente.

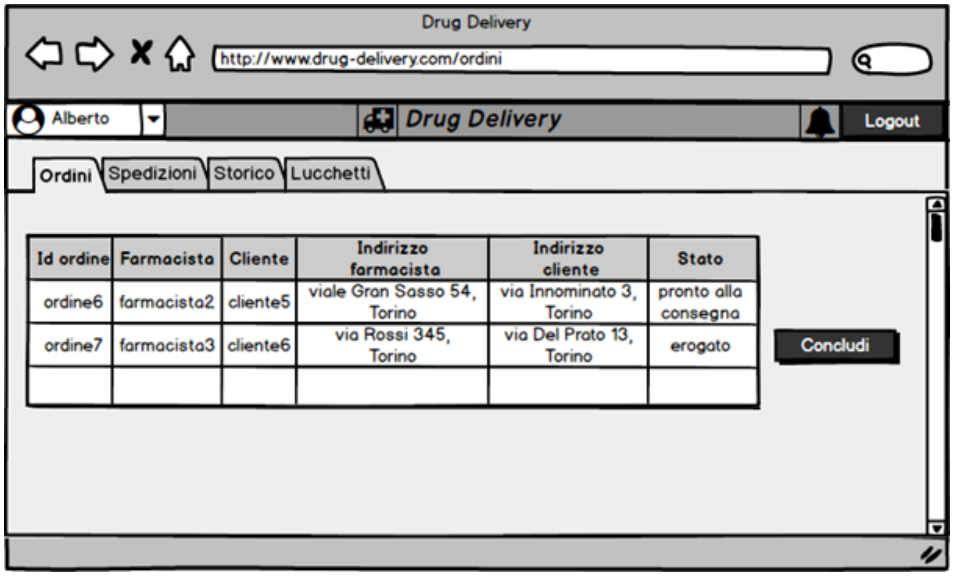



**Figura 6.12:** pagina degli ordini di un fattorino.

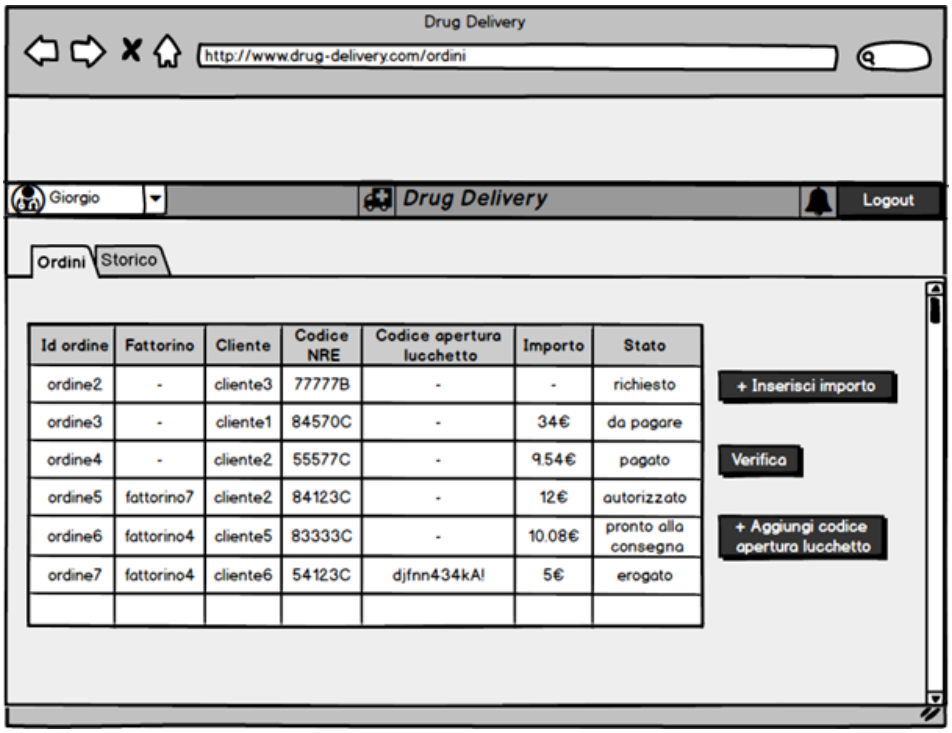



**Figura 6.13:** pagina degli ordini di un farmacista.

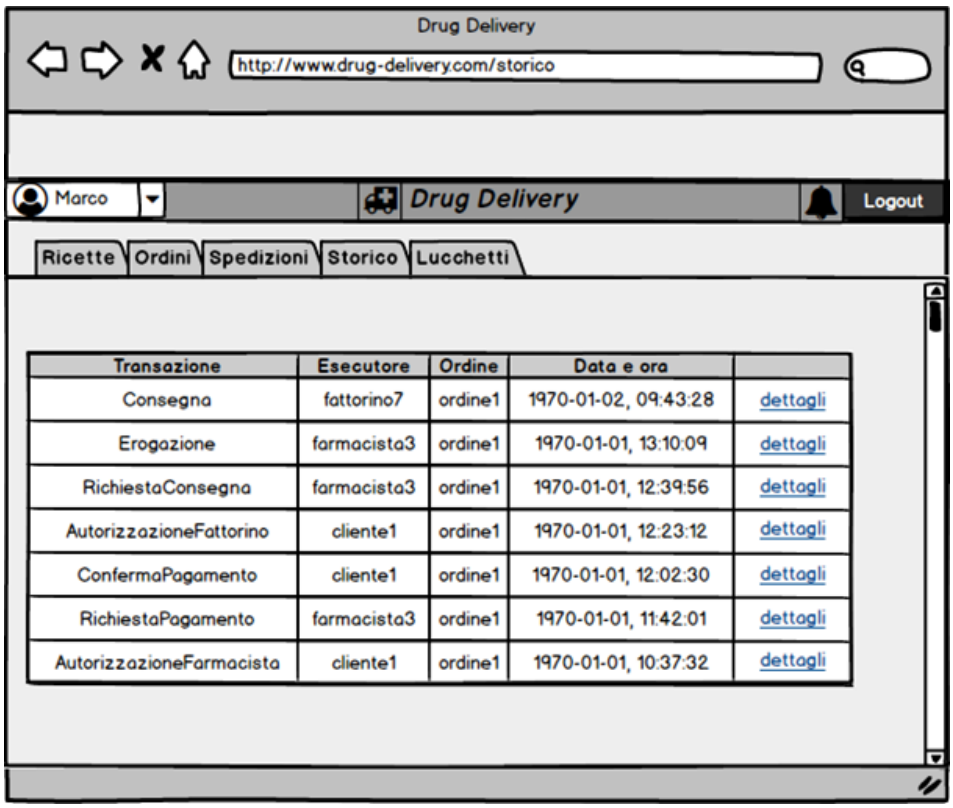



**Figura 6.14:** pagina dello storico di un cliente.

# Capitolo 7

# Conclusione e sviluppi futuri

In questa tesi è stato proposto un Proof of Concept incentrato sull'utilizzo della Blockchain Hyperledger Fabric per migliorare la consegna a domicilio di farmaci con ricetta. Per giungere a questa soluzione è stata studiata la letteratura riguardante l'applicazione della tecnologia Blockchain all'ambito sanitario, cercando dei casi d'uso non ancora affrontati che potessero beneficiarne. Dopo aver trovato il caso d'uso sopra riportato, è stato realizzato un sistema costituito da un server Fabric (su cui è stata caricata la logica delle transazioni e le definizioni dell'asset, dei partecipanti alla rete, delle transazioni, delle regole di accesso, degli eventi e delle query), dalle Web App e da un server REST che si interfaccia con il server Fabric e con le Web App; l'interfaccia con i sistemi esterni (delle ricette elettroniche e di pagamento) e con i lucchetti intelligenti è stata trascurata, perché non strettamente inerente all'ambito della tesi e, quindi, di secondaria importanza. È stata implementata con la piattaforma Angular una versione generica delle Web App degli utenti, mentre per testare le funzionalità specifiche per ogni tipologia di utente (clienti, fattorini e farmacisti) sono state utilizzate le Web App Hyperledger Playground, poiché l'alternativa, ovvero la loro implementazione con Angular, ha presentato problemi risolvibili sono aumentando notevolmente la complessità del sistema e i tempi di realizzazione e testing [70]. Inoltre, il modello della Business Network è stato semplificato riducendo le informazioni da salvare nella Blockchain. Per quello che riguarda invece le regole di accesso, nucleo fondamentale del sistema insieme alla logica delle transazioni, esse sono state scritte e testate accuratamente (eseguendo diversi test in scenari differenti) con un livello di granularità pari alla singola operazione CRUD (Create, Read, Update, Delete) e al singolo campo degli asset (andando oltre all'utilizzo standard del framework Composer privatizzando i dati all'interno degli asset e non solo gli asset per intero) [71].

Come si è detto, il sistema è stato ridotto rispetto a quanto progettato. Anche il modello della Business Network è stato semplificato; ad esempio, è stata tolta la figura del fornitore di farmaci, perché interagirebbe col sistema nella stessa maniera di un farmacista. Come si può vedere in figura 7.1, le maggiori differenze del modello

completo rispetto a quello ridotto sono, appunto, la presenza del fornitore tra i participant, la classe astratta "Utente", i concept e il numero maggiore di proprietà dell'asset "Ordine".

Riassumendo i vantaggi che porterebbe in teoria il sistema qualora fosse adottato:

- **Blockchain**: garantirebbe la privacy, preverrebbe truffe, furti o manomissioni dei prodotti trasportati. Hyperledger Fabric, in particolare, essendo una Blockchain privata e permissioned, permetterebbe di identificare i participant (usando i certificati) e di definire quali siano le azioni possono compiere e su quali risorse. Inoltre, le transazioni verrebbero tracciate, i dati sarebbero al sicuro da modifiche errate, certe operazioni potrebbero essere automatizzate dagli smart contract e tutto questo senza la necessità di terze parti fidate perché le informazioni sarebbero distribuite e ridondanti e il controllo della correttezza delle transazioni sarebbe decentralizzato. Infine un altro vantaggio sarebbe la scalabilità del sistema favorita dalle ridotte dimensioni degli asset (i dati relativi agli ordini, come il codice NRE). I benefici elencati porterebbero ad un aumento della fiducia dei clienti nelle consegne a domicilio di farmaci con ricetta e nei fattorini, oltre che ad un aumento dell'efficienza e della sicurezza.
- **Consegna a domicilio di farmaci**: assicurerebbe al cliente un risparmio in termini di tempo e denaro, eviterebbe la preoccupazione del parcheggio, favorebbe una diminuzione del traffico e inquinamento, ridurrebbe le code in farmacia e lo stress. Aiuterebbe, infine, le persone impossibilitate a muoversi a rifornirsi dei medicinali.
- **Ricette e cartelle elettroniche**: avere un database esterno al sistema in cui sono presenti le ricette in formato digitale eviterebbe ai fattorini di dover andare a casa dei clienti a ritirare la ricetta cartacea (risparmiando così tempo, fatica e soldi), aumenterebbe la fiducia nel servizio da parte dei malati, perché non dovrebbero più fornire la ricetta cartacea ai corrieri (con il rischio di perderla o con timori per la privacy) e permetterebbe la centralizzazione dei dati, un risparmio di carta, tempo e burocrazia, un miglioramento nel monitoraggio della spesa e delle prescrizioni in tempo reale, una verifica accurata dell'appropriatezza delle prescrizioni, dei percorsi terapeutici e della correttezza dei dati anagrafici dell'assistito, senza contare lo snellimento delle code in farmacia e dal dottore.
- **Lucchetto intelligente**: garantirebbe che il fattorino (o qualsiasi altra persona potenzialmente malintenzionata) non apra il pacco nel tragitto tra la farmacia e la destinazione della consegna.

Riguardo allo studio effettuato sulla tecnologia Blockchain, è indubbio che teoricamente possa sembrare un rimedio universale, ma nella pratica mostra diverse

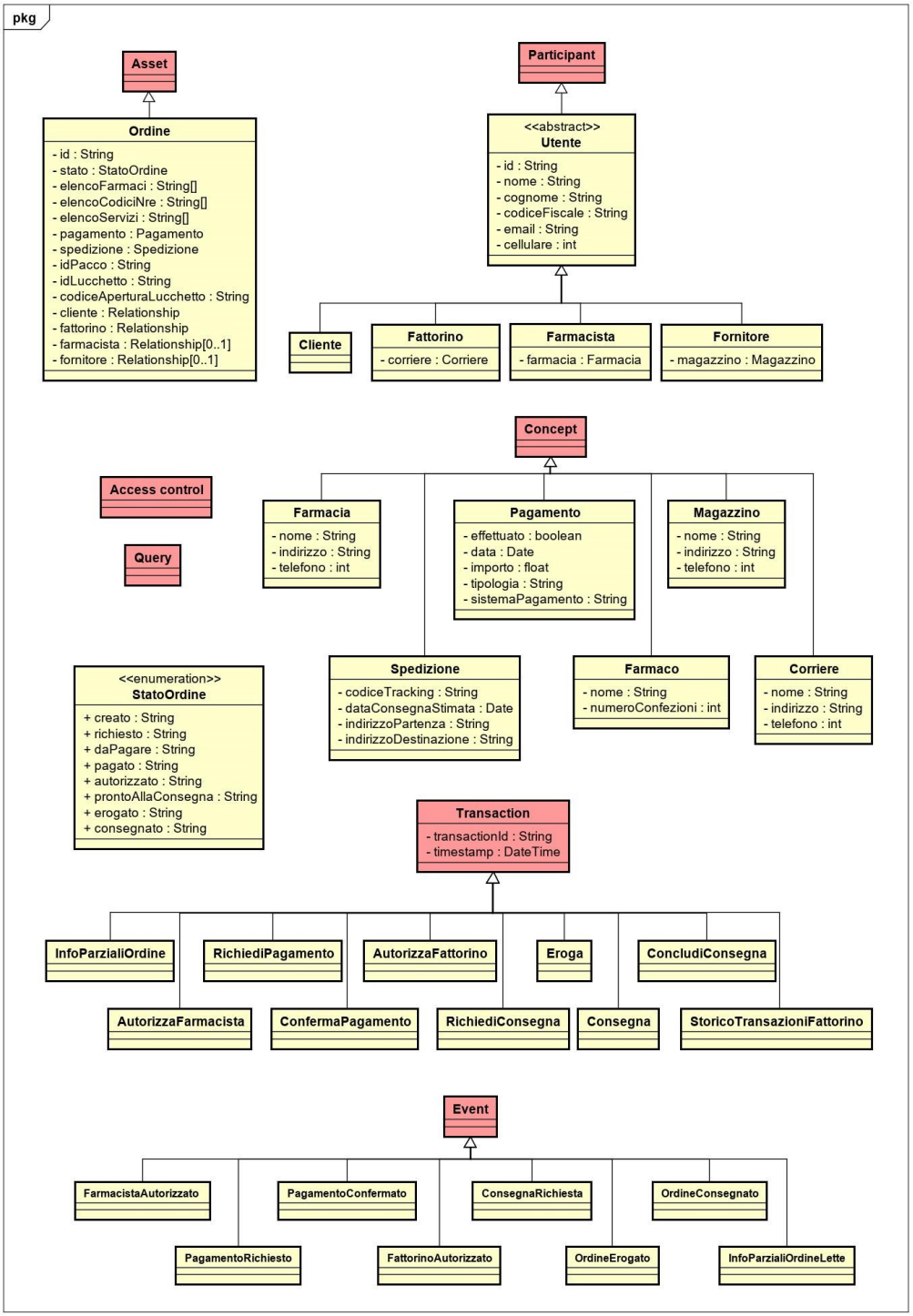



**Figura 7.1:** diagramma di classe completo del modello di Business Network.

criticità, come riportato di seguito [72]. Qualora, ad esempio, venissero compiuti degli errori nella progettazione o nell'implementazione, una Blockchain potrebbe avere difficoltà a scalare con l'aumento dei nodi o delle dimensioni dei dati (se ogni peer ha una copia del ledger e se i dati inseriti nel ledger sono voluminosi il sistema rischia di saturarsi), potrebbe essere vulnerabile ad attacchi informatici, potrebbe essere, paradossalmente, poco trasparente. Se il 51%, o più, dei nodi della rete venisse controllato da una cerchia ristretta di entità, essa potrebbe modificare in modo fraudolento una transazione. In alcuni casi il mining potrebbe risultare troppo lento o dispendioso in termini di risorse per l'uso ipotizzato [73]. E ancora, esiste il rischio che vengano inavvertitamente inseriti dei bug negli smart contract oppure che i singoli nodi possano essere pregiudicati (anche se un piccolo numero di nodi non può far prendere una decisione errata alla rete). Restano i problemi legati agli utenti e al social engineering (corruzione, impersonificazione, contraffazione, phishing, pharming, ricatti, ecc.), gli attacchi DDoS, le vulnerabilità criptografiche, solo per citare alcuni degli innumerevoli possibili punti deboli della Blockchain [74]. Allargando il discorso all'economia e alla finanza (che sono ancora il settore principale di applicazione di questa tecnologia), la storia di Bitcoin e le criptovalute è lastricata di bolle finanziarie e speculazioni (ad esempio, a fine 2018 Bitcoin è crollato dell'ottanta percento dai massimi [75]). Osservando invece l'ambito sanitario, si nota che, oltre alle problematiche già esposte, vi sia la necessità da parte delle applicazioni di soddisfare delle precise richieste che non possono essere ancora gestite dalla Blockchain [76].

Concludendo, eventuali sviluppi futuri sono legati al completamento del Proof of Concept secondo progetto e all'aggiunta di funzionalità secondarie (ad esempio le notifiche e la visualizzazione tramite app delle ricette elettroniche). Ciò si dovrebbe tradurre nello sviluppo e nel test delle interfacce con i sistemi esterni e con i lucchetti intelligenti e di Web App Angular specifiche per ogni tipologia di utente, oltre che nell'aggiunta di un server REST in più (per permettere il corretto funzionamento del sistema in presenza di diversi utenti). Infatti, Hyperledger Fabric richiede che ogni transazione inviatele sia firmata, per sapere chi sia il mittente e, quindi, decidere se autorizzarla. Ma di default è il server REST che firma con il suo certificato, perciò la Fabric vede sempre la stessa firma. Pertanto sono necessari due server REST, uno in modalità single-user (per creare i participant e le identità quando gli utenti accedono al sistema), e un altro in modalità multi-user (per permettere l'autenticazione delle applicazioni client sul server, cosicché possa distinguerle e firmare le transazioni con i loro certificati) [70]. È da sottolineare che questo problema si pone solamente nel caso in cui si utilizzino le Web App realizzate con Angular, mentre per la Web App Playground la questione è già stata risolta dagli sviluppatori. Infine, altri sviluppi futuri potrebbero essere la ricerca di lucchetti intelligenti già presenti sul mercato e l'utilizzo della soluzione proposta in un caso reale (come può essere la startup Pharmercure, nata in Piemonte e attualmente presente in alcune città del nord e centro Italia, che si occupa appunto di consegnare a domicilio i farmaci, ma priva

di un sistema basato su Blockchain).

# Bibliografia


[1] Consoft, da `https://www.consoft.it`, 2019

[2] Krawiec R., Housman D., White M., Filipova M., Quarre F., Barr D., Nesbitt A., Fedosova K., Killmeyer J., Israel A., Tsai L., *"Blockchain: Opportunities for Health Care"*, da `hpps://www.deloitte.com`, 2018

[3] Nakamoto S., *"Bitcoin: A peer-to-peer electronic cash system"*, da `https://www.bitcoin.org/bitcoin.pdf`, 31 ottobre 2008

[4] Berkeley J., *"The promise of the Blockchain: The trust machine"*, da `https://www.economist.com`, 31 ottobre 2015

[5] Ainsworth R.T., Alwohaibi M., *"The First Real-Time Blockchain VAT. GCC Solves MTIC Fraud"*, in Boston University School of Law, Law & Economics, Paper No. 17-23, da `https://www.dx.doi.org/10.2139/ssrn.3007753`, 24 luglio 2017

[6] Lessig L., *"Code is Law: On Liberty in Cyberspace"*, in Harvard Magazine, da `https://www.harvardmagazine.com/2000/01/code-is-law-html`, 1 gennaio 2000

[7] Ainsworth R.T., Alwohaibi M., *"Blockchain, Bitcoin, and VAT in the GCC: The Missing Trader Example"*, in Boston University School of Law, Law & Economics, Paper No. 17-05, da `https://www.dx.doi.org/10.2139/ssrn.2919056`, 16 febbraio 2017

[8] Bellini M., *"Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia"*, da `https://www.Blockchain4innovation.it`, 26 settembre 2019

[9] Gatteschi V., Lamberti F., Demartini C., Pranteda C., Santamaría V., *"To Blockchain or Not to Blockchain: That is the Question."*, IT Professional 20(2): 62-74, da `https://www.doi.org/10.1109/MITP.2018.021921652`, 16 aprile 2018

[10] PwC, *"How Blockchain works (infographic)"*, da `https://www.usblogs.pwc.com`, 28 agosto 2018

[11] Hammerschmidt C., *"Consensus in Blockchain Systems. In Short."*, da `https://www.medium.com`, 27 gennaio 2017

[12] Hackernoon, *"Different Blockchain Consensus Mechanisms"*, da `https://www.hackernoon.com`, 10 novembre 2018

[13] Whittle B., *"What Is a Nonce? A No-Nonsense Dive into Proof of Work"*, da `https://www.coincentral.com`, 18 dicembre 2018

[14] Annamalai D., *"Blockchain – What is Permissioned vs Permissionless?"*, in Core Dump, da `https://www.bornonjuly4.me`, 10 gennaio 2017

[15] Thompson C., *"The difference between a Private, Public & Consortium Blockchain"*, da `https://www.Blockchaindailynews.com`, 26 ottobre 2016

[16] Hyperledger Fabric, da `https://www.hyperledger-fabric.readthedocs.io`, 2019

[17] Kynan R.,*"Understanding Hyperledger Fabric – Endorsing Transactions"*, da `https://www.medium.com`, 9 febbraio 2018

[18] Valenta M., Sandner P., *"Comparison of Ethereum, Hyperledger Fabric and Corda"*, da `https://www.medium.com`, 25 giugno 2017

[19] Tam K., *"Demo of Multi-Channel Network in Hyperledger Fabric"*, da `https://www.medium.com`, 11 dicembre 2018

[20] Hyperledger Composer, da `https://www.hyperledger.github.io`, 2018

[21] Campbell R., *"Banking the Unbanked: Mapping the Biggest Blockchain Projects in the Devel-oping World"*, da `https://www.blockexplorer.com`, 19 gennaio 2019

[22] BitPesa, da `https://www.bitpesa.co`, 2019

[23] Nebeus, da `https://www.nebeus.com`, 2019

[24] IBM, *"Carrefour and Nestlé Partner with IBM to Extend Use of Blockchain to New Food Categories"*, da `https://www.ibm.com`, 15 aprile 2019

[25] Thomas Crown Art, *"Thomas Crown Art smART"*, da `https://www.thomascrown.art`, 2019

[26] MOBI, da `https://www.dlt.mobi`, 2019

[27] Yi H., *"Securing e-voting based on blockchain in P2P network"*, in EURASIP Journal on Wireless Communications and Networking, da `https://www.doi.org/10.1186/s13638-019-1473-6`, 28 maggio 2019

[28] Vangulick D., Cornélusse B., Ernst D., *"Blockchain for Peer-to-Peer Energy Exchanges: De-sign and Recommendations"*, in IEEE Xplore, da `https://www.doi.org/10.23919/PSCC.2018.8443042`, 30 agosto 2018

[29] Atzori M., *"Blockchain Technology and Decentralized Governance: Is the State Still Neces-sary?"*, da `http://www.dx.doi.org/10.2139/ssrn.2709713`, 1 dicembre 2015

[30] Gatteschi V., Lamberti F., Demartini C., Pranteda C., Santamaría V., *"Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?"*, Future Internet 10(2), da `https://www.doi.org/10.3390/fi10020020`, 20 febbraio 2018

[31] Lamberti F., Gatteschi V., Demartini C., Pelissier M., Gomez A., Santamaria V., *"Block-chains Can Work for Car Insurance: Using Smart Contracts and Sensors to Provide On-Demand Coverage."*, IEEE Consumer Electronics Magazine 7(4), da `https://www.doi.org/10.1109/MCE`, 2018.2816247, 15 giugno 2018

[32] Khezr S., Moniruzzaman M., Yassine A., Benlamri R., *"Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, in Applied Sciences"*, da `https://www.doi.org/10.3390/app9091736`, 26 aprile 2019

[33] Criptovalute, *"Blockchain: Cosa è, come funziona"*, da `https://www.criptovalute.io`, 2018

[34] Ivan D., *"Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records"*, da `https://www.healthit.gov`, agosto 2018

[35] Koo M., Linn L., *"Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research"*, da `https://www.healthit.gov`, 2018

[36] Greenspan G., *"Multichain"*, da `https://www.multichain.com`, 2015

[37] RecordsKeeper, da `https://www.recordskeeper.co`, 2018

[38] MedRec, da `https://www.medrec.media.mit.edu`, 2018

[39] Solve.Care, *"Platform for decentralization of healthcare and benefits administration"*, da `https://www.solve.care`, 5 gennaio 2018

[40] Solve.Care, *"A revolution in hearthcare, Healthcare that you can access, that is affordable and works for your family,"* da `https://www.solve.care`, 2018

[41] Invernizzi P., *"Wearable e IoT: pronti a rivoluzionare l'assistenza sanitaria"*, da `https://www.lumiexpo.it`, 20 luglio 2018

[42] CoMEHeRe, *"CoMEHeRe - Co-operative Models for Evidence-based Healthcare Redistribution"*, da `https://www.Blockchain.surrey.ac.uk`, 2019

[43] Franceschi M., Morelli D., Plans D., Brown A., Collomosse J., Coutts L., Ricci

L., *"ComeHere: Exploiting Ethereum for Secure Sharing of Health-Care Data"*, in Mencagli G. et al. (eds) Euro-Par 2018: Parallel Processing Workshops. Euro-Par 2018. Lecture Notes in Computer Science, vol 11339. Springer, Cham, `https://www.doi.org/10.1007/978-3-030-10549-5_46`, 31 dicembre 2018

[44] SciCoins, da `https://www.scicoins.com`, 2019

[45] Novartis, *"Gli studi clinici - Informazioni essenziali per una partecipazione consapevole"*, da *www.policlinicocampusbiomedico.it*, 2018

[46] Jelsma S., *"Consent, clinical trails and the Blockchain"*, da `https://www.hashedhealth.com`, 6 febbraio 2018

[47] Nowami S., *"Benchoufi/DocChain: DocChain release"*, da `https://www.zenodo.org`, 10 gennaio 2017

[48] Benchoufi M., Porcher R., Ravaud P., *"Blockchain protocols in clinical trials: Transparency and traceability of consent"*, [version 5; referees: 1 approved, 2 approved with reservations, 2 not approved], F1000Research 2018, 6:66, da `https://www.doi.org/10.12688/f1000research.10531.5`, 1 febbraio 2018

[49] ClinTex, *"ClinTex - Blockchain Powered Clinical Trial Management"*, da `https://www.clintex.io/`, 2018

[50] Hamacher A., *"Who's using Chainlink to connect smart contracts to the real world? The De-crypt canonical list"*, da `https://www.decrypt.co`, 6 maggio 2019

[51] Tseng J-H., Liao Y-C., Chong B., Liao S-W., *"Governance on the Drug Supply Chain via Gcoin Blockchain"*, International Journal of Environmental Research and Public Health, 2018; 15(6):1055, da `https://www.doi.org/10.3390/ijerph15061055`, maggio 2018

[52] Logica Efficiente, *"Filiera del farmaco"*, da `https://www.logisticaefficiente.it`, 19 ottobre 2017

[53] Biehl Z., *"VeChain Will Solve China's Drug and Vaccine Traceability Problems"*, da `https://www.investinBlockchain.com`, 9 agosto 2018

[54] Petre A., *"Blockchain Use Cases in Healthcare"*, da `www.ancapetre.com`, 3 febbraio 2017

[55] Buchko S., *"What is VeChain (VET)? | The Ultimate Guide"*, da `https://www.coincentral.com`, 5 novembre 2018

[56] VeChain, da `https://www.vechain.org`, maggio 2018

[57] Petre A., *"Blockchains and Pharmacies: a New Way of Leveraging Medication Adherence"*, da `www.ancapetre.com`, 18 ottobre 2017

[58] Jackson R., *"Blockchain Aims to Curb Prescription Drug Abuse"*, da `https://www.hackernoon.com`, 22 gennaio 2018

[59] Gatteschi V., Lamberti F., Paravati G., Sanna A., Demartini C., Lisanti A., Venezia G., *"New Frontiers of Delivery Services Using Drones: A Prototype System Exploiting a Quadcop-ter for Autonomous Drug Shipments"*, Proceedings - International Computer Software and Applications Conference, `https://www.doi.org/10.1109/COMPSAC.2015.52`, 24 settembre 2015

[60] Sanità Informazione, *"Ricetta bianca o rossa? Facciamo un po' di chiarezza"*, da `https://www.sanitainformazione.it`, 22 febbraio 2017

[61] Giancaspro L., *"Ti manca un farmaco e non hai la ricetta? Ecco cosa fare"*, da `https://www.pazienti.it`, 5 giugno 2018

[62] Tuttomed, *"La ricetta elettronica dematerializzata"*, da `https://www.tuttomed.it`, 26 maggio 2017

[63] Regione Piemonte, *"La ricetta medica elettronica"*, da `www.regione.piemonte.it`, 23 gennaio 2018

[64] Losito A., *"Cartella Clinica Elettronica: cos'è e come funziona costi e quali dati"*, da `https://www.guidafisco.it`, 5 novembre 2018

[65] Boxlock, da `https://www.getboxlock.com`, 2019

[66] Quotidiano Sanità, *"Social customer satisfaction delle farmacie italiane"*, da `www.quotidianosanita.it`, 17 settembre 2014

[67] Farexpress, *"Consegna farmaci a domicilio"*, da `www.farexpress.it`, 2019

[68] Pharmercure, da `https://www.pharmercure.it`, 2019

[69] Pillpack, da `https://www.pillpack.com`, 2019

[70] Church C., *"Developing multi-user application using the Hyperledger Composer REST Server"*, da `https://www.medium.com`, 27 febbraio 2018

[71] Umberhocker A., *"Implementing Data Privatization Within Hyperledger Composer"*, da `https://www.medium.com`, 6 agosto 2018

[72] Devibala A., *"A Survey on Security Issues in Iot for Blockchain Healthcare"*, 2019 IEEE Interna-tional Conference on Electrical, Computer and Communication Technologies (ICECCT), Co-imbatore, India, 1-7, da `https://www.doi.org/10.1109/ICECCT.2019.8869253`, 17 ottobre 2019

[73] Khezr S., Moniruzzaman M., Yassine A., Benlamri R., *"Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research"*, in Applied Sciences, da `https://www.doi.org/10.3390/app9091736`, 26 aprile 2019

[74] Valeri M.,*"Attacchi alla blockchain: cause, conseguenze e contromisure"*, da `https://www.cybersecurity360.it`, 1 marzo 2019

[75] Soldavini P., *"Bitcoin, la grande bolla è scoppiata: -30% in una settimana"*, -80% dai massimi, in Il Sole 24 Ore, da `https://www.ilsole24ore.com`, 24 novembre 2018

[76] McGhin T., Choo K.K.R., Liu C.Z., He D., *"Blockchain in healthcare applications: Research challenges and opportunities"*, in Journal of Network and Computer Applications, 135, 62–75, da `https://www.doi.org/10.1016/j.jnca.2019.02.027`, 1 giugno 2019