Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"
Consiglio Nazionale delle Ricerche

ISTI Technical Reports

Le caratteristiche funzionali e tecnologiche della "black box" domestica

Vittorio Miori, CNR-ISTI, Pisa, Italy

Dario Russo, CNR-ISTI, Pisa, Italy

Loredana Pillitteri, CNR-ISTI, Pisa, Italy

ISTI-TR-2020/027

Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"
Consiglio Nazionale delle Ricerche

Le caratteristiche funzionali e tecnologiche della "black box" domestica

Miori V.; Russo D.; Pillitteri L.

ISTI-TR-2020/026

Abstract

Nella home automation tradizionale, i differenti servizi presenti hanno ciascuno un loro framework, col risultato che i vari servizi sono indipendenti, non colloquiano, non interagiscono fra loro e la sicurezza non è completamente garantita. Diversamente, col framework di interoperabilità sviluppato nel presente progetto, i servizi diventano interoperabili, si scambiano informazioni e possono garantire un livello di sicurezza molto elevato. Oltre a ciò, nel framework è stato previsto di sviluppare un servizio del tutto innovativo, che sia in grado di monitorare e tenere traccia di tutte le azioni e i dati degli edifici domestici, ovvero una vera e propria scatola nera domestica (black box). In questa specifica attività, si analizzeranno e si individueranno le caratteristiche funzionali, strutturali e tecnologiche della scatola nera domestica, in modo che possa essere facilmente integrata nel framework.

Black box domestica, Scatola nera della casa, Carta d'identità della casa, Blockchain, Framework di interoperabilità, Domotica, Home automation

Citation

Miori V.; Russo D.; Pillitteri L. *Le caratteristiche funzionali e tecnologiche della "black box" domestica* ISTI Technical Reports 2020/027. DOI: 10.32079/ISTI-TR-2020/027

Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"
Area della Ricerca CNR di Pisa
Via G. Moruzzi 1
56124 Pisa Italy
http://www.isti.cnr.it

Le caratteristiche funzionali e tecnologiche della “black box” domestica

Vittorio Miori (CNR) – Dario Russo (CNR) – Loredana Pillitteri (CNR)

Breve sommario

Nella home automation tradizionale, i differenti servizi presenti hanno ciascuno un loro framework, col risultato che i vari servizi sono indipendenti, non colloquiano, non interagiscono fra loro e la sicurezza non è completamente garantita. Diversamente, col framework di interoperabilità sviluppato nel presente progetto, i servizi diventano interoperabili, si scambiano informazioni e possono garantire un livello di sicurezza molto elevato. Oltre a ciò, nel framework è stato previsto di sviluppare un servizio del tutto innovativo, che sia in grado di monitorare e tenere traccia di tutte le azioni e i dati degli edifici domestici, ovvero una vera e propria scatola nera domestica (black box).
In questa specifica attività, si analizzeranno e si individueranno le caratteristiche funzionali, strutturali e tecnologiche della scatola nera domestica, in modo che possa essere facilmente integrata nel framework.

Parole chiave

Black box domestica, scatola nera della casa, carta d'identità della casa, blockchain, framework di interoperabilità, domotica, home automation.

Indice

1. La Black Box della casa

La Black Box della casa si può intendere come una sorta di "carta d'identità" della casa stessa, che riguarda tutti i suoi aspetti (strutturali e tecnologici); in essa si leggono tutti gli interventi fatti alla struttura e agli impianti, con la descrizione degli stessi e le date in cui sono stati effettuati. Inoltre, nell'ottica dell'architettura SHELL, la Black Box raccoglierà i dati prodotti dai manager per permettere, quando necessario, sia di ricostruire la dinamica di eventuali eventi anomali nel passato, che di prevenire/predire eventuali condizioni critiche che potrebbero verificarsi.

Dal punto di vista architettonico/strutturale, ll concetto di Black Box della casa si innesta nel contesto delle funzionalità cosiddette di *facility management* che oggi stanno trovando nel BIM (Building Information Management) il framework digitale di supporto. La gran parte dei costi di un immobile nei suoi 20 anni di vita "economica" è data dal suo esercizio e manutenzione. Chiunque voglia mettere in atto programmi di efficientamento del proprio patrimonio immobiliare non può che puntare al Facility Management. Il digitale, che trasforma documenti, informazioni, transazioni manuali in bits e flussi automatici è il più importante tra i fattori di efficientamento attualmente a disposizione di amministrazioni pubbliche, aziende e professionisti operanti nella filiera. Applicando la metodologia BIM è possibile creare un modello che associ informazioni geometriche (3D) a quelle alfa-numeriche, le uniche rilevanti ai fini gestionali e manutentivi. Tali informazioni vanno inserite nel sistema parallelamente alla progettazione degli impianti ed alla costruzione fisica dell'asset, in modo da creare il database completo degli elaborati progettuali che serva alla committenza per l'esercizio e manutenzione, con informazioni sui tempi e costi ad essa relativa. In questo senso, il modello progettuale (BIM) evolve in quello costruttivo (PIM) e alla fine in quello gestionale (AIM) lungo la vita del progetto, andando ad arricchirsi di informazioni e dati utili al facility manager nelle sue attività di esercizio e manutenzione dell'asset, come rappresentato in Figura 1.

Figura 1. Modelli informativi e il ciclo di vita di un asset immobiliare.

La manutenzione dell'edificio va gestita con una piattaforma apposita, idealmente bidirezionale, in grado di recepire le prescrizioni del manuale di manutenzione e utilizzarle come input per la programmazione degli interventi. Oltre a gestire la manutenzione, siffatta piattaforma dovrebbe supportare la pianificazione degli spazi, la catalogazione di impianti e mobili, l'archiviazione delle schede di manutenzione di ciascun oggetto, la previsione di massima delle tempistiche e dei costi relativi agli interventi effettuati, secondo funzionalità in parte riportate in Figura 2:

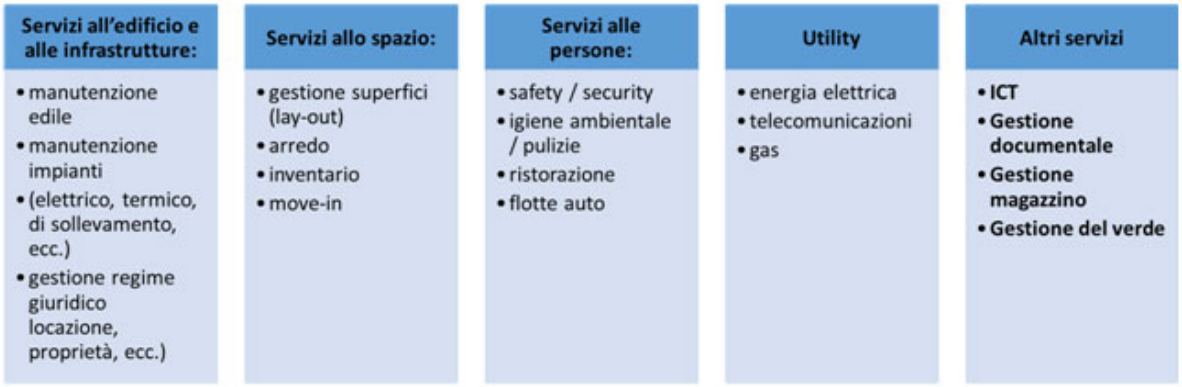


Figura 2. Funzionalità di una piattaforma BIM per il Facility Management.

Un esempio di black box per la casa è stato proposto a seguito dei devastanti eventi sismici nel centro Italia, ed è relativo alla salute strutturale dell'edificio e alla necessità di dati per effettuare verifiche, sentita dal settore assicurativo, in analogia a quanto avviene con la black box per le auto. A farsi promotrice di questo progetto è stata Sysdev, una start up innovativa nata all'interno dell'incubatore del Politecnico di Torino. Proprio questa azienda ha colto la palla al balzo rappresentata dalla discussione che ha fatto seguito alle tremende devastazioni causate dal sisma che ha letteralmente distrutto centri come Amatrice e Norcia, riproponendo il tema della messa in sicurezza delle abitazioni lungo la penisola.

La risposta di Sysdev consiste appunto in una scatola nera, simile a quella che viene installata nelle vetture e basata su dei sensori IoT (Internet of Things), i quali riescono a monitorare le singole parti di un immobile, non soltanto gli edifici civili, ma anche strutture estremamente complesse come gallerie

e ponti. Nel corso dell'analisi il dispositivo provvede a verificare la resistenza della parte esaminata, andando ad estrapolarne i dati e rendendoli fruibili. In tal modo diventa possibile stabilire in tempi brevissimi l'eventuale agibilità o meno dell'edificio interessato. Il tutto senza i lunghi tempi di attesa che sono invece attualmente il corollario dopo eventi sismici importanti. In maniera simile, la compagnia di assicurazioni UnipolSai vuole offrire uno strumento di protezione che associ alle garanzie tradizionali dei prodotti danni per la casa una serie di servizi. Il concetto di protezione legato all'abitazione viene allargato, includendo le opportunità delle tecnologie telematiche e forme di assistenza e supporto diretto in caso di sinistro. Questa idea si fonda su un dispositivo chiamato UniboxCasa, la versione domestica della scatola nera Unibox di Unipolsai, adattata con sistemi di domotica finalizzati al rilevamento di anomalie nell'ambiente interno ed esterno: il dispositivo elettronico, tramite sensori, avvisa l'assicurato in caso di presenza di fumo, perdite d'acqua, gas o monossido, ed è dotato anche di sensori volumetrici e perimetrali, che segnalano movimenti anomali dentro e fuori dell'abitazione, e di un help button da attivare per chiedere aiuto. La box si avvale di una tecnologia digitale anche per la gestione, che avviene completamente tramite la *app* di Unipolsai, la quale riceve le notifiche dei sensori, permette di attivarli, spegnerli e controllare ciò che avviene all'interno dell'abitazione grazie alla telecamera. L'offerta commerciale, che include anche una copertura per eventi catastrofali, è strutturata su tre versioni di UniboxCasa ed è modulabile con l'aggiunta di pacchetti di garanzie che il cliente può scegliere in base alle proprie esigenze e che riguardano la protezione della famiglia.

Le tecnologie digitali possono essere applicate alla gestione e alla tracciabilità dei processi di manutenzione e verifica di qualunque sistema, impianto, apparato. In tal modo, il concetto di Black Box può essere mutuato ad ambiti applicativi anche molto diversi da quello abitativo/domestico.
Esempi di soluzioni simili al concetto di "Black Box" della casa sono infatti costituiti da:

- Libretti Digitali di Manutenzione e Servizio dei veicoli (vedere, ad esempio: https://www.mercedes-benz.it/content/italy/mpc/mpc_italy_website/it/home_mpc/passengercars/home/servicesandaccessories/services_and_workshop/inspection_and_care/digital_servicereport.html). In questo caso, durante tutto il ciclo di vita della auto, viene conservato in una banca dati centrale ogni rapporto di intervento, utile ad esempio nel caso di vendita del veicolo. Se necessario, si

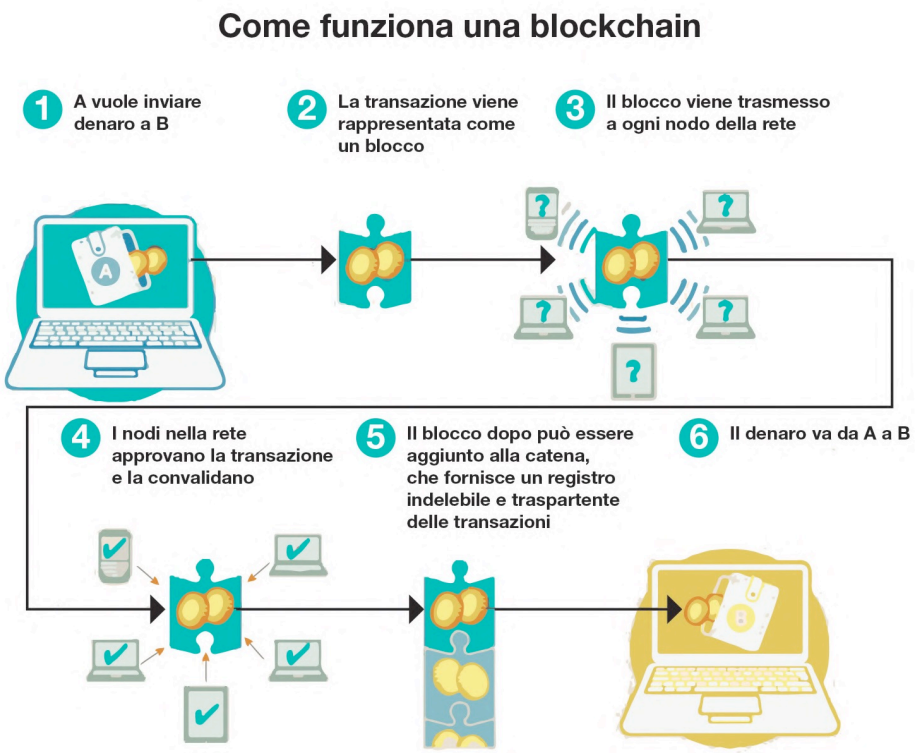
può richiedere una cronologia completa dei servizi ricevuti. Altro esempio: http://www.omniauto.it/magazine/47309/renault-libretto-manutenzione-digitale: grazie a una sorta di "carta d'identità" o di "curriculum" del mezzo che riguarda tutti i suoi aspetti, si leggono tutti gli interventi, con la descrizione degli stessi e le date in cui sono stati effettuati. Così poi il libretto diventa meno soggetto a danni e manomissioni.

- Soluzioni di tracciabilità in ambito alimentare (esperienza IBM con Walmart): https://www.01net.it/tecnologia-blockchain-erp/

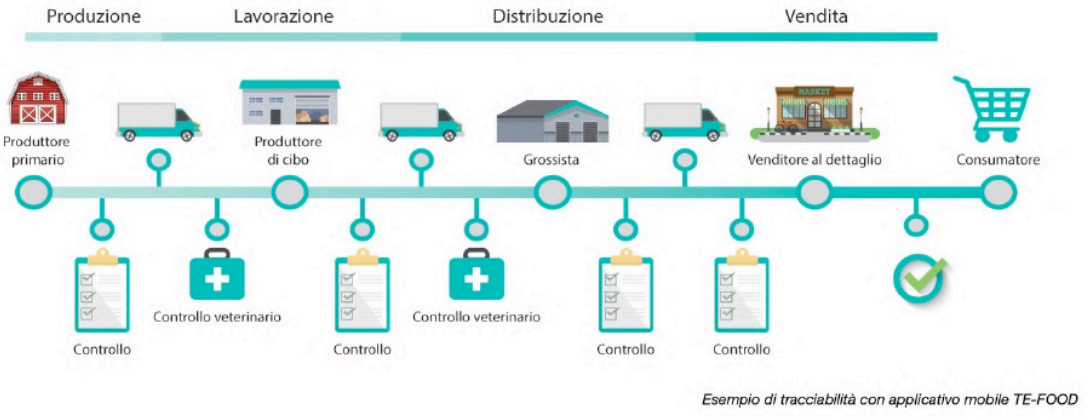
2. Tecnologia Blockchain per l'implementazione della Black Box della casa

Considerati i requisiti che la Black Box della casa dovrebbe rispettare, la tecnologia Blockchain può rappresentare un approccio tecnologico adeguato alla realizzazione della Black Box della casa.

In sintesi, la Blockchain è una tecnologia che permette la creazione e gestione di un grande database distribuito per la gestione di transazioni condivisibili tra più nodi di una rete. Si tratta di un **database strutturato in blocchi** (Block) o nodi di rete che sono tra loro collegati (Chain) in modo che ogni transazione avviata sulla rete debba essere **validata** dalla rete stessa. In estrema sintesi la Blockchain è rappresentata da una **catena di blocchi che contengono e gestiscono più transazioni.** Ciascun nodo è chiamato a vedere, controllare e approvare tutte le transazioni creando una rete che permette la **tracciabilità** di tutte le transazioni. Ciascun Blocco a sua volta è anche un archivio per tutte le transazioni (e per tutto lo storico di ciascuna transazione) che proprio per essere approvate dalla rete e presenti su tutti i nodi (Block) della rete sono immodificabili (*se non attraverso la riproposizione degli stessi a tutta la rete e solo dopo aver ottenuto la approvazione*) e sono dunque **immutabili**. Oltre alla immutabilità l'altra grande caratteristica della Rete Blockchain è data dall'uso di strumenti **crittografici per garantire la massima sicurezza di ogni transazione**. La Figura 3a illustra schematicamente il funzionamento di una blockchain, mentre la Figura 3b illustra il caso di una blockchain applicata nel dominio AgriFood per garantire la tracciabilità di un prodotto agroalimentare.



a)



b)

Figura 3. a) Il funzionamento di una blockchain; b) blockchain per tracciabilità agroalimentare.

Un esempio di applicazione della tecnologia Blockchain ad un ambito simile a quello della Black box della casa viene, di nuovo, dal mondo automobilistico, per il libretto digitale di manutenzione del veicolo. Un progetto portato avanti da Renault in collaborazione con Microsoft e VISEO, ha fatto uso della tecnologia Blockchain Microsoft Azure per il primo libretto di manutenzione dell'auto completamente digitale, che, con la sua architettura aperta, è in grado di custodire tutte le

informazioni vitali dell'auto in un unico elemento accessibile dal cliente, mostrato in Figura 4. Un esempio dell'utilità del libretto digitale è la possibilità di avere a portata di mano l'intera storia del veicolo, utile per stabilire un rapporto di fiducia tra compratore e venditore nell'acquisto di un'auto usata. La tecnologia Blockchain è in grado di creare un protocollo affidabile per i veicoli connessi e per i requisiti di sicurezza delle micro-transazioni associate ad essi.

Figura 4. Libretto digitale del veicolo.

Anche nel settore AgriFood si sta investendo nella tecnologia blockchain. IBM nel 2018 ha annunciato l'ampliamento e il potenziamento del suo network per la filiera alimentare IBM Food Trust33, rete blockchain basata su cloud che offre a rivenditori, fornitori, coltivatori e distributori dell'industria alimentare dati provenienti da tutto l'ecosistema food per consentire maggiore tracciabilità, trasparenza ed efficienza. L'ecosistema dei partecipanti, ad oggi, continua a crescere e Carrefour, il principale rivenditore a livello globale, ha annunciato che utilizzerà la rete blockchain di IBM Food

Trust per rafforzare le proprie attività e raggiungere l'eccellenza alimentare. Con Carrefour, prima tra i gruppi GDO in Europa, la blockchain fa il suo ingresso nella grande distribuzione. L'utilizzo di questa tecnologia nel settore del food fa sì che ciascun componente della filiera possa fornire informazioni di tracciabilità relative al suo particolare ruolo e a ciascun lotto (date, luoghi, edifici per bestiame, canali di distribuzione, potenziali trattamenti ecc..).

Anche Barilla, ha collaborato con IBM per affrontare la trasparenza e la tracciabilità nel suo ciclo di produzione del pesto: dalla coltivazione, al trattamento, alla raccolta, fino al trasporto, allo stoccaggio, al controllo di qualità e infine alla distribuzione, tutti i dettagli sono tracciati e resi disponibili su un sistema di blockchain che il cliente può verificare scansionando il codice QR del pesto.

L'ultimo progetto portato avanti da IBM con Galpagro, azienda agricola spagnola olivicola, conferma l'interesse di facilitare, anche per le piccole realtà, un sistema di tracciabilità basato sulla tecnologia blockchain al fine di poter garantire maggiore sicurezza e garanzia in tutte le fasi della produzione e distribuzione dell'olio extravergine di oliva. Questa sofisticata piattaforma consentirebbe attraverso un codice QR di visualizzare tutte le transazioni attraverso una app: la posizione esatta degli olivi coinvolti, la varietà di olive selezionate, la spremitura, la produzione, l'imballaggio, la distribuzione fino al posizionamento sugli scaffali dei supermercati. Il sistema è interessante non solo per i consumatori ma anche per gli olivicoltori, i produttori, i confezionatori e le esportazioni.

Per implementare una soluzione basata su Blockchain nell'ambito del progetto SHELL, si può ricorrere a soluzioni aperte, come Openchain, Hyperledger e Open Blockchain.

Openchain

Openchain (https://docs.openchain.org/en/latest/index.html) è una tecnologia di libro mastro distribuita open source. È adatto per le organizzazioni che desiderano emettere e gestire risorse digitali in modo robusto, sicuro e scalabile.

- Chiunque può creare una nuova istanza di Openchain in pochi secondi
- L'amministratore di un'istanza di Openchain definisce le regole del libro mastro
- Gli utenti finali possono scambiare valore sul libro mastro secondo tali regole
- Ogni transazione sul libro mastro è firmata digitalmente.

Il meccanismo di consenso utilizzato da Openchain differisce dagli altri sistemi basati su Bitcoin, e

utilizza il Partitioned Consensus:

- Ogni istanza di Openchain ha solo un'autorità che convalida le transazioni.
- Invece di un unico libro mastro centrale, ogni organizzazione controlla la propria istanza di Openchain. Le istanze possono connettersi tra loro.
- Transazioni diverse verranno convalidate da autorità diverse a seconda delle attività scambiate.
- Ogni emittente di attività ha il pieno controllo delle transazioni relative a tale attività.

Openchain utilizza un'architettura client-server che è più efficiente e affidabile di un'architettura peer-to-peer. Non esiste un miner, le transazioni vengono convalidate direttamente dall'amministratore delle risorse. Poiché non esiste un miner, le transazioni sono immediate e gratuite.
I validatori convalidano e archiviano le transazioni, gli osservatori ricevono una copia di sola lettura del libro mastro, fanno la propria convalida del libro mastro e archiviano la propria copia. I validatori e gli osservatori espongono le API standard basate su http: clienti e portafogli si collegano ai validatori per inviare transazioni con firma digitale. I contratti intelligenti sono attori indipendenti che ricevono e inviano transazioni secondo una logica aziendale arbitraria. I gateway creano il pegging bidirezionale tra due istanze di Openchain e possono anche inserire l'istanza di Openchain come sidechain della Blockchain Bitcoin.
Openchain è un registro generico di proprietà. Può essere modellato per funzionare con un numero immenso di casi d'uso: titoli come azioni e obbligazioni, materie prime come oro e petrolio, valute come il Dollaro o persino Bitcoin, titoli di proprietà immobiliare, licenze musicali o software.

Openchain rientra nell'ambito della tecnologia Blockchain. Tuttavia, se prendiamo alla lettera il termine "catena a blocchi", Openchain non è una "catena a blocchi", ma un cugino stretto. Una catena di blocchi è una struttura di dati che ordina blocchi di transazioni e li collega crittograficamente tramite hash. Openchain non usa il concetto di blocchi. Le transazioni sono direttamente concatenate tra loro e non sono più raggruppate in blocchi. Dover raggruppare le transazioni in blocchi introduce un ritardo. Anche se alcuni sistemi riescono a ridurre il tempo di blocco a pochi secondi, qualche secondo è ancora molto tempo per le applicazioni sensibili alla latenza, come il trading. In Openchain, le transazioni sono collegate alla catena non appena vengono inviate alla rete. Di conseguenza,

Openchain è in grado di offrire conferme in tempo reale. Ciò significa che un termine più appropriato per Openchain è una "catena di transazioni" anziché una "catena di blocchi".

Openchain si basa su diverse strutture di dati per la comunicazione tra client e server. Queste strutture di dati sono una parte fondamentale dell'API Openchain, e sono serializzate e deserializzate usando Protocol Buffers.

```
syntax = "proto3";

package Openchain;

message RecordValue {
    bytes data = 1;
}

message Record {
    bytes key = 1;
    RecordValue value = 2;
    bytes version = 3;
}

message Mutation {
    bytes namespace = 1;
    repeated Record records = 2;
    bytes metadata = 3;
}

message Transaction {
    bytes mutation = 1;
    int64 timestamp = 2;
    bytes transaction_metadata = 3;
}
```

Figura 5. Schema completo Openchain.

Lo schema, illustrato in Figura 5, usa la versione 3 dei Protocol Buffers.

Openchain utilizza una gerarchia di account, simile a un file system, come mostrato in Figura 6.

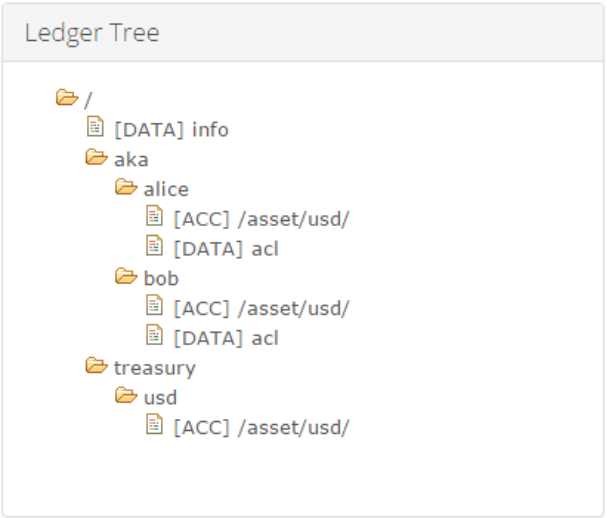


Figura 6. Gerarchia di account.

Questo aggiunge molte opzioni di gestione interessanti che i sistemi come Bitcoin non hanno.

Il Server Openchain espone un'API HTTP pubblica, che può essere chiamata da qualsiasi programma in grado di effettuare chiamate HTTP. Per concludere tutte queste operazioni in un'interfaccia utente intuitiva, viene fornito anche un client: il portafoglio Openchain (Openchain Wallet). Openchain Wallet è un'interfaccia web open source, disponibile su *wallet.openchain.org*.

Il Wallet è un'applicazione lato client in esecuzione nel browser e in grado di connettersi a qualsiasi endpoint Openchain. Può connettersi a più endpoint contemporaneamente, estrarre informazioni e inviare transazioni a più istanze di Openchain, tuttavia la prima volta che lo si utilizza, è necessario connettersi ad almeno un endpoint.

La prima pagina invita a connettersi a un endpoint: il portafoglio tenterà quindi di connettersi all'istanza Openchain e recuperare le informazioni sull'istanza, come mostrato in Figura 7.

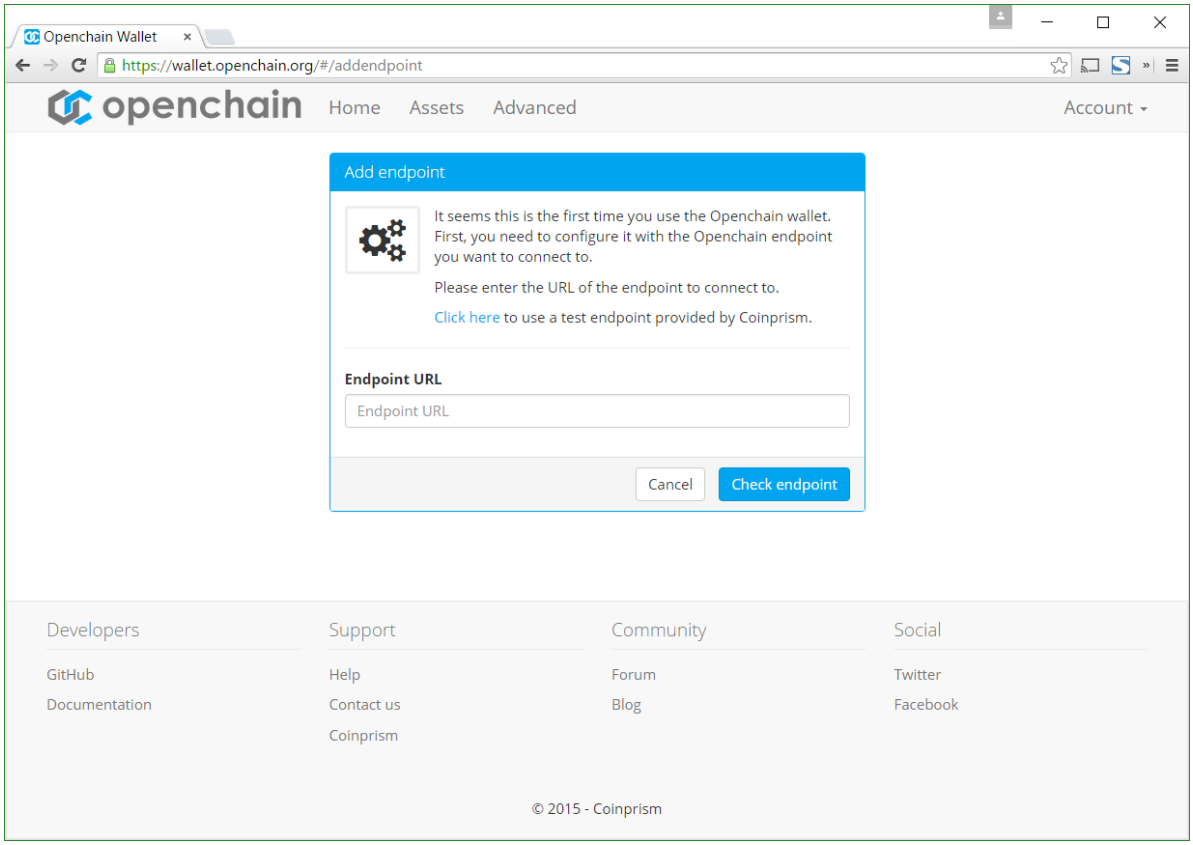


Figura 7. Openchain Wallet.

Il server Openchain espone un endpoint websocket (/stream) chiamato flusso di transazione. Il flusso di transazioni fornisce un flusso live di transazioni man mano che vengono impegnate nel libro mastro.

Il nodo Server Openchain può funzionare in due diverse modalità: modalità validatore e modalità

osservatore.

In modalità validatore, il nodo accetta le transazioni e le convalida. Le regole che rendono valida o non valida una transazione sono personalizzabili. Possono essere definite dall'amministratore del nodo validatore e sono una combinazione di regole implicite e autorizzazioni esplicite. Quando una transazione è considerata valida, viene impegnata nel libro mastro.

I nodi Observer sono nodi che si collegano a un nodo upstream e scaricano tutte le transazioni in tempo reale utilizzando il flusso delle transazioni. Il nodo validatore è sempre il nodo più a monte. Quando verifica una transazione, la transazione arriva ai suoi osservatori. Tutti gli osservatori dovrebbero avere una copia esatta dello stato detenuto dal nodo di verifica. Non è possibile inviare una transazione per la convalida a un nodo osservatore, poiché ha solo una vista di sola lettura del libro mastro. I nodi osservatori hanno la capacità di verificare l'integrità della loro copia del libro mastro attraverso gli *anchors*.

Hyperledger

Ormai il mondo è così connesso che spesso persone diverse devono accedere agli stessi dati. Per soddisfare questa esigenza, sono emersi *database distribuiti*, in cui è possibile accedere a determinati blocchi di dati da più di una persona alla volta. Ad esempio, per semplificare l'impostazione o la riprogrammazione delle riunioni, tutti i membri di un gruppo di lavoro possono condividere le loro riunioni su un calendario online. Non è possibile farlo con un calendario cartaceo. Naturalmente, nel business vengono utilizzati database condivisi più elaborati.

Una volta che inizi a condividere un database con altri, sorgono molte domande:

- Di chi ti fidi per condividere i tuoi dati?
- Come si fa a sapere che qualcuno è chi afferma di essere online?
- Cosa possono fare al database?
- Cosa succede se sia la sede centrale che il rappresentante di vendita vogliono vendere gli stessi articoli?
- Chi risolve eventuali conflitti o controversie?

Chiaramente, ci sono molti problemi pratici con la condivisione di un database. Nel corso degli anni, le persone hanno provato molte soluzioni diverse. Un nuovo modo per condividere database che può aiutare a risolvere questi problemi è attraverso la tecnologia blockchain.

Una blockchain è un database distribuito senza autorità centrale e senza punti di fiducia. Quando vuoi

condividere un database, ma non hai molta fiducia nelle altre persone che potrebbero usarlo, una blockchain può essere molto utile. In questo contesto, "fiducia" potrebbe significare molte cose. Fiducia potrebbe significare fidarsi degli altri per eseguire correttamente le azioni sul database. Fiducia potrebbe significare non cercare di indiscriminare le informazioni private degli altri. Oppure la fiducia potrebbe significare non degradare le prestazioni di qualcun altro per ottenere un vantaggio competitivo. Discutere della fiducia fa apparire i due principali tipi di blockchain. La maggior parte delle criptovalute usano blockchain senza autorizzazione in cui chiunque può unirsi e avere pieno diritto di usarlo. Ad esempio, chiunque può acquistare Bitcoin o Ether perché utilizzano blockchain spalancati e senza autorizzazioni. D'altra parte, le blockchain aziendali tendono ad essere autorizzate. Ciò significa che una persona deve soddisfare determinati requisiti per eseguire determinate azioni sulla blockchain. Alcune blockchain autorizzate limitano l'accesso agli utenti pre-verificati che hanno già dimostrato di essere chi dicono di essere. Altri consentono a chiunque di unirsi, ma consentono solo alle identità affidabili di verificare le transazioni sulla blockchain.

Indipendentemente da come sono costruite, tutte le blockchain si basano sulla crittografia, l'arte e la scienza della codifica delle informazioni in modo che siano difficili da decodificare. Hyperledger (https://www.hyperledger.org/) è un progetto iniziato nel 2015 quando molte diverse aziende interessate alla tecnologia blockchain hanno realizzato che potevano ottenere di più lavorando insieme piuttosto che lavorando separatamente. Queste aziende hanno deciso di mettere in comune le proprie risorse e creare una tecnologia blockchain open source che chiunque potesse usare. Hyperledger è stato messo sotto la tutela della Linux Foundation ed è cresciuto rapidamente negli ultimi anni. Alla data di pubblicazione, Hyperledger ha più di 230 organizzazioni come membri — da Airbus a VMware — oltre a 10 progetti con 3,6 milioni di righe di codice, 10 gruppi di lavoro attivi e quasi 28.000 partecipanti che hanno partecipato a oltre 110 incontri in tutto il mondo.

I registri distribuiti possono avere requisiti notevolmente diversi per diversi casi d'uso. Ad esempio, quando i partecipanti condividono alti livelli di fiducia, ad esempio tra istituti finanziari con accordi legali, le blockchain possono aggiungere blocchi alla catena con tempi di conferma più brevi utilizzando un algoritmo di consenso più rapido. D'altra parte, quando vi è una fiducia minima tra i partecipanti, le blockchain devono tollerare una elaborazione più lenta per una maggiore sicurezza. Hyperledger abbraccia l'intero spettro dei casi d'uso. Riconosciamo che diversi scenari aziendali hanno

requisiti diversi per tempi di conferma, decentralizzazione, affidabilità e altri problemi e che ogni problema rappresenta un potenziale "punto di ottimizzazione" per la tecnologia. Per affrontare questa diversità, tutti i progetti Hyperledger seguono la stessa filosofia progettuale. Tutti i progetti devono essere:

• Modulari
• Altamente sicuri
• Interoperabili
• Criptovaluta-agnostici
• Completi di API.

Tutti i progetti Hyperledger forniscono API ricche e facili da usare che supportano l'interoperabilità con altri sistemi. Un set ben definito di API consente a client e applicazioni esterni di interfacciarsi rapidamente e facilmente con l'infrastruttura di contabilità generale distribuita di Hyperledger. Queste API supportano la crescita di un ricco ecosistema di sviluppatori e aiutano la blockchain e le tecnologie di contabilità distribuita a proliferare in una vasta gamma di settori e casi d'uso.

Tra i vari casi d'uso attualmente supportati da Hyperledger, quello più vicino al caso di interesse della Black Box della casa è probabilmente l'Hyperledger Fabric, relativo ai settori industriali manifatturieri.

Hyperledger Fabric è una piattaforma per la creazione di soluzioni di libro mastro distribuito, con un'architettura modulare che offre alti livelli di riservatezza, flessibilità, resilienza e scalabilità. Ciò consente alle soluzioni sviluppate con Fabric di adattarsi a qualsiasi settore. Fabric consente a componenti, come il consenso e i servizi di appartenenza, di essere plug-and-play. Sfrutta la tecnologia dei container per ospitare contratti intelligenti chiamati "chaincode" che contengono le regole aziendali del sistema. Ed è progettato per supportare vari componenti collegabili e per soddisfare la complessità esistente in tutta l'economia. Partendo dalla premessa che non esistono soluzioni "taglia unica per tutti", Fabric è una piattaforma blockchain estensibile per l'esecuzione distribuita applicazioni. Supporta vari protocolli di consenso, quindi può essere adattato a diversi casi d'uso e modelli di fiducia.

Fabric esegue applicazioni distribuite scritte in linguaggi di programmazione generici senza dipendere da alcuna criptovaluta nativa. Ciò è in netto contrasto con la maggior parte delle altre piattaforme blockchain per l'esecuzione di contratti intelligenti, che richiedono che il codice sia scritto in un linguaggio specifico del dominio oppure si basano su una criptovaluta. Inoltre, Fabric utilizza una

nozione portatile di appartenenza per il modello autorizzato, che può essere integrato con la gestione delle identità standard del settore. Per supportare tale flessibilità, Fabric adotta un nuovo approccio architettonico e rinnova il modo in cui le blockchain affrontano il non determinismo, l'esaurimento delle risorse e gli attacchi alle prestazioni. Fabric può anche creare canali, che consentono a un gruppo di partecipanti di creare un registro separato delle transazioni. Ciò è particolarmente importante per le reti in cui alcuni partecipanti potrebbero essere concorrenti che non desiderano ogni transazione, ad esempio un prezzo speciale offerto ad alcuni ma non a tutti, noto a tutti i partecipanti alla rete. Se un gruppo di partecipanti forma un canale, solo quei partecipanti e nessun altro hanno copie del libro mastro per quel canale.

Figura 8. Progetto Hyperledger Fabric.

Open Blockchain

Open Blockchain (https://developer.ibm.com/open/projects/open-blockchain/) è un libro mastro di eventi digitali, chiamati transazioni, condivisi tra diversi partecipanti, ciascuno con un interesse nel sistema. Il libro mastro può essere aggiornato solo per consenso dei partecipanti e, una volta registrato, le informazioni non possono mai essere modificate. Ogni evento registrato è crittograficamente verificabile con prova di accordo da parte dei partecipanti.

Da un punto di vista tecnico, Open Blockchain è un'architettura fabric che consente alle aziende di sfruttare la potenza di database crittograficamente sicuri, immutabili (solo appendice), distribuiti e peer-to-peer. Questi sono comunemente noti come "blockchain", i pionieri delle comunità Bitcoin ed Ethereum.

Blockchain è una tecnologia di libro mastro distribuita peer-to-peer per una nuova generazione di applicazioni transazionali. Stabilisce fiducia, responsabilità e trasparenza, razionalizzando i processi aziendali. Pensalo come un sistema operativo per le interazioni. Ha il potenziale per ridurre enormemente i costi e la complessità delle attività.

Open Blockchain è un protocollo modulare per la registrazione e l'accesso alle transazioni su un libro mastro privato. Le transazioni, in questo contesto, possono avere un'ampia definizione, che va dai dati alle risorse, istruzioni e identità. Un sistema che combina sia il protocollo di elaborazione

transazionale che l'archivio informazioni è un grande vantaggio per più domini. Ad esempio, il protocollo è modulare in modo che gli amministratori di rete possano definire i propri vincoli e quindi impostare il protocollo di conseguenza.
Questo tessuto open source consente a infiniti gruppi di attori unici di creare le proprie reti. Le comunità creano una rete autorizzata, in cui i nodi di convalida e non di convalida sono gestiti da entità note autorizzate. A queste identità viene concesso l'accesso da un'autorità emittente sulla rete. Questo modello è sostanzialmente diverso dalle blockchain attuali.

Open Blockchain estende le tradizionali tecnologie blockchain incorporando:

- Logica (codice catena): il codice catena estende i contratti intelligenti tradizionali, definiti in generale come accordi di auto-esecuzione scritti in codice che possono interagire e possono innescare altri contratti intelligenti, ma con ulteriori capacità. Il codice catena viene eseguito in contenitori Docker sandbox e può interagire con altre reti hlp-fabric-golang o con il mondo esterno. Ancora più importante, il codice a catena è immutabile, può mantenere lo stato ed ereditare la riservatezza / privacy.

- Riservatezza variabile: le reti possono limitare chi può visualizzare o interagire a diversi livelli dell'ambiente. Le singole transazioni possono persino imporre le proprie regole di riservatezza.

- Identificazione verificabile: sebbene la rete possa impostare l'offuscamento dell'identità, è possibile avere peer anonimi al 100% la cui identità è anche provabile e unica con tecniche crittografiche sicure. Se gli utenti di una rete concedono l'autorizzazione, un revisore sarà in grado di anonimizzare gli utenti e le loro transazioni. Ciò è utile per ispezioni e analisi normative.

- Transazioni private: i dettagli di una transazione, inclusi ma non limitati a chain-code, peer, risorse e volumi sono crittografati. Ciò elimina qualsiasi riconoscimento di modello o informazioni private trapelate agli attori non autorizzati sulla rete. Solo gli attori specificati possono decrittografare, visualizzare e interagire / eseguire (con il codice catena).

- Protocolli di consenso personalizzabili: il tessuto funzionerà facilmente con quasi tutti i meccanismi di consenso. Questo design architettonico personalizzabile rende Open Blockchain adatta per più applicazioni.

Benchmark di Blockchain

Hyperledger **Caliper** è uno strumento di benchmark blockchain che misura le prestazioni di qualsiasi implementazione blockchain utilizzando una serie di casi d'uso predefiniti. Caliper produce report che mostrano una serie di indicatori di rendimento, quali:

• Utilizzo delle risorse

• Latenza delle transazioni

• Transazioni al secondo (TPS)

• Altri da definire.

Prima di Caliper non esisteva uno strumento generale che fornisse valutazioni delle prestazioni per diverse soluzioni blockchain, basato su una serie di regole neutre e comunemente accettate. Caliper non pubblicherà i risultati del benchmark. L'idea è di utilizzare Caliper come riferimento interno per aiutare a scegliere l'implementazione blockchain più adatta alle esigenze specifiche di un'azienda. Hyperledger Caliper fornisce uno strumento di benchmark funzionante che può essere eseguito su molti framework Hyperledger. La comunità continuerà a definire ulteriori indicatori di prestazione e casi d'uso di riferimento. Il successo del progetto dipenderà dal fatto che molti membri della comunità lo utilizzeranno come strumento di riferimento.

Caratteristiche chiave di Caliper:

- Un framework di riferimento unificato blockchain. Viene fornito un livello comune da integrare con i principali framework / piattaforme blockchain esistenti, in modo che gli stessi benchmark possano essere eseguiti per diversi sistemi blockchain Verrà fornito un ambiente di test benchmark per aiutare diverse persone a eseguire test nello stesso ambiente, strumenti di gestione blockchain. Inoltre, gli utenti possono utilizzare il loro ambiente esistente e configurare Caliper per eseguire il test nell'ambiente.
- Una definizione comunemente accettata di indicatori di prestazione.
- Una serie di casi di riferimento comunemente accettati. L'obiettivo di Caliper include la

fornitura di una serie di casi benchmark facilmente comprensibili in modo che ogni soluzione blockchain possa essere confrontata in vari scenari.

3. IOTA

IOTA (https://iotaitalia.com/) è un token crittografico di nuova generazione, creato per essere lightweight e venire utilizzato nell'Internet of Things, contrariamente alle altre crittovalute che sono nate per scopi diversi e che sono basate su Blockchain complesse e gravose.
Nella prossima decade si stima che ci saranno più di 50 miliardi di dispositivi connessi a Internet, i quali renderanno disponibili servizi dall'utilità inimmaginabile dovendo però allo stesso tempo affrontare problematiche di diversa natura, fra cui quella delle microtransazioni. Tali dispositivi infatti dovranno essere in grado di scambiare tra loro minuscole quantità di denaro, in modo immediato e possibilimente senza constringere i produttori a scendere a compromessi nel design e nella dotazione di hardware. Proprio per questo scopo è stato concepito IOTA, che tuttavia rimane adatto anche a qualsiasi altro scenario in cui ci sia necessità di gestire microtransazioni, oltre all'IoT.
Per raggiungere questo obiettivo, al momento della progettazione di IOTA si è scelto di prendere le distanze dalle crittovalute basate su Blockchain. Pur mantenendo la visione legata a un consenso distribuito, risultò necessario un approccio diverso per rendere il network scalabile nell'ambito di un ecosistema di IoT, in cui saranno presenti decine di miliardi di dispositivi connessi. Nacque così la principale innovazione di IOTA, il Tangle.

Caratteristiche di IOTA

- **Nessun costo di transazione**

  Per inviare una transazione IOTA, il dispositivo del mittente deve semplicemente verificare due transazioni precedenti nel Tangle, effettuando Proof of Work con difficoltà molto bassa. Nessun costo di transazione, nessuna separazione fra miners e utenti.

- **Infinitamente scalabile**

  Visto che per inviare una transazione occorre prima confermarne altre due, all'aumentare

degli utenti aumenta anche l'efficienza della rete. IOTA scala proporzionalmente al numero delle transazioni.

- **Transazioni rapide**

  I tempi di esecuzione delle transazioni sono inversamente proporzionali al numero di transazioni nel Tangle. Quando IOTA raggiungerà un'adozione di massa, le transazioni saranno pressochè istantanee.

- **Offerta di moneta fissa**

  Tutti i token esistenti sono stati creati nel genesis block, e tale quantità non varierà mai. La quantità totale corrisponde a 2,779,530,283,277,761 iota, numero ottimizzato per la computazione ternaria e per essere conforme alla notazione del SI.

- **Quantum-resistant**

  IOTA usa firme crittografiche hash-based anzichè crittografia a curva ellittica, ed esse offrono maggior velocità e semplicità nella verifica dei dati, riducendo la complessità del Tangle.

IOTA usa il Tangle, che è un protocollo software basato su grafici aciclici diretti e visceralmente diverso dal protocollo blockchain. L'innovazione del Tangle è che le transazioni vengono processate in parallelo, il che permette a IOTA di scalare in maniera direttamente proporzionale alla crescita del network. Come visto in precedenza, in IOTA non esiste il mining e i blocchi, quindi le transazioni del Tangle vengono confermate in maniera asincrona. Il Tangle è programmato ternariamente, ed è quindi molto più efficiente delle applicazioni binarie.

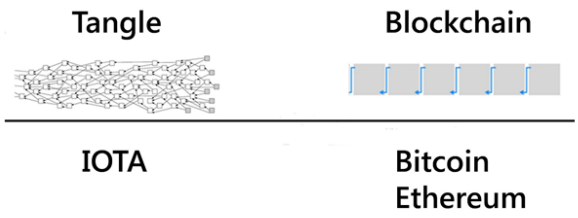


Figura 9. Confronto Tangle-Blockchain.

Il Tangle risolve i seguenti problemi, che invece si presentano con le applicazioni Blockchain:

Centralizzazione del controllo: storicamente è evidente come i miner tendano ad aggregarsi in grandi gruppi per mettere in comune la potenza di calcolo e dividere le ricompense. Questa dinamica porta alla centralizzazione del potere computazionale e di conseguenza anche a una centralizzazione del potere decisionale nelle mani di poche pool di miners, dando loro la facoltà di applicare vari tipi di discriminazione verso determinate transazioni. Nonostante non ci siano ancora stati casi eclatanti di abuso di potere da parte dei miners (anche se il recente dibattito sul block size di Bitcoin potrebbe contare come precedente), la mera possibilità che ciò accada in un sistema monetario alla base di una industria multimiliardaria è inaccettabile.

Crittografia obsoleta: nonostante i computer quantistici non siano ancora prodotti di consumo, è opportuno iniziare già a sviluppare soluzioni che siano quantum-resistant da un punto di vista crittografico. Per quanto riguarda la sicurezza, è ragionevole ipotizzare che hardware capace di craccare algoritmi crittografici classici possa essere presto disponibile.

Difficoltà nel gestire micropagamenti: i costi di transazione delle crittovalute Blockchain sono presenti per ricompensare i miner e per evitare spam del network, tuttavia allo stesso tempo stabiliscono una soglia sotto alla quale diventa antieconomico inviare pagamenti.

Difficoltà nel gestire le partizioni: le crittovalute basate su Blockchain hanno difficoltà a sopravvivere a lungo nel caso di ripetute partizioni della rete, per via del rischio che quest'ultime portino all'annullamento di grandi quantità di transazioni. Risulta anche difficile eseguire partizioni deliberate quando necessario.

Discriminazione degli utenti: le crittovalute esistenti sono sistemi eterogenei con chiare separazioni dei ruoli fra gli utenti, le quali rendono inevitabili successive discriminazioni e conseguenti conflitti.

Limiti di scalabilità: alcune crittovalute hanno limiti immutabili per quanto riguarda il numero di transazioni, e tali limiti non possono essere rimossi in modo decentralizzato. Risulta inoltre quasi impossibile, al momento della creazione di una crittovaluta, riuscire a stimare con esattezza i valori di

tali limiti che saranno ideali nel momento in cui il sistema sarà in esecuzione alla sua massima capacità.

Alti requisiti di hardware: le crittovalute basate su Bitcoin utilizzano l'approccio originale basato su script per l'implementazione di numerosi casi d'uso. Altre crittovalute invece utilizzano approcci più simili a quelli di istituzioni come banche, aggiungendo caratteristiche addizionali. Entrambi tali approcci comportano requisiti hardware sostanzialmente alti, per via della complessa logica di gestione delle transazioni.

Illimitata crescita dei dati: l'immagazzinamento di tutti gli stati di transizione porta alla repentina crescita dei dati, senza però aumentare significativamente le informazioni sui saldi registrate. Questa inefficienza non può essere rimossa nemmeno tramite tecniche di data pruning, e la diffusione esplosiva di una crittovaluta afflitta da tale problema potrebbe portare al suo fallimento.

In ogni caso IOTA non punta a rimpiazzare completamente le applicazioni Blockchain, piuttosto può concorrere all'espansione dell'attuale ecosistema svolgendo il ruolo di oracolo per piattaforme di smart contracts come Etehreum e Rootstock. Inoltre IOTA può aumentare la sicurezza delle Blockchain, offrendo loro la possibilità di includere checkpoint per le transazioni.

4. Caratteristiche funzionali e tecnologiche

Il registro distribuito è solo una componente delle blockchain: la tecnologia delle basi di dati distribuite, infatti, esiste da più di quarant'anni ed è oggi ampiamente utilizzata da una miriade di servizi online che poco o nulla hanno che fare hanno con le blockchain.
Realizzare una blockchain significa implementare non solo un registro distribuito, ma anche vari meccanismi per consentire agli attori della tecnologia di interagire con tale registro (cioè leggerlo e, all'occorrenza, modificarlo e propagare le modifiche a tutte le copie del registro).
Se si considera il Bitcoin come esempio più famoso di sistema basato su una blockchain, tale criptovaluta deve la sua fortuna non soltanto dall'uso di un registro distribuito, ma anche alla sapiente implementazione di algoritmi innovativi per la convalida delle transazioni monetarie (crittografia a chiave pubblica), nonché per la remunerazione, gli incentivi e l'avvicendamento delle code (il

cosiddetto “proof of work”) e dei portafogli elettronici dei suoi correntisti, oltre che mantenere la sostenibilità (tramite i cosiddetti “minatori” di bitcoin) e l’auto-consistenza della sua blockchain. È bene perciò effettuare un’analisi dei costi adeguata prima di realizzare con una blockchain un servizio che potrebbe essere efficacemente (ed economicamente) realizzato mediante un sottoinsieme di tali tecnologie, come ad esempio basi di dati “sublimati” in cloud per ottenere una efficace e conveniente decentralizzazione dei dati.

Riguardo l’affidabilità, vanno anche qui valutati individualmente i diversi componenti tecnologici di una blockchain, per poi considerarne la sicurezza nella sua interezza. Innanzitutto, è sempre l’uomo a programmare gli algoritmi di funzionamento delle blockchain, perciò uno dei passi da affrontare è effettuare valutazioni di impatto proprio su questa componente “software”, prendendo in considerazione scenari ove codice “malevolo” o comunque non autorizzato viene eseguito dai nodi, eventualmente modificando lo schema decisionale della blockchain. In alcune blockchain, ad esempio, la variazione degli algoritmi di funzionamento (cioè le “regole del gioco”) è essa stessa una funzionalità contemplata by design, ma solo a fronte di un quorum tra i nodi che ne fanno parte, stabilita con modalità più o meno automatizzate. In alcuni casi è necessaria una maggioranza assoluta dei nodi, che divengono in quel caso “plenipotenziari” relativamente ai cambiamenti effettuabili. Va considerato, quindi, che le blockchain neonate, formate inizialmente da pochissimi nodi, potrebbero facilmente costituire delle “oligarchie informatiche” auto-regolamentanti, anziché fornire un esempio di democrazia tecnologica.

Anche senza valutare scenari così estremi, la logica di funzionamento di molte blockchain potrebbe essere codificata *ab initio* per subire metamorfosi pre-programmate del proprio codice non appena l’inflazione dei nodi superi determinate soglie, seguendo meccanismi noti dello sviluppo biologico e anche, si badi bene, a prodotti finanziari ben più tradizionali.

Attenzione però: una blockchain pur dotata di una “costituzione democratica” e i cui nodi siano in totale buona fede potrebbe essere vulnerabile a una “congiura tecnica” di agenti malevoli che, violando un numero di nodi pari al quorum, si impossessano dell’intera blockchain, realizzando quello che viene chiamato, appunto, “attacco del 51%”. Tali problematiche sono perciò legate all’inflazione intrinseca nelle blockchain. Proprio per questo motivo è necessario che gli stakeholder coinvolti possano revisionare il codice sorgente e verificare che tale codice sia quello realmente in esecuzione sui nodi dell’effettiva blockchain d’interesse, ad esempio mediante meccanismi di apposizione di firme

o sigilli elettronici sul codice, che siano a loro volta verificabili in maniera indipendente ed "esterna" dalla blockchain. Il governo di molte tecnologie blockchain è decentralizzato e tolto dall'appannaggio di una singola autorità di controllo; questo aspetto sicuramente innovativo e dirompente è spesso uno dei migliori argomenti a favore di tali tecnologie. Tuttavia, una tecnologia senza un'autorità centrale "di governo" è cosa ben diversa da una senza alcun controllo a livello "tecnico"; è bene puntualizzare questa importante differenza, che può generare gravi problemi di sicurezza.

Nel caso delle blockchain "private" (o *permissioned*, come si chiamano in gergo), la robustezza del registro dipende dall'obbligo di identificare coloro che lo consultano e, ancor più, che ne modificano il contenuto, mediante sistemi di controllo sicuro delle autorizzazioni. Tuttavia, anche nel caso di blockchain completamente "aperte" (o *permissionless*) – che possono essere consultate e modificate da chiunque – tale controllo inteso come mera autenticazione continua ad essere requisito fondamentale, in quanto le firme digitali che legano ogni blocco della catena al successivo si basano sul controllo dell'integrità del blocco precedente. La Figura 9 sintetizza le differenze tra le due.

Anche in questo caso l'auto-consistenza dell'intera blockchain è protetta dalla robustezza del sistema di identificazione effettuato dai nodi: chiunque può accedervi, ma l'integrità di ogni transazione (o blocco di transazioni) sarà comunque riconducibile alle entità autenticate per essa.

Guardando alla legislazione italiana, si attribuisce alle blockchain il ruolo di *marcature temporali* che, secondo il Regolamento europeo (UE) 910/2014, denominato "eIDAS", sono una tipologia di servizi

Tipi di blockchain		Chi può accedere e vedere le transazioni	Chi può generare transazioni e inviarle alla rete	Chi può aggiornare
Aperta	Pubblica senza permesso	Aperta a tutti	Chiunque	Chiunque
	Pubblica con permesso	Aperta a tutti	Partecipanti autorizzati	Tutti o un sotto gruppo dei partecipanti autorizzati
Chiusa	Consorzio (più organizzazioni)	Ristretta ad un gruppo di partecipanti autorizzati	Partecipanti autorizzati	Tutti o un sotto gruppo dei partecipanti autorizzati
	Impresa (differenti unità all'interno di una singola organizzazione)	Completamente privata o ristretta a un gruppo limitato di nodi autorizzati	Solo l'operatore di rete	Solo l'operatore di rete

Fonte: World Economic FORUM[28]

Figura 9. Blockchain pubblica vs privata.

fiduciari elettronici che collegano dei dati a una particolare ora e data, così da provarne l'esistenza in quel momento.

Il Regolamento eIDAS disciplina anche le *firme* e i *sigilli elettronici* che, come abbiamo visto, sono anch'essi tasselli fondamentali per qualunque blockchain, in quanto l'immutabilità e l'autenticità di ciascun blocco della catena sono, in ultima analisi, sempre garantiti dall'apposizione di un sigillo elettronico (se in capo a un software o comunque per conto di un soggetto giuridico), ovvero alla sottoscrizione mediante una firma elettronica (se da parte di una persona fisica).

Il Regolamento eIDAS tratta, infine, gli schemi di identificazione elettronica (in Italia, lo SPID e la Carta d'Identità Elettronica) quali tasselli fondamentali per autenticare cittadini e imprese, in maniera interoperabile e transfrontaliera, presso qualunque servizio online. A tali schemi potrebbe, ad esempio, essere demandata la fase di mera autenticazione presso alcune tecnologie blockchain, invece di una vera e propria firma elettronica (argomento trattato, tra l'altro, anche dall'art. 20 del CAD e di prossima emanazione con apposite Linee Guida da parte di AGID). Bisogna precisare, però, che solo le firme, i sigilli e le marcature temporali elettroniche *qualificate* ai sensi del Regolamento eIDAS, così come gli schemi di identificazione elettronica *notificati* alla Commissione Europea (ad oggi solo lo SPID), garantiscono la piena interoperabilità a livello europeo, oltre alla garanzia di poterne facilmente verificare la validità mediante strumenti aperti e disponibili nell'internet pubblico.

Ancora una volta, non va confusa l'assenza di un'autorità centralizzata che governi alcune tipologie di blockchain, con la mancanza di un sistema "aperto" che permetta di convalidare alcuni aspetti quali il codice sorgente, la precisione dell'orario ovvero le modifiche al registro distribuito.

Per l'assenza della prima, infatti, trattasi di una specificità architetturale che, quando presente, è tipicamente voluta by design; per la mancanza della seconda, invece, trattasi di una vera e propria vulnerabilità di sicurezza. Per essere precisi, una caratteristica peculiare delle blockchain consiste nell'autenticità e immutabilità intrinseca dei dati in esse contenuti (ex art. 8-ter del decreto semplificazioni), ottenuta dalla possibilità di verificare l'integrità di ogni blocco risalendo ricorsivamente all'indietro all'integrità di blocchi precedenti, fra di loro incatenati.

Sebbene ciò sia teoricamente realizzabile e potrebbe in linea di principio sostituire l'esigenza di affidarsi ad autorità certificanti per la validità dei suddetti servizi fiduciari elettronici, vi sono due

problematiche di sicurezza associate. Innanzitutto, il *trust model* appena descritto implica che la "fiducia tecnica" dell'intera blockchain dipenderebbe interamente dalla fiducia nelle primissime transazioni avvenute nel registro, ricadendo quindi nelle problematiche del modello inflazionario delle blockchain descritto poco sopra.

Come secondo problema, a fronte della possibilità teorica, vi è invece l'impossibilità tecnica di effettuare tali verifiche ricorsive qualora il registro distribuito diventi una catena di blocchi troppo lunga: la convalida completa dell'intera catena comporterà una richiesta di risorse computazionali e di rete definitivamente eccessiva (che, se non adeguatamente gestita, potrebbe rendere l'intera blockchain indisponibile a causa di eccessive richieste di convalida).

Un ultimo aspetto che ogni valutazione di impatto su una tecnologia blockchain dovrebbe considerare riguarda infine l'infrastruttura tecnologica su cui le blockchain, immancabilmente, vengono eseguite.

Che si tratti di dispositivi mobili sotto il *presunto* esclusivo controllo degli utenti, di macchine virtuali sublimate in qualche cloud più o meno privato, ovvero di server in "vil metallo" che "minano e sminano" senza sosta in locali definiti con precisione catastale, la più tradizionali minacce informatiche non dovrebbero mai essere ignorate.

Il rischio di infettare, corrompere, esfiltrare i dati "incatenati", o di rendere comunque inutilizzabile parte dell'infrastruttura deve essere valutato, possibilmente confrontato con quello legato a diverse scelte tecnologiche e, infine, adeguatamente trattato o mitigato. La decentralizzazione delle blockchain va di pari passo con l'elevata interconnettività tra i suoi nodi ed utenti (questi ultimi spesso connessi tramite il proprio smartphone), contribuendo perciò al perimetro di sicurezza che tende a gonfiarsi e sgretolarsi sempre di più e va, perciò, adeguatamente protetto.

5. Attività di standardizzazione

Prima di analizzare quali sono le attività di standardizzazione in corso sulle tecnologie Blockchain e Distributed Ledger Technologies (BDLT) è utile provare a comprendere quale può essere l'utilità di avere standard in questo ambito posto che finora l'uso massivo di queste tecnologie è stato in ambito criptovalute, ognuna delle quali nata spontaneamente e operante come un'isola a sé stante.

In realtà gli utilizzi più promettenti delle tecnologie BDLT che stanno emergendo e si stanno consolidando, in aree diverse dalle criptovalute, sono ambiti dove gli standard possono svolgere un

ruolo abilitante chiave.

Le tecnologie BDLT abilitano principalmente l'implementazione di infrastrutture di notarizzazione che non prevedono la necessità di una governance centralizzata pur garantendo resistenza alla manomissione delle informazioni e sicurezza attraverso protocolli e tecniche crittografiche che garantiscono consenso condiviso, distribuzione delle risorse e disintermediazione dando disponibilità di dati aggiornati e affidabili in tempi ragionevoli a tutte le parti interessate e collegate all'infrastruttura.

La disponibilità di standard per questo tipo di infrastrutture può svolgere un ruolo abilitante fondamentale in quanto, a differenza del caso delle criptovalute, le esigenze fondamentali sono la possibilità di integrare servizi ed applicazioni gestite da soggetti diversi e garanzie sufficienti di disponibilità, integrità ed origine delle informazioni e delle transazioni.

L'esigenza naturalmente è anche quella di avere standard che devono essere il più possibile globali che tengano però conto della compliance con le esigenze specifiche europee, legate ad esempio all'esigenza di compliance con le normative in materia di protezione dei dati personali (quali il Regolamento Europeo n 679/2016 - GDPR).

La mancanza di interoperabilità crea limiti tecnici che la Commissione europea cerca da tempo di eliminare per realizzare il mercato interno (si veda ad esempio il Libro bianco sul completamento del mercato interno, 14 giugno 1985, COM (85) 310 def).

In ambito BDLT è però particolarmente complesso sviluppare degli standard, dato che si tratta di un mercato con potenzialità elevate ma immaturo dove le uniche applicazioni su larga scala sono ad oggi le criptovalute che sono un fenomeno nato dal basso e piuttosto refrattario a regole imposte dall'esterno. Inoltre, si tratta di tecnologie tipicamente "orizzontali" e gli standard devono poter supportare da un lato una elevata molteplicità di applicazioni in ambiti disparati, dall'altro la compliance a regole comuni, si pensi ad esempio al già citato GDPR ma anche ad eIDAS per identità e servizi fiduciari.

Le attività di normazione tecnica in corso si svolgono a livello internazionale nel comitato tecnico ISO/TC 307. In Europa, per monitorare i lavori internazionali al fine di identificare eventuali carenze rispetto ad esigenze europee e quindi portarle e discuterle sui tavoli ISO, è stato creato congiuntamente da CEN e CENELEC il Focus Group Blockchain and Distributed Ledger Technologies.

Le aree di standardizzazione si concentrano su due aspetti principali:

- l’interoperabilità, identificando architetture di riferimento ed elementi base interoperanti e per consentire l’utilizzo dell’infrastruttura da parte di qualsiasi applicazione che necessita di servizi di notarizzazione;
- la compliance, per consentire la garanzia di livelli di sicurezza e affidabilità accettabili e il rispetto di norme vincolanti come quelle in materia di protezione dei dati personali.

L’uso di standard può supportare entrambe queste esigenze.

ISO/TC 307 “Blockchain and distributed ledger technologies” è un Comitato Tecnico che è stato istituito in ISO per rispondere alla crescente necessità di standardizzazione in questo settore.

L’ISO garantisce modalità di lavoro concordate a livello internazionale e gli obiettivi principali che si pone per migliorare la sicurezza, la protezione dei dati personali e l’interoperabilità al fine di facilitare l'uso a livello globale di questa tecnologia.

Ciò è particolarmente importante sia lato offerta, per supportare una competizione corretta in un mercato che vede la presenza di molte PMI che sviluppano prodotti, soluzioni e servizi basati su questa tecnologia, sia lato domanda, che richiede strumenti interoperabili e che garantiscano livelli certi di compliance, sicurezza e affidabilità.

Per far fronte in modo strutturato alle esigenze che nascono in ambito europeo e mappare queste esigenze sui lavori in corso a livello internazionale è nato un Focus Group in ambito CEN/CENELEC, due dei tre enti di standardizzazione riconosciuti a livello UE.

Il Focus Group CEN/CENELEC “Blockchain and Distributed Ledger Technologies” ha prodotto il white paper “Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies”.

Il Libro bianco affronta temi prioritari quali lo sviluppo sostenibile, l'identità elettronica, la privacy e la protezione dei dati fornendo 26 raccomandazioni e mettendo in evidenza casi specifici di utilizzo europeo. In particolare, la protezione dei dati personali è l’area sulla quale è più urgente un intervento in quanto il GDPR da un lato è una normativa molto stringente e, dall’altro, ha comunque un'applicazione regionale mentre ISO opera a livello globale, è necessario che l’Europa inizi ad avere un ruolo diretto nello sviluppo di standard in quest’area.

Quanto al contesto italiano è stata istituita la Commissione UNI/CT 532 in seno ad UNINFO che svolge attività di mirror rispetto a quelle internazionali ed europee. È infatti fondamentale che qualunque

contributo nazionale tenga conto della collocazione dell'Italia nel contesto europeo e mondiale.

6. Riferimenti

https://docs.openchain.org/en/latest/index.html

https://www.hyperledger.org/

https://developer.ibm.com/open/projects/open-blockchain/

https://iotaitalia.com/