POR-FESR EMILIA ROMAGNA 2014-2020

Asse 1 - Ricerca e innovazione

Azione 1.2.2 - Supporto alla realizzazione di progetti complessi di attività di ricerca e sviluppo su poche aree tematiche di rilievo e all'applicazione di soluzioni tecnologiche funzionali alla realizzazione della strategia di S3

Bando 2018

Progetti di ricerca industriale strategica rivolti agli ambiti prioritari della Strategia di Specializzazione Intelligente

Sistemi interoperabili ed efficienti per la gestione sicura di filiere industriali

Deliverable D2.1:
Analisi dello stato dell'arte delle piattaforme blockchain

Data di consegna prevista:	31 Gennaio 2020
Autori:	CIRI ICT, CRIS, CROSSTEC, MECLAV
Versione:	1

Indice

1. Introduzione

Nell'ultimo decennio abbiamo assistito sempre più alla transizione da sistemi di elaborazione e archiviazione centralizzati a sistemi e architetture decentralizzate. Il Distributed Ledger Technology (DLT) è una delle tecnologie chiave esemplificative di questa transizione. DLT è un tipo di struttura di dati digitali residente su più dispositivi informatici, generalmente dislocati in località geografiche distinte.

Una delle evoluzioni più conosciute del DLT è la blockchain, definita come un registro digitale immutabile e integro e strutturato come un insieme di blocchi di dati concatenati in ordine cronologico. La crittografia consente alle blockchain di superare i precedenti DLT offrendo l'immutabilità dei record in un ambiente decentralizzato. La blockchain segna la convergenza di un insieme di tecnologie esistenti come timestamp delle transazioni, reti P2P, crittografia e computazione condivisa e consente la condivisione e la memorizzazione dei dati senza affidare ad alcuna parte centralizzata la manutenzione del libro mastro.

Nei sistemi convenzionali di archiviazione centralizzata dei dati solo un'entità, il proprietario o l'amministratore, conserva una copia del database. Di conseguenza, questa entità controlla quali dati vengono forniti e quali entità sono autorizzate a contribuire. Con l'avvento della blockchain questo approccio cambia radicalmente a favore dell'archiviazione di dati distribuiti in cui più entità detengono una copia del database sottostante e sono autorizzati a contribuire. I dati vengono replicati su tutte le entità partecipanti alla rete della blockchain chiamati peer. A causa della natura distribuita della blockchain, il principale problema risulta essere la difficoltà nel garantire che tutti i nodi concordino su una verità comune, cioè sulla correttezza dei dati inseriti nel DLT e propagati a tutti gli altri peer nella rete. Questa verità comune raggiunta viene definita come consensus tra i nodi.

In particolare, l'architettura Blockchain [2] è una rete di nodi che condividono uno stato comune. Essa e i relativi protocolli sono progettati in modo tale che, in qualsiasi momento, la maggior parte dei nodi deve concordare sullo stato di una blockchain stessa. Le modifiche allo stato di una blockchain sono registrate come una serie (chain) di gruppi di transazioni (block): ogni transazione si riferisce a un utente specifico (identificato da un identificatore univoco) e a un momento specifico (timestamp). Blockchain in genere agisce come un registro distribuito generico di transazioni che garantisce alcune caratteristiche chiave, quali:

- Non ripudio: ogni transazione che gli utenti registrano sulla blockchain diventa automaticamente non ripudiabile, ad es. una volta effettuata una transazione, l'utente che effettivamente ha eseguito la transazione non avrà la possibilità di negare la propria responsabilità in merito alla transazione stessa;

- Irreversibilità: ogni transazione effettuata dagli utenti sulla blockchain diventa automaticamente irreversibile, ad esempio agli utenti non è consentito annullare o modificare una transazione;
- Timestamp delle transazioni: qualsiasi transazione avviene in un determinato momento, è registrato dalla blockchain in modo non modificabile e sempre identificabile;
- Resistenza alla censura: le singole transazioni e lo stato di un sistema a seguito di una serie di transazioni non può essere negato e sono sempre disponibili al pubblico e verificabile.

Le funzionalità appena elencate rendono blockchain un libro mastro distribuito che autentica gli eventi e li rende universalmente, perennemente accessibile e non ripudiabili.

Blockchain non è semplicemente una tecnologia ma può essere considerato un paradigma/stile architetturale. La prima specifica blockchain è stata quella Bitcoin, rilasciato nel 2008; da allora sono emerse molte altre implementazioni blockchain, con caratteristiche molto diverse. La blockchain Bitcoin è stata considerata l'implementazione di riferimento del paradigma blockchain. Il principale punto di forza di Bitcoin è stato quello di risolvere il problema dei Generali Bizantini che è un classico problema affrontato da qualsiasi rete di un sistema distribuito e approfondito nel capitolo II. L'implementazione originale di Bitcoin si basa su hashcash, un algoritmo di Proof of Work. È un approccio intelligente per raggiungere un consenso distribuito fornendo una forte protezione dagli attacchi con forza bruta, raggiungendo l'affidabilità complessiva del sistema in presenza di una serie di processi “faulty”. Un algoritmo di Proof of Work ha due forti implicazioni: ha bisogno di una grande quantità di energia per funzionare e rende più difficile fornire risultati in tempo reale, poiché è distribuito su un numero elevato e sempre crescente di nodi, e si basa sull'elaborazione casuale ad alta intensità di calcolo. A causa di queste limitazioni, dal rilascio di Bitcoin sono stati fatti molti tentativi per evitare tutto ciò. Queste implicazioni pongono forti limiti al throughput delle transazioni e significativi costi operativi della rete. Le soluzioni proposte si concentrano sul miglioramento delle prestazioni e sulla riduzione dei costi: le modifiche più significative si concentrano sulla centralizzazione del processo di convalida della transazione e sull'adozione di un algoritmo di consenso non basato sul principio della forza bruta computazionale. Questi “miglioramenti” possono essere considerate come una sorta di rilassamento dei vincoli dell'architettura blockchain Bitcoin originale; questi rilassamenti non sono necessariamente una limitazione, ma dovrebbero essere attentamente presi in considerazione quando si determina quale tipo di blockchain si adatta maggiormente alle esigenze aziendali e al contesto.

Sono state proposte alcune categorizzazioni al fine di semplificare la comprensione dei tipi di blockchain:

- Blockchain "Bitcoin-like": blockchain con algoritmo di consenso distribuito e cronologia delle transazioni persistenti in una catena di blocchi matematicamente collegati; quelle sono le blockchain che implementano l'idea originale della blockchain così come è stata proposta da Bitcoin e il loro focus è sull'immutabilità della cronologia delle transazioni e sulla coerenza rispetto al throughput delle transazioni;
- Blockchain "Enterprise": caratterizzati da una centralizzazione delle funzionalità principali come la convalida delle transazioni, la creazione di blocchi e il servizio di denominazione; l'accento è posto su aspetti di governance come la regolamentazione dell'accesso e i meccanismi di riservatezza;
- Distributed Ledger Technology (DLT): lo stato è condiviso tra i nodi della rete, ma non è implementata alcuna catena di blocchi. Altre misure sono stabilite al fine di imporre l'immutabilità delle transazioni, ma l'attenzione è rivolta alle prestazioni al fine di raggiungere la distribuzione delle informazioni quasi in tempo reale nella rete.

Blockchain - e DLT - possono anche essere classificati in base al modello di governance, ovvero la possibilità di accedere alla blockchain con o senza l'autorizzazione di un servizio di emissione di account remoto. Ci sono due principali modalità di funzionamento: permissionless e permissioned spesso indicate in letteratura rispettivamente come blockchain pubblica e privato. Nella prima modalità, la partecipazione è pubblica e ad accesso aperto: chiunque è consentito partecipare alla rete e ai processi di consensus; questa modalità è tipicamente quella adottata dalla prima generazione blockchain (ad esempio Bitcoin). Nella seconda modalità, invece, la partecipazione deve essere autorizzata e i partecipanti hanno delle restrizioni in scrittura (convalida dei blocchi) oppure sia in scrittura che lettura.

2. Consensus Algorithm and Smart Contract

2.1. Algoritmi di Consenso

La parola "consenso" si riferisce alla convergenza su una scelta comune ed è realizzata attraverso un insieme di interazione che gli agenti del sistema distribuito devono eseguire per raggiungere uno stato condiviso. Esso è una caratteristica molto importante per la classificazione delle blockchain.

Raggiungere il consenso in modo sicuro ed efficiente sulle reti distribuite non è un obiettivo semplice da raggiungere. Alcuni nodi infatti possono essere soggetti al fallimento o peggio agire in modo disonesto. Quindi, come può una rete distribuita di nodi concordare su una decisione in modo sicuro? Questa è la domanda fondamentale del cosiddetto problema dei generali bizantini, che ha dato vita al concetto di “Byzantine Fault Tolerance” (BFT - tolleranza ai guasti bizantini).

Il Problema dei generali bizantini è stato concepito nel 1982 come un dilemma logico che illustra come un gruppo di generali bizantini possa avere problemi di comunicazione quando cercano di concordare la loro prossima mossa. Il dilemma presuppone che ogni generale abbia il proprio esercito e che ogni gruppo sia situato in luoghi diversi intorno alla città che intende attaccare. I generali devono accordarsi sull'attacco o sulla ritirata. Non importa se attaccano o si ritirano, purché tutti i generali raggiungano il consenso, cioè concordino una decisione comune al fine di eseguirla in coordinamento. Pertanto, possiamo considerare i seguenti requisiti:

- Ogni generale deve decidere: attacco o ritirata (sì o no);
- Dopo che la decisione è stata presa, non può essere modificata;
- Tutti i generali devono concordare la stessa decisione ed eseguirla in modo sincronizzato.

I suddetti problemi di coordinazione sono legati al fatto che un generale è in grado di comunicare con un altro solo tramite messaggi, che vengono inoltrati da un corriere. Di conseguenza, la sfida centrale del problema dei generali bizantini è che i messaggi possono in qualche modo essere ritardati, distrutti o persi. Inoltre, anche se un messaggio viene recapitato correttamente, uno o più generali possono scegliere (per qualsiasi motivo) di agire in modo dannoso e inviare un messaggio fraudolento per confondere gli altri generali, portando a un fallimento totale. Se applichiamo questo dilemma al contesto delle blockchain, ogni generale rappresenta un nodo di rete e i nodi devono raggiungere il consenso sullo stato corrente del sistema. In altre parole, la maggior parte dei partecipanti all'interno di una rete distribuita deve concordare ed eseguire la stessa azione per evitare un fallimento completo. Pertanto, l'unico modo per

raggiungere il consenso in questi tipi di sistemi distribuiti è avere almeno 2/3 di nodi affidabili e onesti. Ciò significa che se la maggior parte della rete decide di agire in modo dannoso, il sistema è suscettibile a guasti e attacchi (come l'attacco del 51%).

In poche parole, la tolleranza ai guasti bizantina (BFT) è la proprietà di un sistema che è in grado di resistere alla classe di guasti derivati dal problema dei generali bizantini. Ciò significa che un sistema BFT è in grado di continuare a funzionare anche se alcuni dei nodi falliscono o agiscono in modo dannoso. Esiste più di una possibile soluzione al problema dei generali bizantini e, quindi, molteplici modi di costruire un sistema BFT. Allo stesso modo, ci sono diversi approcci per una blockchain per raggiungere la tolleranza ai guasti bizantina e questo ci porta ai cosiddetti algoritmi di consenso.

Le blockchain di prima generazione (es. Bitcoin, Litecoin, Ethereum) sono tipicamente delle blockchain permissionless con un elevato numero di utenti. Esse stabiliscono un consenso tra milioni di utenti mantenendo una visione coerente del sistema tra i partecipanti. La resilienza ai guasti è assicurata dal sistema fintanto che i nodi dannosi rimangono una minoranza nella rete Peer-to-Peer (P2P).

L'idea alla base del primo algoritmo del consenso è di introdurre costi computazionali di tipo Proof-of-Work (PoW) per convalidare un blocco di transazioni. Questo approccio è stato ideato nell’Ottobre del 2008 da Satoshi Nakamoto, inventore della prima blockchain alla base dei bitcoin. I nodi blockchain che mirano a convalidare un blocco di transazioni (ovvero i miners) devono trovare un hash del blocco che soddisfi un determinato requisito di difficoltà. Il vincitore di questa sfida può convalidare il blocco di transazioni creato. I miner vincenti quindi fungono da nodi principali di convalida. Su una blockchain sufficientemente grande, il requisito PoW fornisce effettivamente resistenza ai guasti bizantini (BFT).

Con l'aumento della popolarità delle criptovalute, però, questo tipo di consenso si è rivelato assolutamente poco scalabile, con un’alta latenza ed enorme spreco di risorse computazionali. I punti deboli delle blockchain di prima generazione hanno portato a un'analisi più approfondita della tecnologia sottostante e, in particolare, dell’algoritmo del consenso. Sono così stati progettati una classe di protocolli chiamati PoX indirizzati a blockchain permissionless che consistono nell’elezione di un leader basandosi su di un processo probabilistico.

Il principale algoritmo di questo tipo è conosciuto come Proof of Stake (PoS) è passa da un mining reale ad uno virtuale (ad es. consumo-estrazione gratuita). L'elezione del leader in questo meccanismo è legata allo stake posseduto da ciascun nodo della rete che aumenta la possibilità di essere eletto. La principale blockchain ad adottare questo tipo di algoritmo è stata quella legata ad Ethereum nata tra il 2014 e il 2015.

Esistono diverse varianti del consenso PoS al fine di evitare la centralizzazione tra i nodi più "ricchi" del potere di creazione e convalida dei blocchi. Queste variazioni generalmente si basano sulla stima dello stake detenuto dall'utente oppure su alcuni meccanismi di incentivazione.

Esistono inoltre implementazioni alternative molto performanti come Proof of Elapsed Time (PoET) e Proof of Importance (PoI). Esse combattono contro la tendenza alla centralizzazione (cioè accumulo di monete / risorse) rispettivamente basandosi su un timer casuale per scegliere il leader del round o incentivando i leader ammissibili ad aumentare il flusso e il volume delle loro transazioni nella rete. Inoltre, per essere più efficienti, questi meccanismi possono funzionare con elezioni ristrette, come per esempio Delegated Proof-of-Stake (DPoS).

Vi sono altri tipi di protocolli per il consenso conosciuti come algoritmi BFT-like che funzionano bene nelle blockchain con un numero limitato di partecipanti, quindi non si adattano ai sistemi pubblici ma a quelli chiusi. Gli algoritmi BFT garantiscono sia liveness che sicurezza di una rete a patto che almeno 2/3 dei partecipanti siano onesti. Le diverse varianti basate su BFT funzionano con autorizzazioni aggiuntive sui nodi di convalida. Alcuni esempi di questa categoria sono il Practical BFT (PBFT) e la Proof of Authority (PoA). Esistono inoltre molteplici algoritmi ibridi che hanno come principale fine quello di far scalare facilmente il protocollo.

2.2. Supporto agli Smart Contract

I primi sistemi basati su blockchain erano pensati per la gestione di valute digitali. Tuttavia, un DLT generico può adattarsi a qualsiasi requisito di scambio di risorse (asset) digitali. Ad esempio, gli aspetti contrattuali di uno scambio che coinvolge diritti e obblighi può essere digitalizzato e controllato da contratti digitali chiamati smart contract.

Gli smart contract furono proposti per la prima volta nei primi anni '90 dallo scienziato informatico, avvocato e crittografo Nick Szabo che coniò il termine. Con le attuali implementazioni, tipicamente basate su blockchain, lo smart contract viene utilizzato principalmente in modo più specifico come mezzo di calcolo per scopi generali che si svolge su una blockchain o un libro mastro distribuito.

Uno smart contract è un programma che esegue azioni predefinite quando determinate condizioni all'interno del sistema sono soddisfatte. Gli smart contract possono essere scritti in diversi linguaggi di programmazione che consentono di modificare lo stato del ledger distribuito. Essi facilitano lo scambio e il trasferimento di qualsiasi asset (ad es. azioni, valuta, contenuto, proprietà). Gli Smart Contract risiedono nella struttura della blockchain e vengono attivati insieme alle transazioni. Essi possono essere immaginati

come protocolli digitali utilizzati per facilitare la negoziazione e far rispettare un contratto legale. In questo modo, le azioni eseguite da terzi parti fidate durante uno scambio sono sostituite da pezzi di codice.

La piattaforma che ha principalmente contribuito alla diffusione degli smart contract e allo sviluppo di un supporto avanzato ad essi connesso è stata la blockchain Ethereum. Di seguito un esempio per capire meglio come funziona lo smart contract.

Supponiamo di affittare un appartamento. Lo si può fare attraverso la blockchain pagando in criptovaluta. Si otterrà così una ricevuta contenuta nel contratto virtuale in cui assicuro la consegna della chiave di accesso digitale entro una data specifica. Se la chiave non arriva in tempo, la blockchain rilascia un rimborso. Se invio la chiave prima della data di affitto, la funzione la tiene rilasciando sia la rata d'affitto che la chiave rispettivamente al locatario e al locatore quando arriva la data. Il sistema funziona con la premessa If-Then ed ha come testimoni centinaia di persone quindi ci si può aspettare una consegna senza errori. Se la chiave viene consegnata si è sicuri che sarò pagata. Analogamente, se si invia un determinato importo in bitcoin si riceverà la chiave. Il documento viene automaticamente cancellato dopo il termine e il codice non può essere interferito da nessuno senza che l'altro lo sappia poiché tutti i partecipanti vengono contemporaneamente avvisati.

È possibile utilizzare contratti intelligenti per ogni tipo di situazione che spazia da prodotti finanziari a premi assicurativi, contratti di violazione, diritto di proprietà, controllo del credito, servizi finanziari, procedure legali e accordi di crowdfunding. In Figura 2 possiamo vedere parte del codice per uno smart contract di base che è stato scritto sulla blockchain di Ethereum. In particolare, possiamo vedere la funzione "approve" che permette ad un altro contratto di spendere alcuni token per conto proprio; la funzione "approveAndCall" che approva e poi comunica il contratto approvato; la funzione "transferFrom" che viene chiamata quando un contratto prova a trasferire criptovaluta. Ricordiamo che i contratti possono essere codificati su qualsiasi blockchain.

```
/* Allow another contract to spend some tokens in your behalf */
function approve(address _spender, uint256 _value)
    returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    return true;
}

/* Approve and then comunicate the approved contract in a single tx */
function approveAndCall(address _spender, uint256 _value, bytes _extraData)
    returns (bool success) {
    tokenRecipient spender = tokenRecipient(_spender);
    if (approve(_spender, _value)) {
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }
}

/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw;                 // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw;  // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw;   // Check allowance
    balanceOf[_from] -= _value;                           // Subtract from the sender
    balanceOf[_to] += _value;                             // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
    return true;
}

/* This unnamed function is called whenever someone tries to send ether to it */
function () {
    throw;     // Prevents accidental sending of ether
}
```

Figura 2 *Esempio di Smart Contract su Ethereum*

3. Linee guida su quando utilizzare la blockchain e quale scegliere

Negli ultimi anni, la ricerca insieme all'industria e alle istituzioni governative hanno lavorato intensamente su DLT e blockchain cercando di comprendere meglio questo paradigma e il suo posto nel mercato. Ciò ha portato a numerose pubblicazioni e alcuni tentativi di standardizzazione. Di seguito, cerchiamo di fornire alcune linee guida che aiutino a capire quando ha senso utilizzare la tecnologia blockchain e quale tipo di blockchain si adatta al meglio al particolare caso d'uso.

3.1. Quando utilizzare la blockchain

Questa sezione cerca di indirizzare il progettista descrivendo sia le casistiche per le quali la tecnologia blockchain rappresenta una buona soluzione aziendale, sia quando invece si può optare per una tecnologia differente. Dall'analisi dello stato dell'arte della ricerca nel settore, evidenziamo qui alcuni criteri e linee guida come emerso in [1]. Per capire come utilizzarla è importante porsi alcune domande. Le domande poste qui di seguito e la relativa numerazione fanno riferimento allo schema di scelta in Figura 1 leggendolo dall'alto verso il basso.

1. **È necessario archiviare e condividere uno stato su un ledger?** Partiamo da una situazione in cui è richiesto un database distribuito e condiviso, ovvero i dati nel modulo di transazione devono essere archiviati e condivisi. I dati costituiscono lo stato di contabilità generale che è soggetto ad aggiornamenti che devono essere condivisi sulla rete. Ogni volta che non è necessario condividere uno stato archiviato, architetture complesse basate su crittografia risultano inutili per consentire semplicemente l'accesso ai dati memorizzati. Pertanto, in presenza di una risposta negativa, la blockchain non è certamente necessaria e sono preferibili soluzioni tradizionali come i database.
2. **Ci sono più potenziali scrittori?** L'adozione delle blockchain ha senso solo quando i dati devono essere memorizzati da più utenti e condivisi tra loro. Infatti, in una blockchain si suppone che più utenti (non necessariamente tutti gli utenti della rete) abbiano accesso e permessi di scrittura per partecipare alla procedura e per stabilire il consenso tra parti. La blockchain consente al business di passare da un sistema client-server gerarchico a interazioni P2P decentralizzate con più nodi in grado di scrivere sul libro mastro distribuito (DLT).
3. **A chi è affidata la manutenzione del libro mastro (DLT)?** La blockchain consente interazioni tra attori che non si fidano gli uni degli altri evitando l'intervento di un'autorità centrale. La necessità di sistemi decentralizzati emerge ogni qualvolta i partecipanti della rete perdono la fiducia in un sistema centralizzato. Tuttavia, il passaggio da un sistema centralizzato a un sistema

decentralizzato non è necessariamente radicale; le blockchain possono decentralizzare alcune funzioni mantenendo altre centralizzate. La blockchain ha rivoluzionato il concetto di "fiducia". Essa non è più correlata all'identità degli attori responsabili della procedura di convalida, ma è correlata all'architettura del protocollo. I clienti si fidano della tecnologia che forza i validatori a seguire il protocollo punendo o rendendo impossibile ogni possibile deviazione. Esistono tre tipi di possibilità nello scegliere a chi affidare la manutenzione:

a. **Una terza parte esterna**: la manutenzione del sistema è affidata a un'entità esterna che in caso di fallimento potrebbe essere cambiata. In tal caso, i progettisti dovrebbero optare per un'architettura centralizzata facile da implementare e mantenere da parte di terzi fidati.
b. **Un gruppo di attori selezionati**: ovvero i nodi responsabili dell'aggiornamento del ledger distribuito del sistema. La loro identità può essere nota o sconosciuta, tuttavia, i metodi per selezionare questi nodi e le attività mirate sono aspetti importanti. La classe di sistemi parzialmente centralizzati include una gamma di possibilità come l'adozione di un libro mastro privato distribuito, la creazione di un comitato di consenso e la strutturazione della comunicazione con sistemi di fiducia esterni. Avendo invece un accesso aperto a chiunque, le blockchain potrebbero legare alcune delle loro funzionalità (lettura, scrittura) al meccanismo dei permessi a rischio però di un'escalation di permessi, dal singolo permesso per leggere il log delle transazioni ai permessi per convalidare le transazioni. Come prima cosa, le blockchain permissioned selezionano i partecipanti con controlli dell'accesso alla rete; la loro identità deve essere conosciuta. Solo successivamente, vengono concessi i permessi per implementare modifiche al registro dei dati; diversi livelli di fiducia possono essere associati a ruoli di nodi diversi. Inoltre, ogni volta che la convalida della transazione è collegata a una variabile esterna, si può scegliere se fidarsi o meno dell'attore designato per comunicare con l'esterno. La verifica dei blocchi consiste in un controllo ripetuto dell'integrità, dell'autenticità e della validità dei blocchi concatenati nella maggior parte dei casi dagli stessi validatori. La trasparenza della blockchain consente a qualsiasi partecipante alla rete di verificare se il blocco pubblicato è stato validato secondo il protocollo poiché i nodi della rete hanno la stessa vista sul DLT. I controlli di verifica sono affidati a una autorità centrale ogni volta che i partecipanti differiscono nella visione che hanno del libro mastro. Quindi, la prossima domanda a questo punto è:

   È necessario che il libro mastro sia verificabile pubblicamente? Ogni volta che un sistema richiede verificabilità pubblica, si può utilizzare una

blockchain open-permissioned mantenendo una restrizione sui diritti di scrittura ma, allo stesso tempo, lasciando a tutti la libertà di osservare lo stato del sistema. Invece, per quei casi in cui i controlli di verifica non devono essere di dominio pubblico, la scelta tra una blockchain privata (full-permissioned) e una soluzione tradizionale è legata alla natura dei verificatori. In particolare, si possono scegliere verificatori centralizzati oppure verificatore distribuito. Il verificatore centralizzato porta all'adozione di un database centrale tradizionale dove il gruppo di nodi fidati si organizza in una autorità centrale che rappresenta tuttavia un potenziale SPOF (single point of failure). Il verificatore distribuito invece è costituito da diversi validatori trusted operanti in una rete P2P in cui tutti i partecipanti al sistema possono connettersi l'un l'altro. L'adozione di una blockchain (in questo caso permissioned) anziché una soluzione tradizionale è dominata da compromessi riguardanti l'impatto sulla produttività, i costi, l'interesse alle funzionalità di base della blockchain, la resistenza al fallimento e adattabilità ai diversi usa case.

I database centralizzati tradizionali sono ampiamente utilizzati sia per la loro architettura semplice, facile da adattare ad ogni caso d'uso e spesso conveniente in quanto i dati vengono archiviati e gestiti da un singolo nodo e sono facili e veloci da aggiornare. Ogni modifica è gestita dall'autorità centrale e immediatamente comunicato agli utenti. L'autorità centrale può facilmente modificare i dati con Comandi CRUD (Create, Read, Update, Delete). Pertanto, i punti di forza della tecnologia consistono in alti livelli di performance in termini di tasso di elaborazione delle transazioni, bassi costi di adozione della tecnologia in termini di design e costi di gestione, infatti i software convenzionali sono più economici delle soluzioni blockchain. Inoltre, vi è un alto grado di adattabilità nella gestione di qualsiasi tipo di dato e del suo utilizzo.

Nonostante gli innumerevoli progressi fatti nelle tecnologie blockchain per raggiungere livelli più alti di scalabilità, velocità effettiva e latenza, la blockchain probabilmente sarà sempre meno performante di un database centralizzato. Questo perché eseguire una transazione in un sistema distribuito richiede ulteriori sforzi consistenti in: (i) applicare e verificare la firma digitale, (ii) concordare una visione unica dei dati nel libro mastro, (iii) replicare i dati attraverso la rete e, (iv) aggiornare il libro mastro solo con operazioni di scrittura. Nella blockchain, infatti, l'idea è che i nodi di convalida elaborino autonomamente le transazioni e poi, come seconda fase, confrontino i risultati ottenuti con il resto della rete fino a quando non raggiungono un accordo. Tuttavia, la blockchain offre, allo stesso tempo, i

sei importanti caratteristiche: decentralizzazione, immutabilità, riservatezza, integrità, autenticità e trasparenza che sono totalmente assenti nei database tradizionali. Inoltre, poiché una blockchain è innanzitutto un libro mastro distribuito, è robusto a fronte di failure dei nodi. Adottare o meno la tecnologia blockchain è quindi una questione di quali proprietà privilegiare tra (i) prestazioni, efficienza dei costi e adattabilità e (ii) caratteristiche fondamentali della blockchain e resistenza ai guasti.

c. **La comunità pubblica**: ogni volta che la fiducia non può essere riposta su una serie di nodi di rete, è meglio avere fiducia in un protocollo (cioè un insieme di regole) che garantisce il corretto funzionamento di un sistema gestito da una comunità pubblica. La blockchain permissionless permette a entità che non si fidano le une delle altre di interagire senza fare affidamento su nessuno “man-in-the-middle”. La storia delle transazioni è completamente trasparente per tutti. La convalida e la verifica vengono effettuate in modo completamente aperto e distribuito; qualsiasi nodo di rete può partecipare al processo col proprio pseudonimo.

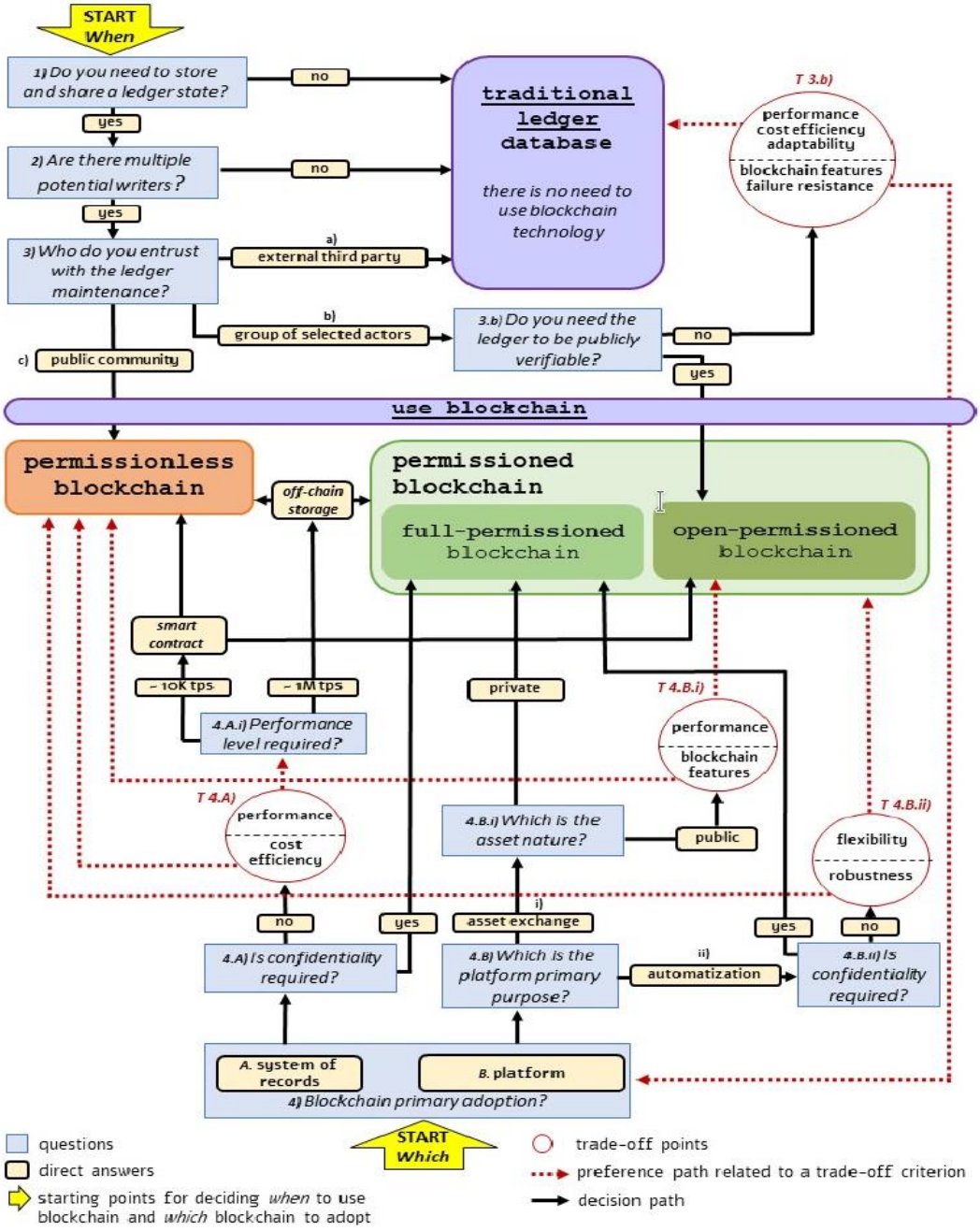

***Figura 1**: Quando usare la blockchain e quale usare (schema)*

3.2. Quale Blockchain scegliere

Le blockchain permissionless richiedono agli utenti di affidarsi alla crittografia e alla matematica correlata, mentre quelle permissioned richiedono fiducia su pochi (o tutti) nodi della rete. Pertanto, assumendo che la blockchain è la giusta tecnologia da utilizzare (vedi paragrafo 3.1), la domanda successiva da porsi è in quale delle due

categorie ricade il nostro use case. Inoltre, se indirizzati a blockchain permissioned, quali restrizioni sull'accesso al registro dei dati si possono scegliere. Il grafico in figura 1 ora può essere anche letto dal basso verso l'alto.

4. Qual è l'adozione primaria della blockchain**?** Una blockchain può essere adottata principalmente come (i) un sistema di record (SOR) oppure come (ii) piattaforma.

    a. L'obiettivo principale di SOR è l'archiviazione e l'elaborazione intelligente dei dati per presentare agli utenti la cronologia dei dati. La blockchain costituisce una soluzione innovativa per tracciare la storia delle modifiche alle informazioni offrendo caratteristiche interessanti, come la sua trasparenza.

    b. L'obiettivo principale di una piattaforma blockchain è quello di formare relazioni digitali P2P a favore degli scambi digitali e automatizzazione aziendale. Essa infatti consente la condivisione e l'archiviazione digitale dei dati e l'interazione virtuale tra peer. In questo caso,

        Qual è lo scopo principale della piattaforma blockchain? Nel caso la risposta alla domanda precedente sia stata la B allora la domanda centrale si basa sullo scopo primario della piattaforma tra le seguenti categorie fondamentali:

        i. **Scambio digitale di asset (beni)**: Blockchain consente la condivisione di asset (es. dati di valore) tra le parti senza nessun vincolo geografico e temporale. Sia la natura dell'asset che la dimensione del flusso di dati impattano sulla scelta della blockchain e il suo design architettonico. **Qual è la natura dell'asset?** L'asset potrebbe essere dati sensibili che devono essere gestiti limitando l'accesso ai record, in questo caso è meglio utilizzare una blockchain permissioned. Se invece non c'è alcun problema di disclosure (divulgazione), la scelta di adottare o meno permessi in scrittura dipendono semplicemente dal trade-off sulle performance. Per prestazioni migliori di quelle offerte dalla blockchain dei bitcoin si dovrebbe pagare il prezzo di non garantire la piena trasparenza (auditability) e pari diritti di partecipazione. La scelta se dare la priorità alla funzionalità di base della blockchain piuttosto che alle prestazioni è strettamente legata alla natura delle attività scambiate nella rete. Per dare un'idea, prendiamo il caso dei token. Blockchain è diventato popolare anche grazie alla tokenization che consiste nella digitalizzazione di un asset in cui ogni token rappresenta la proprietà di una parte dell'infrastruttura sottostante.

Essa ha come obiettivo quello di creare un sistema di trading di oggetti che non possono essere duplicati. Le criptovalute propongono metodi di pagamento alternativi attraverso i loro token che rappresentano una valuta ovvero uno strumento di pagamento generico. Altri tipi di token come quelli di sicurezza (security token) rappresentano invece una partecipazione, in termini di dividendi, diritti di voto, tassi di interesse e/o percentuale degli utili dell'entità emittente.

Nel caso delle criptovalute, tutte le proprietà della blockchain (in particolare l'auditability) sono fondamentali nel sistema, così i designer di blockchain sono stati costretti a perdere qualcosa in termini di performance poiché di solito sono destinate al pubblico più vasto possibile. Dall'altra parte i security token sono considerati come metodo di investimento alternativo, quindi la trasparenza non è essenziale in questo caso e si possono adottare blockchain permissioned che traggono profitto da un più alto tasso di elaborazione rispetto alle soluzioni permissionless.

ii. **Automatizzazione aziendale:** Le piattaforme blockchain consentono il deployment e l'esecuzione di smart contract con l'obiettivo di consentire a qualsiasi azienda di automatizzare le sue funzionalità. Non esiste una blockchain perfetta per tutti i casi d'uso. Tuttavia, quello che incide maggiormente sono (4.B.ii): (i) le proprietà non funzionali di sicurezza e robustezza in termini di resistenza ai guasti e, (ii) tutte le funzionalità relative all'applicazione blockchain ovvero la flessibilità di adattare il protocollo blockchain per diversi casi aziendali. Pertanto, la scelta è una questione di compromessi; le architetture più flessibile sono generalmente meno robuste. Le blockchain permissionless soffrono di limitazioni nella memorizzazione dei dati, scalabilità e prestazioni che non le rendono applicabili a molte situazioni aziendali. D'altra parte, le blockchain permissioned risultano più flessibili nella configurazione poiché governate e ospitate da un unico comitato centrale di nodi fidati; perciò, qualsiasi tipo di modifica viene effettuata più rapidamente rispetto a una versione aperta e senza fiducia.

4. Analisi delle principali piattaforme Blockchain

Una volta deciso di utilizzare la blockchain e il tipo di blockchain da adottare, il prossimo passo è quello di scegliere se sviluppare la propria soluzione o usare una delle piattaforme esistenti.

Piattaforme open-source: diversi framework blockchain possono seguire visioni diverse in termini di campi di applicazione. Alcune architetture possono essere implementate in diversi settori, dalle banche alle supply chain, altre sono guidate da casi d'uso molto specifici. Tuttavia, le principali piattaforme blockchain disponibili possono essere facilmente classificate in quattro gruppi come illustrato nella Tabella I. Considerando che nuovi framework blockchain appaiono regolarmente su base settimanale, abbiamo esaminato nel seguito solo quelli maggiormente utilizzati.

Blockchain on Cloud: Blockchain as a Service (BaaS) è un'offerta che consente ai clienti di sfruttare soluzioni cloud-based per creare e ospitare le proprie blockchain con applicazioni, contratti intelligenti e diverse funzioni. Questo concetto è simile al modello SaaS (Software As A Service). I fornitori esterni gestiscono tutte le attività per mantenere operativa l'infrastruttura

	Transaction Only	**Smart Contract**
Permissionless	Bitcoin	Ethereum
Permissioned	ChainCore	Hyperledger Fabric VeChain[1] Ethereum[2]

Tabella I

[1] open-permissioned (leggibile da tutti, scrivibile solo da nodi autorizzati)
[2] può essere fatto un deployment privato ad hoc di Ethereum

4.1. Bitcoin blockchain

Bitcoin è una blockchain pubblica, permissionless, basata su PoW, che offre un accesso aperto ai suoi registri delle transazioni. Il protocollo Bitcoin facilita anche una versione debole di smart contract, utilizzando il modello UTXO B-A, tuttavia il linguaggio di scripting, per come è implementato, non è Turing-complete. La rete Bitcoin doveva servire come sistema di pagamento pubblico senza un’autorità centrale ed è stato progettato di conseguenza, rendendola inadatta per sistemi permissioned.

I nodi partecipanti in una rete Bitcoin possono scegliere di essere clienti o miner. I clienti (utenti) sono in grado di ricevere e inviare transazioni mentre i minatori sono responsabili del mining utilizzando la PoW (Proo-of-Work). In pratica, quattro processi distinti mantengono la rete in esecuzione: (i) Processo di discovery della rete, (ii) Processo di creazione della transazione, (iii) Processo di convalida del blocco e (iv) Processo di estrazione (mining).

Il protocollo P2P funziona così: al fine di avviare una transazione, un peer mittente trasmette una transazione firmata ai suoi peer vicini. I vicini lo inoltrano nella rete solo se ne hanno verificato la validità; se una transazione non è valida, la propagazione si interrompe. I miner, così come tutti i nodi della rete, ricevono nuove transazioni attraverso la rete P2P. Essi le verificano e le memorizzano in un pool di transazioni. Nel caso in cui il miner scopre dalla rete che un determinato blocco è stato minato, smette di minare, aggiorna il suo pool di transazioni e poi ricomincia tutto di nuovo. Una volta minato, il nuovo blocco viene trasmesso sulla rete P2P. Ogni nodo completo (quelli con un libro mastro) controlla la validità del blocco prima di aggiungerlo al libro mastro (intestazione di blocco, hash, nonce e tutte le transazioni incluse).

Questa architettura di tipo order-execute richiede a tutti i nodi completi di eseguire in sequenza ogni transazione, il che provoca bassa performance di throughput. Di base vengono utilizzati due operazioni di rete P2P: una strategia di “attachment” che definisce come i client stabiliscono connessioni con altri peer, e una strategia di comunicazione, che definisce il modo in cui i nodi comunicano con i loro vicini. La discovery dei peer in Bitcoin viene eseguito tramite query utilizzando un elenco hard-coded di seed DNS. I nodi possono scoprire altri peer anche richiedendo l'elenco IP ai vicini; inoltre, viene mantenuta una blacklist degli indirizzi IP che si comportano male. Bitcoin limita il numero di connessioni per intervallo di indirizzi IP; in questo modo i nodi non stabiliscono troppe connessioni, migliorando la loro resistenza a DoS. Il numero predefinito di connessioni è 8 (tuttavia, è stato proposto di aumentare questo numero). Il codice Bitcoin è rilasciato sotto una licenza MIT.

4.2. Ethereum blockchain

Ethereum è una piattaforma aperta progettata per creare e utilizzare applicazioni decentralizzate che eseguono smart contract, ovvero applicazioni distribuite che eseguono meccanicamente compiti quando sono soddisfatte determinate condizioni. Questo può essere fatto a più ampio raggio di quanto possibile con il modello UTXO di Bitcoin perchè viene utilizzato un linguaggio di programmazione Turing-complete denominato Solidity. Etherium è stata una delle prime piattaforme a supportare gli smart contract di questo tipo.

Come Bitcoin, anche Ethereum è cryptocurrency-based, vale a dire che i miner lavorano per guadagnare il token crittografico chiamato Ether, che viene anche utilizzato per pagare commissioni e servizi di transazione nella rete di Ethereum.

Ethereum utilizza un algoritmo di consenso basato su PoW, chiamato Ethash, creato appositamente per Ethereum, nonostante recentemente ci siano sforzi per passare ad implementazioni alternative basate su PoS. In media, un blocco viene minato con PoW in 15 secondi. Il modo in cui Ethash fornisce un PoW è sfruttando l'accesso alla memoria come un collo di bottiglia, oltre alla potenza di calcolo. Ethash è progettato per consumare quasi l'intera larghezza di banda di accesso alla memoria disponibile; la ricerca del nonce richiede molta memoria e banda di accesso alla memoria, in modo che la memoria non possa essere utilizzata in parallelo per scoprire più nonce contemporaneamente

La manutenzione della rete viene eseguita in quattro processi:

- Rilevamento della rete, che consente di fare join di nuovi nodi.
- Creazione della transazione, che consente agli utenti di creare transazioni o contratti e consente ai contratti di creare transazioni e messaggi.
- Convalida del blocco, eseguita da ogni nodo completo (quelli con un libro mastro) della rete prima di aggiungere il nuovo blocco alla blockchain.
- Mining, responsabile dell'Ether mining e di fare broadcast di un nuovo blocco sulla rete.

Come già anticipato, Ethereum supporta tre tipi di account:

- Contract Account (CA) che può impostare una transazione con indirizzo memorizzato all'interno di un contratto, oppure stabilire una transazione con un'altra CA;
- EOA (Externally Owned Accounts) che avviano la transazione per trasferire Ether verso un altro EOA, oppure creano un nuovo contratto o chiamano una funzione di una CA esistente;
- Miners, che possono raccogliere nuove transazioni non verificate e calcolare uno stato valido di un libro mastro, convalidare transazioni, verifica firme e commissioni per la transazione, eseguire codice e il controllare che esso non “run out of gas”, ovvero che fallisca poiché la commissione di transazione pagata non è adeguata alla complessità dell'elaborazione delle transazioni.

Mentre la piattaforma principale di Ethereum è una blockchain pubblica, il software è open-source e consente di scaricare e configurare una rete locale privata. In questo

caso i partecipanti sono solo quelli a cui è stata concessa l'autorizzazione e si utilizza un diverso algoritmo di consenso come ad esempio la proof of Authority (PoA).

Riferendoci a Ethereum come la rete in una configurazione pubblica, utilizzata per trasferire Ether tra i partecipanti, essa raggiunge circa 15-40 transazioni al secondo (tps) con una latenza stimata di circa 15 secondi per blocco. Nel setup privato Ethereum può raggiungere circa mille tps. Il codice Ethereum è di provenienza aperta in a Licenza GPL.

4.2.1 Ethereum: casi d'uso reali e partnership

- Publica promette di rivoluzionare il settore editoriale utilizzando smart contract che regolano l'accesso a libri, pagamenti e distribuzione del fatturato. Si basa sull'uso dei token Ethereum come chiavi di licenza per accedere agli e-book.
- Mycelia cerca di garantire che l'artista venga pagato per uso della canzone. Essa è una compagnia fondata dal musicista Imogen Heap e sta attualmente tentando di utilizzare la blockchain per "aiutare i musicisti a guadagnare di nuovo".
- La compagnia ConsenSys ha collaborato con la società farmaceutica Glaxo Smith Kline (GSK) e diverse altre aziende per raggiungere gli standard normativi implementando sistemi di catena di fornitura basati su blockchain. L'U.S. Drug Supply Chain Security Act ha imposto una traccia a livello di unità e tracciabilità per i prodotti farmaceutici entro il 2023.
- La compagnia ConsenSys ha collaborato con il WWF per garantire la tracciabilità e la trasparenza del settore della pesca nelle Fiji. Il risultato è stata una prova immutabile e verificabile che il tonno pinna gialla veniva catturato con metodi sostenibili, spedito in celle frigorifere e arrivato in una finestra temporale sicura per il consumo.
- La compagnia ConsenSys ha recentemente collaborato con Luxarity per tenere traccia dei proventi di beneficenza. Luxarity funge da braccio di investimento del marchio di vendita al dettaglio di moda di Hong Kong Lane Crawford. Luxarity ha registrato beni di lusso rivenduti sulla blockchain, quindi i donatori sono stati in grado di tracciare le loro donazioni di beneficenza.
- GenuineWay è un consorzio di oltre 500 fornitori e distributori autorizzati. Il consorzio applica i codici QR agli articoli per alimenti e liquori. Vengono implementati smart Contract per certificare la manifattura di prodotti alimentari artigianali per i consumatori finali.

4.3. Hyperledger Fabric

Hyperledger è un progetto open source della Linux Foundation, creato per favorire le tecnologie blockchain tra diversi settori. Hyperledger è un "ombrello" composto da

quattordici progetti, sei dei quali sono DLT e gli altri otto progetti moduli di supporto. Ci sono più di 270 organizzazioni nella comunità ufficiale di Hyperledger. Considerando che le parti che aderiscono alla rete devono essere autenticate e autorizzate, i framework Hyperledger sono tipicamente blockchain permissioned (tranne Sawtooth).

Fabric è stata la prima codebase proposta dal progetto hyperledger che unisce il lavoro precedente svolto da Digital Asset Holdings e OpenBlockchain di IBM. Fabric fornisce un'architettura modulare che consente a componenti come il consenso e i servizi di membership di essere plug-and-play. Un'importante funzionalità introdotta da Fabric è quella di consentire ai nodi di eseguire transazioni confidenziali sulla stessa rete di peer. Fabric adotta la seguente terminologia relativa al suo flusso di lavoro; un'"applicazione" blockchain gestisce l'interfacciamento con l'utente e con la rete. Gli smart contract sono chiamati "chaincode" e sono forniti con un Node SDK, un Java SDK e un'interfaccia a riga di comando. Leggere o scrivere il libro mastro è un'operazione definita "proposal". Le "proposal" sono inviate ad un blockchain peer che le elabora attraverso uno specifico container chaincode. Il chaincode quindi esegue la transazione; se non ci sono problemi, approva la transazione e la restituisce all'applicazione. Un'applicazione quindi invia la proposal approvata all'Ordering service che confeziona più proposal dell'intera rete in un blocco che viene successivamente trasmesso ai peer di rete. Infine, ogni peer convalida il blocco e lo aggiunge al suo libro mastro. Il flusso di lavoro sopra descritto viene definito come un'architettura "execute-order-validate" destinata ad andare oltre l'approccio comune di "order-execute". Diversi gruppi di nodi hanno un ruolo diverso in rete: i clienti presentano proposte, un sottoinsieme di peer chiamato "endorser" convalida le transazioni eseguendo tutte le transazioni, i nodi "orderer" invece fanno da servizio di ordinamento.

I Chaincode possono essere scritti in Java, Javascript e Golang. Gli sviluppatori usano i chaincode per lo sviluppo di contratti commerciali, definizione di asset e applicazioni decentralizzate gestite collettivamente. È garantito l'isolamento tra diversi chaincode; l'asset creato e aggiornato da uno specifico chaincode non può essere acceduto da un secondo chaincode.

Il chaincode deve essere installato su ogni peer che fa l'endorsment di una transazione. Per sviluppare smart contract con Fabric, si possono (i) codificare i singoli contratti in un'istanza standalone di chaincode o (ii) usare i chaincode per creare applicazioni decentralizzate che gestiscano il ciclo di vita di uno o più tipi di contratti commerciali, lasciando che gli utenti finali istanzino istanze di contratti con queste applicazioni. L'interazione con il chaincode è fatta usando gRPC. Un libro mastro viene gestito utilizzando un key-value store locale implementato da LevelDB o Apache CouchDB. L'isolamento tra i chaincodes è garantito dai canali: un canale può essere visto come un'istanza completamente separata di Fabric; ogni canale è completamente indipendente e non scambia mai dati con un altro canale, ciascuno di loro ha un diverso

insieme di regole e politiche. La rete di Fabric è costituita da peer che non sono in grado di comunicare a meno che non facciano parte dello stesso canale. Pertanto, Fabric abilita i nodi della stessa rete per comunicare in modo indipendente con l'insieme predefinito di nodi in un modo isolato rispetto alle politiche concordate.

In termini di latenza, Fabric può raggiungere fino a 10.000 tps e scrivere una transazione irrevocabilmente nella blockchain in circa 0,5 secondi, anche con peer in diversi continenti.

4.3.1 Hyperledger Fabric: Casi d'uso reali e partnership

- Nell'aprile 2017, IBM ha annunciato diversi nuovi sistemi enterprise blockchain da costruire su Hyperledger Fabric. La società ha stretto una partnership con il conglomerato cinese Sichuan Heijia per costruire una piattaforma di approvvigionamento basata su blockchain per prodotti farmaceutici.
- Nel maggio 2017, IBM ha presentato un altro importante progetto da costruire sulla piattaforma blockchain di Hyperledger. In collaborazione con TenneT, Sonnen e Vandebron, IBM ha sviluppato un DLT per la gestione della rete elettrica nei Paesi Bassi e in Germania.
- Nel dicembre 2017 il grande rivenditore della catena multinazionale Walmart ha stretto una collaborazione con IBM per creare un sistema blockchain aziendale basato su Hyperledger Fabric che tiene traccia dei prodotti alimentari dal fornitore allo scaffale. La soluzione consente una collaborazione completa di tutte le parti interessate del settore alimentare.
- Nel 2019 una collaborazione tra IBM e il MISE (Ministero dello Sviluppo Economico) sviluppano uno studio di fattibilità e un prototipo di soluzione per la tracciabilità nel settore tessile, per la valorizzazione del Made in Italy e per superare le problematiche tipiche dei processi di tracciabilità attualmente utilizzati. Un primo prototipo ha dimostrato che i processi di lavorazione possono essere tracciati rendendoli trasparenti verso tutti gli attori della filiera del tessile (inclusi eventuali Certificatori) e fornendo un primo insieme di funzionalità a questo scopo.

4.4. VeChain

Vechain è una blockchain che si rivolge al mondo dell'Internet of Things; essa inoltre è la piattaforma della criptovaluta conosciuta come VET. Uno degli obiettivi di VeChain è quello di migliorare la gestione della supply chain e i processi di business. I produttori assegnano ad ogni prodotto un identificatore RFID (identificazione a radiofrequenza) registrando così le informazioni lungo la catena di approvvigionamento. Le informazioni RFID diventano successivamente disponibili sulla blockchain VeChain. La blockchain è

governata dalla VeChain Foundation e utilizza Proof-of-Authority (PoA) per mantenere il consenso. In PoA, account approvati chiamati validatori mettono le transazioni nei blocchi. I titolari (holder) di VET guadagnano i diritti per utilizzare la blockchain VeChain e per votare i membri del comitato direttivo della Fondazione VeChain.

4.4.1 VeChain: Casi d'uso reali e partnership

- PwC. Nel maggio 2017, VeChain è diventata una società di portafoglio del programma di incubazione di PwC "per accelerare l'applicazione della blockchain nei mercati di Hong Kong e del Sud-est asiatico".
- DNV GL. Gennaio 2018 ha visto l'annuncio della partnership di VeChain con il fornitore di servizi di certificazione DNV GL.
- Fanghuwang. Annunciata anche a gennaio 2018, questa collaborazione con il prestatore incentrato sui mutui immobiliari delle PMI Fanghuwang è progettata per aiutare questi ultimi a raccogliere, gestire e utilizzare i dati dei clienti in modo più efficace.
- Gui'an (progetto smart city). VeChain è incaricato di essere il partner tecnologico blockchain del governo di Gui'an, una città nella Cina orientale.

5. Conclusioni

Dall'analisi fatta nel capitolo III e IV possiamo notare che in entrambi i casi d'uso l'esigenza è quella di avere un ledger distribuito con più nodi potenzialmente interessati a scriverci. Inoltre, vorremmo che il ledger distribuito fosse privato con un ristretto numero di attori interessati alla gestione. Per quanto riguarda invece il tipo di DLT, esso deve essere in entrambi i casi d'uso (Biancoaccessori e Carpigiani) di tipo blockchain as a platform. Lo scopo primario della piattaforma risulta essere legato allo scambio digitale di asset di diversa natura, all'esecuzione di smart contract e all'automatizzazione aziendale.

Nel caso di scambio di asset digitali la scelta è determinata dalla sensibilità dei dati (confidentiality) che devono essere gestiti limitando perciò l'accesso ai record. Nel caso di un'alta sensibilità dei dati (dati privati) è meglio utilizzare una blockchain full-permissioned mentre se non c'è alcun problema di disclosure (divulgazione), la scelta di adottare blockchain permissioned o permissionless dipende dal trade-off sulle performance. Per prestazioni migliori si dovrà optare per una blockchain open-permissioned non garantendo piena trasparenza (auditability) e pari diritti di partecipazione, caratteristiche che sarebbero invece assicurate con una soluzione permissionless.

Anche nel caso di automatizzazione aziendale la riservatezza dei dati gioca un ruolo fondamentale, se è richiesta infatti si opterà per una soluzione full-permissioned

altrimenti il trade-off sarà tra robustezza, prediligendo una blockchain permissionless, e flessibilità optando per una tecnologia open-permissioned.

Tra le soluzioni blockchain più utilizzate sul mercato e appetibili per il progetto ci sono:

- Hyperledger Fabric: soluzione totalmente permissioned di IBM
- VeChain: soluzione open-permissioned molto utilizzata dal mercato asiatico
- Ethereum: soluzione sia permissionless che permissioned molto conosciuta, utilizzata e versatile

References

[1] M. Belotti, N. Božić, G. Pujolle and S. Secci, "A Vademecum on Blockchain Technologies: When, Which, and How," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3796-3838, Fourthquarter 2019. doi: 10.1109/COMST.2019.2928178
[2] Filippo Bosi, Michele Cappelletti, Stefano Monti, Guido Ravagli, Blockchain Beyond Cryptocurrencies: A Real-World Use Case, Thinkmind Digital Library