POLITECNICO DI TORINO

Corso di Laurea Magistrale in Ingegneria Gestionale
Percorso ICT e data analytics per il management
A.a. 2022/2023
Sessione di Laurea Ottobre 2023

Blockchain e tokenizzazione per la gestione dei processi aziendali

Relatore:
Prof. Danilo Bazzanella

Candidato:
Davide Borgatta

Relatore Aziendale:
Ing. Luca Simonini (Thales Alenia Space)

Sommario

L'obiettivo principale di questa tesi, svolta presso Thales Alenia Space, è quello di studiare l'utilizzo della Blockchain, una tecnologia che si basa su un registro immutabile e distribuito di transazioni ordinate nel tempo ed eseguite dai nodi di una rete. Tale studio è stato effettuato in un contesto aziendale per la gestione dei processi ingegneristici. Tramite la tecnologia Hyperledger viene proposto un Proof of Concept per una soluzione basata sulla gamification dei processi e la distribuzione di token per aiutare l'apprendimento di nuove metodologie. Attualmente si va incontro ad alcune problematiche, tra le quali vi è senza dubbio la messa in pratica delle metodologie E6 sviluppate dall'azienda, da numerosi colloqui con i vari dipendenti di Thales Alenia Space, è emerso che tale metodologia non è rispettata a pieno, ma viene messa in pratica solo in alcune delle sue parti. La difficoltà principale risiede nel fare capire le potenzialità a lungo termine di una sua applicazione costante unita alla difficoltà di introdurre una nuova routine di lavoro. La soluzione progettata utilizza quindi la tecnologia Blockchain di Hyperledger Fabric per registrare i vari passi della metodologia, in particolare quanto questi passi siano completi e svolti correttamente, grazie a tale registrazione unita all'uso di token creati e gestiti tramite Hyperledger FireFly è così possibile incentivare l'utilizzo della metodologia E6 andando a premiare i dipendenti tramite la remunerazione di token. Tale incentivo non viene utilizzato solo in modo tale che la metodologia venga usata nel breve termine, ma in particolare per far sì che chi la usa, riuscirà ad effettuare un cambio di mentalità e vedrà i suoi vantaggi anche nel lungo periodo, che quindi continuerà nel suo utilizzo senza il bisogno di un eventuale incentivo.

INDICE

Elenco delle tabelle

Elenco delle figure

Capitolo 1 - Introduzione

Lo scopo primario di questa tesi, svolta per Thales Alenia Space, è quello di studiare l'utilizzo della blockchain, una tecnologia decentralizzata che registra in modo sicuro e trasparente le transazioni digitali e i dati, come approfondito nel capitolo successivo. Tale studio è stato eseguito in ambito aziendale per rendere più interessante l'applicazione di nuove metodologie per il dipendente, favorendo l'efficientamento della società aiutando i richiesti cambiamenti nel modo di lavorare. L'obbiettivo è la realizzazione di un Proof of Concept di una soluzione, basata sulla distribuzione di token al raggiungimento di determinati obbiettivi.

Nell'era digitale in cui viviamo, l'innovazione tecnologica sta rivoluzionando il panorama aziendale in molti aspetti, in questo contesto in continua evoluzione, la blockchain si è affermata come una delle tecnologie più promettenti, in grado di ridefinire le modalità di gestione, condivisione e sicurezza dei dati. La blockchain, inizialmente nata per supportare la criptovaluta di Bitcoin, ha rapidamente guadagnato consenso in altri ambiti. La sua architettura decentralizzata, la crittografia avanzata e la capacità di garantire l'immutabilità dei dati hanno reso la blockchain una tecnologia adottabile per affrontare sfide complesse e processi aziendali critici.

Per la realizzazione del Proof of Concept si è scelto di utilizzare il framework di Hyperledger Fabric per creare la propria rete blockchain e di utilizzare il Supernodo Hyperledger FireFly per la gestione e la creazione di token, tali token sarebbero poi stati utilizzati come valore scambiato nella blockchain sopra citata. Si è scelto di approfondire tale argomento in quanto nell'attuale panorama aziendale, la tecnologia blockchain sta emergendo come una soluzione innovativa per affrontare diverse sfide legate alla gestione dei processi interni. Una delle applicazioni più interessanti della tecnologia blockchain in questo contesto è l'utilizzo dei token come forma di "gamification" per incentivare e premiare determinati comportamenti o obiettivi raggiunti. La "gamification" è un concetto che si riferisce all'applicazione di elementi e meccaniche tipiche dei giochi in contesti non ludici, al fine di coinvolgere e motivare le persone a raggiungere determinati obiettivi. Questa strategia si basa sulla psicologia umana, che dimostra come l'impiego di elementi come premi, punti, classifiche e

competizioni possa stimolare l'interesse, la partecipazione attiva e la fidelizzazione degli individui. La tecnologia blockchain offre un ambiente ideale per implementare una soluzione di "gamification" aziendale grazie alle sue caratteristiche chiave: trasparenza, sicurezza, immutabilità e decentralizzazione. I token, rappresentazioni digitali di valore su una blockchain, possono essere utilizzati per premiare e incentivare i partecipanti in modo trasparente e sicuro, garantendo la tracciabilità e la fiducia nelle ricompense assegnate.

Nel contesto aziendale, l'implementazione di un sistema basato su token può assumere diverse forme. Ad esempio, un'azienda potrebbe creare un programma di incentivazione interno in cui i dipendenti guadagnano token per il raggiungimento di obiettivi specifici, come il completamento di progetti, o il superamento di traguardi individuali o di squadra. I token potrebbero poi essere scambiati per premi tangibili o vantaggi aziendali, creando così un'esperienza coinvolgente e gratificante per i dipendenti. In questo capitolo introduttivo verrà prima presentata la società Thales Alenia Space, andando poi a presentare la metodologia utilizzata per la gestione dei progetti e le sue problematiche analizzate durante il corso di tale tesi. Infine, verrà proposto il Proof of Concept.

1.1 Presentazione Thales Alenia Space

Thales Alenia Space [1] è la società nata da Alcatel Alenia Space dopo che il gruppo francese Thales ha acquistato l'intera partecipazione della società francese Alcatel nelle due joint-venture con la holding Leonardo, un'azienda italiana di difesa e tecnologia [2]. Thales Alenia Space è una società leader nel settore aerospaziale e delle telecomunicazioni, specializzata nello sviluppo e nella produzione di soluzioni ad alta tecnologia per Telecomunicazioni, Navigazione, Osservazione della Terra, gestione ambientale, ricerca scientifica e infrastrutture orbitali [3].

Figura 1. Thales Alenia Space offre soluzioni per Telecomunicazioni, Navigazione, Osservazione della Terra, gestione ambientale, ricerca scientifica, esplorazione ed infrastrutture orbitali da Terra fino allo spazio profondo.
Con cortesia di Thales Alenia Space.

La società è riconosciuta a livello internazionale per la sua esperienza e le sue competenze nell'ingegneria spaziale, l'integrazione di sistemi, la progettazione di payload, la produzione di satelliti e la gestione delle missioni spaziali. Thales Alenia Space ha una presenza globale con sedi in Europa e Nord America, collabora attivamente con le principali agenzie spaziali, tra cui l'Agenzia Spaziale Europea (ESA), la NASA e altre organizzazioni spaziali internazionali. In totale è presente in dieci paesi, con diciassette siti in Europa e uno stabilimento negli Stati Uniti. L'azienda è impegnata nello sviluppo di soluzioni innovative che soddisfano le esigenze sempre crescenti del settore spaziale. Thales Alenia Space contribuisce in modo significativo alla crescita e allo sviluppo dell'industria spaziale, la società si distingue per l'attenzione alla qualità e all'affidabilità dei suoi prodotti e servizi, garantendo il massimo livello di sicurezza e prestazioni. Thales Alenia Space svolge un ruolo chiave nella realizzazione di missioni spaziali complesse e ambiziose, contribuendo alla comprensione del nostro pianeta, all'esplorazione del sistema solare e al miglioramento delle comunicazioni globali. Attraverso la sua expertise e la sua leadership nel settore, Thales Alenia Space continua a definire gli standard dell'innovazione spaziale, affrontando le sfide tecnologiche e affinando costantemente le sue capacità. La società

si impegna anche nella promozione della sostenibilità ambientale, perseguendo soluzioni e tecnologie che riducono l'impatto dell'industria spaziale sull'ambiente.

Figura 2. Mappa sedi Thales Alenia Space.
Con cortesia di Thales Alenia Space.

1.2 Introduzione metodologia E6 e problematiche

Questo progetto di tesi si pone l'obiettivo di portare su Blockchain la metodologia di "Lean engineering" denominata E6 (E per Engineering, 6 per i sei pilastri su cui si fonda la metodologia) [4], tale framework sviluppato in Thales Alenia Space si pone come scopo il monitoraggio delle attività e degli eventi "pull", come milestones, rilascio di documento o trade-off, aiutando a chiarire quali sono le priorità o le precedenze e quando attivare le competenze in modo opportuno. L'introduzione di E6 nello sviluppo dei progetti ha reso possibile tra le altre cose, un lavoro di squadra efficiente, con una visione chiara e condivisa dei flussi di lavoro, delle interazioni tra i vari attori, definendo chiaramente il chi, il quando, il cosa ed il perché delle diverse attività, partendo dall'elemento chiave delle decisioni di progetto. E6 lavora sull'aspetto visivo e condiviso del funzionamento fisico del progetto, rendendo rintracciabile le incertezze e le incognite, andando a colmare tempestivamente le lacune. Tale metodologia, introdotta a partire dal 2020, è applicata in maniera operativa su tutti i progetti più importanti. Come molte innovazioni, anche tale metodologia, è vista a primo impatto dalle persone

in modo diffidente, in quanto subentra una logica di bias di conferma, che porta a preferire quello che si è sempre fatto rispetto a qualcosa di nuovo e che non si comprende a pieno attualmente. Inizialmente, infatti, si potrebbe creare stress nel lavoro, sia dovuto al fatto che si sta imparando una metodologia nuova sia dovuto al fatto che ci sarebbe da svolgere più compiti e modificare le normali routine lavorative [35]. Questo svantaggio nel breve termine però è più che compensato da vantaggi a lungo termine, sia dal punto di vista globale, ovvero con una maggior efficienza del progetto, sia dal punto di vista individuale con una migliore gestione dell'agenda e una corretta tempistica di presa delle decisioni che causerebbe meno stress per le scadenze. Questo è stato dimostrato empiricamente da Thales Alenia Space, provando ad utilizzare la metodologia E6 in alcuni progetti ed analizzando i risultati ottenuti da tale applicazione, allo stesso modo si prevede che un'applicazione costante possa portane a benefici sempre maggiori [4].

Figura 3. E6 promuove una visione chiara e condivisa dei flussi di lavoro, dalle interazioni tra i vari attori attraverso elementi visivi sia fisici che virtuali.
Con cortesia di Thales Alenia Space

L'obiettivo principale è quello di far capire e attuare una metodologia nuova, avere uno strumento per aiutare a premiare il cambio di mentalità in quanto attualmente le persone non riescono a vedere i vantaggi perché essendo di lungo termine, si tende a concentrarsi di più sul presente. Il token dato come premio è una sorta di incentivo a seguire tale metodologia e deve essere visto in ottica di premio per la trasformazione digitale. La distribuzione di token ha la funzione di dare alle persone un incentivo a breve termine per imparare ad attuare tale trasformazione, una volta effettuato il cambio di mentalità tali procedure diventerebbero quotidiane per gli individui interessati che riuscirebbero quindi a riscontrare tutti i vantaggi che i precedenti bias non permettevano.

Il token può essere visto anche come uno strumento di valutazione, in quanto la ricompensa sotto forma di token è direttamente proporzionale al corretto eseguimento della metodologia E6. Questo strumento è utile in quanto spesso si verifica una carenza nella capacità delle persone di valutare sé stesse in modo oggettivo. Questa tendenza oscilla tra un atteggiamento eccessivamente positivo, in cui si crede che ciò che si fa sia sempre corretto, e un'autocritica debilitante, soprattutto evidente in coloro che potrebbero soffrire della cosiddetta "sindrome dell'impostore"[36-37]. Un esempio concreto di questa dinamica si è manifestato all'interno di Thales Alenia Space, dove è avvenuta una transizione significativa nell'approccio alle valutazioni. Inizialmente, l'azienda adottava l'autovalutazione dello stato di applicazione delle metodologie. Tuttavia, questa modalità ha mostrato alcune limitazioni, spesso caratterizzate da una prospettiva eccessivamente ottimistica. Nel tentativo di superare queste limitazioni e garantire una valutazione più accurata, è stato adottato un nuovo approccio chiamato "co-assessment". In questo nuovo sistema, gli assessment non vengono più condotti esclusivamente in modo autogestito, ma coinvolgono attivamente il personale dedicato alla qualità e agli audit. Questi professionisti eseguono le valutazioni con un occhio critico e imparziale, consentendo un'osservazione più obiettiva dello stato di applicazione delle metodologie all'interno dell'azienda. Tuttavia, va sottolineato che questa nuova modalità, pur promuovendo un livello superiore di obiettività nelle valutazioni, comporta una maggiore richiesta di tempo e risorse. Il processo di co-assessment richiede un impegno significativo da parte dell'azienda, poiché coinvolge

personale specializzato in valutazioni e audit. Questa scelta implica un bilanciamento tra l'obiettività delle valutazioni e la disponibilità di risorse aziendali.

In definitiva, il passaggio da un approccio di autovalutazione a un sistema di co-assessment rappresenta un tentativo di affrontare le sfide legate alla valutazione oggettiva delle prestazioni. In considerazione di questo scenario, un sistema di valutazione basato sulla ricompensa dei token, legato alla corretta esecuzione del lavoro, si profilerebbe come un prezioso strumento per promuovere una valutazione il più oggettiva possibile.

Figura 4. I pilastri di E6.
Con cortesia di Thales Alenia Space.

1.3 Proof Of Concept: Blockchain e tokenizzazione per la gestione dei processi aziendali

Sulla base dell'analisi effettuata durante lo svolgimento di tale tesi, è stato individuato come ambito di studio la tokenizzazione per la gestione dei processi aziendali. Attualmente senza la tecnologia blockchain non è possibile effettuare una distribuzione di token in base ai processi aziendali, questo per via delle ingenti risorse temporali necessarie a adempiere lo scopo.

Per risolvere tale problema è stato realizzato un Proof of Concept per validare la fattibilità tecnologica di un processo di automatizzazione della distribuzione di token al raggiungimento di determinati obbietti. La soluzione progettata si basa su due framework, Hyperledger Fabric e Hyperledger FireFly, il primo per la necessità di avere una blockchain privata e autorizzata, dove i partecipanti hanno una propria identità certificata e, quindi, i dati salvati nella rete sono sensibili. Solo chi ha determinate autorizzazioni può eventualmente leggere o condividere dati sulla blockchain, inoltre vi è la necessità di un sistema a multicanale dove anche la condivisione aziendale sia limitata a specifici utenti e progetti. Il secondo invece è stato scelto per una corretta e semplice gestione dei token.

Inizialmente viene fatta un'analisi sulla metodologia E6, in particolare sugli artefatti essenziali per una sua corretta esecuzione, andando poi a spiegare dal punto di vista teorico come fare per una transizione nella tecnologia blockchain. Viene mostrato quali sono gli attori coinvolti, come verificare che i passi della metodologia siano eseguiti correttamente e come ricompensare l'utente con la giusta quantità di token in base al lavoro svolto. Infine, viene mostrato dal punto di vista pratico, quali elementi sono necessari per la realizzazione della blockchain e quali valutazioni fare per una corretta implementazione del sistema di controllo della metodologia e distribuzione di token. L'obbiettivo di questa Proof of Concept è di dimostrare la fattibilità tecnologica tramite l'utilizzo della tecnologia blockchain, facendo emergere i vantaggi che tale soluzione garantirebbe in un contesto aziendale.

1.4 Struttura tesi

Nel primo capitolo della tesi, quello appena presentato, viene introdotto il contesto generale del lavoro di ricerca, fornendo una panoramica sull'azienda in cui è stata condotta la tesi e sulla Proof of Concept fatta.

Nel secondo capitolo, invece, viene fornita una dettagliata introduzione alla blockchain, fornendo una spiegazione sulle caratteristiche di questa tecnologia, presentando i

componenti principali dell'architettura ed analizzando la differenza tra blockchain pubbliche e private.

Il terzo capitolo, verte sulla presentazione della blockchain di Hyperledger Fabric seguita da un'analisi dei punti forza e delle sfide nell'adottare tale tecnologia, in particolare vengono forniti dettagli per spiegare il motivo dell'impiego di Hyperledger per l'implementazione di una blockchain aziendale. Infine, viene presentato Hyperledger FireFly, un framework per la gestione dei token.

Nel quarto capitolo viene presentato il Proof of Concept della tesi, in tale capitolo viene presentata nel dettaglio la metodologia E6, i suoi artefatti e come fare, dal punto di vista teorico, per tradurre questa pratica nel contesto tecnologico della blockchain.

Nel quinto capitolo viene fornita una spiegazione sulla realizzazione dei concetti analizzati nel capitolo precedente, fornendo un'analisi sugli elementi necessari per una corretta implementazione della blockchain tramite Hyperledger Fabric.

Infine, nel sesto e ultimo capitolo vi è una breve conclusione dove vengono ripresi i concetti analizzati nella tesi e vengono fatte considerazioni su possibili sviluppi di tale studio.

Capitolo 2 - Tecnologia Blockchain

Questo capitolo verte sull'introdurre la tecnologia blockchain in modo teorico, descrivendone i concetti e gli aspetti più importanti. In tale capitolo vengono analizzati i concetti cardine che stanno alla base della creazione e all'utilizzo di tale metodologia, inoltre vengono presentati quelli che sono gli elementi essenziali per capire il funzionamento di una blockchain.

2.1 Blockchain

La blockchain, anche se è una invenzione degli anni '90 [5], si può dire che nasca nel 2008 con la pubblicazione di un documento dal titolo "Bitcoin: A Peer-to-Peer Electronic Cash System"[6] da parte di un autore che è voluto restare nell'anonimato ed ha utilizzato, quindi, lo pseudonimo di "Satoshi Nakamoto", tale documento descriveva i concetti fondamentali della blockchain come base per la creazione e la gestione di una valuta digitale chiamata Bitcoin. Questa è stata la prima volta che tale tecnologia venisse realmente applicata ed in particolare l'obbiettivo era quello di creare un registro immutabile e trasparente delle transazioni digitali, tutte le transazioni tramite blockchain vengono registrate in modo permanente e queste non possono essere modificate successivamente in modo retroattivo. Con tale metodologia si va ad eliminare la necessità di un'autorità centralizzata che verifichi e approvi le transazioni, consentendo agli utenti della rete di poter scambiare valore in modo diretto e sicuro. È proprio dal concetto di fiducia che nasce e si sviluppa la prima blockchain; infatti, il 2008 è un anno di grande sfiducia sia verso il sistema bancario sia verso chi ricopre i ruoli di controllo, mentre la blockchain, nata per contrapporsi a questo, garantisce la fiducia attraverso una struttura decentralizzata e basata sulla crittografia.

La decentralizzazione è un concetto cardine, in quanto, la blockchain opera su una rete di computer, detti anche nodi, distribuiti globalmente senza che ci sia un'autorità centrale che la controlli. Senza questa autorità di controllo centrale il consenso viene

distribuito creando fiducia negli utenti della blockchain, poiché richiede un accordo collettivo per validare le transizioni, tale consenso viene fatto con algoritmi progettati appositamente per garantire che la maggioranza dei partecipanti concordi sulla veridicità delle transazioni.

2.1.1 Elementi base

Di seguito vengono esposti gli elementi che insieme compongono e costituiscono uno schema della tecnologia blockchain, questi sono elementi comuni essenziali per tutte le blockchain [7-8]:

- Registro distribuito: una blockchain è costituita da un registro distribuito, anche chiamato ledger, che rappresenta l'intero storico delle transazioni avvenute sulla rete. Questo registro è condiviso tra tutti i partecipanti della blockchain e viene mantenuto in modo decentralizzato attraverso la collaborazione di nodi o computer partecipanti alla rete.
- Nodo: un nodo è un computer o un dispositivo che fa parte della rete blockchain. I nodi sono responsabili di validare e verificare le transazioni, inoltre mantengono una copia completa del registro distribuito.
- Crittografia: la crittografia svolge un ruolo fondamentale nella sicurezza della blockchain. Le transazioni e i dati all'interno dei blocchi vengono crittografati mediante l'utilizzo di algoritmi, garantendo l'integrità e la riservatezza delle informazioni.
- Transazione: una transazione rappresenta un'operazione o uno scambio di dati che viene registrato sulla blockchain. Può includere informazioni come l'indirizzo del mittente, l'indirizzo del destinatario e la quantità di asset o valuta coinvolta.
- Blocco: le transazioni vengono raggruppate in blocchi, che rappresentano le unità di base della blockchain. Ogni blocco contiene un insieme di transazioni

valide e un riferimento al blocco precedente, formando una catena continua di blocchi.

- Hash: ogni blocco nella blockchain ha un hash univoco, che è formato da una stringa alfanumerica generata attraverso un algoritmo di hash crittografico. L'hash identifica il contenuto del blocco e viene utilizzato per collegare i blocchi in modo sequenziale, formando la catena, tale aspetto è importante in quanto rende immutabile la blockchain; infatti, un eventuale manomissione dei dati modificherebbe l'hash del blocco ad esso associati, andando a cambiare quindi i riferimenti della catena.
- Consenso: la blockchain utilizza meccanismi di consenso per garantire che tutti i partecipanti concordino sullo stato corrente del registro distribuito. Ciò significa che prima che un blocco venga aggiunto alla blockchain, deve essere verificato e accettato dalla maggioranza dei partecipanti, secondo le regole stabilite dal protocollo della blockchain.
- Timestamp: il timestamp, o marca temporale, è l'indicazione dell'orario in cui un blocco viene creato o una transazione viene confermata. Questo è importante per stabilire l'ordine cronologico delle transazioni e dei blocchi all'interno della blockchain.

2.1.2 Funzionamento blockchain

Una blockchain è un sistema innovativo che sta rivoluzionando il modo in cui le transazioni digitali vengono registrate, condivise e conservate in modo sicuro. Il punto cardine di tale tecnologia è il registro distribuito, che sostanzialmente è un libro mastro condiviso tra tutti i partecipanti della rete. Tale libro mastro digitale contiene tutte le transazioni che sono avvenute tra le diverse persone, esso non è controllato da un'autorità centrale, ma viene mantenuto in modo decentralizzato attraverso la partecipazione, nella rete, di numerosi nodi. Ogni nodo possiede una copia completa del libro mastro, che viene costantemente aggiornata e sincronizzata con gli altri partecipanti.

Quando una transazione viene eseguita sulla blockchain, questa transazione viene trasmessa a tutti i nodi della rete. I nodi lavorano insieme per verificare l'autenticità e la validità della transazione utilizzando complessi algoritmi crittografici. Una volta che la transazione è stata verificata, viene raggruppata con altre transazioni simili per formare un blocco. Ogni blocco contiene un insieme di transazioni valide, insieme a un riferimento all'hash del blocco precedente. Un hash ha un valore unico che viene generato attraverso una funzione crittografica. Questo riferimento all'hash del blocco precedente crea un collegamento tra i blocchi, formando una catena di blocchi immutabile [9].

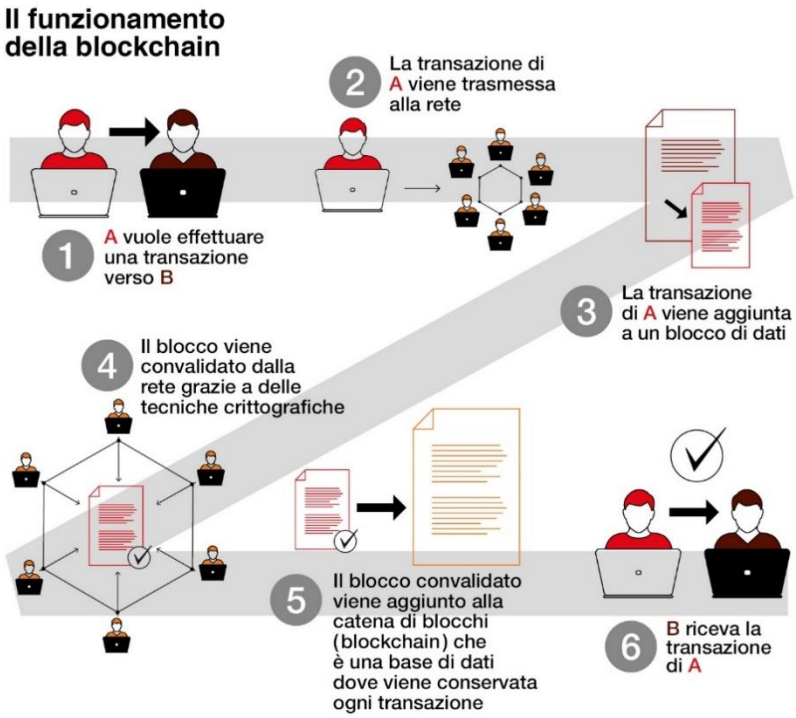

Figura 5. Funzionamento della blockchain [38].

Il processo di creazione di un nuovo blocco richiede anche il consenso della maggioranza dei nodi della rete. Questo processo di consenso può variare a seconda del tipo di blockchain, ma spesso coinvolge algoritmi di consenso come la prova del lavoro (Proof of Work) o la prova della partecipazione (Proof of Stake). Questi algoritmi garantiscono che solo i blocchi validi vengano aggiunti alla blockchain e che la rete sia sicura e resistente a manipolazioni o attacchi maligni. Una volta che un blocco è stato

aggiunto alla blockchain, diventa immutabile e resistente alla modifica. Ciò significa che le transazioni registrate sulla blockchain rimarranno permanenti e non possono essere cancellate o alterate in seguito. Questa caratteristica di immutabilità fornisce una maggiore sicurezza e fiducia nel sistema, consentendo a tutti i partecipanti di avere una visione accurata e affidabile delle transazioni passate. Grazie alla sua natura decentralizzata, trasparente e sicura, la blockchain offre un metodo innovativo per la registrazione e la convalida delle transazioni digitali, rimuovendo la necessità di intermediari centralizzati e migliorando l'efficienza e l'affidabilità dei processi aziendali.

2.1.3 Proprietà chiave

Di seguito vengono presentate quelle che sono ritenute le proprietà fondamentali di una tecnologia Blockchain [10]:

- Decentralizzazione: una delle principali caratteristiche della blockchain è la sua natura decentralizzata. Le informazioni e le decisioni sono condivise tra i partecipanti della rete, eliminando la necessità di un'autorità centrale o di un intermediario. La decentralizzazione favorisce la trasparenza, la resistenza alla censura e la riduzione dei punti di vulnerabilità.
- Trasparenza: la blockchain è intrinsecamente trasparente. Tutti i partecipanti della rete hanno accesso alle informazioni registrate sulla blockchain. Le transazioni e i dati sono visibili e verificabili da tutti i nodi nella rete, creando un alto livello di fiducia e rendendo difficile la manipolazione delle informazioni.
- Sicurezza: le blockchain utilizza algoritmi crittografici per garantire la sicurezza dei dati e delle transazioni. L'integrità dei blocchi è protetta attraverso l'hash crittografico, che collega i blocchi in modo sequenziale e rende difficoltoso alterare o manipolare i dati.
- Immutabilità: una volta che un blocco viene aggiunto alla blockchain, diventa immutabile, questo significa che le informazioni registrate sulla blockchain non possono essere cancellate o modificate in modo retroattivo. Ciò fornisce un alto grado di sicurezza e integrità ai dati registrati sulla blockchain.

- Resilienza e tolleranza ai guasti: grazie alla sua natura distribuita, una blockchain è resiliente ai guasti e ai punti singoli di fallimento. Se un nodo nella rete smette di funzionare o viene compromesso, gli altri nodi continuano a mantenere e convalidare le transazioni. Ciò rende le blockchain robuste e resistenti agli attacchi o alle interruzioni.
- Scalabilità: la scalabilità è una proprietà importante della blockchain. Poiché il numero di transazioni e partecipanti alla rete può aumentare notevolmente, è fondamentale che una blockchain sia progettata per gestire un elevato volume di transazioni in modo efficiente, senza compromettere la velocità e le prestazioni complessive.

2.2 Algoritmi di consenso

In un contesto in cui non esiste un'autorità centrale che verifichi e autorizzi le transizioni, ma le decisioni vengono prese in modo collettivo dagli utenti della rete, serve un meccanismo di consenso che stabilisca regole comuni per la validazione delle transazioni. Per rispondere a questa necessità nascono gli algoritmi di consenso che sono, quindi, un aspetto fondamentale della decentralizzazione delle reti blockchain. Tali algoritmi, infatti, consentono ai partecipanti di raggiungere un accordo sulla validità delle transazioni e sulla creazione di nuovi blocchi all'interno della blockchain. Essi sono progettati per garantire l'integrità, la sicurezza e la coerenza delle informazioni condivise sulla rete, consentendo ai partecipanti una collaborazione affidabile senza la presenza di un intermediario. Di seguito vengono presentati i principali algoritmi di consenso che vengono utilizzati in diverse blockchain [11-13]:

- Proof of Work (PoW): è l'algoritmo di consenso più conosciuto, in quanto implementato in numerose blockchain, tra cui le più famose sono Bitcoin ed Ethereum, anche se quest'ultima nel corso del 2022 attraverso il Merge è passata al PoS che viene presentato successivamente. Nell'algoritmo PoW i partecipanti della rete, chiamati "minatori" competono tra di loro per risolvere un problema crittografico detto di "hash puzzle", per dimostrare che hanno svolto un certo

lavoro computazionale. Il primo minatore che riesce a risolvere il problema diffonde in rete la soluzione, se gli altri nodi della rete validano la soluzione, riceve il diritto di aggiungere un nuovo blocco alla blockchain, insieme a una ricompensa. L'algoritmo PoW richiede un consumo significativo di energia e risorse computazionali, che garantisce un meccanismo di consenso robusto che rende difficile alterare le transazioni passate e richiede un enorme potere computazionale per attaccare la rete.

- Proof of Stake (PoS): tale algoritmo di consenso è alternativo al PoW e si basa sul possesso di un determinato token o criptovaluta della rete blockchain di cui si vuole partecipare. I partecipanti della rete non vengono più chiamati minatori, ma validatori e viene assegnato loro il diritto di creare un nuovo blocco in base alla quantità di token posseduti e messi in "staking", ovvero bloccati come garanzia. La scelta del validatore che avrà quindi la possibilità di aggiunge un nuovo blocco è fatta in modo casuale, ponderata sulla base dei token posseduti e bloccati. Dopo che è stato selezionato un validatore, esso avrà il compito di verificare le transazioni e creare una prova del blocco da propagare, gli altri validatori della rete verificheranno la validità di tale prova e in caso affermativo la rete ricompenserà il creatore del blocco. Il PoS richiede, quindi, un'allocazione significativa di risorse finanziarie per partecipare attivamente alla creazione dei blocchi. Esso però risolve alcune delle preoccupazioni ambientali e di efficienza energetica associata all'algoritmo PoW, in quanto è meno energivoro, inoltre favorisce i partecipanti che hanno un interesse finanziario a mantenere sicura e integra la rete.
- Delegated Proof of Stake (DPoS): l'algoritmo DPoS è una variante del PoS che introduce il concetto di delegazione ed è stato introdotto per affrontare alcune limitazioni dell'algoritmo tradizionale, come la scalabilità e l'efficienza delle transazioni. In un sistema DPoS, i partecipanti votano, in modo proporzionale alla quantità di token posseduti, per selezionare una serie limitata di nodi, noti come "delegati", che hanno il compito di confermare le transazioni e produrre nuovi blocchi. I delegati sono responsabili di garantire la sicurezza della rete e di prendere decisioni consensuali. Poiché solo un numero limitato di delegati è coinvolto nella produzione di blocchi, il processo decisionale e la conferma delle

transazioni possono essere più veloci rispetto ad altri algoritmi di consenso. Questo permette di gestire un maggior numero di transazioni al secondo e riduce i tempi di conferma. Tuttavia, è importante notare che l'algoritmo DPoS può introdurre un certo grado di centralizzazione in quanto la selezione dei delegati si basa sulla quantità di token posseduti. Ciò significa che i partecipanti con una maggiore quantità di token hanno un'influenza maggiore sulla rete.

- Byzantine Fault Tolerance (BFT): gli algoritmi di consenso BFT sono spesso utilizzati nelle reti blockchain permissioned, in cui i partecipanti sono noti e fidati, come ad esempio nelle blockchain utilizzate in contesti aziendali o governativi. Questo tipo di algoritmo offre un elevato livello di sicurezza e garanzie nella validazione delle transazioni anche in presenza di guasti o comportamenti malevoli. Alcuni esempi di algoritmi di consenso BFT includono Practical Byzantine Fault Tolerance (PBFT), Federated Byzantine Agreement (FBA) e Tendermint. In un sistema BFT, viene assunto che fino a un terzo dei nodi possa essere corrotto o non affidabile. Per raggiungere un consenso, l'algoritmo richiede che i nodi si scambino messaggi tra loro e raggiungano un accordo sulla decisione da prendere. L'algoritmo BFT è progettato per gestire i guasti di tipo "Byzantine" ed essere resiliente agli attacchi maligni o ai comportamenti disonesti dei nodi, garantisce che tutti i nodi onesti raggiungano un accordo corretto. Tuttavia, l'algoritmo BFT richiede una maggiore complessità e un maggior numero di scambi di messaggi rispetto all'algoritmo CFT, rendendolo meno efficiente in termini di tempo e risorse computazionali.
- Crash Fault Tolerance (CFT): l'algoritmo di consenso CFT è progettato per gestire i guasti di tipo "crash", in cui i nodi smettono di funzionare o diventano inaccessibili senza comportamenti malevoli. In un sistema CFT, si assume che la maggioranza dei nodi sia affidabile e funzionante correttamente. Di conseguenza, per raggiungere un consenso, è necessario che la maggioranza dei nodi accetti una determinata proposta o decisione. Questo approccio semplifica l'algoritmo di consenso, rendendolo più rapido ed efficiente. Tuttavia, l'algoritmo CFT non è in grado di affrontare i guasti di tipo "Byzantine", in cui i nodi possono comportarsi in modo arbitrario o malevole.

2.3 Tipi di blockchain

Esistono diversi tipi di blockchain che possono essere utilizzate in base alle esigenze specifiche di un'applicazione o di un'organizzazione. I tre tipi principali sono la blockchain pubblica, privata e di consorzio [12].

- Blockchain Pubblica: nella blockchain pubblica tutti possono partecipare, contribuire e accedere alle informazioni sulla rete. Funziona come un registro condiviso e aperto, accessibile a chiunque desideri verificare le transazioni e la cronologia dei dati. Ogni partecipante può unirsi alla rete e diventare un nodo, con la responsabilità di confermare le transazioni e mantenere la sicurezza della rete. L'aspetto più importante delle blockchain pubbliche è la loro trasparenza. Ogni transazione, ogni movimento e ogni modifica registrata sulla blockchain può essere verificata e tracciata. Questo rende le blockchain pubbliche ideali per applicazioni che richiedono un alto grado di fiducia, come le criptovalute o la gestione dei registri di proprietà. Bitcoin, è un esempio noto di blockchain pubblica, in cui chiunque può partecipare alla rete e verificare le transazioni.
- Blockchain Privata: la blockchain privata è una variante in cui l'accesso e la partecipazione alla rete sono limitati e controllati. A differenza delle blockchain pubbliche, in una blockchain privata solo un gruppo selezionato di entità può partecipare attivamente alla rete e avere accesso alle informazioni registrate. Questo tipo di blockchain viene spesso utilizzato all'interno di organizzazioni o aziende che desiderano sfruttare i vantaggi della tecnologia blockchain per migliorare i loro processi interni o affrontare sfide specifiche.

  Una delle principali ragioni per utilizzare una blockchain privata è garantire una maggiore privacy e riservatezza dei dati. Mentre le blockchain pubbliche sono trasparenti, le blockchain private offrono un livello di controllo più stretto sulla condivisione delle informazioni. Un'azienda può utilizzare una blockchain privata per gestire i flussi di lavoro interni, tracciare la provenienza dei prodotti o semplificare la collaborazione tra partner di fiducia. Hyperledger Fabric e Quorum sono esempi di blockchain private ampiamente utilizzate.
- Blockchain Consorzio: la blockchain di consorzio, o blockchain ibrida, è un compromesso tra le blockchain pubbliche e private. In una blockchain di

consorzio, una serie di entità o organizzazioni si uniscono per formare una rete blockchain con accesso limitato ai partecipanti approvati. Questa forma di blockchain consente una condivisione controllata delle informazioni tra i membri del consorzio, consentendo loro di collaborare e gestire processi comuni in modo efficiente.

Le blockchain di consorzio sono spesso utilizzate in settori in cui la collaborazione tra diverse entità è necessaria, come il settore bancario o la gestione delle catene di approvvigionamento. In una blockchain di consorzio, i partecipanti possono condividere informazioni critiche come la provenienza dei prodotti o le transazioni finanziarie, garantendo al contempo una certa privacy e controllo sulle informazioni condivise. Questo approccio consente una maggiore trasparenza rispetto alle blockchain private, mantenendo un certo grado di controllo tra i partecipanti.

Di seguito viene esposta una tabella riepilogativa degli aspetti chiave da considerare quando si confrontano tra di loro le blockchain private, pubbliche e di consorzio.

Tabella 1. Confronto tra tipi di blockchain

ASPETTO	**BLOCKCHAIN PUBBLICA**	**BLOCKCHAIN PRIVATA**	**BLOCKCHAIN DI CONSORZIO**
Controllo	Limitato	Alto	Moderato
Accesso	Pubblico	Ristretto	Selettivo
Scalabilità	Variabile	Buona	Buona
Velocità transazioni	Variabile	Elevata	Elevata
Sicurezza	Elevata	Elevata	Elevata
Decentralizzazione	Elevata	Bassa	Moderata
Consenso	PoW o PoS	Basato su autorizzazioni	Basato su autorizzazioni
Costi	Variabili	Elevati	Moderati
Privacy	Bassa	Elevata	Moderata
Esempi di utilizzo	Bitcoin, Ethereum	Reti aziendali, gestione supply chain private	Settori industriali specifici, reti tra aziende

Le rei blockchain si differenziano anche per il fatto di essere permissionless, senza autorizzazione, o permissioned, con autorizzazione.

Le reti Blockchain permissionless sono registri decentralizzati aperti a chiunque voglia pubblicare un blocco senza la necessità di avere permessi. La caratteristica distintiva delle reti permissionless è l'apertura e l'accesso libero alla rete per chiunque abbia una connessione internet. Tutti i partecipanti possono avere visibilità delle transazioni e delle operazioni sulla blockchain, rendendole completamente trasparenti.

Le reti permissioned invece sono blockchain in cui l'accesso e la partecipazione alla rete sono controllati e limitati solo a un gruppo selezionato di entità autorizzate. In una rete permissioned, l'autorizzazione e la gestione degli accessi sono determinate da regole e protocolli predefiniti. I partecipanti autorizzati possono essere tenuti a identificarsi, fornire credenziali o superare procedure di verifica prima di poter partecipare alla rete.

2.3.1 Esempi di blockchain

In tale paragrafo vengono presentate in forma tabellare le principali blockchain per fare sì di evidenziarne le differenze e favorire un confronto. Tali esempi tecnologici sono tra i più conosciuti ed utilizzati al mondo, tra questi vi è Bitcoin, Ethereum, Ripple, Hyperledger Fabric, Corda e Quorum [7,11-13,17,22].

Nell'analisi sono state prese in considerazione le due blockchain più conosciute, quella di Bitcoin ed Ethereum, entrambe sono pubbliche e decentralizzate, la prima è il pioniere nell'ambito di questa tecnologia mentre la seconda offre valore grazie ai suoi smart contract. Ripple invece è un esempio di blockchain pubblica con una visione di sviluppo più centralizzata, infine, le ultime tre blockchain presentate sono state progettate e sviluppate ad uso industriale e sono private.

In tale tabella vengono prima presentati quelli che sono comunemente ritenuti i punti di forza della tecnologia di analisi, poi è la volta delle debolezze ed infine vengono esposte le differenze tra le sei blockchain studiate.

Tabella 2. Confronto tra blockchain più diffuse.

Caratteristica	**BITCOIN**	**ETHEREUM**	**RIPPLE**	**HYPERLEDGER FABRIC**	**CORDA**	**QUORUM**
Punti di forza						
Sicurezza	Elevata sicurezza	Buona sicurezza	Sicuro	Elevata sicurezza	Buona sicurezza	Buona sicurezza
Decentralizzazione	Altamente decentralizzato	Decentralizzato	Parzialmente decentralizzato	Controllo decentralizzato	Controllo decentralizzato	Controllo decentralizzato
Smart Contracts	Limitate funzionalità	Ottimo	Limitate Funzionalità	Flessibile	Flessibile	Flessibile
Velocità transazioni	Moderate	Moderate	Rapide	Variabili	Variabili	Variabili
Privacy	Ottima	Limitata	Ottima	Elevata	Ottima	Ottima
Interoperabilità	Non inclusa	Limitata	Limitata	Elevata	Buona	Buona
Debolezze						
Scalabilità	Limitata	Scarsa	Scarsa	Limitata	Complessa	Limitata
Complessità	-	-	Complessità tecnica	Complessità tecnica	Complessità tecnica	Complessità tecnica
Centralizzazione	Bassa	Bassa	Limitata	Variabile	Variabile	Centralizzata
Costi transazioni	Variabili	Elevati/Variabili	Bassi	Variabili	Variabili	Variabili
Differenze						
Casi d'uso	Trasferimento valore	Contratti intelligenti	Pagamenti internazionali	Uso aziendale	Uso Aziendale	Uso aziendale
Tipo di rete	Pubblica	Pubblica	Pubblica	Privata	Privata	Privata
Algoritmo di consenso	Proof of Work	Proof of Stake	Consensus Ripple	Variabile	Variabile	Variabile
Ecosistema sviluppatori	Ampio	Ampio	Focalizzato	Aziendale	Aziendale	Aziendale
Regolamentazione	Minima	In evoluzione	Centralizzata	Orientato a regole	Orientato a regole	Orientato a regole

Nota: questa è un'analisi preliminare che verrà sviluppata adeguatamente nei capitoli successivi. In verde sono rappresentate quelle caratteristiche prese maggiormente in considerazione per la scelta di utilizzo della blockchain, in rosso, invece, sono quelle ritenute di scarso interesse per la scelta.

2.4 Smart Contact

Gli smart contract [14] rappresentano un aspetto fondamentale della tecnologia blockchain e offrono molte opportunità per l'automazione e l'esecuzione affidabile di accordi digitali. Sono programmi molto semplici memorizzati sulla rete e programmati per agire autonomamente al verificarsi di determinate condizioni. Gli smart contract eliminano la necessità di intermediari, consentendo ai partecipanti di stipulare e attuare direttamente un accordo utilizzando il codice informatico e la blockchain. Questi contratti intelligenti sono spesso scritti utilizzando il linguaggio di programmazione Solidity e vengono eseguiti sulla piattaforma Ethereum, sebbene siano supportati anche su altre blockchain. Una volta che le parti coinvolte nel contratto digitale hanno raggiunto un accordo e lo hanno codificato in uno smart contract, il contratto viene immutabilmente registrato sulla blockchain, diventando parte integrante del registro distribuito.

Gli smart contract sono diventati velocemente un elemento cruciale nella blockchain, una delle principali ragioni per cui sono così importanti risiede nella capacità di ridurre i costi operativi andando ad eliminare l'uso di intermediari. Inoltre, la loro caratteristica di automatizzare il processo di esecuzione degli accordi aumenta l'efficienza, andando a completare le transazioni in tempi molto più brevi dei metodi tradizionali, garantendo allo stesso tempo trasparenza e l'eliminazione dell'ambiguità.

Quando si parla di smart contract è di fondamentale importanza tenere in considerazione le sfide e le limitazioni di un loro uso. Una delle principali necessità è quella dello scrivere codice sicuro, un errore di codice di programmazione di un contratto incluso in una blockchain, porterebbe gravi conseguenze in quanto non modificabile per l'immutabilità della rete.

Gli esempi concreti di utilizzo degli smart contract nell'uso comune rappresentano una dimostrazione tangibile dell'ampio potenziale che questa tecnologia ha. Ecco alcuni modi di utilizzo [41]:

- Tokenizzazione di beni digitali e NFT (Non-Fungible Tokens): uno dei casi d'uso più noti degli smart contract è la tokenizzazione di beni digitali, spesso associata

agli NFT. Gli NFT sono unità uniche e indivisibili che rappresentano la proprietà digitale di oggetti come opere d'arte, musica, video, giochi e altro ancora. Gli smart contract vengono utilizzati per creare, vendere e trasferire questi token. Lo smart contract, in questo caso, eseguirà automaticamente il trasferimento della proprietà appena l'opera viene acquistata, eliminando la necessità di intermediari.

- DeFi (Decentralized Finance): il settore DeFi è un esempio di come gli smart contract possano rivoluzionare il mondo finanziario. In DeFi, gli smart contract vengono utilizzati per creare piattaforme e protocolli decentralizzati per prestiti, scambi di criptovalute e guadagni passivi. Questi smart contract eliminano la necessità di intermediari finanziari e offrono un accesso più aperto e inclusivo ai servizi finanziari globali.
- Contratti d'assicurazione basati su eventi: gli smart contract vengono utilizzati anche nel settore assicurativo per automatizzare i processi di gestione delle polizze. Ad esempio, un contratto d'assicurazione basato su uno smart contract potrebbe pagare automaticamente un risarcimento in caso di evento specifico, come un incidente stradale o una catastrofe naturale, senza richiedere un intervento umano per valutare i danni o autorizzare il pagamento.

Capitolo 3 - Hyperledger Fabric

In questo capitolo viene analizzata una specifica Blockchain, quella di Hyperledger Fabric, uno dei framework di Hyperledger, un consorzio di tecnologie blockchain ospitato dalla Linux Foundation. In seguito, vengono analizzati i motivi per cui si è scelto di adottare Hyperledger Fabric per la realizzazione della blockchain. In particolare, vengono esposti gli aspetti fondamentali e necessari per la realizzazione del Proof of Concept. Dopodiché segue un'analisi sugli aspetti negativi, che quindi richiederanno una ulteriore analisi e una validazione. Infine, viene presentato Hyperledger FireFly un progetto che viene utilizzato in tale tesi per permettere la creazione e la gestione di token.

3.1 Presentazione di Hyperledger Fabric

Hyperledger Fabric rappresenta un framework blockchain open-source progettato per consentire alle organizzazioni di costruire e gestire reti blockchain private, sicure e scalabili. Tale blockchain viene adattata per rispondere alle esigenze specifiche delle aziende e delle industrie, dove vi può essere una collaborazione trasparente, condividendo dati e processi in modo efficiente, senza dover fare affidamento su intermediari centralizzati.

Hyperledger Fabric offre un'infrastruttura flessibile e altamente configurabile che consente alle organizzazioni di creare reti blockchain adatte alle loro esigenze. Sviluppata dalla Linux Foundation è uno dei progetti principali del consorzio Hyperledger [15], un ecosistema che riunisce una comunità di aziende, sviluppatori e ricercatori con l'obiettivo di promuovere l'adozione e l'innovazione della tecnologia blockchain in ambito aziendale. Una delle principali caratteristiche di Hyperledger Fabric è il consentire la creazione di reti blockchain permissioned, in cui solo i partecipanti autorizzati possono accedere alle informazioni e partecipare al consenso.

Ciò consente alle organizzazioni di mantenere il controllo sulla privacy dei dati e di stabilire regole specifiche per l'accesso e la governance della rete.

Hyperledger Fabric consente, inoltre, la definizione di canali privati, che permettono a gruppi specifici di partecipanti di condividere informazioni e transazioni in modo selettivo. Ciò rende il framework ideale per scenari in cui diverse aziende devono collaborare in modo sicuro senza dover condividere tutte le informazioni con tutti i partecipanti della rete [16]. Hyperledger Fabric offre anche una serie di strumenti e componenti per semplificare lo sviluppo e la gestione delle reti blockchain. Include SDK (Software Development Kit) per sviluppatori, che facilita la creazione di smart contract e l'interazione con la rete, nonché strumenti per la gestione dell'identità, la sicurezza e il monitoraggio delle transazioni [11].

3.1.1 Nodi

In Hyperledger Fabric, i nodi sono le entità che partecipano alla rete blockchain e svolgono vari ruoli e hanno responsabilità diverse all'interno del sistema. Ci sono differenti tipi di nodi che lavorano insieme per consentire il funzionamento della rete. Ecco una panoramica dei principali tipi di nodi in Hyperledger Fabric [17-18]:

- Client: un nodo client rappresenta un’entità esterna alla rete, invia richieste di transazione agli endorser e trasmette le proposte di transazione al servizio di ordinazione. I nodi client comunicano con i nodi peer attraverso API o SDK.
- Peer: un nodo peer rappresenta la parte attiva della rete, che esegue il commit delle transazioni e mantiene lo stato e una copia del libro mastro. Un peer riceve aggiornamenti di stato ordinati sotto forma di blocchi dal servizio di ordinazione. I peer possono essere di Endorser che hanno il compito di approvare le transazioni, di Commiting che hanno il ruolo di confermare definitivamente le transazioni, di Membership che verificano l’appartenenza a una organizzazione, di Leader che è un ruolo di coordinamento che può essere

assegnato all'interno di un canale o di Anchor che hanno il ruolo di rappresentare un'organizzazione all'interno di un canale.

- Orderer: un nodo orderer è il componente preposto per la gestione dell'ordinazione e dell'ordine della sequenza delle transazioni nella rete. Gli orderer node garantiscono che le transazioni siano coerenti e distribuite in modo affidabile a tutti i nodi peer.

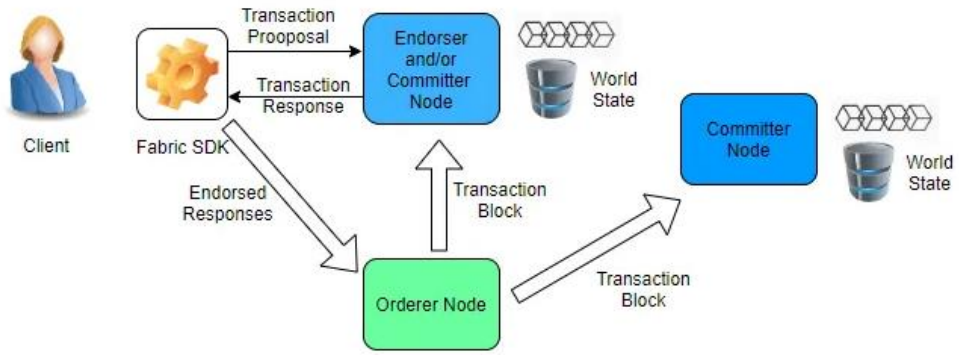

Figura 6. Rappresentazione del flusso di lavoro dei peer [18].

3.1.2 Canali

Nella rete Hyperledger Fabric, è possibile creare e utilizzare più canali per consentire la separazione e la gestione delle transazioni tra le diverse organizzazioni coinvolte. Ogni canale rappresenta una blockchain separata all'interno della rete e offre una visibilità limitata solo ai membri (peer) che fanno parte di quel canale specifico [17]. Utilizzando i canali, ciascuna organizzazione può partecipare alla rete globale senza che le transazioni siano visibili a tutti i partecipanti della rete. Solo i membri del canale specifico possono vedere e accedere alle transazioni create dai membri di quel canale. Ad esempio, come mostrato in figura, se ci sono tre organizzazioni coinvolte nella rete con due canali separati, le transazioni eseguite nel primo canale saranno visibili solo ai membri di quel canale, mentre le transazioni eseguite nel secondo canale saranno

visibili solo ai membri di quel secondo canale. Ciò garantisce una separazione e una privacy dei dati tra i canali. Un peer può essere connesso a più canali contemporaneamente. Questo consente al peer di partecipare a diverse blockchain all'interno della rete Hyperledger Fabric, eseguendo operazioni specifiche, quali la convalida delle transazioni, la sincronizzazione dello stato e l'esecuzione degli smart contract per ciascun canale [19].

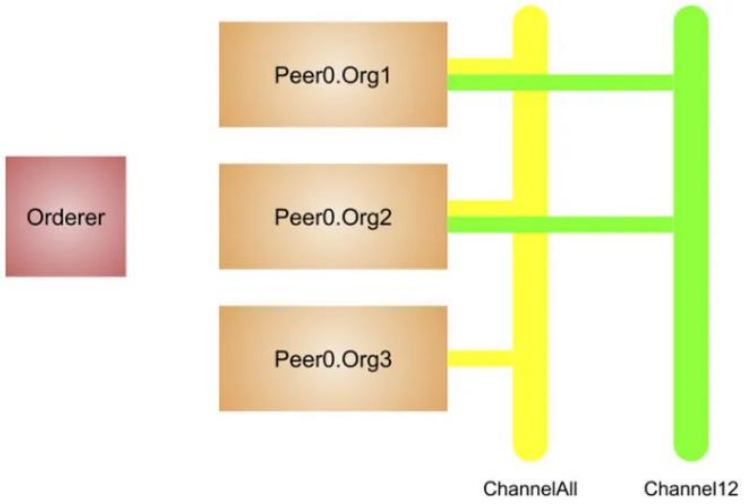

Figura 7. Esempio canali Hyperledger Fabric [20].

3.1.3 Libro mastro

Un libro mastro contiene lo stato attuale di un'azienda come giornale di registrazione delle transazioni. Sebbene i fatti sullo stato attuale di un oggetto aziendale possano cambiare, la storia dei fatti su di esso è immutabile, può essere aggiunta, ma non può essere modificata retrospettivamente.

In Hyperledger Fabric, un libro mastro è costituito da due parti distinte, sebbene correlate: un world state e una blockchain. In primo luogo, c'è un world state, un database che contiene i valori correnti di un insieme di stati contabili. Il world state rende facile per un programma accedere direttamente al valore corrente di uno stato

piuttosto che doverlo calcolare attraversando l'intero registro delle transazioni. Gli stati del libro mastro sono, per impostazione predefinita, espressi come coppie chiave-valore. Lo stato mondiale può cambiare frequentemente, poiché gli stati possono essere creati, aggiornati ed eliminati. In secondo luogo, c'è una blockchain, un registro delle transazioni che registra tutti i cambiamenti che hanno portato allo stato attuale del mondo. Le transazioni vengono raccolte all'interno di blocchi che vengono aggiunti alla blockchain, consentendo di comprendere la cronologia dei cambiamenti che hanno portato allo stato attuale del mondo. La struttura dati della blockchain è molto diversa dal world state perché una volta scritta non può essere modificata; è immutabile. La rete mantiene più copie di un libro mastro, che vengono mantenute coerenti con ogni altra copia attraverso un processo di consenso [18,21].

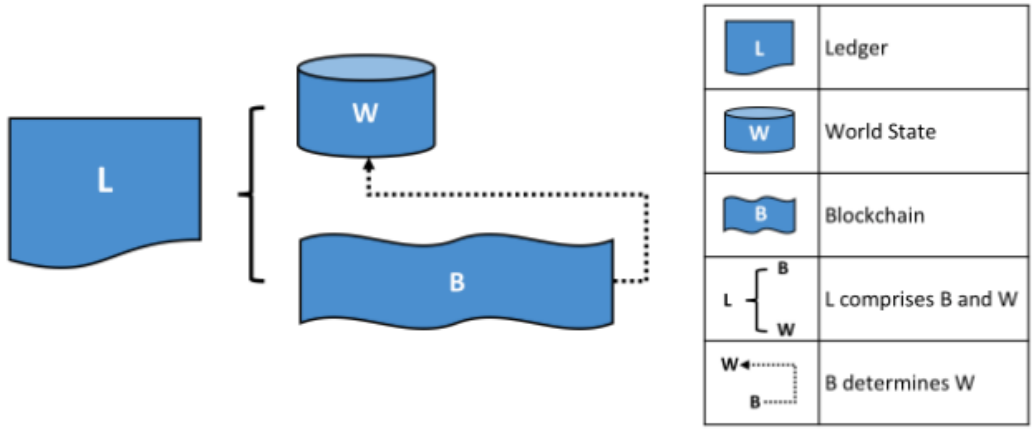

Figura 8. Libro mastro Hyperledger Fabric [21].

3.1.4 Blocchi

In Hyperledger Fabric un blocco si compone di tre sezioni [17-18,21-22]:

- Intestazione del blocco: che a sua volta comprende tre campi, il numero del blocco che indica un numero intero, 0 per il blocco genesi, e viene incrementato ad ogni blocco aggiunto. Hash del blocco corrente che indica l'hash di tutte le transazioni contenute nel blocco corrente. Hash del blocco precedente che indica

l'intestazione del blocco che lo precede. Questi campi assicurano che ogni singolo blocco sia indissolubilmente legato al suo vicino, portando a un libro mastro immutabile.

- Dati del blocco: che contiene un elenco di tutte le transazioni ordinate, viene scritto dal servizio di ordinazione quando il blocco viene creato.
- Metadati del blocco: che contiene il certificato e la firma del creatore del blocco, viene utilizzato per verificare il blocco dai nodi di rete.

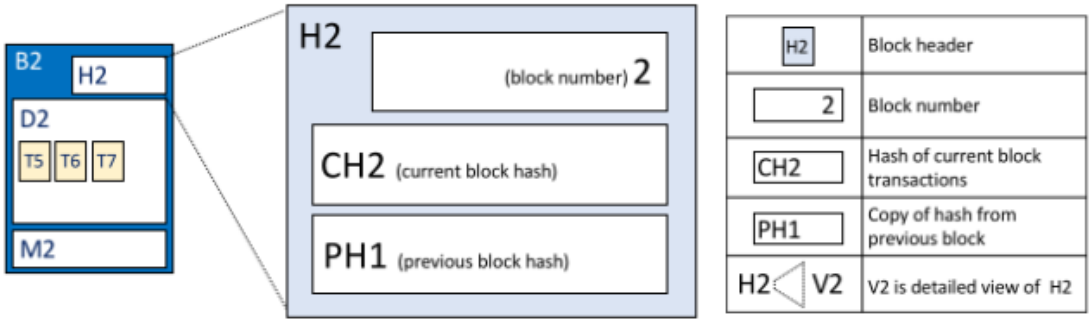

Figura 9. Composizione di un blocco [21].

3.1.5 Membership Service Provider

Il Membership Service Provider (MSP) è un componente fondamentale all'interno di Hyperledger Fabric che svolge un ruolo cruciale nella definizione delle regole e delle politiche di accesso alla rete blockchain. L'MSP si occupa della validazione, autenticazione e gestione delle identità che desiderano partecipare alla rete. Una delle principali responsabilità dell'MSP è gestire gli ID utente e garantire che solo le identità autorizzate abbiano accesso alla rete. Ciò significa che l'MSP autentica i clienti che cercano di unirsi alla rete, verificando la loro identità e fornendo loro le credenziali necessarie per proporre transazioni [18]. L'MSP fa affidamento sull'uso di certificati X.509 rilasciati da un'autorità di certificazione (CA), che funge da interfaccia collegabile per la verifica e la revoca dei certificati utente. L'autorità di certificazione è

responsabile di confermare l'identità degli utenti e di emettere certificati che attestano la loro autenticità. L'API Fabric-CA è l'interfaccia predefinita utilizzata da Hyperledger Fabric per l'MSP, ma le organizzazioni hanno la flessibilità di implementare un'autorità di certificazione esterna di loro scelta [19].

È importante sottolineare che una rete Hyperledger Fabric può essere controllata da più MSP, consentendo a diverse organizzazioni di gestire le proprie politiche di accesso e identità. In altre parole, ogni organizzazione coinvolta nella rete può portare il proprio provider di servizi di appartenenza preferito, che definisce le regole specifiche per gli utenti, i nodi peer e gli ordinatori all'interno di quella specifica organizzazione. Esistono due tipi principali di MSP all'interno di Hyperledger Fabric. Il primo è l'MSP locale, che definisce le identità degli utenti e dei nodi (peer e ordinatori) all'interno di un'organizzazione. Questo MSP stabilisce i diritti amministrativi e partecipativi a livello di organizzazione, specificando chi ha autorità per amministrare la rete e partecipare alle operazioni. Il secondo tipo di MSP è il Channel MSP, che si concentra sulla definizione dei diritti amministrativi e partecipativi a livello di canale. Ogni canale all'interno della rete può avere il suo Channel MSP, che determina le identità e i ruoli autorizzati a interagire e partecipare alle operazioni all'interno di quel canale specifico.

3.1.6 Consenso

Hyperledger Fabric, come framework di blockchain aziendale, offre un'architettura altamente modulare che consente la personalizzazione dei meccanismi di consenso. Gli algoritmi di consenso consentono ai partecipanti di raggiungere un accordo sullo stato dei record all'interno della rete blockchain. Hyperledger Fabric implementa diversi algoritmi di consenso [10,18]:

- SOLO: è il meccanismo di ordinamento Hyperledger Fabric più tipicamente utilizzato dagli sviluppatori che sperimentano le reti Hyperledger Fabric. SOLO coinvolge un singolo nodo di ordinazione.

- Kafka: basato sul protocollo CFT è un meccanismo di messaggistica di pubblicazione e sottoscrizione distribuita in grado di trasferire grandi quantità di dati di registro con una latenza significativamente bassa. La configurazione concettuale ad alto livello si basa sull'impostazione leader-follower, in cui le transazioni vengono replicate del leader eletto dai follower, se il leader si blocca viene sostituito da uno dei follower.
- Raft: è un protocollo CFT basato sul modello "leader-election". Stabilisce il consenso eleggendo un nodo principale per ottenere le voci in arrivo dal client e replicarle. Esistono tre fasi, Queste fasi sono l'elezione del leader, la replica del registro e la sicurezza. Il tempo in Raft procede in periodi di tempo arbitrari, chiamati "termini", con ciascun termine definito da un numero crescente. I nodi in Raft sono ordinati gerarchicamente in diversi stati, con ciascun nodo che può essere un leader, un seguace o un candidato. Il leader è l'entità principale del protocollo ed è eletto per canale con il compito di interagire con i client e quindi replicare le sue immissioni ai suoi follower sincronizzati. Raft ottiene la migliore sincronizzazione possibile inviando sistematici "battiti cardiaci" a suoi seguaci e se il leader va in crash, allora almeno uno dei suoi seguaci rileverà questa divergenza, darà un voto alla rete e tenterà di prendere il suo posto.
- Simplified Byzantine Fault Tolerance (SBFT): questo meccanismo di ordinamento è tollerante sia agli arresti anomali che ai guasti bizantini, il che significa che può raggiungere un accordo anche in presenza di nodi dannosi o difettosi. La comunità di Hyperledger Fabric attualmente non ha ancora implementato questo meccanismo, ma è sulla loro roadmap.

3.1.7 Chaincode

In Hyperledger Fabric gli smart contract prendono il nome di chaincode, essi sono un componente fondamentale all'interno della blockchain in quanto rappresentano il codice che definisce la logica aziendale e le regole di transazione all'interno di una rete. I chaincode sono scritti in linguaggi di programmazione come Go, JavaScript o Java e

vengono eseguiti all'interno di un ambiente isolato all'interno dei nodi peer di Hyperledger Fabric [11]. Ogni chaincode è associato a un canale specifico e può essere installato e attivato solo in quel canale.

I chaincode consentono alle organizzazioni di definire la logica delle transazioni e le regole di business all'interno di una rete Hyperledger Fabric. Essi definiscono le operazioni che possono essere eseguite, le condizioni per l'esecuzione di una transazione e la modifica dello stato del registro distribuito. Inoltre, i chaincode possono includere la validazione delle transazioni, l'applicazione di logiche personalizzate e l'interazione con altri componenti esterni.

Una delle caratteristiche fondamentali dei chaincode in Hyperledger Fabric è la loro flessibilità e modularità. I chaincode possono essere aggiornati in modo indipendente dal resto della rete, consentendo alle organizzazioni di apportare modifiche alla logica aziendale senza interrompere l'intera rete blockchain [16].

3.2 Introduzione punti di forza

Una delle caratteristiche distintive di Hyperledger Fabric è la sua architettura modulare e flessibile. Questa caratteristica è stata una delle principali motivazioni dietro la scelta di utilizzare questo framework per la soluzione proposta. L'architettura modulare di Hyperledger Fabric consente di personalizzare e adattare il sistema in base alle esigenze specifiche del caso d'uso. È possibile selezionare e configurare i componenti necessari, evitando di dover gestire funzionalità superflue. Questa flessibilità permette di creare una soluzione su misura che si integra perfettamente nei processi aziendali già in uso, ottimizzando l'efficienza e garantendo la massima rilevanza.

Un’altra priorità nella realizzazione della soluzione blockchain è la gestione della privacy e del controllo degli accessi. Hyperledger Fabric offre numerosi strumenti sofisticati per garantire la confidenzialità dei dati e il controllo degli accessi. La creazione di canali privati consente di stabilire sotto-reti isolate all'interno della rete principale, dove solo le parti autorizzate possono accedere e condividere informazioni

sensibili. Questo approccio consente di proteggere i dati aziendali più delicati, consentendo una collaborazione sicura e controllata tra le parti coinvolte.

Infine, la sicurezza è una preoccupazione fondamentale quando si tratta di implementare soluzioni blockchain all'interno dell'ambiente aziendale. Hyperledger Fabric eccelle in questo ambito offrendo meccanismi di sicurezza avanzati. L'utilizzo della crittografia asimmetrica per autenticare le transazioni e garantire l'integrità dei dati rappresenta è uno dei pilastri della sicurezza di Hyperledger Fabric. Inoltre, la possibilità di definire politiche di approvazione mediante l'Endorsement Policy assicura che solo le parti autorizzate possano confermare la validità delle transazioni, prevenendo così attacchi malevoli e garantendo la fiducia nelle operazioni. Nei prossimi paragrafi verrà esplorato in dettaglio ciascuno di questi aspetti mostrando come Hyperledger Fabric sia uno strumento all'avanguardia per la realizzazione di un sistema blockchain [26-27].

3.2.1 Architettura modulare e flessibile

Uno dei punti chiave della piattaforma di Hyperledger Fabric è senza alcun dubbio l'architettura modulare e flessibile, tale caratteristica permette di adattare la blockchain alle specifiche esigenze aziendali e offre una serie di vantaggi, tra cui [28-29]:

- Configurazione su misura: gli sviluppatori in Hyperledger Fabric hanno la possibilità di configurare la rete blockchain secondo le specifiche esigenze del proprio caso d'uso. In questo modo vi è una ottimizzazione della piattaforma, in quanto, si va ad includere e scegliere solo i componenti e le funzionalità necessarie allo sviluppo. Si può quindi decidere quali caratteristiche come il consenso, l'identità, la comunicazione e la memorizzazione dei dati andare a integrare oltre che scegliere quale tipologia specifica adottare. Inoltre, questi componenti possono essere sostituiti con altre soluzioni personalizzate per le proprie specifiche esigenze. Infine, permette una integrazione semplificata con sistemi aziendali già esistenti.

- Meccanismi di consenso: come già spiegato nel capitolo precedente, i meccanismi di consenso sono fondamentali nelle reti blockchain, in quanto determinano come le transazioni vengano validate e confermate dai partecipanti della rete. In Hyperledger Fabric vi è la possibilità di scegliere tra diversi algoritmi di consenso in base alla specifica esigenza, inoltre i vari meccanismi possono essere sostituiti o intercambiati tra di loro senza dover modificare la rete. In particolare, nella blockchain di Hyperledger Fabric vi è un consenso distribuito, il quale si verifica tra un sottoinsieme di nodi della rete chiamato "Endorsing Peers", in pratica quando una transazione viene proposta, viene per prima cosa inviata a questi nodi per esser poi eseguita e validata. Questi nodi emettono una firma digitale sulla transazione, che viene utilizzata nella fase successiva del consenso.
- Modelli di storage: in Hyperledger Fabric supporta diversi modelli di storage per la memorizzazione dei dati sulla blockchain, scegliendo tra database relazionali o NoSQL. I primi sono noti per la loro struttura tabellare e la capacità di gestire relazioni tra i dati, ottimi per dati strutturati e complessi. Il secondo tipo è adatto per la gestione di dati non strutturati offrendo, così, maggiore flessibilità nel modo in cui i dati vengono archiviati e organizzati. Hyperledger Fabric, essendo modulare, facilita la sostituzione o l'integrazione di un database a scelta senza dover riscrivere l'intera applicazione.
- Componenti aggiuntivi: grazie alla modularità di Hyperledger Fabric è possibile aggiungere nuovi componenti e funzionalità personalizzate, integrando facilmente strumenti e servizi esterni, come sistemi di autenticazione o componenti aggiuntivi per espandere la sicurezza nella gestione delle chiavi.
- Maggiore scalabilità: questo è possibile partizionando i dati tramite l'utilizzo di sotto-reti all'interno della rete principale, migliorando così le prestazioni complessive. Inoltre, grazie alla gestione dell'identità è possibile controllare gli accessi andando a limitare il numero di partecipanti alla rete, riducendo così il carico complessivo. Infine, attraverso il consenso distribuito che permette ai nodi partecipanti di convalidare e approvare le transazioni in modo parallelo, è possibile gestire in contemporanea un maggior numero di transazioni e migliorare, quindi, l'efficienza e la velocità complessiva della rete. A tale scopo

è utile la politica di approvazione di Endorsement Policy, tramite la quale si può ridurre il numero di partecipanti coinvolti nel processo di convalida delle transazioni, andando a semplificare il processo di consenso.

3.2.2 Privacy e controllo di accesso

Hyperledger Fabric offre un sistema di gestione degli accessi e delle autorizzazioni robusto. Questo tramite l'utilizzo di canali privati che è un meccanismo fondamentale per garantire la privacy e la confidenzialità dei dati. Tali canali privati altro non sono che una sotto-rete della rete principale in grado di consentire a un selezionato gruppo di partecipanti di accedere e condividere informazioni nel canale, permettendo di mantenere i dati delle transazioni private tra le parti coinvolte. Hyperledger Fabric utilizza, inoltre, un sistema di crittografia asimmetrica per la gestione delle identità e delle autorizzazioni. Ogni partecipante possiede una coppia di chiavi crittografiche, la chiave pubblica e quella privata, la prima, condivisa con gli altri partecipanti viene utilizzata per crittografare le transazioni e garantire l'autenticità dei dati. La seconda, invece è utilizzata per de crittografare le transazioni e fornire la firma digitale dell'utente, questa chiave viene mantenuta segreta dall'utente.

L'identità degli utenti della rete, invece, è gestita attraverso i certificati X.509, utilizzati per identificare e autenticare i partecipanti. Attraverso il sistema di Hyperledger Fabric vengono definiti i ruoli e le specifiche autorizzazioni per i partecipanti della rete, controllando così l'accesso al canale e alle risorse. Infine, attraverso la struttura di Hyperledger Fabric è possibile mantenere un controllo rigoroso sui dati registrati in blockchain, la piattaforma offre flessibilità per scegliere quali informazioni includere in una transazione e quali, invece, mantenere private, garantendo così confidenzialità delle informazioni sensibili e limitando gli accessi solo alle parti autorizzate [30-31].

3.2.3 Alti livelli di sicurezza

Hyperledger Fabric è progettato per garantire un alto livello di sicurezza, fornendo una serie di meccanismi avanzati per proteggere i dati e le transazioni su blockchain, tra questi, vi è l'uso della crittografia che svolge un ruolo fondamentale per far sì che i dati siano confidenziali, sicuri e autentici. In particolare, Hyperledger Fabric fa uso di un sistema di crittografia asimmetrica, noto anche come crittografia a chiave pubblica. In tale modalità ogni partecipante possiede una coppia di chiavi: una chiave pubblica e una chiave privata. La chiave pubblica è conosciuta da tutti sulla rete e può essere utilizzata per crittografare i dati o le transazioni. La chiave privata è mantenuta segreta e viene utilizzata per de crittografare i dati segretati con la chiave pubblica e per firmare digitalmente le transazioni.

Inoltre la crittografia asimmetrica consente anche di proteggere la confidenzialità dei dati sulla rete. Questo è permesso in quanto, quando un partecipante invia una transazione o dei dati crittografati con la chiave pubblica di un destinatario, solo il possessore della chiave privata corrispondente sarà in grado di accedere ai dati originali de crittografandoli. In questo modo i dati sensibili restano privati ed accessibili solo ai partecipanti autorizzati. Le transazioni inviate in questo modo e associate con una firma digitale garantiscono l'integrità dei dati, qualsiasi modifica ai dati o alle transazioni invaliderebbe la firma digitale. Pertanto, anche se i dati venissero intercettati o manipolati durante la trasmissione, la verifica della firma digitale rivelerebbe l'alterazione.

Legato alla sicurezza Hyperledger Fabric dispone di uno strumento, l'Endorsement Policy, ovvero una politica di approvazione che contribuisce all'affidabilità e all'integrità delle transazioni e degli smart contract sulla rete. Tale meccanismo si basa sulla convalida delle transazioni prima che vengano registrate sulla blockchain. Tale politica di approvazione consente la convalida e la scrittura delle transazioni solo dopo una verifica e una valutazione eseguita da un gruppo di nodi incaricati. Questi nodi sono gli Endorsing Peers, e i nodi preposti a questo compito vengono definiti dalla politica di approvazione, inoltre si può richiedere una determinata percentuale di Endorsing Peers con valutazione positiva affinché la transazione venga registrata su blockchain. Tale

maccanismo secondo cui i peer di Endorsing debbano solo approvare le transazioni e non eseguirle ha un effetto positivo sul carico della rete, andando a ridurlo e migliorando le prestazioni complessive di convalida delle transazioni. Un altro effetto positivo di tale politica è la fiducia nella rete e la sicurezza da parte di gruppi malevoli, le approvazioni devono essere approvate da uno specifico gruppo; quindi, la manomissione è difficile da realizzare consentendo alle sole transazioni legittime l'approvazione e la scrittura su blockchain.

Infine, vi è l'aspetto di auditing e tracciabilità, Hyperledger Fabric consente di registrare in modo dettagliato tutte le attività sulla rete, in particolare le transazioni, le modifiche ai dati, le azioni degli utenti e qualsiasi altro evento rilevante. In questo modo è facile individuare e correggere eventuali anomalie, rendendo i partecipanti responsabili delle loro azioni andando a verificare chi ha eseguito una determinata operazione. In caso di violazioni o di attività sospette le funzionalità di audit consentono di investigare l'origine e l'entità dell'incidente. Questo è fondamentale per prendere provvedimenti tempestivi e mitigare i danni [31].

3.3 Introduzione agli aspetti negativi

Nell'analisi del framework di Hyperledger Fabric è importante tenere in considerazione alcuni aspetti negativi che potrebbero presentare delle sfide nel percorso di adozione e implementazione di questa tecnologia. L'implementazione e la gestione di una rete Hyperledger Fabric può essere intricata e richiedere competenze tecniche avanzate. La flessibilità architetturale e le numerose opzioni di configurazione potrebbero comportare una curva di apprendimento ripida per il team coinvolto. La necessità di prendere decisioni su componenti, protocolli di consenso, livelli di sicurezza e ruoli dei partecipanti potrebbe richiedere tempo e risorse significative per una configurazione adeguata.

Pur avendo fatto progressi notevoli nella gestione di grandi volumi di transazioni e partecipanti, Hyperledger Fabric può presentare sfide legate alla scalabilità. L'aumento

del carico di lavoro potrebbe influire sulle prestazioni complessive del sistema, aumentando la latenza delle transazioni e richiedendo risorse di sistema aggiuntive. La progettazione di una rete che possa crescere in modo efficiente richiede ottimizzazione continua e pianificazione accurata.

Infine, Hyperledger Fabric utilizza il linguaggio di programmazione Go per la scrittura degli smart contract. Questa scelta potrebbe rappresentare una sfida per gli sviluppatori abituati ad altri linguaggi più comuni nel contesto delle blockchain, come JavaScript o Solidity. La necessità di adattarsi a Go potrebbe comportare una curva di apprendimento aggiuntiva per gli sviluppatori e potrebbe limitare la flessibilità nella creazione di smart contract complessi.

Mentre vengono esplorati questi aspetti negativi, è fondamentale riconoscere che ogni sfida può essere superata attraverso la pianificazione, la formazione e la collaborazione con la comunità di Hyperledger.

3.3.1 Complessità nell'utilizzo di Hyperledger Fabric

Uno dei principali aspetti negativi da considerare quando si adotta Hyperledger Fabric per implementare una propria blockchain è la complessità iniziale associata alla configurazione e all'implementazione di una rete basata su questo framework. In particolare, Hyperledger Fabric è noto per la sua flessibilità e personalizzabilità, come detto in precedenza questo è assolutamente un suo punto di forza, tuttavia porta a una maggiore complessità. La rete può essere configurata con diverse componenti, come canali, nodi peer, nodi ordinatori e smart contract. Inoltre, bisogna prendere decisioni in merito all'algoritmo di consenso da utilizzare, come gestire gli aspetti di sicurezza e quali ruoli assegnare ai partecipanti. Tutto questo può complicare la configurazione iniziale, specialmente per chi non è pratico di tali sistemi.

La curva di apprendimento per comprendere a fondo le componenti, i concetti e le procedure specifiche di Hyperledger Fabric può essere piuttosto ripida. È necessario che gli sviluppatori investano tempo nell'acquisizione di conoscenze dettagliate su come

funziona la rete e su come configurarla correttamente. Questa curva di apprendimento potrebbe comportare, quindi, un rallentamento nella fase iniziale del progetto. Infatti, la configurazione di una rete Hyperledger Fabric richiede competenze tecniche avanzate nel campo delle reti distribuite, della crittografia e della programmazione. Gli sviluppatori devono avere una solida comprensione dei principi blockchain e delle caratteristiche uniche di Hyperledger Fabric.

Infine, date le numerose opzioni di configurazione e le decisioni da prendere, esiste il rischio di commettere errori durante la fase iniziale di implementazione. Un'errata configurazione potrebbe portare a vulnerabilità di sicurezza, inefficienze o addirittura al malfunzionamento della rete. La complessità iniziale aumenta la probabilità di errori, che potrebbero richiedere sforzi supplementari per correggerli in seguito. La complessità iniziale, infatti, rappresenta una sfida nell'adozione di Hyperledger Fabric, per mitigarla è fondamentale investire nella formazione e nell'addestramento del team coinvolto. La creazione di una solida base di conoscenza può aiutare a mitigare i rischi di errori e accelerare il processo di implementazione. Una volta superato questo ostacolo, gli aspetti positivi e i vantaggi di utilizzare Hyperledger Fabric, come l'architettura modulare, la privacy e il controllo degli accessi, possono avere un impatto positivo sulla creazione e sulla gestione della rete blockchain [28-29].

3.3.2 Sfida di scalabilità

Nonostante Hyperledger Fabric abbia fatto notevoli progressi sulla scalabilità rispetto alle sue prime versioni, rimane una sfida significativa la gestione di grandi volumi di transazioni e di partecipanti. La scalabilità è un aspetto cruciale per qualsiasi sistema blockchain in quanto può influire sull'implementazione e sulla gestione di una rete. Infatti, aumentare il numero di transazioni o partecipanti all'interno di una rete Hyperledger Fabric può influire direttamente sulle prestazioni complessive del sistema. Con l'aumentare dei carichi di lavoro, si potrebbero verificare rallentamenti nella conferma e nell'elaborazione delle transazioni. Tutto ciò, potrebbe compromettere

l’efficienza del sistema e il tempo di risposta, influenzando conseguentemente l’esperienza dell’utente finale e l’affidabilità delle operazioni.

Un’altra conseguenza all’aumento del numero di transazioni e a una maggiore partecipazione è l’aumento della latenza nelle conferme. Tale aumento avrebbe un impatto sulle tempistiche con cui le operazioni vengono validate e registrate sulla blockchain. In un ambiente in cui il tempismo è fondamentale, questa latenza rappresenta senza dubbio una sfida critica. Per risolvere i problemi di scalabilità è necessario disporre di risorse di sistema adeguate. Per aumentare il numero di partecipanti e transazioni bisogna richiedere l'allocazione di risorse aggiuntive, come capacità di calcolo, memoria e larghezza di banda. Questo potrebbe tradursi in costi aggiuntivi per l'infrastruttura e per il mantenimento della rete. Gestire la scalabilità richiede, quindi, sforzi continui di ottimizzazione. Infatti, la progettazione e l’architettura della rete devono essere attentamente sviluppate per garantire una gestione efficace del carico di lavoro crescente. Per fare ciò è necessario la revisione dei componenti, l’ottimizzazione degli algoritmi di consenso e la gestione delle risorse di sistema.

Infine, bisogna raggiungere un buon compromesso tra scalabilità e sicurezza, questo in quanto aumentare la scalabilità può influire sulla sicurezza del sistema. Decisioni prese per migliorare la scalabilità potrebbero compromettere la decentralizzazione, la sicurezza dei dati o la resistenza dei guasti. Trovare il giusto equilibrio tra questi aspetti è senza dubbio una sfida che richiede un’approfondita analisi delle esigenze aziendali. In sintesi, è importante riconoscere che gestire grandi volumi di transazioni e partecipanti può richiedere un'attenzione particolare. Per affrontare la sfida di scalabilità in Hyperledger Fabric, è importante adottare un approccio oculato e pianificato. Prima di tutto, è essenziale valutare le reali esigenze di scalabilità del progetto e costituire l'architettura in modo da poter crescere efficientemente. In secondo luogo, è importante condurre test di scalabilità per identificare potenziali problemi e risolverli in anticipo. Infine, potrebbe essere necessario investire in risorse hardware e ottimizzazioni software per mantenere le prestazioni desiderate [32-33].

3.3.3 Rigidità negli smart contract

Uno dei punti critici da tenere in considerazione nell'implementazione di Hyperledger Fabric è la scelta del linguaggio di programmazione per la scrittura degli smart contract. Questo perché a differenza di altri framework blockchain, Hyperledger Fabric utilizza per l'implementazione dei contratti intelligenti Go.

Go pur essendo un linguaggio di programmazione potente e popolare per lo sviluppo di applicazioni è comunque meno diffuso rispetto ad altri linguaggi più comuni nel contesto blockchain come JavaScript o Solidity. L'uso esclusivo di Go per gli smart contract è una limitazione per gli sviluppatori abituati all'uso di altri linguaggi, questo comporta quindi un periodo di studio del linguaggio se non si posseggano già conoscenze in merito, andando a rallentare la curva di apprendimento. Inoltre, Go pur essendo un linguaggio potente, presenta delle mancanze in alcune funzionalità e librerie specifiche presenti in altri linguaggi, questo andrebbe a complicare ulteriormente la creazione di smart contract complessi che richiedono particolari funzionalità non disponibili nativamente in Go.

Tuttavia, l'uso del linguaggio Go da parte di Hyperledger Fabric ha anche i suoi vantaggi, infatti tale linguaggio è noto per le sue prestazioni elevate, la sua efficienza nella gestione delle risorse e la sua capacità di produrre codice altamente ottimizzato. Questi aspetti sono particolarmente vantaggiosi in scenari aziendali in cui la velocità e l'efficienza sono fondamentali.

Per affrontare la sfida della rigidità nei contratti intelligenti di Hyperledger Fabric, è fondamentale investire nella formazione e nell'addestramento del team di sviluppo. Questo può aiutare gli sviluppatori a padroneggiare il linguaggio Go e a adattarsi alle sue peculiarità [34].

3.4 Un bilancio tra vantaggi e sfide

In conclusione, l'adozione di Hyperledger Fabric per la gestione dei processi aziendali attraverso una soluzione blockchain offre un panorama di opportunità e sfide che richiedono un'attenta valutazione. La complessità iniziale nell'implementazione e configurazione, accompagnata dalla sfida di scalabilità e dalla scelta del linguaggio Go per gli smart contract, rappresentano elementi che richiedono attenzione e pianificazione. Tuttavia, questi aspetti negativi devono essere ponderati alla luce dei numerosi vantaggi che Hyperledger Fabric può offrire.

L'architettura modulare e flessibile di Hyperledger Fabric si dimostra un pilastro fondamentale nella personalizzazione delle reti blockchain in base alle esigenze specifiche. La precisione nella gestione dell'accesso e delle autorizzazioni, insieme ai meccanismi avanzati di crittografia e controllo dei dati, conferisce alla piattaforma un alto livello di sicurezza. I canali privati, le chiavi pubbliche e private, oltre alla politica di approvazione, consentono un controllo granulare e una privacy dei dati senza precedenti.

L'orientamento aziendale di Hyperledger Fabric trova fondamento nella sua adattabilità alle esigenze delle imprese, anche se l'implementazione iniziale potrebbe richiedere competenze tecniche avanzate. La scelta di Hyperledger Fabric rappresenta una decisione ponderata basata sull'equilibrio tra queste sfide e i benefici tangibili offerti dalla piattaforma.

In un mondo aziendale sempre più orientato verso la digitalizzazione allora l'efficienza operativa, la tracciabilità e la sicurezza dei processi aziendali rimangono obiettivi cruciali. Hyperledger Fabric, con il suo approccio solido e su misura, si profila come una soluzione che, una volta superate le sfide iniziali, potrebbe conferire a qualsiasi organizzazione un vantaggio competitivo e una base solida per l'evoluzione dei propri processi aziendali.

Di seguito viene presentata una tabella riassuntiva per ricapitolare quali sono i punti di forza e quali sono le sfide nell’adottare Hyperledger Fabric.

Tabella 3. Confronto tra punti di forza e sfide nell'adozione di Hyperledger Fabric.

PUNTI DI FORZA	SFIDE
Architettura modulare e flessibile per adattare e personalizzare il sistema in base alle esigenze. Possibilità di scegliere l'algoritmo di consenso, il modello di storage e i componenti aggiuntivi.	Complessità iniziale nella gestione della flessibilità con numerose scelte da implementare e una curva di apprendimento ripida.
Gestione privacy tramite l'uso di canali privati, delle autorizzazioni, dei ruoli e dell'identità digitale con i certificati X.509.	Scalabilità con il rischio di rallentamento sulle transazioni se si verificano carichi sulla rete e aumento della latenza delle conferme. Ricerca del giusto compromesso tra scalabilità e sicurezza.
Sicurezza eccellente grazie alla crittografia asimmetrica per la sicurezza e l'autenticità dei dati, uso dell'Endorsment Policy per l'affidabilità e l'integrità delle transazioni.	Rigidità degli smart contract dato dall'utilizzo del linguaggio di programmazione Go, in quanto poco diffuso e limitato in alcune funzioni

3.5 Consumo energetico

Negli ultimi anni, il dibattito sul consumo energetico della blockchain è diventato centrale in ambito tecnologico. Infatti, con la sua espansione nell'adozione comune è cresciuto l'interesse legato al consumo energetico, che è attualmente uno dei principali punti di attacco per i conservatori che non vogliono che tale tecnologia emergi nella società. La tecnologia blockchain non è però omogenea e il dispendio energetico dipende da un ampio numero di fattori come lo stoccaggio associato alle operazioni della blockchain, la computazione ridondante e il meccanismo di consenso adottato.

Hyperledger Fabric essendo una piattaforma open-source sviluppata appositamente per l'uso aziendale per consentire la creazione di reti blockchain private e autorizzate non utilizza meccanismo di consenso PoW come richiede Bitcoin, optando per un sistema di consenso basato sui permessi. Questa differenza è significativa in quanto, il non dover utilizzare il processo di mining per la validazione delle transazioni non comporta un dispendio di energia elevato. Hyperledger Fabric grazie a questo suo meccanismo di consenso basato su accordi tra partecipanti autorizzati alla rete, ha un consumo

notevolmente inferiore rispetto alle blockchain pubbliche. Infatti, essendo stata progettata per applicazioni aziendali, la rete è spesso gestita in data center o cloud provider che utilizzano infrastrutture energetiche efficienti.

È comunque da tenere in considerazione che il consumo energetico di un qualsiasi sistema blockchain dipende anche dalla complessità dell'implementazione; ovviamente, reti con un gran numero di nodi e transazioni richiedono più energia rispetto a piccole reti. Quindi, per una valutazione accurata sul consumo energetico devono essere fatte considerazioni su numerosi fattori, primi tra tutti il numero di nodi, le transazioni elaborate e l'efficienza dell'infrastruttura sottostante.

In conclusione, Hyperledger Fabric rappresenta una scelta più sostenibile dal punto di vista energetico rispetto a molte blockchain pubbliche, ma è comunque necessaria una corretta ottimizzazione del consumo energetico tramite implementazioni aziendali adeguate è [39-40].

3.6 Hyperledger FireFly

Hyperledger FireFly rappresenta una soluzione innovativa nel contesto della tecnologia blockchain. Si tratta di un Supernodo open-source sviluppato all'interno dell'ecosistema Hyperledger, che si concentra sulla facilitazione dell'integrazione e dell'interoperabilità tra diverse reti blockchain. Hyperledger FireFly fornisce un framework modulare e scalabile per l'interconnessione delle reti, consentendo lo scambio sicuro e affidabile di messaggi e transazioni tra le diverse blockchain.

Inoltre, Hyperledger FireFly offre la flessibilità di personalizzare le regole e le logiche di interazione tra le reti. Questo consente agli sviluppatori di definire protocolli di comunicazione specifici, nonché le regole per l'elaborazione delle transazioni e la convalida delle informazioni tra le blockchain.

Un altro aspetto importante di Hyperledger FireFly è la sicurezza e la privacy dei dati. Utilizzando crittografia e meccanismi di autenticazione robusti, FireFly garantisce la

riservatezza e l'integrità delle transazioni e dei messaggi scambiati tra le reti blockchain, supportando anche smart contract personalizzati e token di gestione, sia fungibili che non fungibili [23].

3.6.1 Gestione Token

Un token rappresenta un'unità di valore su una piattaforma blockchain, in particolare un token ERC-20 [24], ha uno standard specifico ed un insieme di regole che ne definiscono il comportamento. Tale token viene definito fungibile e quindi ogni identità digitale è intercambiabile con un'altra, oltre a essere divisibile per una frazione. Hyperledger FireFly offre standardizzazione a livello applicativo, fornendo API che operano su standard di token e implementazioni blockchain, garantendo un supporto coerente e interoperabile, fornendo, quindi, API consistenti e ben definite per consentire l'interazione e lo scambio di token tra diverse implementazioni blockchain. Hyperledger FireFly per facilitare la gestione e il trasferimento di token offre una serie di funzionalità [25]:

- Indicizzazione automatica dei token: FireFly offre l'indicizzazione automatica dei token, sia quelli già esistenti che quelli appena distribuiti. Ciò semplifica la tracciabilità e la gestione dei token, consentendo agli utenti di identificare e monitorare facilmente i token nella rete.
- Indicizzazione off-chain di trasferimenti e saldi: FireFly permette l'indicizzazione off-chain dei trasferimenti e dei saldi di beni fungibili e non fungibili. Questa funzionalità consente di tenere traccia dei movimenti dei token e dei relativi saldi senza dover memorizzare tutte le informazioni on-chain, ottimizzando così le prestazioni della rete.
- Indicizzazione off-chain delle approvazioni: Hyperledger FireFly offre anche l'indicizzazione off-chain delle approvazioni, consentendo agli utenti di tenere traccia delle autorizzazioni e delle approvazioni associate ai token. Ciò facilita la gestione dei diritti e delle restrizioni sui token.

- Integrazione con l'identità digitale: FireFly si integra con l'identità digitale, consentendo di associare in modo sicuro e affidabile le identità degli utenti ai token e alle transazioni. Ciò contribuisce a garantire la conformità e la sicurezza all'interno delle reti blockchain.
- Piena estensibilità attraverso gli standard token e le tecnologie blockchain: Hyperledger FireFly è altamente estensibile, poiché si basa sugli standard dei token e può essere integrato con diverse tecnologie blockchain. Ciò consente alle organizzazioni di adattare e personalizzare la soluzione per soddisfare le loro esigenze specifiche.

Inoltre, la gestione del portafoglio e delle chiavi di firma è fondamentale per il trasferimento sicuro di risorse digitali tra portafogli. Pertanto, FireFly, fornisce funzionalità per consentire una gestione sicura e user-friendly dei portafogli, garantendo che solo i proprietari autorizzati possano accedere e trasferire i token.

Capitolo 4 - Proof Of Concept: Blockchain e tokenizzazione per la gestione dei processi aziendali

Il Proof of Concept proposto vuole dimostrare la fattibilità di una soluzione innovativa volta alla distribuzione di token ai dipendenti al raggiungimento di determinati obbiettivi. Più precisamente l'obbiettivo è il corretto eseguimento della metodologia E6, ed è attraverso l'eseguire di tale metodologia che i dipendenti potranno ricevere una remunerazione sotto forma di token. Tale soluzione comprende l'utilizzo della tecnologia blockchain di Hyperledger, in particolare i framework Hyperledger Fabric e Hyperledger FireFly.

In questa sezione vengono fornite informazioni sui punti chiave della metodologia E6, sviluppando per ognuno una descrizione sulle caratteristiche, sui problemi attualmente riscontrati ed una possibile soluzione di controllo attuabile tramite blockchain, seguita poi da un'analisi sui vantaggi apportati. La metodologia E6 è un framework sviluppato internamente in Thales Alenia Space utilizzato per monitorare gli eventi e le attività di interesse, in modo da chiarire quali siano le priorità e le precedenze. Tramite tale metodologia si cerca di migliorare il lavoro di squadra attuando una visione chiara e condivisa dei flussi di lavoro.

4.1 Gestione processi aziendali

La gestione di un team all'interno di un'organizzazione è una parte cruciale della gestione dei processi aziendali. In questa fase vengono coinvolti aspetti per assicurarsi che la squadra sia efficiente, produttiva e in grado di raggiungere gli obbiettivi prefissati. Il processo inizia con un'attenta scelta dei membri del team, questa operazione viene fatta in base alle competenze, all'esperienza e all'abilità necessarie per svolgere il progetto in questione, inoltre a tali membri vengono assegnati ruoli e responsabilità chiare e definite. Successivamente vengono stabiliti obbiettivi, milestone e scadenze chiare per il progetto, questo per far sì che il team possa mantenere il focus e

misurare lo stato di avanzamento. Nella squadra vi deve sempre essere una comunicazione aperta e trasparente con riunioni regolari per aggiornamenti sullo stato del progetto, risolvere problemi e condividere informazioni cruciali; quindi, è essenziale una corretta gestione dell'agenda. Infine, deve essere possibile la modifica del team nel tempo in modo agile e flessibile.

4.1.1 Soluzione Blockchain

La soluzione blockchain in questo caso è estremamente legata alla gestione dell'agenda e alle milestone, questi argomenti sono presentati e analizzati nel corso di questo capitolo, si invita il lettore a visionare i paragrafi 4.2 e 4.4.

In base all'area di competenza del progetto, il team dovrà essere inserito nel sotto-canale adeguato, ad ogni membro dovrà poi essere assegnato un ruolo e dovranno essere definite le responsabilità. Tramite il ruolo assegnato, quindi, sarà in grado di visionare le risorse necessarie oltre che a provvedere al caricamento di documenti o alla validazione tramite firme in base agli specifici compiti assegnati in modo individuale. I ruoli assegnati dovranno essere flessibili, consentendo così di poter modificare nel corso del tempo i membri del team assegnato al progetto, andando, quindi, a modificare le autorizzazioni per l'accesso alle risorse. Inoltre, chi è incaricato della formazione della squadra dovrà impostare la percentuale di tempo del progetto a cui è assegnato ogni specifico membro. In questo mondo le ricompense di squadra dei token al raggiungimento di determinati obbiettivi verranno mediati anche in base al contributo del lavoro svolto.

4.1.2 Valore Aggiunto

Tramite tale soluzione i ruoli e le autorizzazioni di accesso sarebbero chiare e scritte su blockchain, inoltre per ogni progetto sarebbe possibile visionare quali membri sono stati assegnati e per ognuno di essi vedere le competenze specifiche e la percentuale di tempo assegnato al progetto. In tal modo sarebbe facile capire se allo specifico progetto è stato assegnato un numero adeguato di risorse con capacità personali utili allo svolgimento dello stesso, un'altra verifica facile da effettuare sarebbe quella sulla sovra allocazione delle risorse, non sarebbe infatti possibile assegnare ad un singolo individuo una percentuale che superi il totale delle sue ore lavorative. Infine, tramite l'aggiornamento costante dei ruoli è possibile mantenere un certo grado di sicurezza sugli accessi, stabilendo le autorizzazioni per visionare i documenti di progetto e modificarli.

4.2 Gestione Agenda

La gestione di una agenda è una questione estremamente importante in una azienda; infatti, avere un corretto controllo delle riunioni settimanali è fondamentale per non creare sovrapposizioni tra di esse. Quindi è preferibile avere più riunioni, ma corte, nell'arco della settimana che accumulare invece discussioni di gruppo sui progetti da sviluppare.

La metodologia E6 si pone, infatti, proprio tra gli obiettivi quello di migliorare la pianificazione dei meeting, utilizzando riunioni programmate più brevi ma focalizzate su una determinata tematica. Questo al fine di risolvere problemi o avere aggiornamenti sullo stato di avanzamento in modo rapido, cercando di evitare lunghe attese o perdite di tempo. In tale contesto è quindi essenziale che tutti i dipendenti che abbiano un interesse dal punto di vista della tematica discussa partecipino alle riunioni. Se questo non venisse rispettato si creerebbe difficolta nella comunicazione tempestiva di eventuali problematiche con conseguente ritardo nella loro risoluzione.

4.2.1 Soluzione blockchain

Per la realizzazione di un controllo sulle partecipazioni alle riunioni è senza dubbio importante la verifica dell'identità digitale associata ai partecipanti e la possibilità di firma digitale per attestare la loro partecipazione. Inoltre, ci si può appoggiare ad un oracolo esterno che andrebbe ad integrare il chaincode. Ad esempio, potrebbe esserci un servizio di gestione delle riunioni che registra automaticamente la partecipazione delle persone e fornisce informazioni verificabili tramite API. Tramite queste informazioni il chaincode ad ogni mese andrebbe in automatico a distribuire ai dipendenti i token in percentuale alla loro partecipazione nelle riunioni; quindi, è importante che chi programma l'agenda di progetto, che quindi ha le autorizzazioni necessarie, scriva su blockchain la pianificazione delle riunioni in modo tale che il chaincode abbia i dati necessari per eseguire una percentuale tra riunioni totali programmate e riunioni a cui si ha partecipato.

4.2.2 Valore aggiunto

Il valore aggiunto di partecipare a tali riunioni risiede nel fatto che vi è un costante aggiornamento sullo sviluppo del lavoro, che quindi avvantaggia la scoperta tempestiva di eventuali problematiche, inoltre permette un vantaggio in termini temporali al momento in cui andranno prese le decisioni, questo in quanto viene così evitato un lungo tempo impiegato, altrimenti, al coordinamento. In questo caso, infatti, essendo avvenuto in modo costante si riuscirebbe a garantire un maggior focus sul problema, evitando di rimandare discussioni su determinati problemi. Tutto questo permette di conseguire più facilmente uno dei principali obiettivi della metodologia E6, il lavoro di squadra.

Senza la blockchain tutto questo sarebbe possibile, ma con un utilizzo di risorse temporali oltre che di personale, che sarebbe incaricato della verifica delle presenze e della distribuzione di token, molto elevati. In questo modo questi compiti verrebbero

automatizzatati e l'incentivo di ricevere il token spingerebbe più persone a seguire in modo costante le riunioni. Inoltre, essendo che la pianificazione è scritta su blockchain, questa sarebbe tracciabile e trasparente per tutti i soggetti interessati.

4.3 Concept Paper e Trade-off

All'inizio di ogni progetto è importante per il team creare un documento che descriva in maniera chiara e concisa quali sono i valori che il cliente ricerca nel prodotto, valori che permetteranno di identificare in maniera più obbiettiva i parametri tecnici chiave da tenere sotto controllo durante il progetto. Questo documento chiamato Concept Paper viene prodotto in fase di risposta al bando e viene poi validato in una riunione di inizio progetto ed è quindi importante che sia chiaro e completo, con tutti i punti sviluppati adeguatamente per poter partire con lo sviluppo del progetto. Eventuali dati mancanti o incompletezze potrebbero causare ritardi. Inoltre, è importante durante tutto lo sviluppo del progetto la creazione di documenti A3 come strumento di decisione e di comunicazione dei trade-off aziendali per affrontare decisioni complesse che coinvolgono la scelta tra diverse opzioni.

4.3.1 Soluzione blockchain

Il primo vincolo, necessario, per cui la persona o il team incaricato della stesura del Concept Paper o del documento di Trade-off riceva il token è il caricamento dello stesso entro la data limite, questo verificabile tramite il chaincode. Una volta che il soggetto interessato alla creazione della documentazione lo ha caricato su blockchain come parte di una transazione, convertendolo in una rappresentazione digitale attraverso un hash crittografico, è compito del responsabile del progetto apporre la sua firma di validazione in fase di riunione. Il rappresentante di progetto, avendo i permessi necessari, ha il compito di validare il documento aggiungendo come attributo una classificazione del documento: completo, adeguato o incompleto. Il chaincode, se il vincolo temporale

sopra citato è rispettato, distribuirà automaticamente i token ai soggetti interessati in base all'attributo di classificazione.

4.3.2 Valore Aggiunto

Il valore aggiunto di tale soluzione risiede senza dubbio nella trasparenza e tracciabilità di tali documenti, una volta registrati su blockchain sono altamente condivisibili a tutti i soggetti interessati al progetto. Inoltre, l'incentivo della remunerazione tramite il token, è pensata per far sì che i documenti siano il più completi possibili, senza parti rimandate da discutere nella riunione di inizio progetto o in riunioni successive.

L'automatizzazione del processo tramite il contratto digitale è ottima per non dover impiegare personale a tali compiti. Infine, tramite una soluzione blockchain sarebbe possibile tracciare i KVA (Key Value Attribute) e il loro flusso nei Key Performance Indicators (KPI) e nelle successive allocazioni nei vari requisiti. Offrendo una registrazione immutabile e trasparente delle attività con un audit semplificato grazie ai dati su blockchain accessibili e immutabili.

4.4 Milestone

Le milestone vengono utilizzate per indicare il raggiungimento di determinati obbiettivi entro una certa data, sono stabiliti nella pianificazione di un progetto. Solitamente una determinata milestone ha più sotto-obiettivi da raggiungere, e viene verificato il raggiungimento di quest'ultimi in una riunione di controllo. Per fare ciò vengono create delle check-list e poi attraverso un'operazione di controllo vengono spuntati gli obiettivi raggiunti, queste check-list sono utilizzate per avere un elenco di compiti da svolgere, riducendo il rischio di dimenticanze. Inoltre, sono efficaci per par sì che il team di progetto abbia chiaro i compiti da svolgere.

4.4.1 Soluzione blockchain

Per ogni milestone, si dovrà creare una check-list che elenca gli obbiettivi specifici da raggiungere entro una determinata data. La check-list viene rappresentata all'interno del chaincode, contenente gli elementi che devono essere completati. Durante lo sviluppo del progetto i soggetti interessati completeranno gli obbiettivi, quindi, aggiorneranno lo stato di completamento attraverso metodi o funzioni all'interno del chaincode, creati in modo tale da consentire ai partecipanti di segnalare il completamento dei sotto-obbiettivi. Nella riunione di controllo, il responsabile verificherà il corretto raggiungimento degli obbietti spuntati e apporrà la sua firma digitale. A questo punto il chaincode calcolerà in modo automatico la remunerazione di token in base alla percentuale di obiettivi raggiunti ed eseguirà le transazioni.

4.4.2 Valore aggiunto

Tramite questa modalità vi sarebbe completa trasparenza e condivisione, tutti i partecipanti avrebbero modo, quindi, di vedere la check-list e il suo stato di completamento, mantenendo la tracciabilità di chi ha svolto il sotto-obbiettivo della lista.

Questo ridurrebbe il rischio che qualche sotto-obbiettivo venisse ricordato solo in fase di controllo causando un ritardo di sviluppo. Tale metodo sarebbe possibile anche senza blockchain, ma con una condivisione meno efficace, oltre all'uso di personale, ora impegnato altrove, che sarebbe incaricato di verificare e aggiornare le check-list prima di eseguire le remunerazioni.

4.5 Causal Influence Diagrams

All'interno della metodologia E6 i Causal Influence Diagrams (CID), ovvero diagramma di influenza causale, hanno un ruolo molto importante. Rappresentano uno schema che aiuta a visualizzare come delle variabili correlate si influenzino a vicenda e qual è l'effetto di tale influenza. Tramite il diagramma sono collegate le variabili tra di loro ed attraverso una analisi si prevede come varieranno i risultati modificando il valore degli input. In sede di riunione, quindi, è importante avere la documentazione che deve essere quindi consegnata per tempo in un formato compatto e leggibile come un documento A3. Questo documento è utile in fase di riunioni per prendere determinate decisione, avendo a supporto un'analisi pregressa di causa-effetto sugli input.

4.5.1 Soluzione blockchain

Per prima cosa avverrà il caricamento del CID su blockchain, convertendolo in un formato digitale e includendolo come parte del payload della transazione. Questa operazione verrà eseguita dal soggetto incaricato del compito. Il chaincode quindi verrà scritto in modo tale che potrà validare il caricamento di tale documento; nel caso in cui venga caricato entro la data di scadenza allora il contratto farà partire la remunerazione in modo automatico verso i soggetti interessati.

4.5.2 Valore aggiunto

In tale soluzione, rispetto al caso senza blockchain, sarebbe garantita la condivisione e la tracciabilità del documento, tutti i soggetti interessati possono visionare il documento, facilitando la presa di decisioni avendo un'analisi pregressa di causa-effetto sulle prestazioni attese. In sede di riunione tale documento farebbe risparmiare tempo, in

quanto materiale aggiuntivo per prendere decisioni, l'incentivo del token, quindi, spingerebbe ad un utilizzo maggiore della creazione di CID che andrebbero a migliorare lo sviluppo di un progetto.

4.6 Key Decision Tree

Nella metodologia E6 il Key Decision Tree (KDT), ovvero l'albero delle decisioni, è una parte fondamentale. I KDT vengono rappresentati come un diagramma visuale utilizzato per scandire nel tempo le decisioni chiave (KD) e il divario di conoscenza tra quello che si possiede e quello che bisogna raggiungere (KG). Tale conoscenza da colmare e le decisioni chiave da prendere possono essere a livello temporale sia quotidiane, che settimanali o mensili, sono organizzate e scandite secondo un Takt Time in base a ciò che è possibile eseguire con le risorse a disposizione.
Al fine di raggiungere gli obbiettivi, quindi, è essenziale una corretta pianificazione nel tempo, per capire il flusso di decisioni da prendere e la conoscenza da acquisire per poterle prendere. Inoltre, è utile giustificare quello che si è fatto in documenti dal formato compatto e leggibile come gli A3 in modo tale che vengano fornite spiegazioni. Tali documenti devono essere caricati in tempo per rispettare la corretta pianificazione e non causare ritardi.

4.6.1 Soluzione Blockchain

Per tale soluzione il responsabile della pianificazione dovrà quindi scrivere su blockchain la stessa in modo tale che vi sia tracciabilità e collegamento tra i KD e KG, definendo in modo chiaro la sequenza temporale di chiusura. Una sorta di flusso sequenziale che indichi quale conoscenza va acquisita per poter prendere delle decisioni e quali decisioni devono essere prese per prime. Inoltre, dovrà essere costituita una

matrice RACI, uno strumento per definire i ruoli e le responsabilità all'interno del processo in modo che vengano esplicitate quali persone è necessario consultare o informare prima di chiudere un KG o KD. I soggetti interessati che dovranno svolgere questi compiti, quindi, prenderanno delle decisioni cambiando lo stato dello specifico KD in "decision" o acquisiranno conoscenza cambiando lo stato in "learned" del rispettivo KG. Insieme al cambio di stato verrà caricato anche il documento A3 in un formato digitale come payload della transazione.

Il chaincode sarà scritto in modo tale che verifichi innanzitutto la presenza e validità del documento caricato, successivamente verificherà che la KD o il KG sia stato preso in tempo nella pianificazione. In caso contrario calcolerà una percentuale in base al ritardo accumulato. Inoltre, calcolerà anche i KG ancora aperte associate a una KD presa, questo aumenta l'incertezza, quindi, il chaincode calcolerà una percentuale di incertezza in base ai sotto nodi ancora aperti.

Infine, il chaincode farà partire la remunerazione dei token ai soggetti interessati in quantità che dipenderà in base alle tre variabili prima citate: il caricamento del documento, la percentuale accumulata di ritardo e la percentuale di incertezza.

4.6.2 Valore Aggiunto

Lo scopo è quello di aiutare le persone ad imparare una metodologia nel prendere le decisioni correttamente e nei tempi stabiliti. L'uso degli A3, poco sfruttati ad ora, viene così incentivato per la presenza della remunerazione. Il loro uso è essenziale per capire e avere chiara una spiegazione di una determinata decisione, nel contesto della blockchain tali documenti sarebbero altamente tracciabili e condivisibili consentendo agli interessati di poterli visionare.

La blockchain inoltre renderebbe possibile il tracciamento dei KG e delle KD, in modo tale che si creerebbe un flusso temporale tra di essi trasparente e visualizzabile dai membri del team interessato. Ad oggi uno dei principali problemi è il ritardo che viene accumulato nel risolvere i nodi; quindi, l'incentivo del token spingerebbe proprio i

dipendenti a cercare di rispettare i tempi. Inoltre, la risoluzione delle KD sarebbe facilitata grazie al poter consultare agilmente il flusso di decisioni e controllare, per i KG e le KD che si trovano prima, le spiegazioni contenute nei documenti. Infine, l'utilizzo della matrice RACI aiuterebbe la gestione chiara e trasparente dei ruoli assegnati per la chiusa dei KD o KG.

4.7 Tabella artefatti E6

Di seguito è riportata una tabella riassuntiva dei punti chiave discussi in precedenza riguardo alla gestione dei processi aziendali utilizzando la blockchain di Hyperledger Fabric. La tabella fornisce un'overview dei passaggi affrontati, inclusi gli obiettivi, le azioni da compiere e i benefici associati a ciascun punto. Utilizzando questa tabella, è possibile avere una visione d'insieme chiara e rapida di quali siano i punti salienti per gestire i processi aziendali in modo trasparente e automatizzato.

Tabella 4. Artefatti E6

Soggetto	Attributi variabili	Documento caricato	Attivazione contratto	Remunerazione	Valore aggiunto
AGENDA	RiunioneFatta (si/no) RiunioniTot	No	Ogni mese	% in base partecipazione	Aggiornamento costante
CONCEPT PAPER e TRADE-OFF	Firma (si/no) Classificazione	SI	Validazione firma	In base alla classificazione	Documento chiaro, completo e condiviso
MILESTONE	Firma (sì/no)	SI, check-list	Validazione firma	% in base a obbiettivi completati	Tracciabilità e condivisione degli obiettivi
CID	Documento (si/no)	SÌ, A3	Documento caricato	Totale se caricato prima di data stabilita	Analisi pregressa causa-effetto che fa risparmiare tempo

KD	Documento (si/no) KD (si/no)	SÌ, A3	KD ‘decision’	% in base a ritardo e % in base incertezza	Decisioni prese in tempo e tracciabilità
KG	Documento (si/no) KG (si/no)	SÌ, A3	KG ‘learned’	% in base a ritardo	Imparare in tempo per poter decidere e tracciabilità

Capitolo 5 - Realizzazione del Proof of Concept

In questo capitolo viene descritta una possibile realizzazione del Proof of Concept, con particolare attenzione per la blockchain Hyperledger Fabric e per il framework Hyperledger FireFly, utilizzato per la gestione dei token. Nelle prossime sezioni vengono approfonditi gli elementi essenziali per realizzare una propria blockchain andando a tradurre dal punto di vista pratico i concetti analizzati nel capitolo precedente. L'obbiettivo principale è dimostrare la fattibilità tecnologica di un sistema blockchain per il controllo delle pratiche aziendali e la successiva remunerazione tramite token garantendo l'automazione dei processi tramite gli smart contract in un contesto sicuro, tracciabile e immutabile.

5.1 Prospettiva dell'architettura

Hyperledger Fabric è una piattaforma blockchain permissioned che si basa sull'utilizzo di canali come meccanismo di partizionamento all'interno della rete principale. In questo modo i partecipanti possono creare un sottoinsieme privato e isolato della rete in cui possono comunicare e condividere informazioni in modo sicuro, questo metodo è ottimo per mantenere le transazioni private e separare la visibilità dei dati. Questo è un elemento essenziale per tale tesi, in quanto in Thales Alenia Space vi è la necessità di separare progetti diversi. Gli attori coinvolti, ovvero i membri della blockchain, possono avere ruoli diversi all'interno della rete e possedere uno o più nodi. Dopo aver creato i canali separati andranno definiti i ruoli dei vari nodi, ognuno di essi ha, infatti, responsabilità diverse nell'architettura della rete come analizzato nel paragrafo 3.1.1. Tali nodi vanno identificati univocamente tramite indirizzi IP, inoltre devono lavorare insieme per sincronizzare il registro delle transazioni per garantire a tutti una visione coerente dello stato della blockchain e determinare l'ordine corretto delle transazioni, tutto questo reso possibile dalla partecipazione dell'algoritmo di consenso implementato.

5.1.1 Requisiti Hardware e Software

Per una corretta implementazione di Hyperledger Fabric è essenziale una pianificazione attenta sui requisiti hardware e software per garantire un funzionamento affidabile e performante della rete blockchain. In particolare, i requisiti hardware variano in base alle dimensioni e alla complessità delle rete blockchain, questo influenzato dal carico di transazioni previsto [42,44]:

- Processore: in Hyperledger Fabric è richiesta una potenza di calcolo sufficiente per eseguire le attività di consenso e l'esecuzione degli smart contract. Per garantire ciò i processori multi-core con una elevata frequenza di clock sono ottimali per una elaborazione rapida delle transazioni. È adatto quindi un processore multi-core con frequenza di clock di almeno 2.0 GHz, come potrebbe essere un processore Intel Core i5 o superiore.
- Memoria: la quantità di memoria RAM è cruciale per consentire l'archiviazione temporanea dei dati e l'esecuzione degli smart contract, la quantità esatta dipende dalla dimensione e dalla complessità della rete. Si stima che quello da sviluppare sia un ambiente di produzione impegnativo, dove la rete deve gestire un numero significativo di transazioni al secondo avendo bisogno, quindi, di una RAM di 16GB o più. Per una corretta valutazione è necessario comunque effettuare un test di carico e valutare le prestazioni per determinare la quantità esatta di memoria RAM necessaria per una corretta configurazione, in ogni caso l'utilizzo di una RAM di almeno 16GB è una stima prudente per garantire prestazioni ottimali in un ambiente di produzione impegnativo considerando la complessità degli smart contract.
- Spazio su disco: Hyperledger Fabric richiede dello spazio su disco per memorizzare i dati della blockchain e gli smart contract, la stima per una corretta gestione del sistema è di almeno 100 GB, ma questo dovrà essere valutato meglio in base ai test sulla quantità di dati gestiti dalla rete, anche tale stima è una considerazione prudente per garantire che lo spazio su disco non diventi un collo di bottiglia.
- Connettività di rete: in quanto c'è bisogno di una rete affidabile ad alta velocita, questo è essenziale per permettere la comunicazione tra i nodi della rete, inoltre

è conveniente che la latenza sia bassa per garantire una comunicazione rapida ed efficiente.

Oltre alle specifiche Hardware vi sono anche delle esigenze dal punto dei requisiti Software:

- Sistema operativo: solitamente Linux è la scelta preferita per i nodi di produzione, poiché offre maggiore stabilità e controllo. Tuttavia, Hyperledger Fabric supporta diversi sistemi operativi tra cui Ubuntu, CentOS e macOS.
- Dipendenze software Hyperledger Fabric: richiede diverse dipendenze software tra cui Docker e Docker Compose. Questi sono due strumenti essenziali per implementare e gestire le reti blockchain basate su Hyperledger Fabric, semplificano la distribuzione, l'isolamento e la gestione dei componenti della rete.
- GoLang: dato che Hyperledger Fabric è scritto principalmente nel linguaggio di programmazione Go è necessario avere GoLang installato per poter compilare e gestire il codice sorgente.
- Node.js: che viene utilizzato da molti strumenti di gestione e per le interfacce utente ed è quindi necessaria la sua installazione.
- Python: è necessaria la sua installazione per configurare alcuni script e strumenti ausiliari utili.
- Librerie OpenSSL: per poter utilizzare la crittografia per garantire la sicurezza delle comunicazioni e la gestione delle chiavi in un sistema Hyperledger Fabric, è quindi richiesta l'istallazione di tali librerie.

5.1.2 Memoria esterna

Un'alternativa da valutare per la memorizzazione dei dati è quella dell'implementazione di chaincode che interagiscano con un database esterno che potrebbe essere sia un database relazionale che NoSQL in base alle specifiche esigenze. Il chaincode, che in questo caso avrà il ruolo di intermediario tra la blockchain e il database esterno, avrà il

compito di scrivere, leggere ed aggiornare i dati. Il tutto eseguito tramite una connessione al database implementata da una logica per stabile la stessa utilizzando librerie e driver appositi, questo incluso dentro l'apposito chaincode che avrà al suo interno l'implementazione di adeguate funzioni per permettere la lettura di un database esterno.

Inoltre, garantire la sicurezza per proteggere dati sensibili memorizzati nel database esterno ed evitare accessi non autorizzati è essenziale. Questo è reso possibile dalla crittografia, dall'uso delle chiavi crittografiche per proteggere i dati e andando a gestire gli accessi al chaincode tramite meccanismo di controllo che consentono solo ai partecipanti autorizzati di interagire con il database esterno. Infine, per garantire l'immutabilità dei dati salvati esternamente alla blockchain bisogna implementare strutture di dati come hash crittografici che rendono difficile la modifica dei dati stessi senza causare una variazione nell'hash di riferimento.

5.1.3 Smart contract in Hyperledger Fabric

In Hyperledger Fabric, gli smart contract, chiamati chaincode, rappresentano il cuore dell'applicazione blockchain, definiscono le regole di business che governano le transazioni e le iterazioni all'interno della rete. Il loro utilizzo può essere diviso in tre passaggi fondamentali che di seguito vengono analizzati [45]:

- Sviluppo: è la prima fase, dove i chaincode vengono scritti tramite un linguaggio di programmazione supportato, come Go, Node.js o Java. In questa fase vengono definite le logiche di business e le regole fondamentali che determinano le transazioni ammissibili all'interno della rete. La scrittura del codice, da parte degli sviluppatori avviene seguendo le specifiche richieste dall'applicazione blockchain che deve essere sviluppata.
- Installazione: dopo la fase di scrittura dei chaincode, è necessaria una fase di installazione nella rete blockchain. La rete Hyperledger Fabric, come è già stato presentato, può includere più canali e ognuno dei quali può avere la propria

versione dello smart contract. Il primo passaggio di questa fase è quello di includere il codice sorgente del contratto in un package che a sua volta include tutte le dipendenze necessaria. Dopodiché, il package contenente il chaincode viene installato su ogni nodo peer dello specifico canale su cui si intende utilizzare il contratto. Tramite appositi strumenti di gestione gli operatori della rete eseguiranno l'istallazione sui nodi.

- Attivazione: l'ultima fase del processo è quella di attivazione che avviene subito dopo l'istallazione ed è necessario eseguire una transazione di approvazione che coinvolga tutti i nodi di endorsers del canale. Tali nodi hanno il compito di approvare il chaincode e registrarlo in modo definitivo sulla blockchain. Il primo passaggio per fare partire tale procedura coinvolge un membro autorizzato della rete che deve proporre una transazione per attivare il contratto in questione, la transizione viene quindi inviata a tutti gli endorsers del canale che eseguono il codice per verificare che sia conforme alle regole di consenso del canale. Dopodiché, tali nodi, se ritengono il codice valido, firmano la transizione e in base alla politica di approvazione del canale la transazione diventa valida al raggiungimento del numero adeguato di firme. A questo punto la transazione viene registrata definitivamente sulla blockchain e il chaincode può essere ritenuto valido e disponibile per le operazioni.

Una volta superate queste tre fasi, il chaincode può essere chiamato da altre applicazioni o da utenti autorizzati per eseguire le operazioni che sono definite nel suo codice.

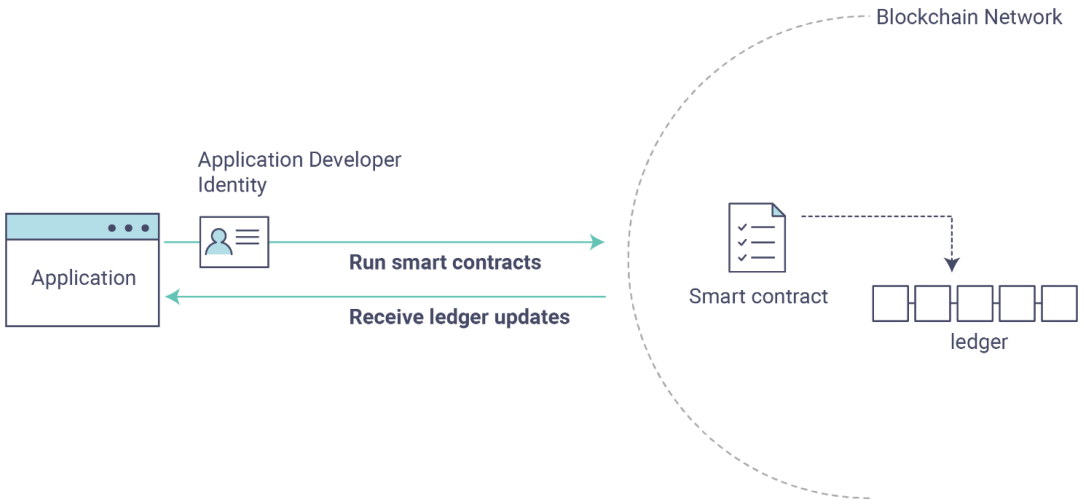

Figura 10. Installazione smart contract.

5.1.4 Interfaccia utente

L'interfaccia utente svolge un ruolo di fondamentale importanza nell'interazione tra gli utenti e la blockchain di Hyperledger Fabric. Avere una buona interfaccia utente semplifica l'accesso alle funzionalità, rendendo più agevole la partecipazione, la consultazione e la gestione delle attività della rete da parte degli utenti. Di seguito vengono analizzate quattro possibili interfacce utente per poter interagire correttamente con la blockchain [46]:

- Applicazioni web: rappresentano un'opzione estremamente flessibile e potente per una corretta interazione con la blockchain. In questo modo viene offerto agli utenti un modo intuitivo per gestire le operazioni e i dati sulla rete combinando l'accessibilità universale che si può avere tramite browser web con la capacità di fornire, allo stesso tempo, un'ampia gamma di funzionalità e un'esperienza utente senza intoppi. L'enorme vantaggio delle applicazioni web risiede nella loro accessibilità, in quanto si può farlo da qualsiasi dispositivo web senza la necessità di dover installare software aggiuntivi, configurazioni complesse o dispositivi con specifici sistemi operativi. Tutto questo è ottimo per garantire un accesso rapido alla blockchain. Le applicazioni web sviluppate per Hyperledger Fabric sono progettate per funzionare come panelli di controllo che offrono agli utenti un'interfaccia centrale per monitorare, esplorare e gestire i dati sulla blockchain. Tali panelli possono essere personalizzati per soddisfare le esigenze specifiche di un'azienda permettendo di eseguire tra le altre cose: la visualizzazione dei dati, la ricerca e la consultazione dei record, la registrazione di nuovi utenti e la gestione degli asset. Per consentire tale iterazione tra utente e blockchain è necessario sviluppare una componente front-end e una back-end. La prima è ciò che vedono gli utenti quando interagiscono con la rete, è quindi essenziale che sia intuitiva, user-friendly e che risponda in modo efficiente alle azioni. La seconda componente, invece, è responsabile della comunicazione con i nodi della blockchain attraverso le API; quindi, è fondamentale che sia in grado

di tradurre le richieste degli utenti nelle corrispondenti operazioni oltre ad essere responsabile della gestione dell'autenticazione e dell'autorizzazione degli utenti.

- Applicazioni mobili: rappresentano un'alternativa per consentire agli utenti di interagire con la blockchain. Tali applicazioni sono estremamente accessibili dato che possono essere facilmente scaricate e utilizzate su smartphone e tablet, consentendo all'utente di accedere alla blockchain ovunque si trovi. Infatti, l'accessibilità e la portabilità sono senza alcun dubbio i due vantaggi principali di tale soluzione, l'utente in questo modo è in grado di accedere alle funzionalità tramite i dispositivi mobili senza dover utilizzare browser web o un computer, ottimo quando esistono situazioni di mobilità. Per un corretto sviluppo di applicazioni mobili per Hyperledger Fabric è necessario avere competenze specifiche per le piattaforme iOS e Android. Le due applicazioni mobili per Apple e Google devono essere sviluppate separatamente su ciascuna piattaforma, gli sviluppatori devono avere familiarità con i linguaggi di progettazione e gli ambienti di sviluppo specifici per ciascuna piattaforma. Questa duplicazione del lavoro rende il processo di sviluppo per le applicazioni mobili più complicato e che richiede più tempo.
- Applicazioni desktop: rappresentano una valida alternativa nella creazione di un'interfaccia utente completa per interagire con la blockchain. Tale soluzione è adatta se è richiesto che l'applicazione sia robusta e altamente personalizzabile in grado di essere eseguita su sistemi operativi diversi. La principale caratteristica distintiva di questa soluzione risiede proprio nell'alto grado di personalizzazione. Gli sviluppatori hanno un controllo significativo sull'aspetto e sul comportamento dell'applicazione, consentendo di adattarla perfettamente alle esigenze degli specifici utenti. Il vantaggio nell'utilizzo di applicazioni desktop è dato dalla capacità di interagire direttamente con la blockchain utilizzando le API, sfruttando completamente tutte le funzionalità della blockchain, inclusa la registrazione di transazioni, la gestione degli asset e la consultazione dei dati. Questo permette un'interazione diretta e potente con la rete, senza la necessità di complesse interfacce di comunicazione. Lo sviluppo di tali applicazioni, tuttavia, richiede competenze specifiche più complesse rispetto a quelle per le applicazioni mobili o web, gli sviluppatori devono avere

familiarità con i linguaggi di programmazione desktop e con gli strumenti specifici di ogni sistema operativo, inoltre è importante porre l'attenzione sulla sicurezza in quanto le applicazioni desktop possono essere esposte più facilmente a minacce locali rispetto a quelle web.

- API RESTful: che consentono di eseguire le operazioni indipendentemente dal formato dell'applicazione, che sia web, mobile o desktop. Le API RESTful svolgono un ruolo fondamentale nell'iterazione tra le interfacce utente e la blockchain, offrendo uno strumento interoperabile per la comunicazione. Le API seguono un'architettura ben definita che si basa su dei principi chiave, tra cui l'uso dell'endpoint, i metodi http e lo scambio di dati nel formato JSON. Questa struttura, essendo standardizzata, rende le API compatibili e facilmente comprensibili per gli sviluppatori, indipendentemente dal linguaggio di programmazione e dalla piattaforma. Tramite API RESTful è possibile eseguire operazioni come: la creazione di transazioni che include la registrazione di dati, la consultazione dei dati interrogando la blockchain, la gestione degli asset e il controllo degli utenti mediante autenticazione o l'autorizzazione.

5.1.5 Gestione sotto-canali, ruoli e responsabilità

In Hyperledger Fabric, essendo una piattaforma open source, è essenziale gestire in modo ottimale i sotto-canali, i ruoli e le responsabilità per garantire sicurezza e una corretta governance della rete. Ad ogni membro della rete va assegnato un ruolo specifico all'interno del canale, questi ruoli possono essere: amministratore, membro o operatore di sotto-canale. I primi, sono i responsabili della corretta configurazione e gestione della rete, hanno il compito di creare canali, installare catene di blocchi, definire le politiche di consenso e gestire l'accesso degli altri membri. I membri invece partecipano alle operazioni di rete eseguendo transazioni, accedendo ai sotto-canali e interagendo con i chaincode. Infine, gli operatori di sotto-canale sono gli attori responsabili della gestione del sotto-canale specifico, essi hanno il compito di definire le

politiche di accesso ed hanno il potere di aggiungere o rimuovere un membro al sotto-canale specifico.

In Hyperledger Fabric i sotto-canali sono utilizzati per separare la rete blockchain, permettendo di creare gruppi di membri in grado di condividere dati e transazioni in modo confidenziale. Per la loro creazione è necessario che un utente con il ruolo di amministratore definisca il sotto-canale specifico nella rete. Aggiungendo i membri e definendo le politiche di accesso. Nel caso analizzato nella tesi il ruolo di amministratore dovrà essere assegnato al responsabile di un determinato progetto, che avrà il compito di creare il sotto-canale specifico e dovrà aggiungere ad esso i membri coinvolti nello sviluppo di tale progetto.

Le politiche di acceso definiscono chi tra i membri di un sotto-canale può accedere allo stesso, eseguire transazioni e interagire con i chaincode. Sarà anche in questo caso compito dell'amministratore di progetto, quello di determinare i permessi dei rispettivi membri in modo tale che possano eseguire transazioni e di definire le condizioni di consenso per la loro approvazione. Ogni utente deve avere quindi nella rete un'identità unica e una coppia di chiavi crittografiche per l'iterazione con la stessa.

5.2 Elementi essenziali

In questo paragrafo vengono presentate quelle procedure necessarie per eseguire la metodologia E6 sulla blockchain. Si cerca di analizzare come fare per caricare un documento, identificare l'identità digitale, firmare un documento o eseguire l'iterazione con un oracolo. Tutte queste procedure sono essenziali per una corretta esecuzione e sono alla base dello svolgimento della metodologia studiata.

5.2.1 Verifica identità digitale

Come già illustrato in precedenza in Hyperledger Fabric la verifica dell'identità digitale è un elemento fondamentale per poter garantire la sicurezza e l'accesso appropriato ai dati. Tale sistema si basa su certificati digitali, ogni partecipante alla rete ne deve possedere uno e tale certificato funziona come prova dell'identità del membro. Tutti i certificati sono emessi da un'entità di fiducia, l'Autorità di Certificazione (CA) e vengono crittografati per motivi di sicurezza sull'identità personale [42].

All'interno di ogni rete di Hyperledger Fabric bisogna avere un proprio Membership Service Provider (MSP) [43], che è il responsabile della gestione dell'identità digitale e definisce le regole per l'aggiunta o la rimozione dei membri oltre ad assegnare i ruoli e le autorizzazioni. Quindi, tutti i ruoli e le autorizzazioni sono gestire dall' MSP, tale meccanismo è essenziale in questo specifico caso di studio per poter stabilire quali membri hanno la possibilità di visionare determinati dati e chi ha il potere di firmare i documenti caricati in attesa di essere validati.

Il sistema di autenticazione e verifica dell'identità digitale è utile anche nell'ambito delle riunioni online. Utilizzando la stessa logica si possono impiegare i certificati digitali per fare in modo che solo i partecipanti autorizzati possano partecipare alle riunioni programmate. Inoltre, mediante l'autenticazione, si riuscirebbe ad effettuare un controllo rigoroso sulla partecipazione che unita all'uso di un oracolo, che verrà presentato in seguito, si riuscirebbe a identificare chi ha preso parte alla riunione e chi invece no. Tutto questo è utile per poter stabile le presenze totali alle riunioni e poter remunerare correttamente tramite token i membri meritevoli.

5.2.2 Oracolo

L'oracolo [47] viene utilizzato come sistema per implementare la verifica e registrazione mensile dei membri che partecipano alle riunioni. Come punto di inizio, è essenziale che in ogni riunione vengano raccolti i dati sulla partecipazione, per fare ciò

deve essere creare una applicazione web o mobile, che consenta ai membri di autenticarsi utilizzando la propria identità digitale in modo da confermare la presenza. A questo punto, entra in gioco l'oracolo, che è un componente esterno al sistema di registrazione delle riunioni, ma ha il compito di verificare le partecipazioni. Infatti, l'oracolo riceve le informazioni di partecipazione da ciascuna riunione e dopo aver effettuato la verifica delle identità ha il compito di registrare i dati sulla blockchain di Hyperledger Fabric. La memorizzazione dei dati può avvenire tramite la creazione di un chaincode, che contiene informazioni sulla partecipazione di ciascun membro, insieme alle relative identità e alle date delle riunioni. I dati, in questo modo, sarebbero immutabili e accessibili con facilità.

Alla fine di ogni mese, in modo automatizzato, tramite l'uso di una applicazione o di uno script appositamente creato, si calcolerebbe facilmente la partecipazione mensile per ogni membro. In questo modo il chaincode incaricato di fare partire la remunerazione dei token avrebbe i dati necessari per calcolare la percentuale di token da inviare ad ogni membro in base alla loro partecipazione alle riunioni programmate.

5.2.3 Caricamento di documenti

Nell'applicazione della metodologia E6 un ruolo importante è dato al caricamento dei documenti, molti dei quali sono nel formato A3, tali documenti inoltre devono essere caricati rispettando una data di scadenza predeterminata. Per fare ciò c'è bisogno di un'applicazione front-end che consentirebbe agli utenti di caricare i documenti desiderati e di inviare la richiesta al chaincode. A questo punto è compito del contratto caricare il documento come transazione nella blockchain includendo al suo interno la data di caricamento e altri dettagli utili. L'utente in questo caso non avrà altri compiti, perché sarà il chaincode appositamente creato a verificare che la data di caricamento sia antecedente a quella di scadenza. Con questi dati a disposizione il contratto scritto appositamente per remunerare i membri al caricamento del documento avrebbe tutto ciò che occorre per inviare i token.

Una considerazione importante va fatta su quanto riguarda l'accesso e la sicurezza dei dati, come spiegato anche nei paragrafi precedenti questo è garantito attraverso meccanismi di controllo sugli accesi che si basano sulle chiavi crittografiche e l'identità digitale, che consentono ai soli utenti autorizzati di caricare o visualizzare i documenti in questione.

5.2.4 Firmare documenti

Legato alla procedura di caricare i documenti sulla blockchain vi è il discorso sulla validazione e l'approvazione da parte dei membri responsabili del progetto, che devono apporre la loro firma digitale sullo stesso. Per fare ciò è senza dubbio essenziale che i membri incaricati abbiano autorizzazioni specifiche per accedere ai documenti e successivamente verificarli, validarli e firmarli digitalmente. Questo è possibile stabilendo chiaramente i ruoli e le autorizzazioni all'interno della blockchain. Ogni documento caricato dovrà essere contrassegnato con la dicitura: "in attesa di approvazione", in modo tale che i membri incaricati della validazione possano individuare facilmente i documenti che richiedono la loro attenzione. Il revisore utilizzando una applicazione front-end visualizzerà il documento in esame, se lo riterrà opportuno a questo punto apporrà la sua firma digitale, oltre che aggiungere eventualmente commenti sulla qualità e sulla completezza del documento. Ogni firma digitale e il relativo timestamp associato verrà registrato come parte della transazione su blockchain garantendo quindi facilità nel tracciamento. In questo modo il chaincode implementato per inviare i token può procedere alla remunerazione quando lo stato del documento cambia da "in attesa di approvazione" a "firmato", inoltre per i documenti che lo richiedono può calcolare la percentuale di token da inviare in base al commento sull'accuratezza.

Anche in questo caso va posta grande attenzione sulla sicurezza dei dati, inoltre è importante garantire che l'accesso ai dati e la conseguente possibilità di firma sia data solo ai membri autorizzati e che hanno il compito di revisionare il progetto. Per

velocizzare il processo si potrebbe pensare di implementare un sistema di notifiche automatiche per informare i responsabili di progetto quando è necessario il loro intervento essendoci un documento in attesa di validazione.

5.3 Gestione dei Token

In questo paragrafo viene spiegato come avviene la gestione e il trasferimento dei token. Per fare ciò viene utilizzato Hyperledger FireFly, una piattaforma open-source di gestione dei token basata su blockchain. Tramite la quale è possibile creare, tracciare e gestire l'uso di tali valute digitali in modo sicuro ed efficiente [25].

Il primo passo da compiere a tale scopo consiste nella configurazione di Hyperledger Fabric, in quando deve essere creato e definito un indirizzo principale che avrà il compito di cassa aziendale di Thales Alenia Space. Tale indirizzo deterrà inizialmente tutti i token creati e da esso partiranno tutte le transizioni verso i membri. Il token può essere creato tramite Hyperledger FireFly, che consente un alto grado di personalizzazione, offrendo un controllo completo sulle caratteristiche, tra cui quelle fondamentali che il token sia divisibile in una frazione e che rimanga fisso nel tempo senza oscillare di valore. Inoltre, durante la creazione deve essere assegnato un nome significativo e un simbolo che riflettano appieno l'identità aziendale. Un esempio potrebbe essere "Space Token" come nome e "TAST" acronimo di Thales Alenia Space Token come simbolo.

Una volta creato il token, dovranno essere implementati chaincode, tale codice avrà il compito di definire la logica di distribuzione al verificarsi di determinati fattori, che altro non sono il corretto eseguimento della metodologia E6 già analizzata nei capitoli precedenti. In tale codice dovrà essere associato l'indirizzo principale dell'azienda da cui parte la distribuzione e l'indirizzo dei membri a cui deve arrivare il token non appena compiono azioni specifiche all'interno della blockchain. Per fare ciò è necessario che ogni membro abbia associato al proprio indirizzo un wallet virtuale,

dotato di un sistema di accesso robusto mediante funzionalità di autenticazione per garantire la sicurezza.

Tramite Hyperledger FireFly è inoltre possibile avere a disposizione una serie di strumenti utili per il monitoraggio e la tracciabilità dei token, che permetto di tenere traccia dei saldi dei wallet dei vari membri e di registrate ogni transazione sulla blockchain garantendo la trasparenza nella rete.

5.3.1 Welfare aziendale

I membri tra di loro non possono scambiarsi i token ma è previsto un sistema per il trasferimento degli stessi verso l'indirizzo principale al raggiungimento di una determinata soglia. L'implementazione di questo meccanismo di scambio di token può essere gestita tramite un chaincode simile a quello definito in precedenza e che verifichi i requisiti di soglia minima per fornire i relativi benefit. Quella di fornire benefit è una pratica comune in molte aziende come forma di incentivo per i propri membri. La scopo principale della restituzione dei token, in questo caso, è quello del ricevere welfare aziendali che possono assumere diverse forme. Un esempio di benefit aziendale comunemente usato è quello dell'ottenere sconti su prodotti, servizi o programmi di benessere. Un altro possibile utilizzo potrebbe essere quello di offrire ferie aggiuntive o ore di permesso come ricompensa per l'accumulo di token, oppure potrebbe essere utilizzato per accedere a corsi di formazione e opportunità di sviluppo professionale sponsorizzati dall'azienda. Questi sono solo alcuni degli esempi di possibili utilizzi del welfare aziendale, per una sua implementazione serve una discussione a livello di alta direzione e del dipartimento risorse umane per capire quale sia il più appropriato per l'azienda.

5.4 Esempio di chaincode

Di seguito viene riportato, a titolo di esempio, lo schema per scrivere un semplice chaincode, tale codice presenta gli opportuni commenti per capire meglio i passaggi logici che stanno dietro la sua scrittura. Quello mostrato di seguito costituisce la base di partenza per sviluppare un chaincode per verificare lo stato del documento da caricare su blockchain, verificando la data di scadenza e se è stato revisionato. In caso affermativo avviene il trasferimento del token dall'indirizzo principale a quello di un membro.

```
package main
import (
	"encoding/json"
	"fmt"
	"strconv"
	"time"
	"github.com/hyperledger/fabric/core/chaincode/shim"
	pb "github.com/hyperledger/fabric/protos/peer"
)
// Document rappresenta un documento con data di scadenza e stato di revisione
type Document struct {
	ID	string	`json:"id"`
	ExpiryDate	time.Time `json:"expiry_date"`
	Reviewed	bool	`json:"reviewed"`
	Owner	string	`json:"owner"`
	TokenAmount int	`json:"token_amount"`
}

// TokenChaincode implementa il chaincode per la gestione dei documenti e dei token
type TokenChaincode struct {
}
func (t *TokenChaincode) Init(stub shim.ChaincodeStubInterface) pb.Response {
	fmt.Println("Chaincode initialized")
	return shim.Success(nil)
}
func (t *TokenChaincode) Invoke(stub shim.ChaincodeStubInterface) pb.Response {
	function, args := stub.GetFunctionAndParameters()
	if function == "uploadDocument" {
		return t.uploadDocument(stub, args)
	} else if function == "reviewDocument" {
		return t.reviewDocument(stub, args)
	} else if function == "transferTokens" {
		return t.transferTokens(stub, args)
	} else if function == "getDocument" {
		return t.getDocument(stub, args)
	}
```

```
        return shim.Error("Function not found")
}
// uploadDocument carica un nuovo documento con data di scadenza

func (t *TokenChaincode) uploadDocument(stub shim.ChaincodeStubInterface, args []string)
pb.Response {
            if len(args) != 3 {
                    return shim.Error("Incorrect number of arguments. Expecting 3: DocumentID,
ExpiryDate, Owner")
            }
            documentID := args[0]
            expiryDate, err := time.Parse(time.RFC3339, args[1])
            if err != nil {
                    return shim.Error(fmt.Sprintf("Failed to parse expiry date: %s", err))
            }
            owner := args[2]
            document := Document{
                        ID:          documentID,
                        ExpiryDate:  expiryDate,
                        Reviewed:    false,
                        Owner:       owner,
                        TokenAmount: 0,
            }
            documentJSON, err := json.Marshal(document)

            if err != nil {
                        return shim.Error(fmt.Sprintf("Failed to marshal document: %s", err))
            }
            err = stub.PutState(documentID, documentJSON)

            if err != nil {
                        return shim.Error(fmt.Sprintf("Failed to upload document: %s", err))
            }

            return shim.Success(nil)
}

// reviewDocument segna un documento come revisionato

func (t *TokenChaincode) reviewDocument(stub shim.ChaincodeStubInterface, args []string)
pb.Response {
            if len(args) != 1 {
                    return shim.Error("Incorrect number of arguments. Expecting 1: DocumentID")
            }
            documentID := args[0]
            documentJSON, err := stub.GetState(documentID)
            if err != nil {
                    return shim.Error(fmt.Sprintf("Failed to get document: %s", err))
            }
             if documentJSON == nil {
                    return shim.Error("Document not found")
            }
            var document Document
            err = json.Unmarshal(documentJSON, &document)
```

```
        if err != nil {
                return shim.Error(fmt.Sprintf("Failed to unmarshal document: %s", err))
        }
        if document.Reviewed {
                return shim.Error("Document already reviewed")
        }

        document.Reviewed = true
        updatedDocumentJSON, err := json.Marshal(document)
        if err != nil {
                return shim.Error(fmt.Sprintf("Failed to marshal updated document: %s", err))
        }

        err = stub.PutState(documentID, updatedDocumentJSON)
        if err != nil {
                return shim.Error(fmt.Sprintf("Failed to update document: %s", err))
        }
        return shim.Success(nil)
}
// transferTokens trasferisce token dall'indirizzo principale all'utente

func (t *TokenChaincode) transferTokens(stub shim.ChaincodeStubInterface, args []string) pb.Response {
        if len(args) != 2 {
                return shim.Error("Incorrect number of arguments. Expecting 2: ToUser, TokenAmount")
        }
        toUser := args[0]
        tokenAmount, err := strconv.Atoi(args[1])
        if err != nil {
                return shim.Error(fmt.Sprintf("Failed to parse token amount: %s", err))
        }

        // Qui verrebbe implementata la logica per verificare se l'utente ha diritto al trasferimento
        // Esegue il trasferimento dei token
        // Ad esempio, si può usare un registro di account per tenere traccia dei token degli utenti
        // e quindi aggiornare l'account dell'utente destinatario

        return shim.Success(nil)
}

// getDocument ottiene un documento

func (t *TokenChaincode) getDocument(stub shim.ChaincodeStubInterface, args []string) pb.Response {
        if len(args) != 1 {
                return shim.Error("Incorrect number of arguments. Expecting 1: DocumentID")
        }

        documentID := args[0]
        documentJSON, err := stub.GetState(documentID)
        if err != nil {
                return shim.Error(fmt.Sprintf("Failed to get document: %s", err))
        }
        if documentJSON == nil {
                return shim.Error("Document not found")
        }
        return shim.Success(documentJSON)
}
func main() {
```

```
	err := shim.Start(new(TokenChaincode))
	if err != nil {
		fmt.Printf("Error starting chaincode: %s", err)
	}

}
```

Capitolo 6 - Conclusione

In questa tesi sono stati trattati vari argomenti riguardante la blockchain, una tecnologia emergente che si sta facendo strada velocemente nel panorama mondiale anche se, attualmente, sono in pochi a sapere realmente di cosa si tratta e merita, quindi, una divulgazione più approfondita. Inizialmente sono stati presentati i componenti principali che la compongono in modo da fare un'analisi generale sulla tecnologia per poi potersi dedicare alla presentazione di una particolare blockchain, quella di Hyperledger Fabric andando ad evidenziane punti di forza e sfide necessarie da affrontare per una sua implementazione.

Successivamente è stato proposto un Proof of Concept incentrato sull'utilizzo della blockchain Hyperledger Fabric per implementare un sistema di distribuzione di token al raggiungimento di determinati obbiettivi nell'eseguimento di una pratica aziendale chiamata E6, sviluppata da Thales Alenia Space, società interessata allo svolgimento di tale tesi. La discussione si è limitata a dimostrare la fattibilità teoria di tale tecnologia applicata in un contesto aziendale, questa analisi avrà bisogno di sviluppi futuri per una dimostrazione pratica eseguendo dei test e delle prove di costruzione della blockchain stessa. Inoltre, tale sistema di remunerazione può essere replicato ad altri contesti per poter incentivare la trasformazione digitale adottando nuove pratiche lavorative o applicandolo in un sistema per il controllo delle valutazioni che va a verificare il lavoro dei dipendenti.

Attualmente la tecnologia blockchain si può ritenere ancora giovane, solo negli ultimi anni ha suscitato l'interesse da parte di aziende che in modo graduale hanno provato una sua integrazione nei sistemi già in uso. In letteratura sono presente esempi non ancora completamente testati o funzionanti, spesso limitati ad una analisi teorica in attesa di una eventuale implementazione. In tale contesto in cui si sono sviluppate molteplice blockchain, con funzioni e scopi diversi, il consorzio di Hyperledger si è dimostrato il più maturo per una implementazione aziendale. Grazie all'enorme grado di flessibilità e modularità che il sistema garantisce è possibile adattare il sistema alle proprie esigenze senza dover rinunciare alla sicurezza e l'immutabilità per cui la tecnologia blockchain è nata. Per affrontare la sfida di costruire una propria blockchain utilizzando il framework

di Hyperledger Fabric bisogna avere un team di sviluppo con solide basi di conoscenza sulla blockchain, sui linguaggi di programmazioni specifici e sul sistema adottato. È quindi necessario investire grandi risorse in formazione senza dimentica di non sottovalutare l'aggiornamento, dato che è una tecnologia in continua mutazione che si sta sviluppando giorno per giorno. Questo è il principale scoglio su cui si sono arenati numerosi progetti che volevano utilizzare tale piattaforma, ma dall'analisi di questa tesi è emerso che una volta superati queste sfide iniziali i vantaggi sarebbero innumerevoli. Potendo sfruttare a pieno tutti i vantaggi della blockchain, come l'immutabilità, la sicurezza, la tracciabilità, l'automatizzazione e la trasparenza oltre che favorire la messa in pratica di una metodologia essenziale per lo sviluppo dei progetti in Thales Alenia Space.

Durante lo svolgimento di tale tesi, è stato dimostrato che è possibile utilizzare la blockchain per remunerare i membri dell'azienda tramite token in base alla corretta esecuzione della metodologia E6. Inoltre, è attuabile eseguire i passi di tale metodologia tramite la tecnologia proposta in modo tale da raggiungere una maggiore tracciabilità, condivisione, sicurezza e automatizzazione del processo.

Acronimi

E6: E sta per Engineering (ingegneria) e 6 sono i pilastri su cui si fonda la metodologia.

ESA: European Space Agency, che in italiano significa Agenzia Spaziale Europea.

NASA: National Aeronautics and Space Administration, che in italiano significa Amministrazione Nazionale per l'Aeronautica e lo Spazio.

PoW: Proof of Work, che in italiano significa Prova del Lavoro.

PoS: Proof of Stake, che in italiano significa Prova della Partecipazione.

DPoS: Delegated Proof of Stake, che in italiano significa Prova della Partecipazione Delegata.

BFT: Byzantine Fault Tolerance, che in italiano significa Tolleranza ai Guasti Bizantini.

PBFT: Practical Byzantine Fault Tolerance, che in italiano significa Tolleranza ai Guasti Bizantini Pratica.

SBFT: Simplified Byzantine Fault Tolerance, che in italiano significa Tolleranza ai Guasti Bizantini Semplificata.

FBA: Federated Byzantine Agreement, che in italiano significa Accordo Bizantino Federato.

CFT: Crash Fault Tolerance, che in italiano significa Tolleranza ai Guasti per Arresto Improvviso.

NFT: Non-Fungible Tokens, che in italiano significa Token Non Fungibile.

DeFi: Decentralized Finance che in italiano significa Finanza Decentralizzata.

SDK: Software Development Kit, che in italiano significa Kit di Sviluppo Software.

API: Application Programming Interface, che in italiano significa Interfaccia di Programmazione Applicativa.

MSP: Membership Service Provider, che in italiano significa Fornitore di Servizi di Associazione.

CA: Certificate Authority, che in italiano significa Autorità di Certificazione.

SQL: Structured Query Language, che in italiano significa Linguaggio di Query Strutturato.

ERC-20: Ethereum Request for Comments 20, che in italiano significa Standard Ethereum 20.

KVA: Key Value Attribute, che in italiano significa Attributi dal Valore Chiave.

KPI: Key Performance Indicators, che in italiano significa Indicatori Chiave di Prestazione.

CID: Causal Influence Diagrams, che in italiano significa Diagramma di Influenza Causale.

KDT: Key Decision Tree, che in italiano significa Albero delle Decisioni Chiave.

KD: Key Decision, che in italiano significa Decisione Chiave.

KG: Knowledge Gap, che in italiano significa Gap di Conoscenza.

RACI: Responsible Accountable Consulted Informed, che in italiano significa Responsabile Accountable Consultato Informato.

RAM: Random Access Memory, che in italiano significa Memoria di Accesso Casuale.

Riferimenti

[1] Wikipedia, https://it.wikipedia.org/wiki/Thales_Alenia_Space

[2] Thales Group, https://www.thalesgroup.com/it/global/activities/space

[3] Thales Alenia Space, https://www.thalesaleniaspace.com/it

[4] L. Simonini, E. De Stefanis, M. Buonocore, G. Gans, “Lesson Learned and Road Map for Lean Process and Product Development Adoption in Early Engineering Phases in Thales Alenia Space”

[5] Young Platform Accademy, https://academy.youngplatform.com/blockchain/blockchain-internet-innovazione/

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", https://bitcoin.org/bitcoin.pdf

[7] É.R. Keresztes, I. Kovács, A Horváth, K Zimányi, “Exploratory Analysis of Blockchain Platforms in Supply Chain Management”

[8] Young Platform Accademy, https://academy.youngplatform.com/blockchain/le-6-verita-della-tecnologia-blockchain/

[9] Young Platform Accademy, https://academy.youngplatform.com/blockchain/crittografia-funzione-hash-blockchain/

[10] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, S. Shiaeles,”On the Suitability of Blockchain Platforms for IoT Applications: Architectures, Security, Privacy, and Performance”

[11] S. Nanayakkara, M.N.N. Rodrigo, S. Perera, G.T. Weerasuriya, A.A. Hijazi, “A methodology for selection of a Blockchain platform to develop an enterprise system, Journal of Industrial Information Integration (2021)”, https://doi.org/10.1016/j.jii.2021.100215

[12] V. Capocasale, G. Danilo, G. Perboli, “Comparative analysis of permissioned blockchain frameworks for industrial applications, Blockchain: Research and Applications (2022)”, https://doi.org/10.1016/j.bcra.2022.100113

[13] M. Dabbagh, K. R. Choo, A. Beheshti, M. Tahir,N. S. Safad,” A Survey of Empirical Performance Evaluation of Permissioned Blockchain Platforms: Challenges and Opportunities”

[14] Young Platform Accademy, https://academy.youngplatform.com/blockchain/smart-contract-ethereum-come-funzionano/

[15] Hyperledger Foundation, https://www.hyperledger.org/

[16] Hyperledger Fabric, https://hyperledger-fabric.readthedocs.io/en/release-2.5/whatis.html

[17] T. Parth, N.N. Senthil, V. Balaji, “Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform “

[18] V. Sumit, “Hyperledger Fabric — Part 1 — Components and Architecture”, https://blog.clairvoyantsoft.com/hyperledger-fabric-components-and-architecture-b874b36c4af5

[19] Hyperledger Fabric, https://hyperledger-fabric.readthedocs.io/en/latest/network/network.html

[20] KC Tam, “Demo of Multi-Channel Network in Hyperledger Fabric”, https://kctheservant.medium.com/demo-of-multi-channel-network-in-hyperledger-fabric-640f7158e2d3

[21] Hyperledger Fabric, https://hyperledger-fabric.readthedocs.io/en/latest/ledger/ledger.html

[22] J. Polge, J. Robert, Y. Le Traon, “Permissioned blockchain frameworks in the industry: A comparison”, http://www.elsevier.com/locate/icte

[23] Hyperledger FireFly, https://hyperledger.github.io/firefly/

[24] Young Platform Accademy, https://academy.youngplatform.com/blockchain/cosa-sono-token-ethereum-standard-erc20/

[25] Hyperledger FireFly, https://hyperledger.github.io/firefly/v1.2.0/tutorials/tokens/erc20.html

[26] Hyperledger Foundation, https://www.hyperledger.org/learn/white-papers

[27] Hyperledger Foundation, https://www.hyperledger.org/projects/fabric

[28] State Street Corp. , IBM, “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains”

[29] Aswin, A.V., Kuriakose, B. (2020). “An Analogical Study of Hyperledger Fabric and Ethereum”, https://link.springer.com/chapter/10.1007/978-3-030-28364-3_41

[30] Hyperledger, https://hyperledger.blocktech.it/privacy-riservatezza

[31] J. Dharani, K. Sundarakantham, S. KunwaR, S. Mercy, “A Privacy-Preserving Framework for Endorsement Process in Hyperledger Fabric”, https://www.sciencedirect.com/science/article/abs/pii/S0167404822000360

[32] Q. Nasir, I. A. Qasse, M. A. Talib and A. B. Nassif, "Performance Analysis of Hyperledger Fabric Platforms"

[33] M. Kuzlu, M. Pipattanasomporn, L. Gurses and S. Rahman, "Performance Analysis of a Hyperledger Fabric Blockchain Framework: Throughput, Latency and Scalability "

[34] K. Yamashita, Y. Nomura, E. Zhou, B. Pi e S. Jun, "Potential Risks of Hyperledger Fabric Smart Contracts

[35] C. Balducci, F. Fraccaroli, “Stress lavoro-correlato: questioni aperte e direzioni future”, https://www.rivisteweb.it/doi/10.1421/93768

[36] D. Dunning, C. Heath, J. M. Suls, “Immagine imperfetta”

[37] Unobravo, “La sindrome dell’impostore: quando un bugiardo fa carriera”, https://www.unobravo.com/post/la-sindrome-dellimpostore-e-il-mondo-del-lavoro-quando-un-bugiardo-fa-carriera

[38] PMI, "La tecnologia blockchain permette di ridurre i costi e accrescere la trasparenza", https://www.kmu.admin.ch/kmu/it/home/attualita/interviste/2017/la-tecnologia-blockchain-permette-di-ridurre-i-costi-e-accrescere-la-trasparenza.html#

[39] J. Sedlmeir, H.U. Buhl, G. Fridgen, R. Keller,” The Energy Consumption of Blockchain Technology: Beyond Myth”, https://link.springer.com/article/10.1007/s12599-020-00656-x#Abs1

[40] The European Union Blockchain Observatory & Forum “Energy Efficiency of Blockchain Technologies”,https://www.eublockchainforum.eu/sites/default/files/reports/Energy%20Efficiency%20of%20Blockchain%20Technologies_1.pdf

[41] Khan, S.N., Loukil, F., Ghedira-Guegan, “Blockchain smart contracts: Applications, challenges, and future trends”, https://link.springer.com/article/10.1007/s12083-021-01127-0, G. Adonopoulos “Smart contract: cosa sono e come funzionano”

[42] Hyperledger Fabricdocs, https://hyperledger-fabric.readthedocs.io/en/latest/deployment_guide_overview.html

[43] Hyperledger Fabricdocs, https://hyperledger-fabric.readthedocs.io/en/latest/ops_guide.html

[44] Hyperledger Fabricdocs, https://hyperledger-fabric.readthedocs.io/en/latest/gateway.html

[45] Hyperledger Fabricdocs, https://hyperledger-fabric.readthedocs.io/en/release-1.3/tutorials.html

[46] M. Pustišek, A.Kos, “Approaches to Front-End IoT Application Development for the Ethereum Blockchain”

[47] V. Mou, “Gli Oracoli Blockchain Spiegati”, https://academy.binance.com/it/articles/blockchain-oracles-explained