
1506
UNIVERSITÀ
DEGLI STUDI
DI URBINO
CARLO BO

# Ipotesi di utilizzo delle blockchain per la gestione dei dati di sistemi IoT

DOCENTE
**Prof. Ing. LUCA ROMANELLI**

CORSISTA
**TOMMASO PETRELLI**

Corso di Sistemi per l'Internet Of Things
Anno Accademico 2022-2023

# Indice

# Introduzione

L'*Internet of Things* (*IoT*) ha esteso la connettività di Internet non solo per raggiungere computer e utenti, ma anche la maggior parte degli oggetti nell'ambiente circostante. L'*IoT* ha il potenziale di connettere miliardi di oggetti simultaneamente e di agevolare la condivisione delle informazioni, riflettendosi, dunque, in un miglioramento della nostra vita. Le aspettative che si hanno per il mondo dell'*IoT* sono alte e prevedono che altre centinaia di miliardi di dispositivi condurranno ad una trasformazione dell'industria elettronica e non solo. Nonostante i vantaggi apportati, nel momento in cui si entra nel mondo reale le sfide da affrontare rimangono numerose. Si è individuata nella centralizzazione dell'architettura la sua debolezza principale. Questo elaborato offre una panoramica sull'integrazione delle *blockchain* nei sistemi *IoT*. La tecnologia *blockchain*, infatti, è capace per sua natura di decentralizzare le operazioni computazionali e la gestione dei processi, risolvendo molti problemi dell'*IoT*, e soprattutto offre la possibilità di costruire sistemi scalabili, sicuri e *trustless*, mantenendo al tempo stesso i dati privati.

# 1 | Aspetti Tecnici Generali

## 1.1 Sistemi IoT

Il termine "*IoT*" (*Internet of Things*) può essere probabilmente attribuito a Kevin Ashton, che nel 1999 presso il MIT diede inizio ad un ecosistema di tag RFID. ARM Ltd stima 1 trilione di dispositivi connessi entro il 2035 [B1]. Nel 2022, secondo Statista abbiamo raggiunto circa 13,14 miliardi di dispositivi connessi [S1].

Quando si parla di sistemi *IoT* si fa riferimento ad ecosistemi, applicazioni o architetture composte da dispositivi i cui requisiti minimi sono:

- sufficiente potenza computazionale da supportare uno *stack* di protocolli di rete
- hardware abbastanza prestazionale per poter utilizzare un protocollo di rete complesso come quello 802.3
- non deve essere una periferica dotata storicamente di connessione ad internet, come ad esempio: PC, laptop, smartphone, tablet o server [B1]

Questi dispositivi utilizzano sensori a basso consumo capaci di performare attività diverse. La tipica architettura di un sistema *IoT* prevede quattro livelli quali: (i) livello di campo, in cui possiamo trovare dispositivi *IoT* a basso consumo, sensori, attuatori e sistemi fisici; (ii) livello di rete locale, che prevede come componenti fondamentali i sistemi di comunicazione con sensori basati su reti WPAN e reti LAN, ma copre anche l'aspetto dell'*edge computing* che abilita ad una elaborazione distribuita dei dati; (iii) nel livello di rete geografica, basata su reti WAN e su protocolli di trasporto quali MQTT, zigbee, e CoAP, l'infrastruttura si compone di aggretatori, router e gateway; (iv) livello *cloud* che fornisce vari tipi di servizi di *cloud computing* per l'elaborazione dei dati *IoT* come *IaaS* (*Infrastructure as a Service*) [S2], *SaaS* (*Software as a Service*) [S3] e *PaaS* (*Platform as a Service*) [S4], ma offre anche strategie di sicurezza e di memorizzazione [B1].

### 1.1.1 Architettura centralizzata dell'IoT

Gran parte dei sistemi *IoT* costruiti finora, poggiano su architetture centralizzate dette *server/client*, necessitando, dunque, che tutti i dispositivi *IoT* che compongono un sistema debbano essere connessi e autenticati da un'unica autorità [B2]. Le conseguenze che derivano dall'avere un server centrale che gestisce tutti i dispositivi, riguardano soprattutto problemi di scalabilità e sicurezza, sebbene sia importante conoscere che intrinsecamente questo porta anche ad avere un *single-point-of-failure*. È chiaro che un modello di questo tipo non sarà in grado di soddisfare le richieste provenienti da un sistema *IoT* in continua crescita.

L'idea dell'*IoT* è quella di far comunicare una vasta gamma di dispositivi via Internet. I dispositivi *IoT* agiscono come nodi di rete che comunicano assieme per condividere dati. I dati vengono raccolti dai sensori presenti nei dispositivi per poi essere essere processati, archiviati o trasmessi. L'architettura sopra la quale si svolge tale processo è centralizzata e come precedentemente citato, composta tipicamente da almeno quattro livelli: (i) livello di campo, (ii) livello di rete locale, (iii) livello di rete geografica e (iv) livello *cloud* (o applicazione). Se il modello è centralizzato, i dispositivi non riescono a trasmettere informazioni direttamente tra di loro, infatti, questi devono passare attraverso un *gateway* centralizzato.

Il modello centralizzato *server/client* è stato spesso utilizzato finora nel campo dell'*IoT* per sostenere reti di dispositivi con una certa capacità computazionale. In futuro, tuttavia, come già oggi, è difficile pensare a come la stessa architettura possa soddisfare i bisogni di un sistema con centinaia di miliardi di dispositivi connessi, ognuno che vuole raccogliere, elaborare e scambiare dati. Si pensi ad esempio a quanto possano aumentare solo i costi di gestione delle comunicazioni sia in termini economici che computazionali. Sarà fondamentale inoltre il contributo dato dalla presenza del *single-point-of-failure*, il quale renderà particolarmente semplice "rompere" la rete interrompendo le comunicazioni tra i dispositivi. Un ultimo aspetto da tenere in considerazione riguarda la sicurezza, la quale sarà messa a rischio soprattutto in quei casi di raccolta dei dati *real-time* [B2]. Un'architettura centralizzata, infatti, non garantisce che i dati che viaggiano tra i dispositivi non siano vulnerabili ad attacchi e manipolazioni.

### 1.1.2 MQTT - Un approccio pub/sub

Dal punto di vista dei protocolli si può già parlare di nuovi *stack* tecnologici che riescono a limitare i problemi dovuti alla poca disponibilità di risorse computazionali, alla banda limitata per la trasmissione dei dati, alla scalabilità e sicurezza. In particolare, vale la

pena citare il protocollo MQTT tra quelli che hanno reso la comunicazione tra dispositivi *IoT* più efficiente.

Nel 1999, presso IBM, Andy Standfor-Clark e Arlen Nipper lavorarono ad un protocollo che avrebbe risolto i problemi di collegamento remoto di impianti di oleodotti e gasdotti utilizzando una connessione satellitare. Oggi si fa riferimento a quel protocollo con il termine MQTT (*Message Queue Telemetry Transport*) [B1]. L'ente ufficiale MQTT.org [S5] lo definisce come un protocollo di messaggistica standard (ISO/IEC PRF 20922) basato sull'approccio *publish/subscribe*. MQTT è progettato per essere leggero, trasparente, semplice e facile da implementare. Queste caratteristiche lo rendono l'ideale in ambienti limitati, come nella comunicazione in contesti *Machine-to-Machine* (M2M) e *Internet of Things* in cui tipicamente si ha una bassa larghezza di banda, alta latenza e reti inaffidabili.

MQTT è ottimo per i dispositivi *IoT* che solitamente devono trasmettere e ricevere dati su una rete con risorse limitate e larghezza di banda limitata. Il protocollo MQTT è diventato uno standard per la trasmissione dei dati *IoT* perché offre i seguenti vantaggi:

- Leggerezza ed efficienza - l'implementazione di MQTT sul dispositivo *IoT* richiede risorse minime. Anche le intestazioni dei messaggi MQTT sono ridotti in modo da poter ottimizzare la larghezza di banda della rete.
- Scalabilità - il protocollo dispone anche di funzioni integrate per supportare la comunicazione con un gran numero di dispositivi *IoT*.
- Affidabilità - definisce diversi livelli di qualità del servizio per garantire l'affidabilità dei casi d'uso *IoT*.
- Sicurezza - semplifica la crittografia dei messaggi e l'autenticazione di dispositivi e utenti utilizzando i moderni protocolli di autenticazione, come OAuth, TLS1.3. Per proteggere i dati sensibili trasmessi dai dispositivi *IoT*, MQTT utilizza il protocollo SSL. È inoltre possibile implementare l'identità, l'autenticazione, l'autorizzazione e protocolli di crittografia [S6].

### 1.1.3 Cloud e Fog computing

Un ecosistema *IoT* richiede un enorme quantità di risorse computazionali e tende a richiederne sempre di più. Il *Cloud* lo possiamo vedere come un insieme di infrastrutture di servizi circa la computazione, le comunicazioni e anche di *storage*. I *cloud provider* supportano tipicamente una serie di prodotti detti *Everything-as-a-Service* (*XaaS*) [B1]. I *Cloud* sono tipicamente degli enormi *data center* posti ai confini delle dorsali Internet

che forniscono servizi verso l'esterno secondo un modello *pay-for-use* [B1]. Una definizione classica di *cloud computing* è data da [B3] secondo qui è un modello che permette di avere un accesso rete a differenti risorse computazionali configurabili in modo pervasivo, conveniente e su richiesta. Queste risorse possono essere assegnate con un minimo sforzo dal punto di vista gestionale e dal punto di vista di interazione con un *service provider*. Le caratteristiche essenziali del *cloud computing* sono: (i) autonomia nella richiesta di utilizzo di risorse computazionali; (ii) le risorse sono accessibili dalla rete per mezzo di protocolli *standard*; (iii) l'insieme delle risorse viene opportunamente assegnato a chi lo richiede ed è modellato con un livello di astrazione per cui il *Cloud* si disloca da una posizione fisica; (iv) l'architettura *Cloud* è pensata per essere scalabile e seguire le necessità di ecosistemi eterogenei; (v) i sistemi *Cloud* ottimizzano e controllano le loro risorse in modo automatico, inoltre, queste ultime possono essere monitorate e regolate nel loro utilizzo.

Anche se l'idea del *cloud computing* è molto robusta ed efficiente, secondo [B4], le necessità e le dimensioni degli ecosistemi *IoT* la rendono impraticabile in diversi scenari. Si propone come soluzione alternativa o complementare il *fog computing*. Il *fog computing* estende il *cloud computing* proponendo un modello orizzontale in cui i dati possono essere analizzati e processati da applicazioni in esecuzione su dispositivi all'interno della rete piuttosto che in un *data center Cloud* centralizzato, rendendo anche risorse e servizi distribuiti. In questo modello *fog*, i nodi della rete che renderanno disponibili servizi e risorse possono essere posizionati ovunque tra il *Cloud* e i dispositivi *IoT*. È proprio questa decentralizzazione dei nodi computazionali che fa ben sperare sulle possibilità di tenere testa alle richieste dei sempre più avanzati sistemi *IoT*.

È bene tenere presente che, quando possibile, il *Cloud* rimane comunque la prima soluzione architetturale di sistemi *IoT*. Il *fog computing* è una potente estensione delle funzionalità del *cloud computing* e risulta essere necessario in alcuni scenari in cui un modello *Cloud* tradizionale non è sufficiente. Nell'articolo [B4] vengono analizzati diversi scenari nel contesto delle infrastrutture *IoT* ed il risultato più evidente sottolinea il fatto che per fronteggiare alcune problematiche è necessario ricorrere all'utilizzo del *fog computing*. Si immagini uno scenario in cui i dispositivi *IoT* che raccolgono e trasmettono dati siano fissi in un punto, allora il *Cloud* sarebbe perfettamente in grado di fornire le risorse computazionali necessarie. Nel momento in cui i dispositivi *IoT* si spostano nel tempo nasce il bisogno di avere una infrastruttura *Fog* che rimanga sempre vicina ad essi. Quindi, avere il supporto di una architettura *Fog* permette di: (i) aggregare e filtrare i dati verso il *Cloud*; (ii) scalare l'infrastruttura a livello geografico; (iii) migliorare le capacità di prendere decisioni *real-time* su diversi sistemi *IoT*. In conclusione, si può dire che per affrontare al meglio parte dei problemi dovuti alla costante crescita degli ecosistemi *IoT*,

l'ideale sarebbe avere un sistema che combina i punti di forza del *cloud computing* a quelli del *fog computing*.

## 1.2 Database distribuiti

Quando si parla di *database* distribuito (o *Distributed Ledger*) si intende un *database* in cui i dati non sono memorizzati in un unico *server* centrale, bensì sono distribuiti in differenti postazioni fisiche. I dati potrebbero risiedere su diversi *server* posti nella stessa località (in questo caso si parla di *data center*), oppure potrebbero trovarsi all'interno di una rete di *server* interconnessi tra loro. Tutti i *server* coinvolti nella gestione degli stessi dati, logicamente correlati tra loro, sono perfettamente sincronizzati su tutti gli stessi documenti [S7][S8].

Il vantaggio principale apportato da questo approccio riguarda l'aumento delle performance. L'informazione, infatti, è reperibile in maniera molto rapida, in quanto la potenza di calcolo sfrutta la potenza di tutti i computer connessi.

Le operazioni essenziali che permettono di mantenere consistenti ed affidabili i dati sono la replicazione e la duplicazione, spiegate qui di seguito:

- Replicazione: un software è incaricato di identificare eventuali cambiamenti nel *database* distribuito; qualora questi si verifichino, il software farà in modo che tutti i cambiamenti vengano replicati cosicché tutti i *database* siano identici.
- Duplicazione: un processo che assicura che tutti i *database* nelle diverse locazioni abbiano gli stessi dati. In primo luogo si identifica un *database* come *master*, successivamente lo si duplica su tutti gli altri *database*. Gli utenti possono modificare soltanto il *database master*, garantendo che i dati locali non vengano sovrascritti erroneamente [S8].

## 1.3 DLT: Distributed Ledger Technology

Con il termine *Distributed Ledger Technologies* (*DLT*) si fa riferimento in senso generale a "libri mastri" (o registri, *ledger*) digitali distribuiti geograficamente, che possono essere usati per conservare informazioni e scambiare valore in modo decentralizzato [B5].

A differenza dei *database* centralizzati, la tecnologia *DLT* per sua natura non richiede un amministratore centrale, e quindi non è soggetta ad un singolo *point-of-failure*; questo indubbiamente è uno dei motivi per cui la decentralizzazione è una qualità sempre più ricercata nei sistemi complessi.

I dati presenti sui registri sono sono protetti da potenziali attacchi informatici poiché le stesse informazioni sono ridondate, verificate e validate mediante l'adozione di diversi protocolli (o regole) comunemente accettati da ciascun partecipante. L'archiviazione delle informazioni, precedentemente criptate, è basata su algoritmi di consenso che coinvolgono tutti o parte dei partecipanti. In questo modo tutti i nodi della rete devono concordare sull'insieme di transizioni valide [S9].

## 1.4 Blockchain

Le *blockchain* sono un particolare tipo di *DLT*.

Una *blockchain* la possiamo considerare come un registro pubblico, digitale, distribuito e strutturato come una catena di archivi, o blocchi, che cresce continuamente nel tempo [B1][B6]. Da questo punto di vista una *blockchain* funziona come una base di dati distribuita, condivisa e immutabile.

Ogni archivio contiene un *hash* crittografato che identifica il blocco precedente, un *timestamp* e dati della transazione. Il *timestamp* identifica in modo univoco, indelebile e immutabile una data e/o un orario per fissare e accertare l'effettivo avvenimento di un certo evento, garantendo così che i dati di una transazione siano validi. L'*hash* crittografato, fornisce la possibilità di ad un blocco di contenere le informazioni circa il blocco precedente, in questo modo si forma una struttura dati concatenata. Così facendo, le transazioni delle *blockchain* sono irreversibili una volta registrate nella catena. Infatti, un dato presente in un certo blocco non potrà più essere alterato retroattivamente se non alterando tutti i blocchi successivi ad esso [S8][S10].

La natura distribuita delle *blockchain* implica che nessuna singola entità deve controllare un registro, infatti l'autenticità degli archivi viene convalidata da diversi partecipanti pari tra loro [B6]. La validazione delle transazioni è affidata a un meccanismo di consenso distribuito che varia a seconda che la *blockchain* sia *permissionless* o *permissioned*. Nel primo caso, le *blockchain* sono pubbliche e tutti i nodi della rete partecipano al processo di consenso, mentre nel secondo partecipano solo i nodi autorizzati poiché le *blockchain* sono private [S8]. Affinché si possa aggiungere un nuovo blocco di transazioni alla *blockchain* è necessario che questo sia controllato, validato e crittografato. Questa operazione viene definita come *mining* ed è svolta dai minatori (o *miner*). Risulta essere molto complicata e richiede un cospicuo impegno anche in termini di potenza e di capacità di elaborazione [S8]. Nelle *blockchain* pubbliche, il ruolo di *miner* viene svolto da qualsiasi partecipante alla *blockchain* e questo viene incentivato con delle forme di remunerazione che dipendono dal tipo di regole o governance definite da ciascuna *blockchain*.

La logica che sta alla base del processo di consenso distribuito per la registrazione di un nuovo blocco, parte dal presupposto che per evitare rischi di frodi, in particolare da parte di un minatore della *blockchain*, è necessario creare degli ostacoli. Ogni nuovo blocco include un insieme di nuove transazioni, l'*hash* del blocco precedente, l'identificativo del minatore che lo propone alla *blockchain* e soprattutto la risposta ad un puzzle. Ogni minatore che intende partecipare alla validazione deve risolvere questo complesso puzzle crittografico. Il puzzle è concepito per mettere in competizione tutti i minatori e tutti contribuiscono alla risoluzione mettendo a disposizione la propria potenza di calcolo. Il minatore che riuscirà a risolvere il puzzle crittografico avrà il diritto di validare il blocco con la presentazione della *Proof-of-Work* ($PoW$) che è anche la prova della soluzione del puzzle. È dopo aver risolto il puzzle che il minatore verrà remunerato [B6][S8]. Il concetto di $PoW$ rappresenta anche il modo per costruire un rapporto di fiducia basato sulla concreta collaborazione alla soluzione delle prove che devono essere validate. Essendo che la risoluzione del puzzle dipende fortemente dalla potenza di calcolo di un nodo della rete, per i minatori, le probabilità di vincere la $PoW$ sono direttamente proporzionali alla capacità di calcolo di cui si dispone [S8].

## 1.5 DLT e blockchain a confronto

Il primo passo da fare è quello di sottolineare il fatto che una DLT non è un *database* distribuito, infatti, si è già detto come quest'ultimo rappresenti un sistema di immagazzinamento decentralizzato su più macchine server. D'altra parte, una DLT consiste in un insieme di sistemi che fanno riferimento ad un registro distribuito, governato in modo da consentire l'accesso e la possibilità di effettuare modifiche da parte di più nodi di una rete [S8]; inoltre, in una DLT non è possibile inserire direttamente ogni tipo di informazione ma è necessario che tutti i nodi concordino sulla validità della stessa, partecipando al processo di verifica [B5].

La caratteristica che accomuna le DLT alle *blockchain* è proprio il fatto di aggiungere informazioni al registro sulla base di un algoritmo di consenso distribuito su tutti i nodi della rete. Partendo da questo vista, possiamo dire che una *blockchain* si può interpretare come una implementazione di DLT caratterizzata da un registro pensato in modo da gestire le transazioni all'interno di una struttura dati, per l'appunto, una catena di blocchi. Un altro punto di intersezione tra le DLT e le *blockchain* riguarda l'utilizzo della crittografica come cardine attorno al quale sono implementati gli algoritmi di consenso [B5].

Vi sono tre ragioni fondamentali che hanno reso la tecnologia *distributed ledger* impor-

tante: (i) la decentralizzazione dei dati, infatti, i dati sono distribuiti su molteplici nodi che compongono una rete *peer-to-peer* (*P2P*) dove (ii) ognuno di essi replica e salva una copia identica del registro e lo mantiene aggiornato indipendentemente dagli altri nodi, senza bisogno di una autorità centrale; (iii) ogni nodo processa nuove transazioni in maniera indipendente dopodiché tutti i nodi assieme utilizzano un algoritmo di consenso per decidere qual è il modo corretto di aggiornare il registro. Secondo [B2], le *blockchain* si distinguono, in particolar modo nel mondo dell'*IoT*, per le seguenti caratteristiche:

1. Immutabilità - una volta che una transazione è stata confermata, diventa quasi impossibile modificarla.
2. Decentralizzazione - la mancanza di un controllo centralizzato garantisce maggiore scalabilità e robustezza dato che si possono utilizzare risorse messe a disposizione da tutti i nodi.
3. Anonimato - si ha la capacità di mantenere privata l'identità degli utenti.
4. Sicurezza - oltre alla forte presenza della crittografia negli algoritmi utilizzati, si elimina il "*single-point-of-failure*".
5. Capacità del sistema - con il vorticoso aumento dei dati e dei dispositivi *IoT* in circolazione, diventa fondamentale avere la capacità di far cooperare assieme i nodi e ricavarne maggiori doti computazionali.

## 1.6 Blockchain nell'IoT

L'*IoT* ha la capacità di connettere e far comunicare tra di loro miliardi di oggetti assieme. Questo settore è uno tra gli ultimi ad essere sviluppato con forti investimenti alle spalle, in quanto porta con sé continue rivoluzioni dal punto di vista della computazione e delle comunicazioni. Oggi internet permette a miliardi di oggetti personali ed industriali, supportati computazionalmente da servizi in *Cloud*, di essere simultaneamente connessi. Gli oggetti forniscono informazioni raccolte dai sensori, agiscono sul loro ambiente e se progettati opportunamente possono arrivare a modellare un sistema complesso come una fabbrica o una città [B7]. Il termine "*things*" in *IoT* indica principalmente dispositivi integrati caratterizzati da risorse limitate quali la larghezza di banda, latenza e memoria. Attraverso l'utilizzo di questi dispositivi economici ed interconnessi tra loro è possibile raccogliere informazioni dall'ambiente circostante aiutando a migliorare lo stile vita dell'uomo [B2].

L'*IoT* è decisamente un settore in forte sviluppo che fornisce molti benefici, ma allo stesso

tempo pone davanti a sé alcune sfide dovute soprattutto all'architettura centralizzata su cui si basa, infatti, tutti i dispositivi vengono identificati, autenticati e connessi attraverso dei *server* centralizzati. Finora, il modello centralizzato è riuscito a supportare le connessioni di un ampio numero di dispositivi permettendogli di eseguire calcoli e trasferire dati contemporaneamente. Questo tuttavia non sarà più sufficiente nel momento in cui le reti *IoT* continueranno a crescere. Integrando i mondi dell'*IoT* e delle *blockchain*, sarà possibile ottenere numerosi vantaggi. In *primis*, la decentralizzazione dell'architettura sarà possibile basando il modello *IoT* su quello delle *blockchain*; questo permetterà di gestire miliardi di transizioni scambiate tra i dispositivi *IoT* e ridurrà notevolmente i costi associati all'installazione e alla manutenzione degli enormi *data center* poiché le operazioni di calcolo verranno distribuite e memorizzate sui miliardi di dispositivi connessi. Inoltre, seguire il modello delle *blockchain* eliminerà il *single-point-of-failure* che caratterizza un architettura *IoT* centralizzata. Infine, combinare l'*IoT* alla tecnologia *blockchain* permetterà ai dispositivi di scambiare i messaggi in modo *peer-to-peer*, distribuire file sulla rete e coordinarsi in modo autonomo senza alcun bisogno di un modello centralizzato *server/client* [B2].

Le capacità di decentralizzazione, autonomia ed affidabilità della tecnologia *blockchain* la rendono un elemento fondamentale nella risoluzioni di molte problematiche che stanno nascendo nel mondo *IoT*. Tuttavia, ad esempio, stabilire come modello di comunicazione quello *peer-to-peer* comporta altre sfide che riguarderanno specialmente la sicurezza, la quale è proprio uno degli aspetti più delicati nell'*IoT*. Le soluzioni che considerano l'uso delle *blockchain*, infatti, dovranno assicurare la riservatezza e la sicurezza nelle reti *IoT* ed utilizzare la validazione e il consenso condiviso dei partecipanti sulle transazioni per prevenire lo *spoofing* e il furto dei dati. Le *blockchain* possono anche essere utilizzate per tracciare miliardi di dispositivi connessi, permettendo a questi ultimi di elaborare transizioni e coordinarsi in modo autonomo. Inoltre, gli algoritmi crittografici utilizzati dalle *blockchain* renderanno i dati molto più riservati [B2].

In una rete *IoT*, una *blockchain* è in grado di rendere immutabile lo storico dei dispositivi *IoT* connessi. Questo tipo di caratteristiche permetteranno alle reti *IoT* di far funzionare autonomamente i dispositivi senza l'intervento di un'autorità centralizzata. Una delle funzionalità più interessanti portate dalle *blockchain* è la capacità di mantenere un registro adeguatamente decentralizzato ed affidabile con tutte le transizioni che si verificano in una rete. In particolare, tale proprietà è essenziale affinché si possano superare conformità e requisiti normativi per applicazioni dell'*IoT* industriale (*IIoT*, *Industrial Internet of Things*) senza dover fare affidamento su modelli centralizzati.

Di seguito si voglio elencare i vantaggi che, secondo [B2], seguono l'utilizzo della tecnologia

*blockchain* nel mondo *IoT*:

- Rete pubblica - tutti i dispositivi *IoT* appartenenti ad un certo sistema hanno la possibilità di consultare il registro contenente tutte le transazioni fatte finora e tutti i blocchi della catena, dato che ogni dispositivo possiederà un proprio registro. Allo stesso tempo, le transazioni rimangono protette dall'esterno dalle chiavi private appartenenti ad ognuno dei dispositivi.
- Decentralizzazione - seguendo il concetto di consenso condiviso, la maggior parte dei partecipanti deve approvare una nuova transazione per poterla aggiungere al registro distribuito. Per questo motivo, le *blockchain* forniranno una piattaforma sicura per i dispositivi *IoT*. Inoltre, si elimina il traffico centralizzato ed il *single-point-of-failure* tipici delle architetture *IoT* centralizzate.
- Resilienza e affidabilità - ogni nodo contiene una propria copia locale del registro distribuito contenente tutte le transizioni che sono state fatte fino ad ora nella rete. In questo modo, la *blockchain* si protegge meglio da eventuali attacchi, infatti, anche se un dispositivo venisse compromesso, la *blockchain* verrebbe mantenuta intatta grazie a tutti gli altri nodi rimanenti.
- Sicurezza - le *blockchain* forniscono la capacità di costruire reti sicure composte da partecipanti inaffidabili; essenziale nelle reti *IoT*, specialmente se si vuole implementare un modello di messaggistica *peer-to-peer*, in quanto composte da numerosi dispositivi eterogenei tra loro. Quindi, tutti nodi di una rete *IoT* dovrebbero essere malevoli per effettuare un attacco.
- Prestazioni - una transazione impiega dei minuti per essere distribuita nella rete e sarà processata in un qualunque momento nell'arco della stessa giornata.
- Abbassamento dei costi - le soluzioni *IoT* ad oggi applicate sono molto costose dal punto di vista della costruzione e del mantenimento delle infrastrutture di enormi *data center* centralizzati. D'altra parte, investire su architetture *untrusted* come *peer-to-peer* sarebbe molto più conveniente all'aumentare dei dispositivi *IoT* connessi e meno costoso.
- Immutabilità - avere un registro immutabile è uno dei principali vantaggi della tecnologia *blockchain*. Ogni cambiamento che colpisce il registro distribuito deve essere verificato dalla maggior parte dei nodi della rete. Inoltre, le transizione non possono essere alterate o eliminate facilmente, infatti, se ciò dovesse accadere verrebbero alterati in cascata tutti i codici *hash* crittografati successivi al blocco contenen-

te la transazione modificata. Avere un registro immutabile nell'$IoT$ vorrebbe dire migliorare la sicurezza e la riservatezza dei dati.

- Anonimato - per elaborare le transazioni, sia i compratori che gli acquirenti usano degli indirizzi anonimi ed univoci che mantengono segreta la loro identità (proprietà molto criticata nell'ambito delle criptovalute).

# 2 | Sviluppo dell'Oggetto del Progetto

## 2.1 IOTA - La DLT per l'IoT

IOTA è una tecnologia *distributed ledger* (DLT), pensata essenzialmente per creare sistemi di transazioni e micro-transazioni *feeless* nel mondo *IoT* [S8]. L'idea alla base di IOTA è l'implementazione di una criptovaluta costruita su una DLT piuttosto che su una *blockchain* [S11]. IOTA si pone come obbiettivo quello di realizzare un "*trust layer*" orizzontale per l'*Internet of Everything* (IoE) sulla rete internet, il quale include un qualsiasi tipo di dispositivo in grado di connettersi [S12].

L'infrastruttura digitale di IOTA si basa sul *Tangle*, una struttura a grafo diretto aciclico in cui le nuove transazioni verificano quelle più vecchie. Il motivo principale per cui IOTA *Foundation* sceglie di non costruire questo sistema sopra una *blockchain* risiede nel modo poco efficiente in cui le transazioni vengono validate ed aggiunte alla catena di blocchi, infatti, immaginando una grossa quantità di transazioni da verificare è naturale pensare che aggiungere un blocco per volta in coda alla *blockchain* generi un collo di bottiglia [S11].

Secondo [B8], articoli redatto dalla IOTA *Foundation*, il protocollo IOTA è:

- Sicuro - l'intero sistema è distribuito tra tutti i partecipanti di una rete e perciò non vi è alcun *single-point-of-failure* o *single-point-of-attack*. Entità attaccanti verrebbero riconosciute e aggirate dalla rete stessa, la quale garantisce la corretta funzionalità del registro distribuito (il *Tangle*). A differenza di sistemi centralizzati vulnerabili, i dati memorizzati su IOTA non possono essere compromessi a meno che tutti i partecipanti della rete siano compromessi allo stesso tempo. IOTA mette a disposizione diverse funzionalità di protezione attraverso l'uso del *framework Stronghold*, come la gestione delle chiavi pubbliche o private e tecniche di crittografia avanzate; inoltre consente di far lavorare insieme i dispositivi in sicurezza.

- *Feeless* - il protocollo IOTA non richiede di pagare tasse ad ogni transazione. In questo modo rende possibile effettuare micro-transazioni in modo vantaggioso. Il protocollo consente, inoltre, il trasferimento separato di dati e valori, così che l'elaborazione delle transazioni sui dati siano risultino meno costose ai partecipanti della rete.

- Leggerezza - le risorse computazionali richieste ai nodi sono molto accomodanti. Lato *client*, IOTA offre libreria in linguaggio `C` per consentire al maggior numero possibile di dispositivi eterogenei di connettersi al *Tangle*. IOTA, per di più, non fa affidamento sul meccanismo di consenso *PoW*, dato che molto dispendioso energeticamente, per cui si riesce a tenere basso il consumo di energia permettendo anche ai dispositivi più piccoli *single-board* e ai dispositivi *edge* di supportare il protocollo. Ad esempio, IOTA è perfettamente supportato dal chip ESP32 [S13].

- Scalabile - la struttura del *Tangle* non pone limiti al numero di dispositivi che possono comunicare tra loro simultaneamente. Anziché adottare un approccio sequenziale nell'elaborazione delle nuove transazioni, *Tangle* supporta approccio operativo parallelo, infatti, IOTA riesce ad elaborare più di 1000 transazioni al secondo. Per fare un paragone, ad esempio, Bitcoin gestisce al massimo 7 transazioni al secondo. Aggiungere dispositivi al *Tangle* non implica necessariamente un aumento dei costi relativi alla successiva manutenzione dell'infrastruttura decentralizzata. Per rendere più agevole la scalabilità di un sistema, IOTA è l'unica DLT ad utilizzare il "Consenso di Nakamoto" [B9] applicato ai grafi diretti aciclici.

- *Permissionless* e *Leaderless* - IOTA può essere impostata per non avere "guardiani", perciò, chiunque potrebbe utilizzare l'infrastruttura senza dover pagare o chiedere permessi a qualcuno. Inoltre, IOTA è anche *leaderless*, vale a dire, ogni singolo nodo della rete deve convalidare una nuova transazione e non solo la maggioranza di essi. Nel caso in cui un nodo nota un'anomalia nella transazione deve segnalarlo agli altri partecipanti, i quali saranno chiamati a dare un'opinione sul conflitto che si è venuto a creare.

- *Standard* - IOTA *Foundation* lavora in collaborazione con *Object Management Group* (omg.org) ed altri enti simili per garantire un alto livello di interoperabilità tra ecosistemi.

- *Open-Source* - la rete basata su IOTA ed i relativi *framework* possono essere utilizzati gratuitamente e senza dover chiedere il permesso a qualcuno.

- Flessibile - mentre molte DLT possono essere usate per implementare registri pub-

blici (*permissionless*) o registri privati (*permissioned*), IOTA è capace di supportarli entrambi. In una tipica *blockchain* pubblica tutti possono partecipare, mentre in una privata ogni nodo partecipante deve essere pre-selezionato. Quest'ultima soluzione risulta essere meno decentralizzata e tipicamente esclude la possibilità di interagire con servizi di terze parti. IOTA è dotata della giusta flessibilità per riuscire ad offrire sia un Tangle privato sia pubblico allo stesso tempo.

### 2.1.1 Il Tangle

L'architettura della rete IOTA è composta da tre componenti fondamentali:

1. Nodi: componenti della rete a cui vengono indirizzate le transazioni.
2. Client: utenti della rete che inviano le transazioni ai nodi.
3. *Tangle*: il registro mastro distribuito che viene replicato su tutti i nodi IOTA.

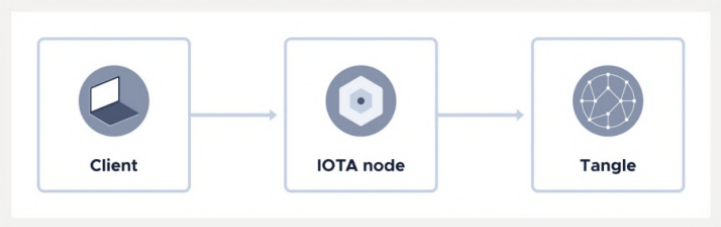


Figura 2.1: Componenti dell'ecosistema IOTA; *Sorgente*: [B5].

Il *Tangle* è prima di tutto una struttura dati che viene replicata in una rete di nodi. La struttura dati consiste in un grafo diretto aciclico di blocchi, piuttosto che una catena, in cui ogni nuovo blocco viene accodato a più blocchi già esistenti [S14]. Il consenso viene raggiunto dai nodi IOTA servendosi dell'aiuto di blocchi particolari detti *milestone*. I blocchi *milestone* vengono emessi da un nodo centrale chiamato *Coordinator* [S14]. In poche parole, il *Coordinator* è un *client* che invia messaggi firmati, cioè i *milestone*, di cui i nodi della rete si fidano e utilizzano per confermare nuove transazioni (non vale la pena approfondire oltre il ruolo di *Coordinator* in quanto IOTA *Foundation* ha dichiarato di volerlo rimuovere a partire da IOTA 2.0) [S15].

Il *Tangle* viene proposto da IOTA *Foundation* come l'evoluzione naturale della tecnologia *blockchain*, capace di affrontare problemi tutt'ora presenti su quest'ultima e di offrire soluzioni *distributed ledger* più efficienti e scalabili. Una *blockchain* viene identificata come una catena di blocchi lineare collegati tra loro attraverso degli *hash* crittografati. Le transazioni vengono aggiunte al registro solo se incluse in un nuovo blocco, il quale deve

essere verificato da quelli già esistenti e, tipicamente, questo processo richiede delle alte commissioni da pagare. È difficile pensare a come si possa velocizzare il meccanismo di verifica senza andare ad intaccare le proprietà di sicurezza, inoltre, se si pensa all'enorme quantità di transazioni emesse da un sistema *IoT*, le prestazioni dovranno essere parecchio elevate. Un altro grosso ostacolo del sistema di approvazione delle *blockchain* è che un solo blocco per volta può modificare il registro mastro, e questo, oltre forti ripercussioni sulle performance, porta anche ad uno spreco delle energie impiegate da tutti quei blocchi candidati a vincere il *PoW* ma che non ce l'hanno fatta. Per questo problema, il *Tangle* offre come soluzione un protocollo di consenso probabilistico e senza minatori, implementando un sistema parallelo per la validazione delle nuove transazioni. Con la capacità di lavorare in modo asincrono, IOTA trova il modo di aumentare enormemente le prestazioni del protocollo di consenso senza dover rinunciare alle importanti misure di sicurezza offerte dalla *blockchain*.

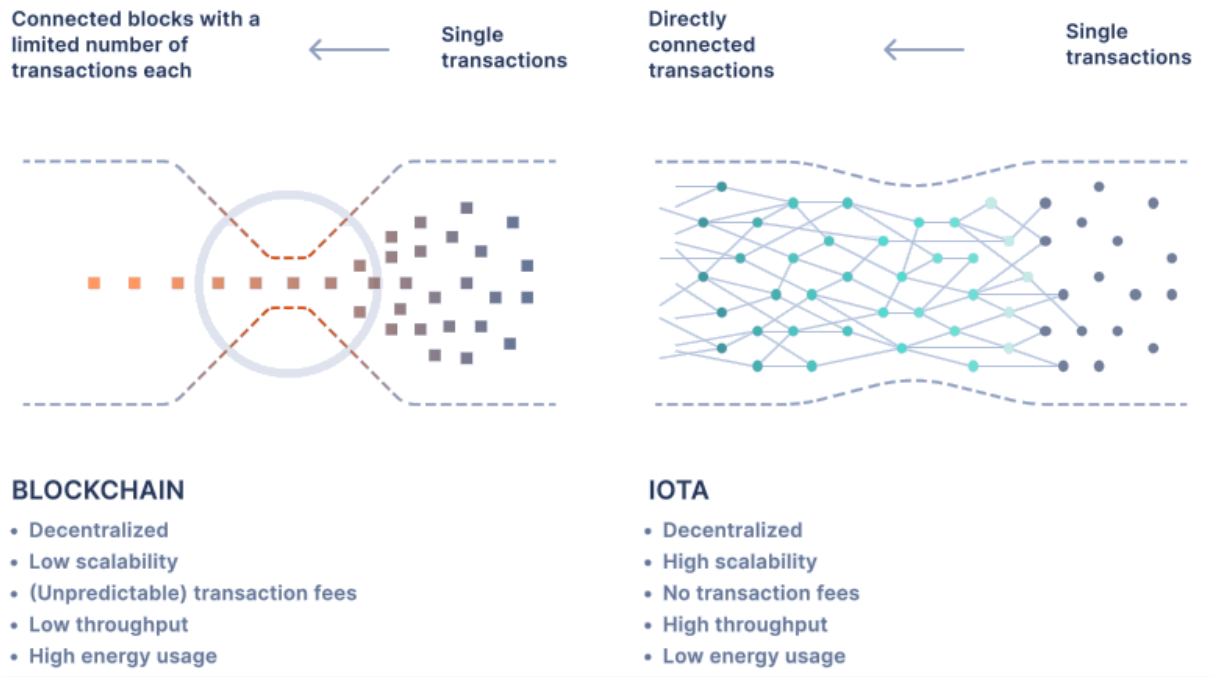


Figura 2.2: Confronto tra IOTA Tangle e tecnologia blockchain; *Sorgente*: [B8].

Come descritto nel *Lightpaper* [B8], il protocollo IOTA può portare benefici in quasi ogni industria ma soprattutto nel settore dell'*IIoT*, infatti, IOTA risulta essere una soluzione particolarmente promettente per l'integrazione dei dispositivi *IoT*. Per quanto non sia una blockchain in senso stretto, il *Tangle* è dotato delle stesse caratteristiche di trasparenza, decentralizzazione e sicurezza. Tuttavia, su questi due ultimi aspetti IOTA *Foundation* sta ancora lavorando per eliminare il *Coordinator* e raggiungere la completa decentralizzazione [B5].

Un problema molto importante dell'ecosistema IOTA è la presenza dei cosiddetti "*snapshot*", eventi periodici in cui il Tangle viene svuotato da tutte le transazioni più vecchie nei casi in cui la rete raggiunga i limiti di capacità di archiviazione. Questa scelta è in netto contrasto con la caratteristica di immutabilità e persistenza delle informazioni sulla DLT [B5].

## 2.2 La Blockchain of Things e applicazioni reali

In questa sezione si vuole discutere del paradigma *Blockchain of Things* (*BCoT*), realizzato dalla combinazione delle due tecnologie *IoT* e *blockchain*. Il concetto di *BCoT* rappresenta, oltre che effettuare operazioni sull'ambiente, la capacità dei dispositivi *IoT* di certificare i dati raccolti in maniera automatica tramite la *blockchain* e di fornirli all'utente finale all'interno di un registro decentralizzato [B5]. Il risultato che si spera di ottenere dall'adozione della *BCoT* in applicazioni reali *IoT* è quello di garantire contemporaneamente le qualità più importanti delle *blockchain* e dei sistemi *IoT*, quali: trasparenza, affidabilità, decentralizzazione, sicurezza e scalabilità [B5].

La tecnologia dell'*IoT* si è sviluppata sopratutto attorno al mondo industriale, e ad oggi, questa è utilizzata fortemente all'interno delle *supply-chain* per automatizzare gran parte dei processi, aumentandone l'efficienza e la qualità. I principali vantaggi portati sono:

- decentralizzazione del controllo;
- eterogeneità dei dispositivi impiegati;
- elevata interoperabilità tra i dispositivi da cui ne consegue la possibilità di integrazione dei sistemi;
- eterogeneità dei dati che possono essere raccolti ed elaborati [B5].

Il punto debole dell'*IoT* è la sicurezza, infatti, i dati che vengono raccolti molto spesso sono sensibili o critici ed è importante garantirne la riservatezza e l'affidabilità. Da questo punto di vista, la *blockchain* è in grado di proporsi come tecnologia capace di certificare le informazioni. La caratteristica della *blockchain* di essere immutabile e decentralizzata risponde almeno in parte al problema di sicurezza dell'*IoT*, garantendo la possibilità di conservare i dati direttamente all'interno di un *ledger* dove questi non possano essere alterati [B5].

A seguire, la problematica diventa quella di trovare un modo per collegare un dispositivo *IoT*, tipicamente *embedded*, con una *blockchain*. I dispositivi *IoT* si contraddistinguono spesso per avere pochissima capacità di computazione e di *storage* e allo stesso tempo

una larghezza di banda limitata. Per questo motivo risulta particolarmente ostico riuscire ad utilizzare gli algoritmi crittografici delle *blockchain* sui sensori di una rete *IoT*. A tal proposito, si è provato a cercare le risposta a questo problema nelle implementazioni di *blockchain* capaci di ridurre i consumi (come IOTA) oppure nell'adozione di topologie orientate al raggruppamento del consumo energetico e delle capacità computazionali su un singolo nodo a cui farà capo un certo numero di dispositivi *IoT* distribuiti su un'area estesa (si pensi al *fog computing*) [B5].

Si può dire, quindi, che la tecnologia *BCoT* sia per molti aspetti la risposta alle domande dell'industria 4.0, infatti, l'automatizzazione delle operazioni mediante dispositivi *BCoT* (sensori ed attuatori) permette di aumentare drasticamente l'efficienza dei processi produttivi. Tuttavia, modellare ed implementare un sistema *BCoT* presenta delle criticità, poiché questo dovrà rispettare diversi requisiti per garantire un sufficiente livello di trasparenza, tranciabilità dell'informazione, affidabilità, sicurezza, inoltre, è importante non tralasciare l'aspetto economico relativo a costi di infrastrutture e manutenzione, come anche l'aspetto del dispendio delle risorse energetiche. In particolare, l'elaborato [B5] evidenzia alcuni aspetti critici a cui un progettista di sistemi *BCoT* deve fare attenzione. Prime tra tutti, le qualità fondamentali che un sistema di questo tipo deve garantire sono stabilità e robustezza, ossia ci si aspetta una alto livello di *disaster recovery* e *fault tollerance*. Questi concetti vanno poi estesi all'insieme dei dati trattati dal sistema stesso, e non sulla infrastruttura di rete, infatti, l'informazione deve essere sempre garantita immutabile, affidabile ed opportunamente accessibile. I sistemi *blockchain* sono disegnati su architetture che prediligono meccanismi di consenso e tecniche crittografiche, perciò vengono scelti come tecnologia difensiva dei sistemi *IoT*, anche definita *Trust Machine* [B10]. Le *blockchain* rimangono comunque vulnerabili sotto alcuni aspetti:

- Attacco del 51% - questo tipo di attacco può essere effettuato qualora la maggior parte dei partecipanti ad una rete *blockchain* utilizzi la propria potenza computazionale in modo malevolo. Se gli agenti malevoli nel sistema sono almeno il 51%, allora avranno la capacità di alterare il processo di consenso, bloccare la verifica su un nuovo blocco e rifiutare o modificare transazioni. Ad esempio, il protocollo *PoW* è vulnerabile a questo tipo di attacco.
- Attacco Sybil - in questo caso, l'attaccante vuole attaccare la *blockchain* con l'obbiettivo di sovvertire il protocollo di consenso creando un gran numero di entità pseudo-anonime. Queste entità verranno utilizzate per manomettere a piacimento il processo di consenso. Un protocollo vulnerabile a questo attacco è quello chiamato *Proof-of-Stake* (*PoS*).

In ogni caso, l'integrazione della tecnologia *blockchain* nei sistemi *IoT* rimane molto vantaggiosa. Ad esempio, avere un sistema *BCoT* permette di avere la proprietà per cui un sistema è capace di resistere ad una certa classe di errori derivati dal problema dei generali bizantini; quindi che riguardano fallimenti dal punto di vista della comunicazione. Questa proprietà viene detta *Byzantine Fault Tolerance* (*BFT*). Un sistema si dice BFT se capace di continuare nelle sue operazioni anche nei casi in cui alcuni nodi sono mal funzionanti o malevoli. Per acquisire la proprietà di BFT, le *blockchain* offrono gli algoritmi di consenso [S16]. Infine, le "*Trust Machine*" riescono a proteggere i sistemi *IoT* da attacchi molto più comuni e distruttivi quali:

- Attacco *Denial-of-Service* distribuito (DDoS) [S17].
- Attacco per iniezione di dati fraudolenti [B11].

Il secondo aspetto critico individuato da [B5] evidenzia la necessità di implementare un modello *BCoT* come un sistema efficiente a livello energetico; in altre parole, il consumo di energia deve essere tale per cui il costo diretto che ne consegue sia sufficientemente basso se paragonato a quello necessario per alimentare l'intero ecosistema che vi è attorno. Il terzo aspetto fondamentale che si richiede di soddisfare ad un sistema *BCoT*, riguarda la conservazione sicura ed affidabile delle informazioni relative ai partecipanti del sistema, garantendone una protezione da eventuali attacchi esterni. Un ultimo problema che colpisce i sistemi *BCoT*, è quello dell'occupazione di spazio di archiviazione; infatti, tra le proprietà fondamentali delle *blockchain* vi è l'immutabilità, la quale impone l'impossibilità di eliminare informazioni già presenti nel registro mastro da cui ne consegue un constante aumento dello spazio occupato nel tempo. Dunque, come ultimo requisito fondamentale, un sistema *BCoT* dovrà basarsi su una *blockchain* la cui implementazione sia capace di sostenere un alto numero di transazioni effettuate.

### 2.2.1 Progetto ADEPT

L'articolo [B12], redatto da IBM *Institute for Business Value*, espone alcune osservazioni riguardanti alcune criticità a cui si dovrà far fronte nel momento in cui i sistemi *IoT* raggiungeranno una dimensione insostenibile in tutti gli scenari dalle attuali architetture. Gli aspetti critici esposti durante il presente elaborato va incontro a quelli individuati da IBM, la quale evidenzia in particolar modo che l'approccio centralizzato attualmente in uso espone i sistemi composti da miliardi di dispositivi connessi ad internet a problemi di sicurezza, problemi economici e problemi legati alla durabilità del sistema stesso nel tempo.

In un secondo momento, IBM e Samsun Electronics sviluppano il *Proof-of-Concept* (*PoC*)

di una piattaforma che dimostrerà come un'architettura ben decentralizzata possa essere capace di affrontare le sfide sopracitate, ovvero, ADEPT (*Autonomous Decentralized Peer-to-Peer Telemetry*). L'obiettivo primario del *PoC* ADEPT è quello di stabilire una base sulla quale dimostrare diverse funzionalità fondamentali per la costruzione di un sistema IoT decentralizzato. Sebbene IBM veda, in ambito commerciale, una piattaforma ADEPT ibrida, il *PoC* verrà progettato in modo completamente distribuito per estremizzare il concetto e provare la non necessità di un'autorità centrale per gestire le attività dei dispositivi IoT [B13].

Secondo IBM [B13], affinché un sistema *IoT* possa svolgere le sue funzioni tipiche senza l'ausilio di un'autorità centrale, un qualsiasi approccio decentralizzato deve supportare tre funzioni fondamentali:

1. *Peer-to-Peer messaging* - la natura decentralizzata delle reti *P2P* migliorano la robustezza di un sistema in quanto viene rimosso il *single-point-of-failure*. I partecipanti alla rete vengono trattati alla pari con la possibilità di condividere risorse computazionali senza dover dipendere da un *cloud* o *server* centrale, ottimizzando così l'utilizzo delle risorse e i costi di sottoscrizione di un servizio centrale. Il P2P messaging in un sistema IoT decentralizzato deve avere le seguenti qualità:
   - Fiducia e tecniche di crittografia per il trasferimento dei messaggi.
   - Bassa latenza e garanzia di consegna di un messaggio.
   - Memorizzazione e inoltro di messaggi con "*hop-on*" ad altri dispositivi collegati.

   Le *Distributed Hash Tables* (DHT) possono soddisfare tali requisiti, consentendo ai *peer* di di cercare altri *peer* sulla rete utilizzando una tabella *hash* con coppie chiave-valore memorizzate nel DHT stesso. Ogni dispositivo può generare il proprio indirizzo univoco basato su chiave pubblica (un *hashname*) per inviare e ricevere messaggi criptati con altri *endpoint*. Per ADEPT, IBM individua come miglior protocollo di messaggistica Telehash [S18], una implementazione *open-source* del protocollo Kademlia [B14] basato su DHT, utilizzato principalmente per scambiare notifiche tra i dispositivi senza l'utilizzo di un ente centrale.

2. *File sharing* distribuito - la condivisione distribuita dei file consente aggiornamenti software/firmware decentralizzati, *report* analitici basati sui dispositivi e la condivisione sicura di file e dati, talvolta di grandi dimensioni. Tali trasferimenti possono essere effettuati anche tramite reti P2P distribuite che utilizzano il DHT. ADEPT baserà questa funzionalità sul protocollo BitTorrent [S19], utilizzando principalmente per distribuire contenuti senza l'utilizzo di un *server* centrale.

3. Coordinazione autonoma dei dispositivi - senza un autorità centrale, i dispositivi devono essere capaci di definire il loro metodo di interazione all'interno della rete, oltre a coordinarsi in fase di registrazione e autenticazione. Interazioni più complesse richiedono, invece, l'intervento dell'utente. Per coordinare i dispositivi si fa uso anche dei contratti, cioè semplici accordi su azioni o controlli, contratti finanziari più complessi che prevedono pagamenti, oppure contratti di baratto che permettono ai dispositivi di di scambiare le proprie risorse per un servizio. ADEPT implementa un *framework* per il coordinamento autonomo basato sulla piattaforma *blockchain* Ethereum [S20].

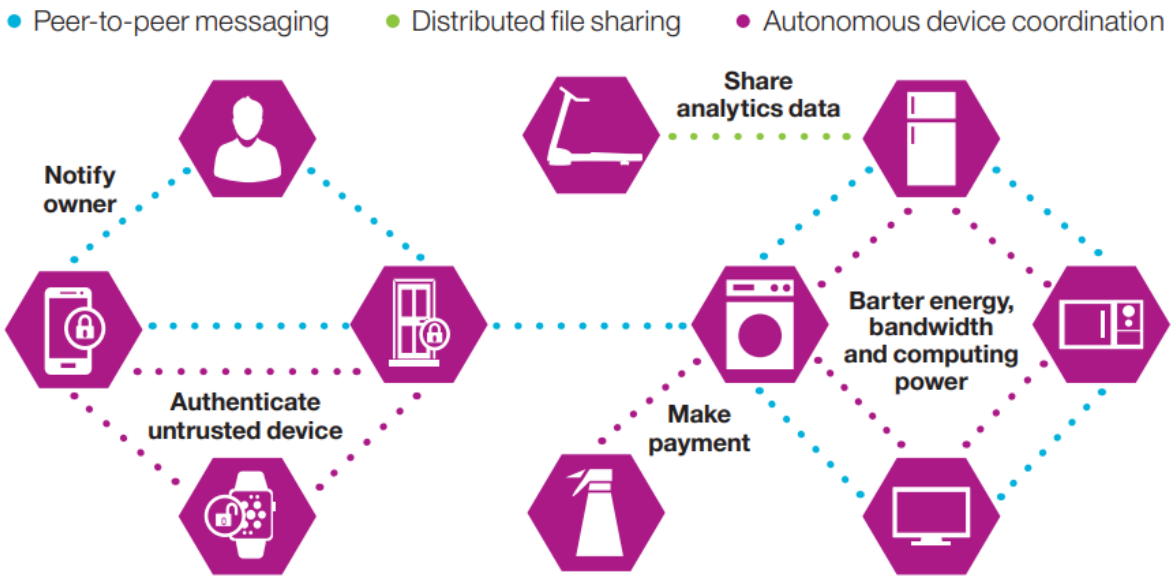


Figura 2.3: Le tre funzioni fondamentali supportate dal *PoC* ADEPT; *Sorgente*: [B13].

Successivamente, nell'*abstract* [B15] pubblicato da IBM *Institute for Business Value*, vengono illustrati differenti casi d'uso del *PoC* ADEPT in ambito B2C e B2B.

**Casi d'uso B2C** Lo studio effettuato dal gruppo IBM ha mostrato come, utilizzando ADEPT, una lavatrice Samsung è diventata un dispositivo autonomo in grado di gestire in modo autonomo il proprio rifornimento di materiali di consumo e la propria manutenzione, inoltre ha acquisito la capacità di negoziare il con altri dispositivi, sia in casa che fuori, per ottimizzare il consumo energetico.

1. Nel primo caso d'uso, una lavatrice Samsung W9000 riordina autonomamente il detersivo; infatti, questa è in grado di effettuare delle analisi *device-level* per capire la scorta di detersivo si andrà ad esaurire. ADEPT aggiunge alla lavatrice W9000 le seguenti funzionalità:

- interrogare la *blockchain* per capire se fosse già presente un contratto con un rivenditore per la ricarica del detersivo.
- richiedere una ricarica di detersivo al rivenditore tramite la messaggistica P2P.
- richiamare il contratto con il venditore ed effettuare un pagamento sicuro per l'ordine tramite la *blockchain*.
- notificare il proprietario della lavatrice tramite messaggio P2P che l'ordine di rifornimento è andato a buon fine.

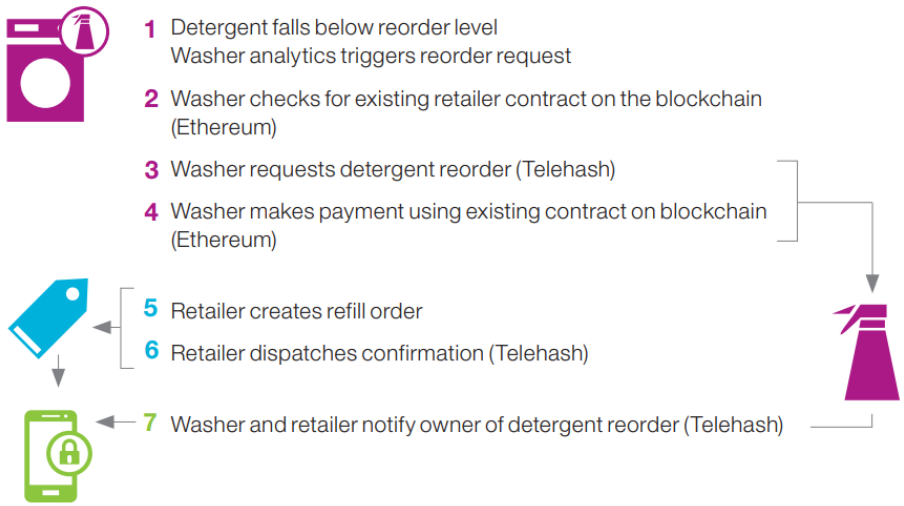


Figura 2.4: Transizioni effettuate per ordinare nuove scorte di detergente; *Sorgente*: [B15].

2. Nel secondo caso d'uso, la lavatrice Samsung W9000 riordina autonomamente i pezzi di ricambio per la manutenzione. Ogni dispositivo ADEPT ha delle informazioni chiave, come un ID univoco e le informazioni sulla garanzia, registrate sulla *blockchain*. Oltre a rilevare un guasto imminente, la lavatrice riesce ad ordinare un pezzo di ricambio sul mercato in completa autonomia. Per riuscire a fare ciò, la lavatrice ADEPT esegue un'analisi per valutare le prestazioni delle componenti; non appena individua un alto rischio di guasto, ordinerà un nuovo pezzo per sostituire il componente mal funzionante. Dalla *blockchain*, la lavatrice ADEPT riuscirà a sapere qual è lo stato della sua garanzia e a che venditore può richiedere il servizio. Solo nel caso in cui la garanzia non copra il servizio richiesto, la lavatrice ADEPT instaurerà un nuovo contratto per effettuare il pagamento al venditore. Una volta che il venditore si è accertato della validità della garanzia, potrà inoltrare la ricevuta di conferma della richiesta con i dettagli sia alla lavatrice che al proprietario.

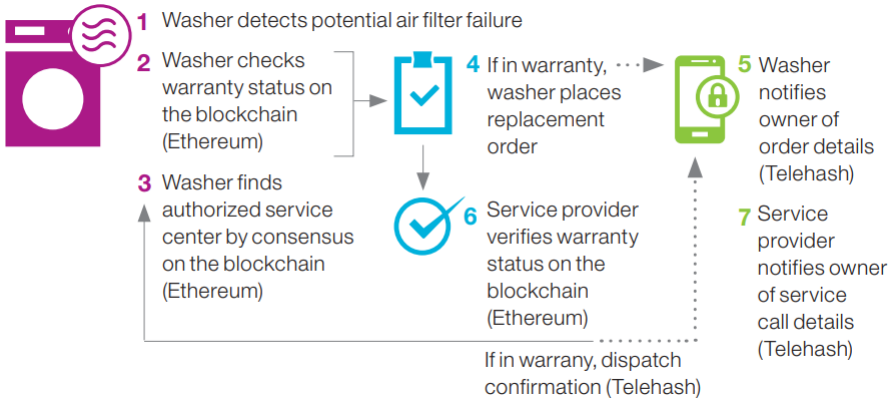


Figura 2.5: Transizioni effettuate per richiedere un servizio di manutenzione; *Sorgente*: [B15].

3. In questo terzo caso d'uso, una lavatrice Samsung W9000 negozia autonomamente il consumo di energia attraverso delle transazioni di baratto. La lavatrice ADEPT crea una contratto per negoziare le transazioni e i pagamenti tra gli elettrodomestici della casa che consumano energia. Lo scenario è descritto correttamente nella figura 2.6.

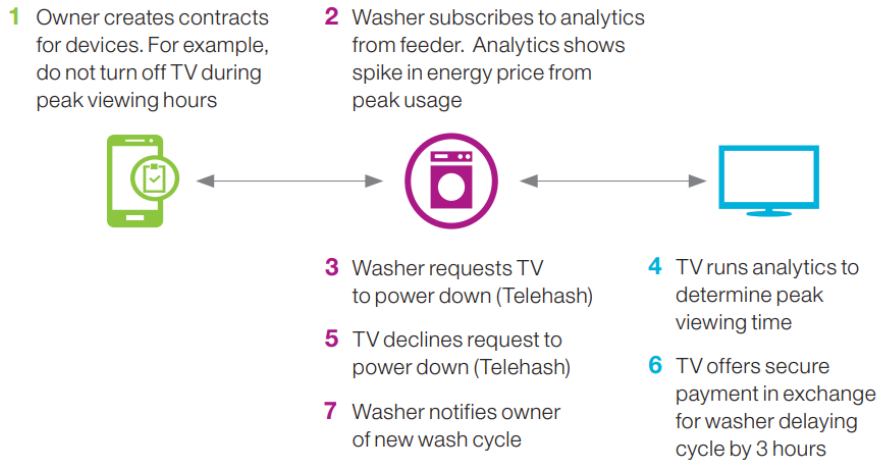


Figura 2.6: Transizioni effettuate per il baratto autonomo di energia tra elettrodomestici; *Sorgente*: [B15].

La lavatrice ADEPT è capace di accorgersi di imminenti impennate di consumo di energia. Di conseguenza, capisce di dover stabilire un contratto per negoziare sull'uso dell'energia con i suoi pari così da tutelare il proprietario eccessivi costi. Ad esempio, si immagina che la fonte di eccessivo consumo energetico è una TV, per cui la lavatrice gli demanda una richiesta di spegnimento. Si ipotizza poi che la TV

rifiuti la richiesta poiché questa è effettivamente utilizzata. La TV può ora mandare una notifica alla lavatrice includendo il risarcimento previsto dal contratto. Infine, la TV e la lavatrice si mettono d'accordo sul fatto che quest'ultima dovrà ritardare la sua fase di lavaggio, inviando anche una notifica al proprietario in cui si avvisa che l'aumento di energia elettrica è stato compensato con il ritardo del ciclo di lavaggio.

**Caso d'uso B2B** IBM ha anche testato un caso d'uso nell'ambito B2B in cui si aggiunge ADEPT ad alcuni dispositivi Samsung Large Format Display (LFD) che autonomamente dovranno visualizzare contenuti pubblicitari. Lo scenario prevede che il proprietario, che dispone di più LFD collocati in posizioni strategiche, sarà capace di pubblicare in tempo reale quali sono gli *slot* pubblicitari disponibili e di affittarli ai candidati dopo aver esaminato i loro contenuti. Allo stesso tempo, gli LFD affittabili sono capaci di comunicare tra loro e trovare in tempo reale quali sono gli *slot* liberi. Un LFD disponibile è in grado di ricevere una richiesta di visualizzazione, la quale verrà gestita recuperando il contenuto caricato dal proprietario sfruttando il meccanismo di *file sharing* distribuito. Quando ci si trova nelle fasce orarie appropriate, ogni LFD è anche in grado di iniziare a trasmettere autonomamente il contenuto previsto. Infine, per aver fatto visualizzare i contenuti, effettua e riceve pagamenti sicuri attraverso la *blockchain*.

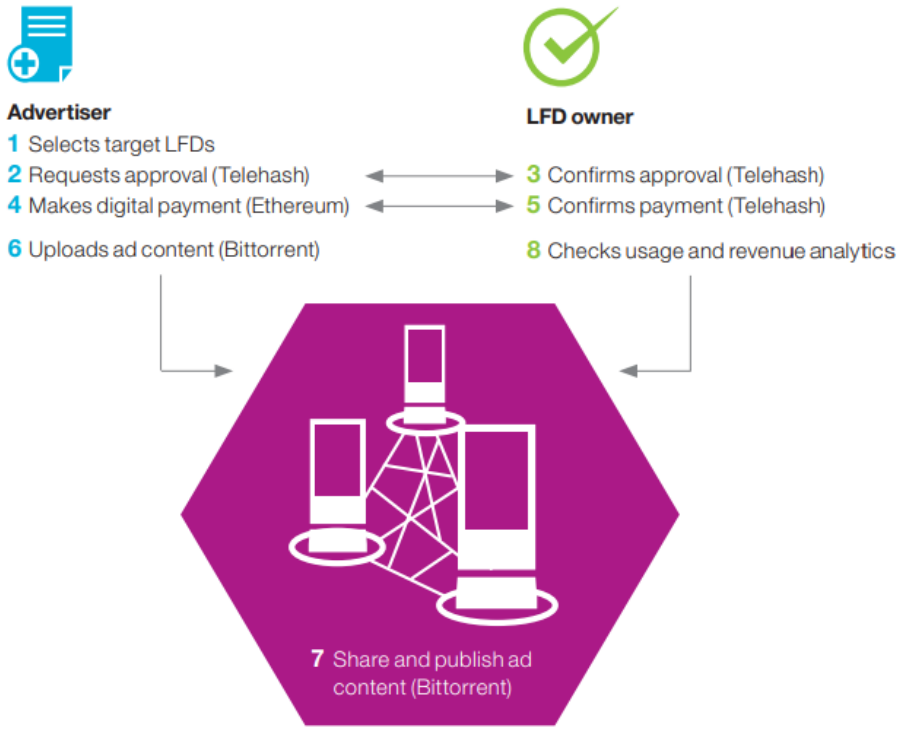


Figura 2.7: Transizioni effettuate all'interno di un *marketplace* pubblicitario autonomo; *Sorgente*: [B15].

### 2.2.2 Progetto SUSEE

Il progetto SUSEE (*Secure Sensor Platforms for Smart Energy Networks*) consiste in una collaborazione tra l'operatore della rete di distribuzione dell'energia SWO Netz GmbH (swo-netz.de), i due istituti di ricerca Fraunhofer FIT/IPT (ipt.fraunhofer.de), l'università TU Chemnitz (tu-chemnitz.de) e le PMI (piccole e medie imprese) peerOS (peeros.de), mCloud Systems (mcloud-systems.com) e TIP GmbH, nonché la fondazione no-profit IOTA. L'obiettivo del progetto di ricerca SUSEE è la progettazione concettuale di una soluzione scalabile per la trasmissione e l'elaborazione affidabile e sicura dei dati nelle reti di sensori, in particolare per le applicazioni di *smart metering*. Questa soluzione sarà realizzata sulla base del protocollo IOTA, del protocollo di rete *wireless LoRaWAN* (*Low-Power Wide-Area Network*) e della rete di *backhaul* WiBACK (wiback.org) autoconfigurante. Il progetto è stato sviluppato in conformtià degli *standard* dell'Ufficio federale tedesco per la sicurezza informatica (BSI) [S21].

Il progetto SUSEE nasce dalla necessità di modernizzare i tradizionali contatori dell'energia elettrica in Germania, i quali richiedono ancora l'intervento di un utente per leggere i dati di consumo e questo comporta costi aggiuntivi al cliente finale o all'impresa che offre il servizio. Oltre ai costi aggiuntivi in bolletta, la misurazione manuale richiede che l'utente si confronti con i moduli online del fornitore di energia, oppure che sia a casa ogni qual volta un operatore vada a fare la verifica. Anche i costi di assumere un operatore vanno a finire sulla bolletta del cliente.

Secondo i collaboratori del progetto SUSEE, i vantaggi che verrebbero portati dall'utilizzo di contatori di energia elettrica intelligenti sono:

- risparmio sui costi e maggiore comodità per i clienti finali, poiché le letture dei contatori vengono trasmesse direttamente all'operatore.
- i contatori possono essere letti più frequentemente, e quindi i fornitori possono gestire la distribuzione dell'energia elettrica in modo più efficiente ed accurato.
- poiché le letture dei contatori vengono elaborate senza alcuna interazione manuale, non vi è alcuna possibilità di errore umano o di frode.

I costi di una tale soluzione sarebbero dovuti all'infrastruttura necessaria per costruire un canale di comunicazione affidabile tra il contatore e gli operatori, ma questo viene affrontato utilizzando per lo più contatori intelligenti *wireless* piuttosto che via cavo. Uno dei principali svantaggi dei contatori intelligenti *wireless* è costo unitario più alto rispetto ai normali contatori elettrici. Tuttavia, connettere i contatori *wireless* tramite il protocollo di rete LoRaWAN è risultata essere una soluzione economica al problema,

infatti, non sono previsti costi per l'utilizzo di bande di frequenza senza licenza per la comunicazione *wireless* e non vi è alcuna necessità di contratto di servizio con operatori.

LoRaWAN è un protocollo di comunicazione wireless che consente di stabilire comunicazioni a lungo raggio a bassa velocità di trasmissione tra oggetti connessi, rendendolo ideale per la tecnologia edge. È stato progettato per funzionare come un livello di rete wireless ridondante, che può essere visto come un protocollo di comunicazione wireless supplementare accanto alle prossime reti di comunicazione mobile 5G o LTE [S22]. In genere, tecnologie come LoRaWAN hanno una velocità di trasmissione dati da 5 a 10 volte inferiore rispetto alle tradizionali connessioni 3G o LTE per implementazioni di grandi volumi (più di 100.000 unità). Essendo uno standard di comunicazione *open-source* disponibile a livello globale, LoRaWAN è diventata un'opzione popolare per la creazione di reti di sensori per i casi d'uso dell'$IoT$, soprattutto nelle *smart city* e nell'$IIoT$ [S22].

Ad ogni modo, è necessario che i contatori *wireless* rispettino i requisiti di riservatezza, integrità dei dati e interoperabilità stabiliti dal GDPR tedesco. Per soddisfare tali requisiti, un contatore intelligente non può comunicare solo basandosi su LoRaWAN senza protocolli di sicurezza aggiuntivi. Il progetto di ricerca SUSEE studia e progetta soluzioni scalabili per la trasmissione e l'elaborazione affidabile e sicura dei dati nelle reti di sensori. In particolare, il Modulo SUSEE consente di leggere informazioni informazioni del contatore tramite le reti e la tecnologia di comunicazione LoRaWAN, soddisfacendo allo stesso tempo i requisiti normativi del mercato tedesco.

Il progetto SUSEE è visto come un trampolino di lancio per esplorare l'applicazione delle DLT nel settore delle future reti energetiche, note come "*smart grid*", in cui i consumatori di energia possono anche essere produttori. Per le future *smart grid*, l'obiettivo è quello di produrre energia in molte centrali rinnovabili decentralizzate di piccole e medie dimensioni, dove l'elettricità può essere acquistata, fornita e immagazzinata da chiunque. È in questo scenario che lo IOTA *Tangle* può servire come infrastruttura di base integrata da protocolli applicativi affidabili per gestire identità, accesso ai dati e dispositivi. Le attuali reti elettriche sono state progettate per distribuire l'energia proveniente principalmente da poche e potenti centrali elettriche a un gran numero di consumatori. L'idea dietro al progetto SUSEE è quella di costruire un'infrastruttura decentralizzata e *permissionless* utilizzando IOTA, che sarà capace di trasformare le reti energetiche tedesche in *smart grid* di consumo, dove la regolamentazione necessaria per stabilizzare la rete è bilanciata dai vantaggi di un sistema economico aperto e decentralizzato [S22]. Un altro motivo che rende IOTA la scelta ideale per il progetto SUSEE è che questa è una DLT *feeless*, rendendo ancora più realizzabile una implementazione a basso costo.

Se al primo livello dell'infrastruttura troviamo IOTA assieme al protocollo LoRaWAN, al secondo troviamo IOTA *Streams*, un protocollo che consente di trasmettere dati strutturati e di gestire i diritti di accesso per tutti i partecipanti alla trasmissione. IOTA *Streams* mette a disposizione algoritmi crittografici utilizzati per proteggere i dati da accessi non autorizzati, autenticare i partecipanti e firmare i messaggi trasferiti da questi ultimi. È proprio grazie alle funzionalità di IOTA *Streams* che il Modulo SUSEE riesce ad effettuare connessioni LoRaWAN sicure ed a soddisfare i requisiti dell'Ufficio federale tedesco. Per garantire un massimo livello di sicurezza, i dati raccolti dai contatori vengono racchiusi in pacchetti *Streams* all'interno del Modulo SUSEE. Di contro, questo vuol dire che i sensori connessi ad un canale LoRaWAN devono trasmettere i dati, e di processi di autenticazione e autorizzazione verso i margini della comunicazione *IoT*. I dati vengono trasmessi dal contatore di energia elettrica al Modulo SUSEE, i quali comunicano attraverso una interfaccia seriale. Poiché sia il contatore che il Modulo SUSEE sono racchiusi in un involucro sigillato, in questa fase è impossibile corrompere i dati senza rompere il sigillo. All'interno del Modulo SUSEE, i dati vengono crittografati e firmati utilizzando IOTA *Streams*. I pacchetti di dati criptati possono ora essere inviati sulla rete LoRaWAN. Nel server applicativo LoRaWAN, viene utilizzato uno IOTA Bridge per collegare i pacchetti crittografati allo IOTA Tangle.

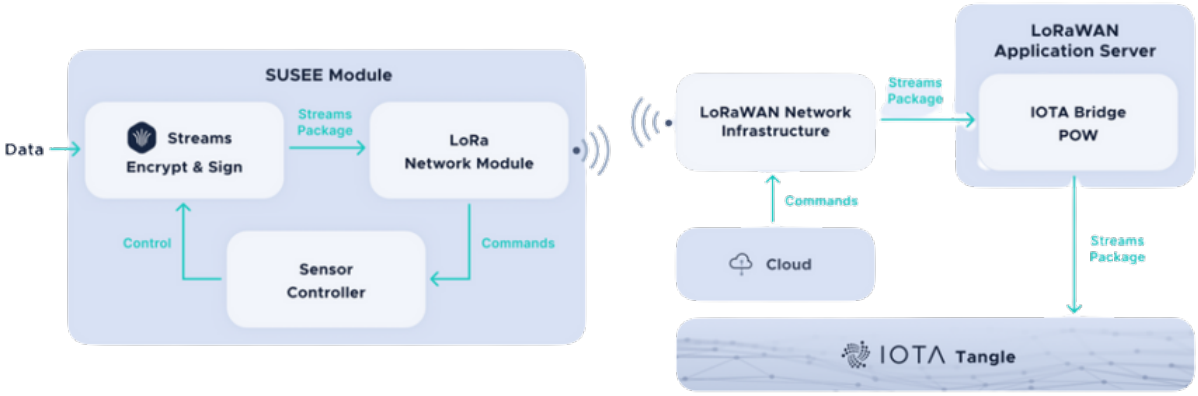


Figura 2.8: Crittografia sicura dei dati all'interno del Modulo SUSEE e trasmissione a un server LoRaWan; *Sorgente*: [S22].

Poiché l'architettura SUSEE prevede che i dati dei contatori di energia elettrica arrivino al *server* applicativo sotto forma di pacchetti *Streams* crittografati, la manutenzione di questi sistemi non richiede un'ulteriore protezione dei dati, il che si traduce in costi di manutenzione inferiori per questi sistemi.

Una delle sfide principali nell'invio di pacchetti di dati crittografati tramite LoRaWAN è la dimensione dello stesso, poiché LoRaWAN è molto limitata in questo senso. Per

questo motivo, è importante scegliere algoritmi crittografici che offrano un *overhead* di crittografia di dimensioni ridotte. Tuttavia, secondo il gruppo di ricerca SUSEE, la libreria IOTA *Streams* mette a disposizione algoritmi adatti all'IoT e all'avanguardia dando ottimi risultati rispetto ad altre librerie come MAM, infatti le dimensioni dei pacchetti si sarebbero ridotte di circa il 75% [S22].

# 3 | Conclusioni

Il presente elaborato ha evidenziato come la combinazione tra *IoT* e *blockchain* possa essere una soluzione efficace ai problemi elencati in precedenza. La tecnologia *blockchain*, infatti, si è dimostrata capace di supportare le qualità necessarie a rendere un sistema *IoT* universalmente scalabile, resiliente, distribuito ed in grado di far interagire i dispositivi *smart* in modo *trustless*, privato e affidabile.
Si offre infine uno spunto di riflessione per possibili ricerche future. Una delle sfide più rilevanti per le nuove tecnologie rimane la sicurezza; infatti, la mole di dati scambiata all'interno di un intero ecosistema *IoT* è enorme. Di conseguenza, per proteggere questi dati è necessario implementare algoritmi crittografici robusti, che richiedono però elevate doti computazionali; al contrario i dispositivi *IoT* spesso si presentano come processori economici e con una limitata disponibilità delle risorse.

# Bibliografia

[B1] Perry L. *IoT and Edge Computing for Architects*. Packt Publishing Ltd Birmingham, 2020.

[B2] Atlam H. Alenezi A. Alassaf M. Wills G. *Blockchain with Internet of Things: Benefits, Challenges, and Future Directions*. 2018.

[B3] Mell P. Grance T. *The NIST Definition of Cloud Computing*. 2011.

[B4] Yannuzzi M. Milito R. Serral-Gracià R. Montero D. Nemirovsky M. *Key ingredients in an IoT recipe: Fog Computing, Cloud Computing, and more Fog Computings*. 2014.

[B5] Giachin M. *Integrazione tra Blockchain e Internet of Things: implementazione, sviluppo e analisi*. Tesi di laurea, Alma Mater Studiorum Università di Bologna, 2020.

[B6] Shafagh H. Hithnawi A. Burkhalter L. Duquennoy S. *Towards Blockchain-based Auditable Storage and Sharing of IoT Data*. 2017.

[B7] Jacobsen J. *The Internet Protocol Journal*. 2015.

[B8] Schiener D. Ramachandran N. *How to enhance your business with IOTA*. IOTA Foundation Berlin, 2022.

[B9] Ren L. *Analysis of Nakamoto Consensus*. 2019.

[B10] Miraz M. H. *Blockchain: Technology Fundamentals of the Trust Machine*. 2017.

[B11] Bostami B. Ahmed M. Choudhury S. *Chapter 4 False Data Injection Attacks in Internet of Things*. Springer, 2019.

[B12] Pureswaran V. Brody P. *Device democracy: Saving the future of the Internet of Things*. 2014.

[B13] Pureswaran V. Panikkar S. Nair S. Brody P. *Empowering the edge: Practical insights on a decentralized Internet of Things*. 2015.

[B14] Ricci L. *Lesson 4: THE KADEMLIA DHT.* https://elearning.di.unipi.it/pluginfile.php/54434/mod$_r$*esource/content*/1/25 − 02 − 22 − *Kademlia.pdf*, 2022.

[B15] Pureswaran V. Panikkar S. Brody P. *Empowering the edge: Use case abstract for the ADEPT proof-of-concept.* 2015.

# Sitografia

[S1] Statista. *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030.* https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide, 2022.

[S2] Wikipedia. *IaaS.* https://en.wikipedia.org/wiki/Infrastructure_as_a_service, 2022.

[S3] Wikipedia. *SaaS.* https://en.wikipedia.org/wiki/Software_as_a_service, 2022.

[S4] Wikipedia. *PaaS.* https://en.wikipedia.org/wiki/Platform_as_a_service, 2022.

[S5] MQTT.org. *MQTT 5 Specification.* https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html, 2019.

[S6] Amazon Web Services. *Cos'è MQTT?* https://aws.amazon.com/it/what-is/mqtt/, 2023.

[S7] Wikipedia. *Distributed database.* https://en.wikipedia.org/wiki/Distributed_database, 2022.

[S8] Bellini M. *Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia.* https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante, 2022.

[S9] Ministero delle Imprese e del Made in Italy. *Tecnologie Distributed Ledger.* https://uibm.mise.gov.it/index.php/en/lotta-alla-contraffazione/servizi-per-imprese-e-consumatori/tecnologie-anticontraffazione/sot-servizio-orientamento-tecnologie-anticontraffazione/tecnologie-distributed-ledger, 2018.

[S10] Wikipedia. *Blockchain.* https://en.wikipedia.org/wiki/Blockchain, 2022.

[S11] IOTA Wiki. *IOTA.* https://wiki.iota.org/learn/about-iota/an-introduction-to-iota/, 2022.

[S12] IOTA Beginner's Guide. *What is IOTA?* https://iota-beginners-guide.com/iota-basics/what-is-iota/, 2021.

[S13] IOTA Foundation. *IOTA ESP32 Wallet.* https://blog.iota.org/iota-esp32-wallet-1b12b45d8a5/, 2019.

[S14] IOTA Wiki. *The Tangle.* https://wiki.iota.org/learn/about-iota/tangle/, 2022.

[S15] IOTA Wiki. *The Coordinator.* https://wiki.iota.org/learn/about-iota/coordinator/, 2022.

[S16] Binance Academy. *Byzantine Fault Tolerance Explained.* https://academy.binance.com/en/articles/byzantine-fault-tolerance-explained, 2022.

[S17] Wikipedia. *Denial-of-service attack.* https://en.wikipedia.org/wiki/Denial-of-service$_a ttack$, 2022.

[S18] *Telehash secure mesh protocol (v3).* https://telehashorg.readthedocs.io/en/latest/, 2015.

[S19] Vellishetty T. *Understanding BitTorrent Protocol.* https://www.beautifulcode.co/blog/58-understanding-bittorrent-protocol, 2019.

[S20] Ethereum.org. *What is Ethereum?* https://ethereum.org/en/what-is-ethereum/, 2023.

[S21] IOTA Foundation. *The IOTA Tangle Selected as Core Technology for SUSEE to Enable Large Scale Sensor Networks.* https://blog.iota.org/the-iota-tangle-selected-as-core-technology-for-susee-to-enable-large-scale-sensor-networks/, 2021.

[S22] IOTA Foundation. *SUSEE: A Smart Meter for the Mass Market.* https://blog.iota.org/susee-a-smart-meter-for-the-mass-market/, 2022.