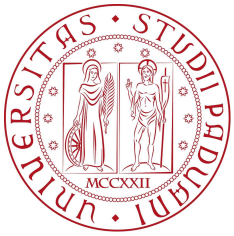

Università degli Studi di Padova
Facoltà di Ingegneria Meccatronica

Tesi di laurea

Analisi della tecnologia blockchain applicata alle reti di sensori wireless

Relatore: Prof. Alessandro Sona

Laureando: Leonardo Mattia Esposito

13 luglio 2023

Indice

Introduzione

L'avanzamento tecnologico ci pone continuamente di fronte a nuovi quesiti e alla ricerca di soluzioni sempre più originali, pratiche ed efficienti, con la finalità di potenziare le possibilità e migliorare le condizioni di vita. La tecnologia ha pervaso rapidamente e trasversalmente ogni ambito e ambiente del nostro quotidiano, tanto da poter parlare oggi di case intelligenti, sistemi di monitoraggio ambientale, automazione industriale, etc. Tutto ciò è stato reso possibile grazie all'aumento della potenza di calcolo in uno spazio sempre più ridotto e allo sviluppo di tecnologie di trasmissione dati veloci ed efficienti.

Tra le tecnologie più interessanti si trovano le reti di sensori wireless, che permettono la raccolta di dati, l'analisi dell'ambiente circostante e soprattutto la prevenzione di incidenti localizzati in un territorio preciso. Ciò che le ha rese così diffuse è soprattutto la possibilità di creare più dispositivi connessi in grado di comunicare in maniera wireless, quindi non cablata e scevra di una difficile e complessa installazione, permettendo inoltre un'ottima scalabilità. Queste reti sono utilizzate in diversi ambiti per la raccolta e la trasmissione di dati. Spesso i dati raccolti e trasmessi da queste tipologie di reti sono dati sensibili che necessitano di un livello di sicurezza sofisticato capace di sventare ogni tentativo di contraffazione o di manomissione.

Per affrontare questo problema, sono state pensate diverse soluzioni possibili, tra cui la possibilità di utilizzare una tecnologia tanto innovativa quanto discussa, ovvero quella della Blockchain. Negli ultimi anni, la Blockchain ha ottenuto notevoli risultati in campo economico, tramite le criptovalute, e come alternativa ai tradizionali strumenti di memorizzazione delle informazioni. Una caratteristica peculiare di questa tecnologia è la conservazione delle informazioni in blocchi collegati tramite crittografia, grazie alla quale è possibile tracciare la storia di un dato e i suoi scambi, arrivando al punto in cui è stato generato all'interno del sistema.

Gli studi sull'implementazione della blockchain nelle reti di sensori wireless sono ancora preliminari, ma già interessanti. Alcune ricerche hanno dimostrato come l'utilizzo della blockchain possa migliorare la gestione dei dati raccolti dalle reti di sensori, rendendo più facile l'identificazione di eventuali anomalie e la loro correzione. Altri studi hanno evidenziato come la blockchain possa essere utilizzata per garantire la provenienza e la tracciabilità dei dati, favorendo una maggiore trasparenza e accountability.

In sintesi, il documento ha come obiettivo principale quello di fornire una comprensione completa dei sistemi analizzati. Conseguentemente verrà condotta un'analisi preliminare sull'implementazione della tecnolo-

gia blockchain nelle reti di sensori wireless, al fine di comprendere a fondo il funzionamento di questa soluzione. Inoltre, verranno analizzati i vantaggi e gli svantaggi di questa tecnologia, in modo da fornire una visione completa e obiettiva delle sue potenzialità e limitazioni.

Capitolo 1

Blockchain

1.1 Cenni storici sulla blockchain

Satoshi Nakamoto, pseudonimo che nasconde l'identità di un individuo o di un gruppo di persone, nel 2008 pubblica "Bitcoin: A Peer-to-Peer Electronic Cash System" [1], un documento nel quale introduce il concetto di blockchain e di sistema di pagamento elettronico crittografato. In questo documento propone una soluzione al problema del "Double Spending", ovvero la vulnerabilità di cui soffrivano gli scambi di valute digitali. A causa della loro natura digitale, esisteva la possibilità di essere duplicate e da questo perdere completamente ogni valore si potesse attribuire loro.

Prima di questo documento che ha sancito la nascita di tutto ciò che le blockchain significano oggi, ne sono stati pubblicati altri che hanno contribuito alla nascita di questa tecnologia. Nel 1976 venne rilasciato "New Directions in Cryptography" [2], un documento sui ledger distribuiti. Successivamente "How to Time-Stamp a Digital Document" di Stuart Haber e Scott Stornetta introduceva il concetto di timestamp applicato ai dati. Un altro importante contributo fu dato da Adam Back con "Hashcash" portando alla pubblicazione nel 1998 di "b-money" di Wei Dai, un documento sulla creazione di denaro in una rete Peer-to-Peer. Tutti questi contributi rappresentano le basi della tecnologia blockchain.

1.2 Definizione

La tecnologia Blockchain è un database immutabile, decentralizzato e distribuito in una rete. Questo è condiviso tra tutti i nodi che formano la rete e le transazioni su di essa sono verificate e confermate tramite algorit-

mi di consenso. Le transazioni, una volta confermate, non potranno mai più essere cambiate o cancellate.

1.3 Descrizione della tecnologia

La tecnologia blockchain appartiene alla famiglia di tecnologie dei "Distributed ledger", cioè database condivisi ad una rete di partecipanti chiamati nodi. Ciò che la contraddistingue è il rivoluzionario metodo del concetto di fiducia, in quanto essa viene garantita attraverso degli algoritmi di consenso che eliminano la necessità di avere un intermediario. Quindi, ogni transazione che viene eseguita deve prima essere confermata da tutti i nodi della rete e, grazie alla crittografia e alla struttura dei blocchi, l'informazione diventa immutabile. Uno degli svantaggi invece, riguarda la velocità con cui queste transazioni vengono confermate in questo sistema. La blockchain più famosa, ovvero Bitcoin, gode di un'ottima decentralizzazione e sicurezza, tuttavia conferma solamente 7 transazioni al secondo, mentre un sistema centralizzato come quello di Visa ha una media di 1700. I sistemi centralizzati potrebbero risultare quindi più semplici e veloci ma, a scapito di queste caratteristiche la sicurezza e robustezza sono compromesse in quanto l'intero sistema è retto da una solo autorità garante. Come è possibile osservare in figura 1.1 il sistema decentralizzato si differenzia in quanto è strutturato con diverse autorità indipendenti che si occupano di porzioni distinte del sistema. Per quanto riguarda il sistema distribuito, la figura restituisce il concetto di delocalizzazione in quanto, più che essere un diverso tipo di controllo del sistema consiste nella possibilità del sistema di essere condiviso in molteplici location contemporaneamente.

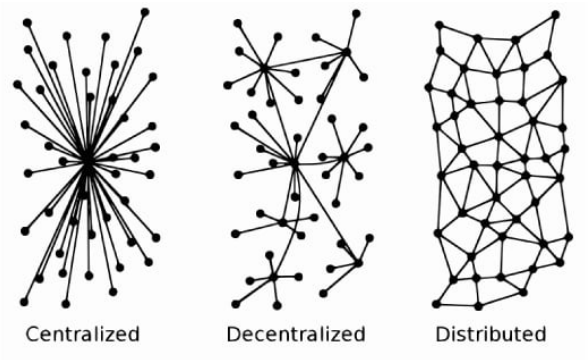

Figura 1.1: Differenze tra i sistemi [30]

Per comodità verrà utilizzato il termine decentralizzato per rimandare ad entrambi questi sistemi per poi specificare successivamente in caso di approfondimento di particolare applicazioni.

1.4 Come funziona

Esistono diversi tipi di blockchain, ma come detto sopra, la più famosa è la blockchain su cui si basa la criptovaluta Bitcoin. Per poter comprendere al meglio come funziona questa e le altre blockchain, è possibile utilizzare la figura 1.2 che ci restituisce intuitivamente i passaggi chiave dell'intero percorso di una transazione, o del pacchetto dati che vogliamo inviare attraverso di essa.

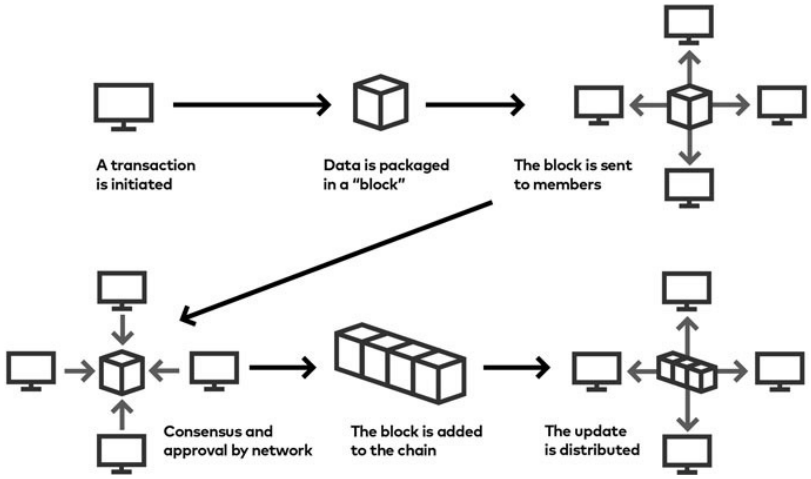

Figura 1.2: Come funziona la Blockchain [31]

Successivamente, verrà trattata la spiegazione di tutte le parti che compongono i passaggi di questa infografica.

1.4.1 Le Transazioni

La transazione è il pacchetto di dati si vuole inviare. In una blockchain che si occupa di scambiare valore è composta da:

- Indirizzo del mittente e valore delle transazioni ricevute e non spese
- Dati sull' autenticità dell'input e firma digitale della transazione
- Una tassa che in base all'ammontare decide la posizione nella coda

- Indirizzo del destinatario e valore inviato
- Change, ovvero l' eccedenza del valore rimandata indietro

Alcune di queste componenti non sono necessarie al fine di comprendere il funzionamento di una blockchain, ma sicuramente un aspetto molto importante da esplorare sono le firme digitali, a cosa servono e cosa garantiscono.

1.4.2 Firme digitali

La firma digitale si utilizza per dimostrare l'autenticità di un messaggio inviato. Questa garantisce che l'identità del mittente sia corretta, che il messaggio non sia stato modificato durante il percorso e che il mittente ha necessariamente inviato quel messaggio.

In una blockchain, la trasmissione di una transazione, cioè di un pacchetto dati, avviene se entrambi, quindi mittente e destinatario, sono in possesso di due chiavi, una privata e una pubblica. A questo punto, i passaggi affinché un pacchetto dati sia trasmesso sono:

1. Il pacchetto dati viene sottoposto alla funzione di hash.
2. Il risultato viene cifrato insieme alla chiave privata del mittente, ricavando dunque la sua firma digitale.
3. Invio del messaggio originale e della firma digitale
4. Il destinatario ricevuti questi due pacchetti dati, decifra la firma digitale utilizzando la chiave pubblica del mittente ottenendo così il messaggio prima che il mittente lo cifrasse con la chiave privata.
5. Il destinatario confronta quindi se il messaggio in chiaro e il messaggio decifrato siano uguali e se lo sono vuol dire che la firma digitale è valida, assicurando quindi le caratteristiche che essa dona.

1.4.3 I Blocchi

La blockchain, così come lascia intendere il nome, è una catena o sequenza di blocchi a cui ne viene aggiunto uno ogni intervallo di tempo prefissato. Questi blocchi dovranno contenere tutti i metadata necessari alla memorizzazione delle transazioni. Il numero di blocchi connessi tra di loro restituisce la lunghezza della blockchain, a partire dal primo blocco chiamato "Genesis Block". I blocchi svolgono una funzione sostanziale nella

blockchain, impedire attacchi "double spending", ovvero attacchi nei quali un attore malevolo esegue transazioni inviando una somma già spesa. La soluzione a questo problema risiede nella struttura intrinseca dei blocchi, in quanto essi riescono a garantire la sequenzialità delle transazioni. Una volta che un blocco è formato da un numero fisso di transazioni, questo viene sottoposto alla funzione di Hashing, includendo anche l'hash del blocco precedente. Questo lega la transazione ad un certo istante temporale, in quanto il nuovo blocco viene posto alla fine della catena e quindi la sua esecuzione è per necessità legata all'esecuzione del blocco precedente e così via. Da ciò si può anche notare che non è possibile aggiungere una tran-

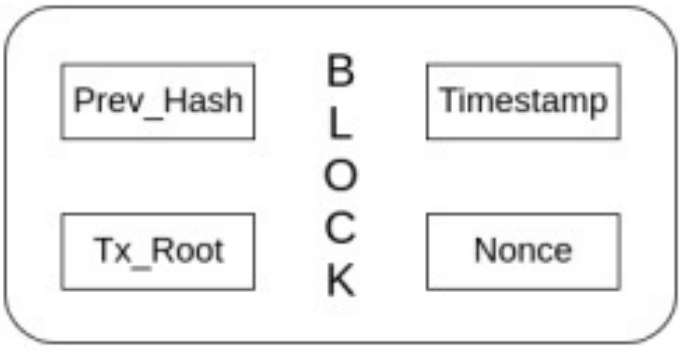

Figura 1.3: Struttura di un blocco

sazione in un blocco precedente, in quanto tutti i blocchi sono legati tra di loro grazie alla funzione di hash, e la modifica di uno invaliderebbe tutti i successivi.

Un blocco, come è possibile osservare nella figura 1.3, è quindi costituito da:

- Hash del blocco precedente
- Timestamp
- Albero di Merkel per le transazioni precedenti
- Nonce

1.4.4 La funzione di hash

La funzione di hash è una funzione deterministica e unidirezionale che trasforma una stringa in input, di dimensione arbitraria, in una in output,

di lunghezza fissa. Come è possibile osservare in figura 1.4, questo tipo di funzione non richiede un input con caratteristiche specifiche. La funzione traduce qualsiasi tipo di testo in un codice hash chiaro e distinto.

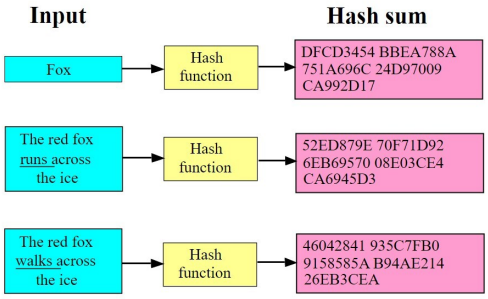

Figura 1.4: Funzione di hash [32]

Le caratteristiche che rendono fondamentale questa funzione crittografica sono:

- Uniformità: Non esistono due input che danno come risultato lo stesso output
- Determinismo: A prescindere dalle iterazioni, lo stesso input darà come risultato sempre lo stesso output
- Efficienza: Il calcolo dell'hash deve essere rapido e semplice a prescindere dell'input

Una volta delineato il comportamento di una funzione di hash, è possibile definire gli elementi che sono contenuti all'interno del blocco.

1.4.5 Hash del blocco precedente

L'hash del blocco successivo sarà generato con all'interno l'hash del blocco precedente, costruendo quella sequenzialità che cristallizza i dati all'interno della blockchain.

1.4.6 Timestamp

Il timestamp è un parametro temporale che indica l'istante di creazione del blocco ed è una mediana dei timestamp restituiti da tutti i nodi. L'implementazione di un timestamp rende il blocco impossibile da ripetere in futuro, poiché oltre all'ora, viene memorizzata anche la data di creazione del blocco e quindi non vi è la possibilità che lo stesso hash venga ripetuto più volte.

1.4.7 Albero di Merkle

L'albero di Merkle semplifica l'operazione di verifica dei contenuti delle transazioni nel blocco. In un blocco possono esserci un gran numero di transazioni. Esse vengono organizzate e crittografate tramite un numero di hash che ha struttura piramidale: ogni foglia dell'albero, la parte più esterna, possiederà un hash, che combinato con le altre foglie e quindi gli altri hash, daranno come risultato l'hash del ramo e così via. Risalendo la struttura dell'albero, si arriverà ad avere un singolo hash che racchiuderà l'intero set di transazioni. Questo fa sì che la modifica di anche uno di questi hash comporterebbe l'invalidazione di tutti gli altri. La verifica di una transazione nel blocco comporta quindi la ricostruzione di un numero di hash pari alla profondità dell'albero. Questa struttura migliora le prestazioni di verifica, passando da una successione lineare a una logaritmica del numero di operazioni necessarie.

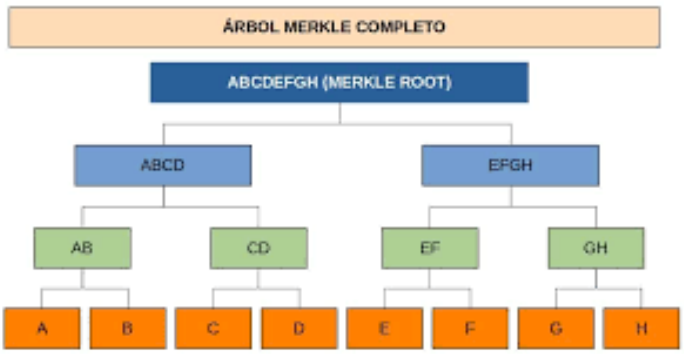

Figura 1.5: Albero di Merkle [34]

La figura 1.5 offre una chiara rappresentazione dello schema di funzionamento di questa sequenza di operazioni ordinate che compongono lo "Albero di Merkle". La struttura ramificata che si può osservare, offre chiari vantaggi alla ricostruzione di percorsi definiti. Si notino, le transazioni, rinchiuse in blocchi nella sezione più in basso dell' immagine denominate con le lettere alfabetiche dalla "A" alla "H". La stringa composta dagli hash dei blocchi, a due a due, verrà sottoposta ad hash, così da ottenerne uno per entrambi. Ottenuti quindi i blocchi superiori, ovvero i blocchi "AB","CD", "EF", "GH", si ripeterà la procedura, fino ad ottenere un unica funzione di hash capace di racchiudere tutte quelle precedenti.

1.4.8 Nonce

Il Nonce è un numero usato per la risoluzione dell'algoritmo di consenso "Proof of Work", ovvero l'algoritmo utilizzato da Bitcoin. Come si vedrà successivamente, però, di algoritmi di consenso ne esistono svariati e molto diversi gli uni dagli altri.

1.5 Algoritmi di Consenso

Gli algoritmi risolvono il problema dei Generali bizantini. Il problema

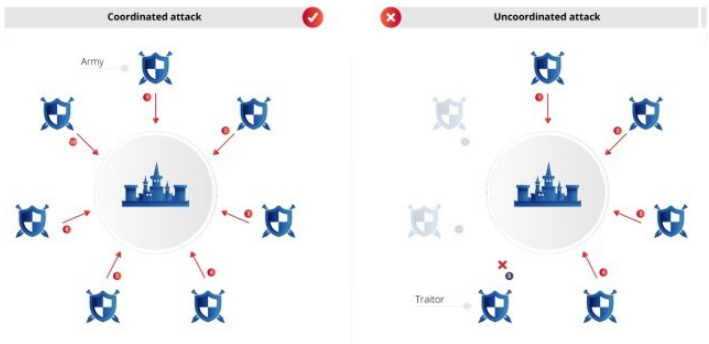

Figura 1.6: Problema dei generali bizantini [35]

consta in tre o più generali bizantini, impegnati in una campagna d'assedio. Essi devono decidere se attaccare o ritirarsi e possono comunicare tra di loro solo attraverso messaggeri. Inoltre, tra le fila dei generali, è probabile che ci siano dei traditori che tenteranno di inviare messaggi in grado di confondere l'organizzazione e quindi non partecipare poi alla battaglia. La vittoria in battaglia potrà essere raggiunta solo se tutti i generali concordano la mossa da fare. Un'immagine esemplificativa di questo è riportata in figura 1.6, nella quale è possibile osservare l' effetto che il traditore ha avuto sui partecipanti alla battaglia. La presenza del traditore, osservabile nella metà di sinistra della figura, ha come risultato quello di far desistere altri generali dalla battaglia, rendendo così impossibile l' ottenimento della vittoria. Ritrasponendo questo problema nel campo della blockchain, come i generali anche i nodi della blockchain devono necessariamente concordare tutti un'unica versione della blockchain. Si deve cioè raggiungere al termine dell'algoritmo o del processo di decisione, lo stato in cui tutti i validatori concordino con lo stesso valore.

Questo è ottenuto tramite gli algoritmi di consenso che, attraverso una votazione vinta per maggioranza, permettono di decidere quale sarà il blocco successivo della blockchain e accordarsi sullo stato del sistema.

Esistono algoritmi di consenso molto diversi tra di loro. Il più famoso è sicuramente quello della rete Bitcoin, l'algoritmo: Proof of Work.

1.5.1 Proof of work

Questo algoritmo si basa su una competizione tra i nodi, detti miners, addetti a risolvere un complesso quesito matematico, ricevendo in cambio un compenso per il lavoro svolto. Come abbiamo detto, in un blocco sono presenti quattro macro elementi e tra questi vi è il Nonce. Una volta inseriti tutti questi elementi e un nonce casuale, si otterrà una funzione di hash con alcuni valori iniziali. L'obbiettivo è quello di ripetere questa operazione modificando sempre casualmente il nonce all'interno, per ottenere un risultato al di sotto di un certo target. Questo target è definito dal numero di zeri all'inizio della stringa della funzione di hash, diversa per ogni input. Inoltre, poiché l'aggiunta di un nuovo blocco deve avvenire una volta ogni circa dieci minuti, il numero di zeri e quindi il target viene modificato in base all'hashrate, ovvero alla potenza di calcolo dei partecipanti alla verifica. Perciò, chi riuscirà a sviluppare un hashrate più alto avrà anche più probabilità di trovare il nonce corretto e assicurarsi la ricompensa in Bitcoin.

Per grandi e diffuse reti questo è un meccanismo quasi inattaccabile, in quanto per poter far approvare un nuovo blocco con transazioni fallate, sarebbe necessario un'ingente quantità di denaro per poter effettuare un attacco del 51 per cento. Questo tipo di attacco consiste nell'ottenere una potenza di calcolo maggiore di più della metà dell'intero network di miners, riuscendo così a risolvere necessariamente l'algoritmo di consenso e decidere tutti i nuovi blocchi della blockchain. Infatti, per piccole e nuove blockchain questo potrebbe rappresentare un rischio, ma attuare un simile attacco ad una piccola blockchain non porterebbe a guadagni così ingenti da giustificare l'impegno e, ugualmente per una grande e diffusa, i costi da sostenere per ottenere quella potenza di calcolo sarebbero nuovamente svantaggiosi. Ad oggi, nel 2022, l'hashrate - ovvero il numero di operazioni di hashing al secondo - si attesta sulle 260 milioni di operazioni al secondo. Questo tipo di algoritmo di consenso si basa quindi su quanta potenza viene spesa per risolvere la funzione di hash con sempre diversi nonce. Una volta arrivati al target, il miner "vincitore" convaliderà il blocco che successivamente verrà aggiunto alla blockchain. Questo avviene per ogni blocco e, poiché è presente anche un grande fattore di casualità, spesso

il miner che convalida il blocco non viene ripetuto, garantendo così una concreta decentralità della rete.

Come riportato sopra, esistono molti altri tipi di algoritmi di consenso che non consumano l'enorme quantità di energia utilizzata per l'algoritmo Proof of Work.

1.5.2 Algoritmi alternativi

- Proof of stake: questo algoritmo è il secondo per utilizzo e importanza dopo il Proof of work e, anzi, sta diventando l'alternativa per eccellenza per molte realtà nel mondo blockchain. Richiede minore energia rispetto al proof of work, e in questo caso la veridicità ed affidabilità dell'operazione viene determinata in base alla quantità di token posseduti da ogni partecipante alla rete. Maggiore è lo stake, cioè il quantitativo di token detenuti dall'utente, più elevate sono le possibilità che non si stia infrangendo il sistema. I blocchi della Proof of Stake vengono coniati e gli utenti abilitati ad effettuare tale coniatura vengono selezionati in maniera causale tra coloro che hanno effettuato lo stake.

- Proof of storage: simile al precedente algoritmo, ma in questo non viene sfruttata la potenza di calcolo bensì lo spazio di memoria del computer che svolge l'operazione, risultando meno energivoro e più efficiente.

- Reputation based: la priorità di costituzione del blocco è data ai nodi più attivi, cioè quelli con il numero più elevato di interazioni intrattenute con gli altri nodi.

- Proof of burn: questo metodo risulta meno dispendioso da un punto di vista energetico, ma al contrario più costoso da un punto di vista economico. Il termine burn fa riferimento alla valuta che necessariamente bisogna bruciare. Per poter costituire il nodo, infatti, si deve inviare una somma a degli indirizzi bloccati.

- Proof of authority: molto simile al precedente Proof of Stake, in questo caso però il consenso non è dato in base alla quota del nodo ma in base alla sua identità. Possono partecipare alla scrittura, solo i nodi dei quali è stata precedentemente verificata l'autenticità. È tipico delle reti provate.

1.6 Tipologie di Blockchain

Nonostante la tecnologia Blockchain abbia delle caratteristiche ben determinate legate alla decentralizzazione e alla massima trasparenza, ne esistono diverse tipologie e derivazioni. Una tecnologia di questo tipo, sarebbe infatti difficile da conciliare con i livelli di privacy e applicazioni più concrete che necessitano di un throughput minimo al fine di funzionare correttamente.

Al modello di blockchain pubblica di cui sopra si affiancano altre tre tipologie che modificano o aggiungono caratteristiche in base a specifiche necessità.

- Pubblica: ogni entità è libera di accedere alla rete, effettuare transazioni, visualizzare i dati e partecipare agli algoritmi di consenso. Coloro che svolgono l' attività di confermare un nuovo blocco, vengono ricompensati e coloro che attuano una transazione dovranno pagare una tassa.

  Esempi di utilizzo: rete di criptovalute, gestione di atti notarili.

- Privata: Il controllo è affidato ad un' organizzazione centrale. Questo fattore si discosta molto dalla definizione di blockchain, in quanto si perde la decentralizzazione in favore di una struttura centralizzata. Si possono definire, per l'appunto, database centralizzati. In questo caso solo gli utenti autorizzati possono visualizzare i dati e partecipare attivamente alla blockchain.

- Ibrida: combina alcune caratteristiche della blockchain pubblica e di quella privata. Ovvero l'organizzazione centrale può decidere quali dati rendere pubblici e quali privati e non accessibili.

  Esempi di utilizzo: gestione di cartelle cliniche, mercato immobiliare.

- Consortium: è utilizzato tra utenti che non si fidano l'uno dell'altro. Il numero di partecipanti a questo tipo di rete è ristretto e questi definiscono le regole per poter partecipare. Questa struttura è in grado di garantire standard di throughput. I dati generati vengono considerati affidabili solo dai membri della rete, mentre gli utenti esterni dovranno verificarli completamente.

  Esempi di utilizzo : wireless sensor network, pagamenti bancari, supply chain.

1.7 Smart contracts

Nel 1994, Nick Szabo introdusse per la prima volta il concetto di smart contract, ovvero un software capace di automatizzare processi e compiti pre-assegnati a una o più parti. Questa tecnologia non fu però adoperata fino a molti anni dopo, ovvero nel 2014, quando Vitalik Buterin pubblicò il Whitepaper di Ethereum. Ethereum è una piattaforma orientata a essere flessibile e programmabile tramite smart contract sulla blockchain. Questa è diventata il punto di riferimento per lo sviluppo di nuovi tipi di applicazioni finanziarie, quali la Defi e gli Nft. Gli smart contract, quindi, hanno rivoluzionato il mondo della blockchain.

1.7.1 Cosa sono

In linea con l'evoluzione della tecnologia blockchain, gli smart contract rappresentano una soluzione innovativa per regolare gli accordi tra le parti interessate. Contrariamente ai contratti tradizionali, gli smart contract sono caratterizzati dalla loro capacità di esecuzione automatica dei termini stabiliti tramite un codice su una blockchain. Questo approccio sfrutta la sicurezza, l'affidabilità e l'accessibilità della tecnologia blockchain, ampliando al contempo le potenzialità della stessa, senza comprometterne la decentralizzazione. Infatti, anche negli smart contract non è necessario l'intervento di intermediari esterni, poiché il codice esegue automaticamente le operazioni programmate.

1.7.2 Come funzionano

Gli smart contracts sono quindi programmi in codice che automatizzano determinati processi con determinate condizioni. Queste condizioni possono essere le più disparate; dall'invio di denaro automaticamente a seguito della vendita di un qualsiasi bene, alla regolazione della temperatura di una casa in base alla temperatura rilevata all'esterno. Questi programmi e il rispettivo codice vengono memorizzati nella blockchain e condivisi, quindi, tra tutti i nodi. Tutti i nodi, una volta che lo smart contract verrà richiamato, lo eseguiranno al fine di raggiungere il consenso sull'esito.

Capitolo 2

Reti di sensori wireless

Negli ultimi anni è nata sempre di più la necessità e la possibilità di monitorare l'ambiente. Il progresso nella miniaturizzazione dei componenti e nella trasmissione di dati in modo wireless ha permesso l'ideazione di dispositivi capaci di adattarsi ad ogni esigenza. Lo sviluppo in questi settori ha portato al delinearsi di una categoria di prodotti denominata "Internet of things", ovvero dispositivi capaci di stimare lo stato di qualsiasi cosa si sia interessati. Le reti di sensori wireless o WSN (Wireless Sensor Network) rientrano proprio in questa categoria, ma la loro applicazione è circoscritta al monitoraggio ambientale, industriale o anche militare, applicazioni quindi più ad ampio raggio. Questo è possibile grazie al fatto che le tecnologie wireless hanno permesso di superare i limiti delle soluzioni cablate, quali la difficile installazione e manutenzione e la pessima scalabilità. In questo capitolo verrà analizzata questa tecnologia e le sfide che la sua applicazione comporta.

2.1 Cenni storici sulle reti di sensori

L'interesse nello sviluppo di reti di sensori wireless si è sviluppato solo negli ultimi anni. Allo stesso tempo, però, l'impiego di sensori atti a monitorare specifiche situazioni non è nuovo.

Come molte tecnologie, il primo campo in cui furono sviluppati sistemi di sensoristica fu l'ambito militare. Durante la guerra fredda, i sottomarini sovietici adoperavano sensori acustici come sistema di sorveglianza. Tecnologia che poi fu ereditata dal National Oceanographic and Atmosferic Administration per la rilevazione di eventi nell'oceano.

Sempre durante il periodo delle grandi guerre mondiali, fu impiegata anche la tecnologia radar per la difesa aerea.

Nel 1969, invece, l'agenzia US DARPA compì il primo passo nello sviluppo della tecnologia che noi oggi chiamiamo internet, ovvero una tecnologia basata sull'interconnessione di più dispositivi.

La prima traccia dello sviluppo di una rete di sensori fu svolta dalla DARPA nel 1980 con la tecnologia DSN (Distribuited Sensor Network). Successivamente, lo sviluppo di tecnologie wireless e il miglioramento dei processi produttivi hanno portato alla realizzazione effettiva delle prime reti di sensori wireless.

2.2 Cosa sono le WSN

Le reti di sensori wireless o WSN sono una tecnologia dagli svariati campi di utilizzo; nonostante questo, la struttura e l'unità fondamentale di questa tecnologia sono sempre molto simili.

Il nodo sensore costituisce l'elemento di base di ogni rete di sensori wireless. Questo termine riassume una serie di dispositivi semplici, versatili e poco costosi, capaci di osservare il mondo fisico.

Una WSN è allora un'interconnessione wireless di nodi sensore atti a monitorare una certa area definita. La connessione wireless permette a questi dispositivi di aumentare le loro potenzialità aprendo a un vasto campo di applicazioni; tuttavia, una tecnologia così versatile porta con sé numerose difficoltà, sia hardware che software.

- Scalabilità: una WSN può essere estesa aggiungendo dispositivi man mano che le necessità lo richiedono e da questo diventare più forte. Sono contraddistinte quindi da un comportamento contrario rispetto alle reti di comunicazione.

- Adattabilità: includere cioè una serie di caratteristiche quali l' auto-organizzazione, la riconfigurazione automatica, una bassa complessità e la ridotta manutenzione. Grazie e ciò, questi dispositivi, sono in grado adattarsi al cambiamento di ogni ambiente e necessità.

- Basso costo: essendo una tecnologia caratterizzata da un alto numero di dispositivi, essi devono essere necessariamente semplici e a basso costo in quanto la quantità di questi rischierebbe di rendere questa tecnologia inconveniente.

Questi requisiti hanno la finalità di rendere questa tecnologia semplice e gestibile anche da utenti poco esperti, così da espandere il suo utilizzo. Come sopracitato, le reti di sensori wireless sono composte principalmente

da dispositivi chiamati nodi sensore. Questi dispositivi sono generalmente semplici e di piccola dimensione, questo perché per monitorare una vasta area si necessita di un gran numero di nodi capaci di memorizzare e trasmettere le informazioni. Essendo una rete, il potenziale di questa tecnologia risiede proprio nella moltitudine di informazioni raccolte localmente e che unite possono descrivere accuratamente una certa area di interesse, e quindi non nella potenza del singolo dispositivo. Essendo così semplici, i nodi sensori non possono svolgere incarichi troppo complessi, perciò una rete di sensori wireless è predisposta di dispositivi che fanno da intermediari tra il nodo sensore e la trasmissione dei dati ad altre reti (spesso internet). si avrà quindi che una WSN è composta da:

- Nodi sensore
- Nodi di calcolo : nodi con funzionalità maggiori rispetto ai nodi sensori, soprattutto in ambito trasmissione dati a medio-lungo raggio, svolgono una funzione sia di potenziamento della rete che di migliorare il consumo di energia. I dati dei nodi sensori viaggiano verso i nodi di calcolo, che fanno da intermediari per il gateway, e permettono ai nodi sensore di non dover utilizzare sofisticati dispositivi di trasmissione dati.
- Gateway: unità che si occupa dell' invio dei dati attraverso le altre reti, spesso internet e che quindi garantisce interoperabilità e reperibilità dei dati da chiunque.

2.3 Descrizione della tecnologia

Una rete di sensori wireless si contraddistingue per alcune caratteristiche che ne determinano le sfide progettuali. I nodi di calcolo e gateway sono dispositivi più complessi dei nodi sensori, in quanto svolgono operazioni computazionalmente ed energicamente più dispendiose e, paradossalmente, questo fa sì che questi dispositivi siano più facili da progettare. Come è possibile osservare in figura 2.1 i nodi sensore sono i componenti più numerosi e trasmettono i loro dati verso i "sink" ovvero i nodi di calcolo e loro verso il gateway. Le sfide progettuali e il fulcro di una WSN si trovano nello sviluppo e gestione dei nodi sensore, in quanto bisogna districarsi nella ricerca di un equilibrio tra prestazioni, consumo di energia e costo. Nella prossima sezione, verranno approfondite, per l'appunto, le componenti del generico nodo sensore.

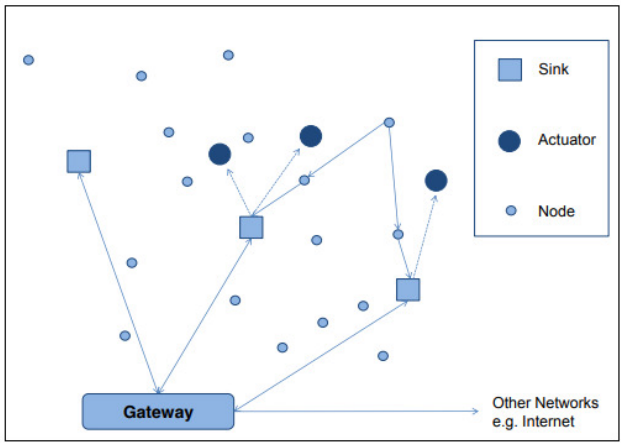

Figura 2.1: WSN [36]

2.3.1 Nodi sensori

I nodi sensori sono i dispositivi che costituiscono la rete e sono quelli che svolgono le funzioni più importanti. Questi si occupano della funzione di sensing, di memorizzazione e trasmissione dei dati raccolti. Quindi come è possibile osservare figura 2.2, i sotto-dispositivi che compongono un nodo sensore sono:

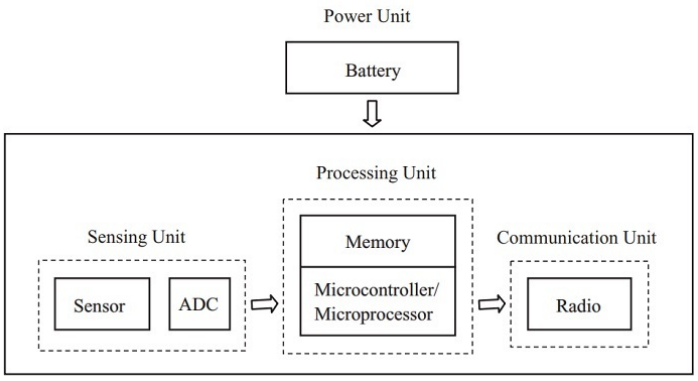

Figura 2.2: Generico Nodo Sensore [37]

- Uno o più tipi di sensori capaci di rilevare predeterminati dati dall' ambiente circostante
- Un' unità di elaborazione e controllo

- Una memoria
- Un' unita di comunicazione
- Un software capace di gestire l' hardware e i dati raccolti
- Una batteria

2.3.2 Sensori

Il termine "sensore" può generare confusione tra coloro che non sono esperti nel campo. In realtà, esso deriva dalla parola inglese "sensing", che si riferisce alla capacità dei trasduttori di trasformare una grandezza fisica in un segnale elettrico. I sensori sono dispositivi che svolgono la funzione di trasduttori, utilizzando leggi fisiche per misurare e codificare una grandezza fisica in una differenza di tensione proporzionale.

Per poter acquisire significato dal punto di vista ingegneristico, il segnale generato dai sensori necessita di varie operazioni di condizionamento. Queste operazioni servono a potenziare il segnale e filtrarne il contenuto dall'eccessivo rumore, al fine di permettere al segnale di svolgere l'intero percorso all'interno del circuito senza eccessive perdite.

Successivamente, il segnale attraversa un multiplexer (mux) che ha il compito di convergere le tante linee da cui arriva il segnale in una unica. In seguito, il segnale passa attraverso un convertitore analogico-digitale (ADC) che svolge l'operazione di campionamento nel tempo e discretizzazione nelle ampiezze, trasformandolo da analogico (continuo) a digitale (discreto).

Dopo aver subito queste operazioni di condizionamento, il segnale digitale è pronto per essere elaborato dal sistema e fornire le informazioni necessarie per la rilevazione e il controllo di una grandezza fisica.

I sensori sono disponibili in una vasta gamma di modelli commerciali e possono includere trasduttori per la rilevazione di temperatura, umidità, intensità luminosa, pressione, nonché sensori per il monitoraggio di sostanze tossiche disperse nell'aria o nel suolo, fumo, radioattività, telecamere, sensori di prossimità e molto altro ancora. La funzione di un sensore è quella di rilevare e/o misurare grandezze ambientali senza influenzarle. Gli attuatori, d'altra parte, hanno un ruolo duale in quanto sono dispositivi in grado di agire sull'ambiente circostante in diversi modi.

2.3.3 Attuatori

Oltre ai trasduttori, i nodi sensore hanno anche la possibilità di avere un attuatore, ovvero un dispositivo in grado di interagire con l'ambiente circostante. Possibili tipologie di attuatori sono bracci meccanici, valvole, irrigatori, ma anche sirene d allarme, altoparlanti, videoproiettori...

2.3.4 Unità di elaborazione e controllo

L'unità di controllo è composta da un microprocessore che sussegue lADC. Il microprocessore rappresenta lintelligenza del sensore e svolge tutte le funzioni di analisi e elaborazione dei dati. Per questo ruolo può essere scelta una CPU (Central Processing Unit), ma anche un FPGA (Field Programmable Gate Array) oppure un DSP (Digital Signal Processing) specifico per lanalisi di segnali in real-time. In generale, l'obiettivo è quello di scegliere un elaboratore capace di svolgere tutte le mansioni, che consumi poca energia e che sia a basso costo.

Nell'unità di controllo spesso è presente anche un convertitore digitale-analogico o DAC che trasforma i segnali in uscita dal microprocessore agli attuatori. In generale, l'obiettivo è quello di scegliere un elaboratore misurato esattamente sulle necessità del sistema.

2.3.5 Memoria

Il sistema necessita di una memoria per ospitare il codice del sistema operativo, i dati acquisiti dai sensori e quelli elaborati dall'applicazione. Per far ciò, spesso i nodi sensore si servono delle memorie integrate allinterno del microprocessore: una memoria ROM (Read Only Memory) e una RAM (Random Access Memory). Queste memorie spesso sono di pochi kilobyte in quanto la gestione di queste richiede un cospicuo dispendio di energia.

Alcune soluzioni aggiungono alle memorie integrate alcune memorie flash, più veloci e performanti ma incidenti sul lifetime del servizio.

2.3.6 Unità di comunicazione

L'unità di comunicazione si occupa di trasmettere i segnali verso gli altri nodi della rete e, di conseguenza, anche di riceverli. Le comunicazioni avvengono spesso tramite segnali radio poiché meno energivori. Sono possibili anche soluzioni di comunicazioni ottiche o a ultrasuoni. Il chip radio è la parte del circuito che consuma più energia. Per limitare questo effetto

si usano modulazioni già consolidate, di cui si conoscono i bassi consumi a scapito delle prestazioni che si attestano su pochi kbit/s.

2.3.7 Software

Il software si occupa della comunicazione tra i nodi e dello svolgimento applicazioni più avanzate. Nonostante le potenzialità, anche il software deve essere calmierato sui limiti energetici e di hardware. Per poter essere efficiente il software di questo tipo di tecnologia deve assicurare alcune specifiche:

- Ridottissima occupazione in memoria
- Basso consumo di energia durante i processi
- Gestione della concorrenza(accesso simultaneo alla stessa risorsa)
- Consumo quasi nullo in stand-by
- Supporto ai controlli di rete
- Accesso alle risorse di basso livello

Oggi esistono alcune soluzioni software generaliste capaci di gestire una rete di sensori wireless. Nonostante questo, la versatilità di questa tecnologia e delle sue unità di base spesso implica la creazione di software dedicati alla specifica applicazione. Questo, potrebbe considerarsi un lato positivo, in quanto lo sviluppo di un software dedicato ad una specifica applicazione porterebbe sicuramente a prestazioni migliori, ma allo stesso tempo, si creerebbe sempre più dispersione e poca integrazione tra i sistemi.

Una delle funzioni più importanti del software è quella di essere predisposto con uninterfaccia di comunicazione funzionale. Durante lo sviluppo di questa tecnologia si sono susseguiti protocolli di comunicazione proprietari che limitavano la potenzialità dell'intero settore delle reti comunicazione wireless. Infatti negli ultimi anni sono stati definiti degli standard comuni che migliorano l'interoperabilità tra prodotti di aziende differenti.

2.4 Stato dell'arte del software

Il rapido sviluppo di questa tecnologia ha messo in mostra i limiti che l'accompagnano e che ne rallentano la diffusione. Tra i problemi principali vi era la mancanza di integrazione tra le diverse soluzioni sviluppate dalle

aziende. Per questo motivo, l'Institute of Electric and Electronic Engineers (IEEE) ha sviluppato un'interfaccia standard utilizzabile da tutti i produttori. Ad oggi, la maggior parte dei dispositivi facente parte di una rete di sensori, si confà a questo standard chiamato: Standard IEEE 1451. Gli obbiettivi di quest'interfaccia sono:

- Definire le informazioni necessarie per interagire correttamente con il trasduttore attraverso una data sheet
- Rendere la rete aggiornabile, usando un'installazione dei dispositivi di tipo plug play ovvero capaci di essere aggiunti, rimossi o spostati senza una precisa procedura.
- Incorporare sotto un'unica interfaccia la maggior parte degli standard di comunicazione.
- Adoperare un modello comune della gestione dei dati, così da facilitare il controllo, la configurazione e la calibrazione
- Far interagire dispositivi obsoleti con le più nuove soluzioni wireless
- Ridurre la complessità dell'implementazione al fine di rendere la produzione dei disositivi più economica.

Questo standard definisce alcune caratteristiche chiave che i dispositivi devono possedere al fine di esserne inclusi. I livelli superiori dello stack inoltre possono essere gestiti tramite le proposte ZigBee che garantiscono interfacce comode e funzionali.

2.5 Limiti della tecnologia

Le reti di sensori wireless soffrono di una difficile progettazione. Questo avviene in quanto i nodi sensori, ovvero le unità fondamentali, sono dispositivi spesso non alimentati, incaricati di svolgere numerose operazioni per lunghi periodi di tempo restando piccoli, compatti e a basso costo. I colli di bottiglia più stringenti sono sicuramente il costo e il consumo di energia. Per quanto riguarda il costo, riducendo le difficoltà nella progettazione e nell'installazione questo dovrebbe subire un ridimensionamento permettendo così la diffusione di questa tecnologia. Dal lato dell'energia invece questi dispositivi dispongono di un'alimentazione a batteria e l'obiettivo è avere un network life-time compreso fra i 3 e 10 anni. Di conseguenza è necessario attuare una serie di scelte progettuali atte a limitare il più possibile i consumi.

Nel bilancio energetico i componenti colpevoli di consumare la maggior quantità di energia sono il microprocessore e il modulo della ricetrasmittente. Entrambi questi componenti necessitano quindi di un'accurata progettazione. I processori scelti per questo tipo di soluzioni sono processori in grado di svolgere solo operazioni base proprio al fine di salvaguardare il consumo energetico. D'altro canto il processore potrebbe alleggerire il carico dei dati da trasmettere se su essi avvenissero operazioni in loco di pulizia. Nonostante questo si è valutato che questo tipo di operazione sui dati provocherebbe un aumento repentino della quantità di energia consumata peggiorando la durata generale del sistema.

Per quanto riguarda l'ambito comunicazione dei segnali si è notato che la fase di lavoro a più alto consumo è quella della ricezione. Questo avviene perché nonostante la trasmissione sia un'attività più dispendiosa a livello energetico essa è però più breve e delimitata. La fase di ricezione può essere molto più lunga rispetto alla trasmissione poiché il dispositivo non sa quando riceverà informazioni e deve quindi rimanere in modalità di ricezione per lunghi periodi di tempo. Per risolvere queste difficoltà sono state sviluppate soluzioni software che rientrano nello standard IEEE 1451.

Capitolo 3

Applicazione della Blockchain alle reti di sensori wireless

Conclusa una descrizione qualitativa di queste due tecnologie, è possibile comprendere adeguatamente il prossimo capitolo di questo documento.

In questo capitolo verrà affrontata la tematica principale, ovvero, le ragioni e le difficoltà applicative di una tecnologia come quella della blockchain nell'ampio settore delle reti di sensori wireless.

3.1 Perchè

L'incontro di queste due tecnologie non è casuale. Ad una prima analisi, osservando gli schemi raffigurativi in 1.1 e 2.1, è possibile notare che queste tecnologie hanno più di un punto in comune. La struttura fondante è comune a entrambe e questo favorisce l'adattabilità di una all'altra. Di fatto entrambe queste tecnologie si basano sui cosiddetti nodi che gestiscono una serie di informazioni da trasferire, organizzare e unire in un'unica rete operativa. Inoltre la struttura gerarchica di una WSN è facilmente interpretabile tramite la tecnologia blockchain.

La parola chiave che guida la maggior parte degli studi applicativi della tecnologia blockchain alle reti di sensori wireless è sicurezza. Il settore delle WSN è in enorme crescita e i campi di utilizzo di queste reti stanno ampliando sempre più la necessità di proteggere i dati trasmessi. Alcune delle applicazioni che più gioverebbero di un robusto sistema di sicurezza sono:

- Applicazione medico-sanitario: con l'avvento dei dispositivi indossabili e impiantabili o dispositivi che monitorano le condizioni di

ambienti controllati, si è aperta la possibilità di monitorare un paziente in modo continuo, generando dati disponibili in modo rapido e preciso. I dati che così condivisi necessitano di essere tutelati e protetti da enti malevoli esterni, creando così la necessità di una sistema di sicurezza di alto livello.

- Applicazione militare: una rete di sensori capaci di monitorare le forze in campo, le munizioni, i danni riportati, la sorveglianza, comporterebbe dei benefici sostanziali.

- Applicazioni ambientali: in questo ambito si potrebbe monitorare prontamente l'incidenza di incendi, la qualità delle acque, l'inquinamento atmosferico, lo spostamento e lo stato dei ghiacciai e molto altro.

- Applicazione commerciali: adoperabili per il controllo dell'ambiente negli uffici, o la rilevazione dei furti d' auto.

- Applicazioni energetiche : implementando una WSN in uffici, fabbriche, abitazioni, si otterrebbe un miglioramento dell'efficienza energetica.

Si può notare come in ognuna di queste applicazioni l'intervento di un ente malevolo e quindi di operazioni atte a modificare i dati raccolti o a disabilitare l'infrastruttura comporterebbe un grave disagio. I sistemi di sicurezza sviluppati per le reti di sensori wireless sono anch'essi limitati dalle caratteristiche tecniche dei singoli dispositivi. L'implementazione della tecnologia blockchain potrebbe determinare un incremento delle prestazioni in questo ambito. Nonostante ciò questo tipo dimplementazione porta con sé numerose sfide progettuali. Di conseguenza è necessario comprendere se i nodi di una rete di sensori wireless siano in grado di gestire un software basato sulla blockchain e garantire comunque un funzionamento corretto e duraturo nel tempo.

3.2 Definizione della problematica

Come suddetto, la reti di sensori wireless, necessitano, a causa del loro utilizzo sensibile, di un sistema di sicurezza efficace. La struttura intrinseca della tecnologia WSN però implica non poche difficoltà nella realizzazione di ciò. I problemi che comporta una tecnologia di questo tipo sono legati sia ai singoli dispositivi che compongono la rete, sia al loro posizionamento

nell'ambiente. Potremmo riassumere le sfide che comporta questa tecnologia, per quanto riguarda la creazione di un framework di sicurezza, in questo modo:

- I canali di comunicazione delle reti di sensori wireless, sono aperti a tutti e chiunque potrebbe monitorarli.
- La limitatezza di risorse dei nodi sensori e in particolar modo la loro memoria, fa si che non sia possibile applicare un sistema di sicurezza avanzato. Nello specifico questi dispositivi sono vulnerabili ad attacchi DDoS, hacking, furto di dati e gestione di memoria da remoto. Attraverso questi metodi, per esempio, da un semplice sistema smart di gestione dei consumi di una casa, un hacker sarebbe in grado di capire quando il proprietario non è presente nell'abitazione.
- I singoli dispositivi sono posizionati nell'ambiente e ciò rende possibile un attacco ti tipo fisico sui componenti dei dispositivi stessi.
- Il modello centralizzato è intrinsecamente vulnerabile alle manipolazioni. Non ci sono garanzie sull'uso dei dati, potrebbero presentarsi fenomeni di manipolazione da parte delle aziende, per incorrere in costi minori o non essere denunciati, nei casi di WSN impiegate nell'ambito dell'inquinamento.
- La semplicità dei nodi sensori, apre la possibilità all'introduzione di nodi malevoli nella rete, capaci di intaccare i dati e lo scopo stesso della WSN.
- Il fallimento di un singolo nodo potrebbe comportare l'interruzione del servizio.

Possiamo riassumere queste considerazioni in tre principali categorie di problemi da risolvere Integrità e riservatezza dei dati, Convalida dell'origine e approvazione e Integrità e disponibilità del sistema.

3.3 Utilizzo della tecnologia Blockchain

Analizzando le problematiche sopra riportate, è facile rendersi conto come la tecnologia blockchain rappresenti una soluzione efficace e meritevole di essere analizzata. Le caratteristiche discusse nel primo capitolo di questo documento, che aumenterebbero il livello di sicurezza delle reti di sensori wireless sono:

- Autorizzazione controllata: le diverse tipologie di blockchain permettono di rendere pubblici, privati o selezionare quali dati mostrare.

- La struttura a blocchi: i blocchi, una volta formati, sono immutabili. Ciò farebbe si che i dati al loro interno non possano essere modificati a posteriori a discrezione di qualche ente esterno.

- Gli algoritmi di consenso: essi permettono di verificare che sia i dati che i nodi della rete siano effettivamente benevoli per la rete limitando la possibilità di introdurre nodi malevoli.

- Decentralizzazione : la natura decentralizzata della blockchain aggiunge un altro layer di sicurezza, riuscendo a sventare ogni tentativo di manipolazione delle informazioni e dei risultati. Da queste considerazioni, l'utilizzo della tecnologia blockchain sembra la soluzione ideale per risolvere i problemi di sicurezza legati alle reti di sensori wireless.

Nonostante ciò, questo tipo di tecnologia introduce nuove difficoltà capaci di mettere in dubbio l'effettiva applicabilità.

3.4 Schemi qualitativi di applicazioni

Sia la tecnologia blockchain che le tecnologie nelle reti di sensori wireless sono ancora in una fase di sperimentazione e sviluppo. Questo fa si che l' interazione di queste due tecnologie avvenga attraverso strade molto diverse. In questa sezione del documento andremo ad analizzare qualitativamente, alcune soluzioni adottate di applicazione di queste tecnologie, per poi riportare i risultati delle più interessanti nel prossimo capitolo.

3.4.1 Struttura gerarchica

Le reti di sensori wireless sono strutturate gerarchicamente come mostrato in figura 3.1, e sono costituite da tre componenti: il nodo sensore, il "cluster head" e il gateway. Questi tre elementi sono interconnessi in modo wireless. Il nodo sensore è responsabile per il rilevamento dell'ambiente per cui è stato progettato e invia i dati al "cluster head". Il "cluster head", può essere un dispositivo con maggiori capacità computazionali e di energia rispetto al nodo sensore base oppure un nodo sensore eletto per assolvere lo scopo in base a determinate condizioni. Questi ricevono e raggruppano i dati da tutti i nodi sensori di cui sono responsabili, e successivamente

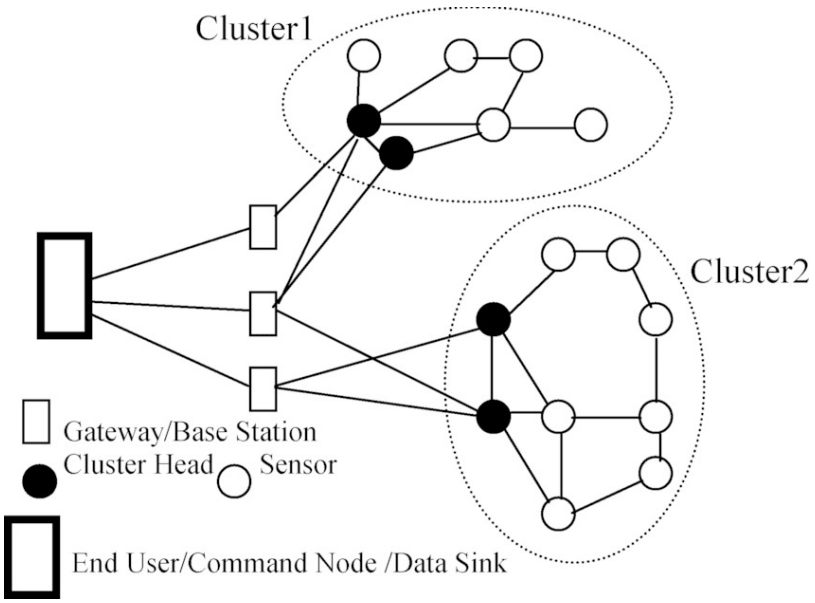

Figura 3.1: Gerarchia WSN [38]

inviano i dati al gateway. Il gateway, che è l'ultimo elemento di comunicazione in una rete di sensori wireless, invia, a sua volta, tutti i dati raccolti a una rete esterna come internet o un cloud privato. La tecnologia blockchain viene utilizzata per interfacciarsi con questa struttura gerarchica al fine di rendere i trasferimenti di dati e la struttura stessa della rete di sensori wireless più sicuri e protetti. Tuttavia, la complessità crittografica della tecnologia blockchain potrebbe limitarne l'utilizzo in questo tipo di reti a causa delle risorse limitate disponibili nei nodi. Per sfruttare i vantaggi della blockchain, spesso viene utilizzata una blockchain privata per evitare la manipolazione dei dati o la falsificazione delle informazioni e per prevenire minacce, attacchi e uso improprio delle informazioni. In questo scenario, il gateway è responsabile dell'autenticazione dei nodi sensori partecipanti e memorizza l'ID del nodo insieme agli ID del nodo blockchain, resi anonimi. Inoltre, il gateway memorizza tutte le chiavi pubbliche di tutti i nodi sensori partecipanti. Durante il percorso dal "cluster head" di origine al gateway, quest'ultimo memorizza le informazioni sul percorso inverso verso la sorgente. In questo modo, il gateway non ha bisogno di riscoprire nuovamente il percorso per il "cluster head". Ciò alleggerisce l'overhead di controllo dalle pesanti comunicazioni peer-to-peer necessarie per gli aggiornamenti dei blocchi. In questo schema, gli aggiornamenti dei blocchi avvengono attraverso il gateway per ridurre gli overhead. Il "cluster head" aggiorna e invia il proprio ID nella blockchain al gateway.

Ogni blocco memorizza il nonce, l'hash dell'intestazione precedente, il timestamp, il tipo di blocco, il conteggio dei dati di ogni tipo e l'hash dei dati, in questo modello i dati effettivi non vengono archiviati nei blocchi, per ridurre i requisiti di archiviazione soprattutto quando i dati sono audio, video o immagini ecc. Tutti i dati raccolti dai nodi del sensore vengono comunicati al gateway crittografando utilizzando la chiave pubblica del gateway stesso. In termini di protezione della comunicazione dei dati è P2P e nel framework viene utilizzata una crittografia a chiave pubblica mentre per l'hashing viene utilizzato SHA-256.

3.4.2 Sistema di autenticazione

Un'altra applicazione citata in: [27] della tecnologia blockchain all'interno delle reti di sensori wireless è la blockchain usata come sistema di autenticazione degli utenti e dei dati benevoli per la rete. Questo tipo di implementazione riesce ad apportare ottimi vantaggi alle attuali tecnologie WSN, come: autenticazione sicura, autenticazione dei nodi, identificazione dei cluster head e aumento della decentralizzazione che, come abbiamo osservato, aumenta intrinsecamente la sicurezza di questo tipo di tecnologie.

I modelli proposti per questo tipo di applicazione sono due e nonostante abbiano un obiettivo similare l'approccio utilizzato e i sistemi in sé sono caratterizzati da grandi divergenze.

Sistema di autenticazione gerarchico: In questa applicazione per aumentare le potenzialità della rete di sensori wireless vengono aggiunti nodi specifici come i nodi firewall e i nodi edge che grazie alle loro specifiche tecniche adatte fungono da ponte tra la rete e la blockchain.

1. Nel sistema blockchain, gli utenti inviano i propri dati ad una rete decentralizzata basata su un consenso globale. Tuttavia, l'aggiunta di tutti i componenti della rete alla blockchain può richiedere un elevato consumo di tempo e risorse a causa della crittografia frequente, compromettendo le funzionalità in tempo reale della rete. Per evitare questo sovraccarico, i nodi blockchain privati devono essere autenticati per accedere alla rete, mentre i peer appartenenti a diversi Wireless Sensor Network (WSN) possono accedere solo con l'autorizzazione degli amministratori delle stazioni base, garantendo così l'accesso controllato alla rete e preservando le funzionalità in tempo reale. Per adattarsi a questo modello di rete, viene sviluppata una metodologia blockchain multi-micro basata su WSN, come rappresentato nella figura 3.2. Il modello multi-micro contiene due parti in

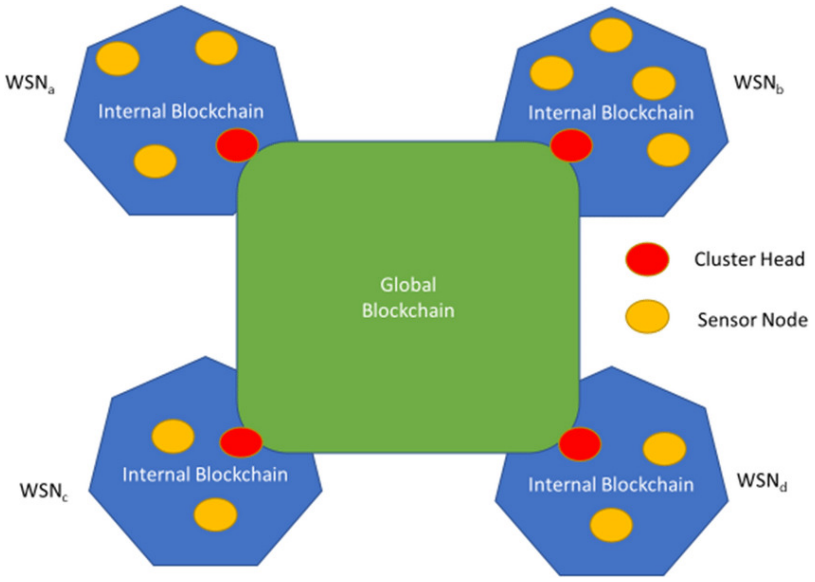

Figura 3.2: Sistema di autenticazione gerarchico [27]

cui sia le stazioni base che i produttori di dispositivi sono collegati al sistema blockchain come nodi minatori. Essi iscrivono e autorizzano i nodi cluster head nella blockchain pubblica e autorizzano il contatto tra i nodi WSN e le identità dei dispositivi degli utenti. I servizi cloud sono implementati per identificare i nodi dei membri del cluster e i dati di identificazione dei nodi vengono visualizzati nella rete blockchain dopo l'autorizzazione. L'autenticazione biometrica dell'utente finale consente il collegamento diretto al sistema blockchain e la convalida dell'utente tramite le reti blockchain pubbliche che sono state stabilite. La blockchain interna è una blockchain privata composta da tutti i membri della rete in un unico WSN. Quando il cluster head è associato ai registri di identità della blockchain pubblica, il nodo viene aggiunto nella rispettiva blockchain di riferimento. La blockchain regionale registra i normali nodi. I servizi cloud sono implementati nei cluster head per convalidare la normale configurazione dei nodi e le query di autorizzazione. La conoscenza del nodo autorizzato viene trasferita alla catena di elaborazione. Poiché il nodo principale del cluster è strettamente collegato al gateway e l'intero elenco di conoscenza del cluster viene prelevato online dal nodo del server centrale durante la configurazione nel nodo locale.

2. Sistema di autenticazione in sistema WMSN: L'applicazione in questione presente in: [18] è specifica per l'implementazione di un siste-

ma di autenticazione per reti di sensori wireless nel settore medico-sanitario. L'obiettivo è aumentare il livello di sicurezza e la decentralizzazione del sistema attraverso lutilizzo di tecnologia blockchain. In questa implementazione, la rete di sensori wireless è composta da nodi sensore, gateway e professionisti medici.

Come è possibile osservare in figura 3.3 i nodi sensore (SN) raccolgono i dati somatici dei pazienti e li trasmettono ai professionisti medici (MP) per lanalisi e la diagnosi. Prima di farlo, il SN viene registrato con il gateway (GWN) e negozia una chiave specifica per quella sessione (SK) con il MP. Questultimo possiede in chiaro le chiavi segrete emesse dal gateway per le future trasmissioni.

I SN sono dotati di funzioni PUF, che sono funzioni non clonabili basate su semiconduttori fisici e simili alle funzioni di hashing. Tuttavia, sono molto sensibili al rumore e richiedono una gestione accurata della loro creazione.

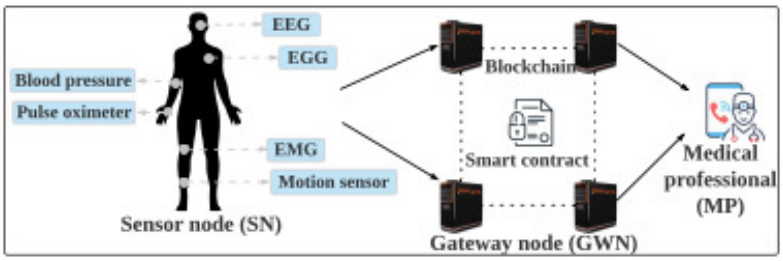

Figura 3.3: Sistema di autenticazione in una WMSN [18]

I gateway formano una rete blockchain e gli smart contract all'interno della blockchain gestiscono automaticamente le richieste dei SN e dei MP. I gateway mantengono il sistema blockchain basandosi su meccanismi di consenso predefiniti e non elaborano alcun codice sorgente relativo alla gestione degli eventi. Inoltre, gli utenti possono scegliere di utilizzare uno smart contract su una piattaforma blockchain matura come Ethereum o EOS per ridurre i costi di sviluppo e comunicazione. I gateway hanno l'obbligo di emettere chiavi segrete in risposta alle richieste di registrazione dei SN e dei MP, che condurranno l'autenticazione reciproca e la generazione della SK nel canale pubblico fornito dal gateway. I professionisti medici devono registrarsi alla rete formata dai gateway inserendo le loro password e dati biometrici. Dopo la corretta registrazione, i gateway distribuiscono le corrispondenti chiavi segrete agli MP, che verranno utilizzate per l'au-

tenticazione dei SN. Una volta confermata l'identità di un determinato MP, il sensore invierà i dati del paziente al MP per l'elaborazione.

3.5 Commento

I modelli applicativi sopra riportati chiariscono in quale modalità la blockchain possa essere utilizzata in una rete di sensori wireless. Le modalità non si limitano a questi modelli, ma essi rappresentano un buon punto di partenza per la comprensione delle potenzialità di queste tecnologie.

Come visto sopra, la tecnologia blockchain riesce egregiamente ad interfacciarsi con la struttura gerarchica delle reti di sensori wireless. Quest'ultima, essendo una tecnologia molto versatile, permette un ampio numero di implementazioni e soluzioni differenti.

Nonostante questo, è utile osservare come ci sia un filo conduttore in questi modelli: ovvero la presenza e la necessità di avere nodi della rete più potenti e capaci di creare strutture dati complesse come può essere la catena di blocchi. Spesso infatti la creazione e la gestione della vera e propria blockchain è affidata ai nodi gateway. Questi nodi hanno specifiche tecniche superiori rispetto ai semplici nodi sensori e capacità energetiche non limitate o comunque molto più ampie.

Oltre ai nodi gateway, possono essere aggiunti nodi con funzionalità specifiche al funzionamento del sistema blockchain. In generale quindi, la necessità di aumentare le capacità tecniche della rete rischia di rendere meno versatile una tecnologia come le reti di sensori wireless che hanno lobiettivo di poter essere implementate facilmente negli ambienti più disparati. Nel prossimo capitolo, verranno trattati alcuni esempi applicativi più raffinati e i loro risultati, definendo quindi in definitiva i vantaggi e gli svantaggi di questa soluzione.

Capitolo 4

Esempi applicativi

Gli esempi applicativi che verranno trattati in questo capitolo costituiranno una sintesi che, seppur limitata, esprime in modo chiaro il livello raggiunto di sviluppo di queste due tecnologie. Nello specifico, gli esempi di cui riporterò sotto la sintesi si delineano in un progetto che ha ottenuto ottimi risultati e incoraggia la sperimentazione in questo tipo di soluzioni e un progetto che, seppur meno strutturato, ne confuta l'applicabilità.

L'obiettivo è quello di riportare, oltre ai diversi approcci trattati nel terzo capitolo, soluzioni concrete e di interesse ingegneristico e riuscire a trarre così delle conclusioni sullo stato dell'arte attuale di queste tecnologie.

4.1 Real-time identification of irrigation water pollution sources and pathways with a wireless sensor network and blockchain framework

Finora la trattazione dell'utilizzo di queste tecnologie è stata affrontata da un punto di vista teorico e sperimentale, a causa anche della natura delle stesse. Nonostante ciò, è necessario anche riportare esempi come quello che andremo tra poco ad illustrare. Questo esplica in maniera pratica come queste due tecnologie interagiscono, riuscendo ad evidenziare i vantaggi e gli svantaggi della loro applicazione congiunta.

4.1.1 Introduzione

Questo studio [25] analizza come una rete di monitoraggio wireless possa essere gestita tramite l'impiego della tecnologia blockchain al fine di rile-

vare l'inquinamento delle acque e dei canali di irrigazione. A causa della rapida industrializzazione, vi è stato un progressivo aumento dell'inquinamento dei terreni agricoli. Lo scarico di acque reflue e, di conseguenza, di metalli pesanti nell'acqua costituisce una grave minaccia per l'ambiente, la produzione agricola e la salute pubblica.

Nonostante ci siano sistemi atti all'identificazione delle fonti di inquinamento, un sistema di monitoraggio delle acque in tempo reale potrebbe garantire dati sullo stato corrente e riuscire a avanzare previsioni future sulla qualità. Inoltre potrebbe garantire l'avvio di azioni di bonifica delle aree interessate. Ad accompagnare questa rete di monitoraggio sarà per l'appunto la tecnologia blockchain.

Questa, porta al sistema numerosi benefici. Grazie alla solida architettura di sicurezza legata all'autenticazione dell'utente, alle chiavi pubbliche, all'immutabilità dei dati e alle funzioni hash essa conferisce dei vantaggi necessari al fine del sistema. Inoltre la natura decentralizzata della tecnologia blockchain la rende particolarmente adatta alla determinazione dei diritti di proprietà. Di conseguenza i registri di transazioni possono essere in realtà i dati caricati e protetti provenienti dalla rete di sensori. La tecnologia blockchain fornisce inoltre un tracciamento costante, riuscendo a determinare così sia la fonte dell'inquinamento sia i percorsi che esso segue.

Questo framework è affiancato inoltre da un software di simulazione della qualità dell'acqua basato sui dati della rete di sensori in tempo reale. In generale negli studi sull'agricoltura le WSN sono state utilizzate per monitorare le condizioni ambientali; programmazione dellirrigazione basata su dati di rete in tempo reale; controllare le condizioni e i parametri ambientali per migliorare i processi colturali e migliorare la quantità e la qualità della produzione.

4.1.2 Materiali e metodi

Questo studio utilizza il backward pollution source tracing (BPST) per l'identificazione dei "percorsi di inquinamento delle acque" o PSP. Queste rilevazioni avvengono attraverso un sistema di monitoraggio wireless in tempo reale organizzato attraverso un grafico aciclico diretto (DAG) accompagnato da una piattaforma blockchain, uno strumento di tracciamento spaziale GIS e un modello WASP (Water Quality Analysis Simulation Program) ovvero un programma di modellazione dinamica dei compartimenti per i sistemi acquatici. Il funzionamento del sistema si riassume in questi passaggi:

1. Rilevazione dei dati sulla qualità dell'acqua in tempo reale attraverso la rete di sensori. Le concentrazioni di pH, temperatura, conducibilità elettrica (EC), cadmio (Cd), rame (Cu2+), zinco (Zn), nichel (Ni) e piombo (Pb) nell'acqua di irrigazione sono state misurate dai sensori che in questo studio sono di due tipi : i sensori regolari (R) e sensori specifici per metalli pesanti(M).

2. Se l'inquinamento supera lo standard normativo, vengono attuati i processi di tracciamento della blockchain e viene seguito il percorso dell'inquinamento in questione

3. Lo strumento di tracciamento spaziale GIS utilizza i dati del sistema di irragazione per tracciare spazialemte il percorso. Lo standard per l'acqua analizzata nello studio, ovvero l'acqua del distretto irriguo di Taoyuan in Taiwan, è di e 750 ţS/cm 25 C and 0.2 ppm.

4. Infine il modello WASP simula le concentrazioni di inquinamento.

.

4.1.3 Sistema blockchain

Il sistema utilizzato in questa applicazione è basato sulla piattaforma di G-Coin. Esso rilascia una licenza e un indirizzo di una moneta che rappresenta, in questo studio, la quantità di inquinamento. Gli indirizzi a cui si fa riferimento sono indirizzi di raccolta o indirizzi delle stazioni. Entrambi inviano e ricevono monete inquinanti.

Se le concentrazioni di inquinamento rilevate sono superiori agli standard, viene coniata una moneta digitale e inviata all'indirizzo della stazione. Le monete sono specifiche per sostanza inquinante; quindi a seconda della sostanza in eccesso presente nell'acqua viene emessa una specifica moneta che ne indica la presenza. Un indirizzo di stazione una volta ricevute le monete inquinanti le invia agli indirizzi di stazione a monte in modo da uniformare lindirizzo per tutte le stazioni.

Una volta che linquinamento supera lo standard viene generata una transazione tra la stazione di monitoraggio a valle e il suo indirizzo di stazione. Il dato successivamente viene contrassegnato con data e ora donando una connotazione temporale alla rilevazione. La stazione che rileva il superamento dei livelli di inquinamento, invia ad una stazione di raccolta le monete e quindi genera il punto temporale, ovvero data e ora.

4.1.4 Processo di transazione

1. Nella fase di pre-elaborazione gli indirizzi delle stazioni vengono ordinati. All'attivazione di un nuovo punto temporale vengono coniate monete di inquinamento e collegate all'indirizzo della stazione. Successivamente vengono generati i valori di hash sha256 (funzione di hashing a 256 bit) e registrati in tempo UNIX (ununità di misura del tempo che prende come riferimento il numero di secondi a partire dal 1970) come chiavi private legate all'indirizzo della stazione da cui sono state ricevute le monete di inquinamento.Questa organizzazione e individuazione è necessaria poiché i dati dovranno avere un punto di partenza specifico e quindi partire da un punto a valle verso le stazioni a monte descrivendo così il percorso dell'inquinamento. Questa organizzazione viene identificata attraverso un grafo aciclico diretto costruito secondo lasserzione: se esiste un bordo(u,v) nel grafico G allora u sarà prima di v. Il grafico DAG presente in figura 4.1 è definito dai vertici definiti dalla posizione delle stazioni e dai corsi dirrigazione. Quello che risulta è l'organizzazione delle stazioni da quelle più a valle a quella più a monte. Anche la WSN segue l'organizzazione del DAG.

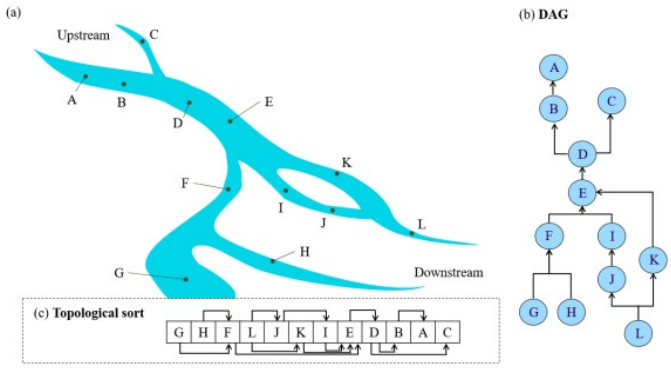

Figura 4.1: Identificazione stazioni a valle e a monte tramite DAG [25]

2. Acquisizione dati: in questa fase, i dati monitorati da una decisa stazione vengono acquisiti e successivamente inizia il processo di verifica che discerne i casi di superamento dello standard dalle rilevazioni regolari. Se non vi è alcun superamento degli standard allora l'operazione prosegue e viene avviata dalla stazione successiva. Se invece viene rilevato un livello di inquinamento eccessivo, inizia un iter atto a comprendere il punto scatenante del fenomeno inquinante e il percorso relativo,

(a) Viene determinato se la stazione rilevatrice possiede già delle "monete inquinamento" significa che la zona a valle di questa stazione è inquinata a sua volta e di conseguenza le monete presenti nella stazione rilevatrici possono essere utilizzate direttamente e non spedite ad altre stazioni.

(b) Se invece la stazione che rilevato il fenomeno non possiede già monete, vuol dire che essa si trova a valle dell'evento inquinante e quindi verranno inviate delle monete dalla stazione che precedentemente possedeva delle monete.

(c) Se anche nelle stazioni a monte vi è la presenza, già precedentemente, di monete inquinamento, allora verrà presupposto che anche la zona a monte sia inquinata.

(d) Se le stazioni a valle invece non sono inquinate, si può considerare la stazione che ha notificato l'evento inquinante come il punto di origine dell'evento e di conseguenza, le sue monete possono essere inviate al punto di raccolta per la definizione del punto temporale.

3. Elaborazione dati: La fase di elaborazione dati consiste nell'identificazione del punto temporale della stazione di raccolta. Esamina delle "monete inquinamento" specifiche per tipo di inquinamento rilevato e analisi della transazione di quest' ultime.

Grazie all'uso di una blockchain si è in grado di valutare, tramite le transazioni, le zone affette da inquinamento e il percorso descritto da esso.

4.1.5 Sensori utilizzati

I sensori utilizzati in questo studio sono stati posizionati in seguito ad unattenta analisi dell'area di interesse. I sensori scelti per questa applicazione sono prevalentemente di due tipologie: Sensori Standard (R) e Sensori per metalli (M). In questo studio il numero di sensori è limitato a causa della natura sperimentale dello stesso. Infatti lintera WSN in questo caso è composta da sette sensori di cui uno specifico per i metalli pesanti (M) e gli altri sei standard (R).

I sensori standard corrispondono alla versione PRO e sono in grado di analizzare lacqua, il PH, la conduttività, lORP; lossigeno disciolto, la torbidità e i solidi sospesi. Inoltre sono connessi tramite linterfaccia di comunicazione RS485 equivalente allo standard Europeo CCITT V11. Questo standard consiste nella specifica a livello fisico di una connessione seriale a due fili half-duplex e multipunto.

Il sistema di gestione del segnale è in forma differenziale ovvero la differenza tra la tensione presente sui due fili costituisce il dato in transito. Questo garantisce una maggiore robustezza per quanto riguarda la trasmissione del segnale in questione. Una polarità indica un livello logico 1 mentre quella inversa indica il livello logico 0. La differenza di potenziale deve essere di almeno 0,2 V per unoperazione valida ma qualsiasi tensione compresa tra +12 V e 7 V permette il corretto funzionamento del ricevitore. Questa specifica permette la configurazione di reti locali a basso costo e comunicazioni multipunto. Permette una velocità di trasmissione molto elevata (35 Mbit/s fino a 10 m e 100 kbit/s a 1.200 m). Dal momento che utilizza un sistema di segnalazione con una tensione non trascurabile, con una linea bilanciata tramite limpiego di un doppino (come avviene nella EIA RS-422), si possono raggiungere distanze relativamente notevoli (fino a poco più di 1.200 m).

Per quanto riguarda la struttura che protegge questi dispositivi, è IP68 ed è equipaggiata con un cavo in kevlar resistente fino a 1500N. Oltre ai sensori standard vengono utilizzati anche sensori per lidentificazione dei metalli nellacqua. Questo tipo di sensori sono specifici e garantiscono alcuni vantaggi come la capacità di registrare la presenza di Cu, Pb, ZN e Ni attraverso operazioni di voltammetria. Inoltre riescono ad avere unaccuratezza migliore per quanto riguarda le interferenze di colore nellacqua, la conduttività e la torbidità.

4.1.6 Tracciamento dell'inquinamento tramite GIS

Questo studio è stato svolto nel distretto irriguo di Taoyuan nel quale l'autorità responsabile delle risorse idriche per l'irrigazione è rappresentata dall'amministrazione locale. La fase che segue l'analisi delle transazioni attraverso la blockchain corrisponde alla mappatura dell'area interessata tramite il GIS. Questa operazione è stata supportata dalle analisi fatte in precedenza tramite il DAG sull'effettivo corso delle acque e dall'amministrazione locale che ha permesso l'identificazione delle aree amministrative lungo il percorso e informazioni sullirrigazione dei terreni agricoli come drenaggi e altri canali.

Successivamente, attraverso le informazioni contenute nel sistema blockchain, sono state mappate tutte le possibili fabbriche presenti nella zona che potrebbero essere responsabili della sostanze inquinanti rilasciate nelle acque. Infine sono stati incrociati i dati delle rilevazioni dei sensori per scremare quelle fabbriche che sicuramente potrebbero comportare il tipo di inquinamento rilevato.

4.1.7 Simulazione tramite WASP

Il sistema di simulazione della qualità dell'acqua sfrutta un'equazione di bilancio sviluppata dell'EPA statunitense, per determinare i costituenti disciolti nell'acqua. Essa tiene conto del materiale in entrata e in uscita, del carico diretto e diffuso, del trasporto advettivo e dispersivo, delle trasformazioni fisiche, chimiche e biologiche. I dati che hanno utilizzato in questo studio, provenivano in parte dal sistema di monitoraggio e dalle indagini svolte sul luogo. Per la simulazione è stata utilizzata l'equazione alle derivate parziali Runge-Kutta e l'equazione di controllo del sedimento. La calibrazione di questo modello è basata su un metodo iterativo. Le concentrazioni seguono delle interazioni consecutive che ne modificano i valori. Il metodo viene interrotto quando questi valori si avvicinano il più possibile ai valori determinati sul campo empiricamente. Si è ottenuto che il sistema è effettivamente capace di simulare la presenza di fattori inquinanti nel sistema idrico interessato.

4.1.8 Commento e risultati

I risultati di questo studio sono stati consistenti e rispettivi degli standard. Lo studio dimostra come l'implementazione della tecnologia blockchain in una rete di sensori wireless non sia solo possibile ma che apporti anche molti vantaggi dal punto di vista della sicurezza e non solo. Come citato nell'articolo di questo studio, lutilizzo di una blockchain come sistema di monitoraggio ha permesso di ottenere dati immutabili, tracciabili e di rendere il sistema trasparente.

Inoltre viene dimostrato come il sistema di monitoraggio basato su una crypto-moneta quale erano quelle citate nello studio sia possibile e che il sistema porti a dei risultati comparabili dal punto di vista empirico con quelli ottenibili tramite i più comuni sistemi in commercio basati su SQL ma donando in più le caratteristiche peculiari della discussa tecnologia blockchain. Lo studio inoltre suggerisce che questo tipo di implementazione rende possibile anche una riduzione dei costi e della quantità di sensori necessari alle rilevazioni.

In generale quindi è possibile affermare che l'utilizzo della tecnologia blockchain rappresenti una valida alternativa alle più comuni soluzioni nel campo delle reti di sensori wireless apportando inoltre notevoli vantaggi.

4.2 Will Blockchain Technology Become a Reality in Sensor Networks?

Il documento [24] citato ha l'obbiettivo di implementare una blockchain in una rete di sensori wireless teorica. Il fine di ciò è il medesimo delle altre implementazioni, ovvero aumentare la sicurezza. Come detto precedentemente, le reti di sensori wireless hanno un ampio range di utilizzo e spesso trattano informazioni sensibili e quindi necessitano di essere protette.

4.2.1 Rete di sensori in esame e blockchain

La rete di sensori wireless simulata è un tipo rete standard e quindi che porta con sé tutti i limiti derivanti. La rete è composta da nodi sensori, potenziali cluster head e il gateway. Le unità che svolgono la funzione di sensing sono unità semplici, alimentate a batteria, con scarsa memoria di archiviazione e risorse computazionali limitate. Questi dispositivi rappresentano esattamente quelli descritti più approfonditamente nel 2.3.1 . I potenziali cluster head sono nodi sensori con capacità sia computazionali che energetiche, superiori ai nodi base della rete. Essi svolgeranno il compito di tramettere i dati ricevuti dal cluster di nodi sensori al sink. Il sistema blockchain invece corrisponde alla struttura gerarchica esposta nel 3.4.1 .

4.2.2 Selezione cluster head

Per quanto riguarda invece la selezione del cluster head nello studio si è preferito non selezionarlo in base alla durata del ruolo che dovrà svolgere ma in base all'energia rimanente. Nel momento in cui questo fattore fosse in comune tra più cluster head, verrà utilizzato come criterio per la selezione, un fattore pseudo-casuale. Una volta selezionato il cluster head esso invierà un segnali di imput a i nodi sensori per riuscire, grazie al segnale di risposta, di quanti sensori esso svolgerà la mansione di cluster head. Dopo di ciò, il cluster head selezionato, comunica con gli altri cluster head nelle vicinanze e, confronta con loro determinate informazioni, tra cui il livello di energia rimanente al fine di determinare la possibilità di diventare cluster head anche dei cluster nelle vicinanze. Se dai valori confrontati non viene determinata una risposta univoca, viene riutilizzato un fattore pseudo-causale. Successivamente avviene l'instradamento del segnale fino al sink.

4.2.3 Risultati

I risultati di questo studio sono chiari. Si può notare come per quanto riguarda la durata della batteria, un sistema che utilizza una blockchain consumi almeno il 150% il consumo che una rete basata su sistemi tradizionali, avrebbe. Questo avviene a causa della necessità per un sistema blockchain di trasmettere un quantità di dati più elevata ed essendo la trasmissione dati, l'operazione che richiede il consumo di energia maggiore nei vari dispositivi, viene spiegata questa ingente quantità di energia consumata in eccesso. Inoltre anche la memoria di archiviazione necessaria in questa tipologia di soluzione supera di gran lunga quella necessaria per un sistema tradizionale, in quanto la memorizzazione dei blocchi della blockchain fa si che la memoria simulata saturi e l'intero sistema ne risenta.

4.2.4 Commento

Lo studio in questione presenta una discussione semi-teorica sull'argomento trattato. Nonostante i dati riportati suggeriscano che limplementazione di una blockchain possa risultare eccessivamente svantaggiosa, emergono soluzioni alternative capaci di risolvere questi problemi. Ad esempio, l'introduzione di nodi specializzati per l'utilizzo di una blockchain può permettere ai sistemi di operare in modo efficiente. Altre soluzioni, come quella riportata nell'esempio iniziale di questo capitolo, riconfermano la reale possibilità di implementare questa tecnologia con successo. Quello che si evince è che per implementare la soluzione blockchain in una rete di sensori, ci sia il bisogno che questa rete venga adattata allo scopo.

Conclusioni

In questo documento si esplorano due tecnologie molto diverse e si cerca di comprendere se l'unione di queste possa portare ad ottenere benefici per il servizio o se le sfide e le difficoltà legate a queste soluzioni innovative costituiscano un limite dimplementazioni invalicabile. Le reti di sensori wireless o WSN sono una tecnologia in rapido sviluppo: si osserva come i campi di utilizzo di questo tipo di soluzione di monitoraggio siano molto ampi e variegati. Le possibilità legate alle sue implementazioni, che spaziano dal monitoraggio al fine di migliorare le condizioni di un luogo di lavoro al monitoraggio di strutture o ambienti inaccessibili, creano un forte interesse nello sviluppo di soluzioni di questi tipo. Ovviamente, questa tecnologia così utile e versatile è accompagnata da difficoltà tecniche considerevoli. Il consumo di energia, la gestione della rete e la sicurezza dei dati costituiscono le sfide maggiormente interessanti. In questa ottica, si riporta in questo documento l'analisi dello stato dell'arte della possibilità di introdurre un sistema sicuro come quello della blockchain all'interno delle reti dei sensori wireless. La blockchain è una tecnologia distante dalle applicazioni ingegneristiche. La sua storia e l'ambito per cui è impiegata maggiormente ovvero la finanza fa sì che le caratteristiche peculiari vengano poste in secondo piano identificandola come appartenente ad un altro campo di studio. Nonostante ciò grazie proprio alla particolarità delle sue caratteristiche stanno nascendo sempre più applicazioni in ambiti diversi da quello finanziario.

In questa trattazione si evidenzia come l'utilizzo della tecnologia blockchain applicato alle reti di sensori wireless porti dei reali benefici al servizio, garantendo una sicurezza dei dati inarrivabile per i metodi tradizionali. Anche in questo tipo di soluzioni sorgono alcune problematiche. Infatti, la tecnologia blockchain comporta una difficile implementazione per quei sistemi che necessitano di un risparmio energetico aggressivo. L'architettura della tecnologia potrebbe comportare un peggioramento del life time del sistema. Nonostante ciò si osserva come sia a livello sperimentale nel terzo capitolo che praticamente nel quarto l'implementazione di questa tecnolo-

gia non solo sia possibile ma porti con sé numerosi vantaggi e benefici sia dal punto di vista della sicurezza dei dati sia nella gestione del sistema e possibilmente anche nel numero di sensori necessari alla rete.

Quindi ciò che si può trarre da questo documento è che i benefici di una rete blockchain in una rete di sensori wireless ne giustifichino l'impiego l'interesse e la ricerca in questo campo.

4.3 Ringraziamenti

Sono passati molti anni ormai da quel primo giorno in università. Avevo aspettato quel momento per tanto tempo e volevo dare il massimo per riuscire finalmente ad accedere al futuro che desideravo. Tutto sarebbe dovuto venire naturale e spontaneo ma la vita non mi ha portato troppe volte a percorrere le strade battute dai miei pensieri. Gli anni sono passati attraverso tanti cambiamenti e per un periodo sembra che tutto mi stesse sfuggendo di mano. Non è stata la carriera universitaria più brillante mai esistita ma alla fine, sono contento. Sono contento perchè ho capito come fare, non solo a passare gli esami ma ho veramente capito le cose importanti che ti permettono di poter affrontare qualsiasi sfida ti si ponga davanti, e nonostante per alcuni sia banale, io l' ho dovuto capire a mie spese. Ovviamente sto parlando delle persone che hai intorno. Ho tentato ogni strada, prima di arrivare a quella conclusione. Ogni strada per poter superare quegli esami. Dallo studiare di più con una routine, a studiare di qualità, dal fare attività fisica per scaricare lo stress alle tecniche di concentrazione, ma nulla ha poi avuto gli effetti sperati. Grazie a mia madre ho preso ripetizioni, poche ore, quelle necessarie a quadrare un cerchio che io disegnavo storto o senza qualche asticella. Ma quelle ripetizioni hanno aggiunto l' ultimo pezzo ad un puzzle che si stava formando pian piano. Avevo capito che non dovevo scappare dalla tensione ma che anzi doveva essere mia amica, e che con qualcuno al mio fianco, non c'erano più difficoltà ma solo passaggi da seguire per arrivare all'obbiettivo. Se questo è vero nello studio, lo è sicuramente nella vita. Quindi iniziamo. Ringrazio in primis, la mia famiglia, che mi ha permesso di arrivare fino a qui e che nonostante le difficoltà nel percorso mi ha sempre sostenuto, non facendomi mancare mai niente. Ringrazio mia sorella Federica, per cui farei qualsiasi cosa e che in questi anni è stata sempre dalla mia parte. Senza di lei, non sarei la persona che sono oggi e questo traguardo lo voglio condividere con lei. Non potrei mai ringraziarla abbastanza. Ringrazio poi a pieni polmoni, la mia coinquilina Ines, che è diventata più del mio punto di riferimento, una persona senza la quale non sarebbe stato

possibile tutto questo. La ringrazio per ogni secondo passato al telefono e per ogni risata che potrebbe rompere qualsiasi muro buio la vita mi possa mettere davanti. Non potrò mai restituirle quello che mi ha donato in questi anni. Anni magici quelli a Vicenza, in cui si è instaurato un rapporto più unico che raro e che ha cambiato per sempre la mia vita. Ringrazio infatti ora la mia coinquilina Rebecca e il mio coinquilino Iacocco, due persone che considero parte della mia famiglia e con cui vivrei per il resto dei miei giorni. Ringrazio il mio amico Massimo che oltre ad essere stato fondamentale per parecchi esami in questi anni, è sicuramente qualcuno che vorrei ci fosse sempre stato nella mia vita. Un grande amico sincero e necessario. Ringrazio per ultimi ma non per importanza e nello specifico i miei amici Valentina, Giovanni, Daniela e Alessandro che mi hanno accompagnato lungo tutto questo percorso, incoraggiandomi, studiando insieme e rendendo tutto più semplice e leggero anche quando di leggero c'era ben poco. Quindi grazie per il passato e non vedo l' ora di vivere il futuro che ci aspetta insieme. Inoltre ringrazio in generale i miei amici e tutti coloro che hanno attraversato la mia vita e auguro a me stesso di non dimenticarmi mai di questa esperienza e di ciò che ho imparato.

Bibliografia

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," May 2009.

[2] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, pp. 644–654, November 1976.

[3] S. Haber and W. S. Stornetta, "How to time-stamp a digital document.," in *CRYPTO* (A. Menezes and S. A. Vanstone, eds.), vol. 537 of *Lecture Notes in Computer Science*, pp. 437–455, Springer, 1990.

[4] A. Back, *Hashcash*, May 1997.

[5] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in *2017 IEEE technology & engineering management conference (TEMSCON)*, pp. 137–141, IEEE, 2017.

[6] E. Tijan, S. Aksentijević, K. Ivanić, and M. Jardas, "Blockchain technology implementation in logistics," *Sustainability*, vol. 11, no. 4, p. 1185, 2019.

[7] C. Gupta and A. Mahajan, "Evaluation of proof-of-work consensus algorithm for blockchain networks," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–7, IEEE, 2020.

[8] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, "Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities," *IEEE Access*, vol. 7, pp. 85727–85745, 2019.

[9] J. Golosova and A. Romanovs, "The advantages and disadvantages of the blockchain technology," in *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)*, pp. 1–6, IEEE, 2018.

[10] M. Di Pierro, "What is the blockchain?," *Computing in Science & Engineering*, vol. 19, no. 5, pp. 92–95, 2017.

[11] Wikipedia, "Funzione crittografica di hash — wikipedia, l'enciclopedia libera," 2022. [Online; in data 22-dicembre-2022].

[12] Wikipedia, "Albero di merkle — wikipedia, l'enciclopedia libera," 2022. [Online; in data 22-dicembre-2022].

[13] Wikipedia, "Problema dei generali bizantini — wikipedia, l'enciclopedia libera," 2019. [Online; in data 22-dicembre-2022].

[14] originstamp, "Public vs. consortium vs. federated vs. private blockchain."

[15] pedrosoftz, "Storia ed evoluzione degli smart contract," 2017.

[16] Wikipedia, "Wireless sensor network — wikipedia, l'enciclopedia libera," 2022. [Online; in data 22-dicembre-2022].

[17] V. Jindal, "History and architecture of wireless sensor networks for ubiquitous computing," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 7, no. 2, pp. 214–217, 2018.

[18] W. Wang, Q. Chen, Z. Yin, G. Srivastava, T. R. Gadekallu, F. Alsolami, and C. Su, "Blockchain and puf-based lightweight authentication protocol for wireless medical sensor networks," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8883–8891, 2021.

[19] M. T. Lazarescu, "Design of a wsn platform for long-term environmental monitoring for iot applications," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, no. 1, pp. 45–54, 2013.

[20] M. Miettinen and N. Asokan, "Ad-hoc key agreement: A brief history and the challenges ahead," *Computer Communications*, vol. 131, pp. 32–34, 2018. COMCOM 40 years.

[21] G. N. Nguyen, N. H. Le Viet, A. F. S. Devaraj, R. Gobi, and K. Shankar, "Blockchain enabled energy efficient red deer algorithm based clustering protocol for pervasive wireless sensor networks," *Sustainable Computing: Informatics and Systems*, vol. 28, p. 100464, 2020.

[22] Wikipedia, "Eia rs-485 — wikipedia, l'enciclopedia libera," 2020. [Online; in data 22-dicembre-2022].

[23] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in iot," *Procedia Computer Science*, vol. 132, pp. 1815–1823, 2018.

[24] J. Marchang, G. Ibbotson, and P. Wheway, "Will blockchain technology become a reality in sensor networks?," in *2019 Wireless Days (WD)*, pp. 1–4, IEEE, 2019.

[25] Y.-P. Lin, H. Mukhtar, K.-T. Huang, J. R. Petway, C.-M. Lin, C.-F. Chou, and S.-W. Liao, "Real-time identification of irrigation water pollution sources and pathways with a wireless sensor network and blockchain framework," *Sensors*, vol. 20, no. 13, p. 3634, 2020.

[26] W. She, Q. Liu, Z. Tian, J.-S. Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," *IEEE Access*, vol. 7, pp. 38947–38956, 2019.

[27] A. Mubarakali, "An efficient authentication scheme using blockchain technology for wireless sensor networks," *Wireless Personal Communications*, pp. 1–15, 2021.

[28] S. Verma, S. Kaur, R. Manchanda, and D. Pant, "Essence of blockchain technology in wireless sensor network: a brief study," in *2020 International Conference on Advances in Computing, Communication & Materials (ICACCM)*, pp. 394–398, IEEE, 2020.

[29] I. Buldin, M. Gorodnichev, S. Makhrov, and E. Denisova, "Next generation industrial blockchain-based wireless sensor networks," in *2018 Wave Electronics and Its Application in Information and Telecommunication Systems (WECONF)*, pp. 1–5, IEEE, 2018.

[30] "Differenze sistemi centralizzati, decentralizzati e distribuiti," 2022.

[31] N. Goni, S. Saad, and A. Ibrahim, *A P2P Optimistic Fair-Exchange (OFE) Scheme for Personal Health Records Using Blockchain Technology*, pp. 1–21. 06 2020.

[32] “Funzione di hash,” 2022.

[33] A. M. Chandranshu Gupta, “Evaluation of proof-of-work consensus algorithm for blockchain networks,” 2020.

[34] “Albero di merle,” 2023.

[35] “The problem of the byzantine generals,” 2020.

[36] “Smart sensor networks : Technologies and,” 2010.

[37] “Sensor node,” 2021.

[38] H. Aboelfotoh, S. Iyengar, and K. Chakrabarty, “Computing reliability and message delay for cooperative wireless distributed sensor networks subject to random failures,” *Reliability, IEEE Transactions on*, vol. 54, pp. 145 – 155, 04 2005.

Elenco delle figure