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

ISTI Technical Reports

La definizione di dati, funzioni e servizi ascrivibili alla Black Box della casa

Vittorio Miori, CNR-ISTI, Pisa, Italy

Dario Russo, CNR-ISTI, Pisa, Italy

Loredana Pillitteri, CNR-ISTI, Pisa, Italy

ISTI-TR-2020/026

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

La definizione di dati, funzioni e servizi ascrivibili alla Black Box della casa

Miori V.; Russo D.; Pillitteri L.

ISTI-TR-2020/026

Abstract

Il documento riguarda la definizione dei dati e delle funzioni riferibili alla cosiddetta "Black Box" della casa. Il concetto di Black Box della casa è da intendersi come una sorta di alter ego virtuale, costituito appunto da dati e funzioni, di tutti i sistemi e gli eventi ad essi relativi che si sono manifestati all'interno della casa, e che ricadono nei domini dell'Energy, Safety & Security, e Comfort manager. La Black Box è dunque concepita come una impronta digitale dello stato della casa, aggiornata e storicizzata nel tempo, che deve essere non modificabile, non accessibile in scrittura, e tale da garantire l'integrità dei dati e l'accesso ad essi ai soli autorizzati. Una sorta di "carta di identità" della casa e di tutti i suoi sistemi e servizi, intesa anche come strumento a garanzia dei diversi proprietari che nel tempo potrebbero entrarne in possesso.

Black box domestica, Scatola nera della casa, Carta d'identità della casa, Dati funzioni e servizi per l'energia, Dati funzioni e servizi per la sicurezza, Dati funzioni e servizi per il comfort, Blockchain, Framework di interoperabilità, Domotica, Home automation

Citation

Miori V.; Russo D.; Pillitteri L. *La definizione di dati, funzioni e servizi ascrivibili alla Black Box della casa* ISTI Technical Reports 2020/026. DOI: 10.32079/ISTI-TR-2020/026

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

La definizione di dati, funzioni e servizi ascrivibili alla Black Box della casa

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

Breve sommario

Questo documento riguarda la definizione dei dati e delle funzioni riferibili alla cosiddetta “Black Box” della casa. Il concetto di Black Box della casa è da intendersi come una sorta di alter ego virtuale, costituito appunto da dati e funzioni, di tutti i sistemi e gli eventi ad essi relativi che si sono manifestati all’interno della casa, e che ricadono nei domini dell’Energy, Safety & Security, e Comfort manager. La Black Box è dunque concepita come una impronta digitale dello stato della casa, aggiornata e storicizzata nel tempo, che deve essere non modificabile, non accessibile in scrittura, e tale da garantire l’integrità dei dati e l’accesso ad essi ai soli autorizzati. Una sorta di “carta di identità” della casa e di tutti i suoi sistemi e servizi, intesa anche come strumento a garanzia dei diversi proprietari che nel tempo potrebbero entrarne in possesso.

Parole chiave

Black box domestica, scatola nera della casa, carta d’identità della casa, dati funzioni e servizi per l’energia, dati funzioni e servizi per la sicurezza, dati funzioni e servizi per il comfort, blockchain, framework di interoperabilità, domotica, home automation.

Indice

1. Il concetto di Black Box della casa

E' una sorta di "carta d'identità" o di "curriculum" della casa che riguarda tutti i suoi aspetti (strutturali e tecnologici); in esso 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 della 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.

Esempi di soluzioni simili al concetto di "Black Box" della casa sono 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. Definizione dei dati inclusi nella Black Box della casa

In questa sezione viene specificato quali dati si ritiene utile inserire o far confluire nella Black Box della casa, ovviamente relativi ai manager in essa presenti

2.1 Dati pertinenti dall'Energy Manager

La necessità di sopperire ai limiti, emersi in anni recenti, relativi all'approvvigionamento e distribuzione energetici delle reti odierne, ha suggerito l'opportunità di migliorare le performance in termini di efficienza, gestione e consumi energetici dell'ambiente domestico, onde fornire supporto ad una nuova classe di reti intelligenti di distribuzione elettrica, le cosiddette "Smart Grid".

Gli studi portati avanti nell'ambito della ricerca scientifica hanno evidenziato, in tal senso, come la gestione automatizzata delle risorse domestiche, fornisca gli strumenti per adottare la tariffazione dinamica dell'energia, dando la possibilità al gestore di promuovere o frenare il consumo su base oraria, al fine di modulare il carico cui la rete di distribuzione è sottoposta, pur massimizzando il comfort per l'utente.
In alcune circostanze, la ricerca può correre il rischio di perdere di vista il contesto nel quale le soluzioni tecnologiche allo studio andranno calate in futuro. Alcuni studi hanno infatti evidenziato come la gestione dell'energia venga orientata alla massimizzazione dell'efficienza anche a discapito del comfort dell'utente, ottenendo dunque uno scomodo ribaltamento delle priorità. Al contrario, la visione di SHELL è che un ambiente non possa ritenersi domestico, se non mette in primo piano il comfort dell'utente e renda quest'ultimo l'assoluto protagonista, libero di scegliere sulla base delle proprie esigenze. Proprio sulla base di queste, l'ambiente domotico dovrà adattare la gestione delle risorse e dell'ambiente, tenendo conto delle direttive ricevute, in modo da migliorare l'efficienza energetica della casa secondo diversi criteri di performance e agevolare l'interazione con il mondo esterno.

Alla luce di questa prospettiva, un manager per le risorse energetiche domestiche avrà le seguenti fondamentali caratteristiche funzionali:

- ausilio per l'utente: fornire informazioni chiare e puntuali sullo stato dei dispositivi energetici e sul consumo effettuato su diversi orizzonti temporali; definizione di what-if scenarios da mettere a disposizione dell'utente per la consumption awareness;
- supervisione energetica dell'ambiente domotico: raccogliere e conservare le informazioni relative all'attività dell'utente, allo stato dei dispositivi, le condizioni meteorologiche, etc.;
- gestione delle risorse dell'ambiente abitativo: allocare le risorse energetiche disponibili all'interno dell'ambiente domotico, in modo da gestire i task energetici in maniera efficiente, tenendo conto dei vincoli imposti dall'utente;
- interazione tra l'ambiente domotico, i fornitori di servizi e altri utenti affini: condividere esperienze, dati e conoscenza con attori esterni alla unità abitativa in ottica Smart Grid.

L'energy manager, dunque, verifica i consumi, attraverso audit ad hoc o, se disponibili, tramite i report prodotti da sistemi di telegestione, telecontrollo e automazione. Si preoccupa quindi di ottimizzare i consumi attraverso la corretta regolazione degli impianti e il loro utilizzo appropriato dal punto di vista energetico, di promuovere comportamenti da parte dei dipendenti e/o degli occupanti della struttura energeticamente consapevoli e di proporre investimenti migliorativi, possibilmente in grado di migliorare i processi produttivi o le performance

dei servizi collegati. Volendo dettagliare il ruolo dell'energy manager riferendosi alle azioni tipiche, si può considerare il seguente elenco:

- Presa di contatto con l'organizzazione e individuazione delle figure di riferimento per lo svolgimento delle proprie attività (decisori, ufficio acquisti, tecnici esperti in gestione dell'energia, manutentori, responsabili di linee di processo, funzioni amministrative e contabili, funzioni finanziarie, etc.);
- Raccolta delle bollette energetiche, valutazione dei consumi mensili e annuali, verifica; individuazione delle curve di carico giornaliere elettriche e termiche;
- Verifica dei contratti esistenti collegati ai servizi energetici (sia per assicurarsi delle prestazioni erogate, sia per pianificare in modo opportuno le proposte di investimento);
- Creazione di un database delle aree di consumo, con dettagli maggiori per quelle più significative (caratteristiche, potenze impegnate e di targa, energia/ore di funzionamento, data di installazione, etc.);
- Individuazione di un set di indicatori di prestazioni energetiche per confrontare i consumi fra le diverse sedi e con la letteratura;
- Realizzazione di diagnosi energetiche e di studi di fattibilità (in prima persona o con l'ausilio di soggetti terzi);
- Proposte di intervento e studi di fattibilità (monitoraggio, riduzione sprechi, programmi di sensibilizzazione ai dipendenti, investimenti in efficienza e rinnovabili);
- Monitoraggio della normativa e accesso agli incentivi;
- Verifica dei risultati conseguiti e programmi di comunicazione degli stessi.

2.2 Dati pertinenti al Safety & Security Manager

Nella home automation tradizionale, ogni servizio ha un proprio framework ad uso esclusivo, col risultato che i vari servizi sono indipendenti, non colloquiano e non interagiscono fra loro. Ciò porta a costose duplicazioni, a difficolta nel coordinare il funzionamento della casa, a costi d'esercizio nascosti e una minor efficacia nel garantire ciò che si richiede all'home automation: sicurezza, comfort e risparmio. L'integrazione dei servizi e la possibilità di comunicazione fra essi attraverso un unico framework che li rende interoperabili risultano di rilevante importanza. Il framework di interoperabilità garantisce un elevato livello di comfort ambientale degli spazi abitativi, assicura protezione e sicurezza contro eventi dannosi alla salute degli occupanti ed alle strutture, e consente di contenere i consumi energetici.

Oltre a ciò, il framework interoperabile evoluto di gestione degli ambienti domestici deve presentare una elevata "safety", ovvero una spiccata capacità di predire e reagire in maniera appropriata all'occorrenza di eventi

inaspettati, quali guasti oppure cambiamenti improvvisi dello scenario operativo che potrebbero comportare danni a persone o cose dell'unità abitativa. La prevenzione dei guasti, l'affidabilità e la continuità di funzionamento in caso di malfunzionamenti, ricoprono un ruolo chiave e sono funzionalità indispensabili del framework di interoperabilità, oggetto del presente progetto. In effetti, il framework di interoperabilità dovrebbe essere in grado di prevedere in anticipo, e quindi rilevare e isolare eventuali malfunzionamenti (diagnostica) nei dispositivi e negli impianti domestici, gestirli tempestivamente in modo da non pregiudicarne drasticamente le prestazioni ed impattare negativamente sulla qualità del comfort dell'ambiente abitativo. Il framework deve essere in grado di attuare delle opportune politiche di gestione guasti che garantiscano la sicurezza ed il comfort dell'ambiente abitativo anche nel caso dell'occorrenza di una o più guasti (tolleranza ai guasti).In questo modo, la casa é in grado di autogestirsi: i sottosistemi sono in grado di auto monitorarsi, o monitorarsi a vicenda, per segnalare necessità di manutenzione, quando si rilevi una riduzione dei livelli prestazionali, o di intervento qualora si evidenziassero problematiche di natura strutturale dell'unità abitativa.

La "security" è un altro aspetto di fondamentale e vitale importanza che deve essere necessariamente integrato come servizio all'interno del framework di interoperabilità. Le funzioni tradizionali del concetto di sicurezza e protezioni degli ambienti domestici sono largamente superate sia dalle opportunità tecnologiche sia dalle nuove esigenze dell'utenza domestica. In effetti, la security, come concetto e come soluzione, non può rimanere disgiunta da una gestione "confortevole" dell'edificio. Il problema degli attuali sottosistemi di sicurezza e protezione, quali ad esempio il sottosistema di sicurezza ambientale, di sicurezza antintrusione interna ed esterna, di sorveglianza, è che, essendo sono stati concepiti come sistemi autonomi, non sono in grado di comunicare fra loro e verso l'esterno. Sebbene con l'attuale tecnologia si possa disporre del migliore sistema di gestione d'edificio possibile, purtroppo questo non sarà in grado di operare in ambiente integrato e non potrà colloquiare con il mondo esterno, presentando una carenza gestionale fondamentale nel mondo odierno dove comunicazione e disponibilità d'informazione sono essenziali per rispettare i livelli attesi di sicurezza.

Con il progetto SHELL, si vuole proporre e sviluppare un "safety and security manager" da integrare come servizio nel framework di interoperabilità, oggetto del presente progetto. Il safety and security manager sarà in grado di gestire e integrare in un unico framework tutti gli aspetti di safety e security. Grazie a questo manager sarà possibile avere la supervisione degli allarmi tecnici, che costituisce un reale vantaggio per l'ottimizzazione delle procedure di manutenzione ordinaria e straordinaria, e la riduzione dei tempi di pronto intervento. In funzione del rischio, la tele-gestione degli allarmi tecnici attiverà, in modo sequenziale, le procedure relative ai livelli di intervento configurati per ogni singolo evento; queste procedure rimarranno attive nel sistema fino all'avvenuta soluzione del problema. I singoli allarmi saranno automaticamente trasmessi a diversi soggetti incaricati, secondo tabelle di priorità: Utente Finale; Centro Servizi; Società per la Sicurezza; Società per la Manutenzione, ecc.

Il safety and security manager sarà sviluppato mediante evoluti algoritmi e modelli per la gestione della manutenzione preventiva e la diagnosi guasti presenti nella letteratura scientifica, così da garantire i più elevati livelli di tutela della incolumità e sicurezza degli abitanti della casa.

2.3 Dati pertinenti al Comfort Manager

Il salto di qualità che il progetto propone per la casa domotica consente di personalizzarne le funzionalità, attraverso l'elaborazione delle informazioni di tutti i sottosistemi presenti e valutando la qualità dello stile di vita delle persone che vi abitano, sotto tanti aspetti (es. cicli veglia/sonno, qualità del cibo, igiene, abitudini quotidiane). E allora la casa può adattarsi, o suggerire configurazioni migliorative, ad esempio variando le condizioni di luminosità, temperatura e ricambio d'aria degli ambienti adibiti al riposo, in funzione delle abitudini degli utenti e in relazione alle condizioni ambientali, rilevate attraverso opportune tecniche di elaborazione di segnali acquisibili mediante reti sensoriali. Questi scenari verranno abilitati mediante lo sviluppo di modelli e servizi per la gestione, l'ottimizzazione, e il miglioramento delle condizioni di vivibilità degli spazi domestici, facenti capo ad un comfort manager, in grado anche di predisporre la casa alla eventuale integrazione di moduli e soluzioni per AAL e Active Ageing.

3. Definizione dei servizi e delle funzioni supportati dalla Black Box della casa

Possiamo immaginare che alcuni servizi (in particolare di sicurezza) debbano essere supportati dalla Black Box della casa, come accesso in sola lettura, garanzia di integrità dei dati, accesso autenticato ai dati, marcatura temporale.

3.1 Servizi di protezione dei dati: accesso in sola lettura, garanzia di integrità, marcatura temporale

In ambito IT garantire la sicurezza di un sistema informativo significa garantirne:
– **riservatezza delle informazioni** (*confidentiality*): solo chi è autorizzato deve poter accedere all'informazione;
– **integrità delle informazioni** (*integrity*): le informazioni non devono essere danneggiate o modificate per caso o con intenzioni malevole;
– **disponibilità delle informazioni** (*availability*): le informazioni devono essere sempre disponibili a chi è autorizzato ad utilizzarle.
Occuparsi di sicurezza informatica significa quindi predisporre **politiche**, **processi**, **controlli** e **contromisure informatiche** in grado di **contrastare le minacce** che rischiano di compromettere la riservatezza, l'integrità e la

disponibilità delle informazioni Nell'ambito della sicurezza informatica l'oggetto più prezioso da proteggere è l'**informazione**, il **dato**, o il **servizio di business** erogato con il supporto del sistema informatico. Le **minacce per un sistema informativo** sono di diversi tipi:

1. catastrofi naturali e **incidenti** imprevisti.

2. aggressione da parte di hacker, ossia da parte di soggetti esterni intenzionati a compromettere la sicurezza del sistema informativo: per danneggiare l'azienda sottraendo informazioni, compromettendo le informazioni o rendendole indisponibili e in questo modo impedendo la corretta erogazione di un servizio di business o la realizzazione di un prodotto.

3. software malevolo, come virus o malware, in grado di danneggiare i dati o i sistemi informatici, anche solo deteriorandone le performance.

4. attività scorrette e illecite da parte di personale interno all'organizzazione aziendale, dipendenti e collaboratori dell'azienda, talvolta effettuate inconsapevolmente.

Ai fini della protezione in questo documento viene presa in considerazione la strategia di **accesso ai dati basata sulla sola lettura**, il che significa che i dati di una pagina possono essere soltanto visualizzati. Esempi tipici sono rappresentati da elenchi, risultati delle ricerche e così via. Gli utenti possono agire sui dati ad esempio filtrando i risultati di interesse, ma queste operazioni non hanno effetti diretti sui dati della pagina stessa.

In questo tipo di scenario è possibile ottimizzare le prestazioni dell'accesso ai dati utilizzando due metodi. Un primo metodo è legato al fatto che per le pagine Web Form non è necessario creare e compilare un dataset. Se nella pagina vengono visualizzati i dati direttamente, non sarà necessario memorizzarli nella cache tramite un dataset. Per questo motivo, un secondo metodo per ottimizzare le prestazioni è legato al fatto che i componenti dati della pagina possono essere ridotti al minimo, in quanto, non essendo necessario un dataset, non è neppure necessario un adattatore dati per compilarlo. In realtà, gli unici componenti di accesso ai dati necessari sono una connessione e un comando dati contenente un'istruzione SQL o una stored procedure che possano essere eseguite per recuperare i dati.

3.2 Servizi di autenticazione: accesso autenticato ai dati, log degli accessi

1. Introduzione

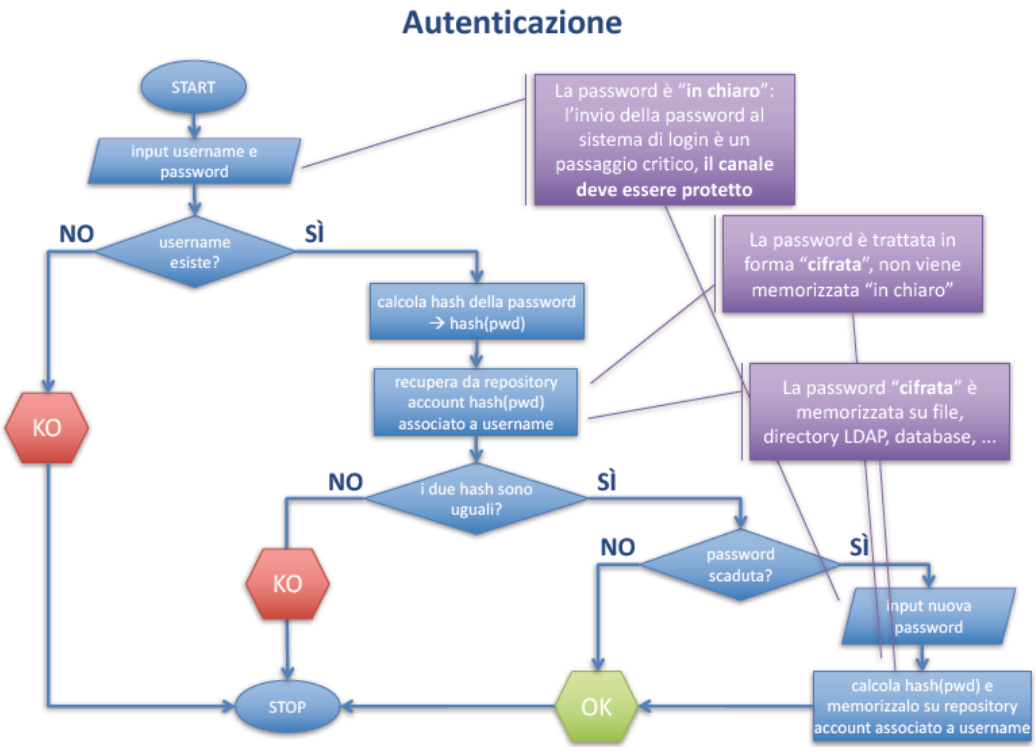
Negli ultimi anni, grazie allo sviluppo di nuove tecnologie, le comunicazioni tra uno o più utenti sono sensibilmente migliorate, aumentando però anche il rischio di intercettazioni. Di conseguenza, nelle comunicazioni tra più utenti, è diventato importante riconoscersi e farsi riconoscere dal sistema. ossia farsi **autenticare**.

I sistemi di autenticazione sono basati su tre principi: ciò che l'utente è (o come si comporta), ciò che possiede e ciò che conosce. Nella categoria di ciò che conosce vi sono le password, le passphrase e i PIN. Le password costituiscono il metodo più comune di accedere alle reti e sono, di solito, associate ad un login, che è un identificativo dell'utente.

La fase di **login** su un'applicazione o su un sistema informatico è quella in cui l'utente dichiara la propria identità (ad esempio attraverso uno *username* univoco) e l'applicazione o il sistema lo autenticano attraverso la verifica di una *password* segreta (nota solo all'utente) inserita contestualmente dall'utente.

Le passphrase, che sono più lunghe e possono essere usate in caratteri ASCII, sono spesso sorgenti di chiavi cifrate. I PIN, che sono un tipo particolare di password, vengono utilizzate per la sicurezza di carte di credito e telefoni cellulari.

Da momento dell'autenticazione in poi viene aperta una **sessione di lavoro** entro cui l'utente può operare sull'applicazione o sul sistema senza doversi autenticare nuovamente. Più sistemi possono stabilire relazioni di fiducia tra di loro per consentire ad un utente di autenticarsi su un sistema senza poi doversi autenticare nuovamente anche sugli altri (anche se gli account sono diversi): ***single sign-on.***



2. Sistema AAA

Sul sistema informativo vengono introdotte delle componenti infrastrutturali che offrono servizi di

autenticazione, autorizzazione e *accounting* degli utenti delle applicazioni

– **Autenticazione**: meccanismi per accertare l'identità dell'utente (o per "autenticare" la dichiarazione di identità fatta dall'utente).

– **Autorizzazione**: meccanismi di verifica e attuazione delle regole di autorizzazione assegnate ad un utente per l'esecuzione di una determinata funzionalità applicativa o per l'accesso ad un dato o tipo di dato.

– **Accounting**: meccanismi di responsabilizzazione dell'utente, anche attraverso il tracciamento delle operazioni svolte sui dati mediante le applicazioni o gli altri strumenti resi disponibili sul sistema informativo.

Se offerte come servizio, le funzioni devono solo essere richiamate dalle applicazioni, attraverso appositi protocolli o funzioni di libreria:

– in questo modo si **semplifica lo sviluppo del software**: non devono essere progettate e implementate le funzioni di autenticazione, autorizzazione e accounting in tutte le applicazioni

– si garantisce **maggiore sicurezza**: le funzioni sono sviluppate una volta per tutte (o sono basate su un prodotto di mercato) e integrate con le applicazioni e i sistemi; non si corre il rischio che le stesse funzioni possano essere implementate in maniera differente da un'applicazione all'altra.

– si garantisce **maggiore flessibilità**: la sostituzione di una funzione di tipo AAA con un'altra può essere fatta centralmente, senza dover modificare ogni applicazione.

3. Autenticazione e password

I sistemi di autenticazione sono caratterizzati da protocolli che trasmettono la password direttamente sulla rete o trasmettono informazioni sufficienti per consentire ad un intruso di dedurre o di indovinare la password. Quando viene stabilita una connessione ciascuno degli utenti (client e server) all'estremità della linea di comunicazione richiede all'altro di autenticarsi. I protocolli usati per l'autenticazione sono PAP (Password Authentication Protocol) e CHAP (Challenge Handshake Authentication Protocol).

L'autenticazione tramite il protocollo PAP esegue una normale procedura di login. Il client autentica se stesso spedendo la coppia <login, password> al server, che confronta questi dati con quelli contenuti nel proprio database. Questo metodo è abbastanza vulnerabile, in quanto se la password viaggia in chiaro sulla linea di comunicazione potrebbe essere facilmente intercettata da un hacker. In questo modo, l'hacher potrebbe accedere ai dati del client assumendone l'identità. Da questo punto di vista CHAP sembra più sicuro.

Con CHAP, il server invia una stringa "challenge" generata casualmente al client con il proprio hostname. Il client usa l'hostname ed il challenge, che gli è stato spedito e li cifra con una funzione hash one-way. Il risultato viene spedito al server con l'hostname del client. Il server esegue la stessa computazione e avverte il client in caso i due risultati sono uguali. Il protocolllo CHAP non richiede all'utente di autenticarsi solo al momento in cui è stabilita la connessione, ma spedisce dei challenge ad intervalli regolari. In questo modo il server è sicuro che il client con cui sta comunicando non sia un hacker. Sia per il protocollo CHAP che per il protocollo PAP esiste un database in cui sono memorizzate le password, che sono rispettivamente: /etc/ppp/chap-secret e pap-secret.

Gli schemi basati su password forniscono un buon livello di protezione e la sicurezza dell'autenticazione dipende fortemente dalla difficoltà di indovinare le password e dall'accuratezza con cui sono protette. Lo schema di autenticazione più presente (in Internet) è basato sulle password statiche. Un utente sceglie, o gli viene assegnato, un nome di account e una password (di solito si tratta di una stringa lunga da 6 a 10 caratteri) che rimane segreta e che solo l'utente dovrebbe conoscere. Messe insieme, queste due informazioni convincono l'host dell'identità dell'utente.

Esistono varie modalità di autenticazione, ma normalmente ciò che avviene nei sistemi multiutente più popolari (Linux, Unix, Windows NT), almeno dal lato dell'utente, è piuttosto standardizzato. E' importante però che sia l'utente che il sistema memorizzino la password; il primo può impararla a memoria o conservarla in un luogo sicuro, mentre il secondo la memorizza, insieme a quelle di tutti gli altri utenti, in un database protetto da ogni tipo di attacco.

Generalmente, prima di essere memorizzate, le password vengono codificate attraverso un algoritmo in una combinazione di bit apparentemente casuale, in modo da non poter essere interpretate da eventuali hacker. A volte i meccanismi di codifica si basano su sostituzioni e trasposizioni dei caratteri del testo, ma possono essere anche molto più complicati. Le password possono essere codificate solo da chi è a conoscenza dell'algoritmo e della chiave di codifica. Solitamente gli algoritmi sono di pubblico dominio, ma la chiave di codifica è, in genere, nota solo all'amministratore. Molti sistemi memorizzano la password solo dopo averla elaborata con una funzione hash non invertibile, in questo modo le password eventualmente sottratte risultano illeggibili. Inoltre, dato che la funzione è non invertibile, non è possibile in alcun modo ottenere la password originale da quella codificata. Quando l'utente immette la propria password per l'autenticazione, il sistema esegue la funzione hash non invertibile sulla password e confronta il risultato con quella codificata presente in una tabella memorizzata in un apposito database. Solo se le due password corrispondono l'utente può accedere al sistema.

4. Autorizzazione

Le applicazioni, i sistemi applicativi, i sistemi operativi sono strumenti attraverso cui l'utente (o un altro programma) può accedere alle informazioni e gestirle eseguendo delle operazioni di lettura, scrittura, modifica e cancellazione. A garanzia della sicurezza delle informazioni (riservatezza, integrità e disponibilità), i sistemi applicativi implementano meccanismi di autorizzazione degli utenti per l'accesso ai dati attraverso le funzionalità messe a disposizione dal sistema stesso. Partendo dal presupposto che l'utente non può in alcun modo operare sui dati gestiti dall'applicazione, un'autorizzazione è il permesso di compiere una determinata operazione su un certo tipo di dato (es.: inserire una fattura, visualizzare un certificato medico, approvare una richiesta di acquisto, ecc.).

I sistemi prevedono anche autorizzazioni necessarie per assegnare o revocare autorizzazioni: generalmente l'amministratore del sistema è autorizzato a priori a gestire le autorizzazioni degli altri utenti. L'applicazione

delle autorizzazioni permette di implementare un meccanismo di controllo degli accessi ai dati:
– l'utente chiede di eseguire una determinata operazione su un dato
– il sistema verifica se l'utente è autorizzato a compiere tale operazione su quel dato
– il sistema concede o impedisce l'accesso al dato: controllo degli accessi
Per poter autorizzare un utente, questo dovrà essere stato precedentemente autenticato. Per garantire una corretta politica di autorizzazione degli utenti è opportuno definire un insieme di **ruoli applicativi** che sia possibile attribuire agli utenti. Ciascun ruolo prevede un **insieme di autorizzazioni** che saranno così attribuite a tutti gli utenti a cui verrà assegnato un determinato ruolo. Si costruisce un **profilo dell'utente** del sistema informativo basato sui ruoli (e quindi sulle autorizzazioni) che si assegnano all'utente. Assegnare o rimuovere un ruolo ad un utente significa assegnare o rimuovere un insieme di autorizzazioni allo stesso utente. In un'organizzazione ben strutturata i *ruoli applicativi* dovrebbero corrispondere ai *ruoli di business* degli utenti. La **RBAC** (***role based access control)***, è una politica di controllo degli accessi alle informazioni basata sui ruoli assegnati agli utenti.

5. Accounting

Per responsabilizzare gli utenti nell'uso delle credenziali e delle autorizzazioni che sono state loro assegnate, è necessario tracciare le operazioni svolte dagli utenti tramite le funzioni rese disponibili dai sistemi applicativi. I sistemi producono delle indicazioni sintetiche sulla sequenza di operazioni svolte nel tempo: tali informazioni vengono chiamati log. I log sono memorizzati su file o su appositi sistemi di raccolta dei log; esistono protocolli (es.: syslog) e librerie software (es.: log4j) che consentono di semplificare la scrittura di log e di inviare i log prodotti da un sistema verso un sistema di raccolta.
Esistono vari tipi di log:
– log di sistema: informano sullo stato di funzionamento di un sistema e tracciano gli errori avvenuto nel corso del funzionamento del sistema stesso.
– log applicativi: informano sullo stato di funzionamento di un programma e sulle operazioni svolte sui dati.
– log di database: informano sulle operazioni svolte sui dati; sono utili anche per ripristinare lo stato del database ad un punto precedente all'esecuzione di determinate operazioni di modifica dei dati.
– log di audit: informano sulle operazioni svolte dagli utenti mediante un sistema o un'applicazione.

Pe quanto concerne la registrazione degli accessi vengono adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (**access log**) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e sono conservate per un congruo periodo, non inferiore a sei mesi.

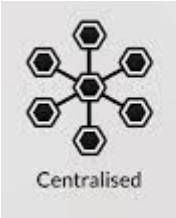
4. Possibili tecnologie per l'implementazione della Black Box della casa

La tecnologia Blockchain può rappresentare una soluzione utile alla realizzazione della Black Box della casa.

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 Blockchain è l'evoluzione **del concetto Ledger (Libro Mastro):** dal **Centralized Ledger**, **Decentralized Ledger** sino al **Distributed Ledger**.

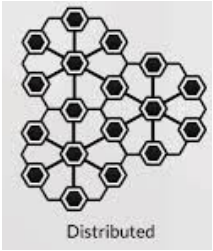
1. **Centralized Ledger:** la logica centralizzata è rappresentata dal tradizionale **Centralized Ledger** con un rapporto rigorosamente centralizzato *Uno-A-Tanti*, dove tutto deve essere gestito facendo riferimento a una **struttura** o **autorità** o sistema centralizzato.
   Nel Centralized Ledger la **fiducia** è nell'autorità, nell'autorevolezza del soggetto o sistema che rappresenta il "**Centro**" dell'organizzazione (Trusted Third Party).



2. **Decentralized Ledger: ripropone la logica della centralizzazione a livello "locale"** con "*satelliti*" organizzati a loro volta nella forma di *Uno-A-Tanti* che si relazionano a loro volta in una forma che ripete il modello *Uno-A-Tanti*. Non c'è più un "*grande*" soggetto Centrale ma ci sono tanti "*soggetti centrali"*. La fiducia anche in questo caso è delegata a un soggetto centrale, logicamente più vicino, ma comunque centralizzato.

Le organizzazioni basate su Decentralized Ledger definiscono una **Governance** che stabilisce delle forme di coordinamento di tipo centralizzato.

3. **Distributed Ledger: il vero cambiamento è rappresentato dal Distributed Ledger**, ovvero una reale e completa logica distribuita dove **non esiste più nessun centro** e dove la logica di governance è costruita attorno a un nuovo concetto di fiducia tra tutti i soggetti. Nessuno (ma proprio nessuno) ha la possibilità di prevalere e il processo decisionale passa rigorosamente attraverso un rigoroso processo di costruzione del Consenso.



La Blockchain è il libro mastro (Ledger) decentralizzato e crittograficamente sicuro, un **grande database per la gestione di transazioni crittografate** su reti decentralizzate di tipo Peer-to-Peer decentralizzato che dà il nome a una nuova piattaforma tecnologica, che consente lo scambio su internet **di informazioni e di proprietà** e permette di ridefinire e reimpostare il modo in cui creiamo, otteniamo e scambiamo valore. La Blockchain sta facendo con le transazioni quello che Internet ha fatto con le informazioni e lo sta facendo grazie a un processo che unisce sistemi distribuiti, crittografia avanzata e teoria dei giochi.

E' anche un Registro pubblico per la gestione dei dati di chi esegue e delle transazioni eseguite. Le transazioni che vengono scambiate sono costituite da dati crittografati e sono verificate, approvate e successivamente registrate su tutti i nodi (Blocchi) che partecipano alla rete. La stessa "informazione" è presente su tutti i nodi e pertanto diventa immodificabile se non attraverso una operazione che richiede la approvazione della maggioranza dei nodi della rete e che in ogni caso non modificherà la storia di quella stessa informazione.

La Blockchain non è una applicazione, non è un sistema, non è una tecnologia, ma un nuovo paradigma per la gestione delle informazioni. La Blockchain è il paradigma del digitale che permette di garantire la reale immutabilità dei dati perchè in grado di garantirne la storia. In questo senso, tale paradigma può trovare applicazione nell'ambito di interesse del progetto SHELL, proprio perché potrebbe consentire di mantenere e

gestire i dati e le informazioni relative all'ambiente di vita senza che questi possano essere alterati e, soprattutto, permette di conservarne lo storico, per poter ricostruire gli eventi che hanno determinato le evoluzioni dell'ambiente di vita stesso.

4.1 Caratteristiche e modalità di funzionamento di una blockchain

La blockchain è un protocollo di comunicazione, che identifica una tecnologia basata sulla logica del database distribuito (un database in cui i dati non sono memorizzati su un solo computer ma su più macchine collegate tra loro, chiamate nodi).

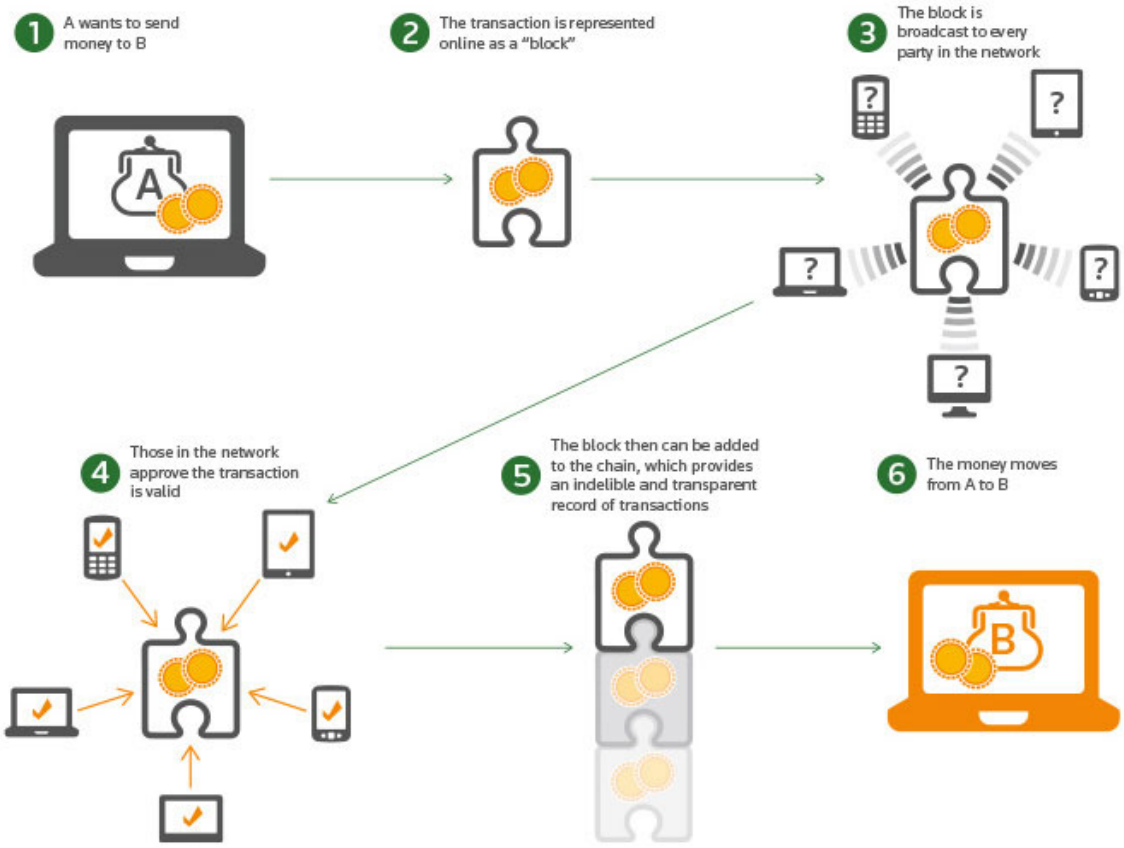
La Blockchain è una base di dati fatta di blocchi che memorizzano blocchi di transazioni valide correlate da un marcatore temporale (**timestamp**). Ogni blocco include l'**hash** (una funzione algoritmica non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita) del blocco precedente, collegando i blocchi insieme. I blocchi collegati formano una catena, con ogni blocco addizionale che rinforza quelli precedenti.

La Blockchain è anche un registro pubblico e condiviso costituito da una serie di client. La Blockchain è organizzata per aggiornarsi automaticamente su ciascuno dei client che partecipano al network. Ogni operazione effettuata deve essere confermata automaticamente da tutti i singoli nodi attraverso software di crittografia, che verificano un pacchetto di dati definiti a chiave privata o seme, che viene utilizzato per firmare le transazioni. Garantendo l'identità digitale di chi le ha autorizzate.

I passaggi che definiscono il funzionamento di una transazione basata sulla Blockchain sono:

1. Necessità di effettuare una **transazione o scambio**.
2. **Cryptographic Keys**: vengono create le informazioni relative alla transazione e vengono applicate le Cryptographic Keys specifiche per gli attori coinvolti.
3. **Verifica sulla Rete** della transazione da parte dei partecipanti alla Blockchain
4. **Creazione di un nuovo BLOCCO** con tutti i dati relativi alla transazione e con i dati relativi all'oggetto della transazione e degli attori coinvolti.
5. **Il Blocco si aggiunge alla Catena di blocchi:** Blockchain è accessibile a tutti i partecipanti ed è nell'archivio di tutti i partecipanti. Diventa il riferimento permanente, immutabile e immodificabile di quella specifica transazione.

6. **La transazione è completata ed è archiviata su tutti i nodi della Blockchain,** se le informazioni sono considerate corrette la transazione viene autorizzata, validata ed effettuata. A quel punto la transazione entra a far parte di un NUOVO BLOCCO che viene creato e che comprende anche questa transazione.



La Blockchain è una catena di blocchi, ovvero di nodi di una rete in grado di gestire in modo condiviso una lista crescente di record con la migliore e massima resistenza alle manomissioni.

Come detto, la Blockchain è un database (base dati) distribuito, ovvero condiviso tra più computer, chiamati nodi, connessi alla rete.

4.2 Database distribuito

Nel momento in cui parliamo di Distributed Ledger ci troviamo davanti un database che non si trova fisicamente solo su un server (computer), ma che invece si trova su più computer nello stesso momento, tutti perfettamente sincronizzati su tutti gli stessi documenti. Ad esempio, può trovarsi su tutti i computer che sono connessi alla rete. In questo modo l'informazione è reperibile in maniera molto rapida, in quanto la potenza di calcolo sfrutta la potenza di tutti i computer connessi.

Ci sono fondamentalmente due processi che permettono ai database distribuiti di funzionare correttamente, e di non perdere dati. Questi processi sono:

-**Replica del database**: ovvero un software è incaricato di analizzare il database per identificare cambiamenti. Una volta identificati questi cambiamenti, il software fa in modo che questi cambiamenti vengano replicati e che tutti i database siano identici.

- **Duplicazione**: è un processo che assicura che tutti i database abbiano gli stessi dati. In pratica identifica un database master, che poi duplica su tutti gli altri database, in modo da renderli uguali. Gli utenti possono modificare soltanto il database master, garantendo che i dati locali non vengano sovrascritti erroneamente.

La blockchain è in pratica una implementazione di database distribuito.

4.3 Distributed Ledger Technology – DLT

Il Ledger si può definire come il "*Libro Mastro*", e tale denominazione fa riferimento a degli **Archivi,** ovvero a una serie di dati che permettono di definire delle regole di analisi, di controllo, di verifica delle transazioni commerciali di una azienda o degli atti di una Pubblica Amministrazione.

Con la digitalizzazione il Ledger ha subito evoluzioni e accelerazioni.

In una prima fase la digitalizzazione ha reso i Ledger più veloci, più facili da usare, più performanti e ha permesso di aggiungere tante funzionalità. In questa prima, lunga fase, la digitalizzazione **non ha però cambiato la logica del Ledger.** Sono rimasti in capo a una struttura centrale che per la gestione si è avvalsa delle opportunità del digitale e soprattutto **sono rimasti chiusi e riservati**. La Governance non è cambiata, le regole di accesso e di gestione sono rimaste in capo al gestore centrale del Ledger, anche quando il rapporto con questo gestore, sfruttando le opportunità del digitale cessava di essere personale e fisico e diventata virtuale passando sulla Rete Internet.

Ma il Grande cambiamento arriva con la Blockchain. La Blockchain permette di garantire la stessa funzionalità nella gestione dei Ledger **ma senza dover fare riferimento a una struttura centralizzata**, senza cioè che sia necessario che una autorità centrale verifichi, controlli e autorizzi la legittimità di una transazione, di uno scambio, di un passaggio.

La Blockchain utilizzando la **decentralizzazione del Libro Mastro, del Ledger,** riesce ad effettuare la verifica della legittimità di una transazione anche senza la presenza si un'autorità centrale che ha la possibilità di effettuare i controlli necessari.

Se prima il Libro Mastro era univoco, uno solo e stava in capo all'autorità centrale, **adesso il Libro Mastro è di tutti,** ovvero tutti gli utenti ne hanno una copia e tutti possono controllarlo, visionarlo e, a fronte di regole che vanno a comporre la Governance della Blockchain, possono modificarlo.

Dunque, il primo, vero, grande passaggio tra la gestione dei Ledger tradizionale e la Blockchain è data dal fatto che i Libri mastro sono molteplici e che sono accessibili a tutti. Il secondo grande passaggio riguarda il fatto che **tutti possono attuare una transazione o modificarne una esistente.** In entrambi i casi questa richiesta potrà essere attuata solo se tutti (*o la maggior parte degli utenti*) accetta di attuarla. E il fatto che siano tutti, la maggior parte o un certo numero di oggetti con determinate caratteristiche ci introduce ancora una volta nell'ambito delle regole che definiscono la **governance della Blockchain.** A prescindere comunque dal fatto che l'operazione sia autorizzata da tutti o da un determinato numero di partecipanti certamente la richiesta di transazione **sarà accettata solo se i partecipanti concordano sulla sua legittimità.** Questa verifica è consentita dal fatto che tutti i partecipanti possono controllare che la richiesta provenga da una persona autorizzata a svolgerla. Con la Blockchain questi controlli vengono eseguiti in modo affidabile e automatico per conto di ciascun utente. **Ogni operazione contribuisce a creare un sistema di Ledger rapido e sicuro che per il fatto di essere distribuito presso tutti i partecipanti (tutti i partecipanti hanno una copia di ciascuna operazione) è anche in grado di resistere a eventuali manomissioni.**

In pratica, ogni nuova transazione da registrare viene unita ad altre nuove transazioni e va a formare un "**blocco**", che viene aggiunto come anello di una lunga "**catena**" di *transazioni cronologiche*. Ogni volta che si genera un blocco si allunga la catena. Questa catena va a comporre il **grande Libro Mastro Blockchain** che è posseduto da tutti gli utenti.

Affinchè un nuovo blocco di transazioni sia aggiunto alla Blockchain è necessario appunto che sia controllato, validato e crittografato. Solo con questo passaggio può poi diventare attivo ed essere aggiunto alla Blockchain. Per effettuare questo passaggio è necessario che ogni volta che viene composto un blocco venga **risolto un complesso problema matematico che richiede un cospicuo impegno anche in termini di potenza e di**

capacità elaborativa. Questa operazione viene definita come "**mining**" ed è svolta dai "**miners**".

Il lavoro del "**miners**" è assolutamente fondamentale nell'economia della gestione delle Blockchain. Chiunque può diventare un "miner" e può competere per essere il primo a risolvere il complesso problema matematico legato alla creazione di ogni nuovo blocco di transazioni in modo **valido e crittografato** che possa essere aggiunto alla Blockchain.

Trattandosi di un impegno importante, come detto con importante dispendio di energie, necessità di essere **remunerato e incentivato**. Nelle Blockchian "**private**" o **Permissioned** questo ruolo è svolto, in funzione della goveranance, dall'autorità che attiva la Blockchain stessa.

Nelle Blockchain **pubbliche** o **Permissionless** questo ruolo può essere svolto da qualsiasi partecipante alla Blockchain e il miners viene incentivato con delle forme di remunerazione che dipendono dal tipo di regole o governance definite da ciascuna Blockchain.

Nella maggior parte dei casi il primo miner che crea un blocco valido e lo aggiunge alla catena viene ricompensato con la **somma delle commissioni per le sue transazioni.** Le commissioni fanno riferimento a valori unitari per ogni singola transazione, ma i blocchi vengono aggiunti regolarmente e possono contenere migliaia di transazioni dunque il valore del miner può essere anche molto significativo. I miner possono inoltre ricevere nuove valute create e messe in circolazione come meccanismo di inflazione, come ad esempio nel caso della Blockchain Bitcoin.

L'operazione che aggiunge un nuovo blocco alla catena aggiorna il Libro Mastro detenuto da tutti i partecipanti alla Blockchain. Questi partecipanti accettano dunque un nuovo blocco nel momento in cui, grazie alla risoluzione del complesso problema matematico, è stata verificata la validità di tutte le sue transazioni.

Nel caso in cui il processo di verifica dovesse rilevare un errore, una anomalia, una discrepanza, il **blocco viene rifiutato** e tutti hanno visibilità del fatto che la transazione non è stata autorizzata. Diversamente, se tutte le transazioni sono validate, il blocco viene creato e aggiunto ed entrerà a far parte della Blockchain (della catena) a tutti gli effetti **come un record pubblico permanente e immutabile**; nessun partecipante alla Blockchain potrà cambiarlo o rimuoverlo.

L'immutabilità è l'altro grandissimo valore della Blockchain che ovviamente attiene anche alla sicurezza dei dati. Nel "vecchio" Libro Mastro per cambiare o danneggiare o distruggere un Central Ledger – Libro mastro centralizzato è necessario violare l'autorità centrale che lo gestisce, nel caso della Blockchain è invece impossibile in quanto sarebbe necessario violare tutte le copie del libro mastro possedute da tutti i partecipanti della Blockchain e occorrerebbe farlo simultaneamente. Una operazione che è praticamente impossibile, anche

se ovviamente occorre valutare la dimensione della Blockchain in termini di partecipanti ovvero di nodi. Nello stesso tempo non può nemmeno esistere un "**falso libro mastro**" in quanto tutti i partecipanti **sono in possesso di una unica versione autentica** che possono impugnare per un confronto e per la verifica. Ecco che arriviamo al concetto di **Trust e di fiducia**. La fiducia e il controllo delle transazioni passano dall'autorità centrale a tutti i partecipanti. Le transazioni basate sulla Blockchain non sono centralizzate e nascoste o "chiuse", ma sono decentralizzate e trasparenti, aperte a tutti.

In questo caso la Blockchain è di tipo **permissionless** cioè "**senza autorizzazioni**" e non esiste nessuna autorità speciale che può negare l'autorizzazione a partecipare al controllo e all'aggiunta di transazioni.

Le Blockchain che invece necessitano di **autorizzazioni** sono definite come **permissioned** e definiscono delle governance che attribuiscono a uno specifico gruppo di operatori la gestione e l'autorità nel definire gli accessi, i controlli, le autorizzazioni e soprattutto **la possibilità di aggiungere transazioni al Libro Mastro.** Le Blockchain Permissioned possono unire i valori di trasparenza, di immutabilità e di sicurezza delle Blockchain garantendo a determinati soggetti come Banche, imprese e Pubbliche Amministrazioni la possibilità di un controllo, anche rilevante e sostanziale, sulle modalità di esecuzione delle transazioni.

Grazie alla Blockchain si passa dai Ledger ai Distributed Ledger. Dai primi Digital Ledger si assiste a una accelerazione a livello di innovazione grazie alla contemporanea disponibilità di due fattori abilitanti: la **criptografia** e lo sviluppo di **algoritmi** di **controllo** e **verifica** dei dati (*complesse operazioni matematiche*) che aprono le porte a quelli che diventano i **Distributed Ledgers Technology.**

Con i Distributed Ledgers Technology si entra nell'ambito dei **Database Distribuiti,** ovvero di Ledgers (Libri Mastro) che possono essere **aggiornati**, **gestiti**, **controllati** e **coordinati** appunto non più solo a livello centrale, ma in modo distribuito, da parte di tutti gli attori.

I presupposti per i Distributed Ledgers Technology sono nella creazione di grandi network costituiti da una serie di partecipanti e ciascun **partecipante** è chiamato a gestire un **nodo** di questa rete. Ciascun nodo è autorizzato ad aggiornare i Distributed Ledgers **in modo indipendente dagli altri ma sotto il controllo consensuale degli altri nodi.**

Gli aggiornamenti o records non sono più gestiti, come accadeva tradizionalmente, sotto il controllo rigoroso di una autorità centrale, ma sono invece **creati** e caricati da ciascun nodo in modo appunto indipendente. In questo modo ogni partecipante è in grado di processare e controllare ogni transazione ma nello stesso tempo ogni singola transazione, ancorché gestita in autonomia, deve essere **verificata**, **votata** e **approvata** dalla maggioranza dei partecipanti alla rete. E' questa la base del concetto di Distributed Ledgers Technology ovvero

al concetto di **Consenso**. L'autonomia di ciascun nodo è subordinata al **raggiungimento di un consenso sulle operazioni che vengono svolte** e solo con questo consenso sono poi autorizzate e attivate.

I Distributed Ledgers vengono aggiornati solo dopo aver ottenuto il consenso e **ogni nodo viene aggiornato con l'ultima versione di ogni singola operazione di ciascun partecipante.** Ogni operazione rimane poi in modo **indelebile** e **immutabile** su ogni singolo nodo.

In altre parole, ciascun partecipante dispone di una copia – **immutabile** – di ciascuna operazione. Come si può notare si tratta di un bel cambiamento rispetto alle tradizionali logiche **centralizzate**, quando la verifica e l'autorizzazione erano centralizzate e quando lo stesso accesso a tutti gli archivi era gestito a livello centrale.

Questo modello di architettura permette di interpretare il database in senso molto più ampio rispetto al passato. Non si può *più semplicemente parlare di Ledgers come archivi*, ma parlare di **Distributed Ledgers Technology come di un nuovo rapporto tra persone e informazioni.**

4.4 Algoritmi e rete Peer-To-Peer alla base delle DLT

Le Distributed Ledger Technology che sono conosciute anche come shared ledger necessitano di una rete Peer-to-Peer e algoritmi in grado di gestire la **raccolta del consenso e la approvazione di operazioni** basate appunto sul raggiungimento di un consenso.

Sono i **modelli di gestione del Consenso** che determinano la differenza tra Distributed Ledger Technology di tipo **Pubblico** e di tipo P**rivato.**

Va comuqnue precisato che non necessariamente tutti i Distributed Ledger fanno riferimento a catene di blocchi o Blockchain allo scopo di gestire il consenso. La Blockchain è una delle diverse possibilità di gestione del consenso utilizzate per applicare Distributed Ledger Technology.

Una delle caratteristiche più importanti della blockchain è la sicurezza, garantita dalla **marca temporale** la quale impedisce che l'operazione, una volta eseguita, venga alterata o annullata.

La caratteristica principale del modello, dunque, è che **il funzionamento non è garantito da un ente centrale,** ma ogni singola transazione è validata dall'interazione di tutti i nodi.

La **marca temporale** consente di associare una data e un'ora certe e legalmente valide ad un documento informatico, consentendo di definire una validazione temporale che può essere opponibile a terzi; è costituita da sequenza specifica di caratteri che identificano in modo univoco e indelebile e immutabile una data e/o un orario per fissare e accertare l'effettivo avvenimento di un certo evento. La rappresentazione della data è

sviluppata in un formato che ne permette la comparazione con altre date e permette di stabilire e definire un ordine temporale. La pratica dell'applicazione di tale marca temporale è un processo che viene definito come **Timestamp o timestamping** ed è una delle basi di funzionamento della Blockchain.

4.5 Consenso Distribuito

Il processo di validazione della Blockchain prevede una fase di verifica e di approvazione basato su risorse di calcolo che vengono messe a disposizione dai partecipanti alla Blockchain e che sono finalizzate alla risoluzione di problemi complessi o puzzle crittografici e che permettono di disporre di un **Consenso Distribuito** e non più di un consenso basato su un **intermediario terzo** o su un ente o istituzione **centralizzata**. Coloro che partecipano alla risoluzione del problema e che dunque concorrono alla validazione del processo e della transazione sono chiamati **Miners** e il loro intervento, che necessità per essere svolto di importanti risorse, viene remunerato attraverso l'emissione di una moneta virtuale o **cryptocurrency**.

Per evitare rischi di frodi in particolare da parte di un "nodo" della Blockchain è necessario creare degli *ostacoli e delle complicazioni su tutto il processo di validazione.* Nello specifico ogni nodo che intende partecipare alla validazione deve anche risolvere un complesso problema nella forma di un **puzzle crittografico**. Il puzzle è concepito per mettere in competizione tutti i nodi e tutti contribuiscono alla risoluzione mettendo a disposizione la propria potenza di calcolo. Il nodo che riuscirà a risolvere il puzzle crittografico avrà il diritto di validare il blocco con la presentazione della **Proof of Work** che è anche la prova della soluzione del puzzle. Per questo impegno e per questo risultato il nodo viene appunto remunerato con una Unita di valore che dipende dalla tipologia di Blockchain.

Va poi aggiunto che nelle Blockchain i nodi non sono "pubblici", ovvero non si conoscono fra loro e il Proof of Work rappresenta anche il modo per costruire un rapporto di "**fiducia**" basato sulla concreta collaborazione alla soluzione delle prove che devono essere validate.

4.6 Funzionamento della Blockchain

Il modello si basa sulla **combinazione tra firma digitale** e **marca temporale (timestamp)**: la prima garantisce che mittente e destinatario di un qualsiasi tipo di messaggio (ad esempio la transazione nel mondo dei pagamenti) siano identificati in modo certo, il secondo permette che un insieme di messaggi, validato con la **marca temporale** da parte di un nodo scelto casualmente da un robusto modello matematico, venga comunicato e scritto nel registro di tutti gli altri nodi della rete e reso irreversibile.

Tutte le operazioni sono confermate dalla rete entro poco tempo, attraverso il **processo di consenso distribuito detto "mining"**. In pratica la correttezza del blocco di operazioni immesse nella rete viene verificata dai

computer dei partecipanti al network confrontandolo con la versione più aggiornata della Blockchain. Il primo nodo che ottiene semaforo verde lo comunica a tutti gli altri, che provvedono a convalidare il blocco aggiornando la Blockchain. In questo modo **si preservano al tempo stesso l'ordine cronologico delle operazioni e la neutralità della rete.**

4.7 Caratteristiche della Blockchain

- **Affidabilità**: la blockchain è affidabile. Non essendo governata dal centro, ma dando a tutti i partecipanti diretti una parte di controllo dell'intera catena, la blockchain diventa un sistema meno centralizzato, meno governabile, ed allo stesso tempo molto più sicuro e affidabile, ad esempio da attacchi di malintenzionati. Se infatti soltanto uno dei nodi della catena subisce un attacco e si danneggia, tutti gli altri nodi del database distribuito continueranno comunque ad essere attivi ed operativi, saldando la catena e non perdendo in questo modo informazioni importanti.
- **Trasparenza**: le transazioni effettuate attraverso la blockchain sono visibili a tutti i partecipanti, garantendo così trasparenza nelle operazioni.
- **Convenienza**: effettuare transazioni attraverso la blockchain è conveniente per tutti i partecipanti, in quanto vengono meno interlocutori di terze parti, necessari in tutte le transazioni convenzionali che avvengono tra due o più parti.
- **Solidità**: le informazioni già inserite nella blockchain non possono essere modificate in alcun modo. In questo modo le informazioni contenute nella blockchain sono tutte più solide ed attendibili, proprio per il fatto che non si possono alterare e quindi restano così come sono state inserite la prima volta.
- **Irrevocabilità**: con la blockchain è possibile effettuare transazioni irrevocabili, e allo stesso tempo più facilmente tracciabili. In questo modo si garantisce che le transazioni siano definitive, senza alcuna possibilità di essere modificate o annullate.

Per comprendere al meglio gli ambiti di utilizzo della Distributed Ledger Technology occorre conoscere anche le:

1. **Unpermissioned ledgers** (Blockchain Pubbliche) di cui l'esempio più famoso e diffuso è rappresentato dalla Blockchain Bitcoin, sono aperte, non hanno una "proprietà" o un attore di riferimento e sono concepite per non essere controllate.

   L'obiettivo delle Unpermissioned ledgers è quello di permettere a ciascuno di contribuire all'aggiornamento dei dati sul Ledger e di disporre, in qualità di partecipante, di tutte le copie immutabili di tutte le operazioni. Ovvero di disporre di tutte le copie identiche di tutto quanto viene approvato grazie al consenso.

Questo modello di Blockchain impedisce ogni forma di censura, nessuno è nella condizione di impedire che una transazione possa avvenire e che possa essere aggiunta al Ledger una volta che ha conquistato il consenso necessario tra tutti i nodi (partecipanti) alla Blockchain.

Le Unpermissioned Ledgers possono essere utilizzate come database globale per tutti quei documenti che hanno la necessità di essere assolutamente immutabili nel tempo a meno di aggiornamenti che richiedono la massima sicurezza in termini di consenso, come ad esempio i contratti di proprietà o i testamenti.

2. **Permissioned ledgers** (Blockchain Private) possono invece essere controllati e dunque possono avere una "proprietà". Quando un nuovo dato o record viene aggiunto il sistema di approvazione non è vincolato alla maggioranza dei partecipanti alla Blockchain bensì a un numero limitato di attori che sono definibili come Trusted. Questo tipo di Blockchain possono essere utilizzate da istituzioni, grandi imprese che devono gestire filiere con una serie di attori, imprese che devono gestire fornitori e subfornitori, banche, società di servizi, operatori nell'ambito del retail. In questo caso le Permissioned ledgers rispondono alle necessità di un aggiornamento diffuso su più attori che possono operare in modo indipendente, ma con un controllo limitato a coloro che sono autorizzati. Le Permissioned ledgers permettono poi di definire speciali regole per l'accesso e la visibilità di tutti i dati. In altre parole le Permissioned ledgers introducono nella Blockchain un concetto di Governance e di definizione di regole di comportamento.

   Tecnicamente le Permissioned ledgers sono anche più performanti e veloci delle Unpermissioned Ledgers

Con il termine Blockchain s'intende il paradigma tecnologico che permette di sviluppare applicazioni *Cryptocurrency-like*: il protocollo Bitcoin rappresenta solo una – la prima – delle possibili realizzazioni.

La Blockchain non è soltanto Bitcoin. La moneta virtuale è infatti solo una una delle sue possibili applicazioni. Priva di gestione centralizzata, infatti, la Blockchain permette di inviare qualsiasi dato in maniera sicura, tagliando drasticamente la catena degli intermediari, e permettendo quindi uno scambio di dati sicuro tra due persone e basta, senza dover utilizzare mezzi di terze parti quali ad esempio un provider di posta elettronica, oppure un servizio di cloud computing esterno.

Altri possibili nu**ovi ambiti applicativi della Blockchain sono**:

1) Blockchain in finanza e banche
2) Blockchain nelle Assicurazioni
3) Blockchain nei Pagamenti digitali

4) Blockchain nell'Agrifood
5) Blockchain nell'Industry 4.0
6) Blockchain nella Sanità
7) Blockchain nella Pubblica amministrazione
8) Blockchain nel Retail
9) Blockchain nell'IoT Anche nell'internet delle cose la Blockchain trova una grande utilità: grazie alla sua facilità di scambio dati, infatti, la tecnologia Blockchain potrebbe essere utilizzata per facilitare la comunicazione tra oggetti IoT connessi, oltre a rendere lo scambio di dati più sicuro e veloce.

5. Analisi di applicabilità della tecnologia blockchain al concetto di Black Box della casa

Guardando alle caratteristiche precedentemente dichiarate e proprie del paradigma Blockchain, è possibile operare un'analisi di applicabilità del paradigma stesso al caso di interesse, ovvero come possibile soluzione tecnologica per l'implementazione di quella che è stata chiamata Black Box della casa.

"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."

Pensando di applicare questa caratteristica al caso di interesse, si può pensare che i nodi della rete siano tutti quei soggetti e quelle entità interessati a lavorare su dati di pertinenza dell'ambiente domestico, relativi ai consumi energetici, al comfort e alla sicurezza. In particolare, i dati di interesse sono quelli che segnalano eventuali anomalie rispetto ad una condizione operativa "normale". E' importante che le segnalazioni relative alle eventuali anomalie possano essere accessibili a tutti gli attori interessati che contribuiscono al database distribuito, che siano strutturate e validate da tutti gli interessati.

"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**."

La tracciabilità e l'immutabilità di tutte le informazioni affidate alla Blockchain sono due caratteristiche

essenziali per il caso d'uso di interesse, proprio perché ci si sta riferendo a dati che riguardano la segnalazione di anomalie intervenute nell'ambiente domestico. Ai fini della possibilità di usare tali dati per verificare quanto accaduto, è fondamentale che essi risultino tracciabili (in modo da poter risalire al sottosistema che ha inserito una nuova segnalazione nel database, e quindi all'evento che ha scatenato tale segnalazione) e immutabili, ovvero deve essere impossibile poter alterare ad arte e a posteriori le informazioni registrate sulla Blockchain, che potrebbero anche avere valenza legale, in relazione a specifiche situazioni che si potrebbero creare.

"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."**

L'utilizzo di meccanismi crittografici può risultare fondamentale sia ai fini di garantire le proprietà precedentemente enunciate, sia allo scopo di rendere confidenziali le informazioni registrate sulla Blockchain, essendo riferite ad ambienti di vita e dunque pertinenti ai soggetti che tali ambienti occupano.

6. Riferimenti

https://www.codecademy.com/learn/introduction-to-blockchain

https://bitsonblocks.net/2015/09/09/gentle-introduction-blockchain-technology/

https://blockgeeks.com/guides/what-is-blockchain-technology/